بـلـديـة عرابـة
ص.ب 10 الـد الـة 30812
تـلـفـون 04-8789666 טלפון

עיריית עראבה
30812 ת.ד 10 מיקוד
פקס 04-6747291 فـا كس

www.arraba.muni.il

דוח מבקר העירייה

לשנת 2023

بلدية عرابة
ص.ب 10 الدالة 30812
تلفون 04-8789666 טלפון

עיריית עראבה
30812 ת.ד 10 מיקוד
פקס 04-6747291 פאקס

www.arraba.muni.il

תוכן עניינים

بلدية عرابة
ص.ب 10 الدالة 30812
تلفون 04-8789666 טלפון

עיריית עראבה
30812 ת.ד 10 מיקוד
פקס 04-6747291 פאקס

www.arraba.muni.il

01/04/2024

לכבוד
דר אחמד נסאר
ראש העירייה

נכבדי ראש העירייה ,

הנדון : <u>דוח מבקר העירייה</u>

ראשית, ברצוני לברך אותך על היבחרך לתפקיד ראש העירייה עראבה בבחירות שנערכו לאחרונה במרץ 2024, ולאחל לך הצלחה רבה במילוי תפקידך כראש העיר בעשייה למען תושבי העיר.
בפניך עומדים אתגרים ועבודה רבה, דרך חדשה לעבר שגשוג והצלחה. לרבות מימוש כל התוכניות שלך לעתיד טוב יותר לעירנו וילדינו .

הנני מתכבד להגיש את דוח מבקר העירייה לשנת 2023, בהתאם לסעיף 170ג' לפקודת העיריות .

1. בהתאם לתוכנית עבודה רב שנתית נערכה ביקורת במהלך שנת 2023 בגין הנושאים הנ"ל .

- ביקורת פרויקטים במחלקת החינוך .
  1. ביקורת צהרוני ניצנים .
  2. ביקורת המחלקה לקידום הנוער .
- ביקורת מחלקת רכש .
- ביקורת ביטוחי העירייה .
- ביקורת הגנת הפרטיות ואבטחת מידע :
  1. ביקורת הגנת הפרטיות .
  2. דוח מבדקים טכנולוגיים .
  3. דוח מבדק חדירה תשתיתי .

2. אני מגיש לעיונכם את דוח הביקורת ואת ממצאי הביקורת המפורטים בדוח שלהלן.

3. דוח הביקורת מצביע על ליקויים ואי סדרים מִנהליים בתהליכי העבודה ובפיקוח עליהם.

4. דוח הביקורת אינו דן בכלל הפעולות של המחלקה, אלא באלה שבוקרו בלבד, וההתמקדות הייתה במספר מסוים של נושאים.

5. אני מודה לכלל עובדי המחלקות על שיתוף הפעולה המלא בהכנת דוח הביקורת. אני מוצא לנכון לציין לחיוב את שיתוף הפעולה המלא לו זכיתי מצד המבוקרים במהלך הביקורת , ומבקש להודות ולהביע את מלוא הוקרתי לעמיתי בעבודה על העזרה שהושיטו לי.

בהתאם לסעיף 170 ג' לפקודת העיריות :

1. המבקר יגיש לראש הרשות אחת לשנה דוח על ממצאי הביקורת שערך , בעת הגשת הדוח ימציא המבקר העתק ממנו לוועדת הביקורת .
2. בתוך שלושה חודשים מיום קבלת דוח המבקר ,יגיש ראש הרשות לוועדת הביקורת את הערותיו על הדוח , וימציא לעירייה העתק מהדוח בצירוף הערותיו .
3. וועדת הביקורת תדון בדוח המבקר ובהערות ראש המועצה הרשות ותגיש למועצה לאשר את סיכומיה והצעותיה בתוך חודשיים מיום שנמסר לה הערות ראש הרשות .
4. תוך חודשיים מן היום שבו הגישה ועדת הביקורת את סיכומיה והצעותיה תקיים המועצה דיון מיוחד בהם ותחליט בדבר אישור ההצעות .
5. סעיף 170 ו' נקבע כי לא יפרסם אדם דוח ביקורת שנערך ע"י מבקר העירייה או את תוכנו לפני שחלף המועד שנקבע להגשתו לעירייה .

בכבוד רב
סאמי ח'וטבא
מבקר העירייה

סודי – אין לפרסם נתונים מדוח זה,
עד למועד המוגדר בחוק לכינוס מליאת מועצת העיר לדיון בדוח

بلدية عرابة
ص.ب 10 الدالة 30812
تلفون 04-8789666 טלפון

עיריית עראבה
30812 ת.ד 10 מיקוד
פקס 04-6747291 פא כס

www.arraba.muni.il

עיריית עראבה

לשכת מבקר העירייה

פרק א

ביקורת

פרויקטים בחינוך

بلدية عرابة
ص.ب 10 الدالة 30812
تلفون 04-8789666 טלפון

עיריית עראבה
30812 ת.ד 10 מיקוד
פקס 04-6747291 פאקס

www.arraba.muni.il

תוכן העניינים :

1. כללי

דוח מבקר המדינה משנת 2012 בנושא 'סל שירותים מוניציפליים ברשויות המקומיות' מתייחס לשירותים השונים שהרשות המקומית מעניקה לתושביה וההשפעה שלהם על איכות חייהם:

"על הרשות המקומית לדאוג לפיתוח היישוב ולהעניק לתושבים שירותים מסוגים שונים כדי להבטיח תנאי חיים נאותים.....

לשירותים שמספקות הרשויות המקומיות השפעה ישירה על איכות חייהם ורווחתם של תושביהן. תהליכי הביזור והעברת תחומי פעילות שונים מידי השלטון המרכזי לידי השלטון המקומי, חיזקו את הקשר שבין ניהול תקין של הרשויות המקומיות, מבחינת ההיקף והאיכות של השירותים שהן מעניקות לתושביהן, ובין רמת חייהם של התושבים".

החוקים והתקנות הקיימים לא מפרטים את סל שירותים שהרשות המקומית מחויבת להעניק לתושביה, כך שכל רשות דואגת לשירותים על פי מדיניותה, צרכיה ותקציבה.

עיריית עראבה, באמצעות מחלקת החינוך, מפעילה את מערך צהרוני ניצנים בעיר כולל צהרוני חופשות.

העירייה מפעילה 84 מסגרות בצהרונים, עבור 2,247 ילדים, לפי החלוקה הנ"ל:

סוג מסגרת	גני ילדים	בתי ספר	סה"כ	הערות
מספר מסגרות (לפי סמל מוסד)	51	7	58	מתוכם 12 גנים, בהם משתתפים 325 ילדים, מופעלים על ידי עמותות.
מספר ילדים מקסימלי בתוכנית	1,323	924	2,247	

כלל הפעילות מתקיימת בשטחי מוסדות החינוך העירוניים- גני ילדים ובתי ספר, כאשר שעות הפעילות כדלקמן:

- בתי ספר- תחילת פעילות בשעה 13:30 וסיום הפעילות בשעה 15:30. בבתי הספר הפעילות מתקיימת על ידי המורה, ללא חוגי העשרה הניתנים על ידי ספק חיצוני.
- גני ילדים- תחילת פעילות בשעה 14:00 וסיום הפעילות בשעה 16:00. בגני הילדים מתקיימים חוגי העשרה על ידי ספק חיצוני בתחום תנועה ואומנות פעמיים בשבוע. יתר הפעילות מופעלת באמצעות גננת הצהרון.

על פי דיווחי רכזת התוכנית, הגב' עביר בדראנה, כוח האדם בתוכנית ניצנים מסתכם ב- 147 עובדות: 45 מורות בבתי הספר, 51 גננות בגני הילדים ו- 51 סייעות בגני הילדים.

פעילות ניצנים עוגנה במספר החלטות ממשלה:

- החלטת ממשלה שמספרה 4088 מחודש ינואר 2012 אישרה סבסוד מסגרות חינוך החל מהשעה בה מסתיימת מסגרת החינוך הפורמלי ועד השעה 16:00, אשר יכללו, בין היתר, חוגי העשרה, פעילות פנאי ועוד.

בנוסף, נקבע בהחלטת הממשלה, כי הסבסוד בשעות אחה"צ ימומן במלואו במוסדות הנמצאים בישובים המדורגים בשלושת האשכולות הראשונים בדירוג החברתי-כלכלי של הלשכה המרכזית לסטטיסטיקה, וכי

חלוקת המימון בין הגופים השונים ובין ההורים במוסדות הנמצאים בישובים המדורגים באשכולות 4-10 תהיה דיפרנציאלית, כאשר מימון המדינה יהיה גבוה יותר ברשויות באשכולות הנמוכים.

- החלטת ממשלה מס׳ 2659 מחודש מאי 2017, במסגרתה הונחה משרד החינוך להרחיב את תוכנית ניצנים לסבסוד מסגרות לימודיות נוספות בשעות אחה״צ, לגני הילדים הציבוריים ולבתי הספר המתוקצבים ע״י משרד החינוך. כן נקבע, כי מרכיבי התוכנית יגובשו ויפוקחו ע״י משרד החינוך, ובכלל זה : רמת השירות, המענה החינוכי והסטנדרטים הפדגוגיים.

1.1 מטרת הביקורת

לבחון את נאותות פעולות העירייה בהפעלת תוכנית צהרוני ניצנים וקידום נוער תוך הקפדה על הוראות משרד החינוך.

1.2 מתודולוגיה

- פגישות עם נציגי מחלקת חינוך, כולל מנהל המחלקה, רכזת צהרונים, מנהל מחלקת ילדים ונוער בסיכון ומנהל היחידה לקידום נוער.
- סקירת קבצים ומסמכים רלוונטיים, כולל דוחות מעבדה ודוחות תקציביים למשרד החינוך, כרטסות הנהלת חשבונות ועוד.

1.3 המסגרת הנורמטיבית

- אוגדן בעלי תפקידים לעובדי חינוך, נוער וקהילה- משרד החינוך, מנהל חברה ונוער, 2023 (להלן : ״**האוגדן**״) ;
- ״מודל תוכנית עבודה אפקטיבית- קווים מנחים לרשויות מקומיות״ , שפורסם על ידי משרד הפנים בשנת 2016 ;
- החלטות ממשלה שמספרן : 4088, 2659.
- הפעלת מסגרות משלימות בשעות אחר הצהריים (צהרונים) בגני ילדים וברשויות מקומיות באשכולות 4-10, מבקר המדינה- 2014 ;
- חוק לפיקוח על הפעלת צהרונים, תשע״ז-2017 ;
- הנחיות להזנה במוסדות חינוך, בתי ספר וגני ילדים, משרד הבריאות 2005 ;
- מידע על עלויות הפעלת צהרונים, מרכז המחקר והמידע- כנסת ישראל, 2017 ;
- הזנה וחינוך לתזונה נכונה במוסדות החינוך, משרד החינוך 2023.

2. עיקרי ממצאים והמלצות

סעיף+ שם הפרק	ממצא	המלצה	תגובת מבוקרים
3 מבנה ארגוני	נמצא כי מורות מובילות וגננות מובילות אינן ממלאות את דף הנוכחות של ילדי הצהרונים במועדים קבועים ואף אינן מציינות יציאה מוקדמת של ילדים מהמסגרת.	מומלץ, כי רכזת תוכנית ניצנים בעיריית עראבה תקפיד, כי כל אחת מעובדות הצהרונים תבצע את כלל המשימות הנדרשות בהוראות משרד החינוך (פרק ה.1 לקריטריונים) , בפרט כאשר מדובר ברישום נוכחות תלמידים. הביקורת מעירה, כי רישום כוזב יגרור סנקציות כספיות משמעותיות של משרד החינוך (ראה בהרחבה פרק 11- דיווח ועמידה בהוראות משרד החינוך).	
4 תוכנית עבודה	תוכניות העבודה אינן כוללות תקציב. תוכניות העבודה מוצגת בפורמט של משרד החינוך, אולם לא קיים פורמט תוכנית עבודה של העירייה, הכולל מטרות ויעדים מדידים, הכוללים אבני דרך לצמצום פערים העולים בתוכנית, דוגמת: רישום נוכחות והערות לגבי יציאה מוקדמת של ילדי התוכנית, בחינת השתתפות הורית בתשלום התוכנית וכדומה.	מומלץ לערוך תוכנית עבודה שנתית בפורמט מובנה של העירייה, אשר תכלול, בין היתר, את הנושאים הבאים: תקצוב תוכניות פעילות; טווח שעות לרישום נוכחות תלמידים במסגרת והערות לילדים המסיימים בשעה מוקדמת; תשלום הורים.	
5 נהלים	במחלקת חינוך לא קיים נוהל כתוב, אשר מסדיר את פעילותה השוטפת בכל נושא צהרונים ויחידת קידום נוער.	מומלץ לערוך נהלי עבודה בנושא צהרונים ויחידת קידום ביניהם: נהלי הרשמה וגבייה; נוהל רישום ושיבוץ לצהרונים; נוהל תפעול צהרונים; נהלי גריעה מפעילות וזיכוי תשלומים; נהלי דיווח למשרד ממשלה רלוונטיים	

סעיף+ שם הפרק	ממצא	המלצה	תגובת מבוקרים
6 תקציב	בשנת 2021, היה ביצוע חסר הן בהכנסות והן בהוצאות. סביר שההסבר לכך הוא משבר הקורונה, שבגינו מסגרות החינוך היו סגורות חלק מהשנה. הביקורת מעירה, כי משבר הקורונה החל ב 3/2020. לאור זאת, במועד גיבוש התקציב, היה כבר ידוע כי לא כולו ימומש. יתרה מכך, לאור העובדה שהתקיים סגר מלא בחודש ינואר ובחלק הראשון של פברואר, היה ידוע כבר במועד זה, כי לא כל התקציב ימומש והיה מקום לעדכון תקציבי לאורך השנה בהתאם למצב בפועל.		
צהרונים			
8 ועדת היגוי	כי בניגוד להנחיות משרד החינוך בנוגע להפעלת תוכנית ניצנים, התכנסה ועדת ההיגוי פעם בשנה ולא כפי שנדרש בהוראות- 3 פעמים בשנה. עוד עולה, כי בניגוד להנחיות, לא מוזמנים נציגי הורים לוועדת ההיגוי הרשותית.	מומלץ, כי העירייה תפעל על פי הוראות משרד החינוך ותכנס את ועדת ההיגוי הרשותית 3 פעמים בשנה, לפחות. עוד מומלץ, להקפיד להזמין לישיבות ועדת ההיגוי את נציגי ההורים, דוגמת נציגי הנהגת הורים במסגרות החינוך.	
9 הכשרות מקצועיות לצוותי חינוך	מנתונים שהועברו לביקורת על ידי רכזת תוכנית ניצנים, בתוכנית מועסקות 147 עובדות, בעוד שמנתוני טבלה מספר 1 (הדרכות עזרה ראשונה) רק 125 עובדות עברו את ההכשרה. כאמור, על פי הוראות משרד החינוך, על כל העובדות בתוכנית לעבור הכשרת עזרה ראשונה.	הביקורת ממליצה, לנהל מעקב אחר העובדות שלא עברו הכשרה פדגוגית מתאימה בכל שנת פעילות וככל והכשרה זו לא הושלמה, יש לשקול המשך העסקה. עוד מומלץ, לבחון את האפשרות לקיים את ההכשרות גם במהלך שנת הפעילות, כך שככל ועולות סוגיות נוספות, המצריכות הנחיה	

סעיף+ שם הפרק	ממצא	המלצה	תגובת מבוקרים
	עוד עולה, כי בשתי מסגרות חינוך בית ספריות ובשלושה גני ילדים לא כל העובדות עברו את ההכשרה הרלוונטית, הנדרשת על פי הוראות משרד החינוך. יודגש כי כל ההנחיה הפדגוגית מתקיימת בחודשים נובמבר- דצמבר וביתר שנת הפעילות לא מתקיימות הדרכות והנחיות.	והדרכה, יינתן מענה לעובדות בתוכנית ניצנים.	
10.1 תפריט בצהרונים	התפריט המפורסם בלוח הצהרון אינו מתאים לתזונת הילדים ביום סיור הביקורת, כנדרש בהוראות משרד הבריאות.	הביקורת ממליצה, כי רכזת הצהרונים תקפיד לאשר מול ספקי הקייטרינג של העירייה את מרכבי ארוחת הצהריים של ילדי הצהרונים. ככל ונדרש לערוך שינוי, יש לאשר את השינוי לספקי ההזנה בכתב.	
10.2 פיקוח תברואתי של הרשות המקומית	בראיון שערכה הביקורת עם רכזת תוכנית ניצנים, עלה, כי במהלך שנות תפקידה לא נדרשה לדווח לווטרינר הרשותי על מוסדות חינוך בהם אמורה להתקיים הזנה וככל והדבר נעשה על ידי חברת מילג"ם, היא אינה מקבלת דיווח על הנושא.	הביקורת ממליצה, לבחון מול הווטרינר הרשותי, האם מתקבלים לידיו דיווחים בנוגע למוסדות חינוך בהם מתקיימת הזנה וככל שכן, לבדוק האם ערך פיקוח תברואתי. עוד מומלץ, לבחון את האפשרות לממשק עם הווטרינר הרשותי, על מנת לוודא כי דיווחים אלה אכן מתקבלים וכיצד הוא פועל מול מוסדות החינוך, חברת מילגם ו/או חברות ההסעדה.	
11 דיווח ועמידה בהוראות משרד החינוך	העירייה מדווחת למשרד החינוך על כלל המשתתפים בתוכנית וזאת למרות שלא כל הילדים משתתפים בתוכנית ניצנים מדי יום, גם אם נרשמו. יודגש, כי בפרק 14 (מדגם הביקורת) נמצאו נתונים על דיווחים	מומלץ, כי העירייה תבחן מול משרד החינוך, את אופן דיווח הנוכחות, במקרים בהם ילדים יוצאים לביתם כחצי שעה לאחר תחילת התוכנית. הביקורת סבורה, כי ככל ונתוני הנוכחות	

סעיף+ שם הפרק	ממצא	המלצה	תגובת מבוקרים
	שגויים של מספרי תלמידים ו/או היעדר של רישום נוכחות תלמידים. ליקויים אלו פוגמים בדיווח נתוני אמת למשרד החינוך ומהווים סיכון תקציבי עבור העירייה, אשר מסתכנת בקיזוז תשלומים עבור התוכנית ממשרד החינוך. רכזת תוכנית ניצנים בעירייה מסרה, כי במהלך השבוע היא עורכת ביקורי שטח במסגרות ואינה רושמת את ממצאיה מהסיור, אלא מנהלת רישום של תאריך ושעה בו ערכה סיור במסגרות ניצנים. מדיווחי תוצאות בקרת השטח, שערך משרד החינוך במסגרות ניצנים בעירייה (טבלה 2), עולה, כי קיימים פערים גדולים בדיווחי העירייה לגבי נוכחות ילדים בתוכנית, לבין הנתונים שנמצאו בבקרות השטח של משרד החינוך. הביקורת סבורה, בהמשך לסיור שערכה במסגרות התוכנית בעיר, כי קיים פער בין מספר הילדים המשתתפים בשעת התחלת התוכנית, כלומר 13:30 בבתי הספר ו- 14:00 בגני הילדים, למספר המשתתפים בתוכנית בשעות מאוחרות יותר. הדבר עלה באופן מובהק בסיור הביקורת, כאשר ילדים נלקחו על ידי הוריהם כחצי שעה מתחילת שעת הפעילות, דבר המשפיע על מספרי הילדים, גם בבדיקות משרד החינוך.	יירשמו בשעת תחילת הפעילות, תוך ציון הערות לגבי ילדים שיצאו במהלך הפעילות, ניתן יהיה להבהיר את הסוגייה באופן מיטבי למשרד החינוך, כך שהקיזוז בגין הפעילות יקטן. מומלץ, כי רכזת התוכנית תערוך בקרות שטח רצופות, בכל אחת ממסגרות ניצנים, ותתעד את הסיור ואת ממצאיו, בפרט בנוגע לנוכחות ילדים במסגרות.	
12 גבייה	העירייה אינה גובה מההורים בגין השתתפות ילדיהם בצהרונים.	הביקורת ממליצה לעירייה, לגבות מההורים סכום של 50 ₪ בחודש,	

סעיף+ שם הפרק	ממצא	המלצה	תגובת מבוקרים
	המשמעות היא, שקיימת פגיעה בהכנסות העירייה בגין ההשתתפות. מדיווחי העירייה למשרד החינוך בשנת 2023, עולה כי בשנה זו השתתפו בצהרונים כ- 2,240 ילדים. סכום ההשתתפות של העירייה עומד על כ- 100 אלפי ₪ לחודש.	כפי שמוגדר בהוראות משרד החינוך, בגין השתתפות ילדיהם. יוער, כי מדובר בהכנסה שנתית של מעל מיליון ₪. יתרה מכך, הביקורת סבורה, כי התשלום גם מהווה דמי רצינות. העובדה שההורים כלל לא משלמים ולו תשלום מינימאלי, מעודדת רישום לצהרונים גם של ילדים, שלהוריהם אין כל כוונה לרשום אותם לצהרון ובכך גדל הנזק לעירייה, בגין אי הגעה של ילדים לצהרון.	
13 משוב	עיריית עראבה אינה עורכת משובי שביעות רצון בקרב הורי הילדים, השוהים בצהרונים המצויים בתחום שיפוטה. רכזת הצהרונים שולחת אחת לתקופה סקר באמצעות אפליקציית וואטסאפ לעובדות התוכנית, לשם קבלת משוב שביעות רצון. יודגש כי בשיחה שקיימה הביקורת עם מספר גננות בעת הסיור שערכה, נמסר כי סקר זה אכן מועבר, אולם מי שעונה עליו הן הגננות עצמן, מבלי לערוך סקר בקרב הורי הילדים.	הביקורת ממליצה, לבחון את האפשרות, לערוך משוב שביעות רצון מפעילות הצהרונים בקרב הורי הילדים המשתתפים בפעילות, המהווה כלי עזר חשוב, בבחינת המצב בפועל ואף נותן כלים לשיפור השירות.	
14 מדגם הביקורת	1. אין בעירייה נוהל קבוע, בנוגע לשעת בדיקת נוכחות ורישום בתוכנית ניצנים. מתוך 10 מסגרות בהן סיירה הביקורת, ב- 7 לא מלאו המורות/גננות דף נוכחות תלמידים. בנוסף, ב- 3 מסגרות בהן דיווחו נוכחות, נמצא כי מספר התלמידים לא זהה לספירת הביקורת.	מומלץ, כי רכזת תוכנית ניצנים בעירייה תפיק דוח נוכחות זהה לכלל מסגרות החינוך ותנחה לגבי שעת בדיקת ורישום נוכחות, אופן דיווח על ילדים שיוצאים לפני שעת הסיום וכדומה. מומלץ, כי העירייה תקפיד על הזנת ילדי הצהרונים כמופיע	

סעיף+ שם הפרק	ממצא	המלצה	תגובת מבוקרים
	2. בכל המסגרות בהן סיירה הביקורת, ספקי המזון סיפקו את אותו האוכל ולא בהתאם לתפריט שמוצג בלוח הצהרון והוצג בפני הביקורת. 3. לוח צהרון- בהוראות משרד החינוך לא קיימת חובה ללוח צהרון, יחד עם זאת, בכל אחד מגני הילדים קיים לוח משעות פעילות הבוקר, בו מפורסם תפריט הצהרון, אשר מועדי הסעודות בו נמצאו לא בתוקף. 4. תיק צהרון- בהוראות משרד החינוך לא קיימת חובה לתיק צהרון, יחד עם זאת, תיק זה יעזור בריכוז כלל הנתונים להם נזקקת המורה המובילה ו/או גננת מובילה להפעלת תוכנית ניצנים, בפרט כאשר חלק גדול של העובדות בתוכנית, אינן מועסקות במסגרת החינוכית בשעות הבוקר. 5. הביקורת מעירה, כי במהלך הסיור שערכה בגן אלנור, נשלחה ילדה מהמסגרת לבדה אל רכב האם. לשאלת הביקורת ענתה הגננת, כי אין הנחיות בנושא וכי האם לא יכלה להגיע לאיסוף מהכניסה לגן. 6. יודגש כי אצל חלק מהמורות בכיתות ב' הוזמנו מספר מנות קטן ממספר הילדים. הדבר מעיד על כך, שמנות האוכל שהוזמנו עבור המסגרת אינו מתאים למספר הילדים במסגרת, ועל כך, שמספר התלמידים המדווחים למשרד החינוך אינו עומד בקנה אחד עם	בתפריט וככל ויש שינוי, יימסר אישור בכתב לחברות המספקות את ההזנה במסגרות. יש להקפיד לרשום לצהרון רק את כמות הילדים האמיתית הידועה למפעילות הצהרונים. כאשר גננת או מורה מקבלת הודעה על היעדרות צפויה של ילד, יש להורידו מהמצבת לצורך הזמנת כמות הארוחות. עוד מומלץ, כי רכזת התוכנית 'תמנף' את המצאות לוח צהרון ותפרסם בו מידע להורים, דוגמת: תוכנית הפעילות, תפריט מעודכן, הודעות בשעת איסוף ילדים מהמסגרת, נהלי המחייבים את ההורים ואת העובדות ועוד. בנוסף, מומלץ כי יוכן תיק צהרון לכל אחת מהמסגרות, שיכלול, בין היתר את הפרטים הבאים: רשימת ילדים, רשימת הורי ילדים ומספרי טלפון, רשימת ילדים עם רגישויות, וכדומה.	

סעיף+ שם הפרק	ממצא	המלצה	תגובת מבוקרים
	מספר התלמידים שהעירייה מצפה בפועל שיגיעו למסגרת. לדוגמה: בכיתה ב' (רוז) דווח למשרד החינוך על 20 תלמידים, בפועל ביום הביקורת היו במסגרת 12 תלמידים וסך מנות האוכל שנמצאו במסגרת היו 15. ככל וכל 20 התלמידים היו מגיעים לצהרון ניצנים, הרי שהיו חסרות מנות ל- 5 תלמידים.		
היחידה לקידום נוער			
2.1 השכלה והכשרות מקצועיות	למנהל מחלקת ילדים ונוער בסיכון ומנהל יחידת קידום נוער קיימות תעודת הכשרה רלוונטיות לתפקידם, המאושרות על ידי מנהל חברה ונוער. יחד עם זאת, הביקורת מציינת כי לא קיבלה לעיונה אסמכתאות המעידות על השכלה רלוונטית לתחום העיסוק שלהם ואף לא הוצגו בפניה אישורי משטרה, כי אין מניעה להעסקת בגיר בעבודה במוסד חינוכי.	מומלץ כי העירייה, באמצעות מחלקת משאבי אנוש ושכר, תוודא כי לבעלי התפקידים הנ"ל קיימים בתיק האישי אישורי השכלה רלוונטיים לתפקידם ואישורי משטרה המעידים על אי מניעת העסקתם כנדרש בחוק.	
3 תוכנית עבודה	תוכנית עבודה של היחידה לקידום נוער לא כוללת תקציב לכל אחת הפעילויות המתקיימות ביחידה. תוכנית העבודה מוצגת בפורמט של משרד החינוך, אולם לא קיים פורמט תוכנית עבודה של העירייה, הכולל יעדים מדידים לצמצום נשירה, למשל, או הגדלה של מספר תלמידים המשתלבים בחלק מהזמן במסגרת החינוך הנורמטיבית.	מומלץ, לערוך תוכנית עבודה שנתית בפורמט מובנה של העירייה, ליחידה לקידום נוער, אשר תכלול, בין היתר, את הנושאים הבאים: תקצוב תוכניות פעילות, חד פעמיות ופעילויות שנתיות; מדדים ישימים לצמצום נשירה ממסגרות חינוך; הגדלת מספר בני הנוער המשתלבים חלק מהזמן במסגרות החינוך ועוד.	
4.1 תקצוב משרד	נמצא כי בכל שנה מהשנים שנבדקו על ידי הביקורת, נרשם תקציב זהה	הביקורת ממליצה, כי העירייה תבחן האם אומנם לא כל כספי	2822

סעיף+ שם הפרק	ממצא	המלצה	תגובת מבוקרים
החינוך את יחידת קידום הנוער	של 220 אלפי ₪ ונראה כי סכום זה לא עודכן בשנים אלו, למרות הגידול התקציבי. בשנת 2023, נראה שנתוני הביצוע (הכנסות בפועל) טרם עודכנו, וזאת למרות שהביקורת קיבלה את הנתונים לאחר תום שנת 2023. תקציב ההוצאות בשנים 2021-2023 מנוצל באחוזים נמוכים מאוד, דבר אשר הביקורת משערת משפיע באופן גורף על הפעילות והשירותים הניתנים ביחידה לקידום נוער לבני נוער הזקוקים לה. הביקורת מדגישה, כי הימנעות מפעילות חברתית ביחידה, ואי ניצול התקציב, עלול להשפיע על קידומם של בני הנוער בחברה, דבר אשר מהווה מטרה מרכזית בפעילות היחידה לקידום נוער. יודגש כי האישורים של כל השנים המבוקרות הונפקו לביקורת על ידי משרד החינוך ביום 22.01.2024 . הביקורת מעירה, כי כל מטרתו של תקציב, לחזות הכנסות והוצאות מראש ולהיערך בהתאם. "העתקה" של סכום התקציב משנה לשנה ואז עדכון תקציב לאחר תום השנה, חוטאים למטרת עריכת תקציב. יש לבחון לקראת סוף כל שנה את הביצוע בפועל של התקציב ובהתאם יש לגבות את הכספים ממשרד החינוך, במקרה שטרם הועברו. כמו כן, יש לעדכן את התקציב לשנה הבאה, על פי הנתונים בפועל ועל פי התחזיות לשנה החדשה.	משרד החינוך הועברו אליה. במידה ואומנם הכספים לא הועברו בשל קיבוץ, או סיבה אחרת, יש לבחון זאת מול משרד החינוך, האם הדבר נובע מאי דיווח על פעילות ו/או דיווח שגוי. מומלץ לבחון האם ניתן בשלב זה לקבל את יתרת התקציב. עוד מומלץ, כי מנהל היחידה לקידום נוער ינצל את תקציב הפעילות, שאינו גבוה, ויממש אותו לטובת פעילויות ביחידה, שאינן קשורות להשכלה בתוכנית הילי"ה. יש להקפיד על עריכת תקציב מעודכן, בהתאם לביצוע שנה קודמת ולתחזית לעתיד. יש לבצע מעקב תקציבי תוך כדי השנה ולא רק לאחר סופה.	

סעיף+ שם הפרק	ממצא	המלצה	תגובת מבוקרים
5 תוכנית היל"ה	נמצא, כי מתוך 72 תלמידים הרשומים בתוכנית, רק 34 נמצאים בסטטוס לומד, כלומר רק 47% מהמשתתפים לוקחים חלק בפעילות המשמעותית של היחידה- השלמת השכלה. מבדיקת הביקורת עולה, כי ביחידה לקידום נוער בעירייה, בתוכנית היל"ה, אין תלמידים הלומדים במסלול לבגרות חלקית או מלאה.	הביקורת ממליצה, כי העירייה, באמצעות היחידה לקידום נוער, תערוך תוכנית עבודה לרכזת ההשכלה, שתכלול יעדים מדידים לגידול משמעותי במספר בני הנוער הרוכשים השכלה בתוכנית היל"ה. יתרה מכך, על תוכנית העבודה לכלול יעדים משמעותיים לקבלת תעודת בגרות חלקית או מלאה בקרב בני הנוער הרשומים לתוכנית היל"ה ומסיימים עם תעודת סיום לימודים.	

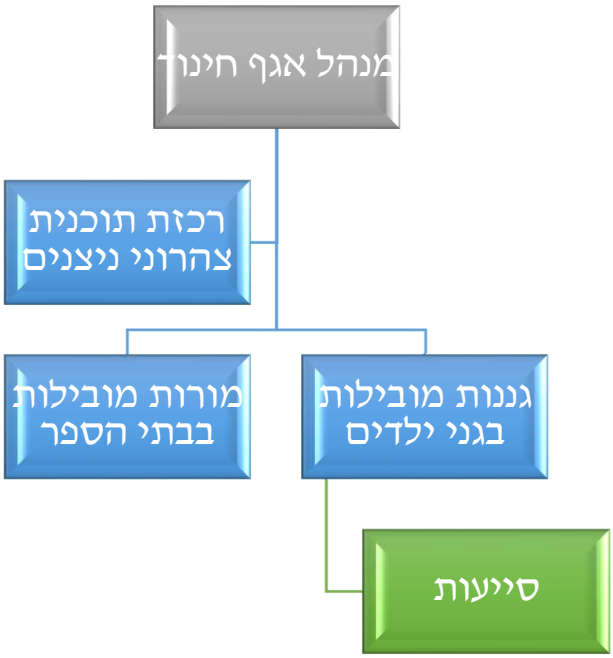
נושא 1: צהרוני ניצנים

עיקרי הממצאים

3. מבנה ארגוני

מבנה ארגוני הוא שם כולל למערך מורכב ומוגדר היטב של תפקידים וקשרי הגומלין ביניהם. המבנה הארגוני משמש בסיס להגדרת אופי הפריסה של הפעילות הארגונית למחלקות, לתפקידים ולתחומי סמכויות והוא מנתב ותוחם באופן רשמי ומחייב את התנועה של אנשים וחומרים בארגון. מבנים ארגוניים נועדו לתת מענה לשיקולי יעילות ותכליתיות בארגון.

להלן תרשים המבנה הארגוני הרלוונטי לביקורת:



להלן תפקידם הרלוונטי לביקורת:

- מנהל אגף חינוך- אחריות כוללת על גיבוש ועיצוב מדיניות החינוך בעירייה, בהתאם להוראות משרד החינוך ומנהל חברה ונוער, כולל תקצוב יחידות המחלקה ובקרה ופיקוח על הפעילויות.
- רכזת צהרונים- ניהול אדמיניסטרטיבי של הצהרונים, כולל גיוס וניהול עובדים, טיפול בחוגים, ציוד ומזון. בנוסף, עבודה מול רכזות, עריכת תוכניות עבודה ועוד.
- מורות מובילות בבתי הספר- אחריות כוללת על תפעול צהרון ניצנים בשעות הפעילות, כולל הגשת ארוחת צהרים, בדיקה ורישום נוכחות, הפעלת תוכנית העשרה.
- גננות מובילות בגני הילדים- אחריות כוללת על תפעול צהרון ניצנים בשעות הפעילות, רישום נוכחות והפעלת תוכנית העשרה, בימים בהם לא מתקיימת פעילות העשרה על ידי ספק חיצוני.
- סייעות בגני הילדים- הגשת ארוחת צהרים לילדי הצהרון, שמירה על הסדר והניקיון.

פרק ה.1. 'השתתפות המדינה וההורים בתוכנית' בקובץ הקריטריונים להפעלת תוכנית ניצנים של משרד החינוך קובע "האחריות הרשות לעדכן את מספרי התלמידים המשתתפים בכל מסגרות ניצנים של הרשות. יש לנהל יומן נוכחות של התלמידים בתוכנית. הרישום לפי תלמיד יהיה יומי בגיליון נוכחות חודשי'.

מבדיקת הביקורת עולה, כי בכל אחת ממסגרות החינוך, קיים כוח אדם כפי שנדרש על ידי הוראות משרד החינוך- תקין.

עוד עולה, כי מורות מובילות וגננות מובילות אינן ממלאות את דף הנוכחות של ילדי הצהרונים במועדים קבועים ואף אינן מציינות יציאה מוקדמת של ילדים מהמסגרת.

מומלץ, כי רכזת תוכנית ניצנים בעיריית עראבה תקפיד, כי כל אחת מעובדות הצהרונים תבצע את כלל המשימות הנדרשות בהוראות משרד החינוך, בפרט כאשר מדובר ברישום נוכחות תלמידים. הביקורת מעירה, כי רישום כוזב יגרור סנקציות כספיות משמעותיות של משרד החינוך (ראה בהרחבה פרק 11- דיווח ועמידה בהוראות משרד החינוך).

4. תוכנית עבודה

"מודל תוכנית עבודה אפקטיבית- קווים מנחים לרשויות מקומיות" , שפורסם על ידי משרד הפנים בשנת 2016 (להלן: "המודל") מדגיש, כי תוכנית עבודה אפקטיבית, הינה כלי לניהול, אשר מאפשר יישום החזון של הרשות באמצעות תכנון עתידי, תוך פיקוח ומעקב אחר ההתקדמות, זיהוי אתגרים וכשלים, הערכת יעילות ושיתוף פעולה חוצה ארגון על בסיס מטרות ויעדים משותפים.

על פי המודל, תוכניות העבודה השנתיות של הרשות, מהוות כלי עזר בחשיבה אסטרטגית ומשקפות את כלל הפעולות, שהרשות מתכננת לבצע בתקופה נתונה, כדי להגיע מהמצב הקיים, למצב עתידי רצוי.

מודל תוכנית עבודה, קובע שלושה תהליכים הכרחיים, בבניית תוכנית עבודה אפקטיבית:

הביקורת קיבלה לעיונה תוכניות עבודה שנתיות של גני הילדים ובתי הספר.

תוכנית העבודה הוצגה לביקורת בפורמט הנדרש על ידי משרד החינוך הכוללת, בין היתר, את הנושאים הבאים:

- פרטי המוסד החינוכי;
- מספר ילדים הרשומים לתוכנית;
- פעילויות העשרה שיועברו על ידי הצוותים החינוכיים;
- כוח אדם להפעלת התוכנית.

מבדיקת הביקורת עולה:

תוכניות העבודה אינן כוללות תקציב.

תוכניות העבודה מוצגת בפורמט של משרד החינוך, אולם לא קיים פורמט תוכנית עבודה של העירייה, הכולל מטרות ויעדים מדידים, הכוללים אבני דרך לצמצום פערים העולים בתוכנית, דוגמת: רישום נוכחות והערות לגבי יציאה מוקדמת של ילדי התוכנית, בחינת השתתפות הורית בתשלום התוכנית וכדומה.

מומלץ לערוך תוכנית עבודה שנתית בפורמט מובנה של העירייה, אשר תכלול, בין היתר, את הנושאים הבאים:

- **תקצוב תוכניות פעילות;**
- **טווח שעות לרישום נוכחות תלמידים במסגרת והערות לילדים המסיימים בשעה מוקדמת;**
- **תשלום הורים.**

5. נהלים

נוהל הוא מסמך שאושר על ידי בעל תפקיד אחראי לפעילות הנדונה בו, מנוהל תחת שיטה לבקרת שינויים ומתאר, מגדיר או מתעד עקרונות, מדיניות, תפקידים, או פעילויות ותהליכי תכנון, תפעול ובקרה ואשר מתאר תהליך עבודה, שיטה או מבנה ארגוני.
מטרת כתיבת נהלים הינה תיעוד שיטת העבודה ו/או דרכי ביצוע פעילות ליצירת נורמת עבודה אחידה, המאפשרת הדרכה, אכיפה ופיקוח, לרבות הגדרת אחריות וסמכות. הנהלים יוצרים שפה משותפת לכלל המנהלים והעובדים ומתארים את שגרת העבודה במקום.

בדוח ביקורת של מבקר המדינה על הרשויות המקומיות לשנת 2022, התייחס המבקר לנושא נהלים וציין כי "לפי הנחיית היועץ המשפטי לממשלה, הנחיות מנהליות, ובכלל זה נהלים, מכוונות לסייע למינהל הציבורי להחליט במהירות וביעילות בכל המקרים הנופלים במסגרת ההנחיות, ולהימנע במקרים דומים מהחלטות הסותרות זו את זו ואף את מטרת הארגון. מטרת הנהלים בארגון היא בין היתר להגדיר ולפרט את תהליכי הביצוע של פעולות שונות; להגדיר תיאום, אחידות, פישוט וייעול של דרכי הביצוע ולתת להן תוקף מחייב; לאפשר שליטה, פיקוח ובקרה על התהליכים ועל הפעולות השונות בארגון."

מבדיקת הביקורת עולה, כי במחלקת חינוך לא קיים נוהל כתוב, אשר מסדיר את פעילותה השוטפת בכל נושא צהרונים ויחידת קידום נוער.

מומלץ לערוך נהלי עבודה בנושא צהרונים ויחידת קידום ביניהם:

- **נהלי הרשמה וגבייה;**
- **נוהל רישום ושיבוץ לצהרונים;**
- **נוהל תפעול צהרונים;**
- **נהלי גריעה מפעילות וזיכוי תשלומים;**
- **נהלי דיווח למשרד ממשלה רלוונטיים**

6. תקציב

תקציב הוא כלי ניהולי, שמטרתו תרגום תכנית העבודה למונחים כספיים ותכנון מראש של הוצאות והכנסות הארגון בחלוקה לנושאים/תחומים. לרוב מתבצע תכנון תקציבי לתקופה של שנה, המקבילה לשנת מס (תקציב שנתי), אך לעיתים מתבצע תכנון תקציבי למשך חייו של פרויקט, או לתקופה ארוכה או קצרה יותר (תקציב רב שנתי, תקציב רבעוני, תקציב חודשי וכדומה).
דיני הרשויות המקומיות קובעים, כי כל רשות מקומית תפעל לפי תקציב שנתי, כאשר שנת הכספים לכל הרשויות תתחיל ב 1 לינואר בכל שנה. תקציב שאושר הינו מסמך משפטי המחייב את הרשות המקומית.
על מנת ללמוד על תקציב התחום הנבדק בשנים האחרונות, הביקורת עיינה בנתונים של תקציב העירייה לשנים 2021-2023. להלן עיקרי הנתונים באלפי ש"ח:

הכנסות*			
	תקציב	ביצוע	אחוז ביצוע
2021	9,100	7,125	78
2022	9,300	9,600	103
2023	11,800	11,026	94
הוצאות**			
2021	7,610	5,176	68
2022	7,660	8,857	116
2023	9,372	8,825	94

***כרטיסי הכנסות: 1319100920 (תוכנית ניצנים), 1319100921 (ניצנים חופשות אביב וחורף).**

****כרטיסי הוצאות: 1819100110 (שכר תוכנית ניצנים), 1819100760 (קיזוז הזנה), 1819100780 (תוכנית ניצנים).**

מבדיקת הביקורת עולה כי בשנת 2021, היה ביצוע חסר הן בהכנסות והן בהוצאות. סביר שההסבר לכך הוא משבר הקורונה, שבגינו מסגרות החינוך היו סגורות חלק מהשנה.

הביקורת מעירה, כי משבר הקורונה החל ב 3/2020. לאור זאת, במועד גיבוש התקציב, היה כבר ידוע כי לא כולו יימומש. יתרה מכך, לאור העובדה שהתקיים סגר מלא בחודש ינואר ובחלק הראשון של פברואר, היה ידוע כבר במועד זה, כי לא כל התקציב יימומש והיה מקום לעדכון תקציבי לאורך השנה בהתאם למצב בפועל.

7. התקשרות הרשות להפעלת צהרונים

משרד החינוך מפרסם כל שנה 'קול קורא' להפעלת תוכנית ניצנים ותוכנית ניצנים בחופשות, וזאת במטרה לקדם מענה חינוכי איכותי לילדים המשתתפים ולהקלה בנטל ההורי.

הקול קורא כולל שורת התחייבויות של הרשות להפעלת התוכנית, ביניהם:

- מנהל תוכנית ניצנים ברשות.
- הכשרות צוותים.
- צוותים חינוכיים בתוכנית- בגני ילדים יהיו שני אנשי צוות, לפחות ויכללו גננת מובילה וסייעת. בבתי הספר יש להעסיק רכזת לכל בית הספר ומורה מובילה לכל כיתה המופעלת בתוכנית.
- ועדת היגוי רשותית.
- חוגי העשרה.

בנוסף, קבע משרד החינוך תקצוב של התוכנית עבור כל ילד, בהתאם לאשכול הסוציואקונומי של הרשות. על פי נתוני הלמ"ס לשנת 2020, מוגדרת עיריית עראבה באשכול סוציואקונומי 3.

להלן התקצוב עבור כל ילד בעיריית עראבה על פי נתוני הקול הקורא שפרסם משרד החינוך (סעיף ו.2.) :

	גן ילדים	בית ספר
השתתפות משרד החינוך	5,104	6,220
גבייה מהורים (על פי קול קורא- אין חובה).	500	500

על מנת לאשר את התוכנית ותקציבה, נדרשת העירייה לחתום על טופס בקשה להפעלת התוכנית והתחייבות של הרשות להפעלת התוכנית כפי שנדרש בקול קורא שפורסם בשנת הפעילות.
הביקורת קיבלה לעיונה את כתב ההתחייבות של הרשות מיום 29.09.2021 שנחתם ואושר על ידי ראש הרשות וגזבר ברשות.

לביקורת אין הערות.

8. ועדת היגוי

קובץ הקריטריונים לתקצוב רשויות מקומיות לתוכנית ניצנים (להלן: "**הקריטריונים**") קובע בפרק ג.3.א. כי העירייה תקיים ועדת היגוי רשותית שתפקידיה יכללו, בין היתר, את הנושאים הבאים:

- בחירת ספק הזנה;
- החלטה על מודל הפעלה;
- קביעת תוכנית שנתית;
- קביעת חוגי העשרה ועוד.

עוד נקבע בקריטריונים כי " **משתתפים: הרשות תקיים ועדת היגוי רשותית בראשות ראש הרשות או מנהל אגף החינוך ברשות ,מנהל ניצנים ברשות, נציגי ההורים, המפקח המתכלל מטעם משרד החינוך, מפקח/ת גני הילדים או נציגתו/ה ברשות, ומרכז/ת תוכנית ניצנים במחוז. גורמים נוספים יצורפו עפ"י שיקול דעת הרשות .הוועדה תתכנס לפחות 3 פעמים בשנה לתוכנית ניצנים בשוטף ופעם נוספת לקראת הפעילות בכל חופשה"**
הביקורת קיבלה לעיונה את פרוטוקולי ועדת ההיגוי הרשותית לשנים 2021-2022 ובחנה את נושאי הדיון בוועדה והמשתתפים כמפורט בטבלה להלן:

תאריך הוועדה	משתתפים על פי הוראות משרד החינוך	משתתפים שהוזמנו בפועל	פער	נושאים עיקריים לדיון
15.06.2021 13.10.2022	ראש רשות/מנהל אגף חינוך, מנהל תוכנית ניצנים, נציגי הורים, מפקח מתכלל מטעם משרד החינוך, מפקחת גני ילדים/ נציג מטעמה ברשות, מרכז/ת תוכנית ניצנים במחוז.	ראש הרשות, מנהל אגף חינוך, רכזים בית ספריים, מנהלת תוכנית ניצנים, מפקחת מתכללת, מפקחות גנים, נציגים נוספים.	נציגי הורים	ספק הזנה, מודל תוכנית ניצנים, חוגי העשרה.

מבדיקת הביקורת עולה, כי בניגוד להנחיות משרד החינוך בנוגע להפעלת תוכנית ניצנים, התכנסה ועדת ההיגוי פעם בשנה ולא כפי שנדרש בהוראות- 3 פעמים בשנה.

עוד עולה, כי בניגוד להנחיות, לא מוזמנים נציגי הורים לוועדת ההיגוי הרשותית.

מומלץ, כי העירייה תפעל על פי הוראות משרד החינוך ותכנס את ועדת ההיגוי הרשותית 3 פעמים בשנה, לפחות.

עוד מומלץ, להקפיד להזמין לישיבות ועדת ההיגוי את נציגי ההורים, דוגמת נציגי הנהגת הורים במסגרות החינוך.

9. הכשרות מקצועיות לצוותי חינוך

על פי הוראות חוק הפיקוח על הצהרונים, סעיף 6, שר החינוך יקבע תנאים לפתיחת צהרון והפעלתו, לרבות "**תנאים הנדרשים מממלאי תפקידים בצהרון... ובכלל זאת תנאים לעניין ניסיון והכשרה מקצועית, לרבות השתלמויות והדרכות ועמידה בבחינות מקצועיות.**"

סעיף ג.5 לקריטריונים קובע "**איכות עבודת הצוותים החינוכיים בצהרונים הנה תוצר של פיתוח מקצועי איכותי ומותאם הבא לידי ביטוי בתהליכי למידה, ליווי והכשרה. השתתפות במפגשים אלו משפיעה באופן ישיר על איכות העשייה החינוכית במסגרות. ההשתתפות היא חובה. משרד החינוך רואה חשיבות רבה בהכשרת הצוותים החינוכיים הפועלים בצהרוני ניצנים ומקיים הכשרה לצוותים אלו**".

צוות כל צהרון בעיריית עראבה כולל גננת מובילה, הנושאת באחריות כוללת לפעילות ילדי הצהרון וסייעת אחת. בנוסף, ככל ונדרש, מתווספת לצוות סייעת צמודה לילד בצהרון. אחריותה של הסייעת כוללת סידור הגן וניקיונו, הכנת המזון לצורך הגשתו לשולחן ועוד.

הביקורת קיבלה לעיונה קבצי הכשרות של כלל צוותי הצהרונים, המפרטות הנחיות פדגוגיות, הדרכות בטיחות והדרכת עזרה ראשונה. להלן טבלאות המפרטות את הנתונים:

- **הדרכות עזרה ראשונה:**

טבלה מספר 1

תאריך	מספר משתתפות	עברו
11.12.2022	17	כן
11.12.2022	19	כן
25.12.2022	18	כן
07.01.2024	40	כן
14.01.2024	31	כן
סה"כ	**125**	

- **הנחיות פדגוגיות בבית ספר:**

טבלה מספר 2

סמל מוסד	שם מוסד	תאריך	אחוז נוכחות במפגש
219584	אלזהראא עראבה	26/11/2022	100%
219584	אלזהראא עראבה	26/11/2022	100%
219584	אלזהראא עראבה	26/11/2022	100%
219584	אלזהראא עראבה	28/11/2022	100%
219584	אלזהראא עראבה	28/11/2022	100%
219584	אלזהראא עראבה	28/11/2022	100%
218834	אבן סינא עראבה	29/11/2022	100%
218834	אבן סינא עראבה	29/11/2022	100%
218834	אבן סינא עראבה	29/11/2022	100%
218842	ע"ש חוסיין יאסין ב	30/11/2022	100%
218842	ע"ש חוסיין יאסין ב	30/11/2022	100%
218842	ע"ש חוסיין יאסין ב	30/11/2022	100%
288175	יסודי אבן רושד	03/12/2022	100%
288175	יסודי אבן רושד	03/12/2022	100%
288175	יסודי אבן רושד	03/12/2022	100%
10047	עראבה	11/12/2022	56%
10047	עראבה	11/12/2022	52%
219832	ראס אלעין עראבה	12/12/2022	100%
219832	ראס אלעין עראבה	12/12/2022	100%
219832	ראס אלעין עראבה	12/12/2022	100%
218842	ע"ש חוסיין יאסין ב	13/12/2022	100%
218842	ע"ש חוסיין יאסין ב	13/12/2022	100%
218842	ע"ש חוסיין יאסין ב	13/12/2022	100%
218842	ע"ש חוסיין יאסין ב	14/12/2022	100%

סמל מוסד	שם מוסד	תאריך	אחוז נוכחות במפגש
218842	ע"ש חוסיין יאסין ב	14/12/2022	100%
218842	ע"ש חוסיין יאסין ב	14/12/2022	100%
288175	יסודי אבן רושד	17/12/2022	100%
288175	יסודי אבן רושד	17/12/2022	100%
227488	אלבירוני עראבה	19/12/2022	100%
227488	אלבירוני עראבה	19/12/2022	100%
227488	אלבירוני עראבה	19/12/2022	100%
219402	אלגזאלי עראבה	20/12/2022	100%
219402	אלגזאלי עראבה	20/12/2022	100%
219402	אלגזאלי עראבה	20/12/2022	100%
227488	אלבירוני עראבה	21/12/2022	100%
219584	אלזהראא עראבה	22/12/2022	100%
219584	אלזהראא עראבה	22/12/2022	100%

- **הנחיות פדגוגיות בגני ילדים:**

טבלה מספר 3

סמל מוסד	שם מוסד	תאריך	אחוז נוכחות במפגש
10047	עראבה	04/12/2022	50%
10047	עראבה	04/12/2022	100%
238675	גן בוסתאן אלאח'דר	05/12/2022	10%
321232	גן אלאבדאע	05/12/2022	100%
149310	גן אלזיתון	06/12/2022	100%
321240	גן אלמג'ד	06/12/2022	100%
149211	גן ואדי אלעין	07/12/2022	100%
603084	אלחנאן	07/12/2022	100%
149492	גן אלביאן	08/12/2022	100%
217976	גן אלזתון	08/12/2022	100%
217968	גן אלנרג'יס	11/12/2022	100%
217992	גן אלמנארה	11/12/2022	17%
149237	גן זיתונת חקלת אלדאר	12/12/2022	100%
238725	גן אלסנאבל	12/12/2022	100%
217984	גן אלבראעם	13/12/2022	100%
238717	אלסועדא	13/12/2022	100%
182360	גן אלנג'ום	14/12/2022	100%
603050	גן אלורוד	14/12/2022	100%
182378	גן אלאזהאר	15/12/2022	100%
901033	גן אלכואכב	15/12/2022	100%

סמל מוסד	שם מוסד	תאריך	אחוז נוכחות במפגש
149187	גן אליאסמין	18/12/2022	100%
149484	גן אלעביר	18/12/2022	100%
10047	עראבה	18/12/2022	100%
10047	עראבה	18/12/2022	100%
298521	אלסראא	19/12/2022	100%
602896	אלאמל	19/12/2022	100%
602854	אלסנאפר	20/12/2022	100%
901041	גן אלפרשאת	20/12/2022	100%
149229	גן אלשמוע	21/12/2022	100%
149245	גן אלסדאקה	21/12/2022	100%
238683	אלעטאא	22/12/2022	100%
603035	גן אלנור	22/12/2022	100%

מבדיקת הביקורת עולה:

1. **מנתונים שהועברו לביקורת על ידי רכזת תוכנית ניצנים, בתוכנית מועסקות 147 עובדות, בעוד שמנתוני טבלה מספר 1 (הדרכות עזרה ראשונה) רק 125 עובדות עברו את ההכשרה. כאמור, על פי הוראות משרד החינוך, על כל העובדות בתוכנית לעבור הכשרת עזרה ראשונה.**
2. **מנתוני טבלה מספר 2 (הנחיות פדגוגיות), עולה, כי בשתי מסגרות חינוך בית ספריות, המסומנות בצהוב בטבלה לעיל, לא כל העובדות עברו את ההכשרה הרלוונטית, הנדרשת על פי הוראות משרד החינוך.**
3. **מנתוני טבלה מספר 3 (הנחיות פדגוגיות גני ילדים) עולה, כי בשלושה גני ילדים, המסומנים בטבלה לעיל בצהוב, לא כל העובדות עברו את ההכשרה הרלוונטית, הנדרשת על פי משרד החינוך.**
4. **יודגש כי מנתוני הטבלאות לעיל עולה, כי כל ההנחיה הפדגוגית מתקיימת בחודשים נובמבר- דצמבר וביתר שנת הפעילות לא מתקיימות הדרכות והנחיות.**

הביקורת ממליצה, לנהל מעקב אחר העובדות שלא עברו הכשרה פדגוגית מתאימה בכל שנת פעילות וככל והכשרה זו לא הושלמה, יש לשקול המשך העסקה.
עוד מומלץ, לבחון את האפשרות לקיים את ההכשרות גם במהלך שנת הפעילות, כך שככל ועולות סוגיות נוספות, המצריכות הנחיה והדרכה, יינתן מענה לעובדות בתוכנית ניצנים.

10. הזנה

דפוסי אכילה נכונים בגיל הילדות ובתקופת ההתבגרות, מקדמים בריאות מיטבית ומסייעים במניעת בעיות בריאות בטווח הארוך.

הורים רבים מתלוננים על איכות המזון המוגש בצהרונים, ופעמים רבות מושמעות טענותיהם גם בכלי התקשורת, כאשר תלונותיהם כוללות, בין היתר, כי ילדיהם אוכלים בשר מעובד ואינם צורכים פירות וירקות במידה מספקת.

במאי 2005 פרסם משרד הבריאות הנחיות לטיפול במזון במוסדות החינוך (להלן ״: **הנחיות משרד הבריאות**״) . ההנחיות מפרטות, בין היתר, את משך הזמן שבו יאוחסן המזון עד לאכילתו, המקום בו יאוחסן, טמפרטורה, מקום האכילה ופינוי האשפה. על פי ההנחיות מחויב ספק המזון ברישיון עסק ובאישורים לכל שלבי ההזנה.

בחודש אוגוסט 2023 פרסם משרד החינוך חוזר מנכ״ל בנושא ״הזנה וחינוך לתזונה נכונה במוסדות החינוך״ (להלן״ ״**הנחיות משרד החינוך**). הוראה זו החליפה את הוראה מספר 0070 מחודש אפריל 2016. הנחיות אלה חלות על בתי הספר וגני הילדים, ומפרטות שורה של הוראות בנוגע לחינוך לתזונה נכונה, להתארגנות להזנה, לנוהלי ההתקשרות עם ספקי המזון, לפיקוח התברואתי על איכות המזון, להובלתו ולהגשתו.

הנחיות משרד החינוך קובעות, כי מחלקת החינוך ברשות המקומית תשלח למנהלי מוסדות החינוך המצויים בתחום השיפוט של אותה רשות, לקראת פתיחתה של שנת הלימודים, חוזר בנושא ההזנה. עוד נקבע בחוזר המנכ״ל, כי על הרשות המקומית לפעול על פי ההנחיות וההמלצות של משרד הבריאות, בכל הקשור להזנה. להלן קישור להנחיות משרד החינוך:

https://apps.education.gov.il/mankal/horaa.aspx?siduri=501

העירייה התקשרה עם 2 חברות קייטרינג לטובת הזנת תלמידי מוסדות החינוך:

קייטרינג מ.ג.ע

קייטרינג אלמנארה.

10.1 התפריט בצהרונים

על פי הנחיות משרד החינוך, ייקבע התפריט לפי הנחיות המחלקה לתזונה במשרד הבריאות ויסתמך על החוברת ״לאכול ולגדול - מדריך להזנת ילדים ובני נוער במוסדות חינוך״ (משרד החינוך- יוני 2012). עוד קובע החוזר, כי ״**הספק יימנע לחלוטין משימוש במזון מעובד ומטיגון המזון, ויספק מזון מבושל**״ (ההדגשה במקור).

בסיור שערכה הביקורת ביום שלישי, 16.01.2024, (ראה בהרחבה פרק 14) נמצא, כי תזונתם של ילדי צהרוני ניצנים הורכבה ממזון מבושל, טרי, שכולל את כל מרכיבי המזון הנדרשים.

מבדיקת הביקורת עולה, כי בתפריט ארוחות הצהריים של קייטרינג מ.ג.ע., אותו קיבלה הביקורת לעיונה, ארוחת צהריים בימי שלישי כוללת יוגורט, מג׳דרה, ירקות ופירות טריים. להלן תמונת מסך מהתפריט שהוצג לביקורת:

קייטרינג מ.ג.ע

שבוע 3 ספטמבר: 17/09/2023-23/09/2023, אוקטובר: 15/10/2023-21/10/2023, נובמבר: 12/11/2023-18/11/2023, דצמבר: 10/12/2023-16/12/2023						
שבוע 1	ראשון	שני	שלישי	רביעי שוברת שגרה 15.11	חמישי	שבת
מנה עיקרית	שניצל הודו	שוקיים	יוגורט	גזים: שוקיים בתי ספר: פרגית	קציצות עוף ברוטב	שניצל הודו
דגנים	פסטה 50% מלא ברוטב	בורגול ואטריות	מג'דרה	חמגשית: פתיתים 50% מלא תפזורת: פתיתים + פירה	אורז לבן	פסטה 50% מלא ברוטב
תוספת חמה	גזר גמדי	תבשיל גרגרי חומוס		שעועית ירוקה	תבשיל שעועית לבנה	גזר גמדי
ירק טרי	ירקות טריים					
פרי טרי	פרי העונה					
לחם	---	לחם עם סמל ירוק	---	לחם עם סמל ירוק	---	---
צמחונים/טבעונים	חזה מהצומח	תבשיל גרגרי חומוס	מג'דרה	רצועות טבעוניות	תבשיל שעועית לבנה	חזה מהצומח
ללא אלרגנים	שניצל, אורז / פסטה, ירקנית	שוקיים, אורז / פתיתים, ירקנית	שעועית לבנה ברוטב, אורז לבן, ירקנית	חזה עוף / פילה עוף, אורז / תפו"א, ירקנית	קציצות עוף, אורז / פסטה, ירקנית	שניצל, אורז / פסטה, ירקנית

יודגש, כי תפריט זה אף מפורסם בלוח הצהרון בגני הילדים. יחד עם זאת, יום הסיור היה יום שלישי והיה שינוי בתפריט, כאשר תזונתם כללה: שוקי עוף, פתיתים, גרגרי חומוס מבושלים. כלומר, ספק הקייטרינג מ.ג.ע לא סיפק לצהרוני ניצנים את ארוחת הצהריים לה התחייב ביום שלישי.

הביקורת ממליצה, כי רכזת הצהרונים תקפיד לאשר מול ספקי הקייטרינג של העירייה את מרכבי ארוחת הצהריים של ילדי הצהרונים. ככל ונדרש לערוך שינוי, יש לאשר את השינוי לספקי ההזנה בכתב.

10.2 פיקוח תברואתי של הרשות המקומית באמצעות ווטרינר הרשות המקומית

הנחיות משרד החינוך קובעות, שווטרינר הרשות המקומית (להלן: "**הווטרינר הרשותי**"), יסייע לרשות המקומית בין היתר בבחירת ספק ההזנה במוסדות החינוך שבתחום שיפוטה ויפקח על מערך ההזנה במוסדות אלה. הרשויות המקומיות נדרשות לדווח בתחילת כל שנת לימודים לווטרינר הרשותי, על מוסדות חינוך שבהם אמורה להתקיים הזנה, כדי לאפשר פיקוח תברואתי נאות.

בראיון שערכה הביקורת עם רכזת תוכנית ניצנים, עלה, כי במהלך שנות תפקידה לא נדרשה לדווח לווטרינר הרשותי על מוסדות חינוך בהם אמורה להתקיים הזנה וככל והדבר נעשה על ידי חברת מילג"ם, היא אינה מקבלת דיווח על הנושא.

הביקורת ממליצה, לבחון מול הווטרינר הרשותי, האם מתקבלים לידיו דיווחים בנוגע למוסדות חינוך בהם מתקיימת הזנה וככל שכן, לבדוק האם ערך פיקוח תברואתי.

עוד מומלץ, לבחון את האפשרות לממשק עם הווטרינר הרשותי, על מנת לוודא כי דיווחים אלה אכן מתקבלים וכיצד הוא פועל מול מוסדות החינוך, חברת מילגם ו/או חברות ההסעדה.

11. דיווח ועמידה בהוראות משרד החינוך

סעיף 2 לקול קורא 'מתווה הדיווחים והתשלומים' קובע את אופן התשלום של משרד החינוך לעירייה. על פי הוראות הסעיף "לתשומת ליבכם, התקצוב הנורמטיבי יקבע על פי מספר הנרשמים, אולם התשלום הסופי יהיה בהתאם למספר המשתתפים בפועל במוסד".

סעיף ה.2.א. מפרט הוראות בנוגע לבקרות שטח בתקופת הפעילות וכולל שורה של הוראות על פיהן יתקצב משרד החינוך את תוכנית ניצנים בעירייה, ביניהן:

- המשרד יבחר מוסדות בהן התוכנית פעילה ויבצע מספר בקרות שטח לאורך שנת הפעילות;
- יקוזז תקציב בגין מסגרת לא פעילה, המדווחת על ידי הרשות כפעילה;
- ייבחן פער בין מספר ילדים במסגרת עליהם דיווחה הרשות למספר ילדים שנספרו בפועל על ידי בקרת השטח של משרד החינוך ויקוזזו סכומים כדלקמן:
  - פער שאינו עולה על 20%- לא יקוזז סכום
  - פער בין 20% ל- 35% יינתן תקצוב בהתאם למספר המשתתפים שנספרו על ידי בקרת השטח של משרד החינוך
  - פער בין 35% ל- 50% יינתן תקצוב לפי 50% ממספר המשתתפים שנמצא על ידי בקרת השטח של משרד החינוך
  - פער העולה על 50%, אשר יימצא ב- 3 בקרות שטח של משרד החינוך, יקוזז כפל תקצוב המסגרת השנתית ובתנאי שלא יעלה על התקציב הרשותי.

הביקורת קיבלה לעיונה 2 דרישות של משרד החינוך לעירייה לתשלום בגין פער במספר התלמידים. בקשות התשלום מפרטות, בין היתר, את מספר המסגרות אותן הפעילה העירייה בתקופה בה נדרש התשלום ומספר הילדים הכולל במסגרות אלה. להלן טבלה המפרטת את הנתונים בגין בקשת תשלום בחודש אפריל 2023 כפי שהוצגה לביקורת:

טבלה 1

תאריך דיווח	29.04.2023
בקשת תשלום עבור חודשים	אפריל- מאי 2023
אפריל- מספר משתתפים גני ילדים	1,348
אפריל- מספר משתתפים בתי ספר	892
מאי - מספר משתתפים גני ילדים	1,348
מאי- מספר משתתפים בתי ספר	892

בנוסף, קיבלה הביקורת לעיונה את תוצאות בקרות השטח שערך משרד החינוך במסגרות ניצנים בעירייה. להלן טבלה המפרטת את הנתונים הרלוונטיים לדיווחי העירייה (מדגם):

טבלה 2

סמל מוסד	תאריך בקרה	פעיל/לא פעיל	מספר תלמידים מתוקצב	מספר תלמידים בפועל	הפרש בין מספר תלמידים למספר בפועל	אחוז הפרד בדיווח
167932	24.03.2022	לא פעיל	-	-	-	-
233130	29.12.2021	פעיל	23	9	14	61
233148	26.12.2021	פעיל	22	13	9	41
328369	28.11.2022	פעיל	31	16	15	48
	06.02.20123	פעיל	29.32	10	19.32	66
328864	06.02.2023	פעיל	26.48	15	11.48	43
	04.05.2023	פעיל	26.6	15	11.6	44
331264	06.02.2023	פעיל	33.1	10	23.1	70

בנוסף, ביום ה- 20 דצמבר 2023 התקבל בעירייה 'מכתב שימוע- אכיפת תוכנית ניצנים בעיריית עראבה', המפרט קיזוז בסך 825 אלפי ₪ בגין הפרשים גדולים, בין דיווחי הנוכחות של העירייה, לדיווחי הנוכחות בפועל, על פי בקרות השטח של משרד החינוך.

מנתוני הטבלה לעיל (טבלה 1) עולה, כי העירייה מדווחת למשרד החינוך על כלל המשתתפים בתוכנית וזאת למרות שלא כל הילדים משתתפים בתוכנית ניצנים מדי יום, גם אם נרשמו. יודגש, כי בפרק 14 (מדגם הביקורת) נמצאו נתונים על דיווחים שגויים של מספרי תלמידים ו/או היעדר של רישום נוכחות תלמידים. ליקויים אלו פוגמים בדיווח נתוני אמת למשרד החינוך ומהווים סיכון תקציבי עבור העירייה, אשר מסתכנת בקיזוז תשלומים עבור התוכנית ממשרד החינוך.

בראיון שערכה הביקורת ביום 16.01.2024 עם רכזת תוכנית ניצנים בעירייה, עלה, כי במהלך השבוע היא עורכת ביקורי שטח במסגרות ואינה רושמת את ממצאיה מהסיור, אלא מנהלת רישום של תאריך ושעה בו ערכה סיור במסגרות ניצנים.

מדיווחי תוצאות בקרת השטח, שערך משרד החינוך במסגרות ניצנים בעירייה (טבלה 2), עולה, כי קיימים פערים גדולים בדיווחי העירייה לגבי נוכחות ילדים בתוכנית, לבין הנתונים שנמצאו בבקרות השטח של משרד החינוך.

הביקורת סבורה, בהמשך לסיור שערכה במסגרות התוכנית בעיר, כי קיים פער בין מספר הילדים המשתתפים בשעת התחלת התוכנית, כלומר 13:30 בבתי הספר ו- 14:00 בגני הילדים, למספר המשתתפים בתוכנית בשעות מאוחרות יותר. הדבר עלה באופן מובהק בסיור הביקורת, כאשר ילדים נלקחו על ידי הוריהם כחצי שעה מתחילת שעת הפעילות, דבר המשפיע על מספרי הילדים, גם בבדיקות משרד החינוך.

מומלץ, כי העירייה תבחן מול משרד החינוך, את אופן דיווח הנוכחות, במקרים בהם ילדים יוצאים לביתם כחצי שעה לאחר תחילת התוכנית. הביקורת סבורה, כי ככל ונתוני הנוכחות יירשמו בשעת תחילת הפעילות, תוך ציון הערות לגבי ילדים שיצאו במהלך הפעילות, ניתן יהיה להבהיר את הסוגייה באופן מיטבי למשרד החינוך, כך שהקיזוז בגין הפעילות יקטן.

מומלץ, כי רכזת התוכנית תערוך בקרות שטח רצופות, בכל אחת ממסגרות ניצנים, ותתעד את הסיור ואת ממצאיו, בפרט בנוגע לנוכחות ילדים במסגרות.

הערת הביקורת: הקריטריונים של משרד החינוך לפתיחת צהרון כוללים, בין היתר, מספר מינימלי של תלמידים במסגרת צהרוני ניצנים. סעיף 1.1. קובע את מרכיבי המודל הבסיסי, המחייב להפעלת התוכנית, כאשר ממוצע הילדים במסגרת נקבע בין 22 (מודל 15 של משרד החינוך) ל- 25 (מודלים 4 ו- 5 של משרד החינוך). במדגם הביקורת שכלל בחינה של 10 מסגרות, נמצא, כי אף מסגרת של התוכנית לא עומדת במספר המינימלי המוגדר להפעלת התוכנית, דבר הפוגע באופן משמעותי בתקציב ההכנסות של העירייה ממשרד החינוך.

על העירייה לבחון את האפשרות, לאחד מסגרות צהרונים ועל ידי כך לשמור על מספר מינימלי של ילדים במסגרת התוכנית וצמצום כוח אדם.

12. גבייה

במסגרת רפורמות ותוכניות של משרד החינוך, התקבלה החלטה בשנת 2017, כי משרד החינוך יממן הפעלת צהרונים וזאת באמצעות קול קורא המתפרסם כל שנה.

המשרד אף קבע מימון עלויות והשתתפות הורים על פי אשכולות סוציואקונומיים, כמפורט בטבלה הבאה:

אשכולות למ"ס	גנים	כיתות א'-ב'	השתתפות הורים	השתתפות המדינה
1	+	+	₪ 50	₪ 600
2	+	+	₪ 50	₪ 600
3	+	+	₪ 50	₪ 600
4	+	+	₪ 300	₪ 350
5	+	+	₪ 350	₪ 300
6	-	+	₪ 350	₪ 300
7	-	+	₪ 450	₪ 200
8	-	+	₪ 500	₪ 150
9	-	+	₪ 500	₪ 150
10	-	+	₪ 500	₪ 150

מנתוני הלמ"ס לשנת 2019 עולה, כי עיריית עראבה מוגדרת באשכול 3 על פי המדד חברתי- כלכלי, כלומר הגבייה מקסימלית מהורים תעמוד על 50 ₪ בחודש.

בראיון שערכה הביקורת עם רכזת הצהרונים ומנהל מחלקת חינוך, עלה, כי העירייה אינה גובה מההורים בגין השתתפות ילדיהם בצהרונים. המשמעות היא, שקיימת פגיעה בהכנסות העירייה בגין ההשתתפות. מדיווחי העירייה למשרד החינוך בשנת 2023, עולה כי בשנה זו השתתפו בצהרונים כ- 2,240 ילדים. סכום ההשתתפות של העירייה עומד על כ- 100 אלפי ₪ לחודש.

הביקורת ממליצה לעירייה, לגבות מההורים סכום של 50 ₪ בחודש, כפי שמוגדר בהוראות משרד החינוך, בגין השתתפות ילדיהם. יוער, כי מדובר בהכנסה שנתית של מעל מיליון ₪. יתרה מכך, הביקורת סבורה, כי התשלום גם מהווה דמי רצינות. העובדה שההורים כלל לא משלמים ולו תשלום מינימאלי, מעודדת רישום לצהרונים גם של ילדים, שלהוריהם אין כל כוונה לרשום אותם לצהרון ובכך גדל הנזק לעירייה, בגין אי הגעה של ילדים לצהרון.

13. משוב

משוב בודק את שביעות רצונם של ההורים והילדים משירותי העירייה בצהרונים. המשוב יכול לסייע באיתור פערים בין הציפיות של המשתתפים בפעילות, לבין השירות הניתן בפועל ומאפשר לשפר את רמת השירות.

מבדיקת הביקורת עולה, כי עיריית עראבה, באמצעות מחלקת החינוך, אינה עורכת משובי שביעות רצון בקרב הורי הילדים, השוהים בצהרונים המצויים בתחום שיפוטה. בראיון שערכה הביקורת עם רכזת הצהרונים בעירייה, עלה, כי אחת לתקופה היא שולחת סקר באמצעות אפליקציית וואטסאפ לעובדות התוכנית, לשם קבלת משוב שביעות רצון. יודגש כי בשיחה שקיימה הביקורת עם מספר גננות בעת הסיור שערכה, נמסר כי סקר זה אכן מועבר, אולם מי שעונה עליו הן הגננות עצמן, מבלי לערוך סקר בקרב הורי הילדים.

הביקורת ממליצה, לבחון את האפשרות, לערוך משוב שביעות רצון מפעילות הצהרונים בקרב הורי הילדים המשתתפים בפעילות, המהווה כלי עזר חשוב, בבחינת המצב בפועל ואף נותן כלים לשיפור השירות.

14. מדגם הביקורת

הביקורת ערכה סיור במספר מסגרות ניצנים המתקיימות בבתי הספר ובגני הילדים ובחנה שורה של נושאים ואת אופן ביצועם במסגרות.

	בי"ס יסודי אלבירוני					גני ילדים				
	ב' מורה- אריג'	א מורה- שרה	ב מורה- רוז	א מורה- קנא	א מורה- הודא	גן זייתו ן	סעד' א	הפרח ים	אל נור	תנו להיות ילדים
מספר ילדים רשומים בפועל	24	21	20	29	25	23	27	22	24	31
מספר ילדים לפי דף נוכחות	לא מלאה דף נוכחות	לא מלאה דף נוכחות	לא מלאה דף נוכחות	לא מלאה דף נוכחות	לא מלאה דף נוכחות	לא מלא ה דף נוכחו ת	**מלאה דף נוכחו ת ובו רשום ים 13 ילדים**	לא מלאה דף נוכחו ת	**מלאה דף נוכחו ת ובו רשום ים 17 ילדים**	**מלאה דף נוכחו ת ובו רשום ים 18 ילדים**
מספר ילדים לפי ספירת ביקורת	21	21	12	18	20	16	10	16	13	16
פער בין מספר ילדים רשומים בפועל למספר ילדים לפי ספירת ביקורת	**3**	**0**	**8**	**11**	**5**	**7**	**17**	**6**	**11**	**15**
מנות אוכל לפי הזמנה	נמצאו 2 מנות אקסט רא	נמצאו 2 מנות אקסט רא	נמצאו 3 מנות אקסט רא	נמצאו 4 מנות אקסט רא	נמצאו 2 מנות אקסט רא	אוכל בכלים מרכזיים. מוגש לצלחות הילדים על ידי הסייעת				
אופן הגשת מנות	אישי לכל ילד.					מוגש לצלחות הילדים על ידי הסייעת				

	בי"ס יסודי אלבירוני					גני ילדים				
צורת ישיבה/אכילה	סביב שולחנות בקבוצות קטנות									
תיאור של הארוחה.	שוקיים עוף, גרגירי חומוס מבושל, פתיתים, ירקות ופירות טריים.									
משקל של המנה העיקרית	תקין	תקין	תקין	תקין	תקין	תקין	תקין	תקין	תקין	תקין
אופן הגעת המזון למסגרת	כלי שומר חום, סגור.									
חוג העשרה במסגרת הסיור	הפעלה על ידי מורה מובילה בכיתה.					תנועה וצליל+ אומנות				
מספר עובדים ותפקידים	מורה מוביל ה.	מורה מוביל ה.	מורה מוביל ה.	מורה מוביל ה.	מורה מוביל ה.	גננת מובילה וסייעת.	גננת מובילה וסייעת.	גננת מובילה וסייעת.	גננת מובילה וסייעת.	גננת מובילה וסייעת.
תיק עזרה ראשונה	ל.ר.	ל.ר.	ל.ר.	ל.ר.	ל.ר.	תקין.	תקין.	תקין.	תקין.	תקין.
ניקיון כללי	+	+	+	+	+	+	+	+	+	+
אחזקת חומרי ניקוי	+	+	+	+	+	+	+	+	+	+
לוח צהרון	ל.ר	ל.ר	ל.ר	ל.ר	ל.ר	+	+	+	+	+
תיק צהרון	ל.ר.	ל.ר.	ל.ר.	ל.ר.	ל.ר.	-	-	-	-	-

بلدية عرابة
ص.ب 10 الدالة 30812
تلفون 04-8789666 טלפון

עיריית עראבה
30812 ת.ד 10 מיקוד
פקס 04-6747291 פאקס

www.arraba.muni.il

מסיור הביקורת עולה:

1. **אין בעירייה נוהל קבוע, בנוגע לשעת בדיקת נוכחות ורישום בתוכנית ניצנים. מתוך 10 מסגרות בהן סיירה הביקורת, ב- 7 לא מלאו המורות/גננות דף נוכחות תלמידים. בנוסף, ב- 3 מסגרות בהן דיווחו נוכחות, נמצא כי מספר התלמידים לא זהה לספירת הביקורת.**
2. **בכל המסגרות בהן סיירה הביקורת, ספקי המזון סיפקו את אותו האוכל ולא בהתאם לתפריט שמוצג בלוח הצהרון והוצג בפני הביקורת.**
3. **לוח צהרון- בהוראות משרד החינוך לא קיימת חובה ללוח צהרון, יחד עם זאת, בכל אחד מגני הילדים קיים לוח משעות פעילות הבוקר, בו מפורסם תפריט הצהרון, אשר מועדי הסעודות בו נמצאו לא בתוקף.**
4. **תיק צהרון- בהוראות משרד החינוך לא קיימת חובה לתיק צהרון, יחד עם זאת, תיק זה יעזור בריכוז כלל הנתונים להם נזקקת המורה המובילה ו/או גננת מובילה להפעלת תוכנית ניצנים, בפרט כאשר חלק גדול של העובדות בתוכנית, אינן מועסקות במסגרת החינוכית בשעות הבוקר.**
5. **הביקורת מעירה, כי במהלך הסיור שערכה בגן אלנור, נשלחה ילדה מהמסגרת לבדה אל רכב האם. לשאלת הביקורת ענתה הגננת, כי אין הנחיות בנושא וכי האם לא יכלה להגיע לאיסוף מהכניסה לגן.**
6. **יודגש כי אצל חלק מהמורות בכיתות ב' (אצל המורות אריג' ורוז), הוזמנו מספר מנות קטן ממספר הילדים. הדבר מעיד על כך, שמנות האוכל שהוזמנו עבור המסגרת אינו מתאים למספר הילדים במסגרת, ועל כך, שמספר התלמידים המדווחים למשרד החינוך אינו עומד בקנה אחד עם מספר התלמידים שהעירייה מצפה בפועל שיגיעו למסגרת. לדוגמה: בכיתה ב' (רוז) דווח למשרד החינוך על 20 תלמידים, בפועל ביום הביקורת היו במסגרת 12 תלמידים וסך מנות האוכל שנמצאו במסגרת היו 15. ככל וכל 20 התלמידים היו מגיעים לצהרון ניצנים, הרי שהיו חסרות מנות ל- 5 תלמידים.**

מומלץ, כי רכזת תוכנית ניצנים בעירייה תפיק דוח נוכחות זהה לכלל מסגרות החינוך ותנחה לגבי שעת בדיקת ורישום נוכחות, אופן דיווח על ילדים שיוצאים לפני שעת הסיום וכדומה.
מומלץ, כי העירייה תקפיד על הזנת ילדי הצהרונים כמופיע בתפריט וככל ויש שינוי, יימסר אישור בכתב לחברות המספקות את ההזנה במסגרות.
יש להקפיד לרשום לצהרון רק את כמות הילדים האמיתית הידועה למפעילות הצהרונים. כאשר גננת או מורה מקבלת הודעה על היעדרות צפויה של ילד, יש להורידו מהמצבת לצורך הזמנת כמות הארוחות.
עוד מומלץ, כי רכזת התוכנית 'תמנף' את המצאות לוח צהרון ותפרסם בו מידע להורים, דוגמת: תוכנית הפעילות, תפריט מעודכן, הודעות בשעת איסוף ילדים מהמסגרת, נהלי המחייבים את ההורים ואת העובדות ועוד.
בנוסף, מומלץ כי יוכן תיק צהרון לכל אחת מהמסגרות, שיכלול, בין היתר את הפרטים הבאים: רשימת ילדים, רשימת הורי ילדים ומספרי טלפון, רשימת ילדים עם רגישויות, וכדומה.

بلدية عرابة
ص.ب 10 الدالة 30812
تلفون 04-8789666 טלפון

עיריית עראבה
30812 ת.ד 10 מיקוד
פקס 04-6747291 פאקס

www.arraba.muni.il

נושא 2: קידום נוער

עיקרי הממצאים

1. רקע

יחידת קידום נוער (להלן: "**היחידה**") פועלת כרשת ביטחון, עבור בני נוער המצויים בנשירה גלויה ונשרו ממסגרת החינוך הפורמלית.

ליחידה מספר עקרונות ליבה, המוגדרים על ידי משרד החינוך- מינהל חברה ונוער, ביניהם:

- **מניתוק לשילוב** - שילוב מחדש של ילדים ובני נוער מנותקים במערכות החינוך הפורמאליות.
- השלמת השכלה - מימוש זכותם של בני נוער מנותקים, להשלים את השכלתם לתעודות פורמאליות, לרבות בגרויות עיוניות וטכנולוגיות
- **הכנת הנוער לעולם העבודה** - הכנת הנוער לעולם התעסוקה העתידי, כולל: פיתוח ראיית תעסוקה עתידית, הכשרות לעיסוקים, פיתוח מסוגלות תעסוקתית, הקניית מיומנויות וחוויית עבודה מוצלחת.
- **מנהיגות ותרומה לקהילה** - חיזוק מעורבותם של בני הנוער בקהילה, תוך שילובם בפעולות התנדבות ותרומה לקהילה.
- **הפחתת התנהגויות סיכון** - חיזוק גורמי חוסן חיוביים בשילוב עם תוכניות למניעת התנהגויות סיכון.
- **מניעת נשירה** - סיוע לתלמידים בסכנת נשירה באמצעות שירותי חינוך-טיפול האמונים על חיזוק יכולתם להשתלב בבתי הספר.

בעיריית עראבה פועלת יחידת קידום נוער, האמונה על הטיפול באוכלוסיית יעד בגילאי 15-18, ומונה 41 תלמידים נכון למועד הביקורת, כמפורט להלן:

18 תלמידים לומדים מסלול 12 שנ"ל

8 תלמידים לומדים במסלול 10 שנ"ל

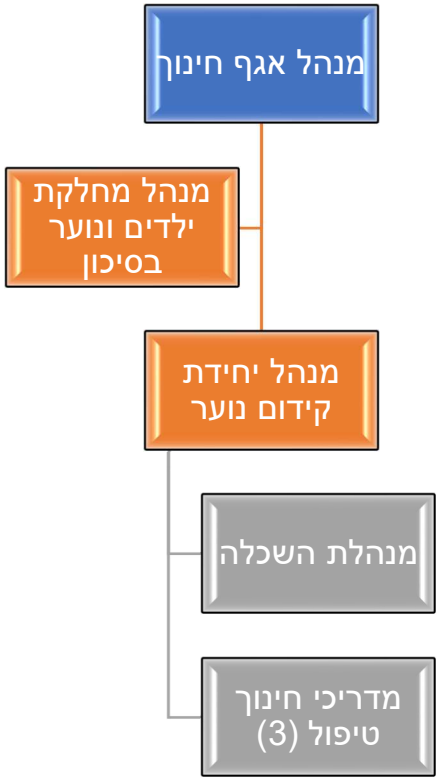
5 תלמידים לומדים במסלול 8 שנ"ל

5 תלמידים לומדים במסלול זריחות .

2. מבנה ארגוני

מבנה ארגוני הוא שם כולל למערך מורכב ומוגדר היטב, של תפקידים וקשרי הגומלין ביניהם. המבנה הארגוני משמש בסיס להגדרת אופי הפריסה של הפעילות הארגונית למחלקות, לתפקידים ולתחומי סמכויות והוא מנתב ותוחם באופן רשמי ומחייב את התנועה של אנשים וחומרים בארגון. מבנים ארגוניים נועדו לתת מענה לשיקולי יעילות ותכליתיות בארגון.

להלן תרשים המבנה הארגוני הרלוונטי לביקורת:



להלן תפקידם הרלוונטי לביקורת:

- מנהל אגף חינוך- אחריות כוללת על גיבוש ועיצוב מדיניות החינוך בעירייה, בהתאם להוראות משרד החינוך ומנהל חברה ונוער, כולל תקצוב יחידות המחלקה ובקרה ופיקוח על הפעילויות.
- מנהל מחלקת ילדים ונוער בסיכון- אחריות כוללת על הפעלת מערך שירותים לילדים ונוער בסיכון, הן בנשירה גלויה והן בנשירה סמויה. תיאום ושיתוף פעולה עם כלל הגורמים, העוסקים בתחום הילדים והנוער בסיכון, עריכת תוכנית עבודה כוללת תקציב ועוד.
- מנהל יחידת קידום נוער- אמון על טיפול בבני נוער אשר נשרו ממערכת החינוך, גיוס צוות ליחידה וניהולם.
- מנהלת השכלה- אחריות כוללת על תחום ההשכלה, כולל: אחריות לאבחון בני הנוער ושילובם בתוכנית למידה מותאמת, אחריות על עבודת מורים ואישור דיווחי שעות, תוכנית עבודה שנתית לתחום ההשכלה ועוד.
- מדריכי חינוך טיפול- הובלת תהליכי ליווי מותאמים אישית, עבודה קבוצתית ופרטנית, לטובת הפעלת התערבות במצבי משבר של נוער בסיכון ונוער בנשירה.

לביקורת אין הערות

2.1 השכלה והכשרות מקצועיות

פרק ג' לאוגדן מפרט הגדרות תפקיד לעובדי החינוך הבלתי פורמלי ודרישות תפקיד. להלן טבלה המפרטת את דרישות מנהל חברה ונוער ועמידה בדרישות של מנהל מחלקת ילדים ונוער בסיכון ומנהל היחידה לקידום נוער:

מסמכים נדרשים	דרישות השכלה	דרישות הכשרה	דרישות נוספות	מצב בפועל
מנהל מחלקת ילדים ונוער בסיכון				
	תואר אקדמי באחד התחומים הבאים: עו"ס, פסיכולוגיה, חינוך, קרימינולוגיה, מדעי ההתנהגות, ייעוץ חינוכי.	סיום בהצלחה קורס ייעודי לניהול שירותים לנוער בסיכון במהלך השנתיים הראשונות בתפקיד	בעלי תעודת הוראה מטעם משרד החינוך או תעודת עובד חינוך בהתמחות קידום נוער אישור המשטרה כי אין מניעה להעסקת בגיר לעבודה במוסד החינוכי	קיימות תעודות של מינהל חברה ונוער הכשרה לפי דרישה.
מנהל יחידת קידום נוער				
	תואר אקדמי באחד התחומים הבאים: עו"ס, פסיכולוגיה, חינוך, קרימינולוגיה, מדעי ההתנהגות, ייעוץ חינוכי		אישור המשטרה כי אין מניעה להעסקת בגיר לעבודה במוסד החינוכי	קיימות תעודות הכשרה של מינהל חברה ונוער.

מבדיקת הביקורת עולה, כי למנהל מחלקת ילדים ונוער בסיכון ומנהל יחידת קידום נוער קיימות תעודת הכשרה רלוונטיות לתפקידם, המאושרות על ידי מנהל חברה ונוער.

יחד עם זאת, הביקורת מציינת כי לא קיבלה לעיונה אסמכתאות המעידות על השכלה רלוונטית לתחום העיסוק שלהם ואף לא הוצגו בפניה אישורי משטרה, כי אין מניעה להעסקת בגיר בעבודה במוסד חינוכי.

מומלץ כי העירייה, באמצעות מחלקת משאבי אנוש ושכר, תוודא כי לבעלי התפקידים הנ"ל קיימים בתיק האישי אישורי השכלה רלוונטיים לתפקידם ואישורי משטרה המעידים על אי מניעת העסקתם כנדרש בחוק.

3. תוכנית עבודה

"מודל תוכנית עבודה אפקטיבית- קווים מנחים לרשויות מקומיות" , שפורסם על ידי משרד הפנים בשנת 2016 (להלן: "המודל") מדגיש, כי תוכנית עבודה אפקטיבית, הינה כלי לניהול, אשר מאפשר יישום החזון של הרשות באמצעות תכנון עתידי, תוך פיקוח ומעקב אחר ההתקדמות, זיהוי אתגרים וכשלים, הערכת יעילות ושיתוף פעולה חוצה ארגון על בסיס מטרות ויעדים משותפים.

על פי המודל, תוכניות העבודה השנתיות של הרשות, מהוות כלי עזר בחשיבה אסטרטגית ומשקפות את כלל הפעולות, שהרשות מתכננת לבצע בתקופה נתונה, כדי להגיע מהמצב הקיים, למצב עתידי רצוי.

מודל תוכנית עבודה, קובע שלושה תהליכים הכרחיים, בבניית תוכנית עבודה אפקטיבית:

הביקורת קיבלה לעיונה תוכנית עבודה לשנת תשפ"ג של היחידה לקידום נוער.

תוכנית העבודה הוצגה לביקורת בפורמט הנדרש על ידי משרד החינוך הכוללת, בין היתר, את הנושאים הבאים:

- נתונים כלליים בדבר היחידה, כולל מספר בני נוער המשתתפים בתוכנית
- קבוצות תהליכיות המתקיימות ביחידה
- השתלמויות עובדים ועוד.

מבדיקת הביקורת עולה:

תוכנית עבודה של היחידה לקידום נוער לא כוללת תקציב לכל אחת הפעילויות המתקיימות ביחידה.

תוכנית העבודה מוצגת בפורמט של משרד החינוך, אולם לא קיים פורמט תוכנית עבודה של העירייה, הכולל יעדים מדידים לצמצום נשירה, למשל, או הגדלה של מספר תלמידים המשתלבים בחלק מהזמן במסגרת החינוך הנורמטיבית.

מומלץ, לערוך תוכנית עבודה שנתית בפורמט מובנה של העירייה, ליחידה לקידום נוער, אשר תכלול, בין היתר, את הנושאים הבאים:

- **תקצוב תוכניות פעילות, חד פעמיות ופעילויות שנתיות;**
- **מדדים ישימים לצמצום נשירה ממסגרות חינוך;**
- **הגדלת מספר בני הנוער המשתלבים חלק מהזמן במסגרות החינוך ועוד.**

4. תקציב

תקציב הוא כלי ניהולי, שמטרתו תרגום תכנית העבודה למונחים כספיים ותכנון מראש של הוצאות והכנסות הארגון בחלוקה לנושאים/תחומים. לרוב מתבצע תכנון תקציבי לתקופה של שנה, המקבילה לשנת מס (תקציב שנתי), אך לעיתים מתבצע תכנון תקציבי למשך חייו של פרויקט, או לתקופה ארוכה או קצרה יותר (תקציב רב שנתי, תקציב רבעוני, תקציב חודשי וכדומה).

דיני הרשויות המקומיות קובעים, כי כל רשות מקומית תפעל לפי תקציב שנתי, כאשר שנת הכספים לכל הרשויות תתחיל ב 1 לינואר בכל שנה. תקציב שאושר הינו מסמך משפטי המחייב את הרשות המקומית.

על מנת ללמוד על תקציב התחום הנבדק בשנים האחרונות, הביקורת עיינה בנתונים של תקציב העירייה לשנים 2021-2023. להלן עיקרי הנתונים באלפי ש"ח:

טבלה מספר 1

הכנסות*			
	תקציב	**ביצוע**	**אחוז ביצוע**
2021	**220**	**254**	**115**
2022	**220**	**315**	**143**
2023	**220**	**156**	**71**
הוצאות**			
2021	**25**	**3.4**	**14**
2022	**14**	**8**	**57**
2023	**14**	**5.5**	**39**

***כרטיסי הכנסות: 1317700921 כולל הכנסות של היחידה לנוער בסיכון.**

****כרטיסי הוצאות: וחזר1817705780 (קידום נוער פעולות), 1817705781 (קידום נוער שונות).**

بلدية عرابة
ص.ب 10 الدالة 30812
تلفون 04-8789666 טלפון

עיריית עראבה
30812 ת.ד 10 מיקוד
פקס 04-6747291 פאקס

www.arraba.muni.il

4.1 תקצוב משרד החינוך את יחידת קידום הנוער

תקצוב משרד החינוך את היחידה לקידום נוער מתבצע באמצעות קול קורא ייעודי להשתתפות בשכרם של עובדי היחידה. בשנים האחרונות תוקן הקול הקורא כך שמלבד עובדי קידום נוער ביחידה לקידום נוער מועברת באמצעותו השתתפות משרד החינוך בתפקידים נוספים שלא מומנו בעבר על ידי המשרד דוגמת: מנהל מחלקה לחינוך ילדים ונוער בסיכון ברשות, רכז/ת תכנית רווחה חינוכית ברשות ועוד.

השתתפות משרד החינוך בשכרם של בעלי תפקידים מתבצעת על פי הכללים הבאים:

ביחידה לקידום נוער ניתנת השתתפות בשכרם של עד 10 בעלי תפקידים. מתוכם תפקידי חובה: מנהל יחידה לקידום נוער, מנהל השכלה (תוכנית הילה) ועובד קידום נוער. יתר בעלי התפקידים הם בהתאם לפעילות היחידה: רכז חינוך -טיפול, רכז תחום תעסוקה ,רכז תרומה לקהילה, מתאם/עובד קידום נוער לאוכלוסיות ייעודיות .

השתתפות בשכרו של מנהל יחידה לקידום נוער ברשות עד 70,000 ₪ למשרה מלאה

השתתפות בשכרם של בעלי תפקידים נוספים – עד 60,000 ₪ למשרד מלאה

בנוסף, רשויות חלשות , במדד טיפוח 7 עד 10, רשאיות לקבל תוספת של 5% בתקצוב כל בעלי התפקידים.

להלן טבלה המפרטת את ההכנסות ממשרד החינוך על פי נתונים שהוצגו לביקורת:

(הביקורת שלפה רק נתונים הרלוונטיים ליחידת קידום נוער)

טבלה מספר 2

שנה	סך משרות	סכום כולל בש"ח שאושר לעירייה	סכום ביצוע
2021	1 מנהל יחידת קידום נוער + 4בעלי תפקידים נוספים	254,212	254,213
2022	מנהל יחידה + 5 עובדים	314,923 ₪ (כולל 81 אלף באישור ועדת חריגים)	314,924
2023	מנהל + 6 עובדים	388,772 ש"ח	*156,000

מנתוני הטבלה לעיל (טבלה מספר 1) עולה, כי בכל שנה מהשנים שנבדקו על ידי הביקורת, נרשם תקציב זהה של 220 אלפי ₪ ונראה כי סכום זה לא עודכן בשנים אלו, למרות הגידול התקציבי. בשנת 2023, נראה שנתוני הביצוע (הכנסות בפועל) טרם עודכנו, וזאת למרות שהביקורת קיבלה את הנתונים לאחר תום שנת 2023.

תקציב ההוצאות בשנים 2021-2023 מנוצל באחוזים נמוכים מאוד, דבר אשר הביקורת משערת משפיע באופן גורף על הפעילות והשירותים הניתנים ביחידה לקידום נוער לבני נוער הזקוקים לה.

הביקורת מדגישה, כי הימנעות מפעילות חברתית ביחידה, ואי ניצול התקציב, עלול להשפיע על קידומם של בני הנוער בחברה, דבר אשר מהווה מטרה מרכזית בפעילות היחידה לקידום נוער.

יודגש כי האישורים של כל השנים המבוקרות הונפקו לביקורת על ידי משרד החינוך ביום 22.01.2024 . הביקורת תוהה – האם אישורים אלו לא היו בידי המנהל בתום כל שנה.

להלן תמונת מסך מאישורים שהועברו לביקורת:

לומדים בביטחון
שנת הלימודים תשפ"א בשגרת קורונה
מדינת ישראל משרד החינוך מחוז צפון רואים רחוק. רואים חינוך.
EFQM Recognised for excellence 4 star - 2016

1/22/2024
1/22/2024

לכבוד
מר/גב' עומר ואכד נאסר, ר' רשות
מר/גב' נסאר ג'בר מנהל/ת מחלקת חינוך
עראבה

שלום רב,

הנדון: תמיכת המשרד בשכר כ"א אגף לחינוך ילדים ונוער בסיכון 2021

כחלק מראייה מערכתית של כלל הילדים ובני הנוער בסיכון ובהמשך לבקשתכם בקול קורא מס' 12926 אנו שמחים להודיעכם על אישור תשלום תמיכות בתפקידי עובדי אגף לחינוך ילדים ונוער בסיכון לשנת תקציב 2021. להלן התפקידים שאושרו על ידי המטה:

מחלקה לחינוך ילדים ונוער בסיכון:

הביקורת מעירה, כי כל מטרתו של תקציב, לחזות הכנסות והוצאות מראש ולהיערך בהתאם. "העתקה" של סכום התקציב משנה לשנה ואז עדכון תקציב לאחר תום השנה, חוטאים למטרת עריכת תקציב. יש לבחון לקראת סוף כל שנה את הביצוע בפועל של התקציב ובהתאם יש לגבות את הכספים ממשרד החינוך, במקרה שטרם הועברו. כמו כן, יש לעדכן את התקציב לשנה הבאה, על פי הנתונים בפועל ועל פי התחזיות לשנה החדשה.

הביקורת ממליצה, כי העירייה תבחן האם אומנם לא כל כספי משרד החינוך הועברו אליה. במידה ואומנם הכספים לא הועברו בשל קיבוץ, או סיבה אחרת, יש לבחון זאת מול משרד החינוך, האם הדבר נובע מאי דיווח על פעילות ו/או דיווח שגוי. מומלץ לבחון האם ניתן בשלב זה לקבל את יתרת התקציב.
עוד מומלץ, כי מנהל היחידה לקידום נוער ינצל את תקציב הפעילות, שאינו גבוה, ויממש אותו לטובת פעילויות ביחידה, שאינן קשורות להשכלה בתוכנית היל"ה.
יש להקפיד על עריכת תקציב מעודכן, בהתאם לביצוע שנה קודמת ולתחזית לעתיד. יש לבצע מעקב תקציבי תוך כדי השנה ולא רק לאחר סופה.

بلدية عرابة
ص.ب 10 الدالة 30812
تلفون 04-8789666 טלפון

עיריית עראבה
30812 ת.ד 10 מיקוד
פקס 04-6747291 פאקס

www.arraba.muni.il

5. תוכנית הילה

תוכנית הילה (השלמת יסוד ולימודי השכלה), היא אחת התוכניות המרכזיות הפועלת במסגרת היחידות לקידום נוער ברשויות המקומיות ואגף חינוך ילדים ונוער בסיכון במשרד החינוך.
התוכנית מיועדת לבני נוער בגילאי 14–18 אשר מצויים מחוץ למסגרת החינוך הפורמאלית, לצורך השלמת השכלתם.

התוכנית מורכבת מארבעה תחומי פעילות בסיסיים הכוללים:

- לימודים להשלמת השכלה לחניכים ברמה פרטנית וקבוצתית ממסלול 8 שנ"ל ועד בגרות וכן אפשרות למסלולי לימוד מקצועיים המשלבים הסמכה ואקרדיטציה;
- פעילות חינוכית, חברתית וערכית לחניכים באופן פרטני וקבוצתי ;
- טיפול וליווי אישי לחניכים על ידי עובד לקידום נוער;
- הקניית מיומנויות יסוד לצורך מיצוי פוטנציאל אישי בתחומי: תעסוקה, השתלבות חברתית, התנדבות והכנה לצה"ל.

התלמידים בתוכנית הילה לומדים במסגרת תוכנית לימודים גמישה, המותאמת לצורכיהם וליכולותיהם. לכל תלמיד נבנית באופן פרטני תוכנית לימודים אישית ומותאמת לרמה הלימודית איתה הוא מגיע, מצבו הרגשי וזמינותו. התוכנית נבנית על ידי ועדת תכנון ומעקב רשותית, שאחראית לבנייה ולאישור תוכנית אישית או קבוצתית לכל הנערים המטופלים בקידום נוער, כולל הקצאת משאבים ולמעקב אחרי ביצועה. היקף הלימודים של כל תלמיד הוא גמיש ומשתנה לאורך השנה. הלימודים מתקיימים בלמידה אישית או קבוצתית, והקבוצות הלימודיות הן קטנות. שנת הלימודים איננה חופפת לשנת הלימודים במערכת החינוך הפורמאלית. ובני הנוער יכולים להתחיל ללמוד בתוכנית בכל יום מימות השנה ולהפסיק ללמוד בה בכל שלב על פי רצונם.

כאמור, יחידת הקידום נוער בעירייה מונה 41 תלמידים נכון למועד הביקורת, כמפורט להלן:

18 תלמידים לומדים מסלול 12 שנ"ל
8 תלמידים לומדים במסלול 10 שנ"ל
5 תלמידים לומדים במסלול 8 שנ"ל
5 תלמידים לומדים במסלול זריחות.

ביחידה מועסקים 8 מורים המלמדים: אנגלית, אזרחות, ערבית, גאוגרפיה, אסלאם, כלכלה, מתמטיקה ועוד.
הביקורת קיבלה לעיונה 'דוח מטופלים' מעודכן לחודש נובמבר 2023, המפרט, בין היתר, את הפרטים הבאים:
שם התלמיד, מספר זהות, מצב שיבוץ, סטטוס טיפול, ותוכניות אישיות מותאמות לצרכי התלמיד.
דוח המטופלים מפרט רשימה של 72 תלמידים מתוכם:
תלמיד אחד הרשום כלומד במסגרות חוץ
37 תלמידים שהסטטוס שלהם מוגדר כ 'הפסיק ללמוד'
34 תלמידים בסטטוס לומד.

بلدية عرابة
ص.ب 10 الدالة 30812
تلفون 04-8789666 טלפון

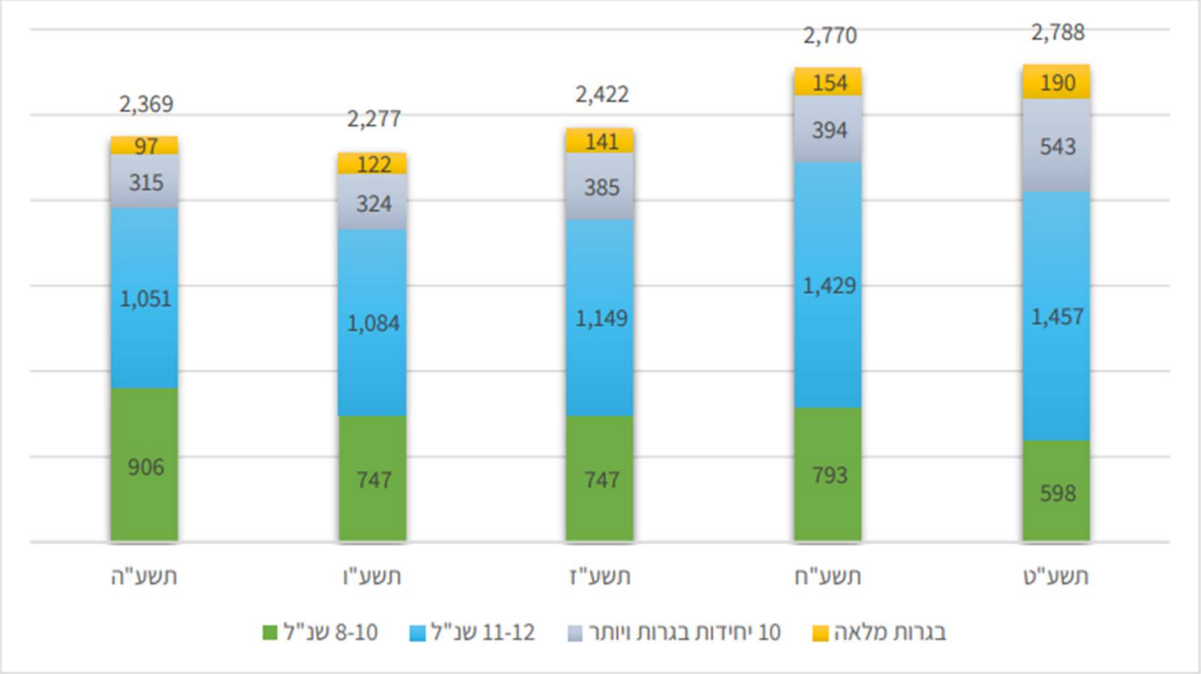
עיריית עראבה
30812 ת.ד 10 מיקוד
פקס 04-6747291 פאקס

www.arraba.muni.il

בשנת 2021 פורסם מחקר של מכון הכנסת בנושא 'היחידות לקידום נוער ותוכנית היל"ה- תמונת מצב'. המחקר מפרט תלמידים בתוכנית היל"ה לשנים 2014-2021, כולל נתונים לגבי בני נוער המסיימים את מסלול היל"ה עם תעודת בגרות מלאה. הזכאות לתעודת בגרות מלאה בשנת 2019 עמדה על 7%.

להלן תרשים תמונת מצב שפורסם במחקר:

תרשים 6: מקבלי תעודות בתוכנית היל"ה, 2015-2019



נמצא, כי מתוך 72 תלמידים הרשומים בתוכנית, רק 34 נמצאים בסטטוס לומד, כלומר רק 47% מהמשתתפים לוקחים חלק בפעילות המשמעותית של היחידה- השלמת השכלה.

מבדיקת הביקורת עולה, כי ביחידה לקידום נוער בעירייה, בתוכנית היל"ה, אין תלמידים הלומדים במסלול לבגרות חלקית או מלאה.

הביקורת ממליצה, כי העירייה, באמצעות היחידה לקידום נוער, תערוך תוכנית עבודה לרכזת ההשכלה, שתכלול יעדים מדידים לגידול משמעותי במספר בני הנוער הרוכשים השכלה בתוכנית היל"ה. יתרה מכך, על תוכנית העבודה לכלול יעדים משמעותיים לקבלת תעודת בגרות חלקית או מלאה בקרב בני הנוער הרשומים לתוכנית היל"ה ומסיימים עם תעודת סיום לימודים.

بلدية عرابة
ص.ب 10 الدالة 30812
تلفون 04-8789666 טלפון

עיריית עראבה
30812 ת.ד 10 מיקוד
פקס 04-6747291 פאקס

www.arraba.muni.il

פרק ב

דוח ביקורת במחלקת רכש
עיריית עראבה

2023

דוח ביקורת רכש

כללי

רשויות מקומיות מתקשרות עם ספקים, באמצעות מכרזים, או הליכי הצעות מחיר לצורך רכישת טובין וקבלת שירותים.

סעיף 198 לפקודת העיריות קובע כי **"השר יקבע בתקנות את צורת המכרז ואת דרכי הזמנתן וקבלתן של הצעות המחירים, ורשאי הוא לקבוע בהן סוגים של חוזים כאמור, שבהם רשאית העירייה להתקשר ללא מכרז פומבי או ללא מכרז בכלל".**

בהתאם לכך, תוקנו תקנות העיריות (מכרזים) תשמ"ח – 1987 (להלן: "תקנות העיריות") המגדירות את האופן בו צריכים להתנהל מכרזים בעירייה ואת דרך ההתקשרות הנדרשת. בין היתר, התקנות קובעות את המקרים בהם יש לקיים מכרז זוטא (מכרז סגור לרשימה סגורה של מציעים שהעירייה מנהלת על פי אמות מידה שנקבעו מראש על ידי הרשות) או מכרז פומבי, את המקרים בהם רשאית העירייה להתקשר ללא מכרז, את אופן התנהלותו של מכרז זוטא ומכרז פומבי.

דרך ההתקשרות נקבעת בהתאם לסכום היקף ההתקשרות הקבוע בתקנות וצמוד למדד. משרד הפנים מפרסם מדי תקופה את סכומי ההתקשרות המעודכנים על בסיסן נקבעת דרך ההתקשרות בה תנקוט העירייה.

להלן סכומי ההתקשרות הצמודים למדד שהתפרסם באפריל 2020 בהתאם לסוג ההתקשרות:

דרך ההתקשרות	סכומים (ב-₪)
פטור ממכרז	עד 143,100
מכרז זוטא (ישלח ל-4 ספקים לפחות)	143,100- 349,400
מכרז זוטא (ישלח ל- 6 ספקים לפחות)	349,400- 698,800
מכרז פומבי	מעל 698,800

מהוראות אלו עולה, כי כל הרכישות עד סכום של 143,100 ₪ כולל מע"מ, יכולות להתבצע באמצעות הליכי הצעות מחיר וללא מכרז פומבי/ זוטא

את כל הליכי הרכש וההתקשרויות מתחת לסכום הפטור ממכרז הקבוע בתקנות, מנהלות הרשויות המקומיות בהתאם לנהלי עבודה פנימיים.

מתודולוגיה

מטרת הביקורת

מטרת הביקורת הינה בחינת נאותות הליך הרכש שסכומו הוא עד הסכום שאינו חייב במכרז. הביקורת בדקה עמידת ההליך הננקט בעירייה בהוראות תקנות העיריות (מכרזים).

היקף הביקורת

התקופה שנבדקה על ידי הביקורת היא 2021-2022. (להלן: "תקופת הביקורת").

בסיס נורמטיבי

- תקנות העיריות (מכרזים), תשמ"ח- 1987.
- פקודת העיריות.
- תקנות העיריות (הסדר רכישות, ניהול מחסנים, רישום וניהול טובין), תשנ"ח-1998.

1. ניהול וארגון

ניהול הוא תהליך או אוסף הפעולות של הנהגה והובלה של ארגון. בניהול נעשה שימוש במשאבים שונים, ובכלל זה משאבי אנוש, הון, נכסים חומריים ונכסים לא-מוחשיים, לצורך השגת מטרות שונות של הארגון. תפקיד המנהל כרוך בשיתוף פעולה עם גורמים רבים, מעבר לעובדים הישירים שתחתיו בארגון, ולכן דורש כישורים בין-אישיים ויכולות תיאום.

נהלי עבודה

נוהל הוא מסמך שאושר על ידי בעל תפקיד אחראי לפעילות הנדונה בו, מנוהל תחת שיטה לבקרת שינויים ומתאר, מגדיר או מתעד עקרונות, מדיניות, תפקידים, או פעילויות ותהליכי תכנון, תפעול ובקרה ואשר מתאר תהליך עבודה, שיטה או מבנה ארגוני.

מטרת כתיבת נהלים הינה תיעוד שיטת העבודה ו/או דרכי ביצוע פעילות ליצירת נורמת עבודה אחידה, המאפשרת הדרכה, אכיפה ופיקוח, לרבות הגדרת אחריות וסמכות. הנהלים יוצרים שפה משותפת לכלל המנהלים והעובדים ומתארים את שגרת העבודה.

הביקורת בקשה לקבל נהלי רכש כתובים, אך מנהל הרכש מסר כי אין נהלים כתובים. קיימות הנחיות עבודה אך אינן כתובות. ההנחיות הנ"ל יפורטו בפרק הדוח העוסק בהליך הרכש.

מבנה ארגוני

מבנה ארגוני הוא מונח כולל לאופן בו מאורגן מערך התפקידים בארגון ולקשרי הגומלין והממשקים ביניהם. הוא מגדיר איך בעלי התפקידים בארגון צריכים לפעול, כדי להגשים את ייעודו ומטרותיו.

בעירייה מועסק מנהל רכש. ואין עובדים נוספים במחלקה. לביקורת נמסר על ידי מנהל הרכש, כי הצעות המחיר מתקבלות על ידי המחלקות ולא על ידי מחלקת הרכש. הביקורת מעירה, כי הגעת הצעות המחיר למחלקות ולא ישירות לרכש, עלולה לכאורה ליצור חוסר הוגנות ופגיעה בהליך הרכש התקין.

מערכת הרכש

לצורך פעילותה השוטפת בנושא הרכש, עושה העירייה שימוש במערכות ממוחשבות. המערכת המרכזית המשמשת את העירייה, היא מערכת האוטומציה.

מודול הרכש (מסך הזמנות עבודה) במערכת האוטומציה (להלן: "מערכת רכש"), משמש לביצוע ההזמנות לנותני השירותים. כל הזמנה מקבלת מספר חד ערכי. מפיק ההזמנה נדרש לסרוק למערכת את המסמכים הנלווים ולצרפם להזמנה. ההזמנה מועברת דרך מערכת הרכש לאישור הגורמים המוסמכים, בהתאם להיקף ההתקשרות הכספית.

הליך אישור ההזמנות מבוצע באופן ממוחשב במערכת הרכש. הזמנות המאושרות אמורות להישלח לספקים לפני תחילת העבודה. הזמנות שלא אושרו בידי הגורמים המאשרים, מוחזרות ליחידות שהפיקו אותן במערכת הרכש.

מערכת הרכש גם משמשת לביצוע הליך התשלום לספק, לאחר מתן השירות.

בהתאם לסעיף 3 לתקנות העיריות (הסדר רכישות, ניהול מחסנים, רישום וניהול טובין), תשנ"ח-1998:

עירייה תנהל פנקס באחד מן האמצעים הנמצאים המפורטים להלן:

(1) מערכת עיבוד נתונים אוטומטית מרכזית, לניהול טובין שעליה יורה המנהל;

(2) מערכת עיבוד נתונים אוטומטית נפרדת, ובלבד שהתקיימו תנאים אלה:

(א) מערכת עיבוד הנתונים, מאפשרת מעקב אחר הרישום של החשבון הנגדי בהנהלת החשבונות של העיריה ואיתור התיעוד המתאים;

(ב) נתקבל דיווח על יתרות כספיות, במתכונת שעליה הורה רואה החשבון של העיריה;

(ג) המערכת מאפשרת העברת הדיווח למערכת עיבוד נתונים מרכזית, באמצעים ממוכנים;

(ד) תכנון עיבוד הנתונים יהיה בהתאם להוראות כל דין ויאפשר בדיקה פנימית ובקרת נתונים;

המלצות

הביקורת ממליצה, להגדיר נהלי עבודה במסגרתם יוגדרו סמכויות ותפקידים בכל נושא הרכש בעירייה. יש לכלול בנהלים את הנושאים הבאים:

- תרשים זרימה של תהליך תקין.
- הגדרת סמכויות של מנהלי מחלקות ואגפים בהזמנות ורכש.
- בקרה ומעקב אחר וועדות רכש - קיום ותיעוד תקין.
- בקרה ומעקב אחר ערבויות וביטוחים.

הביקורת ממליצה להקפיד, כי הצעות המחיר יוגשו למחלקת הרכש בלבד ולא דרך המחלקות וזאת כדי לשמור על מקצועיות, הוגנות ושוויון.

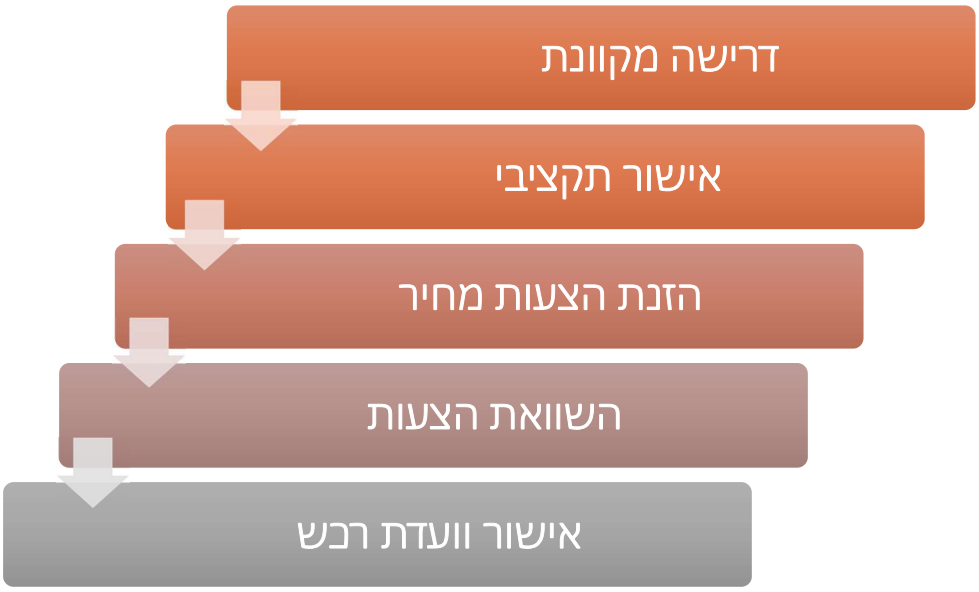
2. תהליך הרכש

תהליך הרכש

תהליך הרכש מתחיל, כאשר עולה צורך באחת ממחלקות העירייה לבצע רכש מסוים. המחלקה מגישה דרישה מקוונת, באמצעות מערכת הרכש של העירייה. על הדרישה לכלול לפחות הצעת מחיר אחת סרוקה. הדרישה מטופלת על ידי מחלקת הרכש. בשלב הראשון, נבדק קיומו של סעף תקציבי מתאים. במידה וקיים תקציב, נבדק סכום הרכישה. ככל וסכום הרכישה אינו מחייב מכרז, וככל שהרכישה לא מתבצעת בספק המקושר עם העירייה בחוזה מסגרת, המחלקה מתבקשת להביא מספר הצעות מחיר. לאחר מכן מובאות הצעות המחיר

לאישור ועדת רכש ובלאי. לאחר האישור, מפיקה מחלקת הרכש הזמנה ומעבירה אותה לחתימת הגורמים הרלוונטיים בעירייה טרם העברתה לספק.

תרשים תהליך רכש הטובין הפטור ממכרז בעירייה



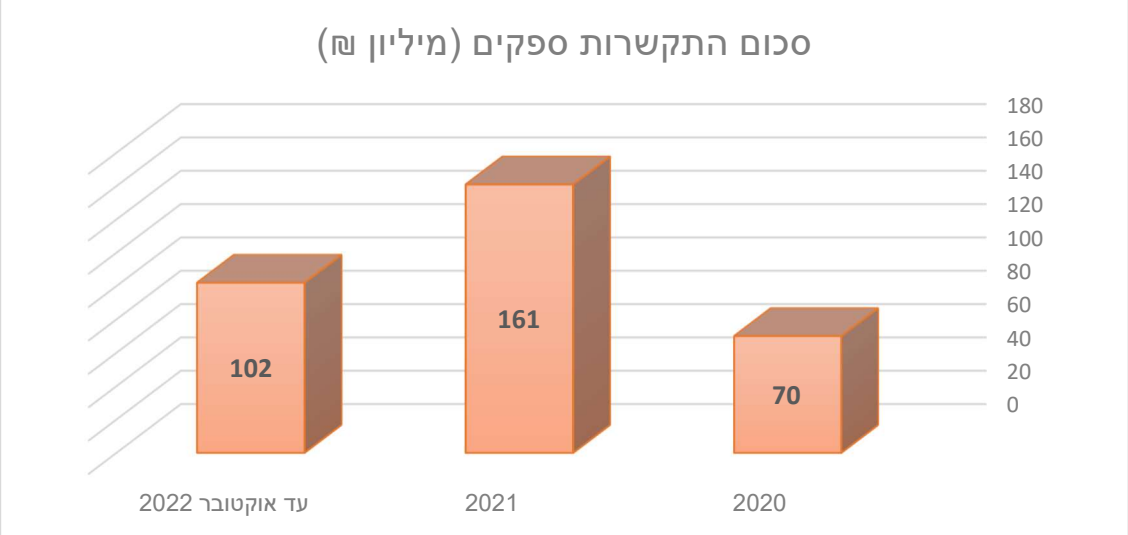
بلدية عرابة
ص.ب 10 الدالة 30812
تلفون 04-8789666 טלפון

עיריית עראבה
30812 ת.ד 10 מיקוד
פקס 04-6747291 פאקס

www.arraba.muni.il

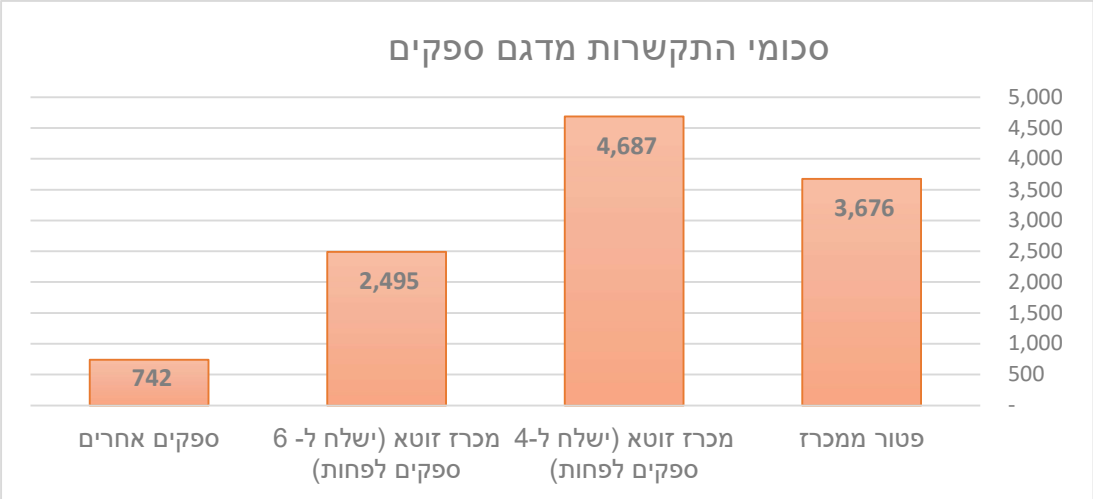
נתונים בתחום הרכש

הביקורת התמקדה בביצוע הליכי רכש בשנים 2020-2022, בשנים אלו בוצעו הליכי רכש במאות מיליוני ₪, להלן גרף המפרט את סכומי הרכש של העירייה בשנים 2020-2021:



הביקורת קיבלה מאזן בוחן תנועות ספקים. דוח זה מציג את סה"כ הרכש השנתי מכל אחד מספקי העירייה. הביקורת ניתחה את הדוח ודגמה ממנו רשימת ספקים שעובדים עם העירייה ברכש בסכומים נמוכים או בינוניים שבדרך כלל אינם מחייבים מכרז פומבי.

להלן גרף המתאר את סכומי התקשרות של הספקים שנדגמו, לפי סוג הליך הרכש, שמחייב סכום ההתקשרות עימם.



- ספקים אחרים- נתוני ספקים ללא ספקים שזכו במכרז פומבי

ממצאים

הצעות מחיר /מכרזים

הביקורת מצאה, כי בהצעות המחיר לעיתים קרובות הפערים בין הספקים קטנים מאוד. בוועדת הרכש נבחרת תמיד ההצעה הזולה ביותר, ולא נבחנים כלל פרמטרים של איכות. לשם דוגמא - לא נעשה שימוש בהמלצות או ניסיון קודם בקביעת ההחלטה.

כמו כן מתבצעים שינויים ידניים בפרוטוקול הוועדה כך ששינוי זה משנה את ההצעה הזוכה ללא חתימה של מורשה החתימה על התיקון עצמו.

כך לדוגמא :

✓ וועדת רכש מתאריך 31/08/2021 "הצעות מחיר למגמת חשמל בית ספר טכנולוגי" הוגשו 3 הצעות כדלקמן:

1. הספק אר.אס.אן בסך 140,117 ₪
2. הספק אפליקום בסך 140,380 ₪
3. הצעה חסרה שנפסלה.

הביקורת מצאה כי סכום הצעה מס' 1 תוקן בכתב יד. כמו כן, חסר דף מס' 1 בהצעת המחיר, כך שעולה חשש מהותי כי תוקנו הנתונים באופן שישפיע על קבלת ההחלטה הזוכה.

כפי שניתן לראות גם אם הצעה מס' 1 הייתה מוגשת באופן תקין אזי פער המחירים הוא מזערי ממש ולא נעשה שימוש בהמלצות או ניסיון קודם.
בנוסף, סכום זה קרוב מאוד לסכום המחייב עריכת מכרז זוטא.

- ✓ וועדת רכש מתאריך 19/11/2020 הצעות מחיר עבודות בטיחות בדרכים גבשושיות הוגשו 2 הצעות כדלקמן:

1. הספק שליש רג'א סכום הצעה בסך 116,663.04 ש"ח (ההצעה המקורית הייתה 116,603.04 ₪ ותוקנה בכתב יד).
2. הספק קראקרה נסיר סכום הצעה בסך 116,663 ₪.

הצעה מס' 2 זכתה בעבודה.
הביקורת מצאה, כי הצעה מס' 1 תוקנה ידנית באופן ששינה את ההצעה הזוכה.

- ✓ וועדת רכש מתאריך 30/08/2021 הצעות מחיר עבור גינון כיכרות ואי תנועה בכביש 804+805 הוגשו 3 הצעות כדלקמן:

1. הספק משתלת סחנין הצעה בסך 166,600 ₪.
2. הספק גני יסמינה סאמח נעמאנה בצעה בסך 157,000 ₪.
3. הספק גינון אלבאטוף חמודי הצעה בסך 156,500 ₪.

הצעה מס' 2 זכתה בעבודה.

הביקורת מצאה כי הפרש המחירים הוא 500 ₪ בלבד ולא נעשה שימוש במרכיבי איכות לקבלת ההחלטה כדוגמת ניסיון מקצועי והמלצות. בנוסף סכום התקשרות זה עולה על הסכום הנדרש לביצוע מכרז זוטא.

חוזים והסכמים

על פי תקנות חובת המכרזים, תשנ"ג-1993, משרד הפנים מגדיר סכומים להגדרת הליכי רכש (על פי הטבלה המפורטת בתחילת פרק זה) .
הביקורת בדקה ומצאה, כי לא מתבצעים מכרזים בסכומי התקשרות המחייבים מכרז. כך לדוגמא:

- ✓ גינון אלבטוף חמודי- על סכום של 150,000 ₪ יש חובת מכרז ולא נעשה מכרז זוטא.

- ✓ שיווק אלג'למה- רכישות שנתית מעל 180,000 ₪ לא נעשה מכרז זוטא.
- ✓ ניבין טיולים והסעות- נמסרה רק כרטסת, רכש שנתי מעל 700 אלפי ₪ לא בוצע מכרז פומבי .

מכרז מסגרת

לפי תקנות חובת המכרזים סעיף 17(ו) , תשנ"ג-1993 מכרז מסגרת הוא:

17ו. *(א) מכרז מסגרת הוא מכרז פומבי שבו נבחר יותר מספק אחד (כל אחד מהם ייקרא להלן בתקנה זו – ספק מכרז מסגרת), אשר על פי תנאי המכרז ייכרתו בעקבותיו הסכמי מסגרת עם כל ספק מכרז מסגרת, וזהות הספק ממנו תבוצע בפועל כל הזמנה של טובין, עבודה או שירותים תיקבע מפעם לפעם במהלך תקופת הסכם המסגרת, לפי תנאי מכרז המסגרת.*

(ב) לעניין זה, "הסכם מסגרת" – הסכם לרכישת טובין, עבודה או שירותים, שנכרת עם ספק מסוים בנושא מסוים ולתקופה מוגדרת, כאשר פירוט הטובין, העבודה או השירותים שיסופקו במסגרתו, כמותם או היקפם, אינו ידוע במועד כריתת ההסכם, והוא נקבע בידי המזמין, בדרך של ביצוע הזמנות מפעם לפעם, בתקופת ההסכם.

(ג) ועדת מכרזים רשאית לערוך מכרז מסגרת, לתקופה המזערית הנדרשת בנסיבות העניין אשר לא תעלה על 5 שנים, אם יש בו יתרון ממשי לעורך המכרז בתנאי רכישת הטובין, העבודה או השירותים, או שיש בעריכת מכרז כאמור כדי לייעל באופן ממשי את עבודת המשרד, ובלבד שהתקיים אחד מאלה.

לביקורת נמסר, כי קיימים מכרזי מסגרת בתחומים ציוד משרדי, חומרי ניקוי וחשמל כולל תיקונים וחומרים.

הביקורת מצאה, כי העירייה לא ערכה מכרזי מסגרת בתחומים נוספים כגון: אחזקה, חומרי בניין, מזון, מזגנים ותיקונים.

כך לדוגמא:

- ✓ ספק למוצרי מזון חוטבא עיסמאיל. מספק לעירייה מוצרי מזון באופן שוטף, ללא הסכם התקשרות או מכרז מסגרת
- ✓ ספק לחומרי בניין בני סעיד עוואד. מספק לעירייה חומרי בניין באופן שוטף, ללא הסכם התקשרות או מכרז מסגרת
- ✓ מ.ב התקנת מזגנים – מבצע תיקוני מזגנים ואף מספק חלפים ומזגנים לפי הצורך, ללא מכרז או הסכם התקשרות

רכישות ע"י המחלקות

כאמור מחלקת הרכש כוללת מנהל רכש בלבד. לביקורת נמסר על ידי מנהל הרכש, כי הצעות המחיר מתקבלות על ידי המחלקות ולא על ידי מחלקת הרכש.

באופן מעשי הליכי הרכש הנ"ל מבוצעים על ידי המחלקות ולא על ידי מנהל הרכש. הגשת הצעות המחיר למחלקות ולא ישירות לרכש, עלולה לכאורה ליצור חוסר הוגנות ופגיעה בהליך הרכש התקין.

בנוסף, קיים סיכון לבחירה בזבזנית ולא מקצועית של פרטי הרכש. כך לדוגמא:

- ☒ רכישת מזגנים שאינם תואמים את הצרכים מבחינת כוח מזגן, דגמים וחברה.
- ☒ הזמנת ציוד דיגיטלי כגון מחשבים ללא הבנה מתאימה בצרכי השטח. לדוגמא, רכישת מחשב לחינוך שכולל פונקציות/ יכולות שאינן נדרשות בגן ילדים/ ביה"ס.
- ☒ הזמנת עבודות מקצועיות בתחום הבנייה והשיפוצים, באמצעות קבלנים ללא רישיונות והסמכות מתאימות.

המלצות

- הביקורת מעירה בחומרה, כי הטיה מכוונת של הצעות מכרזים היא פסולה ועלולה אף להביא לדרישה לחיוב אישי של בעלי התפקידים האחראים על כך.
- הביקורת ממליצה, לשלב מרכיבי איכות של ניסיון מקצועי, המלצות וותק בענף בהליכי ההתקשרות. בעיקר בהתקשרויות בסכומים גבוהים ובעבודות הדורשות מומחיות או מורכבות כגון אחזקה, מחשוב, בניין ושיפוצים.
- הביקורת מדגישה, כי חובה לעמוד בדרישות מנהל תקין ולקיים מכרזים על פי הגדרות החוק ובהתאם לסכומי ההתקשרות. הביקורת מציינת, כי הפרת חובת עריכת מכרז עלולה אף להגיע לכלל חיוב אישי של בכירי העירייה.
- הביקורת ממליצה, כי העירייה תערוך מכרזי מסגרת בתחומים נוספים – כגון רכש מזון וחומרי בניין, אחזקת מזגנים, עבודות עפר וכו''. יתרונות מכרזי מסגרת ברורים - סכום גדול מרוכז ועריכת מכרז בצורה מקצועית מביא להשתתפות ספקים נוספים ולהגדרה מדויקת יותר של הצרכים ומכאן ליעילות וחיסכון הרכש. בנוסף, מכרז כזה אומנם דורש השקעת זמן חד פעמית בעריכתו, אך בתקופת תחולת המכרז, נחסך זמן רב על יציאה

להליך רכש על כל פעילות קטנה (בקשת וקבלת הצעות מחיר, העברה לוועדת רכש ואישור הספק) .

- הביקורת ממליצה על עריכת מכרזי מסגרת בתחומים הבאים: אחזקה, חומרי בניין, מזון, מזגנים, תיקונים, עבודות עפר ועוד. מומלץ, כי מחלקת הרכש תנתח את כל רכישות העירייה ותקבע, באילו מהן יש לצאת להליך של מכרז מסגרת.
- הביקורת ממליצה לרכז את הרכש דרך מחלקת הרכש ולא דרך המחלקות, לאור החסרונות שהוצגו לעיל.

3. מאגר ספקים

מאגר ספקים עירוני, כולל רשימת ספקים שנמצאו מתאימים על ידי העירייה להיכלל במאגר עירוני. המאגר, נועד לשמש את העירייה לצרכי ביצוע פנייה לספקים ומייתר את הצורך באיתור ספקים מתאימים בכל התקשרות. קיומו של מאגר ספקים עירוני, מאפשר לעירייה לנצל את יתרונה הטמון בגודלה ובהיקף התקשרויותיה, וכן מאפשר ייעול תהליכים בפנייה לספק רלוונטי ובתהליכי בקרה.

סעיף 8(ב) לתקנות העיריות (מכרזים), תשמ"ח-1987 קובע, כי בהליכי מכרז זוטא, יש לנהל מאגר ספקים, הועדה תנהל רשימה של ספקים וקבלנים, אשר רשאים להשתתף במכרז זוטא ותקבע את אמות המידה שלפיהן יפנו אל הספקים והקבלנים האלה; רשימה זו תהיה פתוחה לעיון הציבור; כל ספק או קבלן רשאי לבקש לצרפו לרשימה האמורה והועדה תדון בבקשתו; החליטה הועדה שלא לצרף קבלן או ספק כאמור לרשימה, או החליטה למחוק ספק או קבלן מהרשימה, תנמק את החלטתה; לא תחליט הועדה אלא לאחר שאפשרה לאותו ספק או קבלן להביא את טענותיו בפניה.

בהליכי רכש אשר אינם מגיעים לסכום המחייב עריכת מכרז זוטא, אין חובה לנהל רשימת ספקים. למרות זאת, ניהול מאגר ספקים ופנייה לספקים מתוכו, גם לצורך קבלת הצעות מחיר לפני ביצוע הליכי רכש בסכומים הנמוכים מהסכום הפטור ממכרז, מאפשר ניהול הליך קבלת הצעות מחיר שוויוני, שקוף ויעיל יותר.

ממצאים

לביקורת נמסר, כי קיים מעין מאגר ספקים, אך מדובר למעשה בנתונים המבוססים על הנהלת חשבונות והכוללים רק פרטי ספקים שעבדו בעבר עם העירייה. לא קיים בעירייה ספר ספקים על פי התקנות. על ספר כזה לכלול מידע על תחום ההתמחות של הספק, מיון לפי תחומים, מידע על התקשרות קודמת עם הספק, ניסיון בעבודה עימו בעירייה וברשויות אחרות ועוד. על ספר הספקים להיות מעודכן באופן שוטף. יצוין גם, כי בהתבססות על נתוני ספקים המצויים במערכת הנהלת החשבונות, לא ניתנת למעשה הזדמנות לספקים חדשים להירשם ל "מאגר" ורק מי שעבד עם העירייה בזמן האחרון ייכלל ברשימה זו. הביקורת מעירה, כי מאגר ספקים ישן, מביא לכך שאותם ספקים נבחרים שוב ושוב, ללא תחרות אמיתית על רמת העבודה/ השירות והמחירים.

המלצות

יש לנהל ספק ספקים, על פי התקנות, כולל מידע על תחום ההתמחות של הספק, מיון לפי תחומים, מידע על התקשרות קודמת עם הספק, ניסיון בעבודה עימו בעירייה וברשויות אחרות ועוד

יש לפרסם באתר האינטרנט העירוני, הזמנה לספקים להצטרפות לספר הספקים העירוני. על הפנייה לכלול את כל הטפסים הרלוונטיים וצורך ההצטרפות למאגר. ספר הספקים אמור לכלול ספקים מתחומים שונים. יש לבקש מהספקים להגיש הוכחות על הכשרות ואסמכות, ניסיון מקצועי והמלצות.

ניתן לקבוע, כי בתחומים מסוימים, על הספק לעמוד בסטנדרט מקצועי מינימאלי, על מנת להיכלל בספק הספקים. כך לדוגמא, ניתן לקבוע, כי על מנת להירשם כמודד, יש להציג תעודת מודד וניסיון מקצועי של 3 שנים ומעלה.

4. וועדת רכש

על פי הקבוע בסעיף 5 לתקנות העיריות (הסדר רכישות, ניהול מחסנים, רישום וניהול טובין), תשנ"ח-1998 (להלן: "תקנות העיריות (ניהול טובין)"), *על הרשויות המקומיות למנות ועדת רכש ובלאי. כל עסקת טובין של העירייה בכלל, ועסקה הפטורה ממכרז בפרט, מחויבת באישור ועדת רכש ובלאי.*

סעיף 8 לתקנות העיריות (ניהול טובין) קובע כי "לא תבוצע רכישה אלא באישור מראש מאת ועדת רכש ובלאי שניתן באמצעות מנהל רכש ואספקה, ובכפוף להוראות כל דין." כלומר, על ועדת רכש ובלאי לאשר את ביצוען של רכישות הטובין של העירייה הפטורות ממכרז.

חוזר מנכל 1/2009 מתאריך 06.01.2009 (להלן: "חוזר המנכ"ל"), קובע בעניין הרכב ועדת רכש כי *"לאור ההיבטים המקצועיים הנוגעים לפעולת הוועדה והצורך במתן ביטוי – בין היתר – להיבטים הכספיים והמשפטיים הנוגעים לפעילותה, הננו ממליצים ליתן בהרכב הוועדה ייצוג לגזבר העירייה וליועץ המשפטי לעירייה".*

סעיף 166(א) לפקודת העיריות (נוסח חדש) קובע כי *"ועדה שחובה להקימה לפי כל דין תכונס לפחות אחת לשלושה חודשים. לא כונסה ועדה כאמור, יורה ראש העיריה לכנסה, והוא יקבע את סדר היום של ישיבת הועדה..."*. כלומר, על הועדה להתכנס לכל הפחות כל שלושה חודשים.

ואולם, ברכישות טובין שוטפות הפטורות ממכרז בסכום הנמוך 143,100 ₪, ועדת הרכש רשאית לאשר למנהל מחלקת הרכש ביצוע רכישות אלו ללא אישור פרטני מוקדם מאת הוועדה .

בוועדת הרכש חברים - גזבר, יועמ"ש ומנהל רכש. בוועדת התקשרויות חברים - גזבר, יועמ"ש ומנכ"ל.

ממצאים

הגשת הצעות מחיר שלא על טופס רשמי

תנאי סף פירושו, תנאים הכרחיים, שעמידה בהם נדרשת, ממי שרוצה להתקשר בהסכם מסוים. אי עמידה בתנאי סף, פוסל את ההצעה.

בטופס "בקשה להצעת מחיר" רשמי של הרשות, חלק מתנאי הסף הם הגשת הצעת המחיר על גבי הטופס הרשמי.

הביקורת מצאה, הצעות מחיר שלא הוגשו על הטופס ולכן, היו צריכות להיפסל על פי הגדרות טופס הרשות. כך לדוגמא - בהליך רכש בוועדה מתאריך 19/09/2021 "הצעות מחיר ומחשוב לקמפוס גיל הרך" , נתקבלו הצעות מחיר בטופס של המציעים ולא בטפסים הייעודיים של העירייה. יצוין, כי סכום ההצעות היה מעל 70,000 ₪.

פרוטוקולים

הביקורת עיינה בפרוטוקולים רבים של וועדת הרכש. להלן מספר הערות

- ☒ הפרוטוקולים נכתבים בכתב יד ואינם מוקלדים באופן ממוחשב.
- ☒ הפרוטוקולים אינם ממוספרים בסדר רץ, כך שלא ניתן לדעת ולעקוב, האם כל ישיבות הוועדה התקיימו או חסר תיעוד.
- ☒ בפרוטוקול הוועדה קיים רישום נוכחות, אך חסר רישום חברים חסרים.
- ☒ הביקורת בדקה את תיעוד ההצעות בוועדה ומצאה, כי ישנם מקרים שבהם לא נשמרות ההצעות שלא זכו. תיעוד חלקי של הוועדה וההצעות שהוגשו, עלול להעיד על חוסר תום לב בבחירת המציעים.

כך לדוגמא:

- ✓ בהליך רכש לביצוע "עבודות גידור בבי"ס יסודי", בו נבחר הספק אסיל בן עלי ופא הזמנה מס' 210111 בסכום של 39,708 ₪, לא נמצא תיעוד להצעות נוספות שלא זכו/נפסלו.
- ✓ בהליך רכש, לאספקת ציוד מדעי וטכנולוגי "ציוד וריהוט למעבדות בי"ס מקיף אלבטוף", בו זכה הספק סאקאלאב הזמנה מס' 210025 בסכום של 119,422 ₪, לא נמצא תיעוד להצעות נוספות שלא זכו /נפסלו.

לביקורת הוגשו פרוטוקולים נוספים של וועדות רכש משנת 2021 שדנו בהצעות לביצוע עבודות שונות. לפרוטוקולים אלו לא צורף תיעוד להצעות שהוגשו. כך לדוגמא:

- ✓ ועדת רכש מתאריך 23/01/2021 לביצוע "עבודות סימון מגרש הדרכה במסגרת פעילות תוכנית זהירות בדרכים" - לא נמצא תיעוד להצעות מחיר.
- ✓ ועדת רכש מתאריך 09/03/2021 להזמנת עבודות "ביצוע כביש גן אמירה". לא נמצא תיעוד להצעות מחיר.
- ✓ ועדת רכש מתאריך 21/01/2021 לרכישת "טאבלטים במסגרת תקציב משרד החינוך" לא נמצא תיעוד להצעות מחיר.

נימוקים וחוות דעת

לעיתים, נדרשת התייעצות עם מומחה, על מנת לסייע בקבלת ההחלטה על ההצעה הזוכה. הביקורת מצאה, כי לא מתקיים תיעוד ותיוק של חוות הדעת שבה נעשה שימוש בהחלטה על ההצעה הזוכה. כך לדוגמא:

- ✓ בהליך רכש "הצעות מחיר לשירותי ענן" מתאריך 17/02/20 של איי פי מחשבים- לא צורפה חוות דעת של המנמ"ר של העירייה. הוועדה ציינה כי "ההצעה שנבחרה הכי זולה והכי אידיאלית מבחינת פתרון מחשובי".

המלצות

- יש להקפיד על הגשת הצעות מחיר בטופס הרשמי בלבד. הגשה על טופס זה, תקל על השוואת ההצעות ואחידות בין המציעים.

- הביקורת ממליצה, להקפיד על הדפסה ממוחשבת של פרוטוקול וועדת הרכש. יש לקטלג את ישיבות וועדה באופן רציף וזאת על מנת לשפר את המעקב אחר רצף הישיבות
- בפרוטוקול הוועדה, יש לרשום פרטים גם של חברי הוועדה החסרים וזאת כדי לקיים רישום מלא ולעזור בהקפדה על הרכב חוקי של וועדת הרכש וכן על מנת לוודא, כי כל חברי הוועדה משתתפים בה באופן קבוע.
- חובה להקפיד על תיעוד מלא של כל ההצעות, גם אלו שלא זכו. כך ניתן לבצע בקרה ושמירה על מנהל תקין.
- במידה ונעשה שימוש בחוות דעת, בקבלת החלטה על ההצעה הזוכה, חובה לתעד ולשמור את חוות הדעת, בצמוד לפרוטוקול הוועדה.

5. כשלים בניהול תחום הרכש

הזמנות שהופקו בדיעבד

סעיף 203 לפקודת העיריות (נוסח חדש) קובע כי "*חוזה, כתב התחייבות, הסדר פשרה המוגש לבית משפט או לבית דין על מנת לקבל תוקף של פסק דין או תעודה אחרת מסוג שקבע השר בתקנות ושיש בהם התחייבות כספית מטעם העיריה, לא יחייבוה אלא אם חתמו עליהם בשם העיריה, בצד חותמת העיריה, ראש העיריה והגזבר;...*"

הביקורת מצאה, כי לעיתים הרשות מוציאה הזמנות בדיעבד, לאחר חתימה על הסכם פשרה בין הרשות לספק. למרות אזהרות חוזרות ונשנות של מנכ"ל העירייה בנידון, עדיין מנהלים מזמינים עבודות ללא ביצוע הליך רכש וללא הוצאת הזמנה. על פי חוות דעת של היועמ"ש, הרשות חותמת על הסכם פשרה ומשלמת לספק סכום חלקי בגין העבודות שבוצעו.

כך לדוגמא:

- ✓ הזמנה מס' 2110216 מוסך כאמל עלי מתאריך 31/01/2022 על סכום של 5,850 ₪ נחתם הסכם פשרה, ושולם לספק בגין עבודות שבוצעו ללא הזמנה וללא הליך רכש כנדרש

.

- ✓ הזמנה מס' 211002 מתאריך 10/01/2022, הספק בני עוד חומרי בניין, נחתם הסכם פשרה ושולם לספק בגין עבודות שבוצעו ללא הזמנה וללא הליך רכש .

לביקורת לא נמסר תיעוד להנחיות בכתב /מיילים לעובדים והבהרה בדבר האיסור לבצע הזמנות מספקים ללא הזמנת רכש מאושרת

הצעות מחיר פיקטיביות

תנאי יסודי לתקינות תהליך ההתמחרות, לשמירת כללי השוויון והמנהל התקין וליעילות הכלכלית, הינו, שיתקבלו בו הצעות מחיר אמיתיות, מאת ספקים שברצונם ובכוונתם לבצע את השירות המתבקש.
הצעת מחיר פיקטיבית, היא הצעה שמטרתה לאפשר התקשרות או תשלום לספק אחר, תוך שמירת מראית עין בלבד של תקינות הליך ההתמחרות.

פיצול עבודות/הזמנות

תקנות העיריות (מכרזים) סעיף 5 נקבע: " עמדה עירייה להתקשר בזמן אחד במספר חוזים להזמנת אותם טובין או לביצוע עבודות המהוות למעשה עבודה שלמה אחת, יראו את כל אותם חוזים כאילו היו - לעניין תקנות אלה - חוזה אחד"

הביקורת בחנה את הליכי הרכש אצל הספקים השונים ומצאה, כי במקרים רבים, מחלקת הרכש מפצלת עסקאות בתחומים שונים וזאת כדי להימנע מעריכת הליך הצעות מחיר או מכרז. כך לדוגמא:

- ✓ העירייה רכשה ציוד בשנת 2021 בעלות שנתית של 392,341 ₪ מהספק סאקאלאב ציוד מדעי בשלוש הזמנות נפרדות:

1. הזמנה מס' 210025 בסכום של 119,421.99 ₪ ציוד וריהוט למעבדות בי"ס אלבטוף" בתאריך 16/01/2021 .
2. הזמנה מס' 210026 בסכום של 59,498.34 ₪ "ציוד לחדר מדעים לבי"ס מקיף אלבטוף" בתאריך 16/01/2021.

3. הזמנה מס' 210692 בסכום של 71,085 ₪ "מחשוב קמפוס הגיל הרך אלדורה" בתאריך 29/09/2021.

ניתן לראות, כי הזמנות 2+1 הן הזמנות בעוסקות באותו סוג ציוד, מאותו ספק, לאותו המקום ובאותו תאריך בדיוק. ולכן הפיצול בין ההזמנות הוא מלאכותי בלבד וזאת ככל הנראה, כדי להימנע מביצוע מכרז. סכום ההזמנות יחד מגיע כאמור לכ- 392 אלפי ₪ ועובר את הסכום הפטור ממכרז זוטא.

- ✓ העירייה הזמינה קבלן תשתיות, עבודות תיקונים בכבישים בסכום שנתי של 265,551 ₪ בשנת 2021 בשתי הזמנות נפרדות:

1. הזמנה מס' 210682 בסכום של 80,078 ₪ "תיקון שקעים ובורות בכבישים ברחבי העיר" בתאריך 14/09/2021.
2. הזמנה מס' 200698 בסכום של 104,960 ₪ "פסי האטה" בתאריך 19.11.2021.

לאור סמיכות ההזמנות, הביקורת סבורה, כי העבודות פוצלו במכוון וזאת על מנת להימנע מביצוע מכרז זוטא.

סינמאנה הוריזון בע"מ – אספקת תוכניות תרבות

הביקורת קבלה לבדיקה את הליך ההתקשרות של הספק סינמאנה הוריזון בע"מ. הספק זכה במכרז לאספקת תוכניות תרבות, שפורסם ע"י הרשות.
לוועדת הרכש הובאו הצעות של שני ספקים, עם זאת, התברר, כי אחד מהם הוגש בטעות למכרז זה ולכן סימנאנה הוריזון נותר ספק יחיד. הוועדה והיועמ"ש אישרו את הצעת הספק כספק יחיד לאספקת שרותי תרבות.
להלן הערות הביקורת

- ✓ וועדת הרכש בתאריך 24/04/21 לא תיעדה את ההצעה שהוגשה בטעות לוועדה.
- ✓ בוועדת הרכש צידדו סך של 3 חברים בעד הצעת הספק "הוריזון סינמאנה בע"מ" ו- 3 חברים התנגדו. ההחלטה לא נתקבלה ברוב קולות כנדרש.
- ✓ לא ניתנו נימוקים לבחירת הספק כ "הצעה יחידה" במכרז
- ✓ בהזמנה המקורית שמספרה 210365 לא מופיעה חתימת חשב מלווה.

- ✓ פירוט החשבון שמצורף להזמנה הנו על סך 137,206 ₪. אך בפועל שולם סך 204,960 ₪. הסכום אינו מתאים. לא פורט הרכב השירות שסופק ולא ברור איך הסכום היגיע לכ 205 אלפי ₪ - כמעט 50 מעל הסכום המקורי!

חשמל שבאיטה בע"מ

הספק חשמל שבאיטה בע"מ, סיפק חיבור חשמל, להפעלת מכונת כבישת זיתים בחווה החקלאית.

- ✓ הביקורת מצאה, כי ניתנה הנחה נוספת של הספק על המחיר שנקבע במכרז, לאחר סיום ההליך המכרזי. על פי הנחת המכרז בסך 16.5% הסכום שאמור היה להיות משולם על ההזמנה הוא 10,492 ₪, בפועל שולם סכום של 9,492 ₪. מופיע על גבי ההזמנה " קבלתי הנחה נוספת כמתנה לבית הספר".

מתן הנחה לאחר זכייה, מעלה את החשש, כי נוהל משא ומתן, שלא היה חשוף לחברי וועדת הרכש. משא ומתן כזה אינו תקין ועשוי ליצור חוסר הוגנות ושוויון בין הספקים.

המלצות

- הביקורת מעירה, כי חובה להקפיד על ביצוע הליכי מכרז תקינים בתהליך תקין, על פי תקנות חובת המכרזים, תשנ"ג-1993.
- אין לפצל הזמנות כלל. אין לשלם הזמנות שלא עברו תהליך רכש תקין. יצוין, כי הפרת תקנות הרכש, עשויה להביא אף להליכי חיוב אישי של העובדים
- יש לבצע מעקב ובקרה עבור הזמנות באופן שוטף. יש להגדיר סמכויות ותפקידים למנהלי מחלקות וזאת כדי להביא לניהול הליכי רכש תקינים ולצמצם / למנוע כשלים בהליך הרכש.
- הביקורת מעירה בחומרה, כי הליך המכרז של הספק "סינמאנה הוריזון בע"מ, אינו תקין ואינו עומד בקנה אחד עם דיני המכרזים. אין לשלם לספק ללא חתימה מקורית של חשב מלווה, יש לתעד כל הצעה המוגשת לוועדה.
- אין לקבל "הנחות נוספות על מחיר המכרז" ככל ומנוהל משא ומתן עם מציעים - יש לנהלו בהסכמת וועדת הרכש ותוך דיווח שוטף לוועדה על המהלכים שנעשו.

6. ערבויות וביטוחים

ביטוחים

בדרך כלל בהתקשרויות שוטפות, על הקבלן לערוך שלושה סוגים של ביטוחים – ביטוח עבודות קבלניות, ביטוח צד ג וביטוח חבות מעבידים. בכל החוזים עליהם חתמו הקבלנים, כלול סעיף, על פיו על הקבלנים לבטח את העבודות. לכל המכרזים שמוציאה הרשות, מצורף נספח ביטוח, עליו חותמים הקבלנים בעת הגשת ההצעות למכרז. נספח הביטוח מפרט את סוגי הביטוחים בהם יבוטח הקבלן וכן מציין, כי הקבלן יביא אישורים על הביטוח, שבהם מופיעה עיריית עראבה במוטב לפוליסה.

הביקורת קיבלה רשימה של ספקי הרשות וביקשה לבדיקה את פוליסות ביטוח של התקשרויות אלו, ככל וקיימות. עד סיום הביקורת לא נתקבלו הפוליסות שנתבקשו.

ערבויות

על מנת להקטין סיכונים בביצוע העבודות, על הרשות לדאוג לקבלת ערבויות בנקאיות מתאימות מהקבלנים. בהתקשרויות לביצוע עבודות שוטפות, קיימים שני סוגי ערבות על פי השלבים – ערבות הגשה ניתנת לרשות עם מסמכי המכרז, על מנת להבטיח כיבוד ההצעות הניתנות במכרז. ערבות שנייה היא ערבות ביצוע, הניתנת למשך כל תקופת ביצוע העבודות בפרויקט. לעיתים, בעיקר בעבודות גדולות, ניתנת ערבות שלישית – ערבות בדק; ערבות זו ניתנת לאחר סיום הביצוע של הפרויקט ומטרתה להבטיח כי הקבלן יכבד את מחויבותו לתקופת בדק ויבצע את הביקורות ואת התיקונים הנדרשים לאחר המסירה.

ממצאים

הביקורת קבלה גיליון אקסל, הכולל רשימה של 128 ערבויות. ברשימה מופיעים פרטי הערבויות, סטטוס הערבות, תוקף ותיאור המכרז של הערבות.

מבדיקת הקובץ עולים הפרטים הבאים:

- ✓ כל הערבויות, ללא יוצא מן הכלל, אינן בתוקף נכון לחודש נובמבר 2022. כך לדוגמא: הערבות האחרונה בתוקף, היא ערבות מס' 688883/011. ערבות מכרז של בנק הפועלים

09/2022 להפעלת מתקן קשר אלחוטי ותקשורת סלולארית, התקנת אנטנות קשר בקרה ותקשורת. תוקף ערבות זו עד 10.8.22.

- ✓ ערבות מכרז 10/2019 - ערבות ביצוע מס' 873-130100/94-30-0831-0001/2 נפתחה בתאריך 22.10.2019 ונסתיימה בתאריך 01/11/2020.
- ✓ ערבות מכרז מס' 17/2021 בנושא עבודות תשתיות מחשוב - אספקת והתקנת ציוד קצה מס' 224224/00012 ניתנה בתאריך 31.10.2021 ונסתיימה בתאריך 30.04.2022.

מכיוון שכך, לכאורה, לעירייה אין כלל ערבויות בכל חוזי ההתקשרות שלה וזאת על אף, שבחוזים אלו טמון סיכון רב ועל אף שחלק מהחוזים הגדירו חובת קיום ערבות.

המלצות

- הביקורת מדגישה את חשיבות המעקב אחר קיום הערבויות וביטוחים בכל ההתקשרויות, בהם הם נדרשים. עבודה עם ספקים חיצוניים ללא ביטוח וללא ערבות, מעמידה את הרשות בסיכון משפטי וכספי ולכן חובה לבצע בקרה ומעקב.

7. בדיקת חוזים

לביקורת הועברה רשימת חוזים, כולל חוזים משנים קודמות בקובץ אקסל הביקורת קבלה לבדיקה חוזה של מכרז פומבי 8/2019 "הקמת פארק החילזון עראבה".

ממצאים

ברשימת החוזים, מופיעים חוזים החל משנת 2010 ועד מועד הביקורת – 10.2022. הרשימה כוללת חוזים שהסתיימו זה מכבר. נמצא כי 373 חוזים מתוך 478 הכלולים ברשימת החוזים, נסתיימו עד אוקטובר 2022. לדוגמא:

- ✓ חוזה מס' 455 - הסכם הפעלת משפחתונים לשנה"ל תשפ"ב, נסתיים בתאריך 31/08/2022.

- ✓ חוזה מס' 218 - תכנון גני אלזראעייה - עבד נגאר תב"ר 417, נסתיים בתאריך 31/12/2019.

הביקורת מצאה, כי לא כל סכומי החוזים מעודכנים. ב - 278 מתוך 478 חוזים, לא מצוינים ברשימה סכומי החוזה. לדוגמא:

- ✓ חוזה מס' 180 של הספק עלי אחמד-חוזה פיקוח תב"ר 387, לא מצוין סכום חוזה.
- ✓ חוזה מס' 308 של הספק עלי סעדי - הקמת קמפוס גיל רך, לא מצוין סכום חוזה.

הביקורת בחנה מדגמית, חוזה של מכרז פומבי 8/2019 "הקמת פארק החילזון עראבה". חוזה זה נכלל ברשימת החוזים שהועברה לביקורת. תאריך התחלה 25/07/2019 ועד תאריך 31/12/2030. קבלן ראשי – א.א. בהא.

הביקורת מצאה, כי ערבות מס' 1-634-0670-00-022016-0000039 ע"ש הספק א.א. בהא בע"מ על סכום של 242,500 ₪ לפרויקט הקמת פארק חילזון עראבה מתאריך 12.9.2019 ועד 30/09/2021 אינה בתוקף עוד.

המלצות

- לא ניתן לדעת מהרשימה אלו חוזים עדיין פעילים ואילו לא. – יש לערוך מעקב אחר חוזים ולציין מתי נסתיימו.
- ככל שברשימת החוזים נכללים חוזים לא פעילים - יש להפריד בין חוזים פעילים ללא פעילים וזאת, על מנת להקל על מעקב ובקרה שוטפת על החוזים.
- יש להקפיד על מילוי נתונים ברשימת החוזים, כך יתאפשר מעקב וניתוח נתונים.
- עקב פוטנציאל הסיכון הקיים לרשות, חשוב ביותר לעקוב על ערבויות בתוקף, אל מול חוזים פעילים וזאת על מנת להקטין את סיכוני הרשות ככל שניתן בעבודה מול ספקים.

بلدية عرابة
ص.ب 10 الدالة 30812
تلفون 04-8789666 טלפון

עיריית עראבה
30812 ת.ד 10 מיקוד
פקס 04-6747291 פאקס

www.arraba.muni.il

פרק ג

דוח ביקורת במחלקת בנושא
ביטוחי העירייה
עיריית עראבה

2023

بلدية عرابة
ص.ب 10 الدالة 30812
تلفون 04-8789666 טלפון

עיריית עראבה
30812 ת.ד 10 מיקוד
פקס 04-6747291 פאקס

www.arraba.muni.il

תוכן עניינים

א. מבוא

1. רגולציה

הביקורת התבססה על הוראות החוק והצווים שלהלן:

- פקודת הנזקין (נוסח חדש).
- חוק חובת המכרזים, תשנ"ב-1992.
- תקנות העיריות (מכרזים) תשמ"ח-1987.

2. תיאור הסיכונים הפוטנציאליים בנושא הנבדק

<u>סיכון משפטי</u> - תביעות כנגד העירייה בשל מעשה או מחדל אשר גרם לנזק לצד שלישי ו/או נזק שנגרם על ידי צד שלישי ויצר חבות לעירייה, בשל חוסר יכולת להעביר את הנזק לצד השלישי .**<u>סיכון כספי</u>** - נזק לנכסים, תשתיות או למידע בהיקף מהותי. תביעות כנגד העירייה שבהן היא מחויבת לשאת בנזקיו של צד שלישי .
<u>סיכון תפעולי</u> - פגיעה ביכולתה של העירייה לבצע את תפקידה עקב פגיעה בנכסיה או בתשתיותיה, וכן הסיכון התפעולי הנובע מהיעדרם של תהליכי עבודה נאותים לניהול הסיכונים, בחירת המבטחים, רכישת פוליסות ביטוח, חידושן במועד של הפוליסות וטיפול לקוי בדרישות נזק שהתקבלו
<u>סיכון מוניטין</u> - פגיעה בשמה של העירייה בשל טיפול לקוי בצדדים שלישיים אשר נגרמו להם נזקים שהעירייה חבה בהם .לנוכח זאת, העירייה נדרשת להליך סדור ומובנה של ניהול סיכוניה, כדי לוודא את סבירות ונאותות היקפי הביטוח ביחס להיקף הסיכונים.

3. מתודולוגיית הביקורת, מטרתה ואופן עריכתה

מטרת הביקורת הינה לבחון את קיומן של פוליסות ביטוח מספקות ומתאימות לצורכי העירייה ואת הליכי העבודה בתחום חידוש פוליסות הביטוח.
הביקורת בדקה את מערך הביטוחים של העירייה, בחינת נאותות תהליכי העבודה בתחום חידוש פוליסות הביטוח, וידוא קיומן של פוליסות ביטוח מספקות ובעלות תוקף אצל ספקי שירותים, ונאותות תהליכי הטיפול בדרישות נזק. תוך התמקדות בנושאים הבאים:

- מדיניות הביטוחים של העירייה
- נהלי עבודה
- התקשרויות עם יועצים
- חידושי פוליסות
- ביצוע סקרי מחירים וקבלת אישורים בהתאם.
- היקף כיסויים והחרגות בפוליסות
- גבולות אחריות וסכומי השתתפות עצמית.
- תביעות שהוגשו כנגד העירייה
- תשלומי פוליסות.

- סבירות הפרמיות, גבולות אחריות וסכומי השתתפות עצמית
- בחינת ביטוח חסר
- אופן הטיפול בתביעות
- בחינת ההתקשרות מול חברות הביטוח, לרבות אופן ההתקשרות ותהליך חידוש הפוליסות.
- בחינת תהליכי העבודה אל מול היועץ הביטוחי של העירייה, לרבות ההתקשרות, בחינת שירותי הייעוץ המתקבלים, עמידה בתנאי ההסכם ותהליך ההתחשבנות עם היועץ.

הביקורת התבצעה באמצעות:

- קיום שיחות עם בעלי תפקידים רלוונטיים
- סקירת מסמכים רלוונטיים שהועברו ע"י העירייה, כגון: פוליסות ביטוח, מכרזים שפורסמו, הצעות מחיר של יועץ חיצוני, תביעות שהוגשו כנגד העירייה (מכוסות ושאינן מכוסות לרבות), תביעות תלויות ועוד.
- ביצוע בדיקות בלתי תלויות בנוגע לתהליכי העבודה של העירייה, לרבות בחינת החרגות בפוליסות הקיימות, בחינת גובה הפרמיה וגבול האחריות.

4. רקע

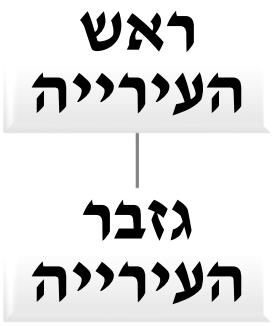
העירייה מחזיקה בנכסים רבים המשמשים אותה לפעולותיה השונות, לרבות נכסים הניתנים לשימוש ללא תמורה ונכסים המושכרים לצד שלישי. מלבד הצורך השוטף להגן על נכסיה, קיימת לעירייה חבות בגין נזקים או פגיעות, שנגרמו לנפגעים בגוף או ברכוש כתוצאה ממעשה או מחדל של העירייה.
פעילות העירייה והיקף נכסיה חושפים אותה לסיכונים רבים. התממשות סיכון עלולה לגרום לנזקים מסוגים שונים, כגון: כספיים, איכות הסביבה, מוניטין. תביעות משפטיות ואף פגיעה בחיי אדם.
על מנת למזער את היקף הנזק העשוי להגרם עקב אותם סיכונים, רוכשת העירייה פוליסות ביטוח בתחומים שונים, כגון: אש, אחריות כלפי צד שלישי, חבות מעבידים, אחריות מקצועית, תאונות אישיות, הוצאות משפטיות ורכב.

להלן הביטוחים הקיימים בעירייה:

תחום ביטוח	חברה מבטחת	פרמיה לשנת 2022-2023	תוקף הפוליסה	קיים אישור ועדת רכש/ מכרזים
ביטוח רכוש וחבויות	הפניקס	989,465 ₪	01.06.22-31.05.23	V
ביטוח הוצאות משפטיות	הראל חברה לביטוח בע"מ	1,648 ₪	15.09.22-31.10.22	ביטוח בוצע באמצעות משכל
ביטוח תאונות אישיות לתלמידים	איילון חברה לביטוח בע"מ	514,050 ₪ (69 ₪ לתלמיד)	01.09.22-21.08.23	-

תחום ביטוח	חברה מבטחת	פרמיה לשנת 2022-2023	תוקף הפוליסה	קיים אישור ועדת רכש/ מכרזים
ביטוח תאונות אישיות לתלמידים השוהים בתאגידים שאינם עירוניים	איילון חברה לביטוח בע"מ	20,700 ₪	01.09.22-21.08.23	-
ביטוח רכב	הכשרה חברה לביטוח/הראל חברה לביטוח			אין

5. מבנה ארגוני:



כפועל יוצא, גזבר העירייה הוא הגורם היחיד מטעם העירייה אשר אמון על תחום הביטוחים. לדעת הביקורת, קיימת ריכוזיות תפקידים לגזבר העירייה ותלות בגורם מרכזי אחד (ראה הרחבה בסעיף 7).

ב. יחידת הביטוח בעירייה

6. נהלים

נהלי עבודה מאפשרים לארגון להפעיל את סמכותו בשקיפות וכוללים מנגנוני בקרה ודיווח של תהליכי העבודה ופיקוח עליהם. קיומם של נהלי עבודה מעודכנים מהווה כלי ניהול אפקטיבי ותורם לשימור הידע, סדר, ארגון, אחידות ולתיאום בין היחידות השונות.

נמצא, כי כלל תהליכי העבודה של יחידת הביטוח נסמכים על הידע והניסיון של גזבר העירייה ועל פי נוהג בעל פה בלבד. הגזבר הינו בעל ידע רב ושנות ותק רבות בעירייה, עם זאת כל שינוי במבנה הארגוני בעירייה עלול להוביל להיעדר שימור ידע.

לא נמצא כל תיעוד לנהלים או הנחיות עבודה כתובים לתהליך רכישה וניהול פוליסות ביטוח בעירייה ובעיקרם:

- ביצוע מיפוי סיכונים ובדיקת הכיסוי הביטוחי הנדרש.
- ביצוע סקרי מחירים לבדיקת שיעור הפרמיה
- אישור מערך הביטוחים על ידי הנהלת העירייה.
- פיקוח ובקרה אחר תשלומים בגין מערך הביטוחים (רכוש, רכב, וכו')

בהיעדר נוהל פורמלי כתוב ישנה חשיפה בין היתר לאי שימור הידע. הביקורת רואה חשיבות רבה לקיום נוהל אשר יסדיר את פעולות העובדים בביצוע תפקידיהם וכן במטרה לסייע בהבנת תהליכי העבודה ושימור הידע בעירייה.

המלצה 1:	<u>נוהל כתוב</u>: שיתייחס לכלל תהליכי העבודה, הבקרות וממשקי העבודה מול הגורמים השונים לצורך ניהול ושימור הידע של החברה ומניעת תלות בגורם מרכזי אחד.

7. הכשרה

כאמור, גזבר העירייה אמון על ביצוע הביטוחים השונים בעירייה. מדובר בתחום מורכב המצריך גורם נוסף לצורך בקרה אחר קביעת הביטוחים והשלכותיו. מסקירת הביקורת עולים הממצאים הבאים:

- לא מונה גורם נוסף האמון על תחום הביטוח, קרי על הטיפול בכל הנושא הביטוחי-עירוני, ובכלל זה, רכישת פוליסות ביטוח, טיפול בדרישות נזק המתקבלות בעירייה ופיקוח על קבלת אישורי קיום ביטוחים של קבלנים[1] העובדים עם העירייה.
- לגזבר קיימת הכשרה בסיסית בתחום, ללא הכשרה פורמלית בעולם הביטוח. הכשרתו מתבססת על ידע מקצועי שנצבר לאורך השנים.
- לא קיימת תוכנית הדרכות רב-שנתית בתחום לגורם. תחום הביטוח עשיר ברגולציה והבנה מקצועית החשובה לניהול ותפעול הנושא, כמו גם שהכשרת גורם בתחום הביטוח עשויה לשפר את ביצועי העירייה ויכולותיה, ואף לאפשר בחינה מקצועית יותר של פוליסות הביטוח השונות מעבר לניסיון שנצבר בפועל.

המשמעות היא שכלל פעילות מערך הביטוח מבוצעת על ידי עובד אחד, גזבר העירייה.

מצד אחד נוצרה תלות של העירייה בגורם אחד ומצד שני בשל עומס הקיים לגזבר מתוקף תפקידו עלול להיווצר קושי במתן מענה להיקפי העבודה והפעילות בתחום הביטוח.

יש לציין, כי לצורך קבלת החלטות ביטוחיות (לצורך מכרז) העירייה התקשרה עם יועץ ביטוחי לקבלת שירותי ייעוץ וליווי בתחום (ראה סעיף 9).

[1] בדוח זה לא נבדק נושא ביטוח קבלנים

המלצה 2:	הביקורת ממליצה לבחון בניית תוכנית הכשרות רב שנתית עבור הגורם שאמון על תחום הביטוח.
המלצה 3:	הביקורת ממליצה למנות גורם נוסף לצורך תכלול ותפעול תחום הביטוח ומניעת תלות בגורם אחד.

8. קביעת מדיניות ביטוחים ותיאבון הסיכון

אישור הביטוחים כרוך בקבלת החלטות בעלות השלכות כספיות מהותיות, הן בעת אישורן והן בזמן עתידי. מדיניות הביטוחים של העירייה אמורה להגדיר, בין היתר, את תיאבון הסיכון עבור סוגי הביטוחים, ובהתאם אליהם נדרש לפעול הגזבר.

קיימת חשיבות לגיבוש מדיניות כתובה של העירייה בנושא מערך הביטוח בדגש על תהליכי בקרה ופיקוח שלהם חשיבות רבה, בעיקר בנושא עתיר תקציב.

מסקירת הביקורת עולה, כי:

- בעירייה לא מבוצע תהליך סדור של מיפוי והערכה לסיכונים אחת לתקופה.
- מערך הביטוח בכללותו לא מובא לדיון ואישור הנהלת העיר.
- לא קיימת מדיניות ביטוחים המאושרת על ידי הנהלת העירייה. נכון להיום, הגדרת תיאבון הסיכון נקבע על ידי הגזבר או מי מטעמו (היועץ החיצוני). משיחות שערכה הביקורת עולה, כי ההחלטה בתחום הביטוח מאושרת בוועדת מכרזים על פי המלצת היועץ החיצוני. נציין, כי האחריות לקיום מערך ביטוחים מותאם לסיכונים הניתנים לביטוח הינה של העירייה ומוטלת על הנהלת העירייה ולא על יועצי הביטוח. להלן לדוגמא:

  רכישת ביטוח הינו מרכיב מהותי במתן מענה לסיכונים שונים בארגון. גבולות האחריות נקבעו תוך התייעצות עם יועץ הביטוח של העירייה, בהתאם לגבולות האחריות בשנה קודמת ובהתאם להערכתו לשינויים שבוצעו ובהתאם להערכת הנכסים ע"י מחלקת הנכסים בעירייה.

  במסגרת הביקורת על מערך הביטוחים בעירייה ציפתה הביקורת למצוא מיפוי והערכה לסיכונים מהותיים שהמענה לחשיפה, יהיה פוליסת הביטוח.

המלצה 4:	יש לבצע אחת לתקופה מיפוי והערכת סיכונים ולעדכן את מערך הביטוחים בעירייה בהתאם לצורך.
המלצה 5:	מומלץ על קביעת מדיניות ביטוחים על ידי הנהלת העירייה שתגדיר, בין היתר, את תאבון הסיכון של העירייה עבור כל אחד מהביטוחים וכן את נאותות הכיסויים והתנאים המרכזיים של הפוליסה, כמו כן לקיים דיון ולקבל את אישור הנהלת הקופה לשינויים מהותיים בתנאי ובעלות הביטוחים

ג. ייעוץ וליווי בתהליכי הביטוח השונים

9. התקשרויות לצורך ייעוץ ביטוחי

בנובמבר 2021 העירייה התקשרה עם יועץ ביטוחי לתקופה של שנה אחת בלבד (ללא אופציה לשנה נוספת) לצורך ייעוץ והכנת נספחי ביטוח לעירייה. ההתקשרות בוצעה באמצעות קבלת הצעות מחיר.
מסקירת הביקורת אחר תהליך ההתקשרות עם היועץ הביטוחי עלו הממצאים הבאים:

- הביקורת לא קיבלה לידיה חוזה התקשרות עם היועץ הביטוחי, אלא רק הצעה שהוגשה מטעמו, המקנה לו תשלום בסך של 680 ₪ לחודש.
- העירייה פנתה ל- 3 יועצים לצורך קבלת הצעת מחיר לבחירת יועץ הביטוח, וקיבלה 2 הצעות בלבד. העירייה בחרה ביועץ הביטוח מכיוון שהצעת המחיר שהגיש הייתה נמוכה משמעותית מהתעריף ששולם בעבר ליועץ הקודם, קרי פער של כ-14,000 ₪.
- התקבל ייעוץ ביטוחי בסך של כ-9,547 ₪ לשנה, קרי מדובר בכמות שעות נמוכה, המצביעה על כך שיחידת הביטוח בעירייה מסתמכת על ניסיון מקצועי והיכרות רבת שנים של הגזבר עם שוק הביטוח, וכמעט ולא נעזרת ביועץ ביטוחי.
- העירייה טרם שילמה את חובה ליועץ- קיים חוב ע"ס של כ-9,547 ₪ בגין תקופה של שנה. יש לציין, כי חשבוניות העסקה תואמת להצעת המחיר שהתקבלה ואושרה בוועדת רכש.
- ההתקשרות הינה לצורך הכנת נספחי ביטוח לעירייה, קרי קיימים נושאים נוספים שלא נכללו במסגרת הצעת המחיר, כדלקמן:
  - ✓ ייעוציים נוספים בתחום, כגון: עריכת מפרטי ביטוח, סיוע בניהול מו"מ עם חברות הביטוח, בדיקת פוליסות הביטוח שתופקנה וכן מתן ייעוץ שוטף במהלך השנה
  - ✓ ייעוץ לעירייה בקשרים עם חברות ביטוח, סוכני ביטוח, מבטחים וגורמי ביטוח אחרים.
  - ✓ עדכון שוטף לגבי שינויים מהותיים בענף הביטוח שיש להם השלכות על תיק הביטוחים העירוני ומתן המלצות מתאימות.
  - ✓ ייעוץ בטיפול בתביעות רכוש.
  - ✓ יעוץ בטיפול בתביעות של צד ג' כנגד העירייה בגין מעשה או מחדל רשלניים של העירייה.
  - ✓ ניסוח פוליסות ביטוח מתאימות, בדיקת הפוליסות המתקבלות מהמבטחים והתאמתן לדרישות ולסיכומים.
  - ✓ המלצות תקופתיות בדבר מערך הביטוחים הנדרש.
  - ✓ בדיקה תקופתית של חשיפות העירייה לסיכונים ותביעות בגין רכוש, נזקי תביעות, נזקי עובדים וכו'.
- ההתקשרות עם יועץ היטוח תמה בחודש אוקטובר 2022, קרי לעירייה לא קיים יועץ ביטוחי לצורך סיוע בנושאים נוספים שהוזכרו לעיל.

המלצה 6:	הביקורת ממליצה להחתים את היועץ הביטוחי על חוזה עבודה, בהתאם לתנאים המקובלים בשוק, בו יוגדר כמות הפניות ליועץ, משך הזמן למתן תגובתו ואופן ההתחשבנות עמו.
המלצה 7:	מומלץ לשקול שימוש משמעותי יותר ביועץ הביטוחי לצורך ליווי בתהליכים השונים.

10. ייעוץ פיננסי

נמסר לביקורת על ידי גזבר העירייה, כי העירייה לא נעזרת ביועץ פיננסי לצורך סיוע בביצוע חישובים כלכליים ובקרות לצורך בחינת כדאיות בעת חידוש מכרז או לחילופין בעת ביצוע שינוי בפוליסה.
נמצא, כי כיום אין פונקציה פנימית אשר נותנת מענה לצורך ביצוע בדיקות כדאיות כלכלית וניתוחי רגישות וכן ליווי כלכלי לאורך חיי הפוליסה.

המלצה 8: מומלץ כי גורם נוסף מיחידת הכספים ישולב בביצוע חישובים מורכבים וכבקרה לניתוחים כלכליים ופיננסיים לאורך חיי הפוליסה.

11. ביצוע סקרי מחירים חידוש ביטוחים ואישורים נדרשים

מסקירת הביקורת אחר הליך חידוש פוליסות הביטוח המהותיות בעירייה עלו הממצאים הבאים:

11.1 ביטוח רכוש וחבויות

ב-19 באפריל 2021, פרסמה העירייה מכרז לקבלת שירותי ביטוח לתקופה שמיום 1.6.2021 ועד ליום 31.05.22. כאשר התקופה תוארך כל פעם באופן אוטומטי לעוד שנה נוספת ועד לסה"כ 60 חודשים מצטברים, כדלהלן:

חברת ביטוח	מועד תחילת הכיסוי הביטוחי לפי המכרז	מועד סיום הכיסוי הביטוחי לפי המכרז
תקופת ההסכם בחוזה	01.06.2021	31.05.2022
הארכה ראשונה לשנה נוספת	01.06.2022	31.05.2023
הארכה שניה לשנה נוספת	01.06.2023	31.05.2024
הארכה שלישית לשנה נוספת	01.06.2024	31.05.2025
הארכה רביעית לשנה נוספת	01.06.2025	31.05.2026

מסקירת פרוטוקול ועדת מכרזים שנערכה ב-20 במאי 2021 וחו"ד של היועץ הביטוחי החיצוני (להלן" **היועץ החיצוני**") עולה, כי במכרז השתתפו 2 חברות ביטוח, כדלקמן:

חברת ביטוח	סכום הצעת המחיר	אומדן העירייה במכרז
הפניקס חברה לביטוח בע"מ	₪ 911,680	₪ 900
איילון חברה לביטוח בע"מ	₪ 1,346,350	

ב-19 במאי 2021, התקבלה חוות דעת מהיועץ הביטוחי לפיה, 2 המצעים לא עמדו בתנאי המכרז שאוסרים שינויים בתוכנו, למעט תוכן שאושר בהליך שאלות הבהרה, וההצעות הוגשו עם שינויים מהותיים בתוכן המכרז. עם זאת, התקבלה הצעת הפניקס לאור מספר סיבות כפי שאפרט להלן:

1. לאור המצב (מתוך ניסיון במכרזים שנערכו בשנים האחרונות) לפיו מכרז נוסף לא ישפר את ההצעות.
2. ביטוחי העירייה פגים בסוף חודש של קבלת חוות הדעת
3. תוכן הביטוח של הפניקס לעומת איילון מיטיב יותר עם העירייה
4. קיים הפרש ניכר בעלות הביטוח בין 2 החברות
5. הצעת הביטוח של איילון חורגת מאומדן העירייה.

מסקירת הליך המכרז וחידושו עולים הממצאים הבאים:

- מהטבלה לעיל עולה, כי העירייה מבוטחת מכוח הארכה של מכרז שיצא בשנת 2021.

מבדיקת חידוש הפוליסה נמצא, כי חלה עלייה בפרמיית הביטוח ובכיסויים.

הביקורת לא קיבלה לידה אישורים פורמליים של יועץ ביטוחי לשינויים אלו.

- בחירת חברת הביטוח במסגרת מכרז הביטוח מאפריל 2021 היה תקין. יחד עם זאת אין להתעלם מהעובדה שלמכרז הוגשו 2 הצעות בלבד עם שינויים מהותיים בתוכנו של המכרז מה שחושף את העירייה לסיכוני ביטוח.

המלצה 9: הביקורת ממליצה למצוא דרכים להגדלת מספר המציעים על מנת להגדיל את הסיכויים לקבלת הצעה ללא שינויים מהותיים מתוכנו של המכרז.
המלצה 10: הביקורת ממליצה כי כל שינוי בהיקף הביטוחי יש להקפיד ולתעד במסמך מטעם היועץ הביטוחי.
המלצה 11: הביקורת ממליצה להקפיד כי כל עליה בפרמיית הביטוח או שינוי בכיסויים הנדרשים יקבלו אישור פורמלי של יועץ הביטוח

11.2 ביטוח רכב

נמסר לביקורת, כי רכישת הפוליסה לא בוצעה באמצעות קבלת הצעות מחיר ולא אושרה על ידי הנהלת העירייה, קרי לא קיים תיעוד בפרוטוקול לאישור רכישת הפוליסה.

עוד עולה, כי חידוש הפוליסה התבצע מול אותו סוכן ביטוח.

לא נמסרה לביקורת כרטסת המפרטת את כל התשלומים שבוצעו לסוכן, על כן לביקורת לא הייתה אפשרות לבצע בדיקה של סך התשלומים ששולמו החל ממועד ההתקשרות ועד שנת 2022.

הביקורת ממליצה לבדוק כי סך התשלומים לא עולים לכדי ביצוע מכרז.

המלצה 12: הביקורת ממליצה כי טרם רכישת הפוליסה ישלחו הצעות מחיר על מנת לבחור את ההצעה האופטימלית והחסכונית יותר לעירייה
המלצה 13: הביקורת ממליצה לבחון כי סכום התשלומים מול הסוכן ביטוח לא עולים לכדי ביצוע מכרז.

ד. פוליסות ביטוח

12. החרגות בפוליסה

להלן הביטוחים העיקריים שנערכו בעירייה, בהתאם למסמכים שהתקבלו:

תיאור	פרמיה שנתית	השתתפות עצמית	השתתפות עצמית במכרז	סכום ביטוח	תקופת פוליסה
אש	244,626₪	נזקי טבע – לא פחות מ-103,964 רעידת אדמה- מינימום 41,586 שוד-נזק ראשון – 519,822 זדון והצתה -311,893 שבר שמשות ושלטים- 832 ש"ח	נזקי טבע – בין 20,000 ל-200,000 רעידת אדמה- כפי שרשום בפוליסה נזק אחר – 15,000	156,986,123	01.06.2022-31.05.2023

אחריות מקצועית	₪ 62,289		₪ 35,000 למקרה מהנדס העיר – ₪ 60,000		01.06.2022-31.05.2023
כסף בכספת ובהעברה	₪ 520	5,189 מכל נזק	₪ 5,000	51,982	01.06.2022-31.05.2023
נאמנות	₪ 3,900	₪ 10,396	₪ 10,000	259,911	01.06.2022-31.05.2023
חבות מעבידים	₪ 163,530	20,000/10000 תלוי מקרה	12,000/10,000 תלוי מקרה	79,000,000	01.06.2022-31.05.2023
צד ג'	₪ 514,600	250,000 עבור נזקי טבע 100,000 בגין נזק אחר	₪ 50,000 למקרה	20,792,864	01.06.2022-31.05.2023
ביטוח הוצאות משפטיות	₪ 1,648	4,500 לכל תביעה		משתנה בהתאם לסוג ההליך וכמות העובדים ברשות (בין 1,350,000 ל-4,500,000)	15.09.22-31.10.22
ביטוח תאונות אישיות לתלמידים	₪ 514,050 (69 ₪ לתלמיד)				01.09.22-21.08.23
ביטוח תאונות אישיות לתלמידים השוהים בתאגידים שאינם עירוניים	₪ 20,700				01.09.22-21.08.23

מסקירת הפוליסות עולים הממצאים הבאים:

- גובה סכומי ההשתתפות מעידים על רמת סיכונים שהארגון "מוכן לסבול".

נמצא, כי נעשו שינויים בסכומי ההשתתפות העצמית בין מה שנרשם במכרז לעלות שנקבעה בפוליסה, קרי ישנו גידול משמעותי בסכומי ההשתתפות העצמית

- בפוליסת רכוש וחבויות בסעיף פריצה ושוד לא נלקח בחשבון ציוד אלקטרוני.
- בפוליסה שנרכשה החל משנת 2021 לא נכלל ביטוח עבודות קבלניות.
- בפוליסת הביטוח נרשם כך: " במקרה בו לא נקט המבוטח באמצעים להקלת הסיכון ו/או לא הפעילם, בהתאם למפורט בפוליסה או ברשימה, יהא המבטח רשאי לבטל את הפוליסה או להקטין את חבותו, הכל בכפוף להוראות החוק, ובמגבלותיו ", קרי בפוליסה קיימות התניות לכיסוי הביטוחי וביניהן, בין היתר, נקיטת אמצעים להקלת הסיכון אשר דורשת מעקב שוטף ע"י גורם אחראי בעירייה. היעדר מעקב אחר קיומם חושף את העירייה להימנעות חברת הביטוח מתשלום כספי התביעה, במקרה של אירוע ביטוחי.

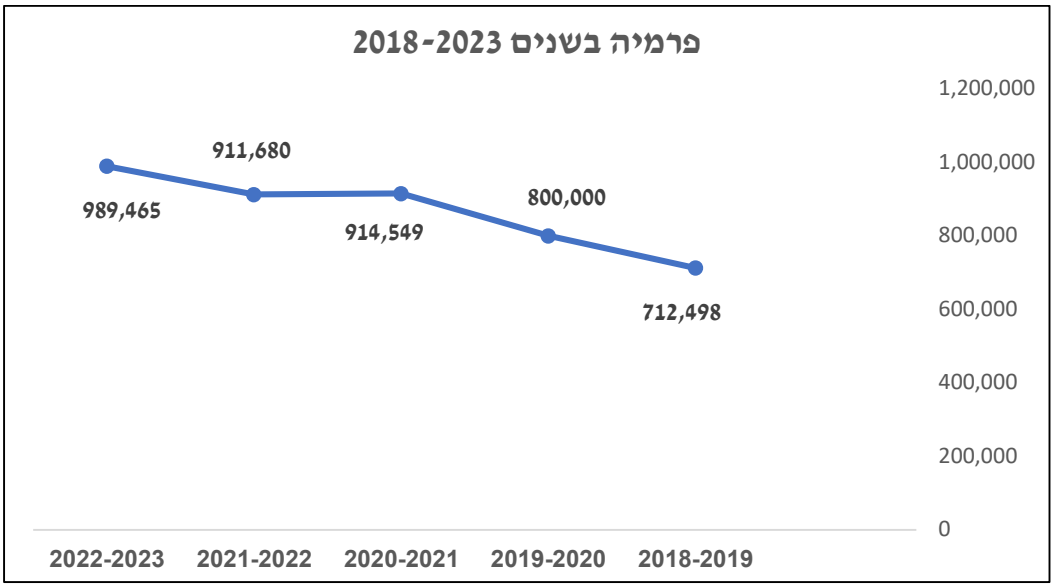
כאמור, לא מונה בעירייה גורם אחראי לצורך וידוא ואימות כל אמצעי המיגון הנדרשים, כולל ביקורת תקופתית שתתועד ותדווח למנהלת מחלקת ביטוח.

המלצה 14: הביקורת ממליצה כי מחלקת הביטוח תנהל מעקב אחר קיום הוראות הביטוח ותוודא כי היחידות השונות בעירייה מבצעות את המחויבויות הנדרשות בהתאם לתנאי הפוליסות.

המלצה 15 : ראה המלצות 4-5.

13. שינויים בפוליסה

להלן תרשים המציג את השינויים בפרמיית ביטוח רכוש וחבויות לאורך השנים :



להלן פירוט ההשתתפות העצמית במהלך חיי הפוליסה:

	2018-2019	2019-2020	2020-2021	2021-2022	2022-2023
אש מורחב - רעידת אדמה	30,027	0	30,388	40,000	41,586
אש מורחב - נזקי טבע	50,046	0	50,647	100,000	103,964
אש מורחב - פריצה - ראשון	501,002	0	507,024	500,000	519,822
אש מורחב - זדון והצתה	300,279	0	300,579	300,000	311,893
אש מורחב - תשתיות	80,074	0	80,154	40000	41,586
חבות עובדים	20,018	0	20,258	20,000	20,000
נאמנות	10,009	0	10,129	10,000	10,396
אחריות מקצועית	45,041	0	45,582	45,000	
צד שלישי לתובע	35,032	0	35,452	-	לא צוין
צד שלישי למספר תובעים	50,046	0	50,647	50000	לא צוין
צד שלישי לתשתיות	100,093	0	100,205	100,000	100,000
כסף להעברה	10,009	0	10,129	5000	5198
קבלנות	10,009	0	150,000	-	

נמצא, כי בשל גידול בעלות התביעות בשנת 2020, בעת חידוש הביטוח חלה עלייה משמעותית בפרמיה העצמית ללא ירידה תואמת בעלות הביטוח.

בפוליסת אש מורחב סעיף נזקי טבע חלה עלייה של כ-100% בסכום ההשתתפות העצמית.

כמו כן, חלה עליה משמעותית (1400%) בפוליסת הביטוח (סעיף קבלנות) בשנים 2020-2021.

המלצה 16 : ראה המלצות 4-5.

14. בחינת ביטוחים חלקיים או חסרים

כאמור בסעיף קודם, ומסקירת הפוליסות השונות בעירייה עולים הממצאים הבאים:

- לעירייה לא קיימת פוליסת נושאי משרה. ביטוח אחריות דירקטורים ונושאי משרה מתייחס לאחריות ניהולית. הפוליסה אינה שמית אלא לפי תפקיד.

פוליסת ביטוח אחריות דירקטורים ונושאי משרה מעניקה הגנה לנושא המשרה בגין תביעות המוגשות נגדו באופן אישי, על מעשים שנעשו שלא כדין ואשר בוצעו במסגרת תפקידו בחברה וגרמו לנזק כספי לתובעים פוטנציאליים. הביטוח מעניק הגנה כנגד תביעות המוגשות עקב פעולה שלא כדין של נושא המשרה במסגרת מילוי תפקידו. פעולה כזו מוגדרת בין השאר כהפרת חובה, התרשלות, הזנחה, טעות, הצהרה מטעה, משגה או חריגה מסמכות, שנעשו על ידי המבוטח בתום לב, תוך כדי ועקב עיסוקו בתאגיד.

- נמנית במערך ביטוחי העירייה פוליסת חבות מעבידים המעניקה כיסוי במקרים של תביעות נזיקין המוגשת על-ידי עובדים בגין פגיעה גופנית או מחלת מקצוע שנגרמה להם תוך כדי / עקב עבודתם. מבדיקת הביקורת עולה, כי הפוליסה מכסה 71% מעלויות השכר (ראה סעיף 15.1).

- ביטוח סייבר כולל כיסוי בגין נזק לעירייה עצמה כתוצאה מסיכוני סייבר, כגון: וירוס ,חדירת גורמים שאינם מורשים וכד, כיסוי נזק הנגרם לצד שלישי כתוצאה מסיכוני סייבר, נזק תוצאתי כתוצאה מנזקי סייבר (כגון: השבתת מערכות מידע), אחזור מידע שניזוק כתוצאה מנזקי סייבר, כיסוי ביטוחי במקרה של סחיטה ואיומים בגרימת נזקי סייבר וכד'.

נכון למועד הביקורת, לא קיימת פוליסת ביטוח סייבר.

- ביטוח מבני ציבור - שערוך נכסי הרשות המקומית לצורך ביטוחם מחייב את הרשות לנהל את נכסי המקרקעין באופן שוטף ולהחזיק מאגר אמין ועדכני של נתונים על הנכסים ,לרבות נתונים על שטחם. מאגר נתונים כאמור יאפשר, בין היתר, לאמוד את ערכם של נכסיה הקבועים ,כדי שערכם החשבונאי ישקף את ערכם העדכני, וכדי שיהיה אפשר לקבוע את ערכי הכינון של הנכסים לצורך ביטוחם ולא להימצא במצב של ביטוח חסר.

הרשות ביצעה סקר מבנים על מנת לאמוד את ערך נכסיה הקבועים עם זאת אינה עדכנה את פוליסת הביטוח בדבר ערכם הכספי ולא קיים כיסוי לכלל מבני הציבור של העירייה. להלן תמונת מצב לגבי סכומי הביטוח בפוליסת הרכוש לעומת סקר המבנים שבוצע:

סעיפים	סכומי ביטוח בפוליסה	פרמיה מקורית	סכומי ביטוח על פי סקר	הפרש סכום ביטוח להוספה	תוספת פרמיה שנתית
מבנים ותכולה	152,827,550	238,146	251,450,000	98,622,450	153,680
תכולה	-	-	37,717,500	37,717,500	58,774
תשתיות	4,158,573	6,480	4,158,573	0	0
סה"כ לרעידת אדמה ונזקי טבע	156,986,123	244,626	293,326,073	136,339,950	212,454

- ביטוח תשתיות מוניציפליות - התשתיות המוניציפליות הם חלק מרכושה של הרשות המקומית וכוללות כבישים ,גשרים, מנהרות, תשתית מים וביוב, תשתית חשמל, מתקני תקשורת, גדרות ושערים ,רמזורים ושלטים .ערכם הכספי הכולל של התשתיות, הפרוסות על כל השטח המוניציפלי של הרשות המקומית, גדול מאוד ונאמד בעשרות מיליוני ש"ח. זאת בעיקר בשל היקפם הרחב של התשתיות ובשל ערכם הרב של מתקני תשתית תחבורה כמו גשרים ומנהרות, שבנייתם ממומנת ברובה על ידי משרד התחבורה.

פיזורן הרחב של התשתיות המוניציפליות בכל תחום הרשות המקומית מקטין את הסבירות שכולן ייפגעו באחת .לפיכך נהוג לבטח תשתיות מוניציפליות על בסיס "נזק ראשון" בביטוח מסוג זה מוסכם בין החברה המבטחת למבוטח כי הרכוש יבוטח בסכום הנמוך מערך הכינון שלו, והחברה המבטחת מוותרת מראש על האפשרות לדרוש הפחתה של תגמולי הביטוח שישולמו לתובע בטענת ביטוח חסר .סכום הביטוח שנקבע ל"נזק ראשון" לתשתיות, הנגזר מחיזוי הנזק המרבי הצפוי, נותן מענה טוב כאשר מבטחים תשתית מוניציפלית רגילה (כבישים ,מדרכות, צנרת מים וביוב וכו') הפרוסה על שטח גדול. זאת משום שפגיעה נקודתית בתשתית כזאת לא תגרום בדרך כלל לנזק גדול. אולם כאשר באים לשקול ביטוח של תשתית נקודתית יקרה כמו גשר מרכזי, אם ערכה יובא בחשבון בחישוב הנזק המרבי הצפוי לשם קביעת סכום הביטוח, תהיה הפרמיה גבוהה מאוד, מכיוון שפגיעה נקודתית בה תגרום לנזק רב. לכן רצוי לשקול לבטח נכס מעין זה בנפרד מהתשתיות הרגילות, כפי שמבטחים מבנה יקר .

הבדיקה העלתה כי היקף הביטוח של תשתיות העירייה המבוטחות כולן יחד על בסיס נזק ראשון הסתכם ב-4,158,573 ₪, תואם לעלות הקמת של פרויקטים שונים בעירייה.**נמצא תקין.**

15. ביטוח רכוש

נכסי הרשות המקומית חשופים לסיכונים רבים ושונים (אש, ברק, פיצוץ, רעידת אדמה, סופה וסערה, שיטפון , פריצה, השחתה בזדון וכד'). מתן הגנה ראויה לרכושה יבוא לידי ביטוי, בין היתר, במיגון ואבטחה של נכסיה ובשמירה על היכולת לקבל פיצוי כספי בסכום ערכי הכינון של כלל הנכסים, לרבות מבנים ותכולתם ותשתיות מוניציפליות, אם יינזקו בדרך כלשהי.

ביטוח נכסים מאפשר לרשות המקומית לעמוד בחובתה להגן על נכסיה על ידי קבלת פיצוי שישמש למימון הקמתם המחודשת של נכסים ותשתיות שייגזקו. רכישת כיסוי ביטוחי מתאים מחייבת היערכות מקצועית, ובכלל זה ביצוע סקר נכסים ושערוכם על פי ערך הכינון שלהם ,ביצוע הערכת סיכוני ,בחירת פוליסות הביטוח המתאימות לכל רשות מקומית ושמירה על עדכניותן .ביצוען של כל אלה מחייב ניהול תקין של מערך הביטוח והכשרת כוח אדם מתאים.

להלן הביטוח העיקרי שנערך בעירייה בהתאם למסמכים שהתקבלו:

שם הענף	חברה מבטחת	פרמיה לשנת 2020	מבוטח	תוקף הפוליסה	קיים אישור ועדת רכש/ מכרזים
אש	הפניקס	244,626 ₪	עיריית עראבה	31.05.2023	V
אחריות מקצועית	הפניקס	62,289 ₪	עיריית עראבה	31.05.2023	V
כספים	הפניקס	520 ₪	עיריית עראבה	31.05.2023	V
נאמנות	הפניקס	3,900 ₪	עיריית עראבה	31.05.2023	V
חבות מעבידים	הפניקס	163,530 ₪	עיריית עראבה	31.05.2023	V
צד ג'	הפניקס	514,600 ₪	עיריית עראבה	31.05.2023	V
סה"כ לתשלום		989,465 ₪			

15.1 חבות מעבידים

כאמור, חבות מעבידים הינה פוליסת ביטוח לעסק, המעניקה לך כיסוי במקרים של תביעות נזיקין המוגשת על-ידי עובדים בגין פגיעה גופנית או מחלת מקצוע שנגרמה להם תוך כדי / עקב עבודתם.
תקופת הביטוח של הפוליסה היא 1 ביוני 2022 עד 31 במאי 2023. בהתאם לפוליסה, שכר עבודה שנתי משוער הינו 79,000,000 ₪.
מבדיקת שערכה הביקורת, עולה, כי נכון למועד הוצאת הפוליסה, קרי חודש מאי 2022, קיימים בעירייה כ-586 משרות בשכר כולל של כ-111,392,568 ₪. דהיינו, העירייה רכשה פוליסה המכסה 71% מעלויות השכר שיש לה בפועל.
תחום חבות מעבידים חושף באופן טבעי את העירייה לסיכונים, על כן נדרש להבטיח כי היקף הכיסוי תואם למצב בפועל.

המלצה 17: הביקורת ממליצה לוודא כי מספר העובדים וסכום עלויות השכר יהיה תואם לפוליסה על מנת שלא יהיה ביטוח חסר.
המלצה 18: הביקורת ממליצה, כי אחת לשנה יחידת הכספים תבצע בדיקה ועדכון בהתאם מול חברה הביטוח.

15.2 רישום הנכסים ושערוכים לצורך ביטוחם

קיימת חשיבות לניהול רישום עדכני של נכסי הרשות המקומית וערכם, על מנת לאפשר לרשות לקבלת החלטות מושכלות בדבר ביטוח נכסיה ולהיות ערוכה מהפן הביטוחי, להתמודד עם נזקים משמעותיים העלולים להתרחש.
כאמור, בהתאם לסעיף 14 לדוח, נמצא כי הפוליסה שחודשה לא מכסה את נכסי הרשות.

15.3 הוספת מבני ציבור חדשים לפוליסת הביטוח

נמסר לביקורת כי קיים מבנה חדש, אולם ספורט אלבטוף אשר החל לפעול לפני מספר חודשים.
מבדיקת הביקורת עולה, כי המבנה לא נלקח בחשבון בעת ביצוע סקר מבנים.
יש לציין, בעת ביצוע הביקורת קיימים מספר מבנים בהליכי בנייה ובעוד כמספר חודשים יתקבלו טפסי 4 בגינם.

המלצה 19: הביקורת ממליצה לעדכן את פוליסת הביטוח בהתאם לסקר המבנים על מנת שלא יהיה ביטוח חסר.
המלצה 20: הביקורת ממליצה כי בעת סיום בניית בתי הספר תעודכן פוליסת הביטוח בהתאם או לחילופין בעת חידוש פוליסת הביטוח (לקראת חודש מאי 2023) יילקחו בחשבון בתי הספר לצורך קבלת כיסוי מלא.

15.4 ביטוח מבנים שבשימוש הרשות המקומית ואינה בבעלותה

רשויות מקומיות משתמשות במבנים שאינם בבעלותן, בין היתר מבנים שנשכרו מגופים עסקיים. נכסים אלו משמשים אותן לפעילותן היומיומית לצורכי חינוך, תרבות, רווחה, חירום ועוד. בחוזי השכירות נקבע, בדרך כלל, כי הרשות המקומית תבטח את הנכס ששכרה בביטוחי רכוש וחבויות. פוליסות ביטוחי הרכוש של הרשויות המקומיות כוללות גם כיסוי ביטוחי וחבויות לנכסים ששכרו.
הסכמי שכירות בגין נכסים יקרים הכוללים התחייבות של העירייה לבטחם מחייבים אותה לעדכן את החברה המבטחת על נכסים אלו ועל ערכם הכספי המוערך ולכלול אותה בביטוח נכסיה.

בפוליסת "ביט" לביטוח אש מורחב של חברות מבטחות נקבע כי נכסים שאינם בבעלות הרשות המקומית אך נמצאים בשימושה, ייחשבו חלק מרכושה "למרות שאינם מכוסים ואינם כלולים בסכום הביטוח... אך בתנאי שהנכסים מבוטחים ביום אירוע מקרה הביטוח על בסיס ערך כינון בביטוח אש מורחב אחר בר תוקף.
מבדיקת הביקורת עולה, כי קיימים 11 מוסדות שאינם בבעלותה.
הבדיקה העלתה כי לעירייה אין נתונים על ערכם הכספי של הנכסים ששכרה, על כן אינה מעדכנת את החברה המבטחת על מבנים ששכרה, סוגיהם וערכם הכספי. עקב כך לחברת הביטוח אין מידע על ערכם של המבנים, ולכן הערך הכספי הכולל של הנכסים המבוטחים ובהתאם גם סכומי הפרמיות המשולמים לחברת הביטוח אינם מעודכנים, משמע קיים ביטוח חסר.

המלצה 21: הביקורת ממליצה לעדכן את החברה המבטחת על נכסים מהותיים ששכרה וכאלה שהתחייבה לבטחם, על ערכם הכספי המשוערך ולכלול אותם בביטוח נכסיה כדי שלא תימצא בביטוח חסר.

15.5 נכסים שהוקצו

משרד הפנים פרסם נוהל הקצאת קרקעות ומבנים ללא תמורה או בתמורה סמלית אשר נועד להסדיר הקצאת קרקע או מבנה בפטור ממכרז ללא תמורה (גם תמורה סמלית במשמע) מאת רשויות מקומיות לגופים הפועלים בתוך תחום הרשות בנושאי חינוך, תרבות, דת, בריאות, רווחה כדי לסייע לו בפעולותיו למען הציבור.
הרשות המקומית יכולה להיעזר בנוהל ובספר ההקצאות על מנת לבצע מעקב אחר ביטוח רכושה הנמצא בחזקת אחר, בין היתר, כדי לדעת אם מקבלי הנכס ביטחו אותו, אם הביטוח נעשה על פי ערך כינון של המכס ואם הרשות נקבעה כמוטבת בפוליסת הביטוח.
מבדיקת הביקורת עולה, כי הרשות אינה מנהלת ספר הקצאות ואין בידיה מידע מדויק/מאגר אמין על נכסים שהוקצו לצורך מעקב ובקרה, ובכלל זה מידע על ביטוח נכסים אלו.

המלצה 22: הביקורת ממליצה לנהל ספר הקצאות לצורך מעקב ובקרה אחר ביטוח נכסים אלו.

15.6 נכסים שהושכרו לאחר

רשויות מקומיות נוהגות להשכיר לגופים אחרים נכסי שבבעלותם ,בדרך כלל בהסכם לשכירות בלתי מוגנת.
כדי להבטיח שהשוכרים יקיימו את תנאי השכירות, ובהם תשלום שכר הדירה שנקבע בהסכם, תנאי השמירה על הנכס ותחזוקתו ותנאי פינויו, יש לעגן את התנאי בהסכם כתוב בין העירייה לשוכרים.
נמסר לביקורת, כי העירייה לא משכירה את נכסיה אלא משכירה לפעמים חדרים בבניין (מרכז מחמוד דרויש) למטרת לימודים, הרצאות, פעילות לילדים מופעים, חוגים.
פעילויות אלו מתבצעות ללא הסכם חתום המסדיר תעריף, מועדים, כמות שעות וביטוח בתוקף.

המלצה 23: מומלץ לעגן הסכם חתום המסדיר את הפעילויות המתבצעות בבניין, לרבות תעריפים, כמות שעות, מועדים וביטוח.

16. פוליסות רכב-

צי הרכב של העירייה מונה כ-14 רכבי עבודה: 7 נגררים, טרקטור, מטאטא ו-5 רכבים רגילים.

מספר רישוי	סוג רכב	ביטוח חובה	עלויות ביטוח מקיף	סה"כ
275-50-801	נגרר כיבוי	799.51	527	1326.51
61-384-89	נגרר תאורה	629.64	141	770.64
61-379-89	נגרר חפ"ק	629.64	527	1156.64
98-538-79	נגרר גנרטור	780.45	504	1284.45
483-25-001	נגרר סע"ר	780.45	504	1284.45
668-74-402	נגרר הובלה	629.54	504	1133.54
241-25-202	גרור רכין לטרקטור	584	504	1088
98-834-79	טרקטור רגיל	1681	1274	2955
159-573	מטאטא		1400	1400
106-903	בובקט		3546	3546
82-917-35	מיצובישי	4544	2272	6816
23-423-37	טויוטה	1990	9000	10990
42-764-64	טויוטה	2224	3569	5793
222-50-102	טויוטה	2393	1390	3783
סה"כ		**17,665**	**25,662**	**43,327**

16.1 היקף הפוליסה

נראה כי העירייה מבטחת את כל כלי הרכב שברשותה, שחלקן הם רכבים ישנים. הביקורת אינה כללה בדיקה של כלי הרכב הללו אך לאור העלויות הבלתי מבוטלות ומכיוון שעבודות תחזוקה מבוצעות על ידי קבלנים, נדרש לבדוק את הצורך ברכישת פוליסות לכל כלי הרכב הללו.

יש לציין, כי ניתן לרכוש פוליסות על אתר, כך שכלי רכב וגרורים שאין בהם שימוש שוטף מחייב לדעת הביקורת בבדיקת הצורך ברכישת הפוליסות המוזכרות מעלה.

16.2 בחירת המבטח

מסקירת עלויות הביטוח עולה, כי רכישת הפוליסות השונות (חובה ומקיף) הינה בהיקף של כ-43,327 ₪.

מדובר בסכום שאינו מחייב מכרז, עם זאת העירייה רוכשת את הפוליסות מאותו סוכן ולכן יכול להיווצר מצב בו על פי דיני מכרזים התקשרות זו תראה כמתמשכת על פני אורך השנים ועל כן תחייב מכרז.

עוד עולה, כי העירייה רוכשת פוליסות מבלי לבצע סקרי מחירים.

המלצה 24: הביקורת ממליצה לבצע תכלול מקיף וניהול תחום הרכב הן בהיבט של התקשרות עם סוכן הביטוח לצורך רכישת הפוליסה והן בהיבט תחזוקה הרכבים ובדיקת הצורך בכלי הרכב או בחינת דרכים חלופיות לצורך בחינת הפוליסות.
המלצה 25: ראה המלצה 13.

16.1 תביעות בתחום הביטוח

מסקירת הליך התביעות אחר מקרה ביטוחי בתחום הרכב עולה, כי העירייה אינה מבצעת בחינה של התאונות שאירעו לעובדי העירייה, קרי העירייה משלמת עבור כל תיקון רכב ללא בוחן מטעם העירייה אשר מוודא שאחריות למקרה התאונה הינה של העובד ותיקון הרכב באחריותו.

המלצה 26: הביקורת ממליצה לבצע בחינה של כל תאונות הרכב שחלו על מנת לבדוק באם התאונות נגרמו על ידי העובד ותיקון התקלה הינה על חשבון העובד.

ה.אופן הטיפול בתביעות

להלן פילוח תביעות (בתחום רכוש וחבויות) לשנים 2017-2020[2]:

שנת חיתום	ענף	תביעות	שולם	תלוי	סה"כ
2017	חבות מעבידים	1	3,873	199,034	202,907
	צד שלישי	7	22,276	636,822	659,097
2018	חבות מעבידים	2	950	181,119	182,069
	צד שלישי	5	102,435	451,658	554,093
2019	צד שלישי	3	200	606,710	606,710
2020	צד שלישי	1	0	635,041	635,041
סה"כ		**19**	**129,734**	**2,710,383**	**2,840,117**

להלן פירוט כלל התביעות בשנים 2019-2021[3]:

שנת חיתום	מספר התביעות	תביעות שנסגרו	סכום תביעה	הערכת יועץ משפטי
2019	25	15 בפשרה/פס"ד	3,132,953	1,920,644
2020	[4]103		[5]955,684	להשלמה
2021	[6]84		[7]819,220	להשלמה
סה"כ	**212**			

מסקירת הביקורת אחר אופן ניהול התביעות, תיעודן, גובה התשלומים, מספר התביעות שנסגרו ביחס לכלל התביעות שהוגשו למחלקה עולים הממצאים הבאים:

- בסוף כל שנה מקבלים רשימת תביעות ומבצעים הפרשה בספרים בהתאם.
- קיים תיעוד מסודר בקבצי אקסל של התביעות, לרבות סטטוס התביעה, סכום התביעה והערכת היועמ"ש, עם זאת לא קיים תיעוד לכל התביעות, קרי לא קיים בכל תביעה מידע אודות עלותה, הערכת יועמ"ש, סטטוס תביעה והשנה בה הוגשה.
- ניהול התביעות אינו מנוהל במערכת ממוחשבת לצורך עדכון, מעקב ובקרה.
- חל גידול משמעותי בכמות התביעות בשנים 2020-2021.
- ברוב התביעות סטטוס התביעה הינו "בטיפול חברת הביטוח", קרי לא קיים מידע בסיסי מחברת הביטוח בנוגע לסטטוס התביעות לצורך מעקב ובקרה אחר תפקוד החברה המבטחת.
- לא קיים נוהל כתוב בתחום תביעות תושבים אשר מסדיר תביעות צד ג' ותביעות תאונות תלמידים – אופן קבלת החלטות בשאלות של כיסוי ביטוחי, ניהול תביעות המוגשות נגד המבוטחים, טיפול במענה על תלונות ומכתבי דרישה, מעקב אחר עמידת חברת הביטוח בהסכם עם העירייה, ניהול מו"מ לפשרה עם תושבים ותשלומי פיצוי.
- הביקורת לא קיבלה לידיה תיעוד לאופן קבלת ההחלטות בתחום התביעות.

---

[2] בהתאם לדוח ניסיון תביעות של חברת הפניקס

[3] בהתאם לדוחות פנימיים של העירייה

[4] מתוכן 5 תביעות משנת 2019

[5] סכומי החשיפה לא מולאו במלואם עבור כל תביעה

[6] מתוכן 47 משנים קודמות

[7] סכומי החשיפה לא מולאו במלואם עבור כל תביעה

המלצה 27:	הביקורת ממליצה לעגן בנוהל כתוב את אופן קבלת ההחלטות בעירייה בתחום הביטוח, ובין היתר: מדרג הסמכויות לאישור תשלום לתובעים, בחינת כמות התביעות המוגשות כנגד העירייה אל מול הפרמיות וההשתתפות העצמית בהן העירייה מחוייבת, סבירות העליות בתשלומי הפרמיה וההשתתפויות העצמיות בחיתוך שנתי, נתונים כספיים, הערכות סיכון, רציפות הכיסוי הביטוחי וסייגים שהוכנסו לכיסוי הביטוחי
המלצה 28:	הביקורת ממליצה לבחון את אופן קבלת מידע מלא אודות סטטוס התביעה מחברות הביטוח.

עיריית עראבה

לשכת מבקר העירייה

פרק ד

ביקורת

הגנת הפרטיות
ואבטחת מידע

1. מבוא

1 בעיריית עראבה פועלות מערכות מידע ממוחשבות ומנוהלים מאגרי מידע רבים לצורך אספקת שירותים חיוניים ומגוונים לתושבים.

2 הגברת שימוש במערכות מידע, וכן הגברת השימוש במאגרי מידע תוך הרחבת אספקת שירותים דיגיטליים לתושבים בשנים אחרונות, מגביר את הסיכון לחשיפת מידע אישי ברבים בזדון או בתום לב דבר שיכול להביא לפגיעה בפרטיות התושבים ו/או עובדי העירייה.

3 כמו כן, שימוש זה חושף את העירייה לסיכונים במרחב הסייבר העלולים לפגוע בפעילותה.

4 סיכוני סייבר עלולים להתממש כתוצאה מניצול של חולשות במערכות, תהליכים וגורם אנושי עד כדי שיבוש הפעילות השוטפת, מניעת יכולת העירייה לספק שירותים לתושבים, חשיפת העירייה לתביעות משפטיות, עיצומים רגולטוריים וכדי.

5 בשנים האחרונות ישנה עלייה משמעותית בהיקף ובעוצמת האיומים בעולם כולו ובישראל בפרט. איומים אלה נובעים מכך שמרחב הסייבר התרחב ממחשב הקלאסי וחושף כל התקן חכם המשתמש ברשת האינטרנט - ובכך מאפשר תקיפה נרחבת, זאת לצד היותו של האינטרנט רשת נטולת גבולות המאפשרת אנונימיות גבוהה לגורמים זדוניים שעברו מפשע פיזי לפשע דיגיטלי, כנ"ל גורמי טרור שבחלק מהמקרים נתמכים על ידי מדינות.

6 בשנים האחרונות גדל היקף התקיפות באמצעות תוכנות נוזקות [8] , (Malware) תוכנות כופרות [9] (Ransomware)שונות ו/או הפרות חוק ו"פשיעת מידע". תוכנות אלה מתפשטות הן דרך רשת אינטרנט בגלישה או דרך דוא"ל והן באמצעות חיבור פיזי של התקני זיכרון שונים למחשבים ברשת העירייה. התקיפות הופכות למתוחכמות יותר ויותר תוך אוטומציה שלהן והפצה המונית ושימוש בטכניקות הנדסה חברתית כדי לפתות משתמשים להפעיל אותן.

7 לשם שמירה על צנעת הפרט ועל הוראות החוק, יש לנקוט אמצעים לאבטחת המידע ומערכי המידע, ולהגן עליהם מפני פגיעה, חשיפה ושינוי במזיד או בשוגג. זאת, באופן שישמרו הזמינות, השלמות, המהימנות, הסודיות והשרידות של המידע ומערכות המידע.

8 <u>חוקים, תקנות והנחיות רלוונטיים בהיבטי הגנת הפרטיות ואבטחת מידע</u>

- חוק הגנת הפרטיות, התשמ"א-1981 (להלן - חוק) להלן הגדרות לפי סעיף 7 לחוק:
  אבטחת מידע - "הגנה על שלמות המידע, או הגנה על המידע מפני חשיפה, שימוש או העתקה, והכל ללא רשות כדין."
  מאגר מידע - "אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב..."
- בחודש מאי 2017 פורסמו תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017 (להלן - תקנות) מכוח החוק. התקנות אשר נכנסו לתוקף ב-8.5.18, מגדירות חובות מפורטות לבעל מאגר מידע, ליישום בקרות תהליכיות וטכנולוגיות לצורך אבטחת מאגרי מידע בהם מנוהל מידע אישי.
- תורת הגנת הסייבר של מערך הסייבר הלאומי, כוללת בקרות מומלצות.
- ב-11 במרץ 2020 פרסם מערך הסייבר הלאומי "המלצות הגנה לארגונים ועסקים לעבודה מהבית בעקבות התפשטות הקורונה" (להלן - המלצות המערך לעבודה מהבית). ראה נספח א'.

[8] תוכנה זדונית המותקנת במחשב ללא ידיעתו של המשתמש ופוגעת בפעולתו התקינה.

[9] תוכנה זדונית המופעלת על מחשב במטרה להצפין את תכולת הדיסק ותוכן המחשב. לאחר מכן מקבל המשתמש דרישה לתשלום כופר על מנת לקבל גישה לקבצים .

9 <u>המשימות העיקריות בהיבטי הגנת הפרטיות ואבטחת מידע של העירייה כבעלת המאגר</u>

- לקבוע מדיניות ונהלים.
- להעריך ולנהל סיכוני סייבר.
- להדריך עובדים ולהגביר מודעות שלהם.
- להקצות משאבים מתאימים.
- לאתר, להגיב ולטפל באירועי אבטחה חריגים.
- לפקח ולבקר באמצעות תפקיד של ממונה אבטחת מידע לגבי יישום דרישות תקנות.
- להטמיע כלים טכנולוגיים נאותים להגנה על מערכות, תשתיות ומאגרים.
- לפקח ולבקר על פעילות מיקור חוץ.

2. מטרת הביקורת והיקפה

מטרת הביקורת הייתה לבחון את נאותות ניהול אבטחת מידע בעירייה על היבטיו השונים, וזאת בהתייחס לדרישות תקנות הגנת הפרטיות, הנחיות רשות הגנת הפרטיות ומערך הסייבר הלאומי ותוך בחינת תהליך יישום הוראות התקנות בעירייה.
כמו כן, ביקשה הביקורת לבחון את אפקטיביות מנגנוני אבטחת מידע הקיימים בעירייה להתמודדות עם מתקפות סייבר, תוך זיהוי חולשות אבטחה, פגיעות ופערים.

התחומים העיקריים שנבדקו:

- פעילות מחלקת מערכות מידע.
- פעילות ממונה אבטחת מידע.
- ממשל תאגידי

במסגרת זו נבדקו, בין השאר, הנושאים הבאים:

- הדרכה והגברת מודעות עובדים.
- ביצוע סקרי אבטחה ומבדקי חדירה.
- פעילות ועדת היגוי בהיבטי אבטחת מידע.
- פעילות ממונה אבטחת מידע.
- גיבוש וביצוע תכנית עבודה בהיבטי אבטחת מידע.
- מדיניות ונהלים בהיבטי הגנת הפרטיות ואבטחת מידע.
- קיום אמצעי אבטחה טכנולוגיים נאותים בפרט בנושא אבטחת גישה מרחוק.
- פיקוח ובקרה על ספקי מיקור חוץ.

3. מתודולוגיה- שיטת הביקורת

לצורך הביקורת נערכו הפעולות הבאות:

- שיחות ותשאול עם בעלי תפקידים שונים בעירייה.
- עיון בחומרים קיימים ותיעוד לפעילות אבטחת מידע.
- ביצוע בדיקות טכנולוגיות מדגמיות:

- שילוב של כלי תוכנה לסריקה מקצועית ובדיקות ידניות שונות.
- מבדקי חדירה דרך האינטרנט בהתאם לכתובות IP חיצוניות שסופקו לביקורת, ומזוהות עם העירייה ואתר העירייה.
- מבדק חדירה תשתיתי.
- ביצוע סריקות לאיתור חשיפות אבטחה בשרתים, בסיסי נתונים, ציוד תקשורת ותחנות קצה באמצעות כלי סריקה מקצועי NESSUS.
- ביצוע בדיקות לנאותות הגדרות אבטחה בתחנת קצה מדגמית.
- בדיקת מחשב נייד ממנו מבוצעת גישה מרחוק.
- בדיקת הגדרות מדגמית במוצרי אבטחה והגדרות גישה מרחוק.
- בדיקת הרשאות גישה, הרשאות חיבור מדיה נתיקה וגלישה באינטרנט.
- בדיקת הקשחת מערכות הדוא"ל.

הביקורת בוצעה בידי יועצים חיצוניים לביקורת, בעלי הסמכות בינלאומיות בתחומי אבטחת מידע וביקורת מערכות מידע (כגון CISSP, CISA, ISO 27001 Lead Auditor) המתמחים בביקורת ויישום רגולציות בתחומי אבטחת מידע והגנת הפרטיות, בניהול סיכוני סייבר ואבטחת מידע ובביצוע מבדקים טכנולוגיים ומבדקי חדירה וסימולציה של תקיפות סייבר.

הביקורת התבססה על בדיקות מדגמיות ואין הכרח שתחשוף כל ליקוי אם קיים. הביקורת מודה על שיתוף הפעולה המקצועי למנהל תחום אבטחת מידע וסייבר בעירייה.

4. תקציר מנהלים

נושאים שנבחנו:

מס' סעיף	נושא
5.1	מדיניות אבטחת מידע ונהלי אבטחת מידע
5.2	ממשל תאגידי (אבטחת מידע)
5.3	ועדת היגוי
5.4	הדרכות ומודעות עובדים
5.5	בקרת הרשאות גישה
5.6	הגנה כנגד מתקפות מתוחכמות
5.7	ניטור דיווח ותגובה לאירועי אבטחת מידע
5.8	מיקור חוץ
5.9	רישום מאגרים ומסמכי הגדרות מאגר
5.10	סיסמאות, זיהוי ואימות
5.11	מיפוי מערכות ונכסים
5.12	גיבוי ושחזור
5.13	אבטחת התקנים ניידים
5.14	גישה מרחוק
5.15	בקרה ותיעוד גישה
5.16	שימוש במערכות הפעלה מעודכנות
5.17	מצלמות אבטחה

תמצית מסקנות מבדקים טכנולוגיים:

בהתבסס על הערכת האבטחה עבור טווחי הכתובות החיצוניות, הפנימיות והמצב הנוכחי של החולשות שזוהו, חלק ניכר מהחולשות שנמצאו וצוינו בדוח המבדקים הטכנולוגיים ובדוח מבדק החדירה התשתיתי, עשויות להוות גורם לפרצות אבטחה. ניתן לתקן פגיעות אלה על ידי ביצוע שיטות העבודה המומלצות וההמלצות שניתנו.

להערכת הביקורת רמת הסיכון של הרשת הפנימית הינה **קריטית**. תוקף זדוני אשר הצליח להגיע לרשת הפנימית, יכול בצורה פשוטה ומהירה להשיג הרשאות דומיין אדמין ושליטה מלאה ברשת הארגונית.

עיקרי הממצאים במבדקים הטכנולוגיים:

- קיימים פרוטוקולים ישנים שאינם מאובטחים
- קיים שימוש חוזר בסיסמאות של משתמשים חזקים
- לא קיים שימוש ב-SMB Signing
- קיימות מערכות הפעלה ישנות
- לא קיימת מערכת EDR\XDR
- קיימות תוכנות לא עדכניות בעלות חולשות אבטחה
- מערכת סינון הדואר, אינה מספקת ומאפשרת קבלה של קבצים זדוניים ופישינג
- חומת האש אינה מוקשחת ברמה מספקת ומאפשרת למשתמשי הארגון גלישה לאתרים העלולים להכיל תוכן זדוני

ריכוז המלצות דוח הביקורת בקצרה:

1. יש להגדיר סט נהלי אבטחה מפורט.
2. יש למנות ממונה אבטחת מידע אשר יבנה תוכנית בקרה לעמידה בתקנות וידווח להנהלה.
3. מומלץ להגדיר ועדת היגוי לנושאי אבטחת מידע אשר תתכנס לפחות אחת לשנה.
4. יש לקיים הדרכות אבטחת מידע לכלל העובדים כאחת לשנתיים, ולהחתים את כלל העובדים על מסמכי שמירת סודיות וכללי אבטחת מידע.
5. יש לבצע מיפוי הרשאות לפי תפקידים ולתקף מיפוי זה לפחות אחת לשנה.
6. מומלץ להחתים עובדים על אישור כניסה לתיבת הדוא"ל שלהם לאחר סיום העסקתם.
7. יש להפעיל בתחנות קצה ושרתים מערכת EDR מתקדמת לאיתור אנומאליות מעבר ליכולות של אנטי וירוס הקלאסי.
8. יש להקשיח הגדרות מערכות האבטחה כמפורט בדוח המבדקים הטכנולוגיים. בפרט להגדיר אימות דו שלבי בכל גישה מרחוק.
9. יש לבצע באופן קבוע (מחזורית) מעבר על הגדרות מוצרי הגנה קיימים, כגון חומת אש, אנטי וירוס וכד'.
10. מומלץ לבחון רכש של מערכת NAC(network access control) אשר תפקידה לחסום גישה לרכיבים לא מאושרים אל תוך הרשת הפנימית.
11. יש לבצע מיפוי מאגרי מידע החייבים ברישום, ולבצע רישום מול הרשות להגנת הפרטיות עבור המאגרים במיפוי. יש לוודא קיום מסמך הגדרות מאגר למאגרים.
12. מומלץ לחזק את מערך הניטור באמצעות מערכת SIEM ו/או צוות SOC מקצועי.
13. יש לוודא קיומם של רשימת מצאי ומיפוי נכסים הכוללים את המערכות והממשקים הרלוונטיים למאגרי המידע. על הרשימה והמיפוי להיות מעודכנים מדי שנה.
14. יש להגדיר בנוהל מדיניות סיסמאות לכלל מערכות המידע והרשת הארגונית.
15. יש לגבש מדיניות סיסמאות מוקשחת ברשת ובכל גישה למערכות/ מאגרי מידע בפועל.
16. מומלץ להגדיר תדירות גיבויים המספקת את צורכי הארגון.
17. מומלץ להחזיק גיבוי קר מנותק לחלוטין מהרשת כהגנה נוספת על המידע במצב בו הגיבויים נפגעו.
18. יש לבצע שחזור מידע גם באופן יזום ולא רק בעת תקלה. מומלץ לבצע שחזור יזום מגיבוי לפחות אחת לרבעון.
19. יש לחסום אפשרות לחיבור מדיה נתיקה בעמדות הקצה. במידת הצורך יש להעביר קבצים דרך שרת הלבנה או להגדיר whitelist לחיבורי מדיה נתיקה מאושרים מראש של הארגון אשר נסרקים ונבדקים לגבי וירוסים בצורה שוטפת.
20. יש להגדיר מדיניות מדיה נתיקה. רצוי לחסום התקנים ניידים באופן גורף ולאפשר רק במקרים חריגים ע"י התקנים אשר נבדקו ואושרו ע"י גורם טכני.
21. יש לשמור את נתוני לוג הגישה לכלל מערכות המידע לשנתיים לפחות. יש לקבע בנוהל ולבצע בפועל בדיקה תקופתית, לפחות מדגמית, של הלוגים.
22. יש לשדרג את כלל מערכות ההפעלה והתוכנות לגרסאות עדכניות ונתמכות.
23. מומלץ לבחון שימוש במנגנון אוטומטי לעדכון מערכות צד שלישי.
24. מומלץ להפעיל באופן תקופתי כלי סריקה ייעודי ומקצועי באמצעותו ניתן לבצע סטאטוס עדכניות מערכות הפעלה ותוכנות המותקנות במחשבים ושרתים ברשת ולבצע עדכונים נדרשים כולל בתוכנות צד ג'.
25. יש להגדיר נוהל מצלמות מפורט המתאר את מורשי הגישה, הנסיבות בהן משתמשים במצלמות וכד'. מומלץ להחתים את מורשי הגישה על סעיפים ספציפיים לעניין מצלמות.
26. קיימת חובה לשים שילוט על מנת ליידע את הסובבים על כך שהמתחמים מצולמים.
27. יש לטפל בכלל הממצאים בדוח המבדקים הטכנולוגיים.

5. ***<u>פירוט</u> הממצאים***

5.1 **מדיניות אבטחת מידע ונהלי אבטחת מידע**

תקנה 3 (2) קובעת כי "הממונה על אבטחה יכין נוהל אבטחת מידע **ויביאו לאישור בעל המאגר;**"

מתוך מדריך ליישום תקנות הגנת הפרטיות של רשות הגנת הפרטיות: "הממונה על אבטחה יכין נוהל אבטחת מידע ויביאו **לאישור ההנהלה הבכירה של הארגון**"

תקנה 4(ג) קובעת כי "נוהל אבטחת מידע" שייקבע בעל מאגר מידע, יכלול, בין היתר:

"(1) הוראות בעניין האבטחה הפיזית והסביבתית של אתרי המאגר...;

(2) הרשאות גישה למאגר המידע ולמערכות המאגר...;

(3) תיאור של אמצעים שמטרתם הגנה על מערכות המאגר ואופן הפעלתם לצורך כך;

(4) הוראות למורשי הגישה למאגר המידע ולמערכות המאגר לצורך הגנה על המידע במאגר;

(5) הסיכונים שחשוף להם המידע שבמאגר במסגרת הפעילות השוטפת של בעל מאגר המידע, לרבות אלה הנובעים ממבנה מערכות המאגר... אופן קביעת סיכונים אלה, ואופן הטיפול בהם, לרבות על ידי מנגנוני הצפנה מקובלים להגנה על המידע השמור במאגר או במערכות המאגר;

(6) אופן התמודדות עם אירועי אבטחת מידע... לפי חומרת האירוע ומידת רגישות המידע;

(7) הוראות לעניין ניהול של התקנים ניידים ושימוש בהם...

תקנה 4(ד) קובעת כי במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, יכלול "נוהל אבטחת מידע" התייחסות אף לסעיפים הבאים:

"(1) אמצעי הזיהוי והאימות לגישה למאגר ולמערכות המאגר...;

(2) אופן הבקרה על השימוש במאגר המידע, ובכלל זה תיעוד הגישה למערכות המאגר...;

(3) הוראות לעניין עריכת ביקורות תקופתיות לווידוא קיומם ותקינותם של אמצעי האבטחה לפי נוהל האבטחה ולפי תקנות אלה...;

(4) הוראות לעניין גיבוי הנתונים... ;

(5) הוראות לעניין אופן ביצוע פעולות פיתוח במאגר ותיעודן, ובכלל זה אופן הגישה של אנשי הפיתוח לנתונים במאגר."

ממצאים:

לא קיים נוהל אבטחה מקיף הכולל את כלל היבטי אבטחת המידע הנדרשים בתקנות, כגון אבטחה פיזית, הרשאות גישה, התמודדות עם אירוע אבטחת מידע, התקנים ניידים, גיבויים וכד'.

המלצות:

יש להגדיר סט נהלים מקיף המתייחס לכלל הנושאים העולים מדרישות תקנות הגנת הפרטיות:

1. נוהל אבטחה פיזית
2. נוהל ניהול הרשאות גישה למערכות הארגון
3. נוהל התחברות וגישה מרחוק
4. נוהל הנחיות למורשי הגישה למאגרי המידע/ כללי אבטחת מידע לעובדים
5. נוהל תגובה לאירועי אבטחת מידע
6. נוהל התקנים ניידים/ מדיה נתיקה
7. נוהל זיהוי ואימות גישה כולל מדיניות סיסמאות

8. נוהל בקרה ותיעוד גישה למערכות המאגר ("נוהל ניטור ותיעוד לוגים")
9. נוהל גיבויים
10. נוהל אבטחת מידע במשאבי אנוש
11. נוהל מיקור חוץ
12. מסמך מדיניות

פרט לנהלים הנ"ל, יש להחזיק מסמך הכולל את:

- רשימת הסיכונים להם חשוף המאגר
- אמצעי ההגנה על המערכות ומנגנוני ההצפנה הקיימים
- רשימת מצאי רכיבי חומרה ומערכות לוגיות

על כלל הנהלים להיות מתוקפים מדי שנה ומאושרים על ידי גורם ניהולי רלוונטי.

5.2 **ממשל תאגידי בהיבטי אבטחת מידע**

חוק הגנת הפרטיות, סעיף 17ב. (א) קובע כי: הגופים המפורטים להלן חייבים במינוי אדם בעל הכשרה מתאימה שיהיה ממונה על אבטחת מידע (להלן – הממונה):

(1) מחזיק בחמישה מאגרי מידע החייבים ברישום לפי סעיף 8;

(2) גוף ציבורי כהגדרתו בסעיף 23;

תקנה 3 קובעת כי:

"חלה חובה למנות ממונה על אבטחת מידע, או מונה ממונה על אבטחת מידע במאגר המידע יחולו הוראות אלה:

(1) ממונה אבטחה יהיה כפוף ישירות למנהל מאגר המידע או למנהל פעיל של בעל המאגר או המחזיק בו, לפי העניין, או לנושא משרה בכירה אחר הכפוף ישירות למנהל המאגר.

(2) הממונה יכין תכנית לבקרה שוטפת על העמידה בדרישות תקנות אלה, יבצע אותה ויודיע לבעל מאגר המידע ולמנהל המאגר על ממצאיו;

(3) הממונה על אבטחה לא ימלא תפקיד נוסף שעלול להעמידו בחשש לניגוד עניינים במילוי תפקידו לפי תקנות אלה;

(4) הטיל בעל מאגר המידע על ממונה על אבטחה משימות נוספות על החובות המנויות... לשם ביצוע תקנות אלה, יגדירן בצורה ברורה;"

(6) "בעל מאגר המידע יקצה לממונה את המשאבים הדרושים לו לשם מילוי תפקידו."

האם ממונה אבטחת מידע יכול שיהיה כפוף למנמ"ר (מנהל מערכות מידע)?

סעיף 3(4) לתקנות קובע כי הממונה לא ימלא תפקיד נוסף שעלול להעמידו בחשש לניגוד עניינים במילוי תפקידו לפי התקנות. המטרה של ההוראה היא לשמר את עצמאות שיקול דעתו וחוסר התלות של ממונה האבטחה. עמדת הרשות היא שלא ניתן להשיג מטרה זו אם ממונה האבטחה יכהן בעצמו גם כמנמ"ר של הארגון. חשש לניגוד עניינים קיים גם במקרה בו הממונה יהיה רק כפוף למנמ"ר, אולם ניתן לצמצם את החשש אם חוסר תלותו ועצמאות שיקול דעתו של הממונה תובטח בדרך יעילה אחרת, בשים לב למבנה הארגון ולמאפייניו הספציפיים. לדוגמא, באמצעות אפשרות דיווח ישיר למנכ"ל או לדירקטוריון, ומעורבות שלהם במינוי הממונה ובקביעת תנאי העסקתו.

האם ניתן למנות ממונה אבטחת מידע חיצוני (מיקור חוץ)?

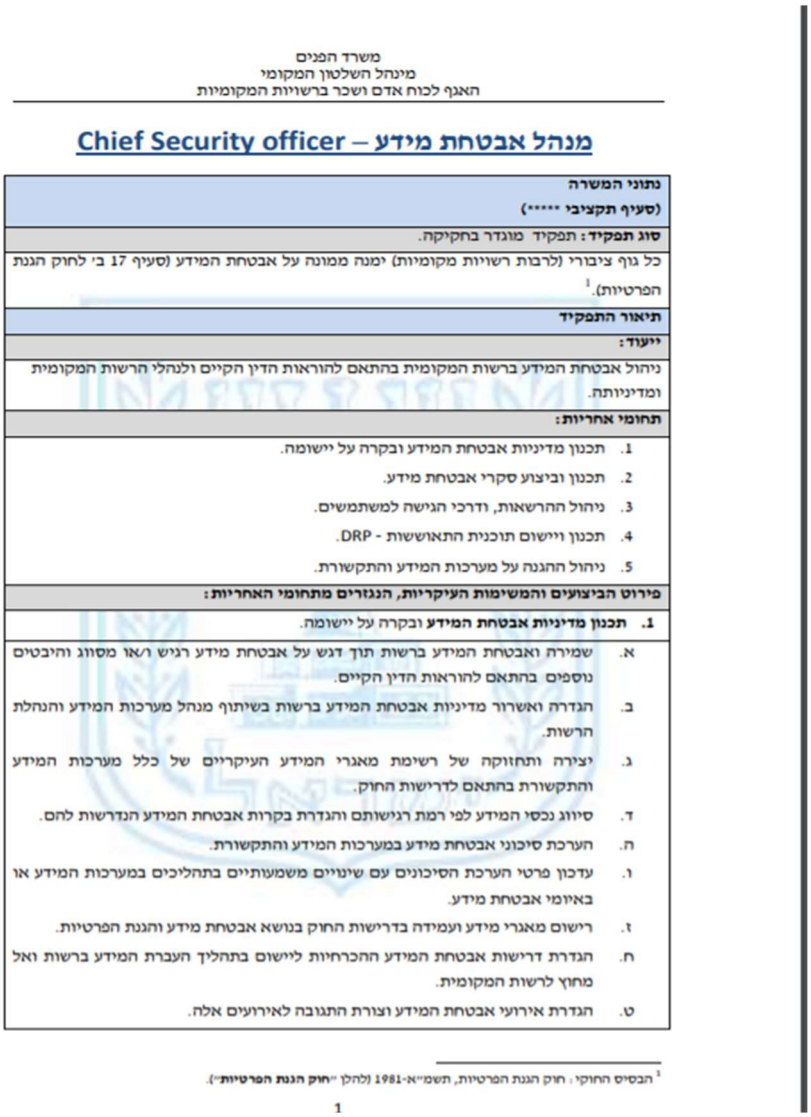
ניתן למנות ממונה אבטחת מידע חיצוני, שאינו עובד הארגון. בעת המינוי יש לוודא כי הממונה מבין כי הינו חב באחריות אישית לאבטחת המידע במאגר כפי שמוגדר בסעיף 17ב(ב) לחוק הגנת הפרטיות.

האם קיים נוהל למינוי ממונה אבטחת מידע, ודרישות ספציפיות לתפקיד?

חוק הגנת הפרטיות ותקנות אבטחת מידע אינם מתייחסים לאופן מינוי ממונה אבטחת מידע. יחד עם זאת, נזכיר כי יש להתייחס לדברי החוק כפי שמופיעים בסעיף 17ב(א), בשים לב לכך שממונה על אבטחת מידע יהיה אדם בעל הכשרה מתאימה לתפקיד, וכן לעמוד בדרישות תקנה 3 לתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017.

משרד הפנים הגדיר תפקיד של ממונה אבטחת מידע, ההגדרה מתפרסת על 6 עמודים. רצ״ב הפרסום של משרד הפנים:

https://www.moin.gov.il/LOCALGOVERNMENT/local%20authority/human_assets/DocLib1/%D7%9E%D7%A0%D7%94%D7%9C%20%D7%90%D7%91%D7%98%D7%97%D7%AA%20%D7%9E%D7%99%D7%93%D7%A2.pdf



משרד הפנים
מינהל השלטון המקומי
האגף לכוח אדם ושכר ברשויות המקומיות

Chief Security officer – מנהל אבטחת מידע

נתוני המשרה **(סעיף תקציבי *****)**
סוג תפקיד: תפקיד מוגדר בחקיקה.
כל גוף ציבורי (לרבות רשויות מקומיות) ימנה ממונה על אבטחת המידע (סעיף 17 ב' לחוק הגנת הפרטיות).[1]
תיאור התפקיד
ייעוד:
ניהול אבטחת המידע ברשות המקומית בהתאם להוראות הדין הקיים ולנהלי הרשות המקומית ומדיניותה.
תחומי אחריות:
1. תכנון מדיניות אבטחת המידע ובקרה על יישומה. 2. תכנון וביצוע סקרי אבטחת מידע. 3. ניהול ההרשאות, ודרכי הגישה למשתמשים. 4. תכנון ויישום תוכנית התאוששות - DRP. 5. ניהול ההגנה על מערכות המידע והתקשורת.
פירוט הביצועים והמשימות העיקריות, הנגזרים מתחומי האחריות:
1. תכנון מדיניות אבטחת המידע ובקרה על יישומה.
א. שמירה ואבטחת המידע ברשות תוך דגש על אבטחת מידע רגיש ו/או מסווג והיבטים נוספים בהתאם להוראות הדין הקיים. ב. הגדרה ואשרור מדיניות אבטחת המידע ברשות בשיתוף מנהל מערכות המידע והנהלת הרשות. ג. יצירה ותחזוקה של רשימת מאגרי המידע העיקריים של כלל מערכות המידע והתקשורת בהתאם לדרישות החוק. ד. סיווג נכסי המידע לפי רמת רגישותם והגדרת בקרות אבטחת המידע הנדרשות להם. ה. הערכת סיכוני אבטחת מידע במערכות המידע והתקשורת. ו. עדכון פרטי הערכת הסיכונים עם שינויים משמעותיים בתהליכים במערכות המידע או באיומי אבטחת מידע. ז. רישום מאגרי מידע ועמידה בדרישות החוק בנושא אבטחת מידע והגנת הפרטיות. ח. הגדרת דרישות אבטחת המידע ההכרחיות ליישום בתהליך העברת המידע ברשות ואל מחוץ לרשות המקומית. ט. הגדרת אירועי אבטחת המידע וצורת התגובה לאירועים אלה.

[1] הבסיס החוקי: חוק הגנת הפרטיות, תשמ״א-1981 (להלן ״**חוק הגנת הפרטיות**״).

1

דוגמה למכרז פומבי לתפקיד ממונה אבטחת מידע בעירייה אחרת בתקציב של 30 שעות שבועיות:

https://betshemesh.muni.il/uploads/n/1591527757.1888.pdf

פסקת תנאי סף לתפקיד ממונה אבטחת מידע:

3.2. **תנאי סף למועמד מטעם המציע :**

3.2.1. מומחה בעל 5-10 שנות ניסיון בתחומי מערכות המידע, אבטחת מידע, חוק הגנת הפרטיות רשתות תקשורת, תשתיות מחשוב וטלפוניה.

3.2.2. המועמד בעל הכשרה של אחד מאלה:

3.2.3. קורס או הסמכה מוכרים בתחום אבטחת המידע (CISSP, CISO, CISA, CEH) - מוסד אקדמאי מוכר יתרון.

3.2.4. הסמכה אחת לפחות בתחום IT (CCNA, MCSA וכו').

3.2.5. מומחה בעל ניסיון מעשי של לפחות שנה בתחום אבטחת המידע וליווי רשויות לעמידה בתקני חוק הגנת הפרטיות.

3.2.6. עדיפות תינתן לבעלי ניסיון בהטמעת GDPR בארגונים מעל 500 משתמשים.

3.2.7. ניסיון בליווי לפחות גוף מוניציפאלי אחד כגון רשות מקומית / תאגיד מים / וכו' המונות מעל 500 משתמשים.

3.2.8. ניסיון מעשי באפיון קמפיין הגברת מודעות עובדים ומנהלים לנושאי אבטחת המידע.

3.2.9. מומחה בעל ניסיון בעבודה מול ספקים וגורמי צד ג' בנושאי אבטחת מידע.

3.2.10. מומחה בעל ניסיון בעבודה מול גורמים רגולטוריים כגון מערך הגנת הסייבר.

ממצאים:

1. טרם מונה ממונה אבטחת מידע בעל הכשרה מתאימה בעירייה.
2. טרם הוכנה תוכנית בקרה מפורטת (שנתית/ רב שנתית) לעמידה בתקנות הגנת הפרטיות.
3. לא מתקיימים דיווחים קבועים בכתב להנהלה בנוגע לפעילות אבטחת מידע.

המלצות:

1. יש למנות ממונה אבטחת מידע בעירייה בעל הכשרה מתאימה שאינו מכהן בתפקיד אחר בהיקף משרה מספק לביצוע כלל המשימות, הממונה לא ימלא תפקיד נוסף שעלול להעמידו בחשש לניגודי עניינים (למשל: מנהל מערכות המידע\ איש הסיסטם לא יהיה גם ממונה על בקרות אבטחת המידע)
2. מומלץ כי, הממונה יכין תכנית בקרה מפורטת שנתית לפחות לעמידה בתקנות ותקציב נדרש מתאים ליישום התוכנית, יגיש לאישור ההנהלה וידווח על ביצועה להנהלה ומנהלי מאגרים.
3. על ממונה אבטחת מידע להעביר דיווח תקופתי בכתב במסגרת ועדת היגוי או ישירות להנהלה בכירה ולמנהלי מאגרים בו יוצגו תוצאות פעולות הבקרה שלו ואיזה פערים עדיין קיימים לעמידה בדרישות התקנות. במסגרת זו על ממונה אבטחת מידע לתעד באופן מפורט כל הפעילות הבקרה המבוצעת על ידו.

5.3 ועדת היגוי בנושא אבטחת מידע והגנת הפרטיות

כיום בארגונים רבים מקובל כי קידום נושאי אבטחת מידע והגנת הפרטיות מובילים באמצעות ועדות היגוי.

להלן תפקידים סטנדרטיים של ועדת היגוי:

- ✓ אישור ועדכון בכל הנוגע למדיניות אבטחת המידע ונהלים.
- ✓ לסייע לעירייה בכל הקשור לניהול תקין של תחום אבטחת המידע בעירייה.
- ✓ אישור תכנית העבודה בתחום אבטחת מידע, הקצאת תקציבים ומעקב אחר יישום תכנית העבודה בתחום.
- ✓ לדון באירועי אבטחת מידע חריגים.
- ✓ להבטיח קיומם של מנגנוני פיקוח ובקרה נאותים.
- ✓ לסייע להנהלת העירייה בקבלת החלטות בכל הקשור לתחום אבטחת המידע מתוך ראיה אינטגרטיבית של התחום בעירייה.
- ✓ קבלת דיווחים תקופתיים ממונה אבטחת מידע והנחיית ממונה אבטחת המידע.

להלן סדרים מקובלים לקיום פגישות ועדת היגוי:

- ⇐ הוועדה תתכנס בתדירות קבועה ומספקת, (אחת לשנה לפחות) ותדווח לראש העירייה ומועצת העירייה, על פעילותה, מסקנותיה והמלצותיה בנושאים בהם הוסמכה לעסוק.
- ⇐ רצוי כי לפחות בדיון השנתי בו תאושר תכנית העבודה ותקציבים יהיה נוכח ראש העירייה.
- ⇐ הוועדה תערוך פרוטוקולים של ישיבותיה.
- ⇐ חברי הועדה צריכים להיות מתחומים מנהליים ולא רק מערכות מידע לרבות יועץ משפטי, קצין הביטחון, מנהל משאבי אנוש, אחראי על תאגידים עירוניים, מנהלי המאגרים שמונו ועוד.

ממצאים:

הביקורת מצאה כי לא הוגדרה באופן פורמאלי ועדת היגוי לנושאי אבטחת מידע באמצעות כתב מינוי או במסגרת נוהל ארגוני לרבות תפקידיה, סמכויותיה וחבריה. לא נמצא תיעוד לפרוטוקולי ישיבות הנהלה בנושא אבטחת מידע.

לא מתקיים דיווח שנתי בנושאי אבטחת מידע לראש העירייה או גורם ניהולי בכיר.

לא מבוצעת בקרה על סטטוס עמידה בתקנות הגנת הפרטיות כחלק מהעבודה השוטפת.

המלצות:

1. להגדיר באופן פורמאלי ועדת היגוי לנושאי אבטחת מידע והגנת הפרטיות לרבות משתתפיה, תדירות התכנסותה, תפקידיה וסמכויותיה, במסמך מדיניות אבטחת מידע תוך הגדרת כתב מינוי לכל אחד מחבריה.
2. לכנס ועדת היגוי בתדירות תקופתית כולל דיון שנתי לפחות בנוכחות ראש העירייה תוך תיעוד מסודר בפרוטוקולים של נושאים שנדונו, החלטות ומעקב ביצוע.
3. מומלץ לבצע דיווח שנתי על מצב אבטחת מידע בעירייה וסטטוס עמידה בתקנות הגנת הפרטיות למועצת העירייה.

5.4 הדרכות ומודעות עובדים

סעיף 7 לתקנות הגנת הפרטיות קובע:

"(ב) בטרם יקבלו גישה למידע ממאגר המידע או לפני שינוי היקף הרשאותיהם, יקיים בעל מאגר מידע הדרכות לבעלי הרשאות בנושא החובות לפי החוק ותקנות אלה, וימסור להם מידע על אודות חובותיהם לפי החוק ונוהל האבטחה.
(ג) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, יקיים בעל המאגר פעילות הדרכה תקופתית לבעלי הרשאות שלו, בדבר מסמך הגדרות המאגר, נוהל האבטחה והוראות אבטחת המידע לפי החוק ולפי תקנות אלה, בהיקף הנדרש לצורך ביצוע תפקידיהם, ובדבר חובות בעלי ההרשאות לפיהם; הדרכה כאמור תיערך אחת לשנתיים לפחות.."

ממצאים:

1. נמצא כי לא קיימת תוכנית הדרכות ולא התבצעו הדרכות לכלל עובדי החברה בשנתיים האחרונות.
2. נמצא כי החתמת עובדים על כללי אבטחת מידע ועל שמירת סודיות לא מתקיימת.
3. נמצא כי העובדים אינם מתורגלים בשוטף בסימולציות פישינג או מבחנים בנושאי אבטחת אבטחת מידע.

המלצות :

1. לבצע הדרכות מודעות בהיבטי אבטחת מידע והגנת הפרטיות לכלל העובדים בעירייה כנדרש בתקנות הגנת הפרטיות, כולל הטמעת מנגנון שמבטיח כי כל העובדים, להם קיימת גישה למערכות העירייה ולמאגרי המידע, יקבלו הדרכה תקופתית בתדירות של 24 חודשים לכל הפחות תוך ביצוע מעקב ורישום לגבי מועדי ההדרכות לכל עובד. \
2. להחתים את כלל עובדי העירייה אשר ניגשים למערכות מידע כל שמירת סודיות ועל כללי אבטחת מידע
3. לבצע תרגולים של סימולציות פישינג להגברת יכולת העובדים להתמודד עם אירועי פישינג אמיתיים.

5.5 **בקרת הרשאות גישה**

בסעיף 8 בתקנות ניהול הרשאות גישה נרשם:

"(א) בעל מאגר מידע יקבע הרשאות גישה של בעלי הרשאות למאגר המידע ולמערכות המאגר, בהתאם להגדרות תפקיד; הרשאת הגישה לכל תפקיד תהיה במידה הנדרשת לביצוע התפקיד בלבד.

(ב) בעל מאגר מידע ינהל רישום מעודכן של תפקידים, הרשאות הגישה שניתנו להם, ושל בעלי ההרשאות הממלאים תפקידים אלה (להלן – רשימת ההרשאות התקפות)."

ממצאים:

1. כל מנהל אגף מחליט לעניין הרשאות העובדים החדשים תחתיו. הרשאות ניתנות על פי תפקיד ותחומי אחריות.
2. לא מתקיימת סקירת הרשאות קבועה/ תיקוף של הרשאות הגישה למערכות/ מאגרי המידע.
3. לא קיים מסמך המתאר את כלל התפקידים והרשאותיהם.
4. עובדים אינם חתומים על כך שמאשרים גישה לתיבות דוא"ל לאחר סיום עבודתם.

המלצות:

1. יש לבצע מיפוי מדויק של איזה סוגי הרשאות נדרשות ברמת כל תפקיד לכלל מערכות המאגרים.
2. יש לבצע תיקוף תקופתי של נאותות הרשאות בכל מערכות המידע/ המאגרים.
3. מומלץ לגבש מדיניות העירייה לגבי הקפאת חשבונות עובדים במקרה של חופשות והיעדרויות ארוכות. כמו כן להחתים עובדים על אישור גישה לתיבות דוא"ל שלהם לאחר סיום עבודתם.

5.6 **קיום הגנה אפקטיבית כנגד מתקפות מתוחכמות**

סעיף 14(א) לתקנות קובע:

"בעל מאגר מידע לא יחבר את מערכות המאגר לרשת האינטרנט או לרשת ציבורית אחרת, בלא התקנת אמצעי הגנה מתאימים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק או שיבוש למחשב או לחומר מחשב."

בשנים אחרונות התגברו מתקפות סייבר מתוחכמות המנצלות פרצות ZERO DAY. אלו הן פרצות שמתגלות על ידי גורמים זדוניים ולא מועברים לידיעת יצרנים לצורך ביצוע תיקונים. לפרצות אלה טרם הוגדרו חתימות המכילים תוכנת אנטי וירוס מתאימה ומוצרי אבטחה נוספים ולכן הן עלולות לא להתגלות ולא להיחסם. גורמים זדוניים כותבים נוזקות ייעודיות לניצול פרצות חדשות אשר לרוב, מופצות בקמפיינים של דיוג הנשלחים בדואר אלקטרוני או דרך האינטרנט ואף מופצות ללא ידיעת המשתמש באמצעות התקן נייד (Disk On Key).

לצורך התמודדות עם פרצות אלה פותחו טכנולוגיות שהוכיחו אפקטיביות בשילוב של מספר טכנולוגיות, כגון: SANDBOX (קופסת חול- סביבה וירטואלית בה נבחנת התנהגות קובץ לאיתור פעילות זדונית לפני שחרורו למשתמש), Endpoint Detection and Response -EDR, Anomaly detection, Behavioral, Code Sterilization analysis (הלבנת קבצים).
ניתן להרחיק את האיום ממשתמשי קצה ולאפשר גלישה מאובטחת באינטרנט באמצעות שימוש במכונות מרוחקות והפרדת רשתות פנים ארגוניות מרשת האינטרנט (Secure browsing). חומת

אש אפליקטיבית = WEB Application Firewall – WAF, נועדה לחסימת מתקפות ברובד האפליקטיבי על אפליקציות ואתרים באינטרנט.

ממצאים:

העירייה משתמש במספר מוצרי אבטחה על מנת להגן על הרשת ועמדות הקצה, ביניהן:

- אנטי-וירוס Windows Defender
- אנטי-וירוס Mcaffee
- אנטי-וירוס Eset
- חומת אש FortiGate כולל מספר מודולי אבטחה מופעלים
- חומת אש אפליקטיבית (WAF) להגנה על אתר האינטרנט של העירייה
- מערכת UPS בחדר שרתים

במסגרת בדיקות טכנולוגיות נמצא בין היתר כי:

1. חומת האש אינה מוגדרת בצורה מספיק אפקטיבית.
2. רישוי מוצר האנטי וירוס של סימנטק הינו פג תוקף, ולא מנע מספר סימולציות תקיפה אשר בוצעו. נמסר כי העירייה נמצאת בתהליך בחינה למוצר בעל טכנולוגיה מתקדמת יותר מסוג EDR/XDR.
3. הגדרות ה-WAF לא מנעו לפחות סוג אחד של מתקפה אפליקטיבית.
4. העירייה כיום ללא פתרון NAC למניעת חיבור בלתי מורשה לרשת העירייה.
5. קיימים רכיבי תקשורת כגון מתגים וכד' בעלי קושחה לא עדכנית וחשופה לחולשות קריטיות.
6. מערכות הדוא"ל לא מנעו מתקפת התחזות אשר בוצעה במסגרת הבדיקות.
7. קיים שימוש בפרוטוקולים פגיעים ברשת הפנימית.

*לפירוט מלא של הממצאים הטכנולוגיים וההמלצות הרלוונטיות יש לקרוא את דוח המבדקים הטכנולוגיים.

המלצות:

בהתאם למבדקים טכנולוגיים שבוצעו ובחינת התיעוד שהתקבל, הביקורת סבורה כי קיים מקום להוסיף שכבות הגנה נוספות כמפורט להלן:

1. להפעיל בתחנות קצה ושרתים מערכת EDR מתקדמת לאיתור אנומאליות מעבר ליכולות של אנטי וירוס הקלאסי.
2. להקשיח את ההגדרות של חומת האש כמתואר בדוח המבדקים הטכנולוגיים.
3. לבצע באופן קבוע (מחזורית) מעבר על הגדרות מוצרי הגנה קיימים, כגון חומת אש, אנטי וירוס וכד'. במסגרתו ייבדקו גרסאות עדכניות, מודולים מוקשחים ומופעלים, עדכוני אינדיקטורים רלוונטיים וכיוצ"ב ע"י גורמים מקצועיים.
4. יש הימנע משימוש בפרוטוקולים פגיעים וישנים.
5. מומלץ לבחון רכש של מערכת NAC(network access control) אשר תפקידה לחסום גישה לרכיבים לא מאושרים אל תוך הרשת הפנימית.
6. להקשיח את מערכות סינון הדוא"ל כרשום בדוח המבדקים הטכנולוגיים.
7. לבצע סריקות מחזוריות ומבדקים תקופתיים לאיתור חולשות ולהציג את תוצאות המבדקים להנהלה הבכירה תוך קבלת אישורה להרחבה תקציבית או קבלת רמת הסיכון הנוכחית.

5.7 **ניטור, דיווח ותגובה לאירועי אבטחת מידע**

<u>סעיף 11 לתקנות קובע:</u>

5.5 בעל מאגר מידע אחראי לתיעוד כל מקרה שבו התגלה אירוע המעלה חשש לפגיעה בשלמות המידע, לשימוש בו בלא הרשאה או לחריגה מהרשאה (להלן – אירועי אבטחה); ככל האפשר יבוסס התיעוד האמור על רישום אוטומטי.

(ב) בנוהל האבטחה יקבע בעל מאגר מידע גם הוראות לעניין התמודדות עם אירועי אבטחת מידע, לפי חומרת האירוע ומידת רגישות המידע, לרבות לעניין ביטול הרשאות וצעדים מיידיים אחרים הנדרשים וכן לעניין דיווח לבעל המאגר על אירועי אבטחה ועל פעולות שננקטו בעקבותיהם.

(ג) במאגר מידע שחלה עליו רמת האבטחה הבינונית, יקיים בעל המאגר דיון אחת לשנה לפחות באירועי האבטחה ויבחן את הצורך בעדכונו של נוהל האבטחה; במאגר מידע שחלה עליו רמת האבטחה הגבוהה, ייערך דיון כאמור אחת לרבעון לפחות."

ממצאים:

1. לא קיים נוהל לטיפול באירוע אבטחת מידע.
2. לא הוגדר צוות תגובה לאירועי סייבר.
3. לא קיים ניטור של מערכות הארגון על ידי צוות SOC חיצוני.

המלצות:

1. יש להגדיר נוהל תגובה\ נוהל טיפול באירוע אבטחת מידע הכולל טבלת אנשי קשר, צוות תגובה, חובות דיווח לגורמים רלוונטיים וכן התייחסות לתרחישים ספציפיים אירועי אבטחת מידע
2. מומלץ לחזק את מערך הניטור, למשל ע"י מערכת SIEM וצוות SOC חיצוני המנטר את הפעילות ברשת 24/7. לחלופין, להטמיע מערכת MDR מתקדמת.

5.8 **מיקור חוץ**

<u>במסגרת תקנה 15 נקבע כי:</u>

(1) יקבע במפורש בהסכם עם הגורם החיצוני (בתקנה זו – ההסכם) את כל אלה, בשים לב לסיכונים לפי פסקה(1):

(א) המידע שהגורם החיצוני רשאי לעבד ומטרות השימוש המותרות בו לצורכי ההתקשרות;

(ב) מערכות המאגר שהגורם החיצוני רשאי לגשת אליהן;

(ג) סוג העיבוד או הפעולה שהגורם החיצוני רשאי לעשות;

(ד) משך ההתקשרות, אופן השבת המידע לידי הבעלים בסיום ההתקשרות, השמדתו מרשותו של הגורם החיצוני ודיווח על כך לבעל מאגר המידע;

(ה) אופן יישום החובות בתחום אבטחת המידע שהמחזיק חייב בהן לפי תקנות אלה, וכן הנחיות נוספות לעניין אמצעי אבטחת מידע שקבע בעל מאגר המידע, אם קבע;

(ו) חובתו של הגורם החיצוני להחתים את בעלי ההרשאות שלו על התחייבות לשמור על סודיות המידע, להשתמש במידע רק לפי האמור בהסכם, וליישם את אמצעי האבטחה הקבועים בהסכם כאמור בפסקת משנה(ה);

(ז) התיר בעל מאגר מידע לגורם החיצוני לתת את השירות באמצעות גורם נוסף – חובתו של הגורם החיצוני לכלול בהסכם עם הגורם הנוסף את כל הנושאים המפורטים בתקנה זו ;

(ח) חובתו של הגורם החיצוני לדווח ,אחת לשנה לפחות ,לבעל מאגר המידע על אודות אופן ביצוע חובותיו לפי תקנות אלה וההסכם ולהודיע לבעל המאגר במקרה של אירוע אבטחה ;

4)ינקוט אמצעי בקרה ופיקוח על עמידתו של הגורם החיצוני בהוראות ההסכם ובהוראות תקנות אלה ,בהיקף הנדרש בשים לב לסיכונים האמורים בפסקה (1).״

ממצאים:

נמסר לביקורת כי לא קיים מיפוי ספקים מלא ומעקב ובקרה על ספקים רגישים מבחינת אבטחת מידע.

המלצות:

1. לבצע מיפוי ספקים למען בקרה על ספקים בעלי גישה למידע רגיש או למערכות המידע של העירייה.
2. לדרוש לקבל מכל הספקים הרלוונטיים דיווח בכתב על סטטוס עמידה בתקנות הגנת הפרטיות בתדירות תקופתית.
3. לדרוש לקבל מספקי מיקור חוץ סיכומי דוחות מבדקי חדירה תקופתיים וסקרי אבטחה ולוודא שאין ממצאים קריטיים שלא מטופלים.
4. לפעול להחתמת כלל הספקים על נספח אבטחת מידע הכולל התייחסות לכל הדרישות בסעיף 15 של תקנות הגנת הפרטיות.

5.9 **רישום מאגרים, מסמכי הגדרות מאגר ושמירת מידע רב מן הנדרש**

בתקנה 2 (הגנת הפרטיות) נקבע :

(א) בעל מאגר מידע יגדיר במסמך הגדרות מאגר(להלן – מסמך הגדרות המאגר) את כל העניינים האלה לפחות :

(1) תיאור כללי של פעולות האיסוף והשימוש במידע ;

(2) תיאור מטרות השימוש במידע ;

סוגי המידע השונים הכלולים במאגר המידע ,בשים לב לרשימת סוגי המידע שבפרט בתוספת הראשונה ; פרטים על העברת מאגר המידע ,או חלק מהותי ממנו אל מחוץ לגבולות המדינה או שימוש במידע מחוץ לגבולות המדינה ,מטרת ההעברה ,ארץ היעד,אופן ההעברה וזהות הנעבר ;

(3) פעולות עיבוד מידע באמצעות מחזיק ;

(4) הסיכונים העיקריים של פגיעה באבטחת המידע ,ואופן ההתמודדות עמם ;

(5) שמו של מנהל מאגר המידע ,של מחזיק המאגר ושל הממונה על אבטחת מידע בו ,אם מונה כזה.

(ג) בעל מאגר מידע יבחן ,אחת לשנה ,אם אין המידע שהוא שומר במאגר רב מן הנדרש למטרות המאגר.

ממצאים:

1. לא קיימים מאגרים רשומים בעירייה.
2. לא נראה כי הצורך ברישום מאגרי מידע נבחן בעבר.
3. לא קיימים מסמכי הגדרות מאגר.

המלצות:

יש לבצע מיפוי מאגרים מסודר – רשימת מאגרי המידע המחייבים ברישום על פי סוגי המידע הקיימים (מאגר רווחה, הנהלח"ש, משאבי אנוש וכו') עבור כל מאגר שלא נרשם יש להגיש בקשת רישום מסודרת בהקדם האפשרי. כמו כן, עבור כל מאגר יש למנות מנהל מאגר. לבקשת הרישום יצורף טופס מינוי מנהל מאגר וכן מסמך מורשה חתימה בתאגיד. עבור כל מאגר יש למלא מסמך הגדרות הנשמר בארגון לצורכי בקרה.

נבקש להבהיר כי תפקידו של מנהל המאגר כולל תחומי אחריות מגוונים וכן מס' בקרות שונות. נמליץ כי האחריות על כלל המאגרים לא תרוכז בידי אדם אחד. זה המקום להדגיש כי יש יתרון לכך שתתקיים אוריינטציה בין תחום עיסוקו של מנהל המאגר ורלוונטיות למידע המצוי מאגר (למשל: נתוני עובדים תחת פיקוח של אחראי משאבי אנוש וכו')

5.10 סיסמאות, זיהוי ואימות

תקנה 9 (הגנת הפרטיות) קובעת:

יש לוודא שמי שניגש למידע במאגר הוא עובד מורשה, ולכן יש לאמת את זהותו באמצעים מקובלים בנסיבות העניין, דהיינו באמצעות סיסמה.

במאגר שחלה עליו רמת האבטחה הבינונית או הגבוהה – אופן הזיהוי יעשה ככל האפשר על בסיס אמצעי פיזי הנתון לשליטתו הבלעדית של המורשה, כגון תעודה המכילה חתימה אלקטרונית מאובטחת, TOKEN .

בנוהל אבטחה יש לקבוע גם את אופן הזיהוי, אם אופן הזיהוי מבוסס על סיסמאות – הנוהל יתייחס לחוזק הסיסמה, מספר הניסיונות השגויים, ותדירות החלפת הסיסמאות שתיעשה בהתאם לתפקיד מורשה הגישה, ובכל מקרה לתקופה שלא תעלה על 6 חודשים, ניתוק אוטומטי לאחר פרק זמן של אי-פעילות, אופן הטיפול בתקלות הקשורות באימות זהות.

מערך הסייבר הלאומי פרסם מאמר על חשיבות חוזק הסיסמה, ובו המלצה על "סיסמה ארוכה ומורכבת- עם שילוב מספרים, אותיות גדולות, קטנות ותווים מיוחדים." שימוש בסיסמאות שונות בממשקים שונים וכד'.

לעיון בכתבה המלאה -> https://www.gov.il/he/departments/news/passwordrec

ממצאים:

1. לא מוגדרת בנהלי העירייה מדיניות סיסמאות.
2. נמצא כי אין אכיפה של סיסמאות מוקשחות של לפחות 9 תווים בגישה לרשת .

המלצות:

1. להגדיר מדיניות סיסמאות לכלל מערכות המידע והרשת הארגונית בנוהל.
2. לגבש מדיניות סיסמאות מוקשחת ברשת ובכל גישה למערכות/ מאגרי מידע:

- אורך – על סיסמאות להכיל מינימום של כ-9 תווים עבור משתמשים רגילים ו-15+ תווים למשתמשים בעלי הרשאות גבוהות / החברים בקבוצות רגישות כמו Admins Domain, גיבויים וכד'.
- חיוב שימוש באותיות גדולות (A-Z)
- חיוב שימוש באותיות קטנות (a-z)
- חיוב שימוש במספרים (0-9)
- חיוב שימוש בסימנים מיוחדים (לדוגמא: !@#$%^&*)(><?", וכד')
- חיוב הגדרת ללא רצפים (לדוגמא: ללא 1234,1234567,98765 כחלק מהסיסמה).
- איסור על שימוש בשם המשתמש חלק מהסיסמא.
- הגדרת מספר ניסיונות התחברות כושלים לכל היותר – 5 ניסיונות.

5.11 מיפוי מערכות המאגר ונכסי מידע

תקנה 5 (הגנת הפרטיות) קובעת כי "על בעל מאגר המידע להכין מסמך מעודכן של מבנה מאגר המידע וכן רשימת מצאי מעודכנת של מערכות המאגר, הכוללת את הפרטים הבאים:

- תשתיות ומערכות חומרה, סוגי רכיבי תקשורת ואבטחת מידע.
- מערכות התוכנה המשמשות להפעלת מאגר המידע, לניהול המאגר ולתחזוקתו, לתמיכה בפעילותו, לניטורו ולאבטחתו.
- תוכנות וממשקים המשמשים לתקשורת אל מערכות המאגר ומהן.
- תרשים הרשת שבה פועל המאגר, הכולל תיאור הקשרים בין רכיבי המערכת השונים ומיקומם הפיזי של הרכיבים.
- תאריך העדכון האחרון של המסמך ושל רשימת המצאי.

ממצאים:

1. דווח לביקורת כי אין בנמצא תרשים רשת עדכני של העירייה.
2. דווח כי אין רשימת מצאי עדכנית.

המלצות:

יש לוודא קיומם של רשימת מצאי ומיפוי נכסים הכוללים את המערכות והממשקים הרלוונטיים למאגרי המידע הן ברמת החומרה והן ברמת מערכות המידע. על הרשימה והמיפוי להיות

5.12 גיבוי ושחזור נתוני אבטחה

תקנות הגנת הפרטיות, בפרט תקנות 17 ו-18, מכילות מספר הוראות הנוגעות לשמירת נתונים וגיבויים, נושאים שהינם מרכזיים באבטחת מידע. על מערך הגיבויים לאפשר בכל עת שחזור אמין של מידע ממאגרי המידע.

ממצאים:

1. לא נמסר מידע בנוגע למדיניות הגיבויים המיושמת.
2. לא מתבצעים שחזורים קבועים בצורה יזומה אלא רק לפי צורך/ עפ"י דרישה.
3. לא קיים נוהל גיבויים.

המלצות:

1. מומלץ להגדיר תדירות גיבויים המספקת את צורכי הארגון (להחלטת הנהלה). למשל ניתן להגדיר גיבויים יומיים הנשמרים לפחות שבוע, שבועיים הנשמרים לפחות חודש, חודשיים הנשמרים שנה וגיבויים שנתיים הנשמרים מס' שנים.
2. מומלץ להחזיק גיבוי קר מנותק לחלוטין מהרשת כהגנה נוספת על המידע במצב בו הגיבויים נפגעו.
3. ש להגדיר נוהל גיבויים מפורט הכולל הנחיות לגבי שחזור מידע גם כן.
4. יש לבצע שחזור מידע גם באופן יזום ולא רק בעת תקלה. מומלץ לבצע שחזור יזום מגיבוי לפחות אחת לרבעון.

5.13 אבטחת התקנים ניידים

תקנה 12 (הגנת הפרטיות) קובעת כי "בעל המאגר יגביל או ימנע אפשרות לחיבור התקנים ניידים למערכות המאגר במתכונת ההולמת את רמת אבטחת המידע שחלה על המאגר, את רגישות המידע, את הסיכונים המיוחדים למערכות המאגר או למידע הנובעים מחיבור ההתקן הנייד ואת קיומם של אמצעי הגנה מתאימים מפני סיכונים אלה; בעל מאגר מידע המאפשר שימוש במידע מהמאגר בהתקן נייד או העתקה שלו להתקן נייד ינקוט אמצעי הגנה בשים לב לסיכונים המיוחדים הקשורים לשימוש בהתקן נייד באותו מאגר מידע; לעניין זה יראו שימוש בשיטות הצפנה מקובלות כנקיטת אמצעים סבירים להגנה על מידע שהועתק להתקן הנייד."

ממצאים:

1. לא קיימת חסימת מדיה נתיקה גורפת בעמדות הקצה.
2. לא קיים נוהל המתייחס להתקנים ניידים / מדיה נתיקה.

המלצות:

1. יש לחסום אפשרות לחיבור מדיה נתיקה בעמדות הקצה. במידת הצורך יש להעביר קבצים דרך שרת הלבנה או להגדיר whitelist לחיבורי מדיה נתיקה מאושרים מראש של הארגון אשר נסרקים ונבדקים לגבי וירוסים בצורה שוטפת.
2. יש להגדיר מדיניות מדיה נתיקה. רצוי לחסום התקנים ניידים באופן גורף ולאפשר רק במקרים חריגים ע"י התקנים אשר נבדקו ואושרו ע"י גורם טכני.

5.14 אבטחת גישה מרחוק למשאבי העירייה

בתקנה 14(ג) (הגנת הפרטיות) נרשם "במאגר מידע שניתן לגשת אליו מרחוק, באמצעות רשת האינטרנט או רשת ציבורית אחרת, ייעשה שימוש נוסף על אמצעי אבטחה כאמור בתקנות משנה (א) ו(ב), באמצעים שמטרתם לזהות את המתקשר והמאמתים את הרשאתו לביצוע הפעילות מרחוק ואת היקפה; לעניין גישה של בעל הרשאה למאגר מידע ברמת האבטחה הבינונית והגבוהה ייעשה שימוש באמצעי פיזי הנתון לשליטתו הבלעדית של בעל ההרשאה."

מערך הסייבר ורשות הגנת הפרטיות פרסמו הנחיות לגבי אמצעי אבטחה נאותים בגישה מרחוק מהבית לרשת ארגונית.

כיום אמצעי אבטחה מקובל בגישה מרחוק הינו מנגנון הזדהות חזקה הכולל שני שלבים בהזדהות לפחות- 2FA . סיסמה קבועה כבר אינה מהווה בקרה חזקה כאשר קיימים דרכים רבות להשגת הסיסמא על ידי גורמים זדוניים. ההזדהות החזקה הנפוצה הינה קיום מנגנון לחילול סיסמה חד פעמית באמצעות התקן הנתון לשליטה של המשתמש כמו טלפון נייד אישי.

ממצאים:

1. אין הנחיות או מדיניות סדורה המיושמת בכל הנוגע לחיבור התקנים ניידים לרשת הארגונית.

המלצות:

1. מומלץ להקשיח את הגדרות הVPN (פירוט בדוח המבדקים הטכנולוגיים) ובפרט להגדיר אימות דו שלבי בכל חיבור מרחוק.
2. יש להגדיר מדיניות ברורה וכתובה לעניין שימוש בהתקנים ניידים ומדיה נתיקה אשר תיכלל בנוהל האבטחה.

5.15 בקרה ותיעוד גישה

בסעיף 10 בתקנות בנושא בקרה ותיעוד גישה נרשם:

(א) במערכות של מאגר מידע אשר חלה עליו רמת האבטחה הבינונית או הגבוהה, ינוהל מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למערכות המאגר(בתקנה זו – מנגנון הבקרה ,)ובכלל זה נתונים אלה :זהות המשתמש ,התאריך והשעה של ניסיון הגישה ,רכיב המערכת שאליו בוצע ניסיון הגישה ,סוג הגישה ,היקפה ,ואם הגישה אושרה או נדחתה.

(ב) מנגנון הבקרה לא יאפשר ,ככל יכולתו ,ביטול או שינוי של הפעלתו ;מנגנון הבקרה יאתר שינויים או ביטולים בהפעלתו ויפיץ התראות לאחראים.

(ג) בעל מאגר מידע יקבע נוהל בדיקה שגרתי של נתוני התיעוד של מנגנון הבקרה, ויערוך דוח של הבעיות שהתגלו וצעדים שננקטו בעקבותיהן.

(ד) נתוני התיעוד של מנגנון הבקרה יישמרו למשך 24 חודשים לפחות.

ממצאים:

1. נמסר לביקורת כי קיימת שמירת נתוני אבטחה (לוגים) ממערכות האבטחה לא נשמרת כנדרש.
2. לא קיים נוהל המחייב בדיקה תקופתית של הלוגים, גם לא מדגמית.
3. לא קיימת מערכת SIEM לריכוז הלוגים או צוות SOC לניתוחם.

המלצות:

1. על מנגנון תיעוד הגישה למערכות להפיץ התראות לזיהוי אנומליות – מומלץ לבחון ולהטמיע פתרון SIEM- SOC או פתרון MDR מתקדם.
2. יש לשמור את נתוני לוג הגישה למערכות המידע לשנתיים לפחות.
3. יש לקבע בנוהל ולבצע בפועל בדיקה תקופתית, לפחות מדגמית, של הלוגים.

5.16 שימוש במערכות הפעלה מעודכנות

סעיף 13(ג) לתקנות קובע כי "בעל מאגר מידע ידאג לכך שייערכו עדכונים שוטפים של מערכות המאגר, לרבות חומר המחשב הנדרש לפעולתן; לא ייעשה שימוש במערכות שהיצרן לא תומך בהיבטי אבטחה שלהן אלא אם כן ניתן מענה אבטחתי מתאים".

ממצאים:

1. קיים שימוש במערכות הפעלה ישנות ולא נתמכות בעמדות הקצה והשרתים.
2. נמסר לביקורת כי קיים שימוש בשרתי וינדוס 2012 אשר יפסיקו לקבל תמיכה באוקטובר 2023.
3. קיימות תוכנות צד שלישי בגרסאות לא עדכניות, למשל: Adobe AIR, ZOOM, VLC Foxit Reader.
4. קיים שימוש באינטרנט אקספלורר, כולל גרסאות לא עדכניות.

המלצות:

1. יש לשדרג את כלל מערכות ההפעלה והתוכנות לגרסאות עדכניות ונתמכות.
2. מומלץ לבחון שימוש במנגנון אוטומטי לעדכון מערכות צד שלישי.
3. מומלץ להימנע משימוש באינטרנט אקספלורר או לפחות להשתמש בגרסאות עדכניות שלו ובמידה מצומצמת היכן שלא ניתן להימנע מכך.
4. מומלץ להפעיל באופן תקופתי כלי סריקה ייעודי ומקצועי באמצעותו ניתן לבצע סטאטוס עדכניות מערכות הפעלה ותוכנות המותקנות במחשבים ושרתים ברשת ולבצע עדכונים נדרשים כולל בתוכנות צד ג'.

5.17 מצלמות אבטחה ומעקב

ממצאים:

1. לא הוצג לביקורת מידע הנוגע למערכת מצלמות האבטחה בתחומי העירייה.

המלצות:

1. יש להגדיר נוהל מצלמות מפורט המתאר את מורשי הגישה, הנסיבות בהן משתמשים במצלמות וכד'.
2. במידה ונעשה שימוש במצלמות חכמות (יכולת זיהוי פנים\ זיהוי רכב לפי לוחית רישוי) יש לרשום את המאגר אל מול הרשות להגנת הפרטיות.
3. יש להחתים את מורשי הגישה על סעיפים ספציפיים לעניין מצלמות.
4. יש להטמיע מנגנון המאפשר אינדיקציה לגבי הנחשפים למידע (שמירת לוג גישה)
5. קיימת חובה לשים שילוט על מנת ליידע את הסובבים על כך שהמתחמים מצולמים.
6. יש לשמור את ההקלטות לזמן המינימלי הנדרש.
7. מומלץ כי מערכת המצלמות תהיה מופרדת מהרשת הארגונית.
8. במידה וניתן לגשת אל המידע מרחוק, יש להטמיע מנגנון אימות דו-שלבי.

סייבר ישראל
מערך הסייבר הלאומי

מכלול עמידות | בלמ"ס

המלצות ליישום

(Best Practices)

גישת משתמשים לסביבה הארגונית ע"י שימוש ברשת וירטואלית פרטית (VPN)

7. המלצות ליישום בעת תכנון תשתית VPN ארגונית

פרק זה בא לסייע לארגון בגיבוש תכנון מיטבי של תשתית ה-VPN הארגונית.

א. מיפוי משתמשים וצרכים

מומלץ למפות את המשתמשים אשר נדרשים להתחבר לסביבה הארגונית ע"י שימוש ברשת וירטואלית פרטית (VPN). **נספח א'** מכיל טבלת עזר בנושא.

ב. הערכת סיכונים (Risk Assessment)

מומלץ כי הארגון יבצע הערכת סיכונים וזאת לשם איתור פערי אבטחה המחייבים מתן מענה. בכלל זה מומלץ כי הערכת הסיכונים תכלול התייחסות לנושאים הבאים:

1. איתור ומיפוי תרחישי תקיפה רלוונטיים;
2. איתור ומיפוי פערים קיימים (Gap Analysis);
3. איתור ומיפוי דרישות חקיקה ורגולציה רלוונטיות;
4. איתור ומיפוי דרישות חוזיות ועסקיות;
5. איתור ומיפוי נכסי הסייבר אשר גישה אליהם מחוץ לסביבה ארגונית עשויה ליצור סיכון לא סביר;
6. איתור ומיפוי פעולות אשר מחייבות נוכחות מקומית של משתמשים (לדוגמה: ביצוע שינויים בהגדרות תצורה של מערך הגנת המידע וסייבר מהווה פעולה רגישה, אשר יתכן כי בהתאם למדיניות הארגונית לא ניתן לבצע מרחוק);
7. המלצה על בקרות הגנה ליישום;
8. הגדרת מסגרת תקציב מומלצת.

ראוי לציין כי את ממצאי הערכת הסיכונים על הנהלת הארגון לאשר בכתב.

ג. אימות משתמשים

מומלץ לוודא כי כברירת מחדל תשתית ה-VPN תחייב השלמה מוצלחת של אימות המבוסס על MFA (Multi-Factor Authentication), וזאת לפני מתן גישה של המשתמש לסביבה הארגונית. דוגמה ליישום: סיסמה אישית בת 14 תווים לפחות + סיסמת OTP בת שישה תווים.

יש לוודא את קיומה של החלפת סיסמאות עתית, הן בתשתית ה-VPN, והן בתשתית הפנים הארגונית.

ה. היגיינה טכנולוגית של נכס הסייבר (Technology Hygiene)[3]

היגיינה טכנולוגית של נכס הסייבר (Technology Hygiene) מהווה שם מאגד לסט בדיקות אבטחה אשר מטרתן להגביר את ודאות הארגון כי ניתן לתת אמון ביעד ההגנה (Trustworthy).

להלן מספר דוגמאות לבדיקות מקובלות אשר ניתן להחילן במסגרת בדיקת רמת ההיגיינה הטכנולוגית של נכס הסייבר:

1. גרסת מערכת ההפעלה הינה עדכנית;
2. גרסת ה-VPN Client הינה עדכנית;
3. עדכוני האבטחה (פאצ'ים) האחרונים הותקנו בהצלחה;
4. אמצעי האבטחה, דוגמת תוכנת אנטי-וירוס, פועלים ועדכניים;
5. גרסת רכיבי התוכנה עדכנית, דוגמת דפדפן (Browser);
6. רשימת רכיבי התוכנה הינה בהתאם למדיניות הארגון (Application Whitelist);
7. וידוא כי כל תעבורת נכס הסייבר (Non-Split-Tunnel) עוברת דרך בקרת גישה מנוהלת (VPN);
8. האנטי-וירוס עושה שימוש בחתימות מזהים עדכניות ל-24 שעות האחרונות;
9. סריקת אנטי-וירוס בוצעה ב-24 שעות האחרונות, ולא דווח על קיומה של נוזקה (Malware);
10. העדר ממצאים/אינדיקטורים (Indicators) המעידים על תוספות לא מורשות בדפדפן;
11. מניעת גישה מכתובת IP בעלת רמת אמון נמוכה (Trust Level). דוגמה לכתובות IP בעלות רמת אמון נמוכה: כתובת IP אשר משויכת לתשתית גישה אנונימית (דוגמת Tor), כתובת IP אשר מודיעין איומים בסייבר גילה וזיהה שמתבצעים דרכה פעולות זדוניות (דוגמת שליחת Spam).

---

[3] חלק מהיצרנים משתמשים במונח חלופי – "בדיקת ציות" (Security Compliance)

נספח ב – דוח המבדקים הטכנולוגיים, במסמך נפרד. יש לציין כי דוח המבדקים הטכנולוגיים כולל נספחים אשר מהווים חלק אינטגרלי ממנו.

נספח ג – דוח מבדק חדירה – עראבה (דוח מבדק חדירה תשתיתי), במסמך נפרד.

דוח מבדקים טכנולוגיים עיריית עראבה

מוגש עבור:
עיריית עראבה

תאריך הגשה:
2023.07.16

בקרת מסמכים

- **סודיות הלקוח**
מסמך זה מכיל מידע סודי של הלקוח ואין להעתיקו ללא אישור בכתב.

- **מידע קנייני**
תוכן מסמך זה נחשב למידע קנייני ואין לחשוף אותו מחוץ לרשת של הארגון המקבל.
Corporate Integrity נותן הרשאה להעתיק דוח זה לצורך הפצת מידע בארגון שלך או בכל סוכנות רגולטורית.

- **מגבלות והגבלות**
הדוח לא משקף תוקף זדוני ללא הגבלת זמן או משאבים.

מטרת המבדק

- הערכת הסיכונים הפוטנציאליים, חשיפת כשלים וליקויים הקיימים באופן יישום מערך האבטחה התומך בשירותים שונים, חשיפת ליקויים באופן היישום של אמצעי טכנולוגיה ותהליכים תפעוליים החושפים את מערכות המידע לפגיעה או לדלף מידע.
- מתן פתרונות הנדרשים לצמצום או ביטול האפשרות למימוש החשיפה לפגיעה במערך הטכנולוגי.
- קבלת תמונת מצב עדכנית ואמיתית המשקפת את נושא אבטחת המידע בארגון באופן שיאפשר לו לבצע הפעילויות הבאות:
  - לזהות כשלים בכל הקשור לנושאי מדיניות, ארגון, ניהול, תפעול וטכנולוגיה במערך המחשוב.
  - לבצע הערכת הסיכונים ולהגדיר את רמת חומרתם.
  - ליישם המלצות לשיפור המצב הקיים.

תכולת המבדק

- במהלך הבדיקות שבוצעו נעשה שימוש בין היתר בכלי סריקה אוטומטיים לאיתור חולשות אבטחה (Nessus Professional) בטווח הכתובות החיצוני וטווח כתובות פנימי.
- בוצעה בדיקת מסנני תוכן בתיבות הדואר וניסיונות spoofing.
- בוצעה בדיקת עמדה סטנדרטית.
- בוצע סקר אבטחה פיזי.
- בוצעה בדיקת Ping Castle לבחינת ה-Active Directory.
- בוצע קמפיין פישינג.
- בוצע מבדק חדירה פנימי אשר פורסם בדו"ח נפרד.
- בוצעה בדיקת מוצר ההגנה הקיים על תחנות הקצה

תקציר מנהלים

סיכום הערכה
בהתבסס על הערכת האבטחה עבור טווחי הכתובות החיצוניות, הפנימיות והמצב הנוכחי של החולשות שזוהו, חלק ניכר מהחולשות שנמצאו וצוינו בדוח, עשויות להוות גורם לפרצות אבטחה במערכת.
ניתן לתקן פגיעות אלה על ידי ביצוע שיטות העבודה המומלצות, וההמלצות שניתנו בגוף הדוח.

המלצות אסטרטגיות

יש לטפל בממצאים הקריטיים והגבוהים בהקדם האפשרי, ולאחר מכן יש לטפל בממצאים הבינוניים והנמוכים, כמו כן, יש להתייחס לממצאים אשר מסווגים כמידע בהקדם האפשרי לצורך בדיקה ומעקב, בכדי לוודא כי אינם מהווים חשיפה של מידע שאינו אמור להיות נגיש.

פירוט כללי

דירוג סיכונים
הטבלה שלהלן מפרטת את שמות הסיכונים והצבעים המשמשים בכל הדוח בכדי לספק מערכת ניקוד סיכונים ברורה ותמציתית.
יש לציין כי קימות הסיכון העסקי הכולל הנשקף מכל אחת מהנושאים שנמצאו בבדיקה כלשהי, אינה בתחום שלנו. משמעות הדבר היא כי סיכונים מסוימים עשויים להיות מדווחים גבוהים מנקודת מבט טכנית, אך כתוצאה מבקרות אחרות שאינן ידועות לנו, הם יכולים להיחשב מקובלים על ידי הארגון.

#	דירוג סיכון	CVSSv3 Score	תיאור
1	קריטי	9.0 - 10	פגיעות ברמת סיכון קריטית. ממצא זה דורש פתרון במהירות האפשרית.
2	גבוהה	7.0 – 8.9	פגיעות ברמת סיכון גבוהה. ממצא זה דורש פתרון בטווח הקצר.
3	בינוני	4.0 – 6.9	פגיעות ברמת סיכון בינונית. ממצא זה דורש פתרון לאחר טיפול בממצאים הקריטיים והגבוהים.
4	נמוך	1.0 – 3.9	פגיעות ברמת סיכון נמוכה. יש לטפל בכך כחלק ממשימות התחזוקה השוטפות.
5	מידע	0 – 0.9	ממצא החושף מידע. יש לוודא כי ממצאים אלו אינם חושפים מידע רגיש.

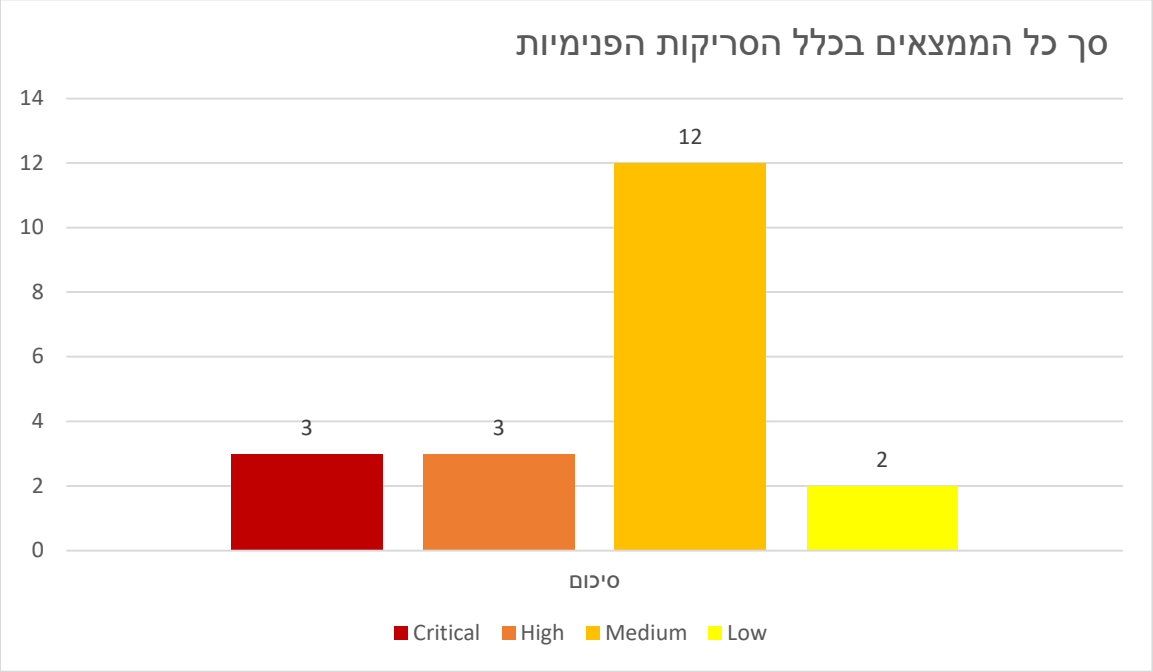
פירוט הממצאים

1. סריקות פנימיות

מדובר על סריקה אוטומטית דרך כלי Nessus ברישוי, יש לעבור על הדוח המלא לצורך קבלת תמונה מלאה, יש להתייחס לכל הממצאים האינפורמטיביים מהסיבה כי מכילים הרבה אינפורמציה וסריקת פורטים, דברים אשר גם משם ניתן למצוא ממצאים קריטיים.

- חשוב לזכור כי Nessus הינו כלי סריקה אוטומטי אשר סורק ברגע שמקבל פינג לעמדה והעמדה זמינה. ייתכן וכי קיימות כתובות נוספות שלא זיהנו במהלך הבדיקה וכי ישנם עוד ממצאים שם. כמו כן, במידה והעמדה מכובה / אינה עונה לפינג או לא זמינה מסיבה כלשהי היא לא תסרק.

- להלן גרף סיכום ממצאים של סריקה פנימית הכולל את כלל הממצאים שנמצאו במהלך הסריקה של הרשת הפנימית של המועצה.



להלן תקציר הממצאים אשר מפורטים בדו"ח ה-Nessus המצורף לנספחים טכניים והמפרט כתובות IP\שם DNS של העמדה עליה התגלתה החולשה והכולל פתרון מפורט:

- SNMP Agent Default Community Name (public) - Solution -> Disable the SNMP service on the remote host if you do not use it.
- לא קיים שימוש במנגנון הגנה חשוב על שירות SMB(SMB Signing).
- נמצא כי קיים שימוש בגרסת ESXi לא נתמכת בעל מספר חולשות אבטחה ברמות סיכון שונות.
- נמצא כי קיים שימוש בהצפנת SSL + TLS נמוכה, נדרש לבטל תמיכה בכל הפרוטוקולים האלו ולהשתמש רק ב TLS 1.2 ומעלה בארגון.
- מספר של רכיבי תקשורת כגון מתגים וכד' בעלי קושחה לא עדכנית וחשופה לחולשות קריטיות.
- זוהי תמצית של הממצאים אשר כל הממצאים לעיל נוגעים לכלל הרשת הפנימית – מומלץ לעבור על דוח הסריקה אשר מצורף לדוח מסכם זה ולפעול על פי הנחיות הממצאים החל מקריטי לגבוה בינוני ומטה ואשר כלול בדוח לכל ממצא פתרון הכולל דרכי יישום לטיפול.

2. סריקות חיצוניות

1. **SSL Medium Strength Cipher Suites Supported (SWEET32)** - קיימת תמיכה בפרוטוקולי הצפנה ברמה בינונית.

רמת סיכון: **גבוהה**

המלצה: יש להחליפם בפרוטוקולים חזקים יותר בעלי מפתחות הצפנה ארוכים.

כתובות:

- https://arraba.muni.il

2. **HSTS Missing from HTTPS Server** - נמצא כי השרת לא אוכף HTTP Strict Transport Security, אשר אחראי על ווידאי תקשורת דרך HTTPS בלבד. ללא מנגנון זה, תוקפים זדוניים יכולים לבצע מתקפות שונות להורדת ההצפנה בתקשורת בין הקלינט לשרת.

רמת סיכון: בינונית

המלצה: יש לייצא תעודה חדשה תקנית או לרכוש תעודה תקנית מגורם מוסמך.

כתובות:

- https://arraba.muni.il

3. **SSL Certificate Cannot Be Trusted** - תעודת השרת X.509 לא trusted. מצב זה יכול לנבוע משלוש סיבות עיקריות:

1. תעודה אשר נוצרה בצורה עצמאית ולא מגורם מוסמך.

2. תעודה אשר פג תוקפה או שגיאת זמן באחד מהפרמטרים של התעודה.

3. תעודה אשר מכילה חתימה אשר לא מתאימה לתיאור התעודה ולא אומתה.

רמת סיכון: בינונית

המלצה: יש לייצא תעודה חדשה תקינה או לרכוש תעודה תקינה מגורם מוסמך.

כתובות:

- https://arraba.muni.il

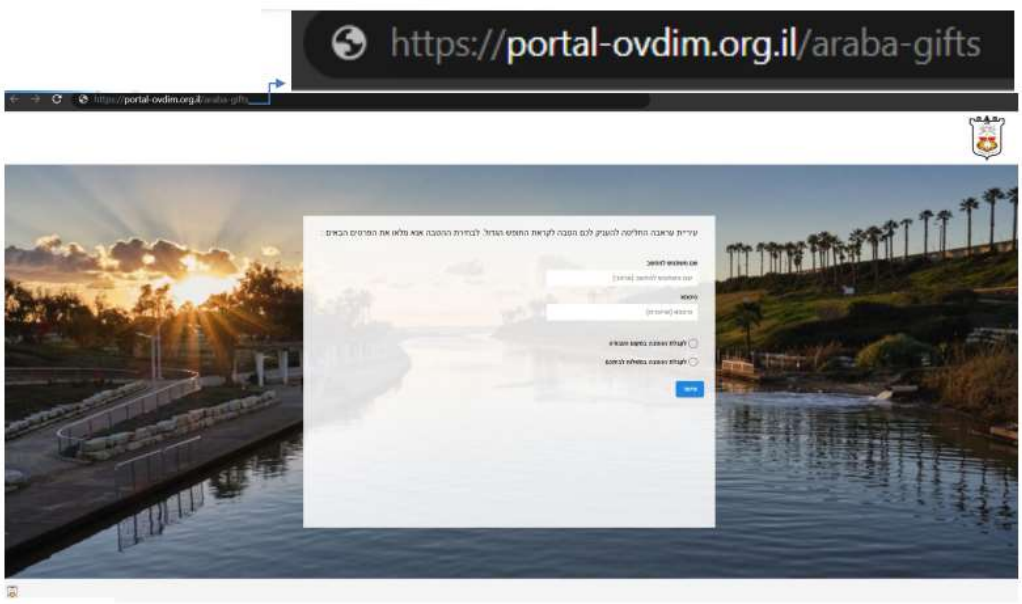
3. קמפיין פישנג

כחלק מתהליך שיפור אבטחת המידע בארגון ומודעות העובדים לסיכונים הקיימים, בוצע תרגיל פישינג על כלל העובדים.
הקמת אתר המדמה פורטל עובדים לצורך קבלת מתנה לחופש הגדול.
שליחת מייל פישינג לעובדי הארגון.
העלאת מודעות וערנות עובדי הארגון בנושא סיכוני אבטחת מידע וסייבר הקיימים כיום בעולם.
להלן תוצאות הקמפיין:

- מספר האימיילים שנשלחו: 72
- מספר העובדים אשר לחצו על הקישור: 13, כ- 18%
- מספר העובדים אשר לחצו והזינו פרטים: 23, כ-32%
- מספר העובדים אשר התעלמו מהקישור: 36, כ- 50%
- מספר הלחיצות הדרוש בכדי לפגוע בארגון: 1

המלצות:

- מומלץ לחזק את מודעות העובדים בנושא לחיצה על קישורים מצורפים במיילים.
- מומלץ להגביר את מודעות העובדים בהכרת url's וכתובות מייל לגיטימיים אירגוניים.
- מומלץ לחזק את מודעות העובדים ועירנותם בכל הנוגע להזנת פרטים וסיסמאות.



Integrity

4. תיבות דואר אלקטרוני

כחלק מהסקר מבוצעות בדיקות לבחינת מנגנוני ההגנה בתיבות הדוא"ל הארגוניות.
מהבדיקה עולה, כי בעיריית עראבה, לא קיים שימוש בתיבות דוא"ל ארגוניות מנוהלות וישנו שימוש בתיבות אישיות מספקים שונים (Gmail, Walla וכו').
יש לציין כי בעירייה נרכש בעבר רישוי עבור תיבות מנוהלות בסביבת 365 של Microsoft, אך לא בוצעה הטמעה כלל של המערכת.
שימוש בתיבות דוא"ל אישיות מגביר את הסיכון של הארגון לזליגה של מידע רגיש, במקרה של עזיבת עובד המידע הרגיש לא נמחק, מונע את האפשרות לבצע הקשחות נאותות לחסימת כניסה של קבצים זדוניים באמצעות המייל, מגביר את הסיכוי לקבלת מיילים של פישינג מגורמים זדוניים ועוד.

המלצה: יש לבצע הטמעה של מגנוני סינון מיילים מנוהלים אשר יוכלו לאפשר לצוות המחשוב של הארגון לבצע ניטור ובקרה על התיבות ולבצע הקשחות במידת הצורך.

5. בדיקת עמדה נייחת

כחלק מהבדיקה התחברנו לעמדת מחשב סטנדרטית בארגון בכדי לבדוק אילו מגבלות קיימות על משתמשים בארגון.
חלק מהבדיקות אשר בוצעו הן: ניסיון גלישה לאתרים העלולים להיות מסוכנים, בדיקת עדכוני אבטחה, בדיקת הרשאות משתמש ועוד.
חלק מבדיקותינו הסתמכו על תשובותיו של איש המחשוב של הארגון.

- **המשתמש הלוקאלי אינו אדמין לוקאלי.**
- **בדיקת חסימת אתרי פורנוגרפיה בגלישה – תקין**
- **בדיקת חסימת אתרי unrated – תקין**
- **בדיקת חסימת אתרים Newly Observed Domains – תקין**
- **בדיקת הורדת קובץ Eicar דמוי זדוני בפרוטוקולים HTTP/HTTPS - תקין**
- **בדיקת שינוי הגדרות מוצר האנטי וירוס – תקין**
- **בדיקת ניסיון הרצת סקריפט PowerShell - תקין**
- **בדיקת קיימות חומת אש של Windows לוקאלית – תקין**
- **בדיקת נעילת מסך – תקין**
- **בדיקת חסימת ניסיון lsass dump – תקין**
- **האם רישוי מערכת ההפעלה חוקי – תקין**

1. בדיקת הכנסת USB לעמדה

חיבור מדיה חיצוני לא נחסם.

רמת סיכון: קריטית

המלצה:
יש לחסום אפשרות לחיבור מדיה נתיקה בעמדות. במידת הצורך יש להעביר קבצים דרך שרת הלבנה או להגדיר whitelist לחיבורי מדיה נתיקה מאושרים מראש של הארגון אשר נסרקים ונבדקים לגבי וירוסים בצורה שוטפת.

2. סיסמא ל-UEFI/BIOS

נמצא כי לא קיימת סיסמא ל-UEFI/BIOS

רמת סיכון: גבוהה

המלצה:
יש להגדיר סיסמאות ניהול לממשקים אלו בכדי למנוע ממשתמשים/גורמים זדוניים לבצע שינויים במערכת בין אם בטעות או בזדון.

3. בדיקת קיימות מערכת LAPS

לא נמצא שירות LAPS

רמת סיכון: **קריטית**

המלצה:
מומלץ להטמיע פתרון LAPS לניהול סיסמאות משתמשי אדמין לוקאלי בארגון.

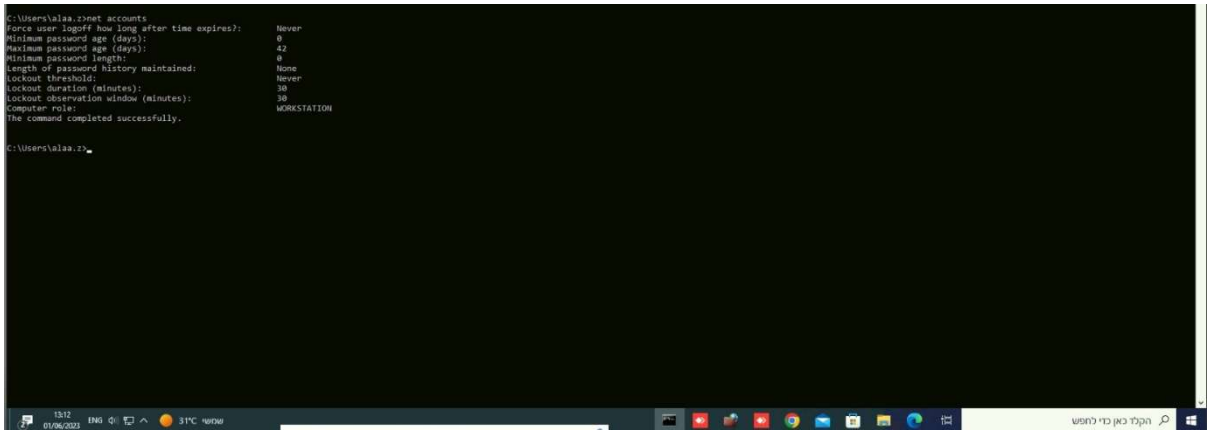
4. בדיקת פוליסת סיסמאות לוקאלית ובדומיין

פוליסת הסיסמאות אינה מספקת ומסכנת את הארגון

רמת סיכון: גבוהה

המלצה: אנו ממליצים להקשיח את פוליסת הסיסמאות של הארגון בכל המערכות הרלוונטיות הקיימות בארגון עם לכל הפחות הפרמטרים הבאים:

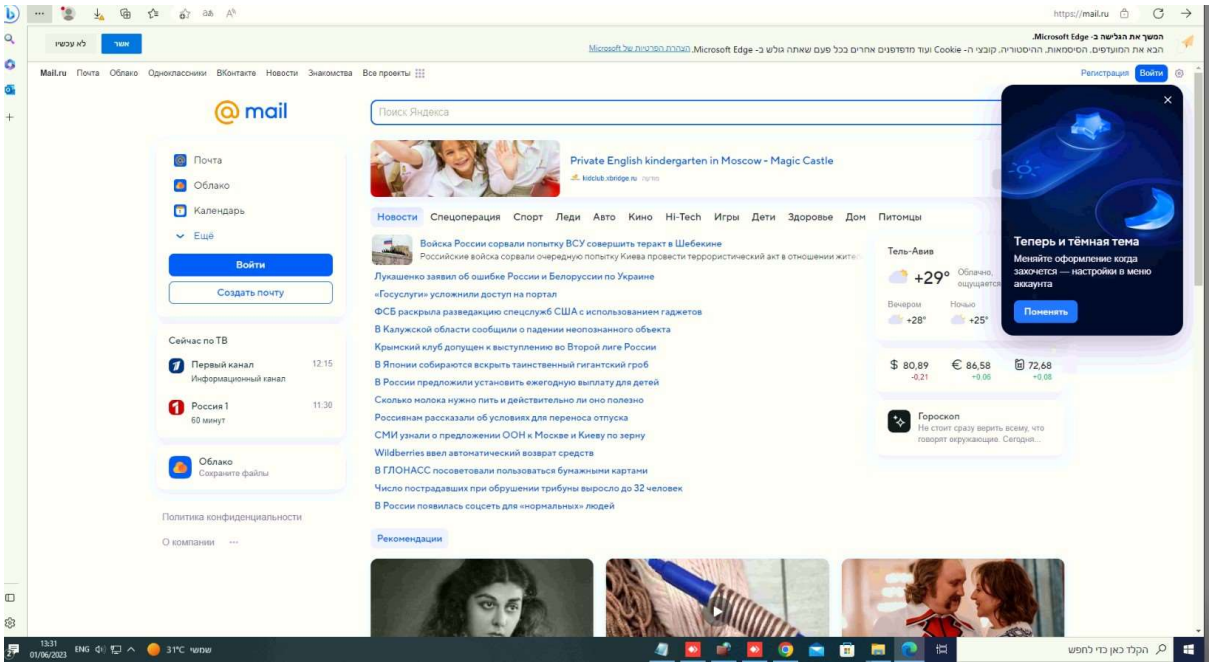
- אורך - על סיסמאות להכיל מינימום של כ-9 תווים עבור משתמשים רגילים ו-15+ תווים למשתמשים בעלי הרשאות גבוהות / החברים בקבוצות רגישות כמו Admins Domain, גיבויים וכדי.
- חיוב שימוש באותיות גדולות (A-Z)
- חיוב שימוש באותיות קטנות (a-z)
- חיוב שימוש במספרים (0-9)
- חיוב שימוש בסימנים מיוחדים (לדוגמא: !@#$%^&*)(><?", וכדי)
- חיוב הגדרת ללא רצפים (לדוגמא: ללא 1234,1234567,98765 כחלק מהסיסמה).
- איסור על שימוש בשם המשתמש חלק מהסיסמא.
- הגדרת מספר ניסיונות התחברות כושלים לכל היותר - 5 ניסיונות.
- הגדרת זמן נעילה לאחר מספר ניסיונות כושלים, לכל הפחות חצי שעה ובנוסף הגדרת התראה לצוות המחשוב על מספר ניסיונות התחברות כושלים ונעילת המשתמש כאשר ההמלצה הינה נעילה קבועה עד שחרור ידני של צוות המחשוב



5. בדיקת גלישה לאתרי מיילים חיצוניים

ממצא: נמצא כי ניתן לגלוש לאתרי מיילים חיצוניים אשר עלולים להיות לא מאובטחים ולהקשות על פורנזיקה במצב של הזלגת מידע.

רמת סיכון: **גבוהה**
המלצה: מומלץ פרט לאתרי אימייל חיצוניים שנחסמים, לחסום גם גישה לאתרי אימיילים לא ארגוניים.

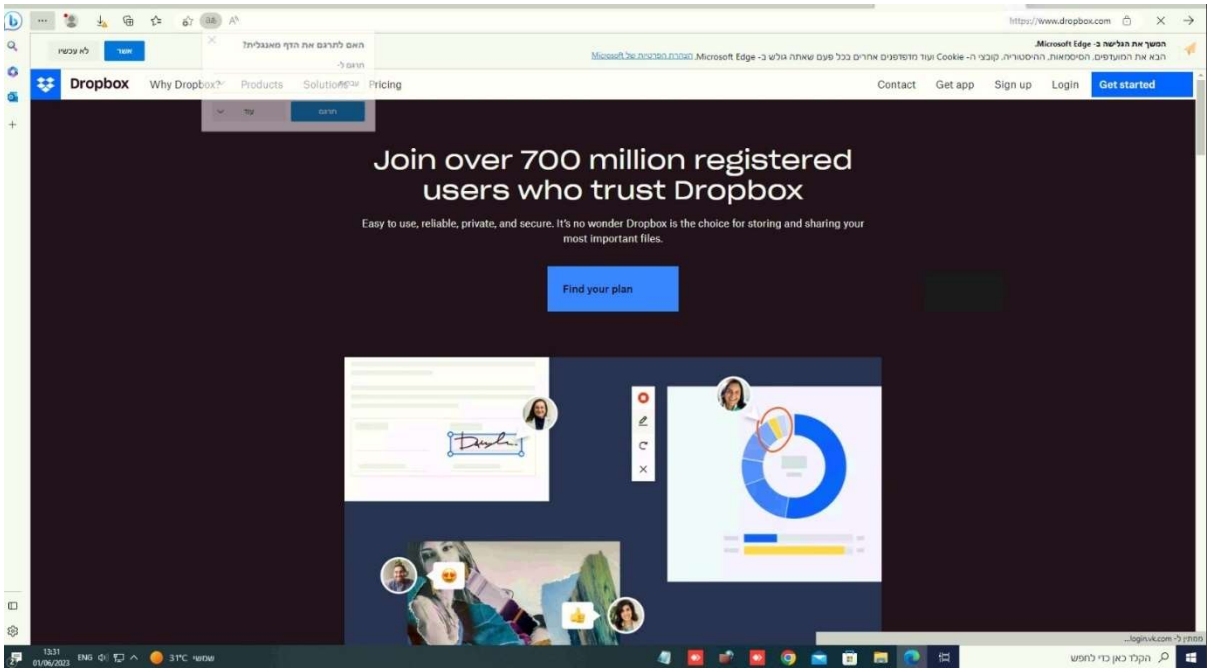


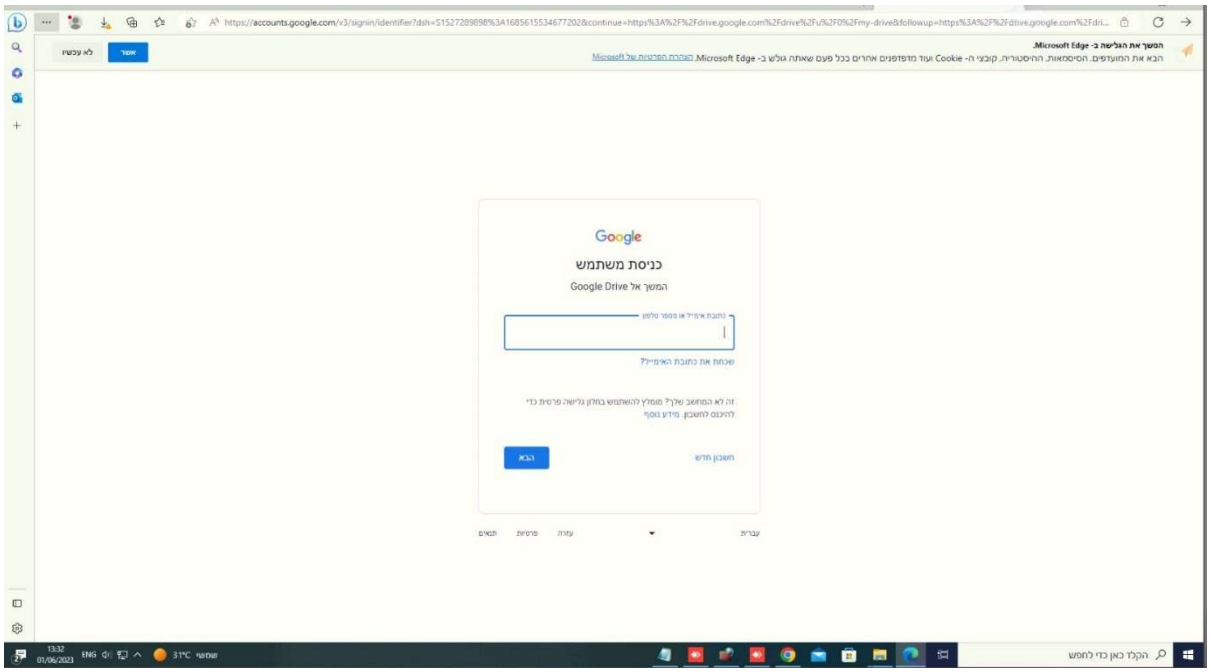
6. בדיקת חסימת אתרי אחסון חיצוניים בגלישה

ממצא: נמצא כי ניתן לגלוש לאתרי אחסון חיצוניים אשר עשויים לסייע בהחדרת קבצי נוזקה ומקשים על מניעה של דלף מידע.

תיאור האיום: נוזקה, זליגת מידע.

רמת סיכון: גבוהה
המלצה: יש לחסום גישה לאתרים אלו.



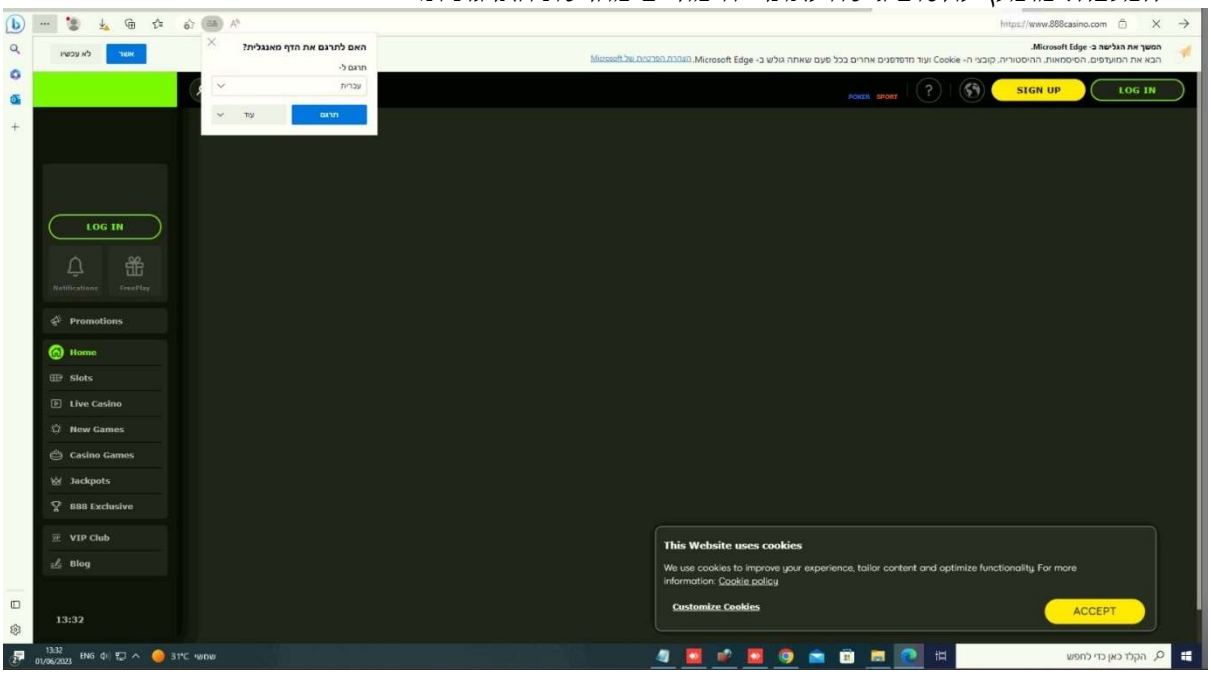


7. בדיקת גלישה לאתרי הימורים

ממצא: נמצא כי משתמשי הקצה רשאים לגלוש לאתרי הימורים.

רמת סיכון: גבוהה

המלצה: מומלץ לחסום גישה לאתרי הימורים מהרשת הארגונית.



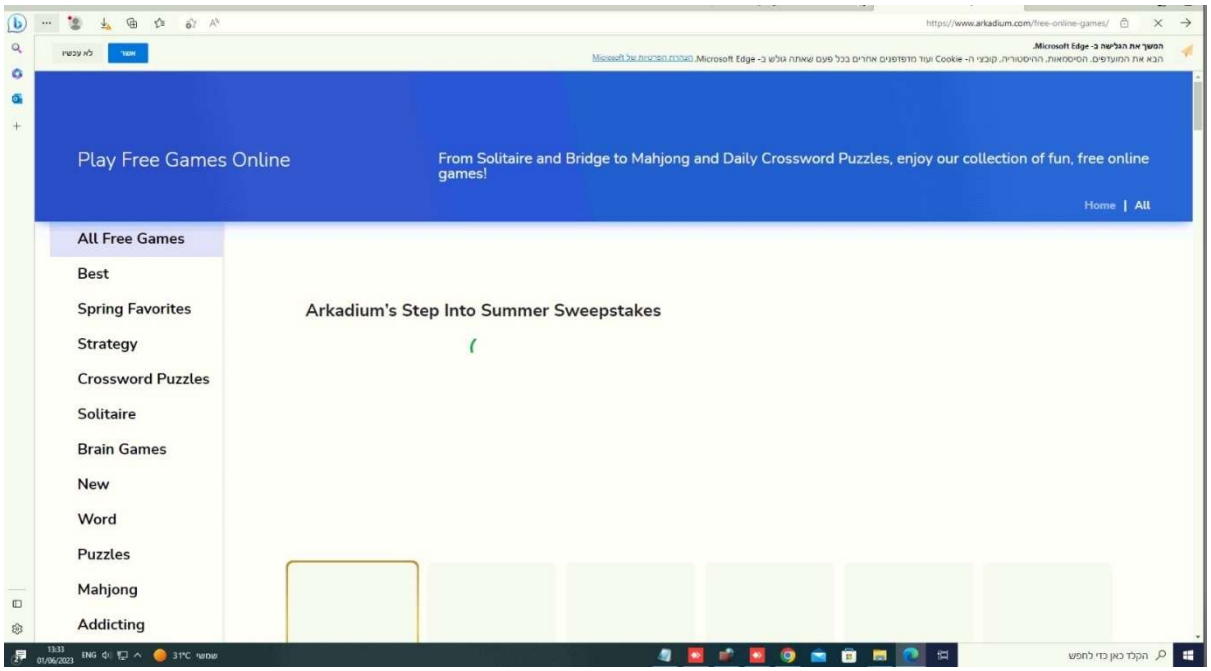
8. בדיקת גלישה לאתרי משחקים

ממצא: נמצא כי ניתן לגלוש לאתרי משחקים אשר עשויים להיות לא מאובטחים.

תיאור האיום: נוזקה

רמת סיכון: **גבוהה**

המלצה: יש לחסום גישה לאתרים אלו.



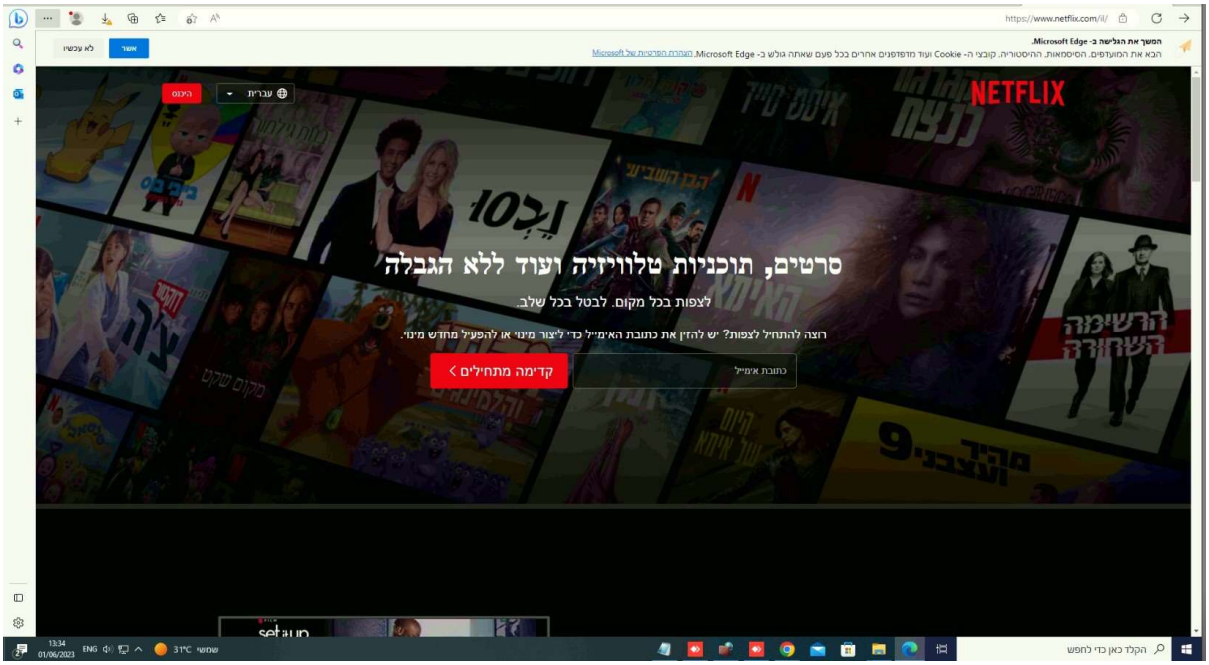
9. בדיקת גלישה לאתרי שירותי סטרימינג

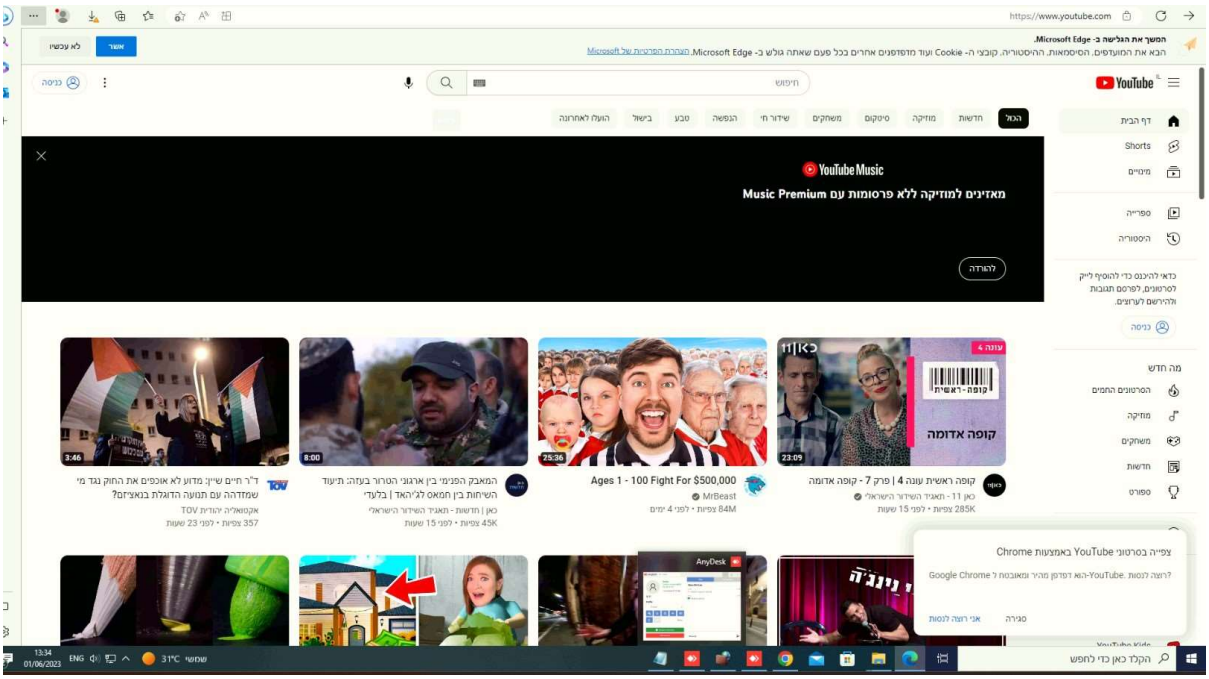
ממצא: נמצא כי ניתן לגלוש לאתרי שירותי סטרימינג אשר עשויים להיות לא מאובטחים.

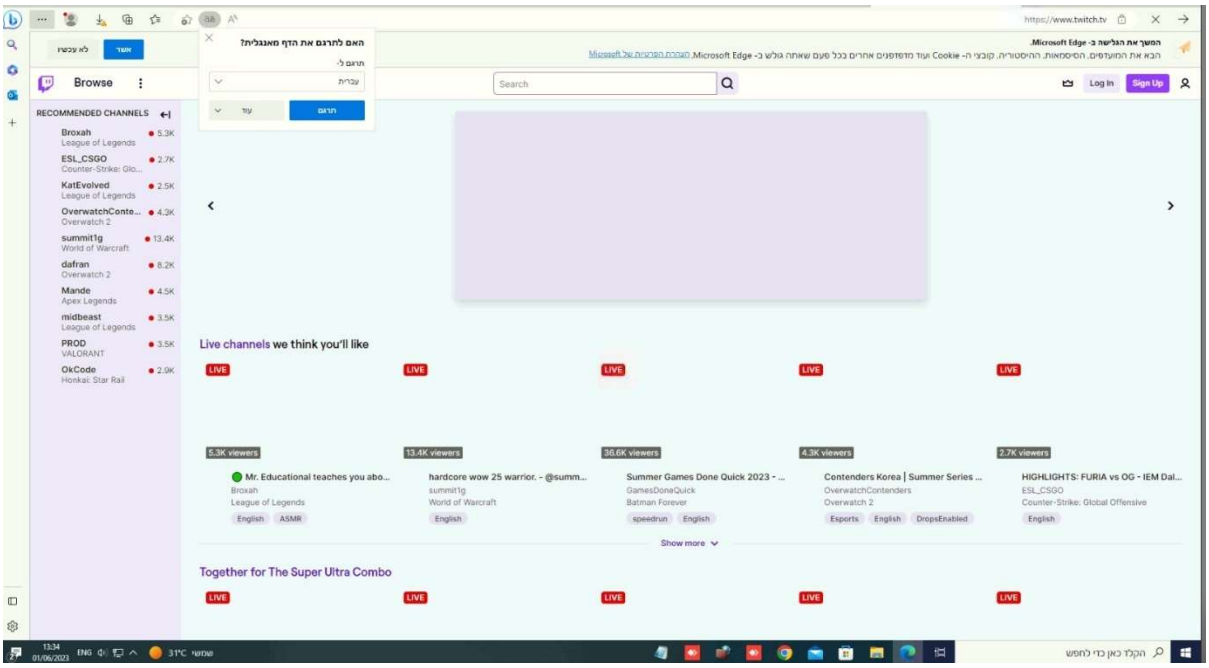
תיאור האיום: נוזקה

רמת סיכון: **גבוהה**

המלצה: יש לחסום גישה לאתרים אלו.





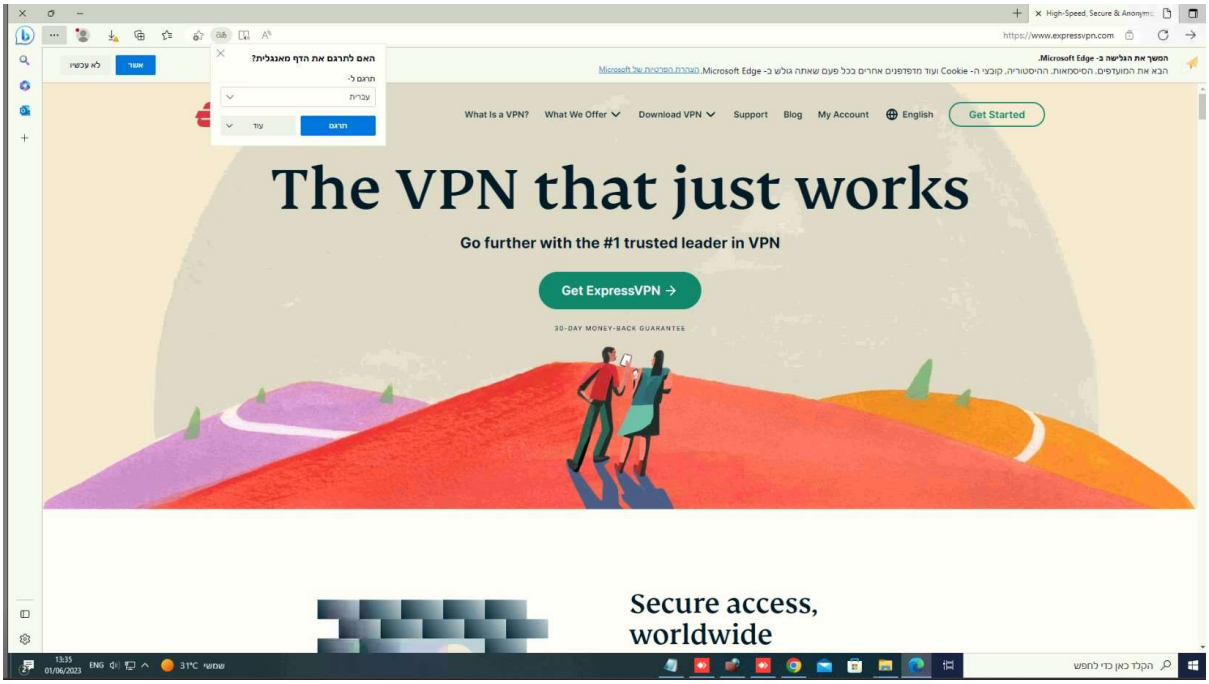


10. בדיקת גלישה לאתרי שירותי VPN

ממצא: נמצא כי ניתן לגלוש לאתרי שירותי VPN אשר עשויים לשמש למעקף של חומת האש.
תיאור האיום: נוזקה, חדירה מבחוץ

רמת סיכון: **גבוהה**

המלצה: יש לחסום גישה לאתרים אלו.



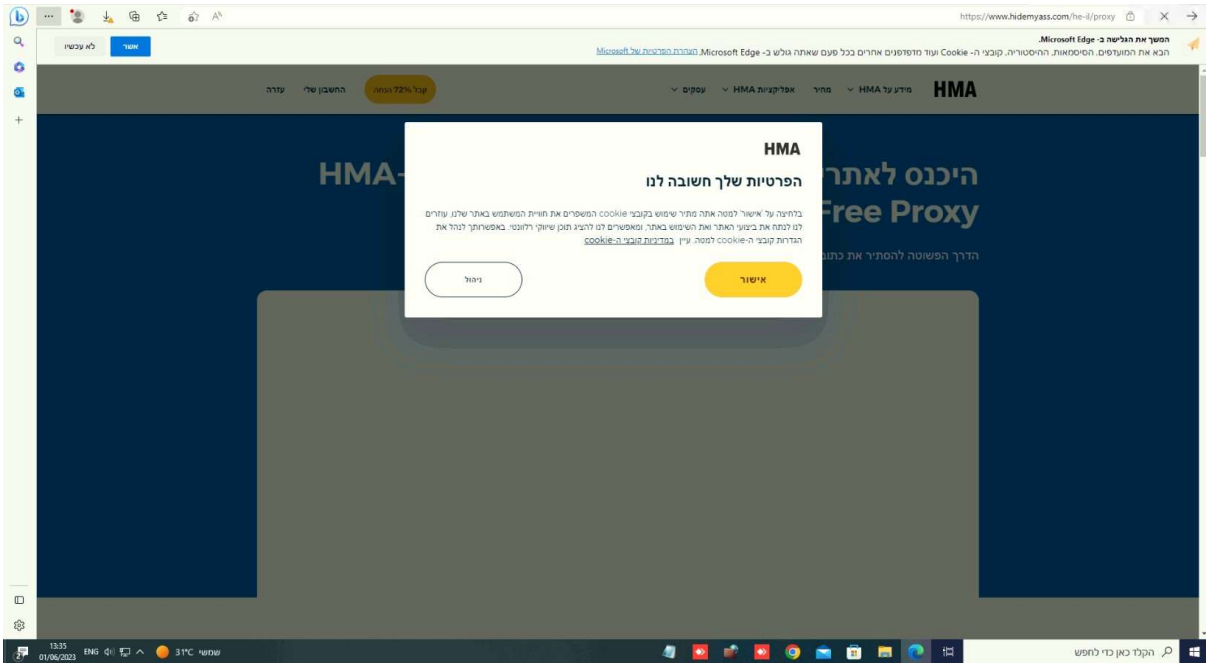
11. בדיקת גלישה לאתרי שירותי פרוקסי

ממצא: נמצא כי ניתן לגלוש לאתרי שירותי פרוקסי.

תיאור האיום: נוזקה, חדירה מבחוץ

רמת סיכון: **גבוהה**

המלצה: יש לחסום גישה לאתרים אלו.



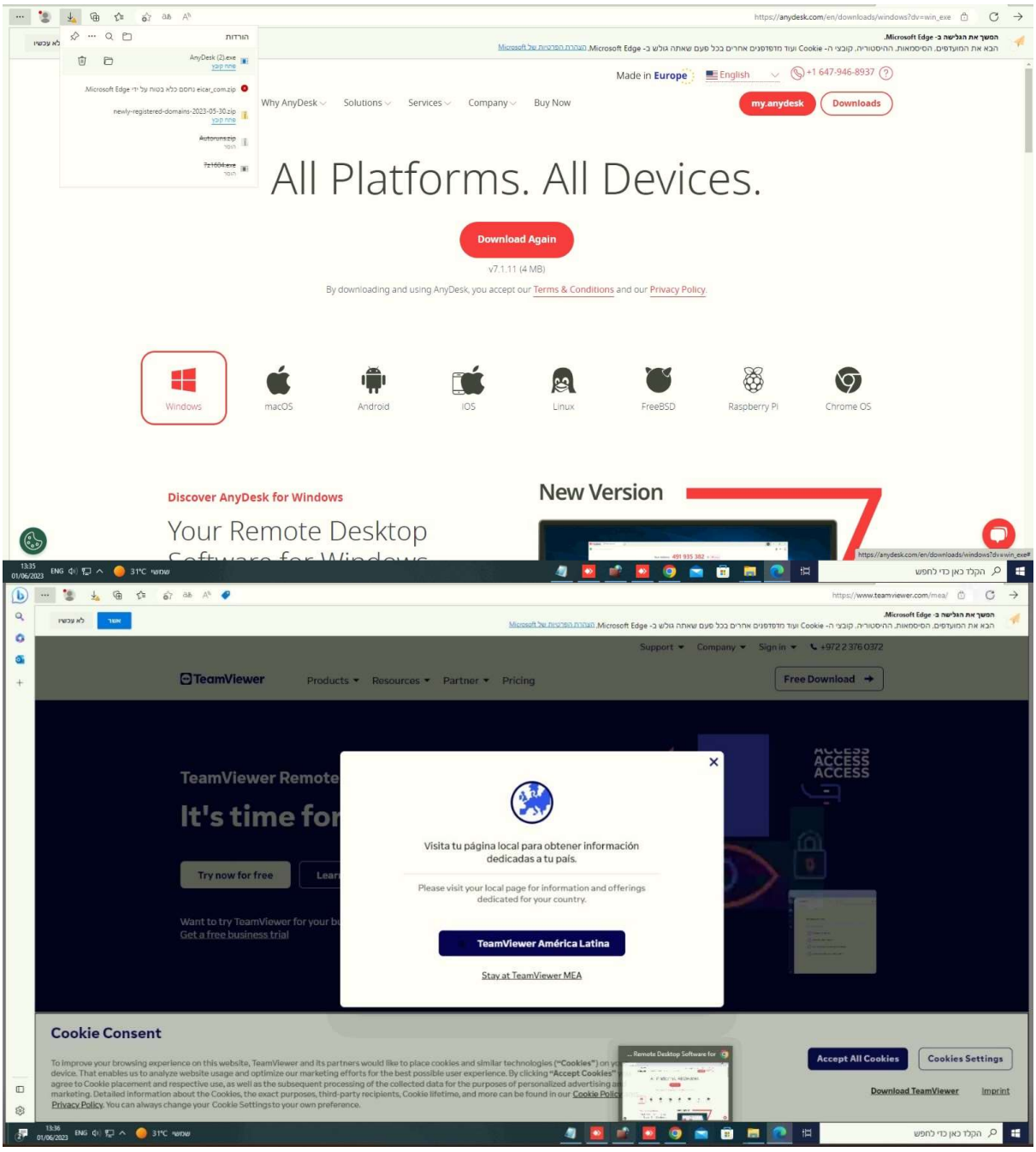
12. בדיקת גלישה לאתרי שירות חיבור מרוחק בגלישה

ממצא: נמצא כי ניתן לגלוש לאתרי שירות חיבור מרוחק אשר יכולים לאפשר חיבור מרחוק לעמדה.

תיאור האיום: חדירה מבחוץ

רמת סיכון: **גבוהה**

המלצה: יש לחסום גישה לאתרים אלו. מומלץ להשתמש רק באפליקציה אחת קבועה לחיבור מרחוק במוצר עם רישיון.



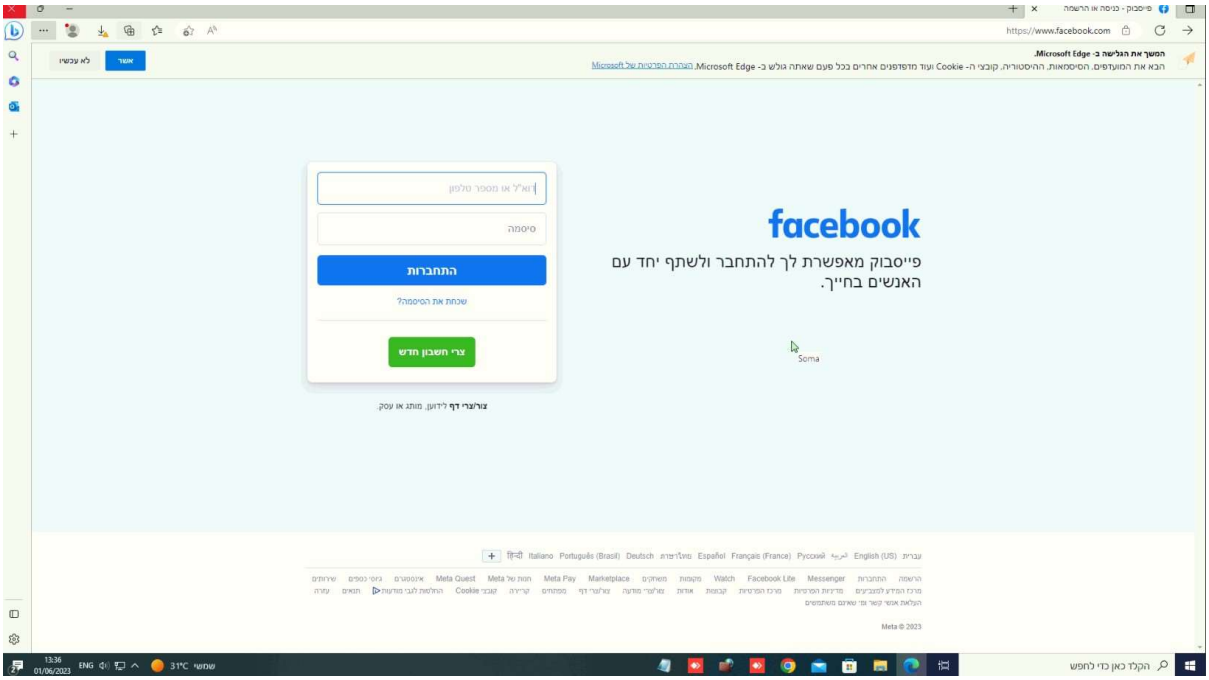
13. בדיקת גלישה לאתרי מדיה חברתית

ממצא: נמצא כי ניתן לגלוש לאתרי מדיה חברתית אשר עשויים להיות לא מאובטחים.

תיאור האיום: זליגת מידע, נוזקה

רמת סיכון: **גבוהה**

המלצה: יש לחסום גישה לאתרים אלו.



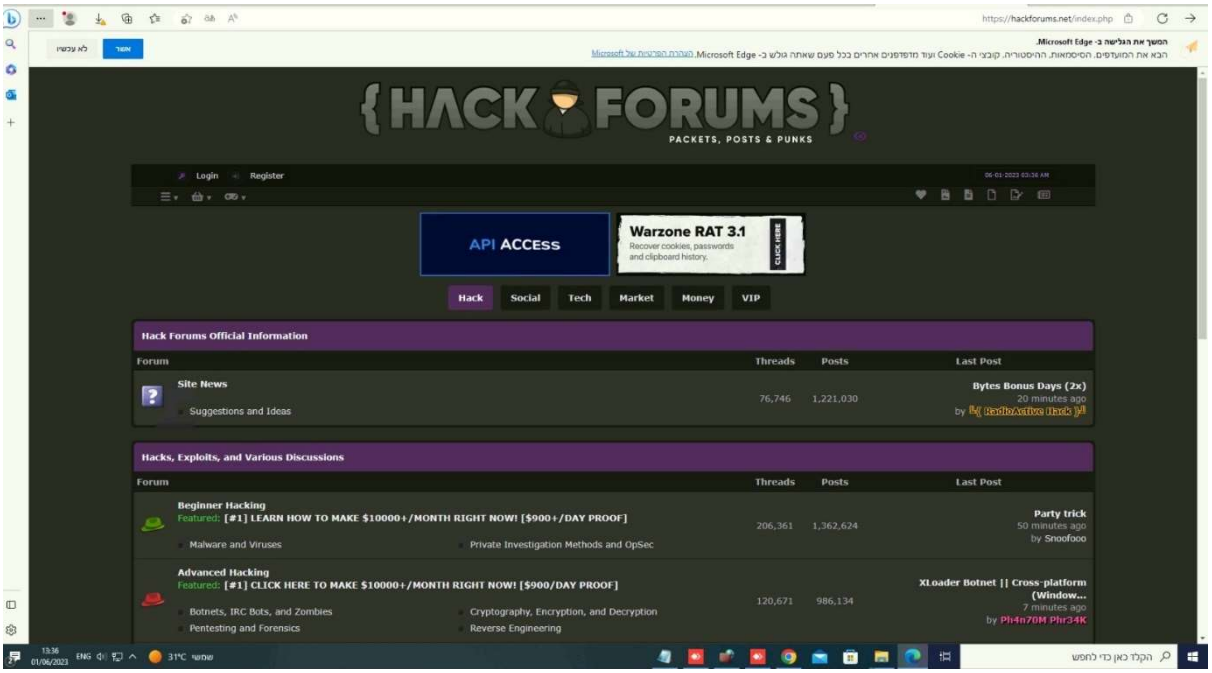
14. בדיקת גלישה לאתרים עם כלי האקינג

ממצא: נמצא כי ניתן לגלוש לאתרים עם כלי האקינג אשר עשויים לשמש תוקף.

תיאור האיום: נוזקה, השתלטות על מערכות

רמת סיכון: **גבוהה**

המלצה: יש לחסום גישה לאתרים אלו.



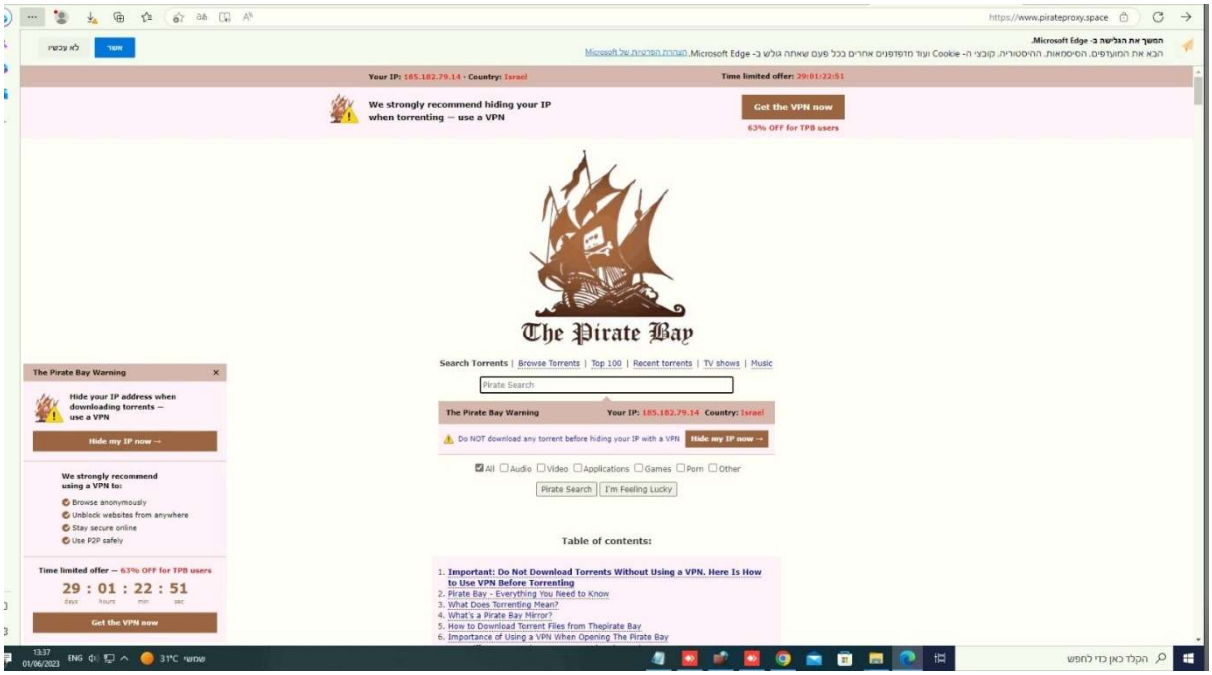
15. בדיקת חסימת אתרי Torrents בגלישה

ממצא: נמצא כי ניתן לגלוש לאתרים מקטגוריה זו.

תיאור האיום: נוזקה, השתלטות על מערכות

רמת סיכון: **גבוהה**

המלצה: יש לחסום גישה לאתרים אלו.



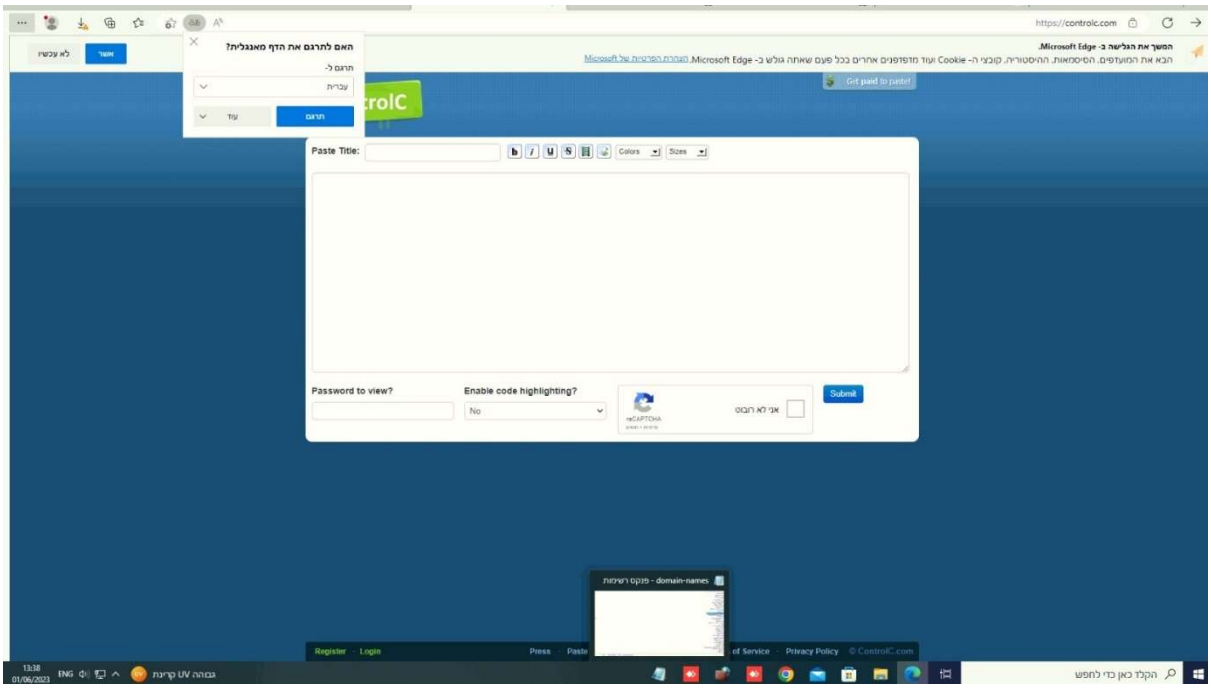
16. בדיקת גלישה לאתרי שירותי Information Technology

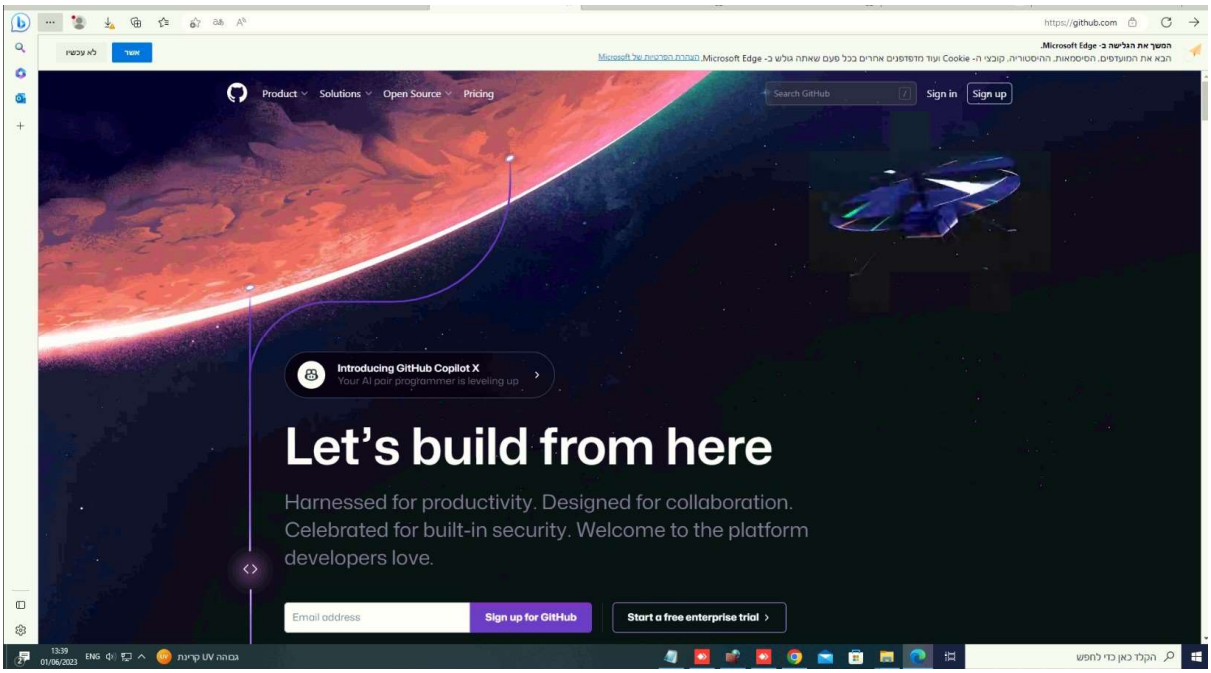
ממצא: נמצא כי ניתן לגלוש לאתרים IT אשר עלולים להכיל קוד זדוני להורדה/ העתקה.

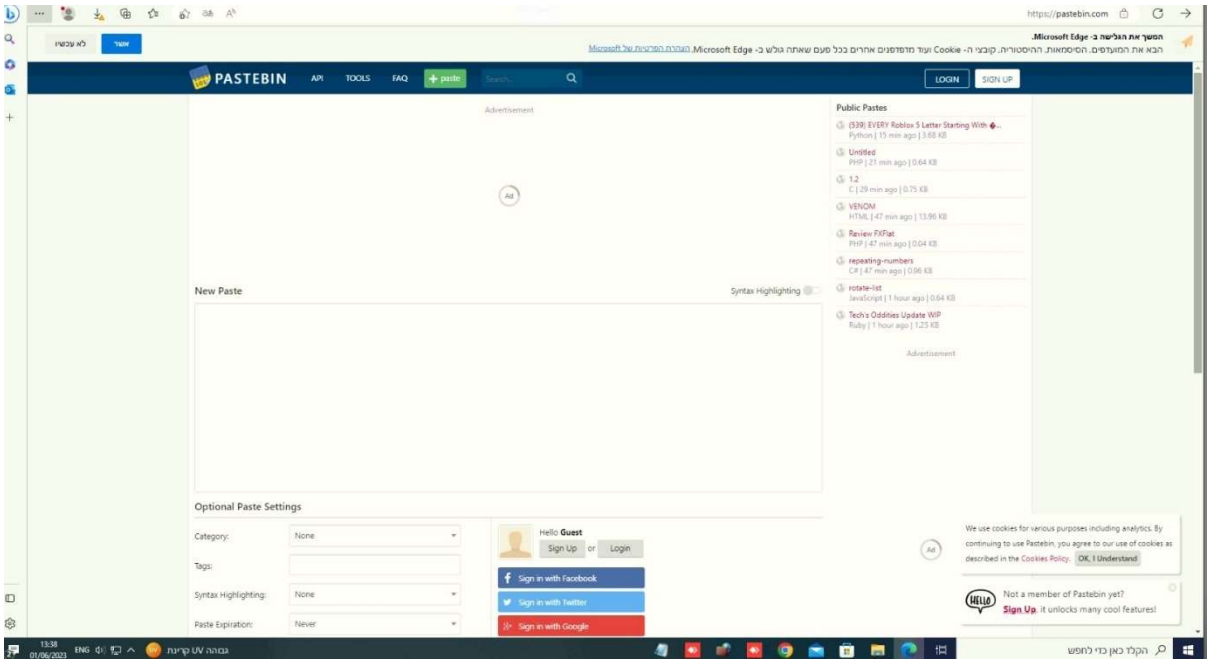
תיאור האיום: נוזקה, השתלטות על מערכות

רמת סיכון: **גבוהה**

המלצה: יש לחסום גישה לאתרים אלו למעט עבור מי שיש לו בהם צורך.


Paste Title:
Password to view?
Enable code highlighting?
Submit


Product
Solutions
Open Source
Pricing
Search GitHub
Sign in
Sign up
Introducing GitHub Copilot X
Your AI pair programmer is leveling up
Let's build from here
Harnessed for productivity. Designed for collaboration.
Celebrated for built-in security. Welcome to the platform
developers love.
Email address
Sign up for GitHub
Start a free enterprise trial



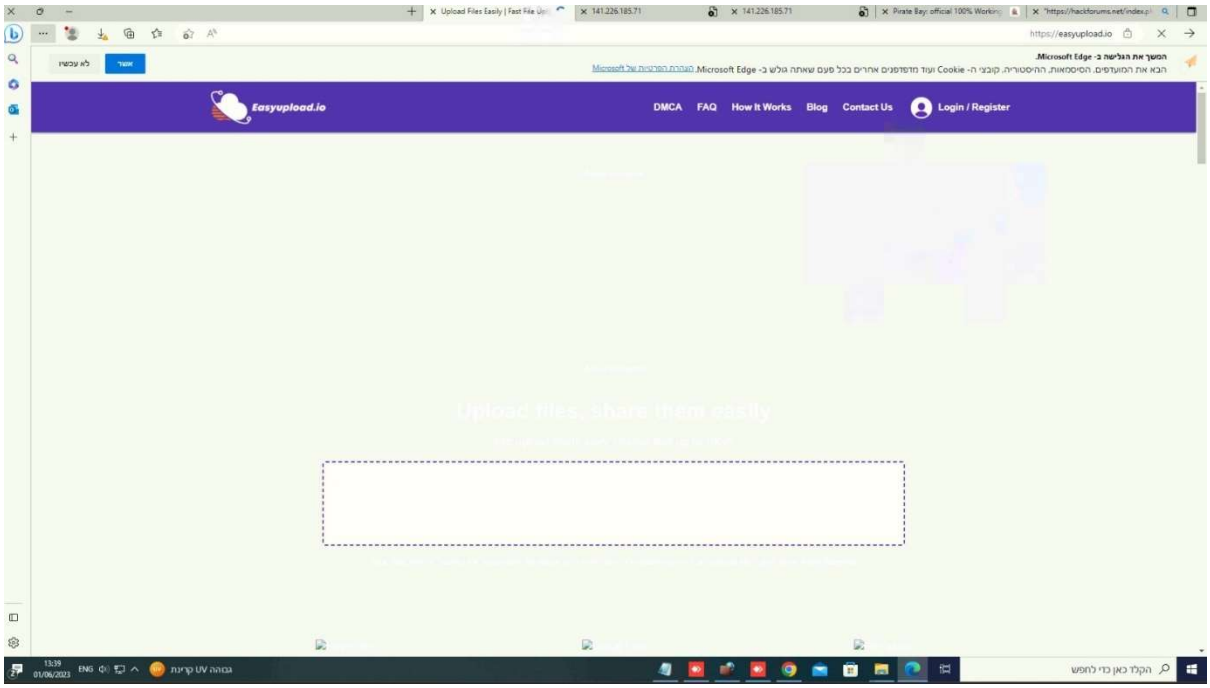
17. בדיקת גלישה לאתרי שירותי file sharing and storage

ממצא: נמצא כי ניתן לגלוש לאתרי file sharing & storage אשר עלולים להוביל לזליגת מידע והחדרת נוזקות.

תיאור האיום: זליגת מידע, החדרת נוזקה.

רמת סיכון: גבוהה

המלצה: יש לחסום אפשרות לגלישה לאתרים מסג "File Sharing and Storage"



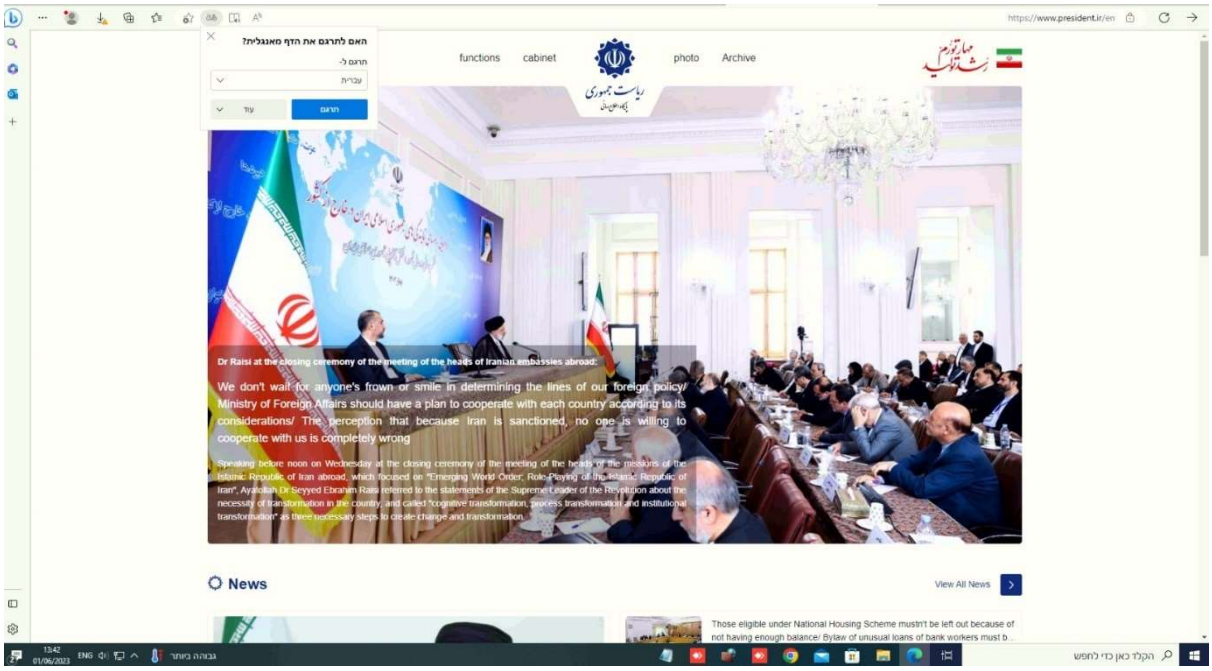
18. בדיקת גלישה לאתרים של מדינות עוינות – geo protection

ממצא: נמצא כי ניתן לגלוש לאתרים של מדינות ללא יחסים דיפלומטיים עם ישראל. ביניהם עשויים להיות אתרים מסוכנים וזה מגדיל את הסיכון להיפגע. כמו כן מגדיל את הסיכוי להיפגע מאתר מתחזה אנטי- ישראלי.

תיאור האיום: גישה למדינות וממדינות עוינות עם פעילויות ענפות במרחב התקיפה של הסייבר.

רמת סיכון: קריטי

המלצה: יש לחסום גישה לאתרים אלו.



19. בדיקת הורדה והרצת קובץ EXE

ממצא: נמצא כי המשתמש רשאי להוריד קבצי הרצה אך לא להריצם.
יש לחסום הורדה של קבצי הרצה. היכולת להוריד קבצי הרצה מסירה בפני תוקף מכשול בדרך להפעלת קובץ זדוני. כמו כן משתמשים עשויים להוריד גם שלא בכוונה קובץ לא מאובטח.

תיאור האיום: נוזקה, השתלטות על מערכות

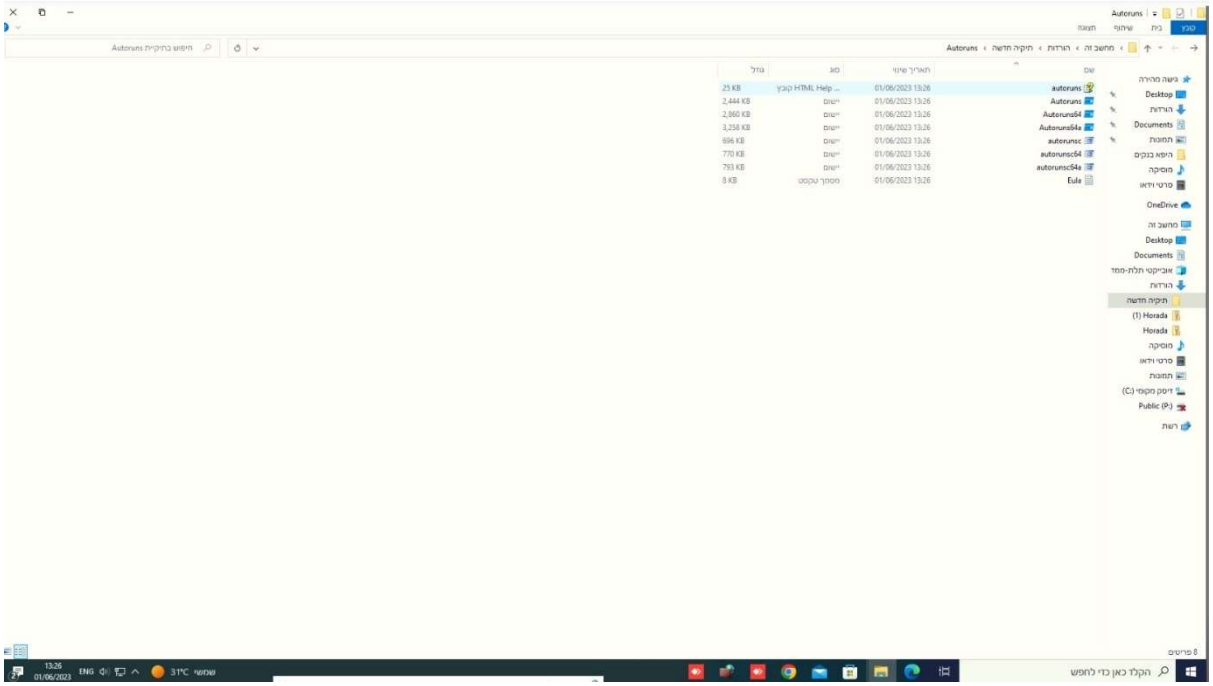
רמת סיכון: קריטי
המלצה: אנו ממליצים לחסום את האפשרות מהמשתמשים להוריד קבצי הרצה.

20. בדיקת הורדה וחילוץ קבצי ארכיב (zip)

ממצא: נמצא כי המשתמש יכול להוריד ולחלץ קבצים מתוך קבצי ארכיב שעלולים להכיל קבצים זדוניים.
העובדה שהקובץ מורד בעודו מכווץ מקשה על כלי ההגנה לגלות האם הוא זדוני.

תיאור האיום: נוזקה, השתלטות על מערכות

רמת סיכון: קריטי
המלצה: יש לחסום הורדה של קבצי ארכיב.

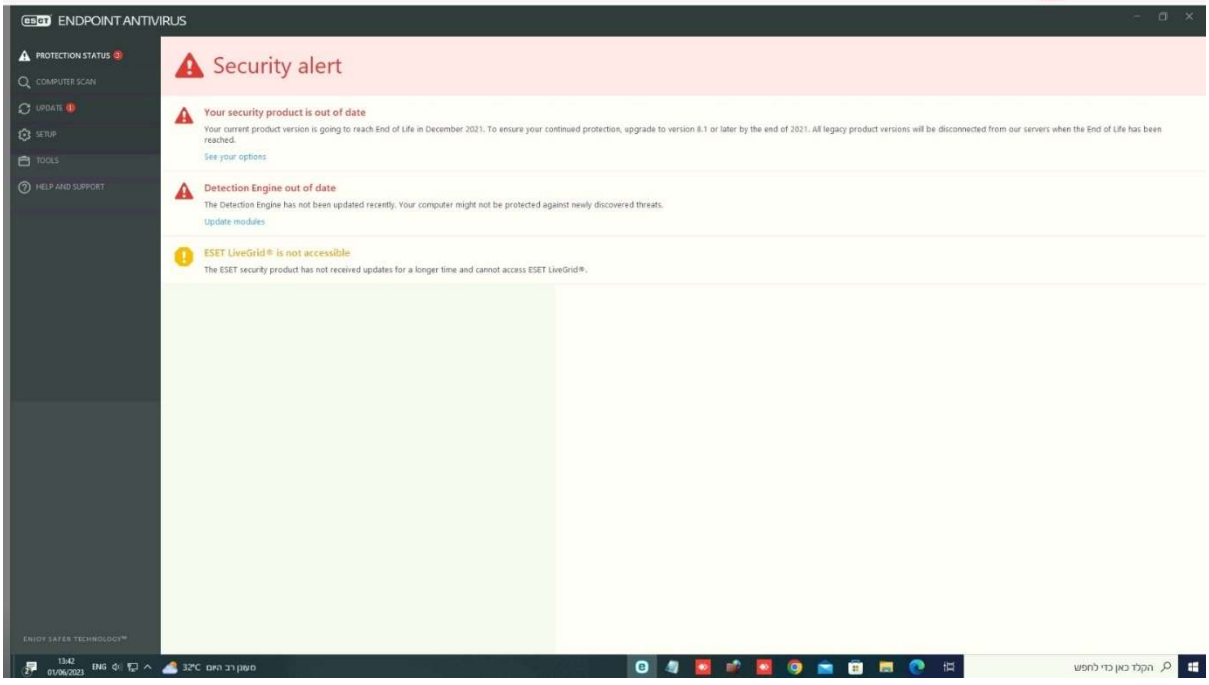


21. בדיקת גרסת אנטי-וירוס

ממצא: נמצא כי על התחנה הנבדקת מוצר ההגנה מסוג אנטי-וירוס הינו לא עדכני ואף פג תוקף הרישוי שלו.

רמת סיכון: קריטי

המלצה: יש לוודא כי קיים מוצר הגנה מסוג אנטי-וירוס (בעדיפות XDR, מפני שכיום מוצרי הגנה המבוססים חתימות אינם מספקים) עדכני וברישוי על כלל תחנות הקצה כולל השרתים בארגון.

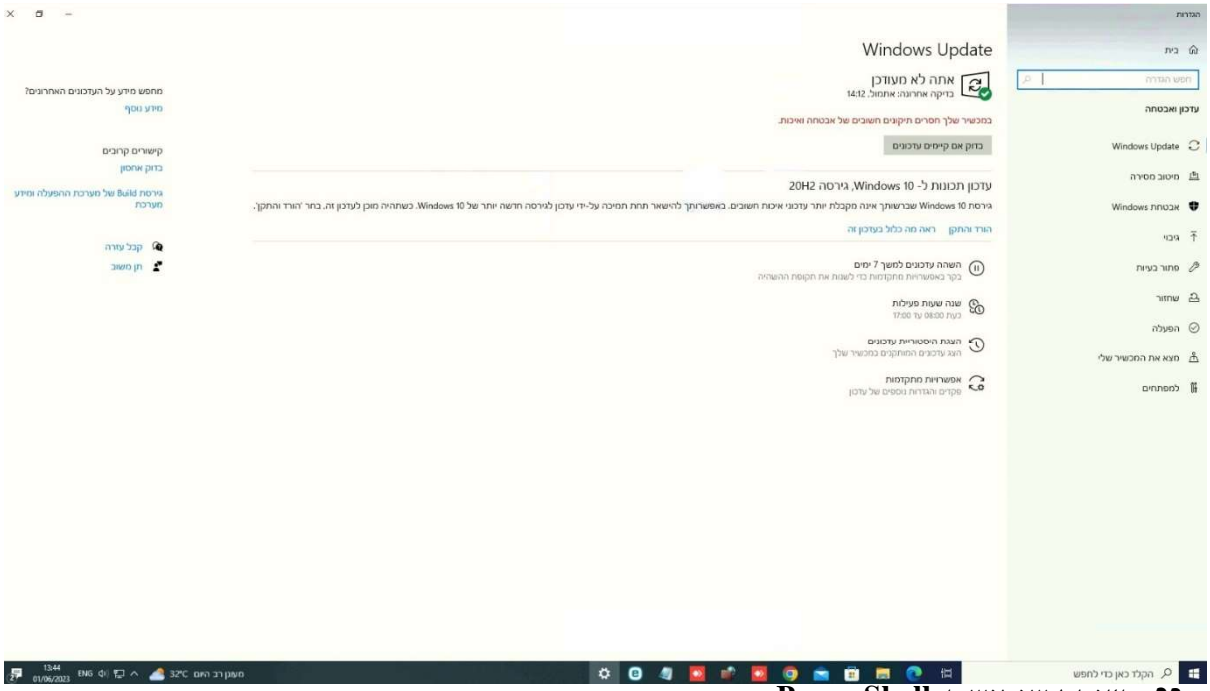


22. בדיקת עדכוני מערכת ההפעלה ועדכוני אבטחה של Windows

ממצא: נמצא כי על התחנה הנבדקת נדרש לבצע עדכוני אבטחה ועדכוני מערכת, ישנם מספר עדכוני אבטחה קריטיים חסרים.

רמת סיכון: **קריטי**

המלצה: יש לוודא כי כלל מערכות ההפעלה בארגון מעודכנות, נתמכות וקיימים בהן כלל עדכוני המערכת ועדכוני האבטחה העדכניים של Microsoft.



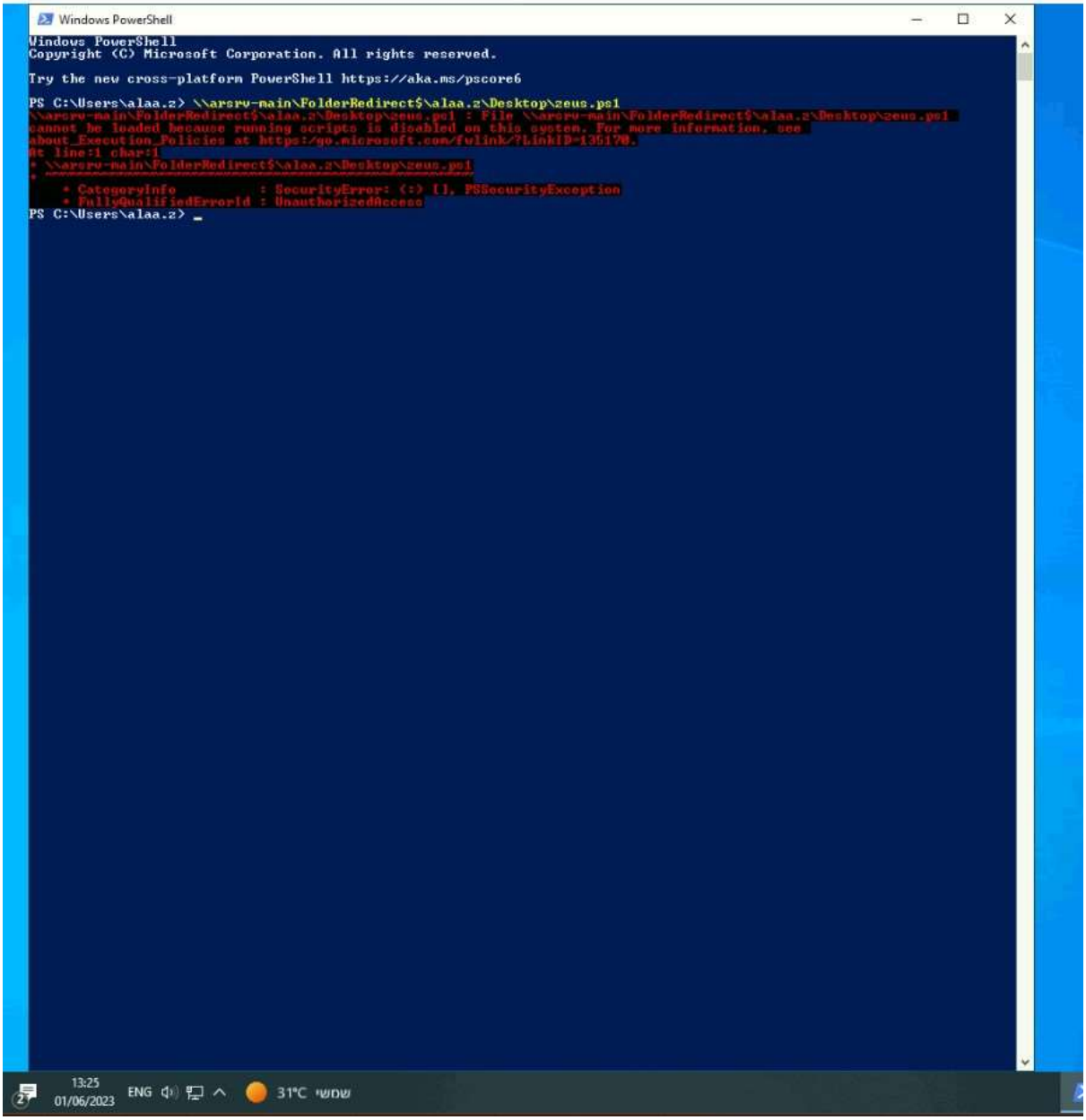
23. בדיקת שימוש ב-PowerShell

ממצא: נמצא כי משתמש הקצה יכול להפעיל PowerShell

תיאור האיום: נוזקה.

רמת סיכון: **קריטי**

המלצה: מומלץ לחסום גישה ל-PowerShell למשתמשי הקצה ולהחריג רק למי שיש צורך בכך.

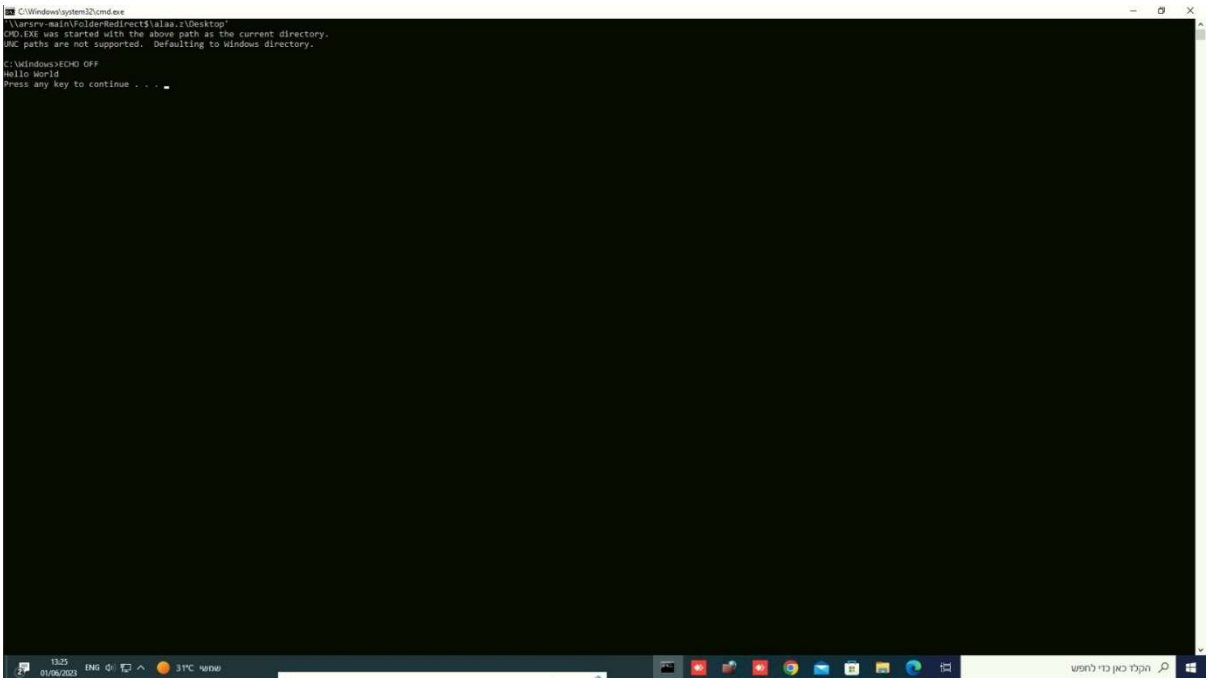


24. בדיקת הרצת סקריפטים

ממצא: נמצא כי ניתן להריץ סקריפטים מסוג BAT.

תיאור האיום: נוזקה, השתלטות על מערכות

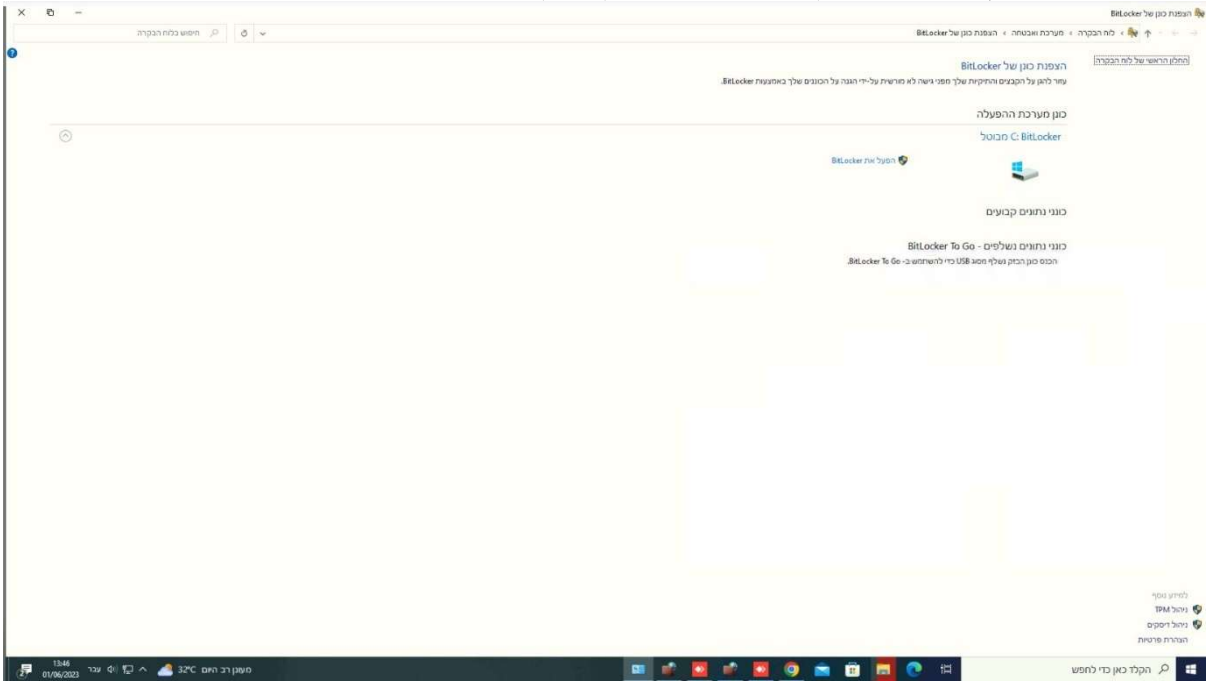
רמת סיכון: קריטי
המלצה: יש למנוע ממשתמשי הקצה להריץ סקריפטים על עמדות הקצה.



25. בדיקת הצפנת מחשבים

ממצא: נמצא כי המחשב הנבדק לא מוצפן (לדוגמא באמצעות תוכנת Bitlocker).
תיאור האיום: זליגת מידע

רמת סיכון: קריטי
המלצה: מומלץ להפעיל מנגנון הצפנה של הדיסק המקומי של המחשב כדוגמת bitlocker.

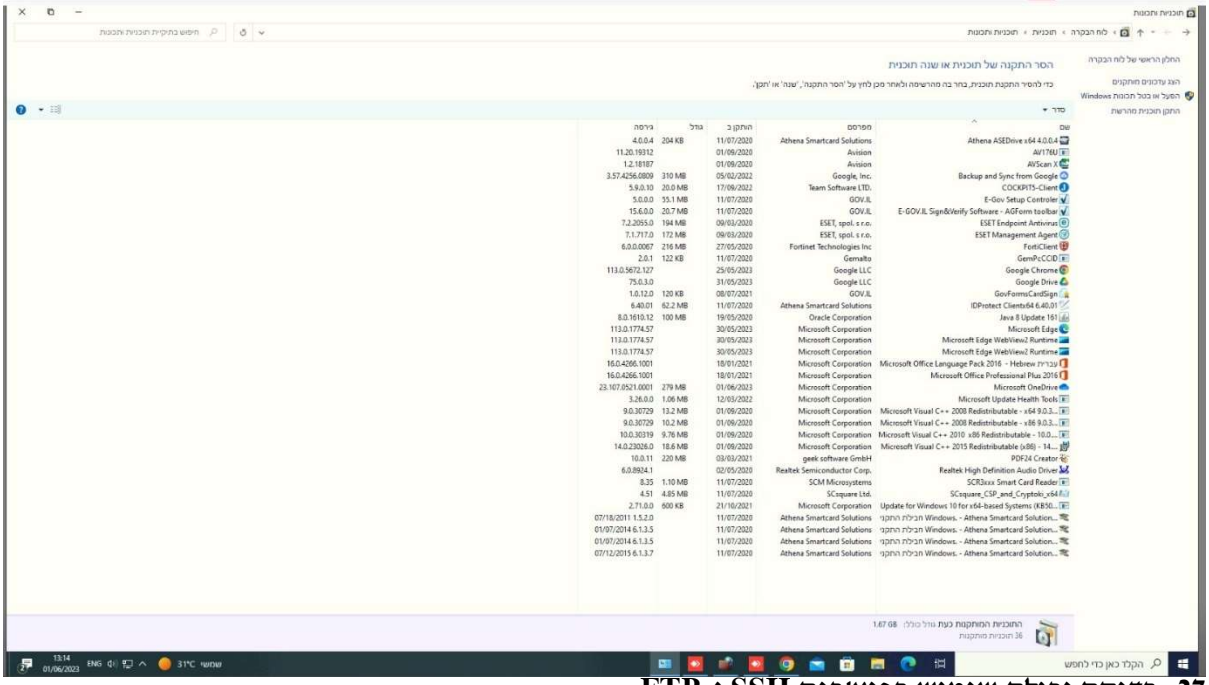


26. בדיקת גישה ללוח הבקרה

ממצא: נמצא כי משתמש הקצה יכול לגשת ללוח הבקרה ולהסרת התוכנות.

תיאור האיום: איסוף מידע, התבססות תוקף בתוך הרשת

רמת סיכון: בינוני
המלצה: מומלץ לחסום ממשתמשי הקצה את האפשרות לגשת ללוח הבקרה בכדי למנוע מהם לבצע שינויים/ למנוע מתוקף לאסוף מידע על המערכת.

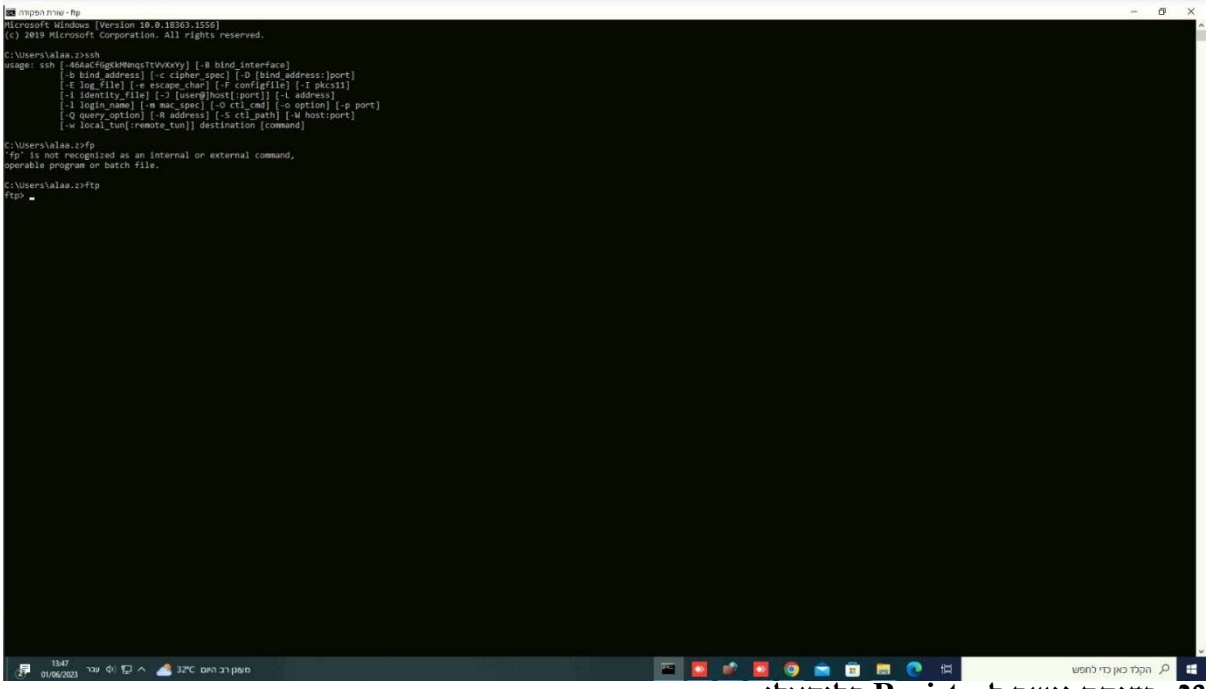


27. בדיקת יכולת שימוש בפיצ'רים SSH ו-FTP

ממצא: נמצא כי משתמש הקצה רשאי להשתמש בפיצ'רים אלו אשר באמצעותם פוטנציאלית ניתן לבצע חיבור מרוחק לעמדת הקצה וממנה ובנוסף מאפשרים העברת קבצים. מה שעלול להוביל לזליגה של מידע רגיש או לחלופין הכנסה של נוזקות אל הארגון.

תיאור האיום: חדירה מבחוץ, נוזקה

רמת סיכון: קריטי
המלצה: מומלץ לחסום אפשרות לשימוש בפרוטוקולים אלה עבור משתמשים אשר אינם זקוקים להם.



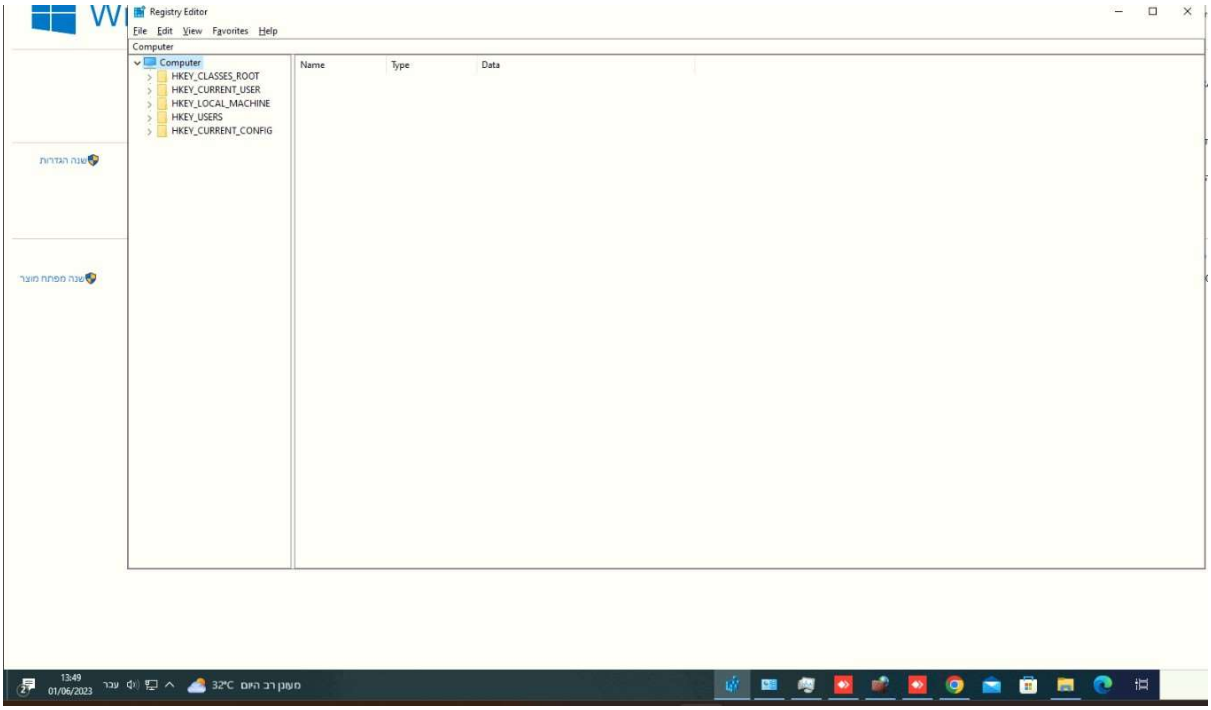
28. בדיקת גישה לRegistry הלוקאלי

ממצא: נמצא כי המשתמש הלוקאלי יכול לגשת לRegistry. גישה זו עשויה לאפשר למשתמש הקצה לבצע שינויים במערכת אשר יחלישו את הגנותיה

תיאור האיום: איסוף מידע, התבססות תוקף בתוך הרשת

רמת סיכון: קריטי

המלצה: יש לחסום ממשתמשי הקצה את האפשרות לגשת ל- Registry בכדי למנוע מהם או מגורמים זדוניים לבצע שינויים במערכת.

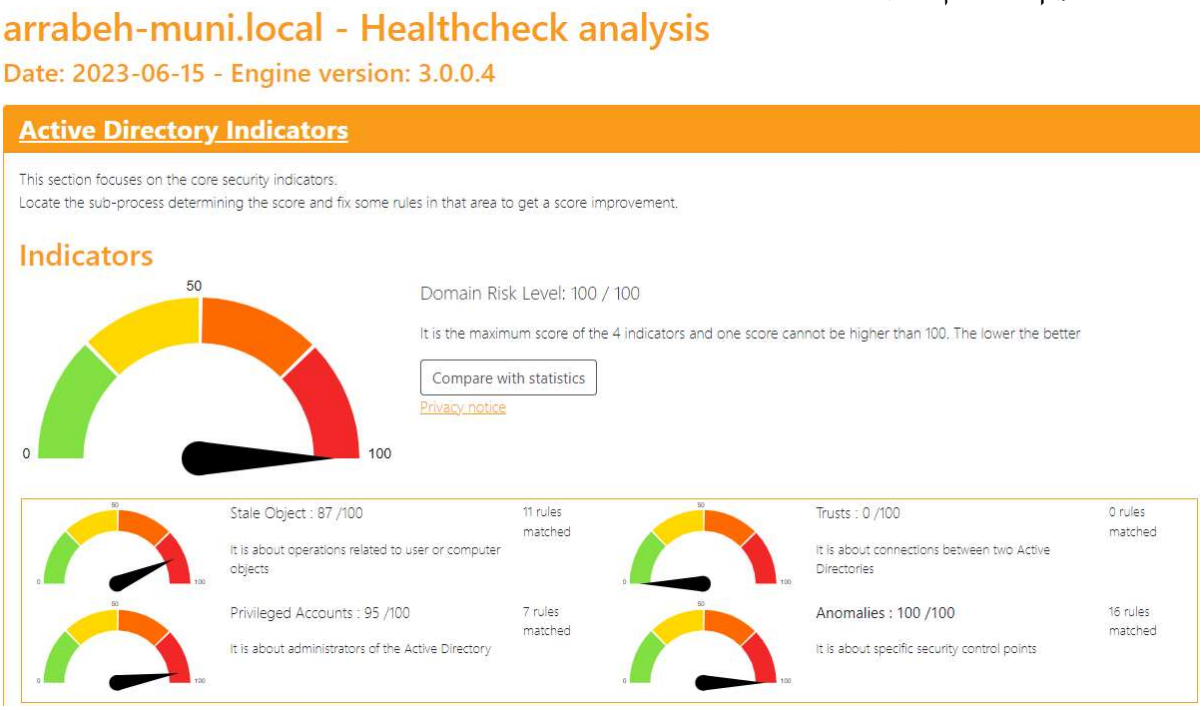


6. בדיקת הקשחת Active-Directory.

כחלק מהבדיקות הרצנו גם כלי PingCastle. ביצענו באמצעותו מספר בדיקות שונות:

1. AD Health Check - דוח הסוקר את הActive Directory ומעריך את רמת הסיכון שבה מצוי הDomain.

הדוח מחלק את הממצאים לארבע קטגוריות ונותן לכל ממצא ניקוד – ככל שהניקוד גבוה יותר הממצא מוערך כמסוכן יותר.



2. הדוח כולל בתוכו תיאור של כל ממצא, הסבר טכני, פתרון מומלץ ותיעוד.

Stale Objects

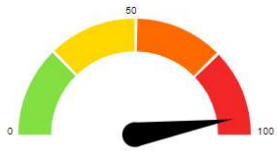
Stale Objects : 87 /100

It is about operations related to user or computer objects

Stale Objects rule details [11 rules matched on a total of 47]

Relatively high number of inactive computer accounts: 53% (more than 30% of all computers)	+ 30 Point(s)
The LAN Manager Authentication Level allows the use of NTLMv1 or LM.	+ 15 Point(s)
Non-admin users can add up to 10 computer(s) to a domain	+ 10 Point(s)
SMB v1 activated on 1 DC	+ 10 Point(s)
Relatively high number of inactive user accounts: 47% (more than 25% of all users)	+ 10 Point(s)
Presence of non-supported versions of Windows 10 or Windows 11 = 5	+ 5 Point(s)
The subnet declaration is incomplete [1 IP of DC not found in declared subnets]	+ 5 Point(s)
Number of accounts which have never expiring passwords: 33	+ 1 Point(s)
Presence of Windows 7 = 1	+ 1 Point(s)
Verify Kerberos Armoring is enabled on DCs and the domain functional level is at least Windows Server 2012	Informative rule
Verify Kerberos Armoring is enabled on clients and the domain functional level is at least Windows Server 2012	Informative rule

Privileged Accounts

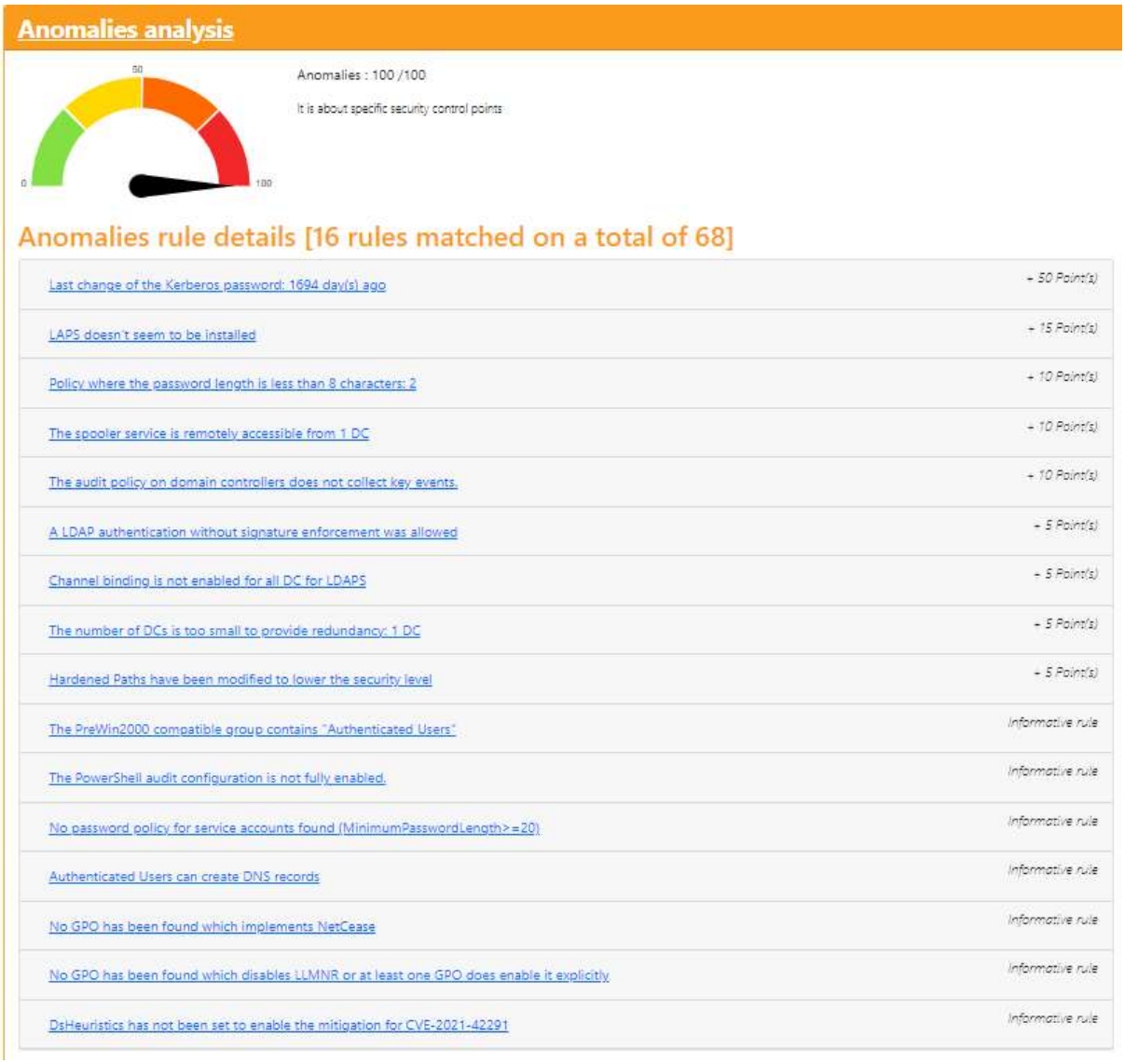


Privileged Accounts : 95 /100

It is about administrators of the Active Directory

Privileged Accounts rule details [7 rules matched on a total of 43]

The native administrator account has been used recently: 4 day(s) ago	+ 20 Point(s)
Presence of Admin accounts which do not have the flag "This account is sensitive and cannot be delegated": 5	+ 20 Point(s)
Presence of accounts with non-expiring passwords in the domain admin group (at least 2 accounts): 3	+ 15 Point(s)
Number of admins not in Protected Users: 5	+ 10 Point(s)
The Recycle Bin is not enabled	+ 10 Point(s)
Number of admin with a password older than 3 years: 3	+ 10 Point(s)
The group Schema Admins is not empty: 4 account(s)	+ 10 Point(s)



Anomalies analysis

Anomalies : 100 /100

It is about specific security control points

Anomalies rule details [16 rules matched on a total of 68]

Last change of the Kerberos password: 1694 day(s) ago	+ 50 Point(s)
LAPS doesn't seem to be installed	+ 15 Point(s)
Policy where the password length is less than 8 characters: 2	+ 10 Point(s)
The spooler service is remotely accessible from 1 DC	+ 10 Point(s)
The audit policy on domain controllers does not collect key events.	+ 10 Point(s)
A LDAP authentication without signature enforcement was allowed	+ 5 Point(s)
Channel binding is not enabled for all DC for LDAPS	+ 5 Point(s)
The number of DCs is too small to provide redundancy: 1 DC	+ 5 Point(s)
Hardened Paths have been modified to lower the security level	+ 5 Point(s)
The PreWin2000 compatible group contains "Authenticated Users"	Informative rule
The PowerShell audit configuration is not fully enabled.	Informative rule
No password policy for service accounts found (MinimumPasswordLength>=20)	Informative rule
Authenticated Users can create DNS records	Informative rule
No GPO has been found which implements NetCease	Informative rule
No GPO has been found which disables LLMNR or at least one GPO does enable it explicitly	Informative rule
DsHeuristics has not been set to enable the mitigation for CVE-2021-42291	Informative rule

3. בדיקת תיקיות שיתופיות – רשימה של התיקיות השיתופיות וחלוקתן לפי Is Everyone Allowed, כאשר הכוונה תיקיות עם הרשאות מאחת מ-4 הקבוצות הבאות:

- Everyone
- Users
- Domain Users
- Authenticated Users

יש לעבור על כל התיקיות השיתופיות ולוודא שהן נחוצות בכלל. מומלץ לבצע סקירה מלאה ומסודרת על ההרשאות שלהן ובפרט יש לוודא שאין מידע רגיש בתיקיות שיתופיות הפתוחות לכלל משתמשי הדומיין – מצורפת טבלת אקסל המפרטת את כלל השיתופים בהרשאות EVERYONE לנספחים של הדוח הטכנולוגי.

IsCurrentUserAllowed	IsEveryoneAllowed	Share	Computer
TRUE	TRUE	ADMIN$	JihanPC.arrabeh-muni.local
TRUE	TRUE	C$	JihanPC.arrabeh-muni.local
TRUE	TRUE	print$	JihanPC.arrabeh-muni.local
TRUE	TRUE	scan	JihanPC.arrabeh-muni.local
TRUE	TRUE	ADMIN$	arsrv-main.arrabeh-muni.local
TRUE	TRUE	C$	arsrv-main.arrabeh-muni.local
TRUE	TRUE	D$	arsrv-main.arrabeh-muni.local
TRUE	TRUE	Data	arsrv-main.arrabeh-muni.local
TRUE	TRUE	ESET	arsrv-main.arrabeh-muni.local
TRUE	TRUE	FileServer	arsrv-main.arrabeh-muni.local
TRUE	TRUE	FolderRedirect$	arsrv-main.arrabeh-muni.local
TRUE	TRUE	NETLOGON	arsrv-main.arrabeh-muni.local
TRUE	TRUE	S$	arsrv-main.arrabeh-muni.local
TRUE	TRUE	SYSVOL	arsrv-main.arrabeh-muni.local
TRUE	TRUE	VBRCatalog	arsrv-main.arrabeh-muni.local
TRUE	TRUE	scan	Lenovo-PC.arrabeh-muni.local
TRUE	TRUE	Users	Lenovo-PC.arrabeh-muni.local
TRUE	TRUE	print$	DESKTOP-Muhanad.arrabeh-muni.local
TRUE	TRUE	SCAN	DESKTOP-Muhanad.arrabeh-muni.local
TRUE	TRUE	Users	DESKTOP-OSHPLAK.arrabeh-muni.local
TRUE	TRUE	print$	DESKTOP-4UHCOVV.arrabeh-muni.local
TRUE	TRUE	scan	DESKTOP-4UHCOVV.arrabeh-muni.local
TRUE	TRUE	print$	AMENE.arrabeh-muni.local
TRUE	TRUE	print$	rawyahPC.arrabeh-muni.local

TRUE	TRUE	scan	rawyahPC.arrabeh-muni.local
TRUE	TRUE	print$	fidaaPC.arrabeh-muni.local
TRUE	TRUE	scan	fidaaPC.arrabeh-muni.local
TRUE	TRUE	Education	arsrv-ts.arrabeh-muni.local
TRUE	TRUE	FD	arsrv-ts.arrabeh-muni.local
TRUE	TRUE	HR	arsrv-ts.arrabeh-muni.local
TRUE	TRUE	print$	arsrv-ts.arrabeh-muni.local
TRUE	TRUE	scan	DESKTOP-S9C45BH.arrabeh-muni.local
TRUE	TRUE	print$	elham-kh.arrabeh-muni.local
TRUE	TRUE	print$	shada-y.arrabeh-muni.local
TRUE	TRUE	scan	shada-y.arrabeh-muni.local
TRUE	TRUE	scan	Legal-Jawad.arrabeh-muni.local
TRUE	TRUE	share folder	Legal-Jawad.arrabeh-muni.local
TRUE	TRUE	print$	Social-Maram.arrabeh-muni.local
TRUE	TRUE	print$	DESKTOP-JT4PEBI.arrabeh-muni.local
TRUE	TRUE	print$	muhammad-nass.arrabeh-muni.local

7. בדיקת חומת אש

כחלק מהסקר ומבדיקות העמדה שבוצעו, עולים הממצאים הבאים על אי קיימות של מודולי אבטחה בחומת האש:

מודולי אבטחה

מודולים לבדיקה	האם המודול קיים?	פרופיל	פערים והמלצות
Anti-Virus	לא קיים		Virus outbreak prevention + External Connectors לא קיים
Application Control	לא קיים		מומלץ להקשיח על פי ההמלצות המצורפות
IPS	לא קיים		מומלץ לוודא כי קיים פרופיל כזה והוא מוגדר על פי ההמלצות המצורפות
Web Filter	לא קיים		פרופיל לא מוקשח מבחינת קטגוריות מומלץ להקשיח את הפרופיל על פי ההמלצות המצורפות
DNS Filter	לא קיים		מומלץ להגדיר פרופיל עם הטמעה של External Connectors
File Filter	לא קיים		מומלץ להגדיר פרופיל על פי ההמלצות המצורפות
SSL inspection	לא קיים		לא קיים שימוש ב-Deep Inspection, מומלץ להפיץ תעודה על כל המחשבים בארגון
SandBox	לא קיים		מומלץ להטמיע ולהפעיל את השימוש בפיצ'רים שלו בכל פרופילי האבטחה הרלוונטים

להלן המלצות להגדרת פרופילי אבטחה מוקשחים:
המלצות למודולי אבטחה
על כל חוק המאפשר יציאה החוצה למשתמשים נדרשת הפעלה של כל פרופילי האבטחה שלהלן.

Web Filter

- מומלצת העברה של הפרופיל ל- Proxy-Based (יש לדאוג שגם החוק בחומת אש יהיה ב-Proxy Mode)
- קטגוריות לחסימה בפרופילי Web Filter לכלל המשתמשים:
כל הקטגוריות תחת Security Risk, Potentially Label, Adult/Mature Content
File Hosting Sites, Fake News Sites, Gaming Sites, E-commerce Sites, Social Networking Sites, Freeware and Software downloads, Peer to Peer File Sharing, Streaming Media and downloads, File Sharing and storage.

- נדרשת הפעלה של Block Invalid URL,
- מומלצת הפעלה של Block Malicious URL discovered by Forti Sandbox לאחר הטמעה של מוצר Sand Box

Application Control

- קטגוריות לחסימה בפרופילי Application Control לכלל המשתמשים:

Can Exclude WhatsApp Massages only **not WhatsApp File sharing**, Facebook etc. for a relevant user.

IPS

- מומלץ להגדיר את כל החתימות מדרגה 3 ומעלה ב-Block, כמו כן, לחסום Botnet C&C.

Anti-Virus

הגדרת פרופיל אנטי וירוס לכלל המשתמשים:

SSL/SSH Inspection

יש להגדיר פרופיל של Full SSL Inspection (Deep-Inspection) על כל החוקים המאפשרים למשתמשים יציאה החוצה.

מומלץ להתסכל בהדרכה של Fortigate כיצד להגדיר פרופיל כזה, מדובר בתעודה שצריך להפיץ לכלל המשתמשים.

8. סקר אבטחה פיזית

כחלק מסקר האבטחה בוצע סיור אבטחה פיזית בבניין העירייה.

<u>להלן ממצאי הסיור שעלו וההמלצות:</u>

1. חדר השרתים נמצא בממ"ד אשר נמצא בו בנוסף חדר ישיבות וציוד שאינו שייך למחשוב.

<u>המלצה:</u>

- מומלץ להגדיר חדר שרתים ייעודי לצורך בקרה של גישה לגורמים מורשים בלבד.
- מומלץ לשקול הטמעה של מנגנון בקרת גישה לחדר השרתים המאפשר כניסה למורשים בלבד ומבצע רישום לוג של הנכנס הכולל שעה תאריך וכד'.

2. לא קיימת רצפה צפה בחדר השרתים ולא קיימים חיישני הצפה- היות ומדובר בחדר תת קרקעי הסיכון הוא גבוה במקרה של הצפות סביבתיות.

<u>המלצה:</u>

- מומלץ לבחון התקנה של רצפה צפה כולל חיישני הצפה וכולל מנגנון שאיבת נוזלים לניקוז במקרה של הצפות.
- לכל הפחות ועד ליישום מנגנון שכזה מומלץ כי כלל רכיבי התקשורת יותקנו בגובה של לפחות 80 ס״מ מגובה הרצפה ע״ג ארונות התקשורת.

3. לא קיימת מערכת לכיבוי אש ולא מערכת לגילוי והתראה מפני חשש לשריפה.

<u>המלצה:</u>

- מומלץ להתקין מערכת כיבוי אש הכוללת איתור וכיבוי ע״י מטפי גז לכיבוי שריפות, וזאת על-מנת למזער נזקים במקרה של הפעלת המערכת כיבוי ולמנוע קצרים ברכיבים אלקטרוניים וחשמליים.

4. חדר השרתים לא מנוטר ע״י מצלמות אבטחה.

<u>המלצה:</u>

- מומלץ כי חדר השרתים ינוטר ע״י מצלמות אבטחה ייעודיות אשר ממוקמות מחוץ לחדר השרתים ומצלמה נוספת אשר ממוקמת בתוך חדר השרתים.

5. לא קיימת אזעקה.

<u>המלצה:</u>

- מומלץ להתקין אזעקה בחדר שרתים לצורך זיהוי ניסיונות גישה של גורמים לא מורשים.

6. לא קיימים גלאי נפח.

<u>המלצה:</u>

- מומלץ לבצע התקנה של גלאי נפח בחדר השרתים.

7. לא קיים מד טמפרטורה ומד לחות.

8. <u>המלצה:</u>

- מומלץ לבצע התקנה של מדי טמפרטורה ולחות.

9. לא קיימת בקרת גישה, יומן מבקרים ורישום לוגים.

<u>המלצה:</u>

- מומלץ לבחון הטמעה של מערכות לבקרת גישה, יומן מבקרים ומערכת רישום לוגים לחדר שרתים ייעודי.

10. בעקבות זאת שהשרתים אינם ממוקמים בחדר שרתים ייעודי, לא קיימות מערכות מיזוג אוויר אשר אמורות לספק תנאי טמפרטורה מתאימים לשרתים.

<u>המלצה:</u>

- מומלץ להתקין חיישני טמפרטורה וחיישני לחות המסונכרנים עם מערכת המיזוג.

11. לא קיים גנרטור חירום לגיבוי במידה והספק ה-UPS אוזל במקרה של הפסקות חשמל ממושכות.

<u>המלצה:</u>

- מומלץ לבדוק נושא גנרטור חירום והיכולת לשלב את חדר השרתים לקבל מתח בסנכרון עם מערכת ה-UPS עת הפסקת חשמל.

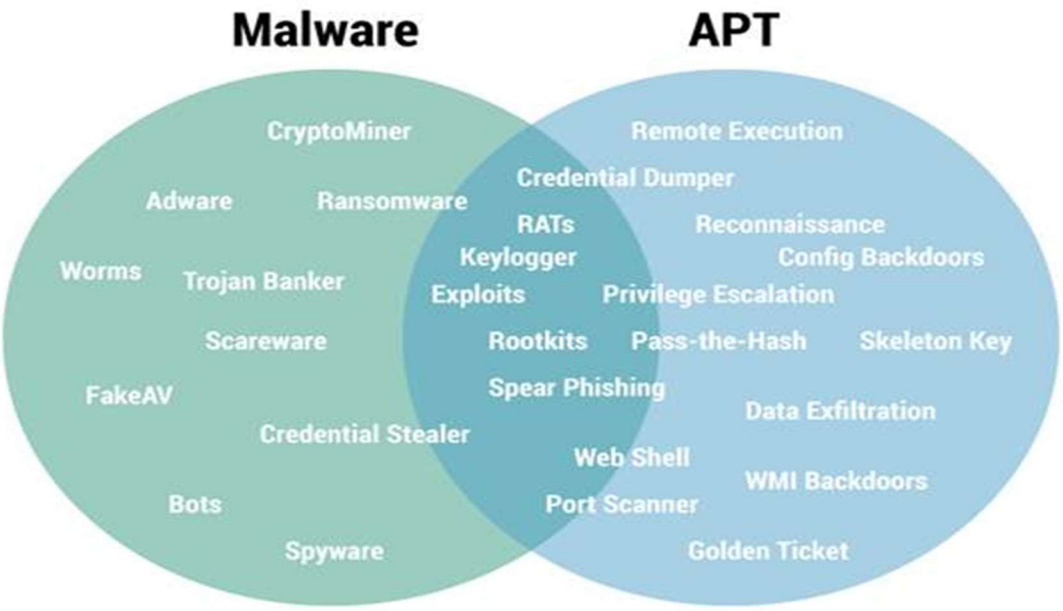
12. קיימת מערכת UPS

הבדיקה	חדר שרתים ראשי
מיקום	עיריית עראבה
אזעקה	לא קיים
רצפה צפה	לא קיים
בקרת גישה	לא קיים
מצלמות אבטחה	לא קיים
מערכת UPS	קיימת מערכת UPS
גנרטור חרום	לא קיים גנרטור חירום
מערכת כיבוי אש	לא קיימת מערכת כיבוי אש
רישום לוגים	לא מתבצע רישום לוגים - ממוקם בממ"ד אשר מכיל בתוכו חדר ישיבה וציוד שלא שייך למחשוב
גלאי עשן	לא קיים
גלאי נפח	לא קיים
מד טמפרטורה	לא קיים
מד לחות	לא קיים
גלאי הצפה	לא קיים
ציוד מחשוב בלבד	לא קיים
ביקורת בדיקת מטפים	לא קיים
ביקורת בדיקת הארקות	לא קיים
יומן מבקרים	אין יומן מבקרים בחדר שרתים
מיזוג אוויר	לא קיים
מיזוג אוויר גיבוי	לא קיים
נעילת דלת וסוג הדלת	אין מנעול לחדר שרתים - מדובר בחדר ממ"ד של העירייה

9. בדיקת מוצר הגנה להתראות וחסימות

כחלק מסקר הסיכונים שבוצע, זיהינו כי קיים מוצר הגנה מסוג ESET ללא רישוי על חלק מהתחנות , מוצר הגנה מסוג McAffee ללא רישוי ומוצר בסיסי של Windows Defender.
הבדיקות התבצעו עם משתמש רגיל לחלוטין. הבדיקות התבצעו לפי מיפוי של MITRE - https://attack.mitre.org/
הבדיקות התבצעו על עמדה עם מוצר הגנה מסוג McAffee ללא רישוי. חשוב לציין שבמהלך המבדק התשתיתי , בוצע מגוון רחב של מתקפות רשת ופעולות אשר לא התקבלה עליהם אף התראה או חסימה.

- בוצע ניסיון לבצע מתקפת LSASS DUMP אשר הצליח ולא התקבלה התראה או חסימה על הפעולה.
- בוצע ניסיון יצירת קשר לשרת שלנו ויצירת ערוץ תקשורת אשר הצליח ולא התקבלה התראה או חסימה. הצלחנו לייצר Reverse Shell.
- בוצע ניסיון להריץ מתקפת Password Spray בעזרת קובץ PowerShell והפעולה הצליחה. התוצאות זהות לתוצאות המבדק חדירה תשתיתי.
- בוצע ניסיון להריץ מתקפת Password Spray מקובץ VBS אשר הצליחה ונמצאו משתמשים אשר צוינו בדו"ח מבדק חדירה תשתיתי.
- בוצע ניסיון להריץ סימולטור של KnowBe4 של Ransim והתקבלה התראה רק על 11 הדמיות מתוך 23. 11 פעולות לא נחסמו המדמות פעולות של Mover Ransomware, Collaborator Ransomware, InsideCryptor Ransomware וכדומה.
- בוצע ניסיון להריץ בדיקת CheckMe של CheckPoint והבדיקה לא הצליחה בעקבות מחסור בהתקנה של.NET Framework 3.5.
- בוצע ניסיון לבצע הצפנה של מספר קבצי TEST אשר הועתקו לעמדה ללא התראה או חסימה של מוצר ההגנה. מומלץ לבחון שמודול Anti-Ransomware פעיל. חשוב לציין שהפעולה יכולה להצליח על כל סוגי הקבצים ולא הוגדרו קבצים רגישים ולא קיימת תיקיית root המונעת מתקפות מסוג Ransomware.
- בוצע ניסיון להפעיל מתקפת Responder אשר הצליח על Windows בעזרת קובץ ההרצה Responder.exe. לא התקבלה התראה על הפעולה ולא חסימה של הקובץ.
- בוצע ניסיון פתיחת PowerShell מ WMIC ויצירה של עץ תהליכים Process Tree ללא התראה או חסימה של מוצר ההגנה.
- בוצע ניסיון לטעון Mimikatz לזיכרון אשר לא הצליח עקב זיהוי של קובץ הבדיקות.
- בוצע ניסיון להריץ קובץ אקסל עם Macro אשר מריץ מספר פעולות ולא התקבלה התראה או חסימה על הפעולה.
- בוצע הרצת סריקת פורטים פתוחים על העמדה בעזרת כלי בשם NMAP אשר הצליחה ולא התקבלה התראה או חסימה על TCP Port Scanning.
- מומלץ לציין שלא קיימת סיסמא של הסרה למוצר ההגנה הקיים על העמדה שנבדקה.
- בוצע הרצה של ATP Simulator – סקריפט מסוג batch file שמבצע מספר רב של בדיקות לפי MITRE ולפי קטגוריות של Malware, APT אשר מפורטות בתמונה הבאה:



Blocked/Not Blocked	Test Case
Failed	Collect Local Files
Failed	C2 Connects
Failed	DNS Cache 1 (Cache Injection)
Failed	Malicious User Agents (Malware, RATs)
Failed	Ncat Back Connect (Drop & Exec)
Failed	WMI Backdoor C2
Failed	LSASS Dump (with Procdump)
Failed	Mimikatz 1 (Drop & Exec)
Failed	WCE 1 (Eventlog entries)
Blocked	Active Guest Account Admin
Failed	Fake System File (Drop & Exec)
Blocked	Hosts File (AV/Win Update blocks)
Blocked	Obfuscated JS Dropper
Failed	Obfuscation (RAR with JPG ext)
Failed	Nbtscan Discovery (Scan & Output)
Failed	Recon Activity (Typical Commands)
Failed	PsExec (Drop & Exec)
Blocked	Remote Execution Tool (Drop)
Failed	At Job
Blocked	RUN Key Entry Creation
Failed	Scheduled Task Creation
Blocked	StickyKey Backdoor
Failed	UserInitMprLogonScript Persistence
Failed	Web Shells
Failed	WMI Backdoor

<u>המלצות:</u>

- מומלץ להעביר ליצרן את הממצאים שעלו במהלך הבדיקות
- מומלץ לבחון שכל התחנות עם התקנה של מוצר הגנה מתקדם מסוג EDR/XDR/MDR וברישוי.
- מומלץ לבחון רכישת שירותי SOC מנוהלים אשר יוכלו לזהות פעולות חריגות ולהתריע בפני צוות המחשוב.

<u>המלצה להקשחת סיסמאות:</u>

אנו ממליצים להקשיח את פוליסת הסיסמאות של הארגון בכל המערכות הרלוונטיות הקיימות בארגון עם לכל הפחות הפרמטרים הבאים:

- אורך - על סיסמאות להכיל מינימום של כ-9 תווים עבור משתמשים רגילים ו-15+ תווים למשתמשים בעלי הרשאות גבוהות / החברים בקבוצות רגישות כמו Admins Domain, גיבויים וכד'.
- חיוב שימוש באותיות גדולות (A-Z)
- חיוב שימוש באותיות קטנות (a-z)
- חיוב שימוש במספרים (0-9)
- חיוב שימוש בסימנים מיוחדים (לדוגמא: !@#$%^&*)(><?", וכד')
- חיוב הגדרת ללא רצפים (לדוגמא: ללא 1234,1234567,98765 כחלק מהסיסמה).
- איסור על שימוש בשם המשתמש חלק מהסיסמא.
- הגדרת מספר ניסיונות התחברות כושלים לכל היותר - 5 ניסיונות.
- הגדרת זמן נעילה לאחר מספר ניסיונות כושלים, לכל הפחות חצי שעה ובנוסף הגדרת התראה לצוות המחשוב על מספר ניסיונות התחברות כושלים ונעילת המשתמש כאשר ההמלצה הינה נעילה קבועה עד שחרור ידני של צוות המחשוב.
- הגדרת החלפת סיסמה כל מספר חודשים - מומלץ על לכל היותר 3 חודשים.
- הגבלת שימוש בסיסמאות שנעשה בהן שימוש לאחרונה, לכל הפחות חמישה סיסמאות אחורה.
- הסרה של הגדרת "Password Never Expired" מכלל המשתמשים בארגון.
    - המלצות למערכות אקסטרה לניהול פוליסת סיסמאות: https://www.netwrix.com/password_policy_enforcer.html
    - המלצות למערכות אקסטרה לניהול פוליסת סיסמאות: https://www.manageengine.com/mobile/self-service-password/

<u>המלצות לחסימה של Powershell:</u>

חסימה של "PowerShell" ו-"Windows PowerShell ISE" על ידי שמות, נתיבים ו-Hashים שונים של גרסאות שונות ו-GPO.
הגדרת חסימה גם על ידי מוצר ה-אנטי וירוס ו/או EDR/XDR במידה והאפשרות קיימת.

חסימת קובץ הרצת ה-PowerShell לא מספיקה מהסיבה כי ה-PowerShell משולב במערכת ההפעלה במספר דרכים וקיימים טכניקות מעקף אשר מאפשרות להריץ את הפאוור-של ללא קובץ ההרצה המקורי של המערכת.
מהסיבה הזאת אנו ממליצים לבצע הקשחות נוספות בארגון:

הגבלת שטח התקיפה ב-PowerShell על ידי אכיפת והפעלת מודל "Constrained Language Mode".

https://devblogs.microsoft.com/powershell/powershell-constrained-language-mode

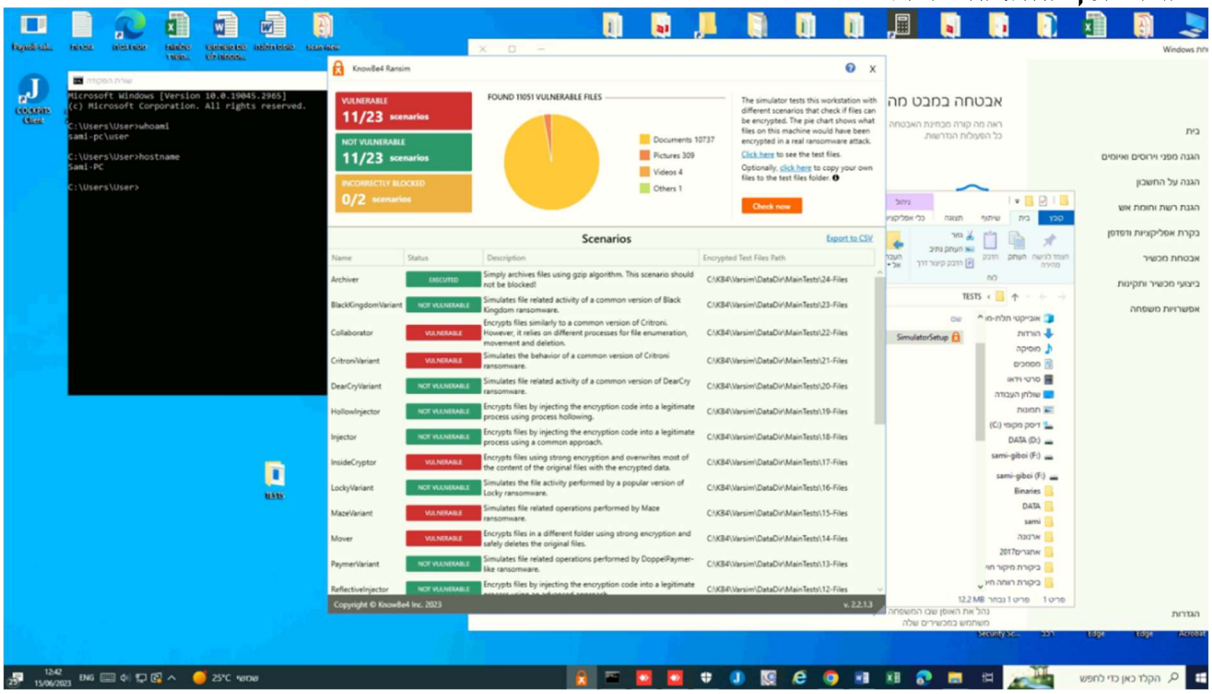
הטמעה ושימוש במערכת מסוג Application Control בתצורת Whitelist לצורך הגדרת whitelist לקבצי בינאריים וסקריפטים אשר מאופשרים להרצה.
מנגנון לזה לרוב מגיע כחלק ממוצרי האבטחה Anti-Virus או מוצר ה-EDR/XDR, ניתן לבדוק אם היצרן / ספק.
קיים פתרון חינמי חלקי של מייקרוסופט בשם AppLocker אך הוא לא תומך בכול מערכות ההפעלה ומאפשר גם חסימה של סקריפטים - https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview

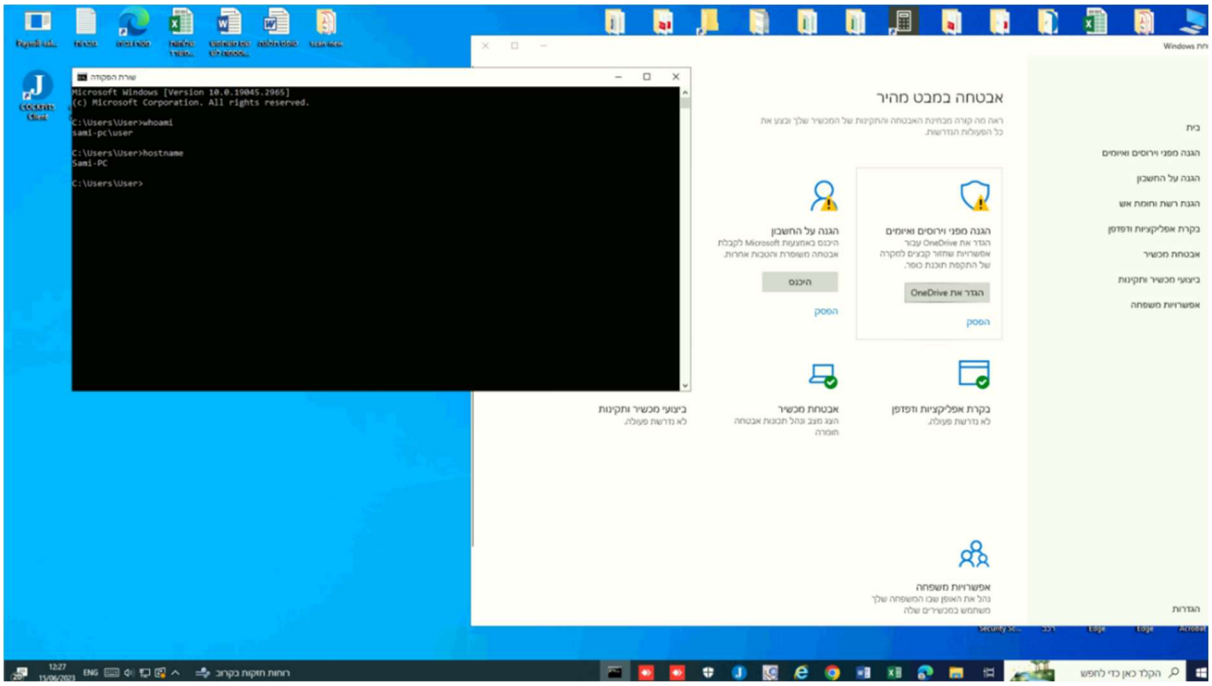
חסימת הרצת סקריפטים של PowerShell ושפות תכנות בכללי על ידי משתמשים רגילים בארגון. מספר דוגמאות לקבצי סקריפטים ושפות תוכנות נפוצות: "vbs", "bat", "ps1", "sh", "c", "cpp", "js", "py", "go", "php", "psc1", "ps1xml", "psd1", "psm1", "pyc", "pyo", "rdp".

במידה והארגון משתמש בסקריפטים פנימיים ארגוניים של PowerShell, ניתן לחתום את הקבצים על ידי Code Signing Certificate חוקית ולאפשר הרצה רק של אותם סקריפטים ספציפיים.
במידה ויש לכם על המחשב "private certificate", תוכנות זדוניות עלולות לבצע חתימה על סקריפטים בשימך ויאפשר ל-PowerShell להריץ אותם. בכדי למנוע זאת, ניתן להשתמש ב" Certificate Manager

Certmgr.exe" בכדי לייצא את תעודת החתימה לקובץ .pfx עם אפשרות "Enable Strong Protection" ובחירת סיסמה מוקשחת.
שמירת לוגים ב-PowerShell על ידי הפעלת "Turn on Module Logging" דרך ה-Group Policy בנתיב הבא: Computer Configuration\Policies\Administrative Template\Windows Components\Windows PowerShell ולהגדיר "*" ב-Module List. בנוסף, להפעיל " Turn on PowerShell Script Block logging".
חשוב מאוד לשתף את צוות ה-SIEM SOC בתהליך בכדי שיוכלו להגדיר לקיחת לוגים אילו והתרעות רלוונטיות.
חסימת הנתיבים C:\Windows\System32\ftp.exe , wmic.exe , wscript.exe , cscript.exe במידה ואין בהם שימוש.
למאמר מלא בנושא אשר ההמלצות מבוססות עליו: https://adsecurity.org/?p=2604
חסימת אפשרות הרצה ל- CMD למשתמשים רגילים. את החסימה מומלץ לבצע על ידי שמות, נתיבים ו-Hashים שונים של גרסאות שונות ו-GPO.
חסימה של הרצת סקריפטים cscript.exe במידה ואין שימוש אתו.
חסימה של הרצת סקריפטים wscript.exe במידה ואין שימוש אתו.
חסימה של ftp.exe במידה ואין שימוש אתו.

צילומי מסך להדגמה בלבד:





מתודולוגית הבדיקה

1. לצורכי תיעוד המצב הקיים, בוצע סקר האבטחה תוך לימוד מערך המחשוב הקיים ואופן תפעולו על בסיס ביצוע תשאול ובדיקת גורמים ותהליכים תפעוליים רלוונטיים שונים. כמו כן נבדקו רכיבים ואמצעים טכנולוגיים שונים הקשורים למערכות המידע ולהם רלוונטיות לנושאי הסקר השונים.
2. התשאול והתיעוד בוצעו באופן שאיפשר למידה והבנה של כלל התהליכים הניהוליים והתפעוליים הקיימים ומיושמים הלכה למעשה בכל הקשור לאבטחת מערכות המידע בארגון.
3. בחינת הנושאים הטכנולוגיים בוצעה באופן שאיפשר לנו להכיר את מעגלי ההגנה במערך ויישומם הלכה למעשה, דרך השימוש באמצעי אבטחה לוגיים ופיזיים וכן תצורת הקשחת רכיבי המערך הטכנולוגי.
4. בדיקות חוסן המדמות פורץ פוטנציאלי למערכות המידע, לצורך בחינת איכות יישום הפרמטרים ואמצעי האבטחה הלוגית של הרכיבים הטכנולוגיים השונים.

להלן פירוט הקריטריונים על פיהם נבחן המערך על סמך מתודולוגיות אינטגרטי יעוץ וניהול סיכונים בע"מ:

ג : דוח מבדק חדירה פנימי נספח

תאריך: 19/06/2023

תוכן עניינים

תוכן

- **סודיות הלקוח**
מסמך זה מכיל מידע סודי של הלקוח ואין להעתיקו ללא אישור בכתב.

- **מידע קנייני**
תוכן מסמך זה נחשב למידע קנייני ואין לחשוף אותו מחוץ לרשת של הארגון המקבל.
Corporate Integrity נותן הרשאה להעתיק דוח זה לצורך הפצת מידע בארגון שלך או בכל סוכנות רגולטורית.

- **מגבלות והגבלות**
עקב מגבלת הזמן אשר הוקצתה לבדיקה, הבדיקה עלולה שלא לשקף את מצב האבטחה האמיתי של המערכת.

  - הדוח לא משקף תוקף זדוני ללא הגבלת זמן או משאבים.
  - המבדקים שבוצעו היו מסוג תשתיתי בלבד.

דיסקליימר

דוח זה מכיל מידע סודי ביותר המסופק על ידי **אינטגריטי יעוץ וניהול סיכונים לעיריית עראבה** ומיועד לשימוש פנימי של הלקוח בלבד. הלקוח הוא האחראי הבלעדי לכל הפצה נוספת של מסמך זה ולשמירה על גישה סודית אליו. בזמן הבדיקות נעשה שימוש בגישה כבולה לביצוע בדיקת חדירה בהיקף מוגבל, חברת אינטגריטי יעוץ וניהול סיכונים אינה מתחייבת שכל חולשות האבטחה אפשריות בנכסי החברה התגלו.
בדיקות האבטחה והתוצאות חלות רק על המקרים של בדיקות אלו. כל פגיעות עתידיות אפשריות אינן מובאות בחשבון ואין כל סוג של תכנון לטפל בפגיעויות אלו מכיוון שהערכת אבטחה מהדוח יכולה להיות ישימה רק למועד הבדיקות, איננו ממליצים להעריך את רמת הסיכון העתידית ואת מצב האבטחה על סמך דוח זה. דוח זה אינו משקף תוקף ללא הגבלת זמן.
במהלך הבדיקות ייתכן ונוצרו בצורה ידנית או אוטומטית קבצים, לוגים וסקריפטים. ייתכן והרבה מהקבצים הוסרו אבל ייתכן גם כי הקבצים עדיין נוכחים במערכות שונות מהסיבה כי הסרתם לא עבדה מסיבה זאת או אחרת. הקליינט צריך הלקוח צריך להסיר את הקבצים השיוריים הללו .

מטרת המבדק

- הערכת הסיכונים הפוטנציאליים, חשיפת כשלים וליקויים הקיימים באופן יישום מערך האבטחה התומך בשירותים שונים, חשיפת ליקויים באופן היישום של אמצעי טכנולוגיה ותהליכים תפעוליים החושפים את מערכות המידע לפגיעה או לדלף מידע.
- מתן פתרונות הנדרשים לצמצום או ביטול האפשרות למימוש החשיפה לפגיעה במערך הטכנולוגי.
- קבלת תמונת מצב עדכנית ואמיתית המשקפת את נושא אבטחת המידע בארגון באופן שיאפשר לו לבצע הפעילויות הבאות:
  - לזהות כשלים בכל הקשור לנושאי מדיניות, ארגון, ניהול, תפעול וטכנולוגיה במערך המחשוב.
  - לבצע הערכת הסיכונים ולהגדיר את רמת חומרתם.
  - ליישם המלצות לשיפור המצב הקיים.

תכולת המבדק

- המבדק הפנימי בוצע בשיטת Black Box פנימי – התקבל גישה למחשב נייד / נייח מחוץ לדומיין עם הרשאות אדמין לוקאלי המחובר לרשת הארגונית. חשוב לציין כי המחשב לא מחובר לדומיין החברה וכי לא קיימת מערכת NAC אשר היה צורך באכיפה.

סיכום הערכה

בהתבסס על מבדקי החדירה הפנימים ותוצאות סקירת האקטיב דירקטורי היינו מגדירים את רמת הסיכון של הרשת הפנימית כ-**קריטית**. תוקף זדוני אשר הצליח להגיע לרשת הפנימית, יכול בצורה פשוטה ומהירה להשיג גישה לקבצים ארגוניים רגישים ועוד עקב פוליסת סיסמאות חלשה אשר מאפשרת למשתמשי הדומיין לבחור סיסמאות קלות לניחוש ופריצה. בנוסף, להלן מספר בעיות קריטיות בארגון:

- לא קיימת מערכת הגנה אשר מונעת מתוקף זדוני להתחבר לרשת החברה.
- קיימת בעיה בסגמנטציה פנימית ומיקרו סגמנטציה.
- משתמשי דומיין בארגון בעלי הרשאות אדמין לוקאלי.
- פוליסת סיסמאות חלשה ומשתמשים בסכנה ממשית לפריצה. סיסמאות בסיסיות עם רצפים קלים לניחוש.
- קיימות של פרוטוקולים אשר אינם נתמכים יותר ומהווים חולשות אבטחה קריטיות בארגון.
- לא מופעל פ׳יצר חשוב (smbsign) להגנה על תעבורת SMB.
- ניתן לצאת לאינטרנט ולהוריד קבצים משרתים פנימיים.
- קיימות של ממשקי התחברות עם סיסמאות ברירת מחדל ושמירה של סיסמאות בצורה לא מאובטחת.
- ניהול הרשאות לקוי בתיקיות רשת והרשאות NTFS.
- תעבורת רשת IPv6 מאופשרת המאפשרת לבצע מגוון מתקפות רשת שונות.
- חוסר בניטור והתראות על מתקפות רשת.

לבסוף, במהלך המבדק הצליחו הבודקי חדירות להגיע להשתלטות מלאה על הדומיין על ידי השגה של משתמש דומיין אדמין.

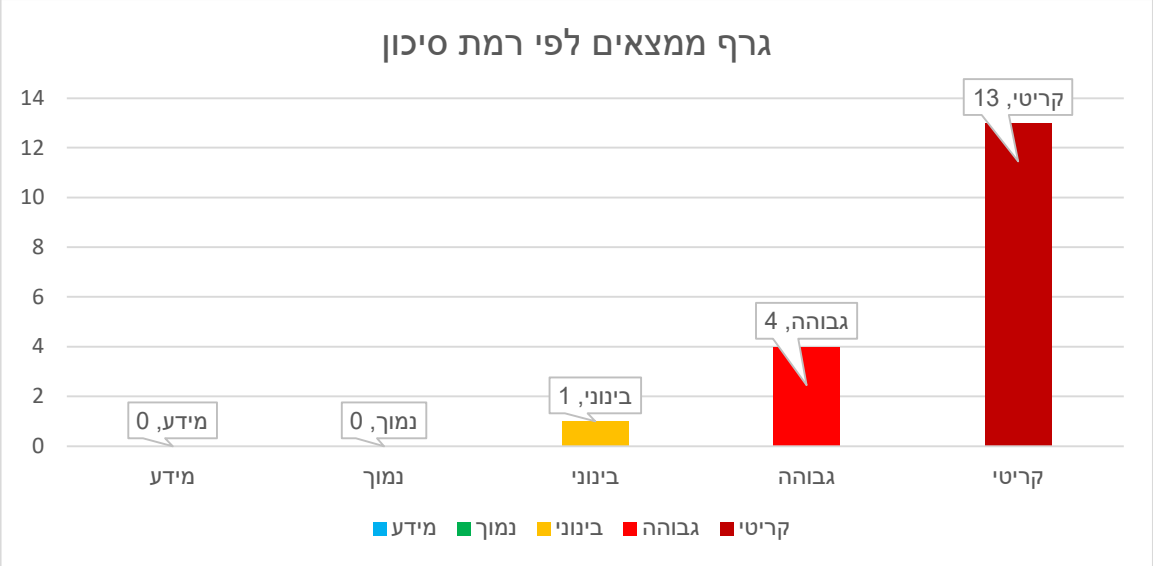
כמו כן, על פי דוח סקירת האקטיב דירקטורי, רמת הסיכון הינה המקסימאלית ביותר, 100 מתוך 100.

חלק ניכר מהחולשות שנמצאו וצוינו בדוח, עשויות להוות גורם לפרצות אבטחה במערכת. ניתן לתקן פגיעות אלה על ידי ביצוע שיטות העבודה המומלצות, וההמלצות שניתנו במהלך הדוח. יש לשים לב כי חולשות שהוגדרו בדוח ברמת סיכון קריטית, יש לטפל בדחיפות.

הטבלה הבאה מייצגת את בדיקות החדירה של פריטי היקף ומפרקת את הנושאים שזוהו וסווגו לפי חומרת הסיכון. (שימו לב כי טבלת סיכום זו אינה כוללת את פריטי המידע):

מספר	תיאור	נמוך	בינוני	גבוהה	קריטי	סה״כ
1	מבדק חדירה פנימי	0	1	4	10	15
2	סקירת אקטיב דירקטורי	0	0	0	3	3
3	סה״כ	0	1	4	13	18

התרשימים שלהלן מייצגים סיכום של מספר החולשות שנמצא עד להוצאת הדו״ח הנוכחי:



ניקוי הארגון לאחר המבדק

ניקוי הארגון לאחר המבדק

יש להסיר או להשבית, לפי הצורך, את כל חשבונות הבדיקה אשר נוצרו עבור בדיקה זו יחד עם כל תוכן משויך (כולל מחיקת תיקיות Home Folder שנוצרו לאחר חיבור המשתמש שנוצר) ופירמוט המחשב שממנו הבודקים בדקו את הארגון.

כמו כן, יש להסיר את כל המשתמשים אשר נוצרו במהלך הבדיקה (כולל משתמשי חיבור מרוחק שיצרתם כדי שנתחבר) ומחיקת הרשאתם, ניתן לראות רשימה מסודרת למטה למשתמשים שאנו יצרנו במהלך הבדיקה.

בנוסף, במידה ונוספו כתובות IP כלשהם לרשימות Whitelist למיניהם או חוקי חומת אש לצורך המבדק, חשוב לזכור למחוק אותם.
כמו כן, נמליץ על החלפת סיסמאות לכלל הארגון, עם יישום ההמלצות של מהפוליסה החדשה שהמלצנו.
משתמשי האדמין הלוקאלי בשם integrity שיצרנו נמחקו וגם משתמש דומיין אדמין שנוצר נמחק בשם "inthacked" מהכתובת 10.161.41.238

פירוט כללי

דירוג סיכונים
הטבלה שלהלן מפרטת את שמות הסיכונים והצבעים המשמשים בכל הדוח בכדי לספק מערכת ניקוד סיכונים ברורה ותמציתית.
יש לציין כי כימות הסיכון העסקי הכולל הנשקף מכל אחת מהנושאים שנמצאו בבדיקה כלשהי, אינה בתחום שלנו. משמעות הדבר היא כי סיכונים מסוימים עשויים להיות מדווחים גבוהים מנקודת מבט טכנית, אך כתוצאה מבקרות אחרות שאינן ידועות לנו, הם יכולים להיחשב מקובלים על ידי הארגון.

#	דירוג סיכון	CVSSv3 Score	תיאור
1	קריטי	9.0 - 10	פגיעות ברמת סיכון קריטית. ממצא זה דורש פתרון במהירות האפשרית.
2	גבוהה	7.0 – 8.9	פגיעות ברמת סיכון גבוהה. ממצא זה דורש פתרון בטווח הקצר.
3	בינוני	4.0 – 6.9	פגיעות ברמת סיכון בינונית. ממצא זה דורש פתרון לאחר טיפול בממצאים הקריטיים והגבוהים.
4	נמוך	1.0 – 3.9	פגיעות ברמת סיכון נמוכה. יש לטפל בכך כחלק ממשימות התחזוקה השוטפות.
5	לידיעה ולבדיקה	0 – 0.9	ממצא החושף מידע. יש לוודא כי ממצאים אלו אינם חושפים מידע רגיש.

סקירת ממצאים
כל הנושאים שזוהו במהלך ההערכה מפורטים להלן עם תיאור קצר ודירוג סיכון לכל נושא. דירוגי הסיכון המשמשים בדוח זה מוגדרים בסעיף דירוגי סיכון.

#	סעיף	רמת סיכון	תיאור
מבדק חדירה פנימי			
1	1.1	קריטית	חוסר בניטור והתראות על מתקפות רשת
2	1.2	קריטית	סגמנטציה רשתית וסגמנטציה בין רכיבים
3	1.3	קריטית	פרוטוקול SMBV1 ו - SMB SIGN
4	1.4	קריטית	קיימות של מערכות הפעלה לא נתמכות
5	1.5	קריטית	LLMNR, MSDNS & NTB-NS POISONING
6	1.6	קריטית	אנומרציה של משתמשים ומתקפת PASSWORD SPRAY מחוץ לדומיין
7	1.7	קריטית	מתקפת PTH והוספת משתמש דומיין אדמין
8	1.8	קריטית	הוצאת סיסמאות קריאות ומעורבלות מזיכרון
9	1.9	קריטית	יציאה לאינטרנט בשרתים פנימיים
10	1.10	קריטית	הורדה והעלאה של קבצים
11	1.11	גבוהה	שמירת סיסמאות בצורה לא מאובטחת

12	1.12	גבוהה	ממשקי ניהול וסיסמאות ברירת מחדל
13	1.13	גבוהה	ניהול הרשאות לקוי בתיקיות רשת והרשאות NTFS
14	1.14	גבוהה	מתקפת רשת MITM6
15	1.15	בינוני	מערכת NETWORK ACCESS CONTROL
סקירת אקטיב דירקטורי			
1	2.1	קריטית	Privileged Accounts
2	2.2	קריטית	Stale Objects
3	2.3	קריטית	Anomalies
4	2.4	לא קיים	Trusts

פרטי מחשב נייד / נייח פיזי שהתקבל מהארגון:

- שם מחשב (hostname) של התחנה שהתקבלה – Computer\Jenia
- כתובת IP של התחנה שהתקבלה – 10.161.40.159

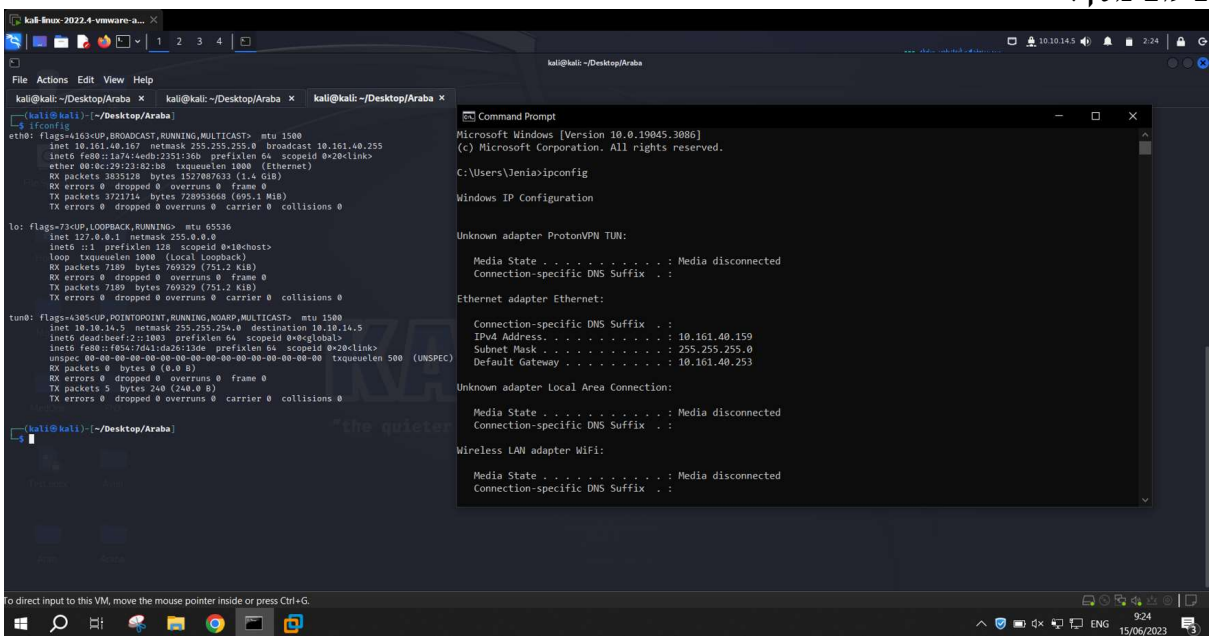
פרטי המערכת הווירטואלית שממנה בוצע המבדק:

- שם מחשב (hostname) של המערכת הווירטואלית (Kali) – kali
- כתובת IP של המערכת הווירטואלית (Kali) – 10.161.40.167

תיעוד זמני מתקפות מדגמי:

1. מתקפת Responder בשעה 09:42 בתאריך 15/06/2023 ולאורך כל המבדק
2. מתקפת Password Spray על כתובת ה-IP בשעה 09:47 בתאריך 15/06/2023 ולאורך כל המבדק
3. מתקפת Mitm6 על כל הרשת בשעה 10:21 בתאריך 15/06/2023
4. הוצאת סיסמאות קריאות ומעורבלות מהזיכרון בשעה 12:03-04 בתאריך 15/06/2023
5. מתקפת PTH והוספת משתמש דומיין אדמין בתאריך 15/06/2023 בשעה 11:09

צילום מסך:



1. מבדק חדירה פנימי

1.1. חוסר בניטור והתראות על מתקפות רשת

רמת סיכון: קריטי

ממצא: במהלך המבדק בוצעו מגוון רב של מתקפות שונות, ביניהן מתקפות רשת ומתקפות על תחנות קצה. יש לציין כי לא קיבלנו שום אינדיקציה על כך שחלק מהמתקפות זוהו או נחסמו על ידי שום גורם בארגון ולא על ידי מוצרי הגנה כאלה ואחרים.

המלצה:

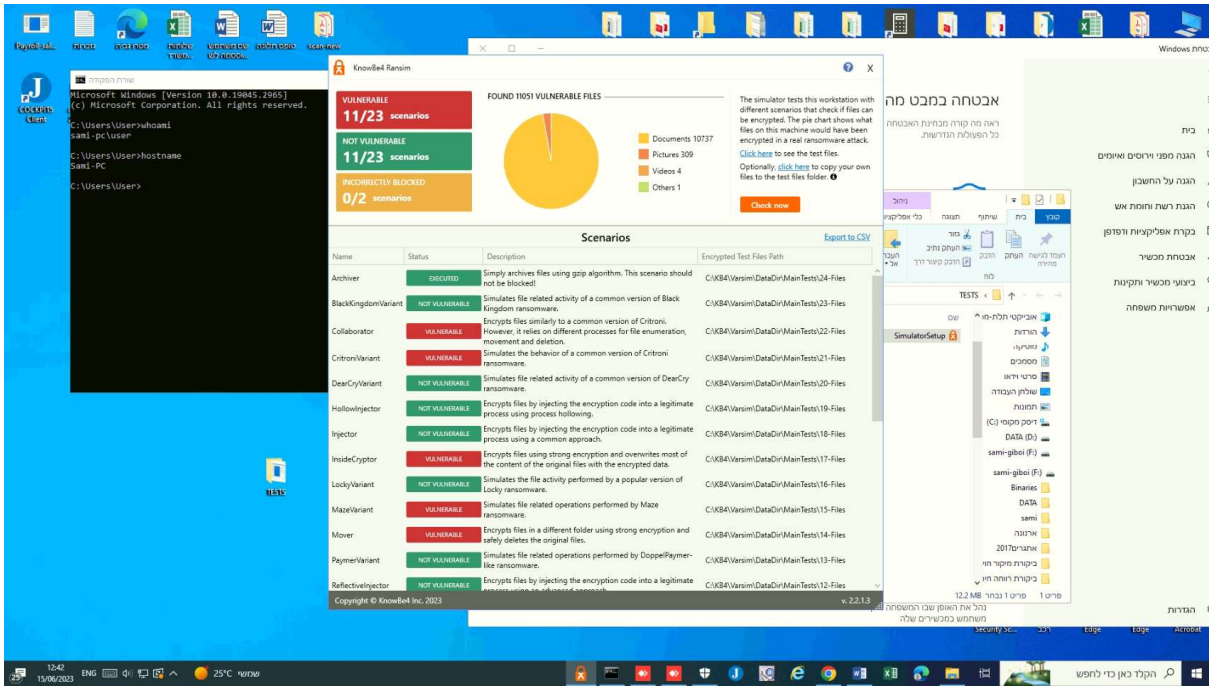
1.1.1. לבחון הטמעה של מוצר הגנה מתקדם מסוג XDR/EDR אשר יכול לזהות פעולות חריגות של משתמשים גם על תחנות הקצה וגם ברמת הרשת.

1.1.2. לבחון רכישת שירותי SOC מנוהלים אשר יוכלו לזהות פעולות חריגות ולהתריע בפני צוות המחשוב.

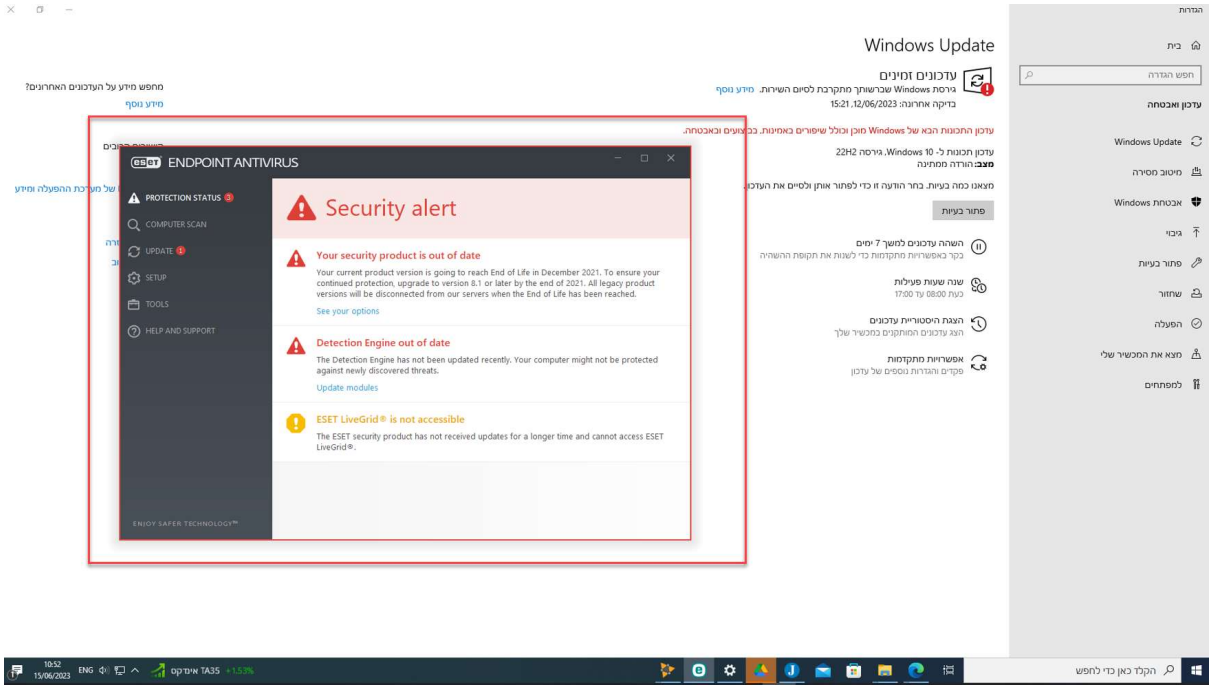
כתובות פגיעות: כלל הרשתות.

תמונות:

- בתמונה ניתן לראות דוגמה להרצה של כלי בדיקה לבדיקת Ransomware המדמה פעולה של כופרות מוכרות שונות , ללא התראה או חסימה של מוצרי ההגנה הקיימים וללא ניטור של הפעולות



- בתמונה ניתן לראות תחנה עם מוצר הגנה לא עדכני וללא רישוי ותחנה אשר לא התבצע בה עדכון אבטחה המון זמן


Windows Update
עדכונים זמינים
מידע נוסף
בדיקה אחרונה: 15:21 ,12/06/2023
עדכון התכונות הבא של Windows מוכן וכולל שיפורים באמינות, בביצועים ובאבטחה.
עדכון תכונות ל- Windows 10, גירסה 22H2
מצב: הורדה ממתינה
מצאנו כמה בעיות. בחר הודעה זו כדי לפתור אותן ולסיים את העדכו
פתור בעיות
השהה עדכונים למשך 7 ימים
שנה שעות פעילות
הצגת היסטוריית עדכונים
אפשרויות מתקדמות
מחפש מידע על העדכונים האחרונים?
מידע נוסף
הגדרות
בית
חפש הגדרה
עדכון ואבטחה
Windows Update
מיטוב מסירה
אבטחת Windows
גיבוי
פתור בעיות
שחזור
הפעלה
מצא את המכשיר שלי
למפתחים
ENDPOINT ANTIVIRUS
PROTECTION STATUS
COMPUTER SCAN
UPDATE
SETUP
TOOLS
HELP AND SUPPORT
ENJOY SAFER TECHNOLOGY™
Security alert
Your security product is out of date
Your current product version is going to reach End of Life in December 2021. To ensure your continued protection, upgrade to version 8.1 or later by the end of 2021. All legacy product versions will be disconnected from our servers when the End of Life has been reached.
See your options
Detection Engine out of date
The Detection Engine has not been updated recently. Your computer might not be protected against newly discovered threats.
Update modules
ESET LiveGrid® is not accessible
The ESET security product has not received updates for a longer time and cannot access ESET LiveGrid®.
הקלד כאן כדי לחפש

1.2. סגמנטציה רשתית וסגמנטציה בין רכיבים

רמת סיכון: קריטי

ממצא: במהלך המבדק הרגשנו כי קיימת סגמנטציה רשתית אשר מהפרידה בין הרשתות השונות הארגוניות עם בעיות. זה מתבטא בכך שהצלחנו בתור תוקפים לנוע בצורה חופשית במרבית הרשת הארגונית.

התחלנו בתוך רשת משתמשים והצלחנו לתקשר בצורה חופשית עם רשתות אחרות, לדוגמה רשת שרתים דבר אשר אפשר לנו לתקוף שרתים ולבסוף גם להשתלט על מרביתם.

כמו כן, שמנו לב כי לא קיימת בארגון מיקרו סגמנטציה (סגמנטציה בין רכיבים), זה מתבטא בכך שהצלחנו לפרוץ למחשבים או שרתים באותה השרת ולנוע בצורה חופשית בניהם.

המלצה:

1.2.1. ניהול סגמנטציה רשתית פנימית לצורך מידור ואכיפה. ניתן לבצע זאת על ידי מערכות אבטחה מתקדמות עם הגבלת חוקים מסודרים למקור ויעד, פרוטוקולים, שירותים, כתובות IP, מודלי אבטחה ועוד בין רשתות שונות.

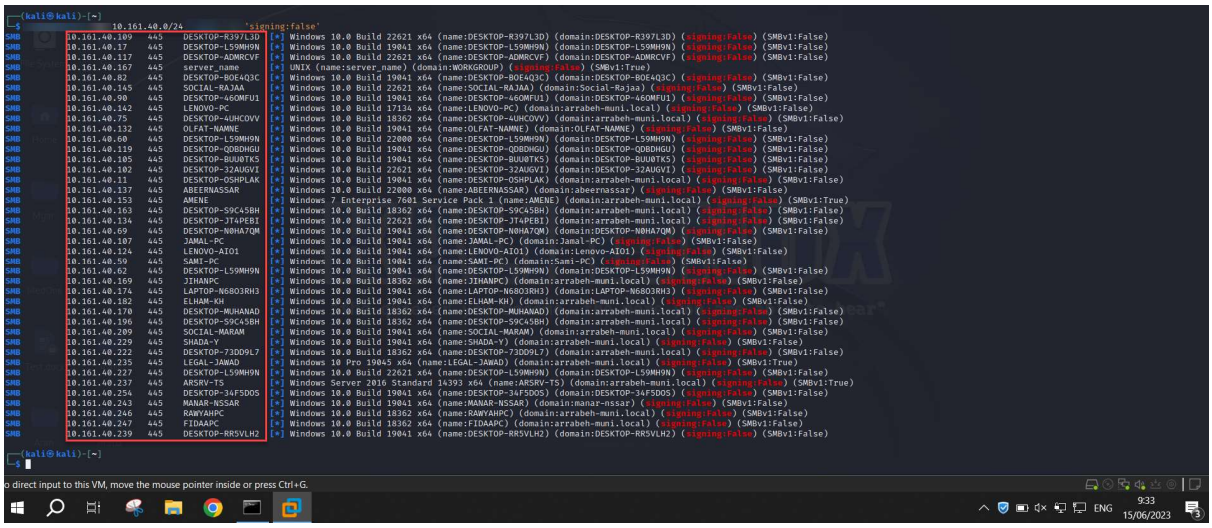
1.2.2. ניהול מיקרו סגמנטציה (סגמנטציה בין רכיבים) באותה הרשת לצורך מידור ואכיפה. ניתן לבצע זאת על ידי ניהול חומת אש מובנת במערכות ההפעלה / מוצרי אבטחה עם מודלים של חומת אש לוקאלית אשר מאפשרות הגבלת חוקים מסודרים למקור ויעד, פרוטוקולים, שירותים, כתובות IP, מודלי אבטחה ועוד בין רשתות שונות.

1.2.2.1. את ניהול המיקרו סגמנטציה יש לשים לב כי מאוד חשוב גם להטמיע במערכות וירטואליות אשר יושבות לדוגמה על אותו ESXI.

כתובות פגיעות: כלל הרשתות.

תמונות:

- בתמונה ניתן לראות כי הצלחנו לגשת לתחנות משתמשים ולשרתים



1.3. פרוטוקול SMBv1 ו-SMB Sign

רמת סיכון: קריטי

ממצא: פרוטוקול SMB הינו פרוטוקול אשר מספק גישה משותפת אל קבצים, מדפסות, יציאות טוריות ותקשורת בין המחשבים ברשת. לפרוטוקול קיימות מספר גרסאות כגון:

SMBv2ו-SMBv3 כאשר SMBv1 הינה גרסה ישנה ובעלת מספר רב של חולשות אבטחה שונות.

- חשוב לזכור כי אם בארגון קיימים מערכות הפעלה מסוג Windows 2000, 2003, XP, CE או מדפסות ישנות אשר משתמשות בשירות scan2shares וכד', השבתת הפרוטוקול יכולה למנוע מהשירותים אשר משתמשים בפרוטוקול זה מלעבוד.

במהלך המבדק זיהנו כי שירות ה-SMBv1 פעיל בשרתים ותחנות קצה.

בנוסף, ראינו כי לא קיימת אכיפה מלאה כנגד הפעלה וחיוב של SMB Sign - פיצ'ר זה הינו מנגנון אבטחה קריטי לפרוטוקול SMB. חבילת המידע עוברת Hash ובמידה וה-Hash של חבילת המידע שונה, הם יודעים כי החבילה עברה שינוי כלשהו.

המלצה:

1.3.1. ביטול של פרוטוקול SMB איכן שניתן.
1.3.1.1. איכן שלא ניתן לבטל את הפרוטוקול, אנו נמליץ על הקשחה בחומת האש הלוקאלית על ידי הגדרת חוקה מוסדרת. לדוגמה:

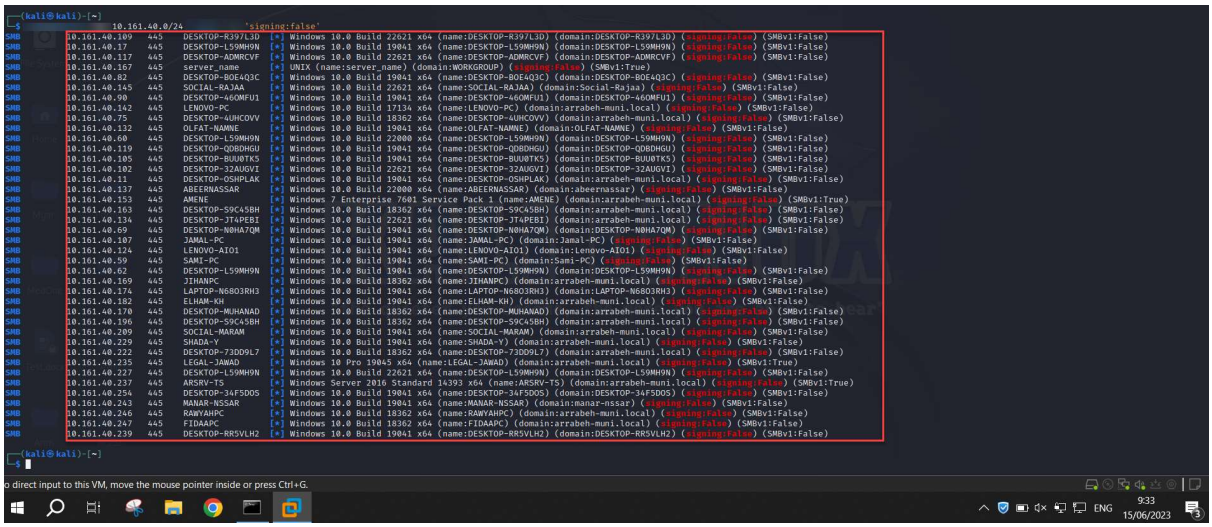
- הגדרת חוקים מסודרים לאן ניתן לצאת ולמי מותר להיכנס ולאן ע"י בשימוש בפרוטוקול.
- אפשר יציאה בלבד ב-SMB לכתובות מסוימות וחסימה גורפת לכניסה ב-SMB.

1.3.2. סקירה מקיפה על כלל המחשבים והשרתים בארגון וביטול פרוטוקול SMBv1 בכלל השרתים והערכות בארגון.
1.3.3. הפעלת "SMB Signing" – אנו נמליץ על הפעלת אפשרות זאת בכלל התחנות ושרתים בארגון על ידי הפצת Group Policy מסודר אשר מפעיל זאת בכלל המחשבים והשרתים בארגון.
1.3.3.1. למערכות הפעלה של Windows – להפעיל " Microsoft network server: Digitally sign communications" כ-"always"
1.3.4. למערכות הפעלה של Unix/Linux ההגדרה ב-Samba נקראת "Server Signing".

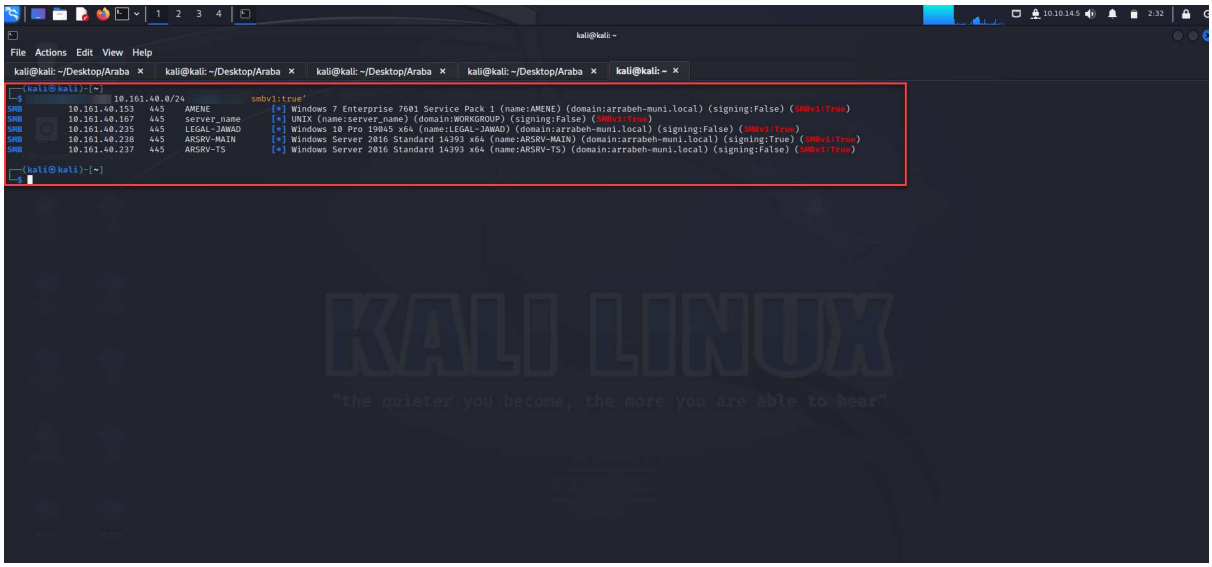
- יש לשים לב כי אפשרות זאת עלולה לגרום לאיטיות ברשת הפנימית בארגון, יש להעירך בהתאם ולבדוק זאת בסביבה מבוקרת בהתחלה.

תמונות:

- בתמונה ניתן לראות כי פיצ'ר SMB Signing אינו פעיל ו SMBV1 פעיל



- בתמונה ניתן לראות כי פיצ'ר SMB Signing אינו פעיל ו SMBV1 פעיל



1.4. קיימות של מערכות הפעלה לא נתמכות

רמת סיכון: קריטי

ממצא: במהלך המבדק נתקלנו במספר מערכות הפעלה לא נתמכות. קיימות של מערכת הפעלה לא נתמכת מסכנת מאוד את הארגון היות ובין היתר אינם מקבלים עדכוני אבטחה ועדכונים כלליים בצורה שוטפת ולכן עלולים להכיל חולשות אבטחה שונות לא ידועות לפומבי או חולשות אבטחה ידועות אשר לא קיבלו עדכון אבטחה ולכן הימצאותם בארגון מסכנת את הארגון באופן קריטי.

בין מערכות ההפעלה הלא נתמכות שזוהו בארגון ניתן לראות:

- Windows 7

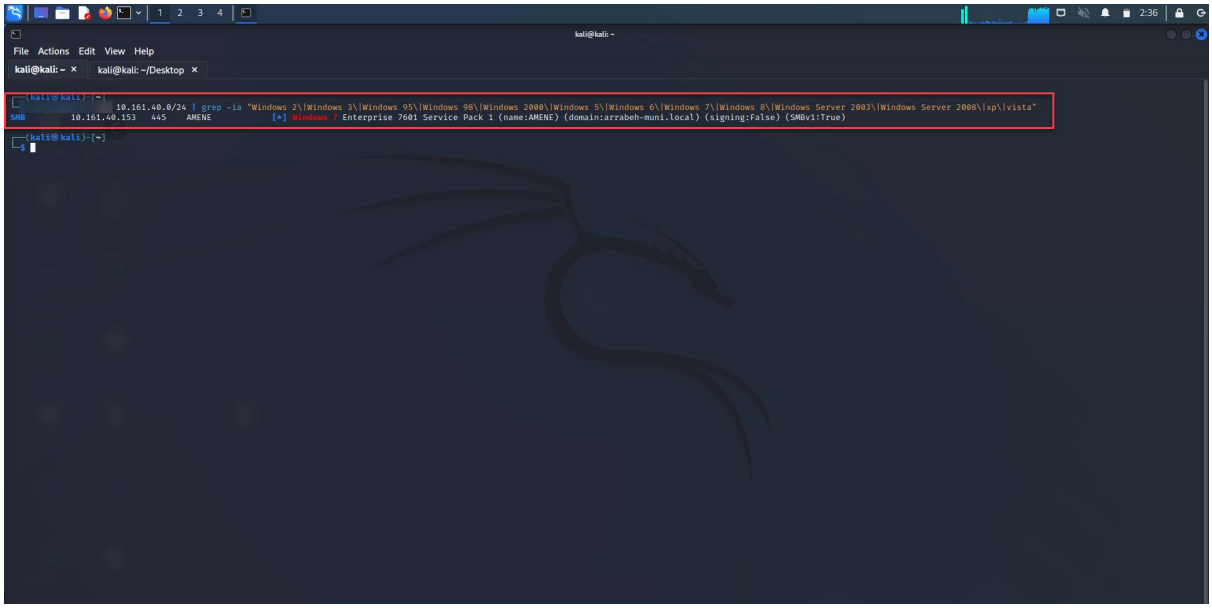
המלצה:

1.4.1. ביצוע סקירה מקיפה על כלל הארגון למיפוי מלא של מערכות הפעלה קיימות ולאחר מכן שדרוג מערכות ההפעלה אשר לא נתמכות יותר לגרסה נתמכת ומעודכנת ביותר בצורה שוטפת.

כתובות פגיעות: יש לבצע מיפוי מלא בארגון לכלל המערכות ההפעלה הקיימות לצורך מציאת כלל מערכות ההפעלה הלא נתמכות הקיימות.

תמונות:

- בתמונה ניתן לראות דוגמה למערכות הפעלה לא נתמכות



1.5. LLMNR, mDNS & NBT-NS Poisoning

רמת סיכון: קריטי

ממצא: בעזרת טכניקת הרעלת שאילתות LLMNR, mDNS & NBT-NS ברשת הארגון הצלחנו לתפוס Hashים של משתמשי הדומיין הארגוני. בנוסף לכך בעזרת טכניקה אחרת של מתקפת NTLM Relay הצלחנו לתפוס עוד Hashים.

המלצות:

- לצורך צמצום החשיפה למתקפה מסוג LLMNR Poising, אנו נמליץ על ביצוע ההקשחות אשר מפורטות מטה. **חשוב לזכור** כי יש לבדוק את השפעת ההמלצות בסביבת מעבדה ניסיונית לפני הפצה מלאה לכלל הארגון לצורך בדיקה כי אינם משפיעים או מפריעים לפעילות השותפת . חשוב לזכור שבמידה וקיימים דומיינים נוספים או מספר GPO / שרתי DHCP - יש להגדיר בכולם את ההמלצות.

1.5.1. הגדרת GPO לביטול פרוטוקול – NTLMv1 פרוטוקול זה אינו נתמך יותר ואינו מאובטח היות והוא חשוף למספר מתקפות שונות כגון Relay לעצמו ומשתמש בהצפנה חלשה ופריצה.

1.5.1.1. Computer Configurations -> Policies -> Windows Settings -> Security Settings -> Local Policies -> Security Options and find the policy Network Security: LAN Manager authentication level.

1.5.2. הגדרת GPO לביטול פרוטוקול LLMNR – מטרת הפרוטוקול הינה לאפשר למשתמשים הנמצאים באותו Subnet לבצע תרגום שמות מבלי להשתמש בשרתי DNS. הפרוטוקול מחשב כ-"Legacy" ולא אמורה להיות בעיה להורידו במידה ויש שרת DNS מתפקד. היות והפרוטוקול בנוי בתצורת "Multicast", תוקף ברשת יכול להאזין לבקשות ה-LLMNR הנשלחות ברשת ולענות להם. ברגע שהוא עונה להם, המחשב הנתקף מעביר פרטי התחברות למחשב של התוקף. לכן, נמליץ על ביטול שימוש בפרוטוקול זה, במקביל לביטול פרוטוקול זה, חשוב גם להמשיך לבטל את

הפרוטוקול NetBIOS over TCP/IP. נבצע זאת על ידי הפעלת ערך אשר נמצא תחת ה- Group Policy הבא:

- Computer Configuration -> Administrative Templates -> Network -> DNS Client
  - הפעלת (enable) ל-"Turn Off Multicast Name Resolution" .
  - במידה ובארגון משתמשים בחומת אש לוקאלית, לדוגמה: חומת אש של וינדוס אשר מנוהל ב-GPO או מוצר אנטי וירוס שמנהל חוקים, ניתן ליצור ולהפיץ חוק אשר חוסם תקשורת מסוג "Outbound" בפורט UDP 5355.

1.5.3. הגדרת GPO לביטול פרוטוקול NetBIOS over TCP/IP – פרוטוקול זה קודם לפרוטוקול ה-LLMNR וחשוב מאוד לכבות אותו גם, היות שהעמדות / שרתים יעברו להשתמש בו לאחר ביטול ה-LLMNR. את הביטול נבצע על ידי שינוי ערך בכלל ה-DHCP Managers בארגון לעמדות / שרתים אשר מנוהלים דרך ה-DHCP. לעמדות / שרתים אשר מקבלים כתובת סטטית לבד (שלא דרך ה-DHCP) יש לבטל את הפרוטוקול ידנית דרך הגדרות כרטיסי השרת (יש לבצע על כל כרטיסי השרת).

- ביטול דרך ה-DHCP Manager – לאחר כניסה לניהול ה-DHCP יש לבחור את הדומיין ותחת "IPV4" יש ללחוץ לחיצה ימנית על "Scope Options" ובחירה ב-"Options Configure" ואז לגשת ללשונית ה-"Advanced". לאחר מכן, לבחור "Microsoft Windows 2000 Options" ב-" Vendor Class" ולסמן וי ב-" Microsoft Disable Netbios Option 001" ובערך למטה תחת "Long" להכניס את הערך "0x2".
  - **חשוב לשים לב** כי במידה ויש כמה שרתי DHCP, יש להגדיר זאת בכולם.
  - במידה ובארגון משתמשים בחומת אש לוקאלית, לדוגמה: חומת אש של וינדוס אשר מנוהל ב-GPO או מוצר אנטי וירוס שמנהל חוקים, ניתן ליצור ולהפיץ חוק אשר חוסם תקשורת מסוג "Outbound" בפורט UDP 137 ו-TCP 137.

- ביטול ידני דרך ה-Registry הלוקאלי לעמדות / שרתים אשר אינם מקבלים את הכתובת דרך שרת ה-DHCP. ברג'יסטרי הבא:
  - "HKLM: SYSTEM\CurrentControlSet\Services\NetBT\Parameters\Interfaces" יש לשנות את הערך של הפרמטר "NetbiosOpstions" ל-"2".
  - **שימו לב** שיש לבצע הגדרה זאת על כל כרטיס רשת בעמדה / שרת אשר קיימת תחת ה-"Interfaces".

- במידה ובארגון משתמשים בחומת אש לוקאלית, לדוגמה: חומת אש של וינדוס אשר מנוהל ב-GPO או מוצר אנטי וירוס שמנהל חוקים, ניתן ליצור ולהפיץ חוק אשר חוסם תקשורת מסוג "Outbound" בפורטים UDP137/139 .

1.5.4. הגדרת GPO להפעלת "SMB Signing" – פיצ'ר זה הינו מנגנון אבטחה קריטי לפרוטוקול SMB. חבילת המידע עוברת Hash ובמידה וה-Hash של חבילת המידע שונה, הם יודעים כי החבילה עברה שינוי כלשהו. לכן, אנו נמליץ על הפעלת מנגנון אבטחה זה בכלל התחנות ושרתים בארגון.

- למערכות הפעלה של Windows – להפעיל " Microsoft network server: Digitally sign communications" כ-"always" ולהפיץ בצורה מסודרת לכלל התחנות והשרתים בארגון דרך ה-GPO.
- למערכות הפעלה של Unix/Linux ההגדרה ב-Samba נקראת "Server Signing".

- יש לשים לב כי אפשרות זאת עלולה לגרום לאיטיות ברשת הפנימית בארגון, יש להעירך בהתאם ולבדוק זאת בסביבה מבוקרת בהתחלה.

1.5.5. הגדרת GPO לביטול WPAD – פרוטוקול זה אחראי להפצת הגדרות פרוקסי אוטומטית במערכות וינדוס. במידה ואתם משתמשים בו בארגון על ידי מערכת כלשהי, השבתתו עלולה לגרום לניתוק מהפרוקסי בתחנות. לכן, יש לבצע מראש הכנות בנושא.

את ביטול המנגנון יש לבצע זאת על ידי הפצת פוליסה ב-GPO הארגוני, בנתיב הבא:

"Computer Configuration > System Services > WinHTTP Web Proxy Auto-Discovery Service Properties" ולאחר מכן לבחור ב-"disabled"

- במידה ולא ניתן לבטל את השימוש בפרוטוקול, ניתן להקל על התקפת שירות ה-"WPAD על ידי הוספת ערך עבור "WPAD" ב-"DNZ Zone". ערך ה- DNS אינו צריך להצביע על שרת WPAD חוקי. כל עוד השאילתות נפתרו, ההתקפה תימנע – **יש לשים לב** כי במידה ויש כמה שרתי DHCP, יש להגדיר זאת בכולם.

1.5.6. אנו ממליצים לצוותי ה- SIEM SOC / NOC לנטר את הנושאים הבאים:

1. תנועה בפורטים 139 & 137, 5355 UDP.
2. שינויים לערך ה-"EnableMulticast" ברג'יסטרי - HKLM\Software\Policies\Microsoft\Windows NT\DNSClient
3. הגדרת ניטור לוגים ל-7045 & 4697 Windows Events ID במערכות הבקרה והניטור הארגוניות לזיהוי מתקפות Relay.

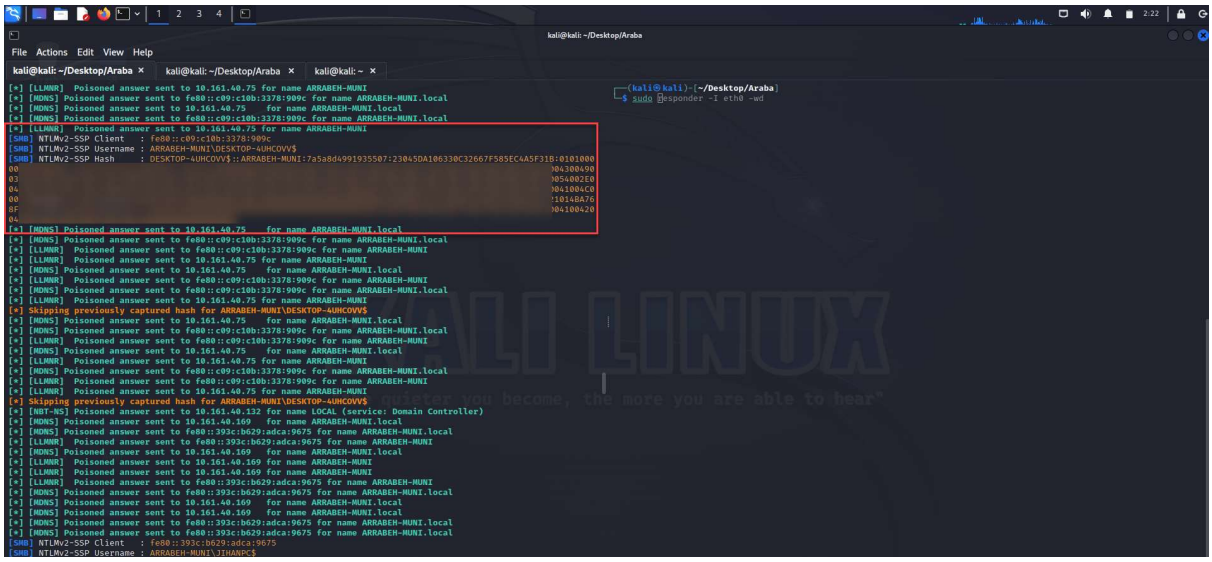
1.5.7. בדיקה מול ספקים / יצרנים של מערכות ההגנה בארגון מסוג Anti-Virus ו-EDR מדוע אינם חסמו את המתקפה.

1. **כתובות פגיעות:** כלל הארגון פגיע למתקפה, ככל שהיינו מריצים את המתקפה יותר זמן, היינו מוצאים יותר Hashים. דוגמה ל-HASHים שהצלחנו לתפוס במהלך המבדק התשתיתי:

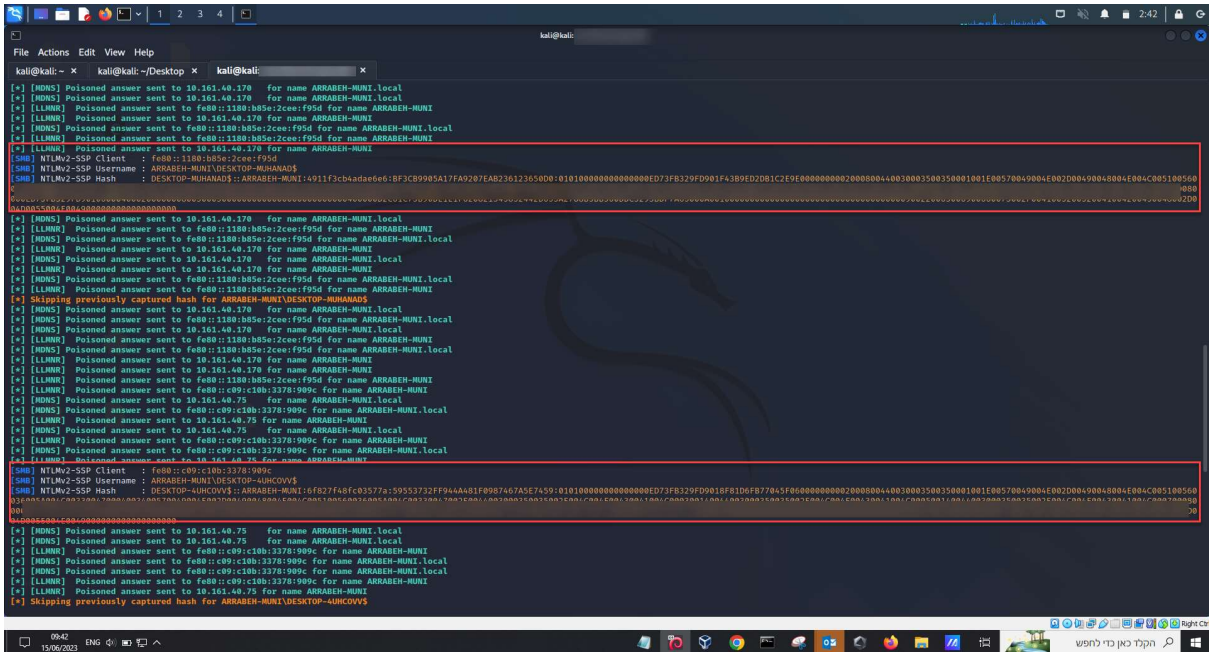
- SMB-NTLMv2-SSP-fe80::393c:b629:adca:9675.txt
- SMB-NTLMv2-SSP-10.161.40.170.txt Config-Responder.log
- SMB-NTLMv2-SSP-fe80::c09:c10b:3378:909c.txt
- SMB-NTLMv2-SSP-fe80::1180:b85e:2cee:f95d.txt

תמונות:

- בתמונה ניתן לראות דוגמה לתפיסה של Hashים שונים במהלך המתקפה

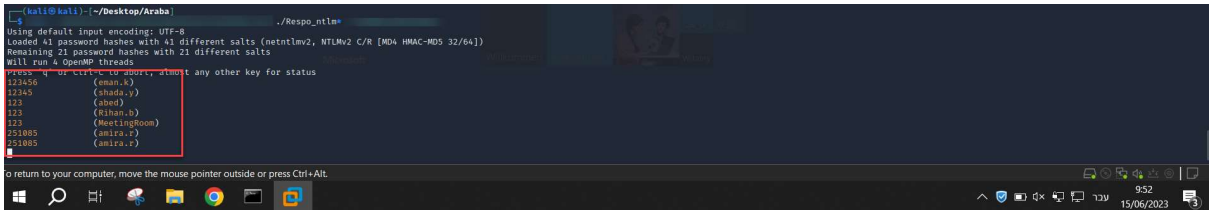


- בתמונה ניתן לראות דוגמה לתפיסה של Hashים שונים במהלך המתקפה



- בתמונה ניתן לראות דוגמה לפיצוח של ה – HASHים שהצלחנו לתפוס

- בתמונה ניתן לראות דוגמה לפיצוח של ה – HASHים שהצלחנו לתפוס



1.6. אנומרציה של משתמשים ומתקפת Password Spray מחוץ לדומיין

רמת סיכון: קריטי

ממצא: בוצע אנומרציה של משתמשי דומיין על ידי שליחה של אלפי בקשות TGT עם פרמטר "pre-authentication" לשרת ה-DC כאשר ומתקבלת שגיאה "Principal Unknown" אנו יודעים כי המשתמש לא קיים. במידה ושרת ה-KDC ממשיך לתהליך "pre-authentication" אנו יודעים שהמשתמש קיים. תהליך זה אינו נועל את המשתמשים אך במידה ומופעל, נוצר ווינדוס איוונט 4768.

על ידי שיטה זאת הצלחנו להוציא 6 שמות משתמשים בדומיין. לאחר שהצלחנו למצוא שמות משתמשים ארגוניים, המשכנו לבצע מתקפת Password Spray על כלל המשתמשים שנמצאו. חשוב לציין שלמקפת ה-Password Spray בחרנו סיסמאות חלשות אשר ידועות כבעיתיות וקיימות כמעט בכל קובץ מילון התקפי ומתוך ה-6 הצלחנו לפרוץ משתמשים , וביניהם משתמשים אשר היו משתמשי אדמין לוקאלי על תחנות הקצה.

פוליסת סיסמאות חלשה מאפשרת למשתמשי הארגון לבחור בסיסמאות קלות ולא מוקשחות אשר קלות לפיצוח או לניחוש ומסכנות את חשבון המשתמש לחדירה אינה מורשת לחשבונם. בעזרת הרשאות דומיין ניתן לצפות קבצים רגישים ופרטים של הארגון אשר עלולים לדלוף במידה ומדובר בתוקף זדוני.

המלצה:

1.6.1. אנו ממליצים להקשיח את פוליסת הסיסמאות של הארגון בכל המערכות הרלוונטיות הקיימות בארגון עם לכל הפחות הפרמטרים הבאים:

- אורך - על סיסמאות להכיל מינימום של כ-9 תווים עבור משתמשים רגילים ו-15+ תווים למשתמשים בעלי הרשאות גבוהות / החברים בקבוצות רגישות כמו Admins Domain, גיבויים וכד'.
- חיוב שימוש באותיות גדולות (A-Z)
- חיוב שימוש באותיות קטנות (a-z)
- חיוב שימוש במספרים (0-9)
- חיוב שימוש בסימנים מיוחדים (לדוגמא: !@#$%^&*)(><?", וכד')
- חיוב הגדרת ללא רצפים (לדוגמא: ללא 1234,1234567,98765 כחלק מהסיסמה).
- איסור על שימוש בשם המשתמש חלק מהסיסמא.
- הגדרת מספר ניסיונות התחברות כושלים לכל היותר - 5 ניסיונות.
- הגדרת זמן נעילה לאחר מספר ניסיונות כושלים, לכל הפחות חצי שעה ובנוסף הגדרת התראה לצוות המחשוב על מספר ניסיונות התחברות כושלים ונעילת המשתמש כאשר ההמלצה הינה נעילה קבועה עד שחרור ידני של צוות המחשוב.
- הגדרת החלפת סיסמה כל מספר חודשים - מומלץ על לכל היותר 3 חודשים.
- הגבלת שימוש בסיסמאות שנעשה בהן שימוש לאחרונה, לכל הפחות חמישה סיסמאות אחורה.

- **חלק מההמלצות לצורך הקשחת פוליסת סיסמאות מצריכות רכישה של מוצר ניהול פוליסת סיסמאות צד ג'. מוצרים לדוגמא:**
- **ADSelfService Plus**
  https://www.manageengine.com/mobile/self-service-password/
- **Netwrix**
  https://www.netwrix.com/password_policy_enforcer.html

1.6.2. הוספת חיוב סיסמה חד פעמית לחיבור (MFA) במערכות תומכות כחלק מתהליך החיבור גם בדומיין הארגוני וגם בכל מערכת תומכת לדוגמה 365, Azure, GSUIT מערכות VPN ועוד.

1.6.3. לבדוק מול היצרן / ספק מדוע מוצר ההגנה מסוג EDR אינו זיהה וחסם את המתקפה.

1.6.4. ביטול של פרוטוקול SMB היכן שניתן.
1.6.4.1. היכן שלא ניתן לבטל את הפרוטוקול, אנו נמליץ על הקשחה בחומת האש הלוקאלית על ידי הגדרת חוקה מוסדרת. לדוגמה:

- הגדרת חוקים מסודרים לאן ניתן לצאת ולמי מותר להיכנס ולאן ע"י שימוש בפרוטוקול.
- אפשור יציאה בלבד ב-SMB לכתובות מסוימות וחסימה גורפת לכניסה ב-SMB.

1.6.5. לוודא כי Kerberos Authentication Service תחת Account Login מופעל ב- Success & Failure וכי צוות ה-SIEM SOC יודע להתריע מפני Windows Event ID 4768 - איוונט זה נוצר כאשר מתבצע תהליך Kerberos Pre-Authentication וריבוי איוונטים יכול להצביע על User Enumeration וגם על Password Spray דרך Kerberos.

1.6.6. לוודא כי Audit Kerberos Authentication Service תחת Account Login מופעל ב- Success &Failure וכי צוות ה-SIEM SOC יודע להתריע מפני Windows Event ID 4771 - איוונט זה נוצר כאשר מתבצע תהליך Kerberos Pre-Authentication אך הוא נכשל וריבוי איוונטים יכול להצביע על Password Spray.

1.6.7. לוודא כי Audit Logon תחת Logon/Logoff מופעל ב-Success & Failure וכי צוות ה- SIEM SOC יודע להתריע מפני ריבוי Windows Event ID 4625 – איוונט זה נוצר כאשר בוצע ניסיון התחברות כושל ולכן יכול להצביע על מתקפת Password Spray.

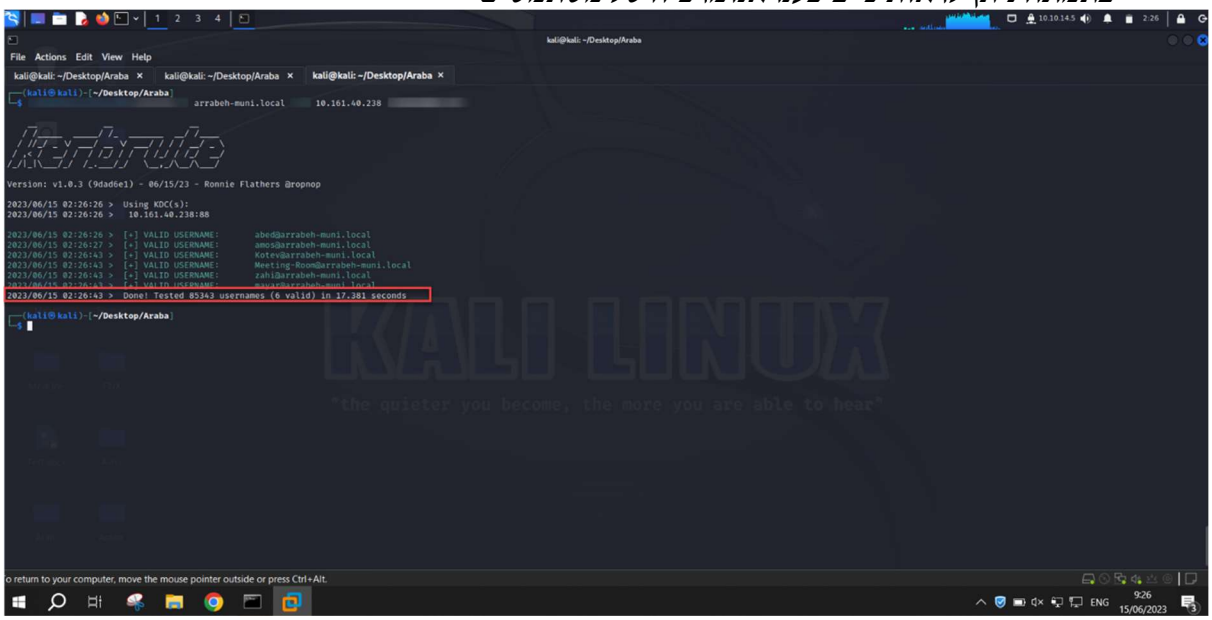
1.6.8. לוודא כי Audit Logon תחת Logon/Logoff מופעל ב-Success & Failure וכי צוות ה- SIEM SOC יודע להתריע מפני ריבוי Windows Event ID 4648 - איוונט זה נוצר כאשר המשתמש שאליו מחוברים מנסה להתחבר עם הרשאות של משתמש אחר ולכן יכול להצביע על מתקפת Password Spray.

1.6.9. לוודא כי Audit Credential Validation Properties תחת Account Login מופעל ב- Success & Failure וכי צוות ה-SIEM SOC יודע להתריע מפני ריבוי 4776 Windows Event ID – איוונט זה נוצר כאשר מתבצע אוטנטיקציה מול שרת ה-DC דרך NTLM ויכול להצביע על Password Enumeration גם כנגד מחשבי קצה / שרתים שהם לא ה-DC מהסיבה כי אותה תחנה מותקפת תפנה ל-DC כחלק מהמתקפה.

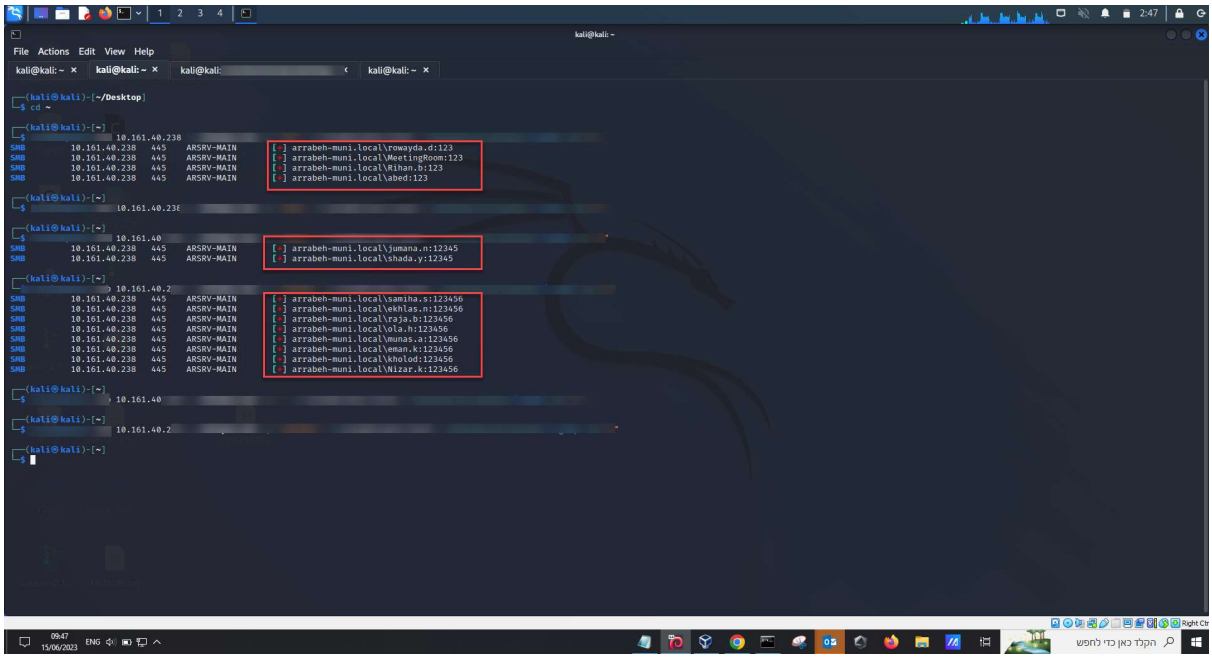
כתובות פגיעות: כלל הרשת.

תמונות:

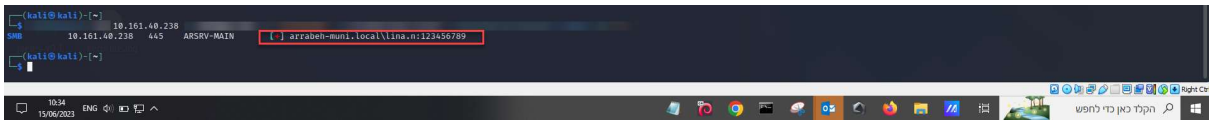
- בתמונה ניתן לראות כי ביצענו אנומרציה של משתמשים



- בתמונה ניתן לראות ניסיונות להריץ מתקפת Password Spray כמה פעמים לאחר ביצוע אנומרציה של משתמשים

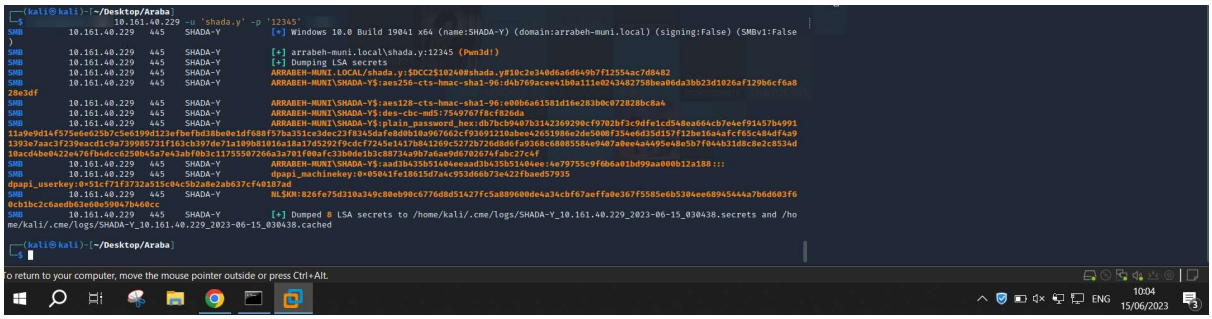


- בתמונה ניתן לראות ניסיונות להריץ מתקפת Password Spray כמה פעמים לאחר ביצוע אנומרציה של משתמשים



- בתמונה ניתן לראות כי המשתמש שהצלחנו להשיג את הסיסמא שלו הוא משתמש לוקאלי על התחנה

- בתמונה ניתן לראות כי המשתמש שהצלחנו להשיג את הסיסמא שלו הוא משתמש לוקאלי על התחנה



1.7. מתקפת PTH והוספת משתמש דומיין אדמין

רמת סיכון: קריטי

ממצא: בהמשך לממצא קודם בו הוצאנו את קובץ ה-SAM שבו היה את ה-HASH של המשתמש האדמין זיהנו כי הוא אדמין לוקאלי בשרתים והמחשבים ובעזרת מתקפת Pass The Hash הצלחנו למצוא מספר סשנים של משתמשי דומיין אדמין במצב "disconnected" (רדום).

לאחר מכן הצלחנו לבצע מתקפת PTH הוספנו משתמש לוקאלי בשם integrity והמשכנו ממנו למתקפת RDP Session Hijacking והצלחנו להשתלט על משתמש "administrator" שהיה גם דומיין אדמין ובשלב זה הסתיים המבדק חדירה.

המלצה:

1.7.1. יישום מערכת Local Administrator Passwords Solution (LAPS) בארגון לצורך ניהול אדמינים לוקאלים גם בשרתים או הסרה מלאה של משתמש אדמין לוקאלי.

1.7.2. הקפדה על ניתוק מלא "Sign Out" ולא להשאיר Sessions של משתמשים על סטטוס "disconnected".

1.7.3. הקמה של Group Policy למטרת לניתוק משתמשים בסטטוס "disconnected" במיידי או מעט אחרי הניתוק של המשתמש בכדי לא להשאירם במצב רדום.

1.7.4. הקמה של Group Policy למטרת ניתוק כלל המשתמשים הפעילים משרתים לאחר סיום יום העבודה.

1.7.5. הפסקת התחברות ב-RDP למחשבים / שרתים בארגון ושימוש במערכת PAM לניהול הרשאות גבוהות, חשבונות פריווילגים, חשבונות רגישים וחיבורים לעמדות קצה / שרתים מרוחקים.

1.7.6. בדיקה מול מערכת ה-SIEM SOC הקיימת מדוע לא התקבלו התרעות בנושא הוספת משתמש הדומיין אדמין החדש.

1.7.7. הקמת מערכת ניטור לוגים ואיוונטים כגון SIEM SOC.

1.7.8. בדיקה מול מערכת ה-EDR מדוע אינה זיהתה את המתקפה וחסמה אותה.

1.7.9. הפעלת "SMB Signing" – אנו נמליץ על הפעלת אפשרות זאת בכלל התחנות ושרתים בארגון.

1.7.9.1. למערכות הפעלה של Windows – להפעיל " Microsoft network server: Digitally sign communications" כ-"always"

1.7.9.2. למערכות הפעלה של Unix/Linux ההגדרה ב-Samba נקראת "Server Signing".

- יש לשים לב כי אפשרות זאת עלולה לגרום לאיטיות ברשת הפנימית בארגון, יש להעירך בהתאם ולבדוק זאת בסביבה מבוקרת בהתחלה.

1.7.10. הפעלה ואכיפה ל-LDAP Signing ו-LDAPS Channel Binding ב-Domain Controllers כולל ניטור לוגים לאיוונטים.

1.7.10.1. https://support.microsoft.com/en-us/topic/2020-ldap-channel-binding-and-ldap-signing-requirements-for-windows-ef185fb8-00f7-167d-744c-f299a66fc00a

1.7.11. במידה ומשתמשים ב-Active Directory Federation Services (ADFS) נמליץ על הפעלת " Enabling Enhanced Protection for Authentication"עליו וגם בשרתי ה-web הרלוונטיים.

1.7.12. במידה ומשתמשים ב-Active Directory Federation Services (ADFS) נמליץ לאפשר עליו לקבל רק בקשות שבהן מופעל EPA ולהגדיר בשרתי ה-web הרלוונטיים.

1.7.13. יישום המלצות חדשות של מייקרוסופט מפני מתקפת NTLM Relay חדשה בשם Petit Potam:

1.7.13.1. https://support.microsoft.com/en-gb/topic/kb5005413-mitigating-ntlm-relay-attacks-on-active-directory-certificate-services-ad-cs-3612b773-4043-4aa9-b23d-b87910cd3429

1.7.14. הגדרת Windows Defender Credential Guard - מטרת השימוש במנגנון זה היא צמצום הסכנה מפני מתקפות מסוג Pass The Hash ו-Pass The Ticket.

למאמר רשמי של Microsoft בנושא:
https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-manage
לפי ההטמעה יש לוודא שהעמדה תומכת בשימוש ברכיב זה:

- Windows 10
- Windows 11

- Windows Server 2016
- Windows Server 2019

ניתן לבדוק אם מנגנון זה פעיל בשני צורות:

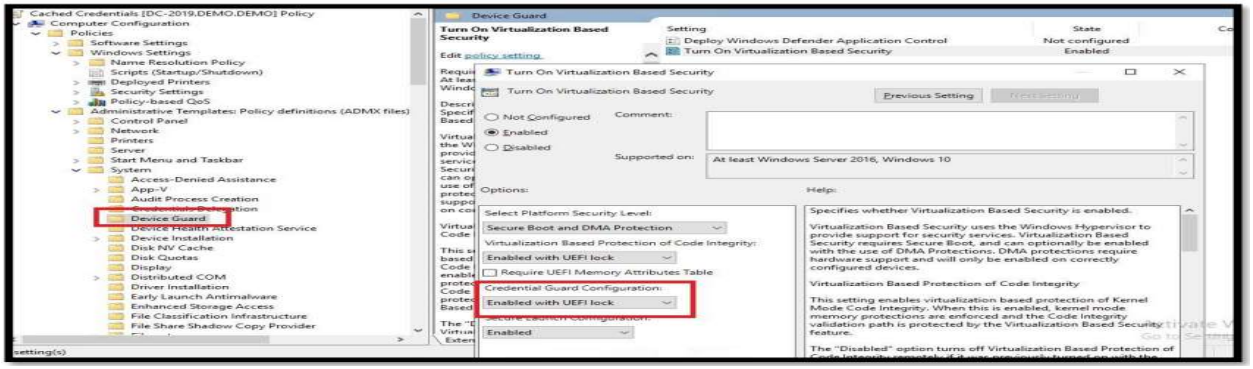
1.7.14.1. לבדיקה עם סקריפט:
https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/dg-readiness-tool

1.7.14.2. לבדיקה ידנית:

- להיכנס ל-msinfo32.exe וללחוץ על "System Information".
- להיכנס ל-"System Summary"
- לוודא כי "Credential Guard" מוצג ליד "Virtualization-based security Services Running". לדוגמה:

Virtualization-based security	Running
Virtualization-based security Required Security Properties	Base Virtualization Support, Secure Boot
Virtualization-based security Available Security Properties	Base Virtualization Support, Secure Boot, DMA Protection, UEFI Code Readonl...
Virtualization-based security Services Configured	Credential Guard, Hypervisor enforced Code Integrity
Virtualization-based security Services Running	Credential Guard, Hypervisor enforced Code Integrity

1.7.14.3. הקמת ה-Policy נתיב הבא, והגדרה על פי התמונה:
Computer Configuration\Administrative Templates\System\Device Guard\Enable

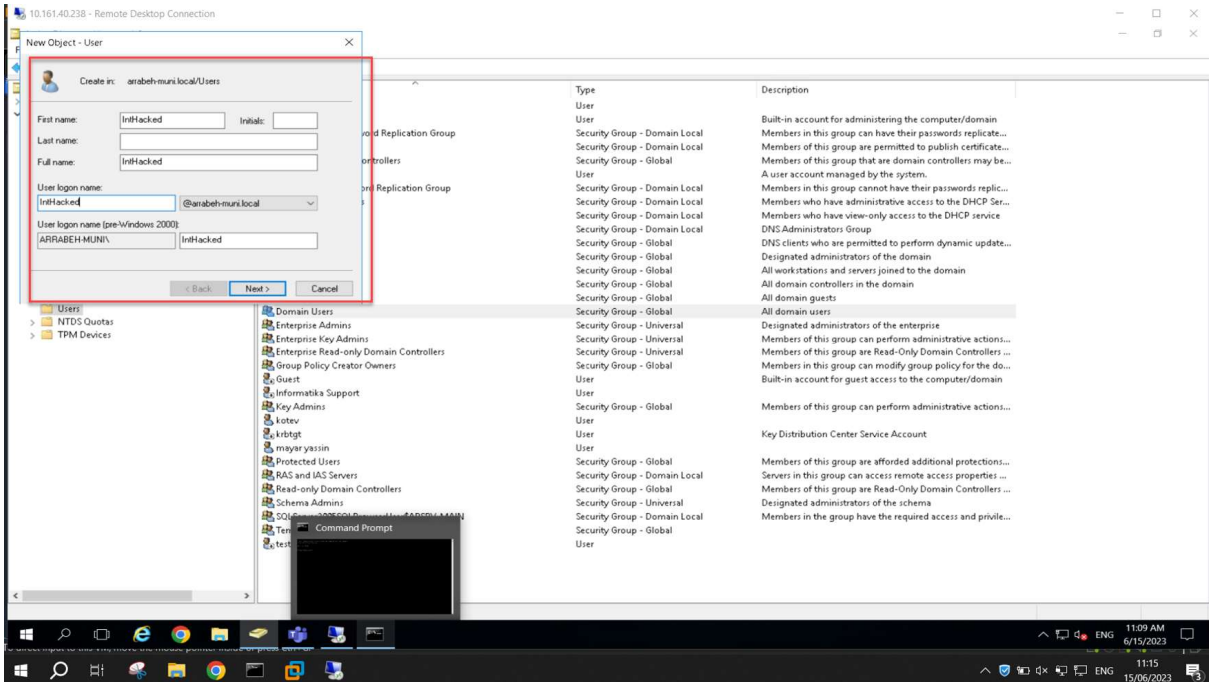


- על מנת שזה יעבוד צריך שהמחשב יתמוך בווירטואליזציה ולהפעיל Hyper V.

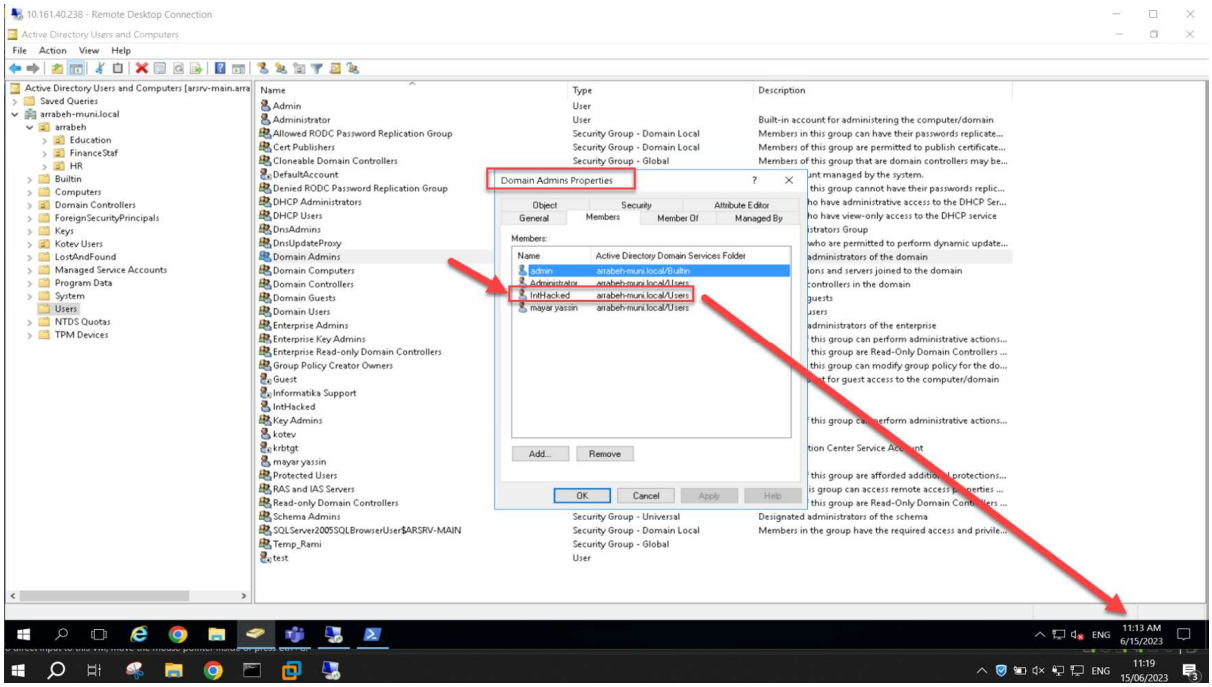
כתובות פגיעות: כלל הרשת.

תמונות:

- בתמונה ניתן לראות כי הצלחנו להוסיף משתמש חדש בשם "inthacked" לקבוצת "Domain Admins"



- בתמונה ניתן לראות את המשתמש בקבוצה החזקה של "Domain Admins"



1.8. הוצאת סיסמאות קריאות ומעורבלת מהזיכרון

רמת סיכון: קריטי

ממצא: בהמשך לממצא קודם בו הצלחנו לייצא קובץ עם סיסמאות קריאות ומעורבלות מהזיכרון. מצורף המלצות לצורך הקשחת הוצאת הקובץ:

המלצות:

1.8.1. גרסאות מחשבים ושרתים ישנים לא מכילים את כל המנגנוני ההגנה החדשים של מייקרוסופט ועלולים גם להכיל חולשות אבטחה שונות. לכן, אנו ממליצים לעדכן לגרסאות עדכניות ביותר.

1.8.2. כאשר צוות המחשוב מתחבר למחשבים / שרתים דרך פרוטוקול RDP, התחנה / שרת אליו התחברו שומרת את הסיסמה / Hash של אותו משתמש בזיכרון. במידה ותוקף משתלט על אותה תחנה / שרת, הוא יכול לייצא את אותם סיסמאות / Hashים ששמורים. כאשר משתמש דומיין אדמין מתחבר, גם הסיסמה שלו נשמרת, כאשר תוקף מייצא את הסיסמאות, הוא יכול לייצא גם סיסמה / Hash של משתמש דומיין אדמין.

לכן, אנו ממליצים בהקדם האפשרי לבדוק הטמעת מערכת PAM בארגון לצורך ניהול הרשאות גבוהות, חשבונות פריווילגים, חשבונות רגישים ועוד. התחברויות למחשבים / שרתים יבוצעו דרך המערכת PAM אשר משתמשת להתחברות במשתמש שלה וניתן להגדיר החלפת סיסמה כל יום / מספר שעות וכך ה-Hash שנשמר במערכת כבר לא רלוונטי לאחר מספר שעות / יום / על פי הגדרת הזמן שבחרתם.

1.8.3. אנו ממליצים על ביצוע סקר מקיף ומלא על כלל המחשבים / שרתים בארגון לצורך ווידוי כי על כולם מוקנים כלי ההגנה הארגונים. לדוגמה: אנטי וירוס / EDR. כלי הגנה אלה הם חלק אינטגראלי במערך ההגנה מפני מתקפות מסוג זה.

1.8.4. אנו נמליץ על הטמעת מערכת הגנה מתקדמת מסוג XDR/EDR אשר המזהים אנומליה בהתנהגות תחנת הקצה או אנומליה בהתנהגות המשתמש ומאפשרים תצורת הגנה יותר מתקדמת מאנטי-וירוס בסיסי.

1.8.5. במידה ומותקן מוצר הגנה מסוג אנטי-וירוס או EDR/XDR יש לבדוק מול נותן השירות / יצרן מודע ההתקפה אינה נחסמה והתריעה.

1.8.6. לוודא כי במוצרי ההגנה הקיימים בארגון כגון אנטי-וירוס EDR/XDR וכד' מופעל בצורה מלאה הגנה מסוג Tampering Protection על כלל הגדרות הקיימות וכי לא ניתן גם לבצע החרגות.

- **חשוב מאוד לבצע את השינויים קודם בסביבת ניסיונית בהתחלה בכדי לוודא השפעות אפשריות על הארגון.**
- לינק למאמר עליו מבוססות מרבית ההמלצות: https://medium.com/blue-team/preventing-mimikatz-attacks-ed283e7ebdd5

1.8.7. ביטול הרשאות SeDebugPrivilege במדיניות הארגונית GPO - הרשאות אלו על פי מייקרוסופט מאפשרות למשתמשים לצרף debugger לכל תהליך או לקרנל עצמו .כברירת מחדל הרשאות אלו ניתנות למשתמשי אדמין לוקאלי. לכן, אנו ממליצים לבטל את הרשאות "SeDebugPrivilege" למשתמשים.

1.8.7.1. ההגדרה במדיניות הארגונית להפצה:

1.8.7.2. Group Policy Management Editor -> Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment -> Debug programs -> Define these policy settings

1.8.7.3. להגדיר שהפוליסה לא תכיל משתמשים או קבוצות.

1.8.8. ביטול פרוטוקול WDigest במדיניות הארגונית GPO - פרוטוקול זה מאופשר כברירת מחדל בגרסאות ישנות של וינדוס:

- Windows 2003
- Windows XP
- Windows 7~8
- Windows 2012

ומאפשר לסיסמאות להיות מאוחסנות בתהליך ה-LSASS בצורה קריאה (clear-text). במערכות הפעלה ישנות, יש צורך בהפצת עדכון אבטחה אשר יוסיף את האפשרות לבטל את השימוש בפרוטוקול זה. לינק לקריאה בנושא:
https://support.microsoft.com/en-us/topic/microsoft-security-advisory-update-to-improve-credentials-protection-and-management-may-13-2014-93434251-04ac-b7f3-52aa-9f951c14b649

1.8.8.1. ההגדרה במדיניות הארגונית להפצה:
1.8.8.2. HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\W Digest
1.8.8.3. עריכת הערך ל-0.

1.8.9. הקשחת פרוטוקול LSA במערכות הפעלה קודמות ל-Windows Servers 2012 R2 ו- Windows 8.1 במדיניות הארגונית GPO – הקשחה זאת מונעת מתהליכים אשר מסווגים כ-"untrusted" מלקרוא את הזיכרון של עצמו או להזריק קוד.

1.8.9.1. ניתן לבצע זאת על ידי יצירת מפתח ברג'יסטרי בשם RunAsPPL והוספת נתיב:
1.8.9.2. "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA"
1.8.9.3. בעל ערך 1.

1.8.10. הפעלת Restricted Admin Mode במדיניות הארגונית GPO - פיצר זה מונע משנים של RDP עם הרשאות "administrators" מלשמור פרטי התחברות בזיכרון של התחנה אליה התחברתם. לצורך הפעלתו צריך לבצע מספר פעולות:

- חשוב להבין כי פעולה זאת גורמת לפרטי ההתחברות (מרגע ההפעלה והאכיפה) לא להישמר ב-Cache באותה מחשב ולכן, באותו מחשב שהתחברתם אליו דרך ה-RDP, לא תוכלו לבצע פעולות לעמדות אחרות מרוחקות עם אותם הרשאות.

1.8.10.1. יצירת מפתח בשם "DisableRestrictedAdmin" עם ערך DWORD מוגדר כ-"0" בנתיב:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa
מפתח זה יאפשר לקבל RDP Session במצב Restricted Admin Mode.

1.8.10.2. באותו נתיב, צריך ליצור מפתח נוסף בשם "DisableRestrictedAdminOutboundCreds" עם ערך DWORD מוגדר כ-"1".
מפתח זה מבטל אימות דרך הרשת בתוך המערכת שהאדמין ביצע אליה RDP.

- לעוד מידע ניתן לקרוא את הלינק הבא:

https://docs.microsoft.com/en-us/archive/blogs/kfalde/restricted-admin-mode-for-rdp-in-windows-7-2008-r2

1.8.10.3. הגדרת Restricted Admin Mode כברירת מחדל במדיניות הארגונית GPO –

בנתיב:
Computer Configurations > Policies > Administrative Templates > System > Credential Delegation.
לערך את ערך "Restrict Delegation of credential to remote servers" ל-"Enabled" ו- " Require Restricted Admin".

- למערכות הפעלה יותר מלפני Windows 2012 R2 ו-Windows 8.1 יש צורך בהתקנת עדכון אבטחה KB2871997 בכדי להשתמש בפיצ'רים אילו.

1.8.10.4. במידה ובארגון אתם מאפשרים חיבור RDP SSO / שרת טרמינל עם SSO (חיבור RPD דרך מחשב בדומיין עם הרשאות המשתמש דומייני הנוכחי ללא צורך הכנסת סיסמה שוב) אז הסיסמה נשמרת בזיכרון של התחנה אליה התחברתם בצורה קריאה (clear text).לכן, במידה ובמדיניות הדומיין מאופשר חיבורים בתצורת SSO, אנו ממליצים לבטל זאת.

1.8.11. ביטול Credentials Cache במדיניות הארגונית GPO – בעת התחברות המשתמש למחשב, במידה וה-Domain Controller לא זמין, המחשב ישווה את ה-Hash של הסיסמה שהוכנסה למערכת בעת ניסון ההתחברות האחרון ל-Hash שנשמר ב-Cache של המחשב לצורך אימות החיבור. כברירת מחדל, וינדוס שומר ב- caching את ה-10 סיסמאות האחרונות, אנו ממליצים למנוע לוקאל caching על ידי:

Computer Configuration -> Windows Settings -> Local Policy -> Security Options -> Interactive Logon: Number of previous logons to cache -> 0

עריכת ערך זה תחייב את המחשב לבצע את האימות דרך ה-DC ולא דרך הסיסמאות שנמרו ב-Cache.

- במחשבים ניידים זה עלול לגרום לבעיה במידה ורוצים שהעובד ישתמש בלפטופ גם כשהוא לא בעבודה, לכן במחשבים ניידים ניתן לצמצם ל-2 ולא ל-0.

1.8.12. Protected Users Group - בשרתים Windows Server 2012 ומעלה, מייקרוסופט הכירה למשתמשים קבוצה חדשה בשם "Protected Users". קבוצה זאת מאפשר לדומיין אדמין להגן על משתמשים בעלי הרשאות גבוהות לדוגמא לוקאל אדמין, גיבויים וכד' (או כל משתמש שבקבוצה) לבצע אימות לדומיין רק דרך Kerberos. פיצ'ר זה אמור לסייע בהפחתת הסיכון להדלפת NTLM Password או סיסמאות Clear TXT.

קבוצה זאת נמצאת ב-Active Directory תחת Users and Computers, המשתמשים שבקבוצה זאת יהיה תחת ההגדרות הבררת מחדל של אימות דרך Kerberos.

- **חשוב לציין כי קבוצה זאת משנה את תצורת העבודה ודברים עלולים שלא לעבוד. לפני הכנסת משתמשים לקבוצה יש לחקור בצורה מקיפה . בנוסף, משתמשי תהליך לא יעבדו אם יהיו בקבוצה הזאת. מצורף לינקים בנושא:**

https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group
https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/how-to-configure-protected-accounts

1.8.13. מניעת שמירת סיסמאות בתצורת LM Hash ב-Active Directroy ובקובץ SAM -

כאשר הסיסמה של המשתמש הינה פחות מ-15 תווים, מערכת ההפעלה וינדוס מייצרת LM Hash ו- NT Hash לסיסמה. הסיסמאות הללו נשמרים בקובץ SAM הלוקאלי או באקטיב דירקטורי. ה-LM Hash נחשב מאוד פריץ וחלש לאומת ה-NT Hash, המאמר הבא מדריך כצד לשמור רק את ה-NT Hash.
https://docs.microsoft.com/en-us/troubleshoot/windows-server/windows-security/prevent-windows-store-lm-hash-password

1.8.14. הגדרת Windows Defender Credential Guard - מטרת השימוש במנגנון זה היא צמצום הסכנה מפני מתקפות מסוג Pass The Hash ו-Pass The Ticket.

למאמר רשמי של Microsoft בנושא:
https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-manage
לפי ההטמעה יש לוודא שהעמדה תומכת בשימוש ברכיב זה:

- Windows 10
- Windows 11
- Windows Server 2016
- Windows Server 2019

ניתן לבדוק אם מנגנון זה פעיל בשני צורות:

1.8.14.1. לבדיקה עם סקריפט:

https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/dg-readiness-tool

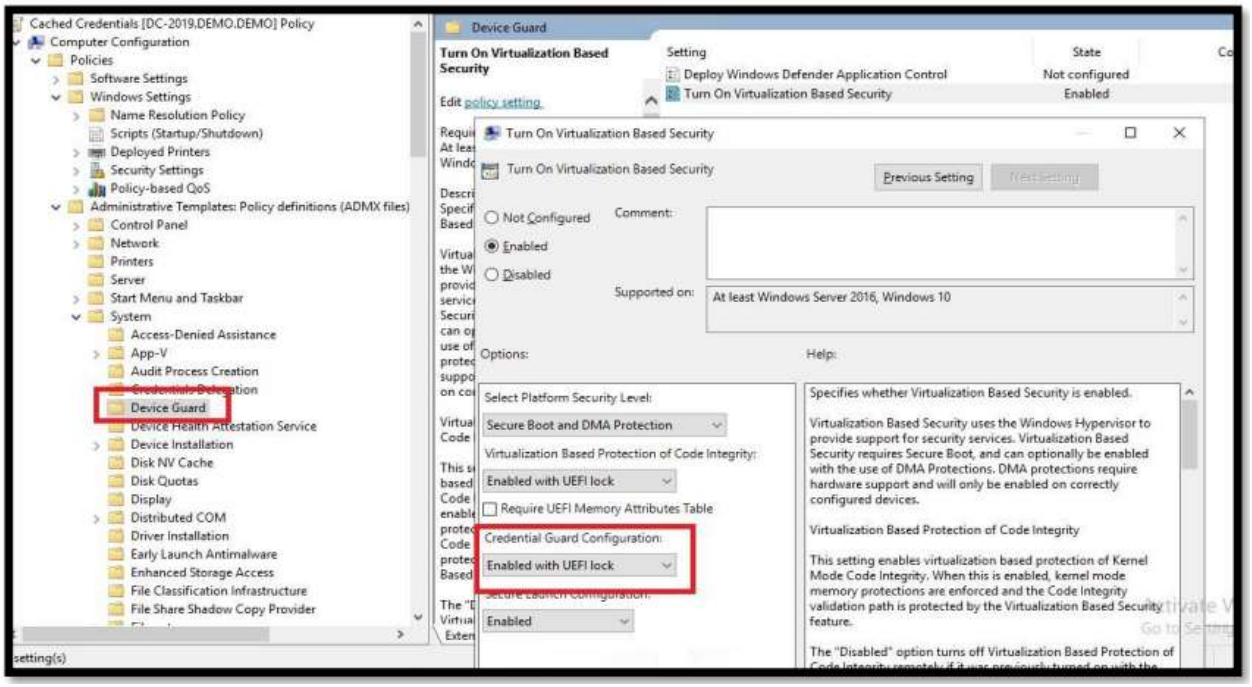
1.8.14.2. לבדיקה ידנית:

- להיכנס ל-msinfo32.exe וללחוץ על "System Information".
- להיכנס ל-"System Summary"
- לוודא כי "Credential Guard" מוצג ליד " Virtualization-based security Services Running". לדוגמה:

Virtualization-based security	Running
Virtualization-based security Required Security Properties	Base Virtualization Support, Secure Boot
Virtualization-based security Available Security Properties	Base Virtualization Support, Secure Boot, DMA Protection, UEFI Code Readonl...
Virtualization-based security Services Configured	Credential Guard, Hypervisor enforced Code Integrity
Virtualization-based security Services Running	Credential Guard, Hypervisor enforced Code Integrity

1.8.14.3. הקמת ה-Policy נתיב הבא, והגדרה על פי התמונה:

Computer Configuration\Administrative Templates\System\Device Guard/Enable



- על מנת שזה יעבוד צריך שהמחשב יתמוך בווירטואליזציה ולהפעיל-Hyper V.

1.8.15. הקשחת Credential Manager - לצורך הגבלת מספר החשבונות שישמרו בManager Credential יש להגביל במדיניות הארגונית ב-GPO.

1.8.15.1. Computer Configuration\Security Settings\Local Policies\Security Options\ Interactive logon: Number of previous logons to cache (in case domain controller is not available)

1.8.15.2. במחשבים נייחים יש להגדיר ערך זה כ - 0, ובמחשבים ניידים יש להגדיר ערך זה כ –"2".

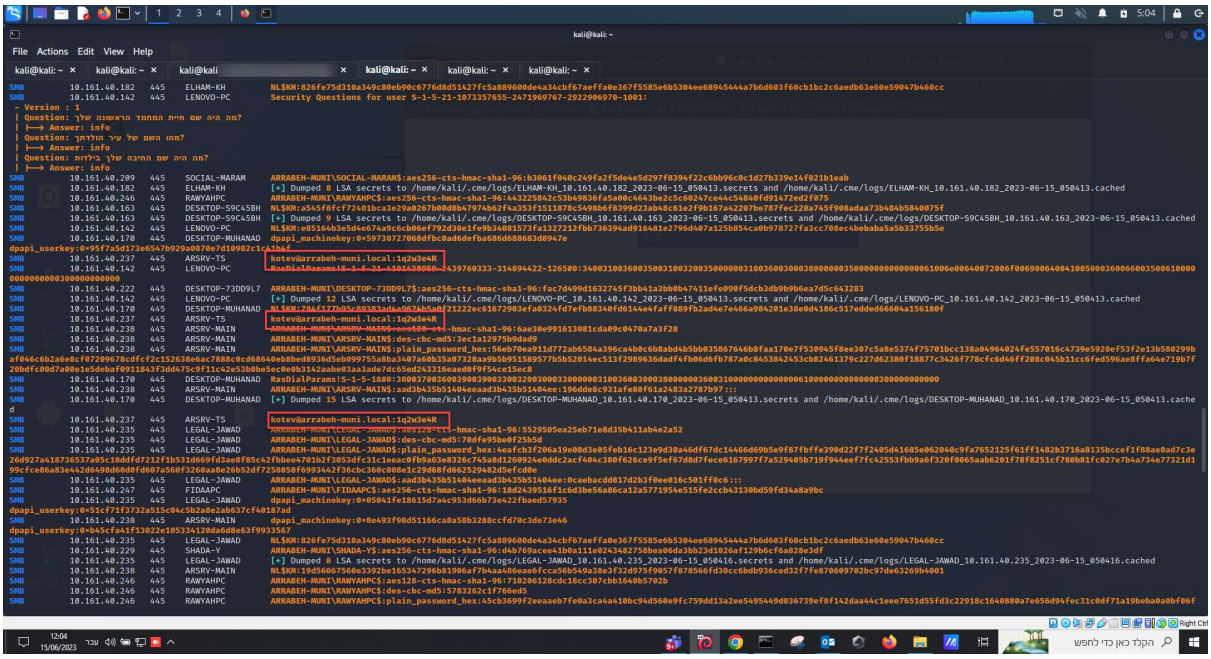
1.8.15.3.

כתובות פגיעות: כלל הארגון.

תמונות:

- בתמונה ניתן לראות הוצאה של סיסמאות מעורפלות מהזיכרון כ Plain Text

- בתמונה ניתן לראות הוצאה של סיסמאות מעורפלות מהזיכרון כ Plain Text



1.9. יציאה לאינטרנט בשרתים פנימיים

רמת סיכון: קריטי

ממצא: מבדיקה שביצענו, ראינו כי ניתן לגלוש מהשרת לאינטרנט בצורה חופשית, משמע, לא קיימת אכיפה של יציאה לרשת החיצונית דרך השרתים.

שרתים פנימיים לרוב אינם צריכים יציאה ותקשורת לרשת החיצונית, אפשרות זאת עלולה להקל בצורה משמעותית לתוקפים, לדוגמה: הוצאת קבצים רגישים מהשרת, הכנסת קבצים זדוניים לשרת, יצירת דלת כניסה מהעולם ועוד.

המלצה:

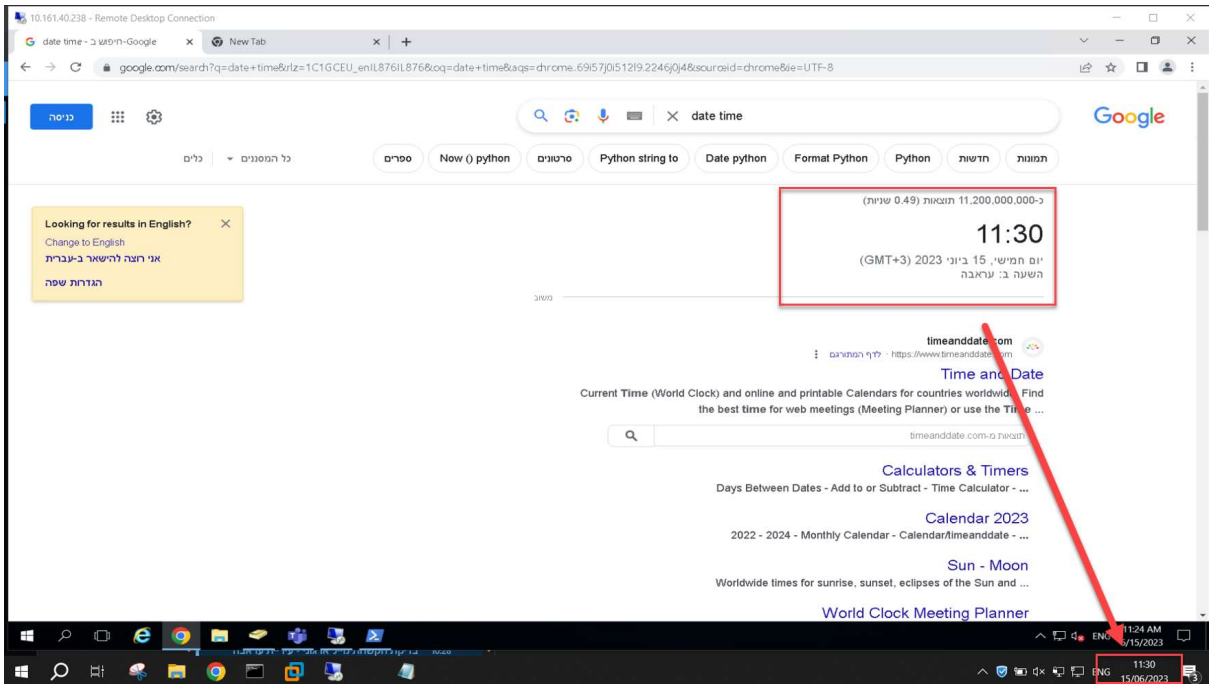
1.9.1. חסימת גלישה לשרתים פנימיים לרשת החיצונית – העדכונים של מערכות ההפעלה ועדכונים צד ג' אמורים להתבצע דרך מערכות רלוונטיות פנימיות בארגון.

1.9.1.1. במידה והשרת צריך יציאה לרשת החיצונית, יש למקם את השרת בסביבה ייעודית(כגון DMZ) עם חומות אש בשני הצדדים (בין השרת לרשת החיצונית ובין השרת לרשת הפנימית וגם WAF במידה ומדובר בשרת אפליקטיבי) עם סט חוקים יעודים מוקשחים על ידי הגדרת פרוטוקולים יעודים בלבד, מתן כתובות from / to ייעודיות והפעלת סט של מודלי אבטחה כגון: Anti-Virus, HTTPS Inspection / Deep Inspection, DLP, Anti-Bot, IPS, Application Control, Web Application Filter, File Control ועוד.

כתובות פגיעות: כלל השרתים בארגון.

תמונות:

- בתמונה ניתן לראות כי בדקנו דרך הדפדפן והרשת החיצונית את השעה



1.10. הורדה והעלאת קבצים

רמת סיכון: קריטי

ממצא: כחלק מתהליך מבדק החדירה היינו צריכים להוריד קבצים "זדוניים" או קבצי הרצה לגיטימיים אשר תוקפים רבים משתמשים בהם לצורך ביצוע פעולות זדוניות ולכן הורדתם מסוכנת לארגון. חשוב לציין כי לא נתקלנו בחסימות כלשהם במהלך ההורדה. דוגמה לסוגי קבצים שהורדו:

- קבצי הרצה מסוג exe.
- קבצי rar.

לאחר הרצת הכלים, היינו צריכים לייצא את הפלט שלהם או לחלופין לייצא קבצים ארגונים לצורך מציאת חולשות / הדגמת סיכונים ולא ניתקלנו במנגנוני חסימה כלשהם. דוגמאות לסוגי קבצים שייצאו מהארגון:

- קבצי Excel
- קבצי Word
- קבצי TXT

המלצות:

1.10.1. הטמעת מערכת Data Lost Prevention (DLP) לצורך ניטור קבצים רגישים ומניעת הוצאתם מהארגון.

1.10.2. חסימת אפשרות העלאת קבצים למשתמשים בארגון גם במחשבי הארגון וגם במיילים – ניתן לבצע זאת לרוב על ידי שילוב של חסימות בחומת האש, מערכות פרוקסי, גלישה בטוחה ומוצר ניהול האימייל הארגוני.

1.10.3. הפעלת מודל בחומת האש בחוקה רלוונטית לצורך ניטור תעבורה מוצפנת. דוגמה לשמות המודולים בחומות אש שונות: HTTPS Inspection / Deep Inspection / SSL Inspection.

1.10.4. ווידוי כי מודל האנטי-וירוס מופעל בכל החוקה הרלוונטית בחומת האש.

1.10.5. הקשחת מודל חסימות קבצים בחומת האש על ידי הקשחת סוגי קבצים נוספים לחסימה:

- **קבצי הרצה, כגון:** קבצי "exe", "bin", "elf", "dll" ו-"so".
- **קבצי התקנה, כגון:** "msi" ו-"msix".
- **קבצי Physical recordable media archiving כגון:** "dmg","iso", "img".

- **קבצי סקריפט ושפות תכנות, כגון:** "ps1", "bat", "vbs", "sh", "c", "cpp", "go", "py", "js", "php", "ps1xml", "psc1", "psd1", "psm1", "pyc", "pyo", "rdp".
- **קבצים מוצפנים, כגון:** קבצי pdf, zip, doc, xml.
- **קבצים עם מאקרו (macro), כגון:** "xlsm".
  - במידה ולא ניתן לחסום בצורה מלאה, יש ליישם מערכת הלבנה לקבצים עם מאקרו להסרתם.
- **קבצי ארכיון, כגון:** "7z", "gzip", "jar","rar" ו-"zip".
  - במידה ולא ניתן לחסום בצורה מלאה, יש ליישם מערכת הלבנה להסרה של קבצים אסורים בתוך קבצי ארכיון.

כתובות פגיעות: כלל הרשת / ארגון.

1.11. שמירת סיסמאות בצורה לא מאובטחת

רמת סיכון: גבוהה

ממצא: במהלך בדיקות מסוג "כריית מידע" נמצאו מספר רב של קבצים מסוגים שונים אשר מכילים סיסמאות קריאות / אשים למערכות שונות כגון:

בעזרת סיסמאות למשתמשים / מערכות שונות ניתן לצפות קבצים רגישים ופרטים של הארגון אשר עלולים לדלוף במידה ומדובר בתוקף זדוני.

המלצה:

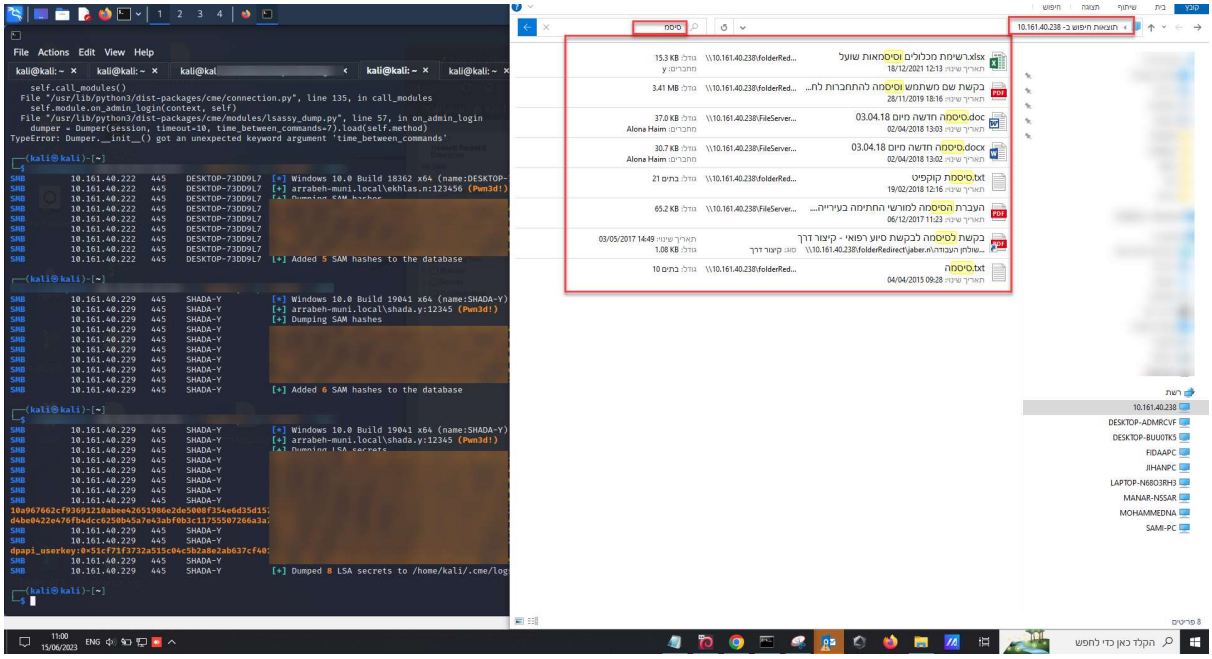
1.11.1. הפצת אימייל לעובדים עם איסור על שמירת סיסמאות בקבצים לא מוגנים ומתן פתרון ארגוני מקצועי לשמית סיסמאות בצורה מאובטחת.
1.11.2. הפצת אימייל לעובדים עם איסור על שמירת סיסמאות בדפדפנים, מחיקתם ומתן פתרון ארגוני מקצועי לשמירת סיסמאות בצורה מאובטחת.
1.11.3. ביצוע סקירה מקיפה בנושא לאיתור ומחיקת קבצים אשר מכילים סיסמאות.
1.11.4. התייחסות לכלל הסיסמאות שנמצאו כסיסמאות פרוצות ולחייב שינוי סיסמה בהקדם האפשרי תוך כדי יישום מהלצות הקשחת הסיסמאות על פי פוליסה מוקשחת.
1.11.5. הוצאת אימייל מסודר לכלל העובדים על איסור שמירת סיסמאות בפתקים פיזיים בנוסף.

כתובות פגיעות:

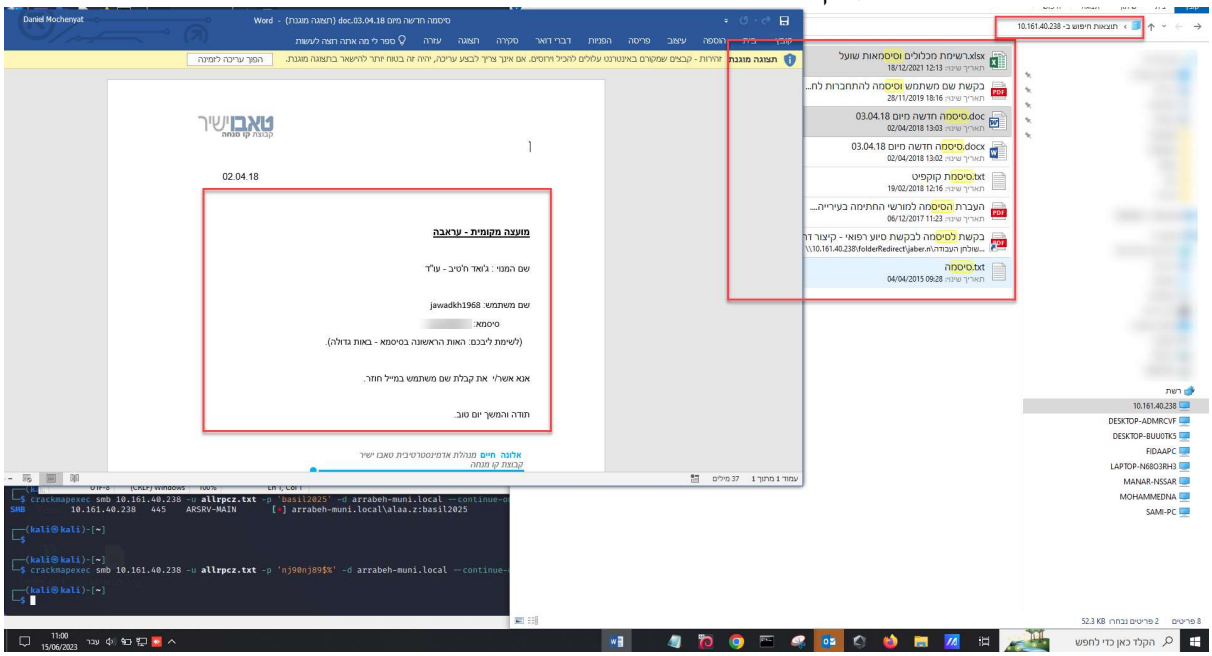
- יש לבצע סקירה מקיפה בכלל המחשבים, השרתים, שיתופי רשת, כונני רשת הארגוניים למציאת קבצי סיסמאות והסרתם.
- קבצי סיסמאות נמצאו בשרתי הקבצים המשותפים.

תמונות:

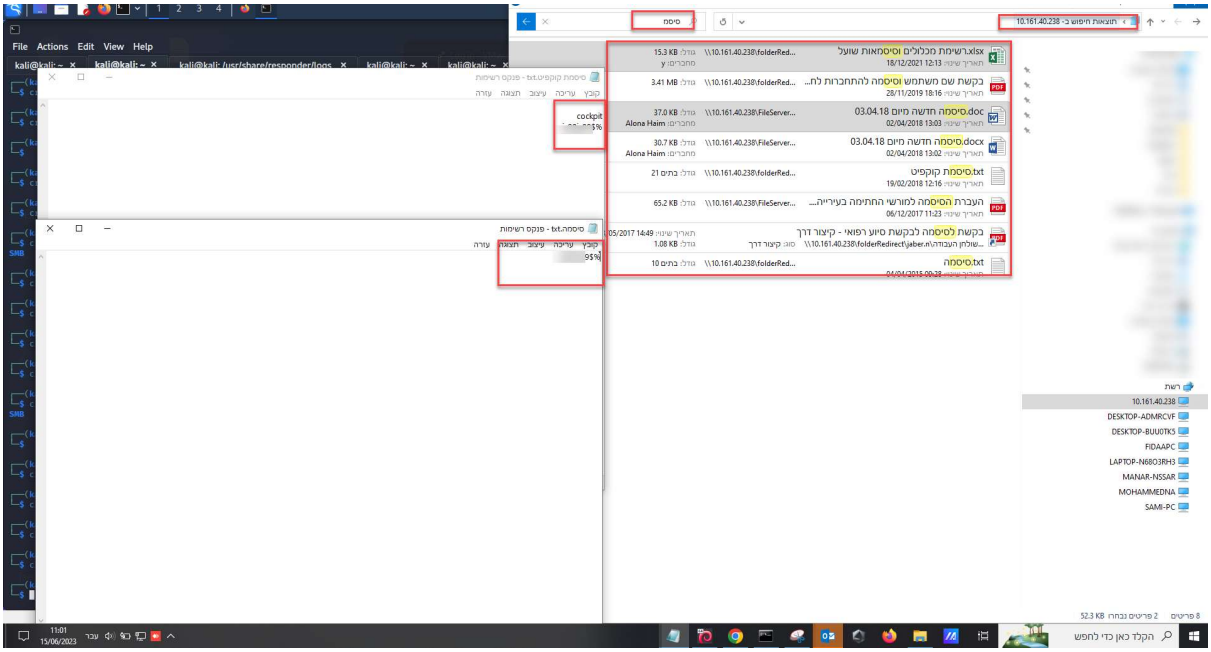
- בתמונה ניתן לראות קבצי סיסמאות חשופים עם סיסמאות בצורת Plaintext שמכיל את כל הסיסמאות של הארגון



- בתמונה ניתן לראות קבצי סיסמאות חשופים עם סיסמאות בצורת Plaintext שמכיל את כל הסיסמאות של הארגון



- בתמונה ניתן לראות קבצי סיסמאות חשופים עם סיסמאות בצורת Plaintext שמכיל את כל הסיסמאות של הארגון



1.12. ממשקי ניהול וסיסמאות ברירת מחדל

רמת סיכון: גבוהה

ממצא: מצאנו מספר ממשקי ניהול של מערכות שונות כגון: ניהול מתגים, מדפסות, מרכזיות בעלי סיסמאות ברירת מחדל ואפילו ללא צורך בפרטי התחברות.

סיסמאות ברירת מחדל לניהול מתגים הן דבר מאוד בעייתי מהסיבה כי ניתן להשתמש בהם לצורך מעבר בין רשתות, מתקפות מניעת שירות ועוד.

סיסמאות ברירת מחדל למשתמשי אדמין מאוד מסוכנות מהסיבה כי הם מביאים הרשאות ניהול לאותם מוצרים ומכן תוקף זדוני יכול לבצע מספר התקפות שונות כגון הוצאת מידע, שיבושים לפעולות שוטפות ועוד.

המלצה:

1.12.1. במידה ואין צורך בממשק ניהול מומלץ להשביתו.

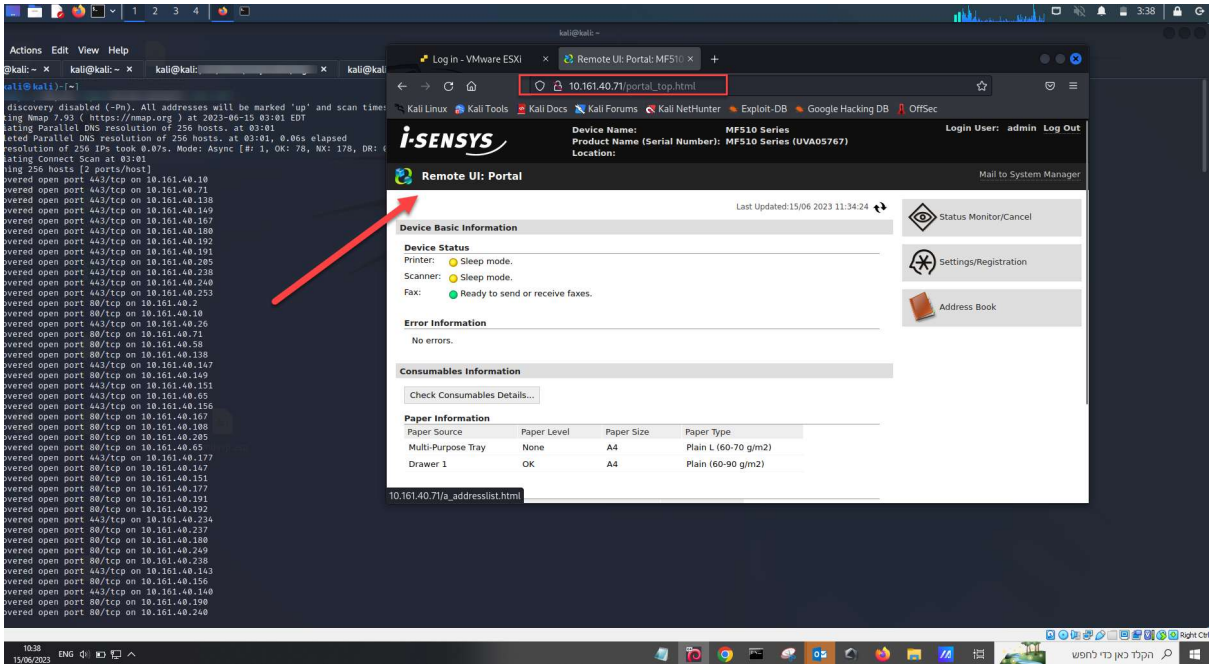
1.12.2. מידה ויש צורך בממשק הניהול מומלץ לשנות את כל פרטי ההתחברות של כלל המשתמשים ברירת מחדל הקיימים במערכת. ולהגדיר Whitelist לממשקי החיבור לכתובות ניהוליות בלבד.

כתובות פגיעות:

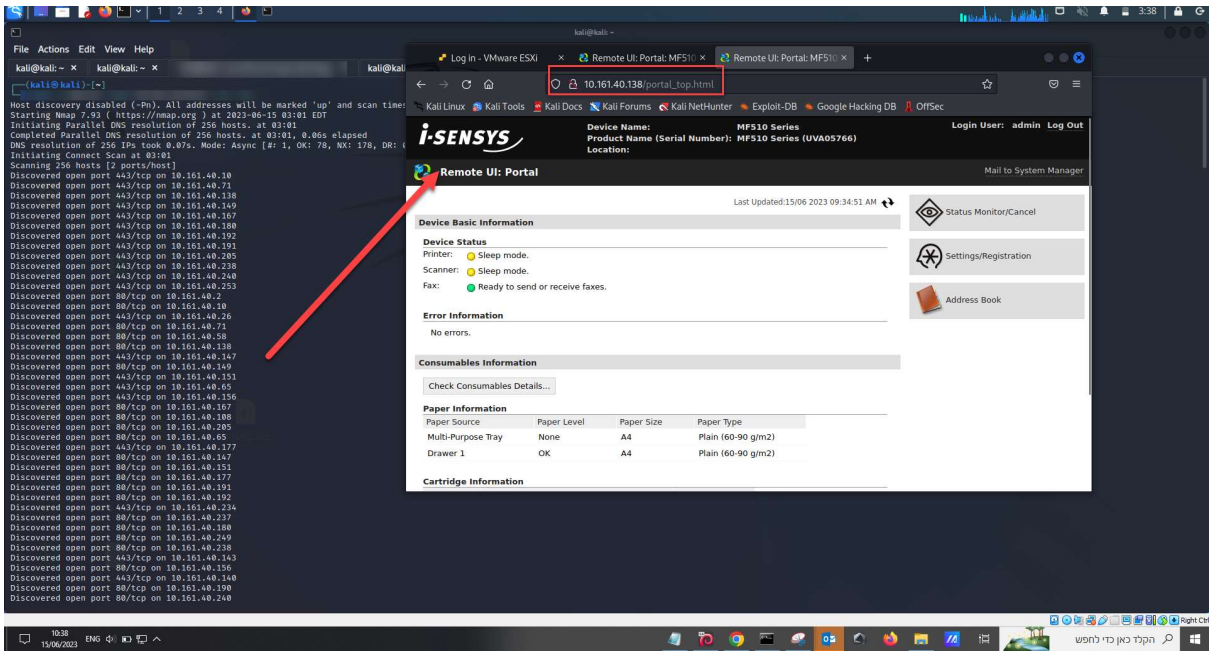
- ממשקי ניהול בכתובות: 10.161.40.71, 10.161.40.138, 10.161.40.143, 10.161.40.147, 10.161.40.58, 10.161.40.2

תמונות:

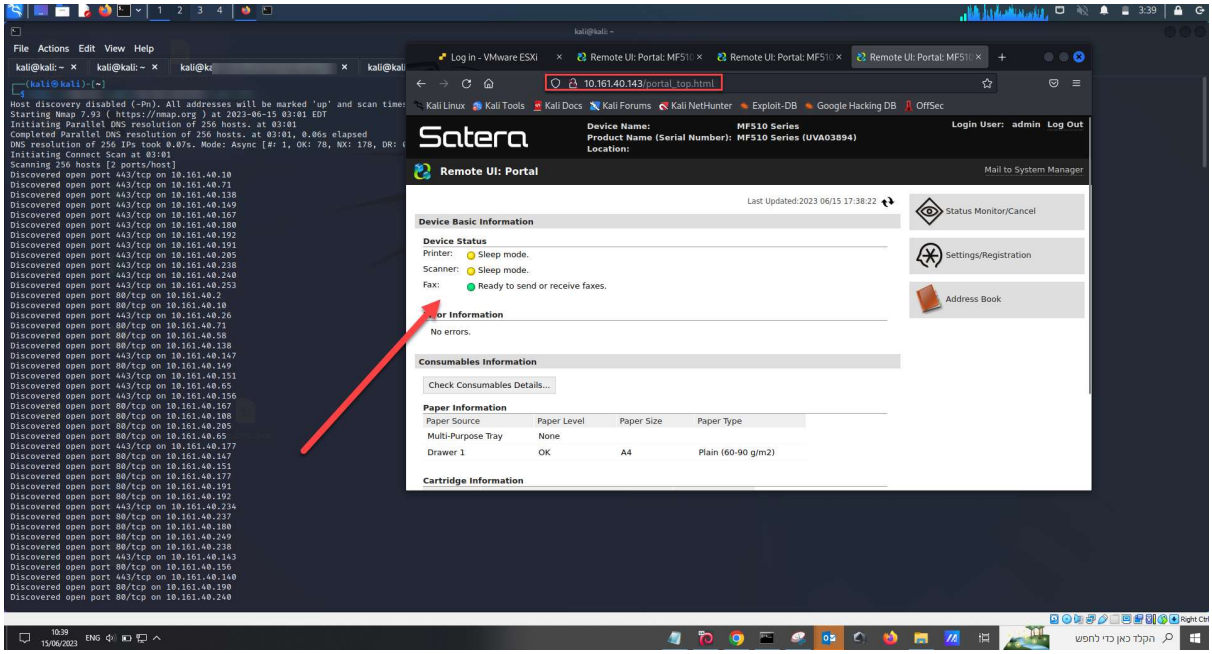
- בתמונה ניתן לראות ממשק ניהול עם פרטי התחברות ברירת מחדל



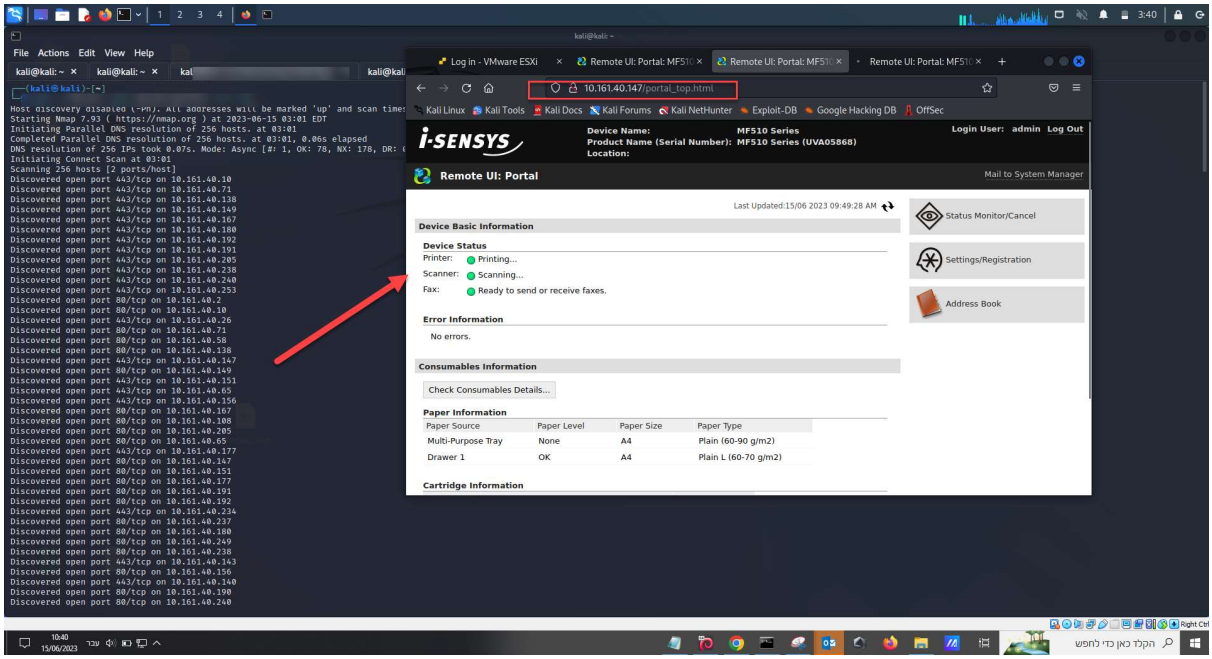
- בתמונה ניתן לראות ממשק ניהול עם פרטי התחברות ברירת מחדל



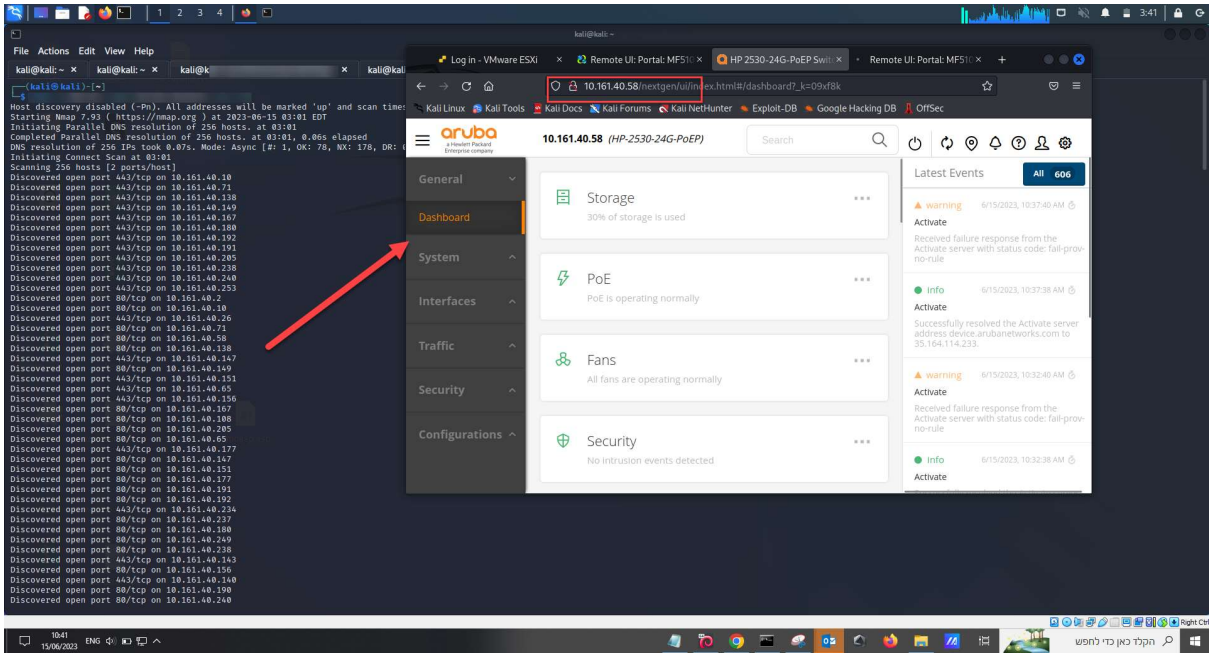
- בתמונה ניתן לראות ממשק ניהול עם פרטי התחברות ברירת מחדל



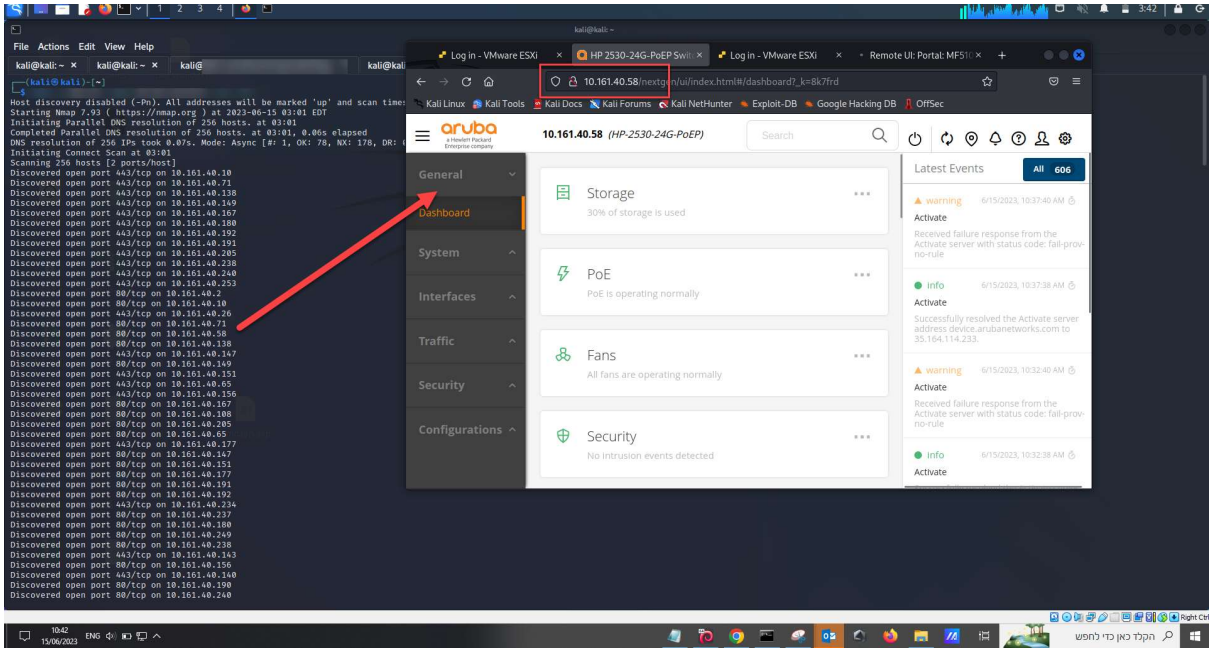
- בתמונה ניתן לראות ממשק ניהול עם פרטי התחברות ברירת מחדל



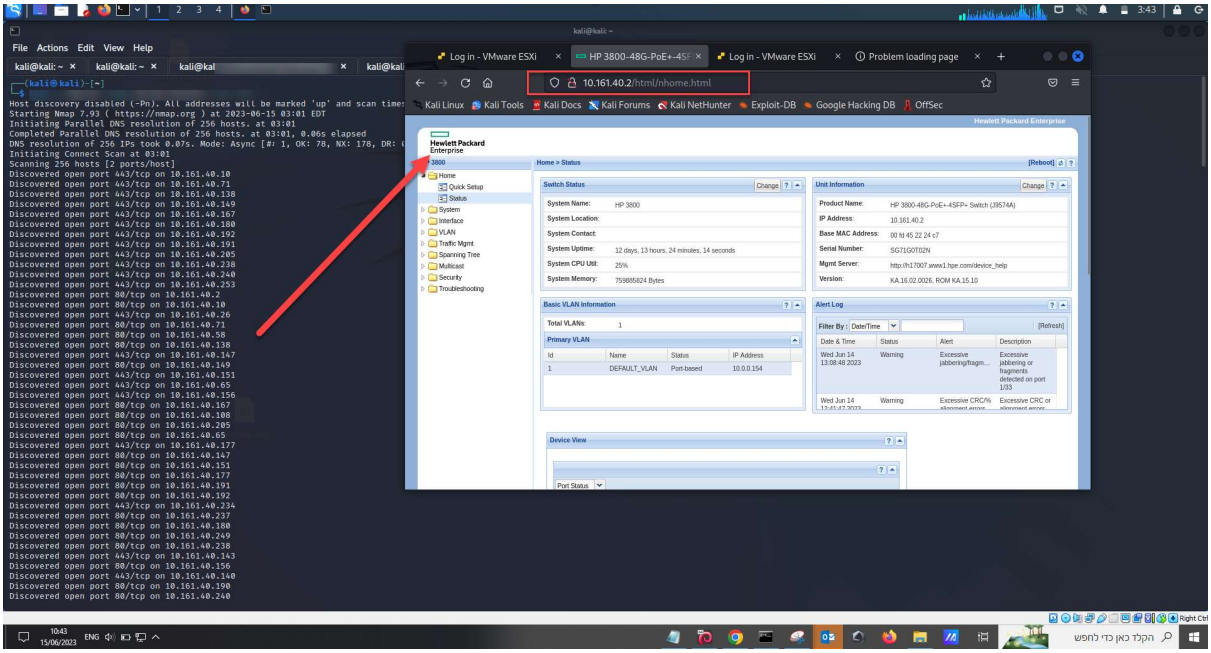
- בתמונה ניתן לראות ממשק ניהול עם פרטי התחברות ברירת מחדל



- בתמונה ניתן לראות ממשק ניהול עם פרטי התחברות ברירת מחדל



- בתמונה ניתן לראות ממשק ניהול עם פרטי התחברות ברירת מחדל



1.13. ניהול הרשאות לקוי בתיקיות רשת והרשאות NTFS

רמת סיכון: גבוהה

ממצא: במהלך המבדק שמנו לב כי לשרתים רבים קיימים תיקיות רשת אשר בעלי הרשאות פתוחות ומאופשרות מידי כגון: everyone, users, domain users ו-authenticated users.
הצלחנו בדרך זאת למצוא מספר רב של קבצים רגישים בחברה.
תוקפים זדוניים עלולים לנצל זאת על מנת הוצאת מידע רגיש של החברה לצורך ריגול תעשייתי, סחיטה, הדלפת מידע, למידת הרשת הפנימית, מציאת חולשות ועוד.

- לדוח מצורף קובץ אקסל עם השיתופים בשם "**שיתופים.xlsx**"

המלצה:

1.13.1. ביצוע סקירת הרשאות מלאה בכלל התיקיות המשותפות בחברה וסידור הרשאות פרטני תוך כדי הימנעות משימוש בהרשאות כלליות כגון:

- Everyone
- Users
- Domain Users
- Authenticated Users

1.13.2. ביצוע סקירת הרשאות ברמת NTFS מלאה בארגון בחברה וסידור הרשאות פרטני תוך כדי הימנעות משימוש בהרשאות כלליות.

1.13.3. הטמעת מערכת Data Lost Prevention (DLP) לצורך ניטור קבצים רגישים ומניעת הוצאתם מהארגון.

1.13.4. התייחסות לכלל הסיסמאות שנמצאו כסיסמאות פרוצות ולחייב שינוי סיסמה בהקדם האפשרי תוך כדי יישום מהלצות הקשחת הסיסמאות על פי פוליסה מוקשחת.

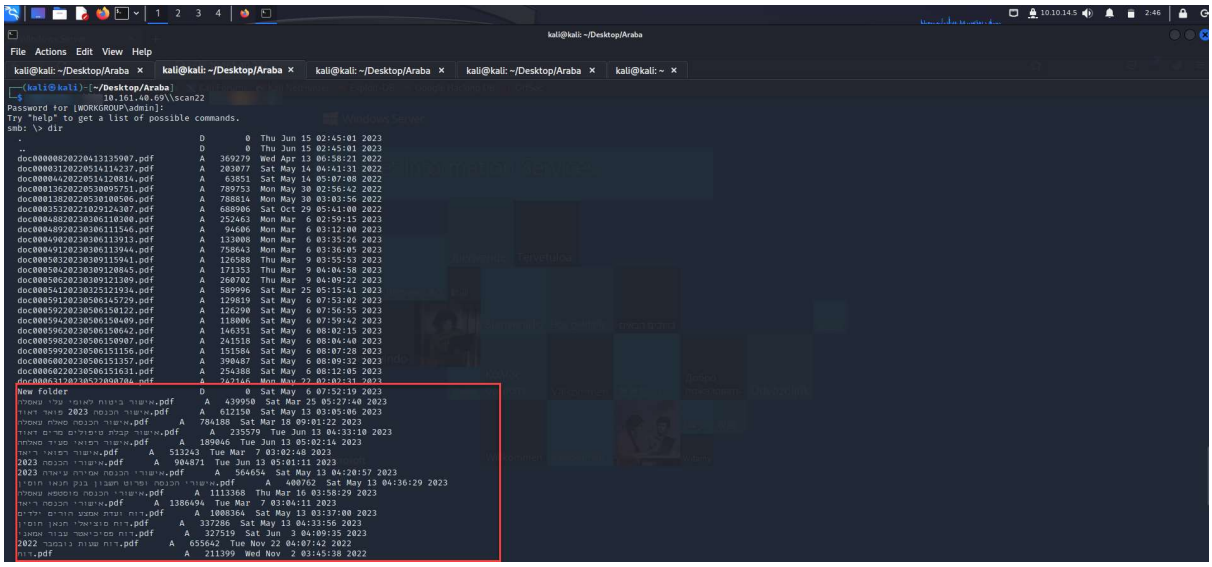
1.13.5. מחיקה והסרה של כלל הקבצים שנמצאו בהם סיסמאות.

כתובות פגיעות: כלל הרשת / ארגון.

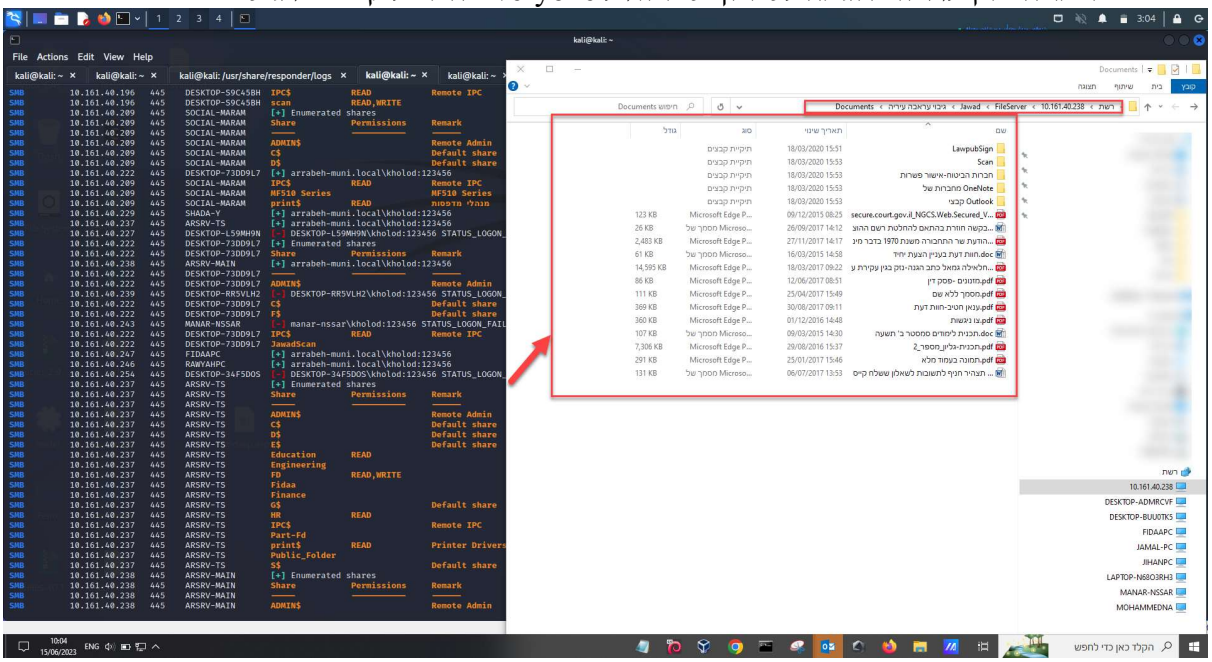
- יש לגשת לקובץ אקסל המצורף לדוח המבדק.

תמונות:

- בתמונה ניתן לראות דוגמה לשיתוף שפתוח ל Everyone המכיל קבצים רגישים



- בתמונה ניתן לראות דוגמה לשיתוף שפתוח ל Everyone המכיל קבצים רגישים



- בתמונה ניתן לראות דוגמה לתיקיות שמצאנו. לדוח מצורף גם האקסל מהתמונה עם הרשימה המלאה.

CurrentUserAllowed	EveryoneAllowed	Share	Computer	1
TRUE	TRUE	ADMIN$	JihanPC.arrabeh-muni.local	2
TRUE	TRUE	C$	JihanPC.arrabeh-muni.local	3
TRUE	TRUE	print$	JihanPC.arrabeh-muni.local	4
TRUE	TRUE	scan	JihanPC.arrabeh-muni.local	5
TRUE	TRUE	ADMIN$	arsrv-main.arrabeh-muni.local	6
TRUE	TRUE	C$	arsrv-main.arrabeh-muni.local	7
TRUE	TRUE	D$	arsrv-main.arrabeh-muni.local	8
TRUE	TRUE	Data	arsrv-main.arrabeh-muni.local	9
TRUE	TRUE	ESET	arsrv-main.arrabeh-muni.local	10
TRUE	TRUE	FileServer	arsrv-main.arrabeh-muni.local	12
TRUE	TRUE	IderRedire(	arsrv-main.arrabeh-muni.local	14
TRUE	TRUE	NETLOGON	arsrv-main.arrabeh-muni.local	15
TRUE	TRUE	S$	arsrv-main.arrabeh-muni.local	16
TRUE	TRUE	SYSVOL	arsrv-main.arrabeh-muni.local	17
TRUE	TRUE	/BRCatalog	arsrv-main.arrabeh-muni.local	18
TRUE	TRUE	scan	Lenovo-PC.arrabeh-muni.local	21
TRUE	TRUE	Users	Lenovo-PC.arrabeh-muni.local	22
TRUE	TRUE	print$	DESKTOP-Muhanad.arrabeh-muni.local	25
TRUE	TRUE	SCAN	DESKTOP-Muhanad.arrabeh-muni.local	26
TRUE	TRUE	Users	DESKTOP-OSHPLAK.arrabeh-muni.local	29
TRUE	TRUE	print$	DESKTOP-4UHCOVV.arrabeh-muni.local	33
TRUE	TRUE	scan	DESKTOP-4UHCOVV.arrabeh-muni.local	34
TRUE	TRUE	print$	AMENE.arrabeh-muni.local	38
TRUE	TRUE	print$	rawyahPC.arrabeh-muni.local	41
TRUE	TRUE	scan	rawyahPC.arrabeh-muni.local	42
TRUE	TRUE	print$	fidaaPC.arrabeh-muni.local	45
TRUE	TRUE	scan	fidaaPC.arrabeh-muni.local	46
TRUE	TRUE	Education	arsrv-ts.arrabeh-muni.local	55
TRUE	TRUE	FD	arsrv-ts.arrabeh-muni.local	57
TRUE	TRUE	HR	arsrv-ts.arrabeh-muni.local	61
TRUE	TRUE	print$	arsrv-ts.arrabeh-muni.local	63
TRUE	TRUE	scan	DESKTOP-S9C45BH.arrabeh-muni.local	68
TRUE	TRUE	print$	elham-kh.arrabeh-muni.local	72
TRUE	TRUE	print$	shada-y.arrabeh-muni.local	76
TRUE	TRUE	scan	shada-y.arrabeh-muni.local	77
TRUE	TRUE	scan	Legal-Jawad.arrabeh-muni.local	80
TRUE	TRUE	share folde	Legal-Jawad.arrabeh-muni.local	81
TRUE	TRUE	print$	Social-Maram.arrabeh-muni.local	86
TRUE	TRUE	print$	DESKTOP-JT4PEBI.arrabeh-muni.local	89
TRUE	TRUE	print$	muhammad-nass.arrabeh-muni.local	92

1.14. מתקפת רשת MITM6

רמת סיכון: גבוהה

ממצא: מתקפת רשת בשם mitm6 המבוססת על תעבורת רשת של IPv6 מהווה רמת סיכון גבוהה לארגון. בעזרת המתקפה הצלחנו לשנות את כלל הכתובות ברשת מIPv4 לכתובות של IPv6 ולנתב את התעבורה דרך המכונה וירטואלית שלנו שכביכול שימשה כמעבר באמצע הרשת שתפסה את כל הפקטות והבקשות שהועברו. בעזרת המתקפה הצלחנו לייצא את כל רשימת המשתמשים בדומיין , הקבוצות ואת פוליסת הסיסמאות לקבצי json וקבצי HTML .

המלצה:

1.14.1. לבדוק מדוע מוצר ההגנה לא התריע מפני המתקפה.

1.14.2. לבטל תעבורת רשת של IPv6 דרך ה-GPO

1.14.3. ניתן לגשת ל Computer Configuration -> Policies -> Administrative Templates -> Network -> IPv6 Configuration -> Open the IPv6 Policy -> "Disable all IPv6 components".

1.14.4. אלטרנטיבה נוספת לביטול תעבורת IPv6 ניתן לערוך את הרג'יסטרי בנתיב: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\
ע"י שינוי הערך של "DisableComponents" ל "255 (0xff)" .

כתובות פגיעות: כלל הרשת / ארגון.

1.15. מערכת Network Access Control

רמת סיכון: בינוני

ממצא: מבדיקה שביצענו עולה כי לא מוטמעת מערכת מסוג Network Access Control (NAC) אשר מטרתה לחסום ולמנוע גישה לרשת הפנימית של הארגון למכשירים לא מאומתים.

גורם זדוני בעל גישה פיזית למשרדים / סניפים וכד' יכול להתחבר לנקודת רשת פיזית בסביבה הארגונית ולקבל גישה לתוך הרשת הפנימית של הארגון ובכך לבצע מתקפות שונות לצורך הוצאת מידע רגיש, העלאת הרשאות, השתלטות עוינת ועוד.

המלצה:

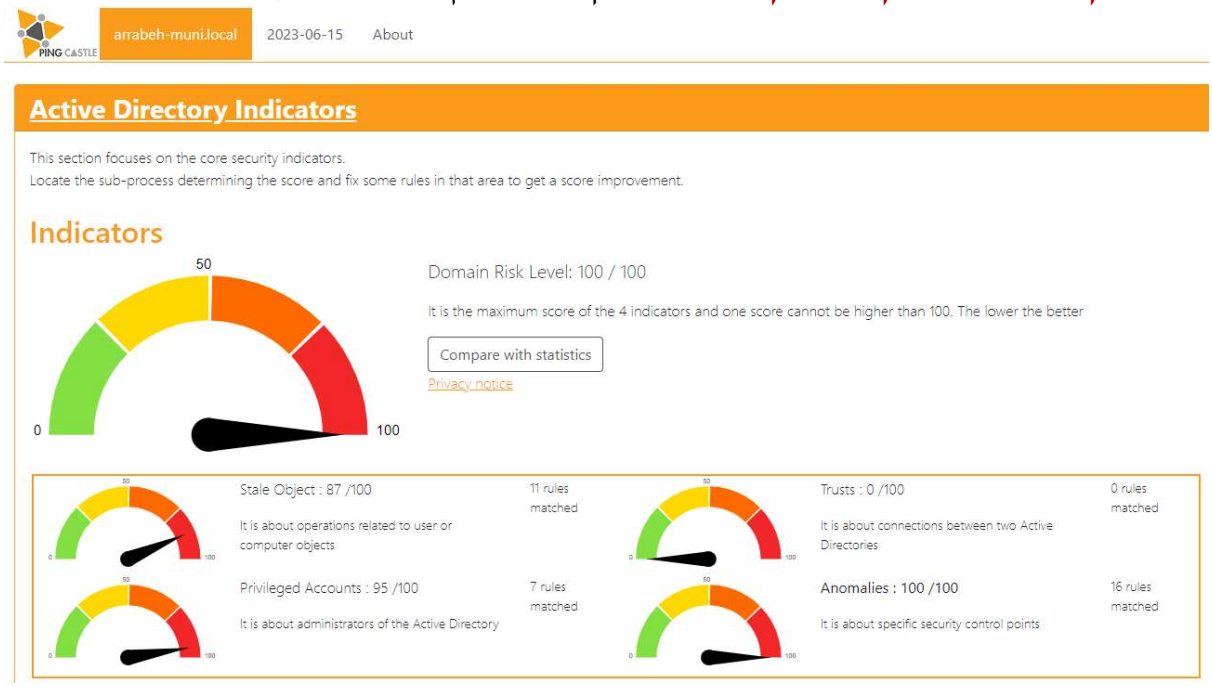
1.15.1. הטמעת מערכת Network Access Control בארגון לצורך בקרה וניהול מכשירים מחוברים פיזית לרשת - לצורך כך יש לבצע סקירה על כלל כי הם תומכים במערכת (לדוגמה: תומכים ב-SNMP Write). יש לבדוק תאימות מול כל יצרן ולבצע את השדרוגים.

2. סקירת אקטיב דירקטורי

דוח Ping Castle AD Health Check הינו דוח שסוקר את ה-Active Directory ומחלק את הממצאים לארבע קטגוריות ראשיות שעל פיהם מגדיר רמת סיכון כללית ל-AD הארגוני.
הדוח המלא אינו כלול בדוח זה, הוא מצורף בדוח נפרד כקובץ נפרד עם תיאורים כללים, תיאורים טכניים והמלצות לטיפול.

1. **Stale Object** - It is about operations related to user or computer objects - רמת סיכון : 87 מתוך 100.
2. **Privileged Accounts** - It is about administrators of the Active Directory - רמת סיכון : 95 מתוך 100.
3. **Trusts** - It is about links between two Active Directories - רמת סיכון : 0 מתוך 100.
4. **Anomalies** - It is about specific security control points - רמת סיכון : 100 מתוך 100.

רמת סיכון כללית לכלל האקטיב דירקטורי: 100 מתוך 100 – המקסימאלית ביותר.



דוח:

- הדוח ישלח מקובץ ב-RAR עם הדוח הסופי. שם הדוח המצורף: **ad_hc_arrabeh-muni.local.html**

המלצות:

2.1.1. לעבור על הדוח בצורה מסודרת ולהתחיל לטפל בממצאים המפורטים בדוח זה על מנת להוריד את רמת הסיכון של הדומיין.

פרק 4 : <u>הבסיס החוקי לעבודת המבקר</u>

פקודת העיריות (נוסח חדש)

149ג. ועדה לענייני ביקורת (תיקון: תשל"ט, תש"ן, תשנ"ח, תשס"ב)

(א) המועצה תבחר מבין חבריה ועדה לענייני ביקורת שתפקידה לדון בכל דו"ח של מבקר המדינה ושל נציב תלונות הציבור על הביקורת בעיריה, בכל דו"ח של משרד הפנים על העיריה ובכל דו"ח של מבקר העיריה, ולעקוב אחרי תיקון הליקויים שהעלתה הביקורת, והיא רשאית לדון בכל דו"ח ביקורת אחר על העיריה שהוגש לפי דין; הועדה תגיש למועצה את סיכומיה והצעותיה.

(ב) מספר חברי הועדה לא יעלה על שבעה; הרכב הועדה יהיה תואם, ככל שניתן, את ההרכב הסיעתי של המועצה; ראש העיריה, סגניו וחברי ועדת ההנהלה לא יהיו חברים בועדה לעניני ביקורת.

(ג) (1) יושב ראש הועדה לעניני ביקורת יהיה, בכפוף להוראות פסקה (2) מהאופוזיציה ולא יכהן כדירקטור בהנהלת גוף עירוני מבוקר; לענין סעיף זה יראו את יושב ראש הועדה לעניני ביקורת כשייך לאופוזיציה אם התקיימו בסיעתו, בין היתר, לפחות כל אלה:

(א) סיעתו שונה מסיעתו של ראש העיריה;

(ב) לסיעתו אין ייצוג בועדת ההנהלה;

(ג) מסיעתו לא מונו סגנים לראש העיריה;

(ד) סיעתו אינה קשורה בהסכם המתייחס לכהונת ראש העיריה או לניהול העיריה.

פרק תשיעי: עובדי העיריה

סימן א': מינוי עובדים ופיטוריהם

167. מינוי פקידים(תיקון: תשל"א, תש"ן, תשנ"ה, תשס"א, תשס"ב, תשס"ד, תשס"ה, תשס"ו)

(א) מועצה רשאית, ולפי דרישת הממונה חייבת, למנות לעיריה מזכיר אם לא מונה מנהל כללי, ורופא וטרינר; כן חייבת המועצה למנות מהנדס; מינוי לפי סעיף קטן זה יהיה של אנשים ראויים, בדרך של מכרז פומבי בכפוף להוראות סעיף קטן (א2), ואפשר למנות אדם ליותר ממשרה אחת מהמשרות האמורות.

(א1)ראש העיריה רשאי, ולפי דרישת הממונה חייב, למנות לעיריה מנהל כללי ובלבד שהמועצה לא מינתה מזכיר.

(א2)לא תמנה המועצה ולא ימנה ראש העיריה אדם, שעליהם למנותו, למשרה מהמשרות הנקובות בתוספת החמישית אלא את מי שועדת המכרזים לבחירת עובדים בכירים בחרה בו, ולענין מנהל כללי, לא ימנה ראש העיריה אלא את מי שועדת המכרזים לבחירת עובדים בכירים אישרה את כשירותו והתאמתו לתפקיד.

(ב) המועצה, בהחלטה ברוב חבריה, תמנה לעיריה מבקר במשרה מלאה.

(ג) לא ימונה ולא יכהן אדם כמבקר עיריה אלא אם כן נתקיימו בו אלה:

(1) הוא יחיד;

(2) הוא תושב ישראל;

(3) הוא לא הורשע בעבירה שיש עמה קלון;

(4) הוא בעל תואר אקדמי מאת מוסד להשכלה גבוהה בישראל או מוסד להשכלה גבוהה בחוץ-לארץ שהכיר בו, לענין זה, מוסד להשכלה גבוהה בישראל, או שהוא עורך דין או רואה חשבון;

(5) הוא רכש נסיון במשך שנתיים בעבודת ביקורת;

(6) הוא אינו חבר בהנהלה פעילה של מפלגה או בהנהלה פעילה או בגוף דומה אחר של רשימת מועמדים שהתמודדה בבחירות לרשות המקומית.

(ג1) לא ימונה ולא יכהן כמבקר עיריה מי שכיהן כחבר מועצה, אלא אם כן עברו עשר

שנים מתום כהונתו כחבר מועצה באותה עיריה, או שנתיים מתום כהונתו כחבר מועצה בעיריה גובלת.

מיום 26.12.2005

תיקון מס' 107

ס"ח תשס"ו מס' 2042 מיום 26.12.2005 עמ' 106 (ה"ח 102)

החלפת סעיף קטן 167(ג1)

הנוסח הקודם:

(ג1) מי שכיהן כחבר מועצה לא ימונה ולא יכהן כמבקר עיריה בשום עיריה אלא אם כן עברו עשר שנים מתום כהונתו כחבר מועצה.

(ג2) מי שהיה מועמד בבחירות למועצת העיריה, לא יכהן כמבקר אותה עיריה, למשך כל תקופת כהונתה של אותה מועצה שאליה היה מועמד.

(ד) על אף הוראות סעיף קטן (ג), רשאי הממונה על המחוז לאשר מינויו של אדם אשר לא נתמלא בו אחד מן התנאים המנויים בפסקאות (4) ו- (5) לסעיף קטן (ג), כמבקר העיריה, אם הוא רכש נסיון במשך עשר שנים בעבודת ביקורת בגוף ציבורי כמשמעו בחוק הביקורת הפנימית, תשנ"ב-1992.

(ה) (1) המועצה, בהחלטה ברוב חבריה, תמנה גזבר לעיריה; השר, בהתייעצות עם שר המשפטים ועם שר האוצר, יקבע תנאים לענין כשירות ופסלות לכהונה לגזבר.

(2) נבצר מהגזבר זמנית למלא את תפקידו, תמנה המועצה ממלא מקום לגזבר לתקופה שלא תעלה על שלושה חודשים; חדל הגזבר למלא את תפקידו וטרם מינתה המועצה גזבר אחר במקומו, תמנה המועצה ממלא מקום לגזבר לתקופה כאמור; ואולם רשאי השר להאריך תקופה זו בתקופה נוספת שלא תעלה על שלושה חודשים, ובלבד שנוכח כי המועצה נוקטת את כל הפעולות הדרושות למינוי גזבר וכי הארכה כאמור דרושה לשם השלמת הליך המינוי; ההוראות לפי פקודה זו החלות לגבי גזבר יחולו גם לגבי ממלא מקומו, למעט ההוראות לענין דרכי המינוי, תנאי הכשירות למינוי ופיטורים.

167א. מועצה שלא מינתה מבקר (תיקון: תשנ"ה, תשס"ה)

(א) ראה הממונה כי המועצה אינה ממנה מבקר, רשאי הוא לדרוש ממנה בצו כי תמנה מבקר, כאמור בסעיף 167, תוך הזמן הנקוב בצו.

(ב) לא מילאה המועצה אחרי הצו תוך הזמן האמור, רשאי הממונה למנות מבקר לעיריה ולקבוע את שכרו.

168. משכורת (תיקון: תשל"ט)

אנשים שנתמנו כאמור בסעיף 167 יקבלו את המשכורת שתקבע המועצה.

169ב. ועדת המכרזים לבחירת עובדים בכירים (תיקון: תשס"ה)

(א) בכל עיריה תוקם ועדת מכרזים לבחירת עובדים למשרות המנויות בתוספת החמישית; החלטתה של הועדה תובא לאישור המועצה או ראש העיריה, לפי הענין.

(ב) ואלה חברי ועדת המכרזים לבחירת עובדים בכירים –

(1) ראש העיריה או נציגו מקרב סגניו, אשר ישמש כיושב ראש ועדת המכרזים לבחירת עובדים בכירים;

(2) שני חברי המועצה שייבחרו על ידה, אשר לפחות אחד מהם נציג סיעה שאינה מיוצגת בועדת ההנהלה, ואם כל הסיעות מיוצגות בועדת ההנהלה, חבר המועצה שאינו חבר בועדת ההנהלה;

(3) המנהל הכללי של העיריה;

(4) נציג שימנה השר, שהוא בעל תפקיד מקביל בעיריה אחרת לתפקיד הנדון במכרז.

(ג) על אף האמור בסעיף קטן (ב)(3), בתהליך בדיקת כשירותו והתאמתו של מועמד למשרת המנהל הכללי, יהיה היועץ המשפטי של העיריה חבר ועדת המכרזים לבחירת

עובדים בחירים במקום המנהל הכללי.

(ד) היועץ המשפטי של העיריה יהיה משקיף בישיבות ועדת המכרזים לבחירת עובדים בכירים, למעט בישיבות שענינן מינוי היועץ המשפטי של העיריה.

(ה) נקבע בדין כי לא ימונה אדם למשרה מסוימת אלא אם כן הוא בעל כשירות והתאמה לתפקיד, תהיה ועדת המכרזים הועדה המוסמכת לבדירה ולאישור כשירותו והתאמתו כאמור.

170.דרכי מינוי עובדים וכשירות עובד ביקורת (תיקון: תשל"ט, תש"ן, תשנ"ה, תשס"א, תשס"ב, תשס"ג, תשס"ד, תשס"ה)

(א) ראש העיריה רשאי למנות לעיריה עובדים שלא הוזכרו בסעיף 167 למשרות שיש עליהן הקצבה בתקציב המאושר.

(ב) לא יתמנה אדם לעובד עיריה, לרבות למשרות המנויות בתוספת החמישית, למעט המנהל הכללי, אלא לאחר שראש העיריה או מי שהוא הסמיך לכך הכריז על המשרה בפומבי על פי כללים לפי סעיף קטן (ג).

(ב1)(1) במהלך מינוי למשרה המנויה בתוספת החמישית או למשרת פקח תונח לפני ועדת המכרזים הדנה בענין, חוות דעתו של היועץ המשפטי של העיריה בדבר קיום הרשעה של המועמד בעבירה שבשל אופייה, חומרתה או נסיבותיה אין הוא ראוי לשמש בתפקיד; במהלך מינוי למשרת יועץ משפטי תונח לפני ועדת המכרזים לבחירת עובדים בכירים חוות דעת כאמור, על ידי היועץ המשפטי של משרד הפנים; החליטה ועדת המכרזים בניגוד לחוות דעתו של היועץ המשפטי, תחליט המועצה בענין מינוי אדם למשרה כאמור; בפסקה זו, "פקח" - לרבות נושא משרה בעיריה הממלא תפקידי פיקוח;

(2) שר הפנים, בהתייעצות עם השר לביטחון הפנים ושר המשפטים, ובאישור ועדת הפנים ואיכות הסביבה של הכנסת רשאי לקבוע בעלי תפקידים נוספים שלגביהם תידרש חוות דעת היועץ המשפטי של העיריה כאמור בפסקה (1);

(3) השר לביטחון הפנים בהתייעצות עם שר המשפטים ובאישור ועדת הפנים ואיכות הסביבה של הכנסת יקבע דרכי מסירת מידע בדבר קיום הרשעה של מועמד כאמור בסעיף זה.

(ג) השר, באישור ועדת הפנים ואיכות הסביבה של הכנסת, יקבע בתקנות כללים בדבר דרכי מכרז ופרטיו, אם בדרך כלל ואם לסוגי משרות, ורשאי הוא בתקנות כאמור לקבוע משרות וסוגי משרות שעליהן לא תחול, בתנאים שיקבע, חובת מכרז.

(ד) לא תחול חובת מכרז לפי סעיף קטן (ב) על משרות שלהן מתקבל אדם באמצעות לשכת תעסוקה לפי חוק שירות התעסוקה, תשי"ט-1959.

(ה) ראש העיריה בהסכמת מבקר העיריה ימנה עובדים ללשכת מבקר העיריה בהתאם לתקנים שיקבע שר הפנים בתקנות ועל- פי האמור בהוראות סעיפים קטנים (א) עד (ד). תקנים לפי סעיף קטן זה ייקבעו בידי השר בהתחשב במספר התושבים, בתחומה של העיריה ובגודל תקציבה השנתי.

(ה1)לא ימונה עובד ולא יכהן אדם כעובד ביקורת בלשכת מבקר העיריה אלא אם כן התקיימו בו הוראות סעיף 167(ג)(1) עד (4).

(ה2)על אף הוראות סעיף קטן (ה1), רשאי ראש העיריה, בהסכמת מבקר העיריה, לאשר מינויו של אדם אשר לא נתמלא בו התנאי האמור בסעיף 167(ג)(4) אם רכש ניסיון במשך שבע שנים בעבודת ביקורת בגוף ציבורי כמשמעו בחוק הביקורת הפנימית, תשנ"ב-1992.

(ו)עובדי לשכת מבקר העירייה דינם כשאר עובדי העירייה, ואולם הם יקבלו הוראות מקצועיות ממבקר העיריה בלבד.

(ז) לא יופסק שירותו של עובד אצל מבקר העיריה, שלא בהסכמתו של מבקר העיריה, אלא בכפוף להוראות סעיף 171א(1).

(ח) בסעיף זה, "עובד ביקורת" - עובד המבצע פעולת ביקורת.

170א. (א) ואלה תפקידי המבקר: (תשל"א, תשל"ט, תש"ן, תשנ"ה, תשס"ב)

(1) לבדוק אם פעולות העיריה, לרבות פעולות לפי חוק התכנון והבניה, תשכ"ה- 1965, נעשו כדין, בידי המוסמך לעשותם, תוך שמירת טוהר המידות ועקרונות היעילות והחסכון;

(2) לבדוק את פעולות עובדי העיריה;

(3) לבדוק אם סדרי הבחון והוראות הנוהל הנהוגים בעיריה מבטיחים קיום הוראות כל דין, טוהר המידות ועקרונות היעילות והחסכון;

(4) לבקר את הנהלת חשבונות העיריה ולבדוק אם דרכי החזקת כספי העיריה ושמירת רכושה והחזקתו מניחות את הדעת.

(ב) הבקורת לפי סעיף קטן (א) תיעשה גם לגבי המועצה הדתית שבתחום העיריה וכן לגבי כל תאגיד, מפעל, מוסד, קרן או גוף אשר העיריה משתתפת בתקציבם השנתי כדי יותר מעשירית לגבי אותה שנת תקציב או משתתפת במינוי הנהלתם. למי שעומד לבקורת לפי סעיף קטן זה ייקרא להלן "גוף עירוני מבוקר".

(ג) בכפוף לאמור בסעיף קטן (א), יקבע המבקר את תכנית עבודתו השנתית, את נושאי הביקורת בתקופה פלונית ואת היקף הביקורת -

(1) על פי שיקול דעתו של המבקר;

(2) על פי דרישת ראש העיריה לבקר ענין פלוני;

(3) על פי דרישת הועדה לעניני ביקורת, ובלבד שמספר הנושאים לביקורת לא יעלה על שני נושאים לשנת עבודה.

(ד) המבקר יקבע על פי שיקול דעתו את הדרכים לביצוע ביקורתו.

(ה) מבקר העיריה יכין ויגיש לראש העיריה מדי שנה הצעת תקציב שנתי ללשכתו, לרבות הצעת תקן, במסגרת הכנת התקציב לפי הפקודה. היקף הצעת התקציב לא יפחת משיעור קבוע באחוזים מהתקציב השנתי של העיריה, כפי שיקבע השר בהתחשב במספר התושבים בתחומה של העיריה ובגודל תקציבה השנתי.

(ו) ועדת הכספים והמועצה ידונו בהצעות התקציב והתקן של לשכת מבקר העיריה, כפי שהגיש אותן מבקר העיריה, במסגרת דיוניהן בהצעת התקציב השנתי.

170ב. המצאת מסמכים ומסירת מידע (תשל"א, ,תשל"ט, תש"ן, תשס"ב)

(א) ראש העיריה וסגניו, חברי המועצה, עובדי העיריה, ראש המועצה הדתית וסגניו, חברי המועצה הדתית, עובדי המועצה הדתית, וחברים ועובדים של כל גוף עירוני מבוקר, ימציאו למבקר העיריה, על פי דרישתו, כל מסמך שברשותם אשר לדעת מבקר העיריה דרוש לצרכי הביקורת ויתנו למבקר העיריה כל מידע או הסבר שיבקש בתוך התקופה הקבועה בדרישה ובאופן הקבוע בה.

(ב) למבקר העיריה או עובד שהוא הסמיך לכך תהיה גישה, לצורך ביצוע תפקידו, לכל מאגר מידע רגיל או ממוחשב, לכל בסיס נתונים ולכל תוכנת עיבוד נתונים אוטומטי של העיריה או של המשרתים את העיריה או של גוף עירוני מבוקר.

(ג) לגבי מידע החסוי על- פי דין, יחולו על מבקר העיריה ועל עובדים מטעמו המגבלות הקבועות בחוק או לפיו לגבי המורשים לטפל באותו מידע.

(ד) עובדו של מבקר העיריה שאינו עובד העיריה, יחולו עליו, לענין עבודתו האמורה, כל איסור והגבלה החלים על עובד הציבור שהוא עובד מבקר העיריה.

(ה) לצורך ביצוע תפקידו יוזמן מבקר העיריה ויהיה רשאי להיות נוכח בכל ישיבה של מועצת העיריה או כל ועדה מועדותיה או כל ועדה מועדותיו של גוף עירוני מבוקר; בישיבה שאינה סגורה רשאי הוא להיות נוכח אף על ידי עובד מעובדיו.

170ג. דו"ח המבקר (תיקון: תשל"א, תשל"ט, תש"ן, תשס"ב)

(א) המבקר יגיש לראש העיריה דוח על ממצאי הביקורת שערך; הדוח יוגש אחת לשנה, לא יאוחר מ- 1 באפריל של השנה שלאחר השנה שלגביה הוגש הדוח; בדוח יסכם המבקר את פעולותיו, יפרט את הליקויים שמצא וימליץ על תיקון הליקויים ומניעת הישנותם בעתיד; בעת הגשת הדוח לפי סעיף קטן זה, ימציא המבקר העתק ממנו לועדה

לעניני ביקורת; אין בהוראות סעיף קטן זה כדי לפגוע בהוראות סעיפים 21א ו- 21ב לחוק מבקר המדינה, תשי"ח- 1958 [נוסח משולב].

(ב) בנוסף לאמור בסעיף קטן (א) רשאי המבקר להגיש לראש העיריה ולועדה לעניני ביקורת דו"ח על ממצאי ביקורת שערך בכל עת שייראה לו או כאשר ראש העיריה או הועדה לעניני ביקורת דרשו ממנו לעשות כן.

(ג) תוך שלושה חדשים מיום קבלת דו"ח המבקר יגיש ראש העיריה לועדה לעניני ביקורת את הערותיו על הדו"ח וימציא לכל חברי המועצה העתק מהדו"ח בצירוף הערותיו.

(ד) הועדה לעניני ביקורת תדון בדו"ח המבקר ובהערות ראש העיריה עליו ותגיש למועצה לאישור את סיכומיה והצעותיה תוך חדשיים מיום שנמסרו לה הערות ראש העיריה כאמור בסעיף קטן (ג). לא הגיש ראש העיריה את הערותיו על הדוח עד תום התקופה האמורה, תדון הועדה בדוח המבקר ותגיש למועצה לאישור את סיכומיה והצעותיה עד תום חמישה חודשים ממועד המצאתו על ידי מבקר העיריה לועדה; בטרם תשלים הועדה את סיכומיה והצעותיה רשאית היא, אם ראתה צורך בכך, לזמן לדיוניה נושאי משרה של העיריה או של גוף עירוני מבוקר כדי לאפשר להם להגיב על הדו"ח.

(ה) (1) תוך חדשיים מן היום שהגישה הועדה את סיכומיה והצעותיה תקיים המועצה דיון מיוחד בהם ובדוח המבקר ותחליט בדבר אישור הסיכומים או ההצעות כאמור;

(2) לא הגישה הועדה את סיכומיה והצעותיה לחברי המועצה עד תום התקופה כאמור בסעיף קטן (ד), או לא המציא ראש העיריה לכל חברי המועצה העתק מהדוח בצירוף הערותיו, ימציא המבקר עותק הדוח לכל חברי המועצה והמועצה תדון בדוח ובהמלצותיו לא יאוחר משבעה חודשים ממועד הגשתו לראש העיריה.

(ו) לא יפרסם אדם דו"ח מן האמורים בסעיף זה או חלק ממנו או תכנו, לפני שחלף המועד שנקבע להגשתו למועצה, ולא יפרסם ממצא בקורת של מבקר העיריה, ואולם מבקר העיריה או ראש העיריה רשאי, באישור הועדה, להתיר פרסום כאמור.

(ז) היה למבקר העיריה יסוד להניח שראש העיריה או היועץ המשפטי של העיריה, הוא צד לעשיית עבירה לפי הוראות פרק ה' סימן ב' לחוק העונשין, תשל"ז- 1977, יעביר המבקר את הענין במישרין לידיעת מבקר המדינה.

170ג1. חומא שאינו ראיה (תיקון: תשס"ב)

דוחות המבקר, חוות דעת או כל מסמך אחר שהוציא או שהכין מבקר העיריה במילוי תפקידו, לא ישמשו ראיה בכל הליך משפטי, אך לא יהיו פסולים בשל כך לשמש ראיה בהליך משמעתי.

170ג1א. צוות לתיקון ליקויים (תיקון: תשס"ה)

(א) בסעיף זה, "הצוות" – עובדי העיריה החברים בצוות לתיקון ליקויים, שמונה לפי הוראת סעיף 21א(ב) לחוק מבקר המדינה, התשי"ח-1958 [נוסח משולב] (בסעיף זה – חוק מבקר המדינה).

(ב) הצוות ידון בדרכים ובמועדים לתיקון ליקויים שנמצאו בדוח שהגיש מבקר העיריה ושנדון על ידי המועצה לפי סעיף 170ג(ה)(1) או (2), לפי הענין, ובדרכים למניעת הישנותם של ליקויים בעתיד.

(ג) הצוות יגיש את המלצותיו לראש העיריה בתוך שלושה חודשים מיום שדוח מבקר העיריה נדון על ידי המועצה, וידווח לוועדה לעניני ביקורת על יישום המלצותיו אחת לשלושה חודשים.

(ד) ראש העיריה רשאי לדחות את תיקונו של ליקוי מסוים, ובלבד שינמק דחיה זו לפני מבקר העיריה והוועדה לעניני ביקורת, בכתב, לא יאוחר משלושה חודשים לאחר שהוגשו לו המלצות הצוות.

(ה) אין בהוראות סעיף זה כדי לגרוע מהוראות סעיפים 21א ו-21ב לחוק מבקר המדינה.

21א. דיון בתיקון הליקויים (תיקון:תשס"א)
(א) בסעיף זה "ראש הגוף המבוקר"- כל אחד מאלה:
(1) בגוף מבוקר לפי סעיף 1 (9) או (2)- השר אחראי על אותו גוף;
(2) בגוף מבוקר לפי סעיף 4 (9)- ראש הרשות המקומית
(3) בגוף מבוקר אחר 0 הדריקטוריון או גוף מקביל לו בגוף המבוקר.
(ב) בכל גוף מבוקר ימנה ראש הגוף המבוקר צוות לתיקון ליקויים. שבראשו יעמוד המנהל הכללי באותו גוף ובאין מנהל כללי – בעל התפקיד במקביל לו באותו הגוף (להלן – הצוות).

171. פיטורי עובדים בכירים (תיקון: תשל"ח, תשל"ט, תש"ן, תשס"ב, תשס"ד, תשס"ה)

(א) בכפוף להוראות סעיף זה, עובד העיריה שנתמנה לפי סעיף 167(א) לא יפוטר, אלא אם כן, לפי המלצת ראש העיריה, הוחלט על כך בישיבת המועצה, לאחר שניתנה הודעה כדין לכל חברי המועצה שדבר הפיטורים יידון באותה ישיבה.

(א1)מנהל כללי שנתמנה לפי סעיף 167(א2), רשאי ראש העיריה לפטרו.

(ב) (1) לא יפוטר היועץ המשפטי לעיריה שהוא עובדה או הגזבר, אלא לפי המלצת ראש העיריה ובאישור המועצה ברוב של שני שלישים מחבריה, לאחר שניתנה הודעה כדין לכל חברי המועצה שדבר הפיטורים יידון באותה ישיבה;

(2) לא יפוטר מבקר העיריה שהוא עובדה, אלא באישור המועצה ברוב של שלושה רבעים מחבריה, לאחר שניתנה הודעה כדין לכל חברי המועצה שדבר הפיטורים יידון באותה ישיבה.

(ג) לא תתקבל במועצה החלטה לפיטוריו של מבקר העיריה, הגזבר או היועץ המשפטי לעיריה אלא לאחר שניתנה להם זכות לשאת לפני המועצה את דברם בענין הפיטורים.

(ג1) (1) החליטה המועצה לפטר גזבר כאמור בסעיף קטן (ב)(1) וסבר הגזבר כי ההחלטה לפטרו התבססה על טעמים שאינם ענייניים, רשאי הוא לפנות לועדה שימנה השר לענין סעיף קטן זה בבקשה לבחון את החלטת המועצה; בועדה יהיו חברים נציגי השר ונציגי שר האוצר שימנו השרים מבין עובדי משרדיהם, ושמספרם ייקבע בידי השר; נוכחה הועדה לאחר שנתנה הזדמנות לראש העיריה להשמיע את טענותיו, שהחלטת המועצה אינה נובעת משיקולים ענייניים, רשאית היא לבטל את החלטת המועצה.

(2) הועדה האמורה בפסקה (1) רשאית, מיזמתה או לבקשת ראש העיריה, לבדוק האם פעל גזבר שלא בהתאם להוראות פקודה זו או להוראות כל דין; מצאה הועדה כי גזבר פעל כאמור, רשאית היא, לאחר שנתנה לגזבר הזדמנות להשמיע את טענותיו, להמליץ לפני מועצת העיריה לפטר את הגזבר; ראש העיריה יכנס, בתוך 14 ימים מיום קבלת המלצת הועדה כאמור, ישיבת מועצה לענין פיטוריו של הגזבר, שבה תינתן לגזבר הזדמנות להשמיע את טענותיו; החלטת המועצה לפיטוריו של הגזבר לפי פסקה זו תתקבל, על אף הוראות סעיף קטן (ב)(1), ברוב של חברי המועצה הנוכחים באותה ישיבה; לא החליטה המועצה על פיטוריו של הגזבר, רשאי השר להורות על פיטוריו לאחר ששקל את החלטת המועצה.

(ד) הוראות סעיפים קטנים (ב), (ג) ו-(ג1) יחולו, בשינויים המחוייבים, גם על השעיית מבקר העיריה, הגזבר או היועץ המשפטי לעיריה.

(ה) האמור בסעיף זה אינו בא לגרוע מסמכותו של בית דין למשמעת לפי חוק הרשויות המקומיות (משמעת), תשל"ח- 1978, לפסוק בדבר פיטוריו של עובד עיריה שסעיף זה דן בו, בשל עבירת משמעת כמשמעותה בחוק האמור.

173א. תקנות לענין תנאי כשירות ופסלות לכהונה (תיקון: תשס"ד)

השר רשאי לקבוע תנאי כשירות ופסלות לכהונה לעובדי עיריה ולנושאי משרה בה, וכן לעובדים בתאגיד עירוני כהגדרתו בסעיף 249א ובחברה עירונית מיוחדת כהגדרתה בסעיף 249ב, ורשאי הוא לקבוע תנאים כאמור לפי סוגי משרות ותפקידים; לענין זה, "עובד" – לרבות עובד ארעי, עובד זמני ועובד על פי חוזה מיוחד.

216. עריכת דוחות כספיים (תיקון: תשנ"ז, תשנ"ט, תשס"א, תשס"ה)

(א) עיריה תערוך דוחות כספיים שנתיים וחצי שנתיים (להלן — דוחות כספיים); ראש העיריה והגזבר יחתמו על הדוחות הכספיים; רואה החשבון יבקר את הדוחות הכספיים השנתיים ויסקור את הדוחות הכספיים החצי שנתיים (להלן — דוחות מבוקרים), והם יידונו בועדת הכספים ובמועצה ויוגשו לממונה על ביקורת החשבונות במשרד הפנים (להלן — הממונה על החשבונות).

(ב) תמצית הדו"חות הכספיים השנתיים הכוללת פרטים כפי שיקבעו שר הפנים ושר האוצר (בסעיף זה – תמצית הדוחות הכספיים), תפורסם בעיריה שבה קיים עיתון מקומי — בעיתון מקומי, לא יאוחר מיום 1 באוקטובר של כל שנה לענין דו"ח המתייחס לשנה הקודמת, וכן תפורסם בכל עיריה בדרך ובמועד שיקבע שר הפנים, דרך כלל או לסוגי עיריות; בסעיף זה, "עיתון מקומי" — שבועון היוצא לאור בעיריה או באזור שבו נמצאת העיריה, המיועד לרוב תושבי העיריה.

(ג) לא פרסמה העיריה בעיתון מקומי את תמצית הדו"חות הכספיים כאמור בסעיף קטן (ב) עד יום 1 באוגוסט, יפרסם הממונה על החשבונות את תמצית הדו"חות, על חשבון העיריה.

(ד) בלי לגרוע מהאמור בסעיף קטן (ב), העיריה תשלח או תפרסם את תמצית הדוחות הכספיים, לא יאוחר מיום 1 באוקטובר של כל שנה לענין דוח המתייחס לשנה הקודמת באחד מאלה:

(1) בדואר לכל מחזיק כהגדרתו בסעיף 269;

(2) בעיתון יומי אשר רווח במדינה ושהוא מיועד לאופי מרבית האוכלוסיה באותה עיר.

(ה) לא שלחה העיריה או לא פרסמה את תמצית הדוחות הכספיים כאמור בסעיף קטן (ד), רשאי הממונה על החשבונות לשלוח או לפרסם את תמצית הדוחות, על חשבון העיריה.

217. דוחות כספיים (תיקון: תשנ"א, תשנ"ז)

השר ושר האוצר יקבעו את מתכונת הדוחות הכספיים, היקפם, הפרטים הכלולים בהם ומועדי הגשתם לממונה על החשבונות, וכן את המועד להגשת הדוחות המבוקרים.

218. תנאי העסקה ואי- תלות (תיקון: תשנ"ז)

(א) רואה החשבון לא יהיה עובד העיריה; תנאי העסקתו ייקבעו בידי המועצה, בהתאם לסימן זה.

(ב) רואה החשבון יהיה בלתי תלוי בעיריה, בין במישרין ובין בעקיפין, וישמור על אי תלות בעבודתו המקצועית.

(ג) תשלום שכר טרחתו של רואה החשבון לא יותנה בתנאי כלשהו הקשור לאחריותו המקצועית, ולא ייקבע כל הסדר לשיפוי רואה החשבון בידי העיריה או מי מטעמה בשל חיוב שמקורו בהפרת אחריותו המקצועית של רואה החשבון או באי קיום חובה המוטלת עליו לפי כל דין.

219. סמכויותיו, חובותיו ואחריותו של רואה החשבון (תיקון: תשנ"ז)

(א) לצורך מילוי תפקידיו רשאי רואה החשבון, בכל עת, לעיין במסמכי העיריה ולדרוש מאת ראש העיריה, מחבר המועצה, מעובד העיריה או מכל בעל תפקיד בה, כל מידע והסבר הדרושים לו וכן רשאי הוא לדרוש כל מסמך של העיריה מאת המחזיק בו.

(ב) רואה החשבון יוזמן להשתתף בכל ישיבה של המועצה ושל ועדת הביקורת, אשר בה יידונו חשבונות שביקר או שמסר עליהם דין וחשבון, ויהיה רשאי למסור כל הודעה או

הסבר שנראה לו בנוגע לאותם חשבונות.

(ג) היה סבור רואה החשבון, אגב עריכת הביקורת, כי יש בפעולות העיריה משום סטיה מהוראות חוק יסודות התקציב, תשמ"ה–1985, ידווח על כך לממונה על החשבונות; התפטרות או פרישה של רואה החשבון מתפקידו או הפסקת העסקתו אין בהם כדי לפטור אותו מקיום חובתו לפי סעיף קטן זה.

(ד) מי שנדרש כאמור בסעיף זה, חייב למלא אחר הדרישה.

219א. כללים למינוי רואה חשבון (תיקון: תשנ"ז)

השר ושר המשפטים, בהתייעצות עם שר האוצר, יקבעו כללים בדבר מינוי רואה חשבון לפי סימן זה, תנאי כשירותו, אי-תלות, העדר ניגודי עניינים, שכרו ודרכי פעולתו, וכן נוהל להפסקת העסקתו של רואה החשבון והגבלות על פיטוריו בידי המועצה.

219ב. סמכויות השר (תיקון: תשנ"ז)

(א) ראה השר כי עיריה אינה ממנה רואה חשבון או אינה מגישה דוחות כספיים במועדים או במתכונת הקבועים לפי סימן זה, רשאי הוא לעשות אחד או יותר מאלה:

(1) למנות רואה חשבון לעיריה ולקבוע הוראות לפעולתו, לרבות השכר שתשלם לו העיריה;

(2) לקבוע כי לא יועבר לעיריה תשלום חובה כמשמעותו בחוק הרשויות המקומיות (העברת תשלומים מהמדינה), תשנ"ה–1995, וכי סעיף 2 לחוק האמור לא יחול, לתקופה כפי שיקבע;

(3) לשלם, על חשבון העיריה, את שכרו של רואה החשבון.

(ב) השר רשאי למנות לעיריה גם רואה חשבון מטעמו שיבקר את הדוחות הכספיים, כולם או חלקם, כפי שיקבע, והוראות סעיף 219(א) ו-(ד) יחולו.

220. פעולות לפי דרישת הממונה על החשבונות (תיקון: תשנ"ז)

הממונה על החשבונות רשאי לדרוש מרואה החשבון כל מידע, מסמך והסבר על פעולתו ועל פעולות העיריה שבידיעת רואה החשבון, וכן רשאי הוא לדרוש השלמות ותיקון ליקויים בדוחות הכספיים.

221. אישור תשלום וחיוב על תשלום אי-חוקי (תיקון: תשנ"ז)

על פי עצתו של רואה החשבון בפעולתו לפי סימן זה, יפסול הממונה כל פריט בחשבון שהוא בניגוד לדין, ויחייב בו את האדם ששילם או שהרשה את התשלום הבלתי חוקי, וכן יחייב הממונה כל אדם האחראי לחשבון בכל סכום של חסר או הפסד שנגרמו בשל התרשלותו או התנהגותו הרעה או בכל סכום שהיה צריך להביא בחשבון ולא הביא, ובכל מקרה כזה יאשר בכתב את הסכום המגיע מאותו אדם; הממונה יפרש בכתב את טעמי החלטתו בדבר הפסילה או החיוב וכן בדבר כל סכום שהכשיר, אם נתבקש לכך על ידי מי שנפגע בהחלטתו זו.

225. פסק- הדין בתביעת העירייה

(ב) הסכום שנגבה בדרך זו על ידי העיריה ישולם מיד לקופת העיריה.

227. הפסקת העסקה על ידי השר (תיקון: תשנ"ז)

השר רשאי להפסיק העסקתו של רואה חשבון אם מצא שרואה החשבון אינו ממלא את תפקידיו כראוי, או אם מצא שלא מתקיימים בו תנאי הכשירות הנדרשים לפי סימן זה.

334א. פרסום דו"ח ביקורת או ממצא ביקורת (תיקון: תש"ן)

המפרסם דו"ח או חלקו או תכנו או ממצא ביקורת, ומפר בכך את סעיף 170ג(ו) או תנאי בהיתר שניתן לו לפי הסעיף האמור, דינו - מאסר שנה.

347. תקנות (תיקון: תש"ן)

השר רשאי להתקין תקנות בכל ענין הנוגע לביצועה של הפקודה. תקנות כאמור לענין פעולתו של מבקר העיריה או לענין הטיפול בדו"ח שהוא מגיש טעונות אישור הועדה לעניני ביקורת המדינה של הכנסת.

פקודת העיריות (נוסח חדש)

פרק רביעי: זימון ישיבות

17. זימון בעלי תפקידים (תיקון: תשס"ד)

מרכז ישיבות המועצה יזמן לישיבות המועצה, מן המניין ושלא מן המניין, את עובדי העיריה כאמור להלן:

(1) עובד עיריה המתמנה על פי חיקוק או על פי סעיף 167 לפקודה;

(2) עובד עיריה שהמועצה קבעה כי הנושא הנדון בישיבה נוגע לתפקידו;

(3) עובד, הכפוף באופן ישיר לראש העיריה או למנהל הכללי של העיריה, שהוזמן, על פי דרישה בכתב של חבר המועצה למזכיר, 24 שעות לפני מועד הישיבה.

פרק שני- עשר: דיונים מיוחדים

57. דינים וחשבונות, הצעות תקציב והיטלי ארנונות (תיקון: תשמ"א, תש"ן)

(א) ראש עיריה יקבע מועד לדיון מיוחד בדוח השנתי והדוח החצי שנתי כאמור בסעיף 216 לפקודה, שיהיה, לכל המאוחר, חודש לאחר הגשתו; הדיון בדוח מבקר העיריה ובדוח מבקר המדינה, יהיה באופן ובמועדים הקבועים בסעיף 170ג לפקודה.

(ב) ראש עיריה יקבע מועד לדיון מיוחד בהצעת התקציב ובתשלומי החובה, שיתקיים בישיבות שלא מן המניין.

(ג) ראש עיריה יגיש למועצה פעם בשנה לפחות דוח על המצב בכל תאגיד שהעיריה משתתפת בו, ולפי דרישה של חבר המועצה יקוים דיון בדוח זה.

(ד) סעיף 6(א) לתקנון זה לעניין ימי השבוע יחול גם על דיונים לפי סעיף זה.

58. ישיבות בעניינים מיוחדים

(א) בישיבות בעניינים המפורטים בסעיף 57 לתקנון זה (בסעיף זה – עניין מיוחד), יפתח היושב ראש, או מי שהוא יורה, בדברי ההסבר, ובכפוף לאמור בסעיף 48 לתקנון זה, תקבע המועצה בעצמה את משך הזמן שיוקדש לדיון; ואולם שליש מחברי המועצה רשאי לדרוש שהזמן שיוקדש לדיון בהצעת התקציב לא יפחת משש שעות; הוראות סעיף 48 לתקנון זה לא יחולו על ישיבות בנושא התקציב.

(ב) בישיבה הראשונה בעניין המיוחד לא יידון כל דבר אחר מלבד אותו עניין מיוחד.

תוספת חמישית (תיקון: תשס"ה)

(סעיף 167 (א2)

ועדת המכרזים לבחירת עובדים בכירים – רשימת המשרות:

(1) מנהל כללי;

(2) מזכיר;

(3) מהנדס;

(4) רופא וטרינר;

(5) היועץ המשפטי;

(6) מנהל מחלקת חינוך;

(7) מבקר;

(8) גזבר.

תקנות העירייה

(הסדר רכישות, ניהול מחסנים, רישום וניהול טובין), התשנ"ח- 1998

26. ספירת מלאי

(א) אחת לשנה לפחות, בסוף שנת הכספים, ליערך ספירת המלאי (להלן הספירה) בכל מחסני העירייה; מנהל הרכש ואספקה אחראי לספירה שתערך בפיקוח מבקר העירייה, ובהשתתפות הגזבר.

(ב) בעת ספירת המלאי ייסגרו מחסני העירייה לכניסה של טובין ולהוצאתם מהם, למעט במקרים חריגים ובאישור מנהל רכש ואספקה.

(ג) תוצאות הספירת יירשמו בטפסים המיועדים לכך ויכללו את מספרם הקטלוגי של הפריטים, תיאורם והכמויות בפועל שנמצאו במחסן בעת הספירה; מבצעי הספירה יחתמו על הטפסים.