המועצה המקומית קרית-יערים (טלזסטון)

בס״ד

לכבוד

הרב יצחק רביץ - ראש המועצה

הנידון: **<u>דוח מבקרת המועצה לשנת 2023</u>**

על פי הוראות סעיף 170ג לפקודת העיריות, שהוחל על פקודת המועצות , הנני מתכבדת להגיש בזאת את דו״ח על ממצאי הביקורת שערכתי בשנת 2023 .

הביקורת בשנת 2023 עסקה בנושאי אבטחת מידע, , בחלוקת קמחא דפסחא, ובניהול הידע. הדוחות נידונו בועדת הביקורת ובמועצה, וההמלצות אומצו על ידי ועדת הביקורת ועל ידי מליאת המועצה.

אני רואה חובה נעימה לציין את שיתוף הפעולה המלא לו זכיתי מגזבר המועצה, מנכ״ל המועצה מנהלי מחלקות ועובדים שונים אליהם פנתה הביקורת. הדבר מבטא את תפיסתם את הביקורת הפנימית ככלי ניהולי שמטרתו לשפר ולייעל את הארגון. שיתוף פעולה זה מניב תוצאות חיוביות וטיפול יעיל בכל הנושאים שמעלה הביקורת ואף תיקון חלק מהליקויים עוד במהלך הכנת הדוח.

בברכה,

דליה קליימן, רו״ח, C.I.A., M.B.A,

מבקרת המועצה

המועצה המקומית קרית יערים

דו"ח ביקורת בנושא ניהול הידע

אוקטובר 2023

תוכן

תוכן עניינים

רקע והקדמה

כללי

ניהול הידע הוא תורה ניהולית המבוססת על ההבנה כי הידע מהווה משאב חשוב וחיוני, עם השלכות רוחביות רבות, שיש לנהלו בקפידה ובתבונה, בדומה לכל תהליך ומשאב בארגון. הניהול של הידע מתמקד באופן מקיף בכל שלביו: זכרון ארגוני וידע הסטורי, דרך תיעוד נכון של מסמכים, נתונים וידע עכשווי שנוצר באופן שוטף, ועד הדגרה וניהול של ידע חדש, דרך יישומו ועד לשימוש מחדש ואפילו לחידושו על מנת לשפר את ביצועי הארגון.

שיטה מקובלת בניהול הידע הוא התמקדות בידע הליבה, כלומר הידע שמשפיע ישירות על מיטוב המטרות הארגוניות. ניהול הידע הוא עשיה מתמשכת העוסקת בלמידה ובשיפור תהליכי העבודה באורך וברוח הזמן. בסביבת עבודה דינמית חשוב לנהל מידע בצורה שתקטין תלות בעובדים ספציפיים וביותר, תקטין תלות בנסיון ומידע שנצבר על ידם ולא תועד.

ברמת הרשות המקומית, חשוב מאד הרצף התפקודי, שנשען גם על מידע מצטבר במחלקות השונות שנאסף לאורך השנים.

הביקורת בוצעה על מנת לאמוד את תהליכי העבודה הנוגעים לניהול המידע והידע ברשות, לזהות את האתגרים והפערים ולגבש המלצות לשיפור וקידום התהליכים באופן יעיל, כדי לשמר את הידע ולמנוע תקלות הנובעות ממידע חסר.

בשל השלב הבוסרי בו נמצאת המועצה בהתייחס לניהול הידע, התמקדה הביקורת בשלב ראשון בניהול מסמכים (מסמכי עבר ומסמכים שוטפים), וניהול קבועי זמן.

כבר לפני כעשרים שנה, התריע מבקר המדינה על ניהול לקוי (או אי ניהול) של תהליכי הארכוב במשרדי הממשלה וברשויות המקומיות.

עיקרי הממצאים וההמלצות

ניהול הידע של המועצה לא מבוצע בצורה מתוכננת, והראיה לגביו היא לא מתכללת. המידע מבוזר, נשמר בצורה לא אחידה, ונדרשת החלטה ארגונית על צורת הניהול של ידע ומסמכים במחלקות השונות.

כמו כן, העבטח קבועי זמן (עמידה במטלות שמוגבלות בזמן), מנוהלת היום על ידי העובד הממונה לפי צורת עבודה שגיבש לעצמו.

הביקורת ממליצה על חשיבה וקשב ניהוליים לתחומים אלו, ובחינת האפשרות להיעזר בכלים טכנולוגיים, מערכות תומכות (כגון Monday), המתממשקות למערכות המועצה, כדי לארגן את הידע לתועלת המועצה העכשווית והעתידית, ולמניעת נזקים, וכדי לוודא שהעבודה השוטפת מנוהלת בצורה שתוודא שמטלות שבועות בזמן תבוצענה במועד, וכי

תהיה מערכת התראות מראש על מועד מתקרב, על היות המטלה בטיפול, וגיבוי במקרה שהעובד איננו או אינו מבצע.

בדו"ח מוזכרות דוגמאות שהינן רק כדי להדגים את חשיבות הנושא. תחום זה ארוג ושזור בעבודה השוטפת של הרשות המקומית ולא ניתן להגזים בחשיבותו.

לוח זמנים:

הביקורת נערכה בחודשים פברואר- אוקטובר, 2023

הליך הביקורת

הביקורת כללה:

- ישיבות עם גורמים רלוונטיים במועצה
- בחינת מסמכים מהארכיב וקלסרי הנדסה וגזברות ישנים
- בחינת תיוק מסמכים במחלקות השונות
- בחינת מסמכים ותיעוד במשרדי המועצה

זיכרון ארגוני

כיום, דה פקטו, הזיכרון הארגוני ארוך הטווח, אינו מסודר וממוסמך, ומתבסס בעצם על זכרונו של הגזבר יחד עם עוד עובדים ותיקים בודדים.

הזכרון הארגוני קצר הטווח, ממוסמך ומתויק בצורה לא אחידה ולא בהכרח נגישה לכל מי שנדרש לידע זה, כמו שיפורט להלן.

ארכיב המועצה

למועצה ארכיב, בו מתוייקים קלסרים המכילים מסמכים ממחלקות שונות, מהשנים האחרונות.

מסמכי חלק מהמחלקות מתוייקים בצורה שיטתית, ומסמכי מחלקות אחרות בצורה אקראית וספורדית.

על הארגזים מצויינים תוכנם הכללי של הארגזים, אולם אין אינדקס של הארגזים השונים או הקלסרים שבתוכם.

הארכיב נעול, והמפתח מצוי בידי מנהל הארכיב.

בארכיב אין ספרינקלרים, ויש מטף כיבוי בצמוד לכניסה לארכיב.

בחדר הגזבר יש קלסרים עם מסמכים הסטוריים או בעלי חשיבות, לפי שיקול דעת הגזבר ושיטת התיוק שלו. חדר הגזבר אינו נעול, ואין אמצעי הגנה מאש.

במחלקת הנדסה ישנם תיקים לכל תב"ע. את העתקי התבע"ות ניתן למצוא גם באתר רישוי זמין ובועדה המרחבית הראל.

הלכה למעשה, לארכיב אין חשיבות רבה, כיוון שאין שיטתיות ברב התיוק. וקשה עד בתלי אפשרי יהיה לאתר מסמכים משנים קודמות.

תיוק בכוונני רשת של המועצה

עובדים המבקשים לתייק מסמכים סרוקים או קבצים אלקטרוניים אחרים, יכולים לתייק אותם באחד מכוונני הרשת.

חל איסור על תיוק או שמירת קבצים על המחשבים המקומיים, כדי לאפשר גיבוי.

כל מחלקה ואף כל עובד שומרים את המסמכים בספריות שהם מגדירים, ללא כל שיטה אחידה.

אין אחידות לשם הקבצים, או שיטה מתודולוגית בה שומרים מסמכים, או אינדקס של מסמכים קיימים.

רק למספר תיקיות מצאה הביקורת הגבלת גישה, או הגבלה על מחיקת מסמכים.

בשאר התיקיות, אין הגבלת גישה וכל עובד יכול לצפות במסמכים. יתרה מזאת, גם כל עובד יכול למחוק מסמכים ותיקיות, ללא שום תיעוד של המחיקה.

הנזק שהמועצה חשופה אליו הוא גדול, כיוון שמחיקה, אף בטעות, יכולה שלא להתגלות בזמן שמאפשר העלאה מגיבוי, או אף בכלל.

תועלות מניהול תקין של רשומות (מתוך הנחיות מבקר המדינה)

ניהול נכון של רשומות במערכות מחשב הינו בסיס טוב לתפקוד הארגון, מכיוון שהוא תומך בפעילות הארגון ומספק בסיס למתן שירות טוב.

יעילות – הרשומה הינה חלק מהזיכרון הארגוני .ניהול רשומות מאפשר הפיכת התוכן לזמין במהירות, כשנדרש לקבלת החלטות ולפעילות שוטפת. כמו כן שימוש בכלים לסילוק/ביעור של רשומות לא פעילות לפי תקופות שמירה מאפשר להתמקד בעיקר .

אחריות – יצירת רשומה שלמה ומוסמכת מאפשרת להציג ולהדגים את אחריות הארגון ופעילותו

תאימות – הרשומה נגישה, מובנת ומאוחסנת בפורמט מתאים למשתמשים ברשומה . הקטנת סיכונים שעלולים לנבוע מתקלות, פעולות בזדון או בשוגג או ביעור שלא בהתאם לתקופות השמירה של רשומות, דהיינו, פעולות שעלולות לגרום לאובדן רשומות .ומניעת גישה לא מורשית לרשומות ובכך להבטיח שמירה של התוכן מסיבות מסחריות, ביטחוניות, צנעת הפרט וכו

נגישות - הרשומה נגישה בו זמנית למספר רב של אנשים, ניתן לאתרה עפ״י קריטריונים שונים לגישה.

שמירת מאפייני מסמך לצורך אינדקס

ארכוב נאות מחייב הקמת אינדקס מתעדכן של מסמכים קיימים.
לצורך כך מומלץ לקבוע שיטה למתן שם לקבוץ, כמו גם נתונים נוספים לפי מפתח קבוע שיאפשרו איתור ואחזור בשעת הצורך

ניהול קבועי זמן

מהלך עבודה שוטפת של ארגון כדוגמת מועצה מקומית מחייב עמידה בלוחות זמנים במחזוריות קבועה, או ביצוע מטלות שתחומות בזמן.
כשל בעמידה בלוחות זמנים אלה כרוך בהשלכות קשות כמו אי עמידה בדרישות החוק, חוסר יכולת לגבות כספים, או אובדן של בטחונות או חיוב בהוצאות גבוהות, כמו שיובהר בדוגמאות להלן.
כיום, כל גורם במועצה מנסה לבנות לעצמו מערכת תזכורות, לפי העדפתו האישית.
השיטות רבות, מקוריות ומגוונות, כמו : משלוח מייל לעצמו עם תאריך עתידי, קביעת פגישה עתידית באאוטלוק, פתקים על המחשב, או פשוט זכרון אישי.
שיטות כאלה, הן מועדות לכשל, אינן נותנות מענה למקרים בהם נדרש גיבוי, ואין מעקב אחר הביצוע. בנוסף, אין שום זכרון ארגוני מובנה לגבי הנדרש, כדי להקל על תחלופות תפקידים, תחלופות עובדים, למידת עמיתים, ותהליכים ממוקדי שיפור.
כדי לוודא עמידה בקבועי הזמן, יש צורך בשיטת התראה מובנית, אחידה וכוללת. מן הראוי שהגורם האחראי יתוזכר לצורך עמידה במטלה, עם מעקב ביצוע, וגיבוי לגורמים נוספים למקרה שהגורם האחראי לא מגיב, או שהוא בחופשה/חופשת מחלה/עזב את העבודה וכדומה.

מספר דוגמאות לנחיצות הטיפול בקבועי זמן:

מכרזים

- במכרזים משמעותיים, יש ערבות בנקאית של הספק, שתקפה לשנה. חובה לחדש את הערבות או לחלט אותה לפני תום התקופה, אחרת הערבות פוקעת, והמועצה מאבדת את הערבות המהווה מנוף לחץ על הספק, ומקור לשיפוי באם יעלה הצורך.
- במכרזים יש אישורי קיום ביטוח שיש לחדשם בכל שנה. זהו מרכיב חשוב שיש לוודא שקיים בכל שנה.
- מרכזים הם מטבעם בעלי תוקף מוגבל, וניתנים לעיתים להארכה בהודעה מראש, או שנדרשת הודעה על הפסקת התקשרות, או התראה פנימית מספיק זמן מראש על צורך במכרז חדש.

חוקי עזר

- חוקי העזר הם בעלי תוקף מוגבל המוגדר בחוק.

כדי לחדש את תוקף הגביה, יש לעדכן חישובים המהווים בסיס לגביה על פי החוק, לקבל אישור חברת ג׳יגה, ולקבל אישור משרד הפנים.
זהו הליך שלוקח זמן, ולכן, יש חשיבות רבה שכל הגורמים האחראיים וגורמי גיבוי, יהיו מודעים בטווח זמן מתאים לצורך בנקיטת הצעדים הנדרשים לשמירה על תוקף הגביה.

פרסומים נדרשים, ודו"חות על פי חוק – מספר דוגמאות

- דו״ח שנתי של הממונה על חופש המידע.
- דו״ח שנתי לתושב

דוחות כספיים רבעוניים למשרד הפנים

חישובים ודיווחים וקולות קוראים

- **קולות קוראים**- קולות קוראים מטבעם הם מוגבלים בזמני ההגשה, וגם לאחר ההגשה, ובהתאם, יש מועדים קבועים להגשת דיווח ואסמכתאות על הביצוע.
- **דיווח על ביצוע פרויקטים מתוקצבים** – כל הליך הדיווח גם הוא מוגבל בזמן, ולעמידה בזמנים יש משמעות כספית מהותית.

הדוגמאות המנויות להלן הן חלק קטן (מאד) מביצוע מטלות שוטפות שמוגבלות בזמן ומבצועות באופן שוטף ורציף. ברב הדוגמאות הללו, היו או כמעט היו כשלים בעבר, וישנה חשיבות רבה להטמעת הליכי עבודה שיאפשרו מעקב אחר ביצוע המטלות, והתראות במקרים של עיכובים.

סיכום והמלצות

נדרשת חשיבה מערכתית כוללת, כדי למפות את המידע הקיים וההסטורי, ולדאוג לתייק אותו ולגבות אותו בצורה מסודרת, וגם לגבש שיטת שימור ידע אחידה שתאפשר התנהלות דומה של כל האורגנים במועצה, ואיתור מסמכים כשעולה הצורך.
יש לגבש נהלי עבודה לגבי תזכורות לקבועי זמן, עם התראות לעובדים מגבים לפי הצורך.

המועצה המקומית קרית יערים

דו"ח ביקורת – חלוקת קמחא דפסחא תשפ"ג

מאי 2023

תוכן עניינים

מבוא ועיקרי המימצאים

המועצה המקומית מחלקת בכל שנה לקראת חג הפסח, קמחא דפסחא, לתושבי הישוב הנזקקים.

התקציב לקמחא דפסחא הוא חלק מתקציב רווחה, ונקרא "משפחות במצוקה- מועצה".

בשנים קודמות חלוקת הקמחא דפסחא היתה באמצעות תווי קניה המכובדים על ידי שני המרכולים שבישוב. בשנת תשפ"ג הונפקו תווי שי המכובדים על מגוון רחב של חנויות ונותני שירותים בישוב.

שוברי קניה הינם למוכ"ז (למוסר כתב זה), כך שהם משמשים כעין הילך חוקי, דינם ככסף מזומן, ועל כן, יש לנהוג בהם בזהירות יתירה, בכל שלבי החלוקה, החל מהדפסת השוברים, שמירתם, חלוקתם, ואיסופם חזרה מהחנויות.

לוח זמנים:

הביקורת נערכה בחודשים מרץ- מאי, 2023

הליך הביקורת

הביקורת כללה:

- עיון בתקציב המועצה לשנת 2023
- בחינת תכתובות המייל בעניין תמיכות קמחא דפסחא תשפ"ג
- בדיקת קובצי מעקב קליטת הבקשות והכנת התשלומים
- ישיבות עם הגורמים שהיו מעורבים בתמיכות, הכנת השוברים והפצתם
- בחינת מסמכים ותיעוד במשרדי המועצה
- עיון בפרוטוקולים של החלטות התמיכה

תמיכות – משפחות במצוקה- מועצה

בכל שנה מאשרת מועצת הרשות במסגרת התקציב סעיף "משפחות במצוקה- מועצה", לקידום הביטחון התזונתי של משפחות מוחלשות.
עד וכולל שנת 2019, חלק מהתקציב הועבר כתמיכה בעמותות חסד.
החל משנת 2020, אוחדו שני התקציבים לסעיף "משפחות במצוקה-מועצה", והכספים מחולקים על ידי המועצה.
הביקורת השנה נערכה כמעקב לוודא שאכן הופנמו הלקחים וההנחיות לניהול תקין ונכון של הליך חלוקת תווי הקניה.

כבדיקת מעקב, נבדקה כל שרשרת הפעילות שהובילה לחלוקת השוברים.

שוברי קניה פסח תשפ"ג

כחלק מההיערכות לחלוקת תמיכות לחג הפסח, ולאור ממצאי העבר ביקשה המועצה לקבל הנחיות מפורטות כיצד לבצע חלוקה בשוברי קניה לפי כל כללי מנהל תקין, ופעלה בהתאם.
הביקורת נתנה את ההנחיות, וההמלצות העולות מדו"חות ביקורת קודמים, ועקבה בזמן אמת אחר ההליך.

שיפור מהותי בהליך ההרשמה לחלוקת קמחא דפסחא

ההרשמה לחלוקת קמחא דפסחא נעשה ברובו ע"י מילוי טופס מקוון באתר המועצה.
לינק לטופס ההשמה נשלח בקבוצות וואטסאפ של המועצה, במייל ייעודי לתושבים ובפרסומים בעיתון המקומי.
טפסים ידניים שהתקבלו הוזנו אף הם לאותה מערכת.
צורת רישום זו מנעה טעויות סופר, היתה מהירה ויעילה יותר, ואפשרה בסיס נתונים שנגיש לכל מי שטיפל בחלוקת השוברים.

שיפור בפיזור העסקים המכבדים את השוברים

בשנת תשפ"ג אפשרה המועצה לכל העסקים הפועלים בקרית יערים ומבקשים לכבד את השובר, להיכלל.

כך, 26 עסקים כבדו את שוברי קמחא דפסחא, כולל שני המרכולים היחידים בישוב, והחלוקה נעשתה בצורה שוויונית אף יותר מבחינת אפיקי הפרנסה לעסקים הפועלים בישוב.

הכנת המעטפות לחלוקה

בשנת תשפ״ג בחרה המועצה לחלק שוברים שני 20 ₪, כדי לאפשר לתושבים לחלק את קניותיהם בין העסקים השונים.
שני עובדים עסקו בחלוקת שוברים למעטפות בהתאם לרשימה שאושרה.
לאחר הכנת המעטפות, נספרו השוברים שנשארו, והסתבר שחסר סכום של 920 ₪.
ההפרש נובע ככל הנראה מטעות אנוש בהכנת המעטפות.
בזמן אמת לא נבדקו כל המעטפות מחדש.
במהלך חלוקת המעטפות, נקרעו מספר לא מבוטל של מעטפות.
עובי השוברים, ומספרם הגבוה בגלל שהיו בערך של 20 ₪, גרם לקריעה של המעטפות.

פירוט הפעולות שנעשו כראוי בחלוקת פסח תשפ"ג

- שוברי הקניה הודפסו ממוספרים מראש, כשבהזמנה ותעודת המשלוח מצוין מספר הפנקסים והשוברים.
- המועצה אפשרה ל- 26 עסקים הפועלים בישוב לכבד את שוברי הקמחא דפסחא.
- השוברים נשמרו במקום נעול.
- רישום המבקשים להיכלל בחלוקה נעשה בצורה מקוונת ואמינה
- החלוקה בהתאם לרשימות נעשתה ע״י שני עובדים.
- השוברים שמומשו נמוכים מהרשימה שגובשה ב-2,100 ₪.
- השוברים הממומשים התקבלו לאחר התאריך האחרון לשימוש.
- כשהתקבלו השוברים הממומשים, נעשתה ספירה בשניים, וסיכום חתום על הסכום שהגיע, אך השוברים לא נגרסו.
- השוברים שלא נעשה בהם שימוש, נספרו ע״י שני עובדים יחד, נערכה תרשומת חתומה, ונגרסו השוברים, בסמוך למועד החלוקה.

לקחים לשיפור לשנת תשפ"ד

- לשקול הכנת שוברים בסכומים של 100 ו- 50.
- הכנת מעטפות עבות לחלוקת תווי הקניה.

- לשקול טעינת כרטיסי התושב בסכום התמיכה, או העברת התמיכה בהעברה בנקאית.
- בדיקה כפולה של הסכומים במעטפות, אם קיימת אי התאמה לרשימות.
- להקפיד על גריסת השוברים לאחר קבלתם

הביקורת מודה על שיתוף הפעולה של כל הגורמים במועצה, הפקת הלקחים היסודית שנעשתה ע״י כל הגורמים המעורבים, והחתירה לשיפור מתמשך, בהנחיית ראש המועצה.

המועצה המקומית קרית יערים

דו"ח ביקורת בנושא אבטחת מידע במועצה המקומית

דצמבר 2023

תוכן דו''ח ביקורת בנושא אבטחת מידע

רקע והקדמה

כללי

בשנים האחרונות, אבטחת מידע הפכה צורך בסיסי לכל ארגון באשר הוא, וביותר לרשות מקומית. ככל שהזמן חולף, ועם התקדמות הטכנולוגיה והאוריינות הטכנולוגית של הציבור, הופכים התהליכים הדיגיטליים להיות ברירת המחדל של הקשר בין המועצה המקומית לתושבים. יחד עם ההזדמנויות והיתרונות שנוצרו מקלות הקישוריות וזמינות המידע, נוצר אתגר מהותי של אבטחת המידע והגנת הפרטיות.

כמו מרבית הארגונים גם המועצה המקומית קרית יערים חשופה היום, יותר מאי פעם, לנסיונות ולאיומי חדירה למאגרי המידע שלה ולהתקפה על המידע המועבר באמצעות רשתות התקשורת.

אבטחת מידע במועצה המקומית חשובה מספר סיבות מרכזיות:

הגנה על מידע אישי ומניעת שימוש לא מורשה במידע: הרשויות המקומיות מחזיקות במערכותיהן הממוחשבות מידע אישי ופיננסי חשוב, מידע על צריכת שירותים כגון השתתפות באירועי חינוך ותרבות, רישום לגני ילדים, מעונות ומשפחתונים, רישום לחוגים ואירועי חינוך בלתי פורמלי, מידע מרשויות ממשלתיות, פרטי אמצעי תשלום ועוד. מצב זה מחייב את הרשויות המקומיות לנקוט פעולות לשמירה על המידע שנמצא בידיהן ולאבטחתו.

תמיכה בתהליכי קבלת החלטות: הזנת מידע במערכות מידע מקומיות עוזרת לניהול לקבל החלטות מושכלות בנוגע למדיניות ציבורית, תכנון עירוני, תכנון צרכי ציבור במגוון תחומים ועוד. הפסקת שירותים במערכות מידע עלולה להוביל לעצירה או עיכוב תהליכים מנהליים חשובים.

הגנה על תשתיות ושירותי ציבור: רשויות מקומיות מפעילות תשתיות ושירותים חיוניים לציבור, כמו מערך תשלומי ארנונה וחיובי מים וביוב, שירותים סוציאליים, שירותי חינוך לא פורמלי ועוד. חשיפת מערכות המידע שלהן לתקיפות סייבר או גניבות מידע עשויה לגרום להפסקת שירותים חשובים לציבור.

תמיכה בחדשנות טכנולוגית: המועצה המקומית חותרת לייעול השירות ומיטביות כלכלית, גם באמצעות הנגשת טכנולוגיה ושימוש באתר המועצה לשיפור נגישות שירותים ולהפחתת הוצאות. אבטחת המידע חיונית להבטחת תהליכי דיגיטציה המבוצעים באחריות ובבטחה, ומחויבים על פי חוק.

בסיכום, אבטחת מידע ברשויות מקומיות היא חיונית להגנה על פרטיות האזרחים, למניעת שימוש לא מורשה במידע, לתמיכה בתהליכי קבלת החלטות, ולהגנה על תשתיות עליהן. השגת האיזון הנכון תוך בקרה נאותה מציבה אתגר משמעותי לפני כל ארגון.

בסיס חוקי:

הבסיס החוקי לנושא אבטחת מידע:

חוק הגנת הפרטיות התשמ"א 1981.

תקנות הגנת הפרטיות)אבטחת מידע(, תשע"ז2017.

לוח זמנים:

הביקורת נערכה בחודשים מאי-נובמבר, 2023

הליך הביקורת:

הביקורת כללה:

- ישיבות עם בעלי תפקידים רלוונטיים במועצה המקומית
- פגישות עם אחראי המחשוב ואחראי אבטחת מידע ומערכות מידע במיקור חוץ
- בדיקת רישום מאגרי המידע של המועצה
- סקירת דוחות, קבצים, מסמכים ותיעוד הדרכות בתחום מערכות המידע

עיקרי הממצאים וההמלצות

תחום אבטחת המידע נמצא בשנתיים האחרונות בהליך שיפור מתמיד במועצה המקומית, אולם עדיין ישנם פערים , שאיתורם ותיקונם, מצויים בתוכנית העבודה של הממונה על אבטחת המידע שמונה בשנה האחרונה.

נדרשת ביקורת מעקב בחודשים אוגוסט- ספטמבר, 2024, כדי לעמוד על ההתקדמות והשלמת הפערים

מנהל אבטחת מידע ותוכנית עבודה לאבטחת מידע

בחודש מאי , עם תחילת הביקורת2023 התקשרה המועצה לראשונה עם חברה במיקור חוץ לאספקת שירותי יעוץ וניהול אבטחת מידע וניהול מערכות מידע, בחלקיות משרה.

מנהל אבטחת המידע הגיש תוכנית עבודה לקידום ובקרת אבטחת המידע, לתקופות 11.23 ועד סוף שנת 2024.

אידיאלי היה כי היקפי המשרה של מנמ"ר וממונה אבטחת מידע יהיו גבוהים יותר, אך בהתחשב בגדול הרשות ואילוצי התקציב, הביקורת לא מוצאת מקום להמליץ על הגדלת היקף ההתקשרות.

הביקורת ממליצה כי תיערך בדיקת יישום והתקדמות תוכנית העבודה בשנה הבאה

כתובת דו"אל רשותית

לא נמצאו מקרים בהם עובדי הרשות משתמשים בתיבות דואר שאינן רשותיות.

מאגרי מידע

תקנות הגנת הפרטיות (אבטחת מידע)(, התשע"ז- 2017 (להלן - תקנות אבטחת מידע) מפרטות את אופן יישומה של חובת אבטחת המידע המוטלת בחוק הגנת הפרטיות, התשמ"א- 1981 (להלן – חוק הגנת הפרטיות) על כל בעל מאגר של מידע אישי, מנהל המאגר והמחזיק בו. תקנות אבטחת מידע קובעות הגדרות לרמת האבטחה החלות על מאגרי מידע - רמת אבטחה בינונית או גבוהה. בהתאם להגדרת רמת האבטחה של כל מאגר מידע שברשותה, נדרשת הרשות המקומית לבחון אילו תקנות חלות על המאגר. התקנות מגדירות שעל מאגר מידע הנמצא בבעלות גוף ציבורי, כמו רשות מקומית, חלה לכל הפחות רמת האבטחה הבינונית.

עד לחודש אפריל 2023, פעלה המועצה לרישום שלושה מאגרי מידע, אולם טרם השלימה את הרישום.

לצורך עמידת המועצה המקומית בדרישות תקנות הגנת הפרטיות (אבטחת מידע) ויישום ניהול מאגרי המידע של המועצה, יש צורך לוודא כי מופו כל מאגרי המידע של המועצה ונרשמו בהתאם לחוק.

לצורך כך נדרש לבצע:

- זיהוי מאגרי המידע הקיימים במועצה אשר דורשים רישום, בתיאום עם הגורמים הרלוונטיים במועצה.
- הכנת מסמך הגדרות מאגר המידע ומינוי מנהלים למאגרי המידע שהוגדרו.
- רישום המאגרים אצל רשם מאגרי המידע
- הגשת המידע לרשות להגנת הפרטיות.
- כתיבת מסמך הגדרות למאגרי המידע בהתאם לתקנה 2 לתקנות אבטחת המידע.

תגובת המועצה המקומית:

מיד עם תחילת הביקורת, והתרעת הביקורת, פעלה המועצה בהתאם להמלצה, התקשרה עם חברה המתמחה בתחומי מאגרי המידע ופעלה לרישום כדין של 11 מאגרי מידע. הרישום הושלם בחודש אוקטובר 2023.

התקנים ניידים

בכל מחשבי המועצה חל איסור על הכנסת התקנים ניידים, ואין אפשרות פיזית לחבר

התקנים מיידים.
ככל שעולה צורך, יש אפשרות לפנות באישור מנהל מחלקה, לאחראי המחשוב במועצה והוא יכול לפתוח אפשרות לשימוש בהתקן נייד לזמן מוגבל וקצר.

ביצוע מבדקי חדירה

כחלק מתוכנית העבודה של הממונה על אבטחת מידע, ולבקשת הביקורת, נערכה בדיקת פישינג בחודש 11.23. כ-15% מכלל העובדים נכשלו במבחן החדירה.
כהפקת לקחים, נערכה הדרכה ביום 25.12.23 לכלל עובדי המועצה (עם נוכחות חובה), לגבי כללי ההתנהגות הנדרשים במקרים של פישינג או נסיונות חדירה אחרים.

הדרכות בנושא אבטחת מידע במעמד קליטת עובדים

כל עובד חדש מקבל הדרכה בכתב, עליה נדרש לאשר בחתימתו שקרא והבין.

הביקורת בחנה את נוסח ההדרכה וסבורה שיש מקום לרענן ולהרחיב את ההדרכה בתחומי אבטחת המידע.

הדרכות עובדים;

בוצעה הדרכת עובדים לעל עובדי המועצה, כולל רישום נוכחות ביום 30.5.23.
בוצעה הדרכה לכלל עובדי המועצה, בתחומי הדרכת מידע בדגש על מיילים זדוניים ופישינג ביום 25.12.23, כולל רישום נוכחות

סקר - בקרות תשתיות אבטחת מידע

כחלק מהביקורת התבקש ספק המחשוב החיצוני ומנהל אבטחת המידע לערוך סקר על תשתיות אבטחת המידע, להצביע על ליקויים ולדרג את רמת החומרה שלהם, ולהציע תוכנית פעולה לשיפור אבטחת המידע.

המלצות הסקר אומצו במלואן על ידי המועצה.

לסיכום - תיערך בדיקת מעקב בחודשים אוגוסט-ספטמבר 2024, כדי לעקוב אחר ביצוע ההמלצות בהתאם ללוחות הזמנים הנקובים.

TROT
פתרונות מחשוב

www.trot.co.il | טלפון: 03-6129111 | רחוב התדהר 5 | ת.ד. 4445
trot@trot.co.il | פקס: 03-6126961 | קומה 2, רעננה | רעננה 4366507

בקרת אבטחת מידע רבעונית

רבעון 4 - 2023

מועצה מקומית קריית יערים

סימוכין: Yearim13920

תאריך: 20/12/2023

TROT
פתרונות מחשוב

www.trot.co.il | טלפון: 03-6129111 | רחוב התדהר 5 | ת.ד. 4445
trot@trot.co.il | פקס: 03-6126961 | קומה 2, רעננה | רעננה 4366507

יום ראשון ד' שבט תשפ"ד 14/01/2023

סימוכין: Yearim13920

א.ג.נ.

הנדון: סקירת בקרות תשתיות אבטחת מידע במועצה מקומית קריית יערים - רבעון 4/2023

1. בתאריך 18/12/2023 התקיימה פגישה במועצה המקומית קריית יערים עבור ביצוע בקרה טכנולוגית רבעונית ברשת המועצה והשלמת המשימות הטכנולוגיות הכלולות בתוכנית העבודה לשנת 2023.

2. בפגישה נכחו אסף כץ ושמואל הלפרין מחברת TROT - ספק המחשוב של המועצה, ומנהל אבטחת המידע של המועצה.

3. פירוט הבדיקה:

3.1. **טופולוגית הרשת**

3.1.1. בחינת תרשים הרשת ובחינת שינויים ועדכונים ברשת המועצה.

3.2. **מערכת וירטואליזציה של השרתים - Proxmox**

3.2.1. תאימות הגרסה

3.3. **שרתים – בדיקה מדגמית**

3.3.1. עדכוני מערכת הפעלה.

3.3.2. עדכוני EDR.

3.3.3. תוכנות המותקנות על השרת.

3.4. **מערכת ה-Firewall של החברה**

3.4.1. מעבר על עדכוני תוכנה, רישוי, עדכוני הגנות מתקדמות, גיבויים, מעבר על חוקים מרכזיים, והרשאות ניהול.

3.5. **Local Policy**

3.5.1. בדיקת מדיניות סיסמאות, מדיניות נעילת משתמשים והגדרות נעילת מסך.

3.5.2. הקשחת מערכות הפעלה.

3.6. **שירותי דוא"ל**

3.6.1. מערכת סינון הדוא"ל.

3.6.2. גיבויים סדירים לתיבות הדוא"ל.

3.7. **תשתית End Point Security**

3.7.1. מעבר על הגדרת תחנות קצה.

3.7.2. טיפול שוטף ועדכונים.

3.7.3. חסימת מדיה נתיקה – Device Control.

3.8. **עדכוני אבטחה**

3.8.1. בקרת עדכוני אבטחה למערכות מבוססות Microsoft בהתייחסות לתחנות העבודה והשרתים.

3.8.2. בקרת עדכוני אבטחה לתוכנות צד שלישי בתחנות העבודה ובשרתים.

3.9. **גיבויים, שרידות ושחזורים**

3.9.1. בקרת תקינות תהליכי גיבוי.

www.trot.co.il
trot@trot.co.il
טלפון: 03-6129111
פקס: 03-6126961
רחוב התדהר 5
קומה 2, רעננה
ת.ד. 4445
רעננה 4366507

4. פירוט הממצאים וההמלצות

סידורי	הממצא	המלצה לביצוע	אחריות לביצוע	רמת חומרה	תאריך יעד
טופולוגיית רשת					
4.1.	לא קיים תרשים רשת מעודכן הכולל את כל מערכות הרשת. תרשים רשת חיוני לתכנון, ניהול ותחזוקה יעילה של הרשת	עדכון תרשים רשת, הכולל את כלל התשתיות ומערכות החומרה, רכיבי תקשורת ואבטחת מידע, אופן הגישה למערכות ותיאור הקשרים בין רכיבי המערכת השונים ומיקומם הפיזי של רכיבים אלה.	ספק המחשוב	נמוכה	**01.03.2024**
Local Policy					
4.2.	קיימים מספר Local Admins בשרת ה-DC, בעיקר עובדי מחלקת גזברות.	הסרת כל עובדי המועצה מ-Local Admin.	ספק המחשוב	גבוהה	**01.03.2024**
4.3.	כלל המחשבים מופיעים תחת Container Computers ולא תחת OU. בתיקיית Computers מופיעים מחשבים שאינם פעילים.	העברת כל המחשבים ל-OU ייעודי, עליו יחולו כלל ה-policies, והסרת מחשבים לא פעילים מה-OU.	ספק המחשוב	נמוכה	**01.03.2024**
4.4.	בתיקיית Disable Users מופיעים משתמשים פעילים, ומשתמשים רבים נוספים במצב	העברת משתמשים פעילים ל-OU המתאים, ומחיקת משתמשים במצב Disable. בחינת הצורך בשמירת המשתמשים, גיבוי/העברה	ספק המחשוב	נמוכה	**01.03.2024**

	Disable.	של תיבות הדוא"ל לארכיון, לאחר מכן יש למחוק את המשתמשים מה-OU.			
4.5.	קיימים Domain Administrators רבים, בהם משתמשים עובדי המועצה, משתמשים במצב Disable ומשתמשים רבים עובדי TROT	הסרת משתמשים לא פעילים מהקבוצה, הסרת משתמשים עובדי המועצה, בחינת עובדי TROT הרלוונטיים לשמש כ-Domain Administrators ושמירת ההגדרה כמשתמשים פעילים רק עבור עובדים אילו.	ספק המחשוב	**גבוהה**	**01.03.2024**
4.6.	לא קיימת שמירת לוגים בקטגורית ה-Security מה-Active directory לאורך זמן. הדבר לא מאפשר חקירת אירועי אבטחה, ולא עומד בדרישות חוק הגנת הפרטיות.	שמירת הלוגים למשך 24 חודשים, באחת משתי החלופות הבאות: 1. שמירה לוקאלית לשרת, באמצעות ה-script המצורף למסמך זה. 2. רכישת מערכת SIEM/SOC לניהול ושמירת לוגים.	ספק המחשוב	**גבוהה**	**01.03.2024**
4.7.	לא קיימת מדיניות הפעלה שומר מסך עם סיסמא לאחר 30 דקות של אי-פעילות. מאפשר הפעלת המערכת ע"י גורם עוין, לאחר עזיבה זמנית של המחשב ע"י המפעיל המקורי.	הגדרת Policy של הפעלת שומר מסך עם סיסמא לאחר 30 דקות של אי-פעילות	ספק המחשוב	**גבוהה**	**01.03.2024**
4.8.	מדיניות נעילת משתמשים- נעילה למשך 30 דקות בלבד. נעילה לזמן קצר מידי	הגדרת נעילה למשך 60 דקות.	ספק המחשוב	**בינונית**	**01.03.2024**

www.trot.co.il
trot@trot.co.il
טלפון: 03-6129111
פקס: 03-6126961
רחוב התדהר 5
קומה 2, רעננה
ת.ד. 4445
רעננה 4366507

	מאפשרת ביתר קלות ביצוע התקפות brute force לאיתור סיסמת המשתמש.				
4.9.	מדיניות סיסמאות – לא הוגדר password using reversible encryption.	הגדרת store password using – reversible encryption Disabled.	ספק המחשוב	נמוכה	**01.03.2024**
שרתים					
4.10.	מערכת הפעלה בשרת Microsoft – SQL Windows Server 2012 R2 Standard. מערכת ההפעלה הוכרזה כ-EOL באוקטובר, 2023. היא אינה מקבלת יותר עדכוני אבטחה, עדכוני מערכת הפעלה, תיקון באגים ותמיכה טכנית.	שדרוג מערכת ההפעלה של השרת.	ספק המחשוב	**גבוהה**	**01.03.2024**
4.11.	קיימת גישה ישירה מהאינטרנט אל שרת הדוא"ל הפנימי. השרת מכיל גם את שרת הקבצים ואת ה-DC, קיימת חשיפה של השרתים לאינטרנט, ללא הגנת Firewall פעילה.	1. מעבר ל-Microsoft 365 2. הפרדת ה-Exchange לשרת נפרד והפעלתו ב-DMZ נפרד.	ספק המחשוב	**גבוהה**	**01.03.2024**
4.12.	בשרת exchange	יש להסיר את Winrar 5.11,	ספק	**גבוהה**	**01.03.2024**

	מותקנות תוכנות לא מעודכנות ובעלות חולשות אבטחה. מאפשר ניצול חולשות אבטחה בתוכנות אילו, לתקיפת השרת עצמו.	ולהתקין 7zip בגרסה מעודכנת במקומה. יש לוודא הצורך בשאר התוכנות המותקנות על השרת, ולוודא עדכון בגרסאות אחרונות.	המחשוב		
4.13.	ניתן להתחבר לשרת הטרמינל באמצעות רשת ה-Wi-Fi. כל אדם שמתחבר לרשת יוכל להתחבר לשרת ומשם לשאר מערכות הארגון.	התחברות לכלל שרתים תתבצע באמצעות VPN בלבד.	ספק המחשוב	**גבוהה**	**01.03.2024**
4.14.	במערכת הווירטואלית קיימים 2 שרתים מושבתים שאינם בשימוש.	יש להסיר שרתים שאינם בשימוש מהמערכת הווירטואלית.	ספק המחשוב	**נמוכה**	**01.03.2024**
	Firewall				
4.15.	קיימים מספר משתמשי Admin. ריבוי משתמשים בעל הרשאות גבוהות מעלה את הסיכון של תוקף שיצליח לקבל הרשאת גישה ולבצע נזק.	יש לבדוק כי כלל משתמשי ה-Admin הכרחיים, ולהסיר את אלו שאינם רלוונטיים.	ספק המחשוב	**בינונית**	**01.03.2024**
4.16.	לשני משתמשי ה-VPN, roy ו-yohanan לא מוגדר MFA. המשתמש roy אינו חלק מקבוצת SSL VPN Users.	הגדרת MFA למשתמשי VPN. הוספת כלל משתמשי ה-VPN לקבוצה.	ספק המחשוב	**גבוהה**	**01.03.2024**

www.trot.co.il | טלפון: 03-6129111 | רחוב התדהר 5 | ת.ד. 4445
trot@trot.co.il | פקס: 03-6126961 | קומה 2, רעננה | רעננה 4366507

.4.17	מוגדר רישוי חינמי ל-FortiGuard cloud retention, ועל כן הלוגים נשמרים לשבעה ימים בלבד. במקרה של אירוע אבטחה, לא ניתן יהיה לבצע תחקור אירוע ולהבין את מקור האירוע. בנוסף, זו דרישה הלוגים מהווים את הכלי המרכזי לטובת חקירת אירועי אבטחה, ולטובת טיוב חוקי ה-Firewall.	מומלץ לרכוש רישוי לשמירת הלוגים בענן Fortinet ולקבל את שירותי ה-Forti Analyzer ושמירת הלוגים למשך 90 יום לפחות.	ספק המחשוב	**בינונית**	**01.03.2024**
.4.18	חוקת Firewall – לוגים של חוקי ה-Firewall נשמרים על בסיס התראות UTM בלבד, בשל כך, קשה לבחון את יעילות הפעלת החוקים, ולא ניתן יהיה לתחקר את כלל התעבורה בעת תחקור אירוע.	בחינה מחודשת של אפשרות שמירת הלוגים, כולל שמירה לאורך זמן.	ספק המחשוב	**נמוכה**	**01.03.2024**
.4.19	חוקת Firewall – חוקים רבים הוגדרו כ- Any to Any, לא הוגדרו בהם Services ולא מופעלים בהם שירותי הגנה מתקדמים. ללא הגדרת מקור ויעד	יש להגדיר ב-Destination ו-Source - מי מורשה הגישה ולאן רשאי להתחבר. יש להגדיר בכל חוק מה ה-Services המותרים. יש להרחיב את השימוש בשירותי הגנה מתקדמים בחוקים	ספק המחשוב	**גבוהה**	**01.03.2024**

	לחוקי התעבורה, והגדרת שירותי הגנה מתקדמים, לא מתקיים מיצוי יכולות ההגנה שמערכת ה- Firewall יכולה לספק.	הרלוונטיים.			
4.20.	קיימים חוקים רבים אשר לא מתקיימת בהם תעבורה כלל. טיוב חוקי ה-Firewall הכרחי לניהול תקין ובטוח של התקשורת הארגונית.	יש למחוק חוקים שאינם נמצאים בשימוש, או חוקים שאינם רלוונטיים.	ספק המחשוב	**נמוכה**	**01.03.2024**
4.21.	קיימת גישה מהאינטרנט אל רשת מצלמות האבטחה. באמצעות גישה מהאינטרנט, כל תוקף יכול לחדור לרשת המצלמות, לפגוע בפרטיות העובדים ואף להוות איום בטחוני.	הגדרת חיבור אל המצלמות באמצעות VPN ו-MFA בלבד. מצורף למסמך זה הנחיות מערך הסייבר להנחיות למצלמות נגישות מרשת האינטרנט.	ספק המחשוב	**גבוהה**	**01.03.2024**
4.22.	בעת ביצוע הבקרה נעשה שינוי בהגדרות ה-FortiGuard, כך שעדכוני חתימות יתבצעו אחת לשעה, במקום אחת ליום.			**לידיעה**	
מערכת הגנה - ESET					

4.23.	אין הגבלת חיבור מדיה נתיקה. מתבצעת סריקה של ההתקן הנייד מחובר למחשב ע"י מערכת ההגנה. אחת מהדרכים הנפוצות ביותר להכנסת נוזקות לארגון היא באמצעות התקנים ניידים בזמן חיבורם למחשבי הקצה.	הגבלת חיבור מדיה נתיקה וניהול המקרים בהם יש את הצורך בחיבורים אלו.	ספק המחשוב	**גבוהה**	**01.03.2024**
4.24.	קיימות התראות על 22 תחנות, נראה שחמש תחנות לא התחברו לאחרונה – יש לוודא שכל ההתראות מטופלות.	מומלץ להקדיש זמן קבוע אחת לשבוע לצרוך מעבר על ממצאי הדו"ח על מנת לוודא שהממצאים מטופלים לשלילת אפשרות פגיעה במערכות הארגון.	ספק המחשוב	**נמוכה**	**01.03.2024**
גיבויים					
4.25.	גרסת התוכנה של רכיב ASUSTOR DATA MASTER מכילה חולשות אבטחה, העלולות לאפשר לתוקף לפגוע בשלמות, זמינות ואמינות הגיבויים. המערכת שודרגה בעת ביצוע הביקורת.	בוצע עדכון גרסה במהלך הבקרה.		**לידיעה**	
4.26.	גיבוי חודשי נשמר לשישה חודשים	יש לבחון כהחלטה עסקית האם שישה חודשים מהווים	ספק	**נמוכה**	**01.03.2024**

	בלבד. כמו כן מתבצע גיבוי יומי לענן ולשרת בקומה השלישית, אשר לא ידוע כמה זמן נשמר.	מועד מספק לשמירת הגיבוי החודשי, וכי קיימת תאימות בין זמן השמירה של כלל הגיבויים לבין צרכי המועצה.	המחשוב		
דוא"ל					
.4.27	הרישוי לתכנת סינון הדוא"ל Symantec בתוקף, אך לא נמסרו הגדרות הסינון ולא הודגם סינון בפועל.			**לידיעה**	
.4.28	לא קיימות רשומות DKIM לדוא"ל.	יצירת רשומות DKIM.	ספק המחשוב	**נמוכה**	**01.03.2024**

בברכה

יאיר קץ - CISO

יועץ אבטחת מידע וסייבר

www.trot.co.il | טלפון: 03-6129111 | רחוב התדהר 5 | ת.ד. 4445
trot@trot.co.il | פקס: 03-6126961 | קומה 2, רעננה | רעננה 4366507

5. טופולוגיה

5.1. המועצה מעסיקה 50 ~ 70 עובדים.

5.2. השרת המרכזי המחובר לאל-פסק מותקן בחדר השרתים במשרדי המועצה, בחדר השרתים בו קיים גלאי עשן, ופועל מזגן על 24 מעלות, אין בקרת טמפרטורה. השרתים וכלל הרכיבים מותקנים על מדפים ולא מונחים ישירות על הרצפה. חדר השרתים נעול והכניסה אליו היא באמצעות מפתח הנמצא אצל עובד התחזוקה בלבד.

5.3. קיימת מערכת שרתים וירטואלית Proxmox, גרסה 8-6.1, בה קיימים ארבעה שרתים:

5.3.1. Exchange – בו נמצאים DC, Exchange ו- File Server. מערכת הפעלה Microsoft Windows Server 2016 Standard.

5.3.2. SQL – מערכת הפעלה Microsoft Windows Server 2012 R2 Standard.

5.3.3. Terminal – מערכת הפעלה Microsoft Windows Server 2016 Standard.

5.3.4. Backup – מערכת הפעלה Microsoft Windows Server 2016 Standard.

5.4. חיבור מרחוק:

5.4.1. מוגדרים שני משתמשי SSL-VPN ברכיב ה-Firewall. לא מוגדר חיבור MFA.

5.4.2. משתמשי קצה מתחברים באמצעות OTP של ESET לשרת הטרמינל.

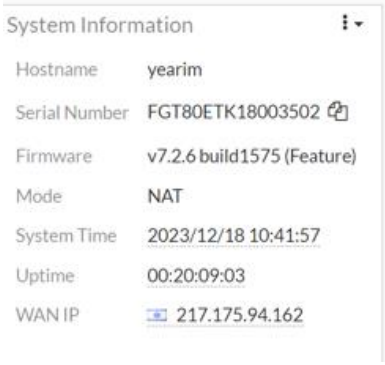
5.5. קיימים שני אתרים בעלי חיבור מרחוק:

5.5.1. שפ"ח – חיבור ישיר לאינטרנט באמצעות ADSL-IPSec.

5.5.2. Trot_VPN – חיבור ישיר לאינטרנט באמצעות ADSL-IPSec.

5.6. רכיב Firewall:

5.6.1. FortiGate 80E, המערכת מעודכנת לגרסה 7.2.6, Build1575.



5.6.2. הרכיב מותקן בחדר השרתים במשרדי המועצה. אל הרכיב מחוברים שני קווי תקשורת:

5.6.2.1. ITC WAN1 – חיבור לאינטרנט.

5.6.2.2. WAN2 milgam-metropolinet – חיבור לספק מערכות הליבה.

5.6.3. רשת ה-Wi-Fi מחוברת באמצעות השרתים.

5.6.4. ממשקים נוספים:

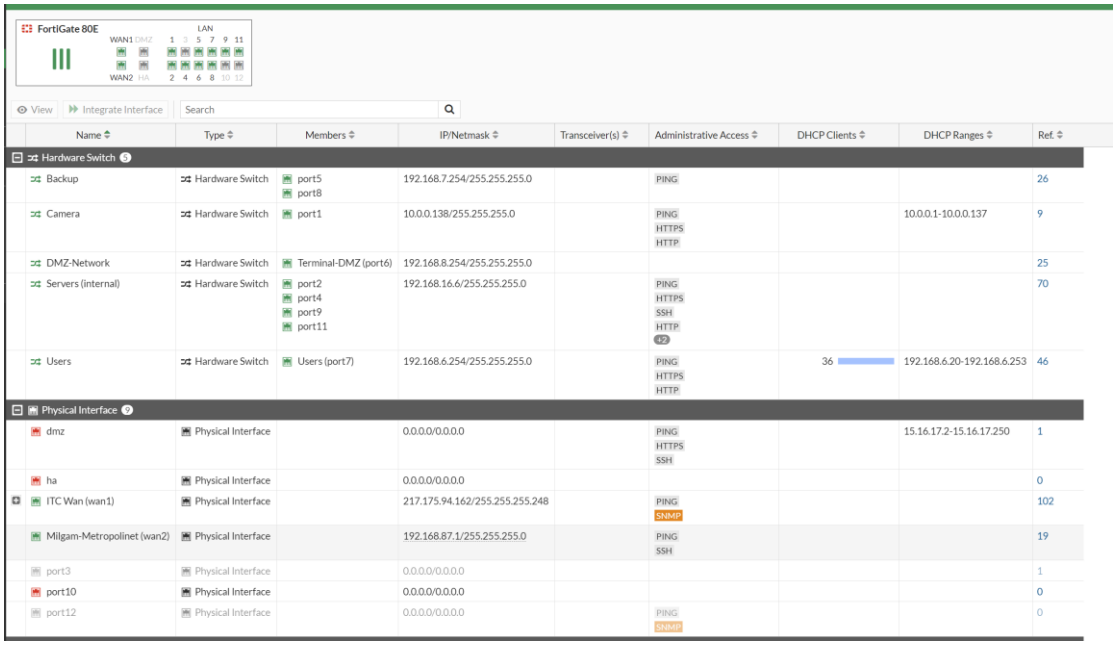
5.6.4.1. סגמנט גיבוי – port 5, 8

5.6.4.2. סגמנט מצלמות – port 1

5.6.4.3. סגמנט DMZ – port 6

5.6.4.4. סגמנט שרתים – port 2, 4, 9, 11

5.6.4.5. סגמנט משתמשים – port 7



5.6.5. עדכוני חתימות מבוצעים פעם ביום – בוצע עדכון הגדרה במהלך ביצוע הבקרה.

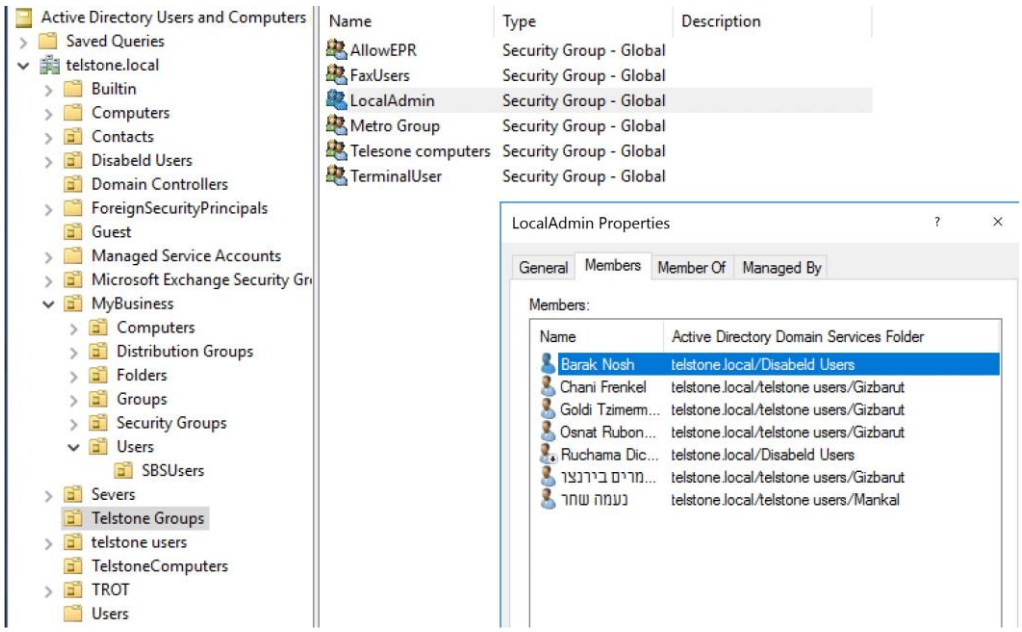
www.trot.co.il
trot@trot.co.il
טלפון: 03-6129111
פקס: 03-6126961
רחוב התדהר 5
קומה 2, רעננה
ת.ד. 4445
רעננה 4366507

6. פירוט הבדיקה עבור הממצאים שפורטו בטבלה

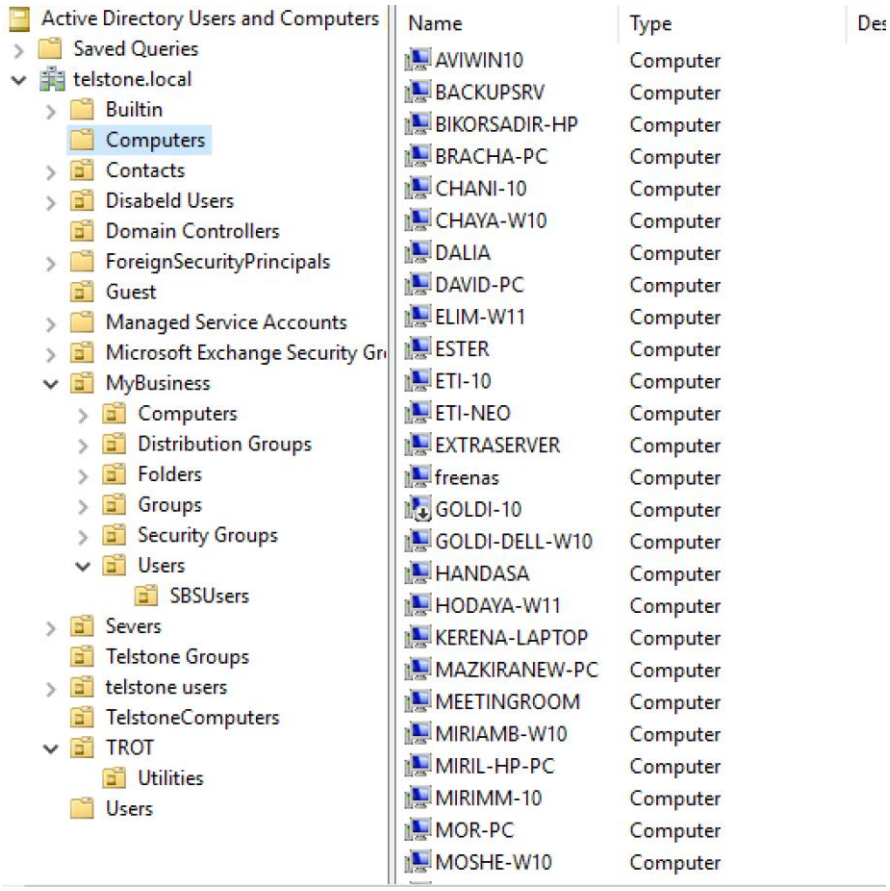
בפרק זה מוצגים תיעודים שעלו כממצא, עבורם יש התייחסות בטבלת הממצאים, או כאלו שנדרשת עבורם התייחסות מיוחדת. כלל התיעודים שנאספו בבקרה והוצגו על ידי חברת TROT מופיעים בנספח המצורף בסוף מסמך זה.

6.1 **Local Policy**

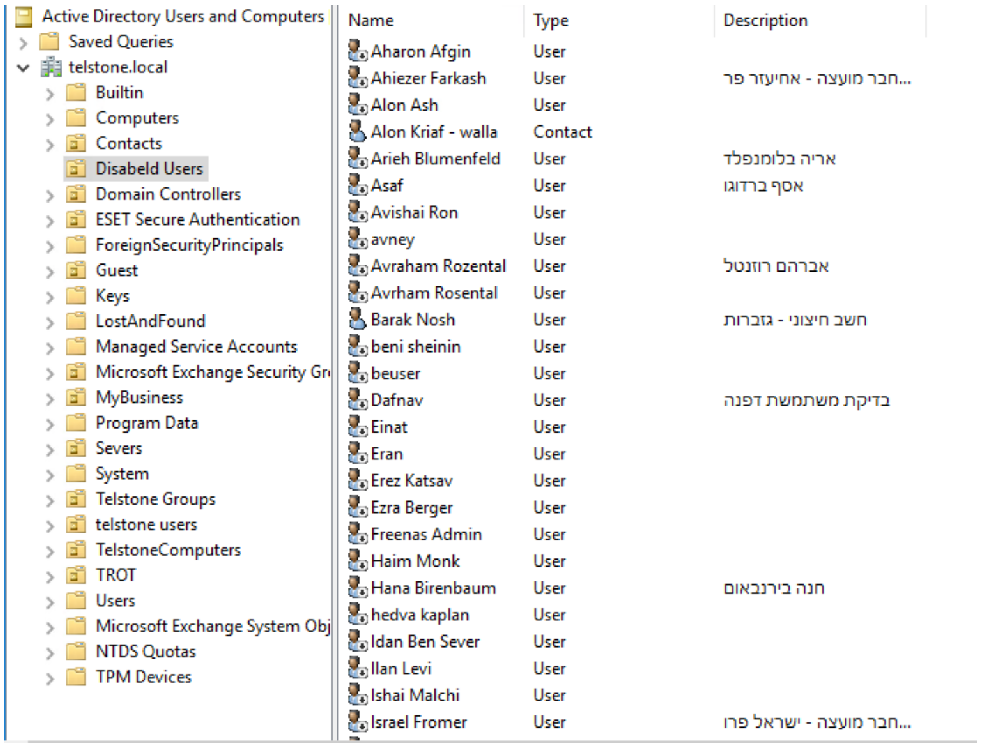
6.1.1 קיימים משתמשים של עובדי עירייה המוגדרים כ-Local Admin, על אף שאינם עובדים IT.



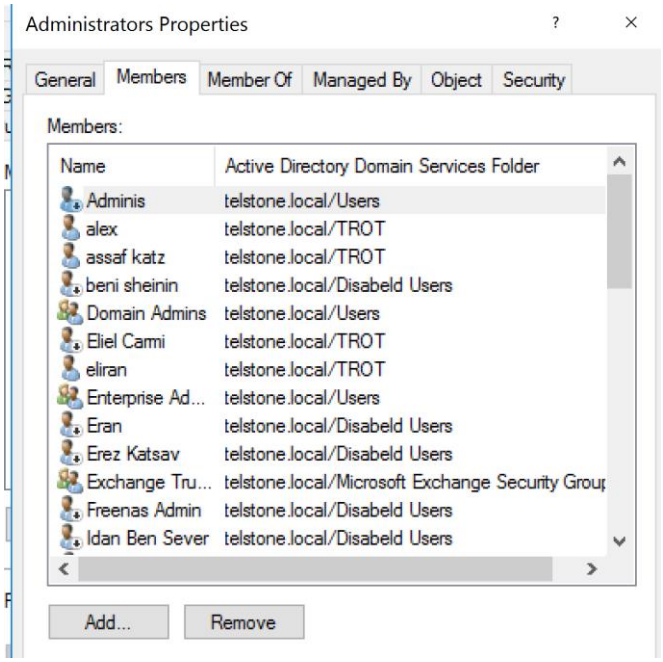
6.1.2. כלל המחשבים מופיעים תחת Container Computers ולא תחת OU, ועל כן לא חלה עליהם עף Policy מוגדרת. בנוסף, בתיקיה Computers מופיעים מחשבים שאינם פעילים. קיים OU המיועד למחשבים, TestoneComputers, אך הוא ריק.



6.1.3. בתיקיית Disabled Users מופיעים משתמשים פעילים, ומשתמשים רבים נוספים במצב Disable, שיש למחוק אם אינם פעילים.



6.1.4. קיימים Domain Administrators רבים, בהם משתמשים עובדי המועצה, משתמשים במצב Disable ומשתמשים רבים עובדי TROT. אין לאפשר ריבוי Domain Administrators, בפרט של עובדי המועצה שאינם עובדי מחשוב, או משתמשים שאמורים להיות במצב Disable. משתמשים מחברת TROT – יש לבחון מי הם המשתמשים הרלוונטיים לשמש כ- Domain administrators.



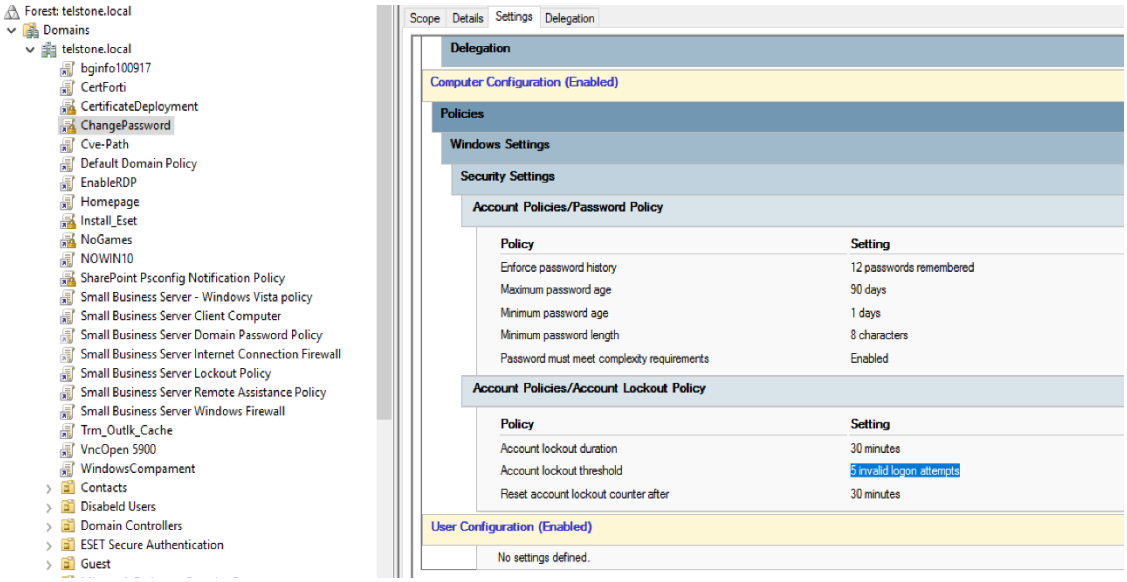
6.1.5. בבדיקה שנעשתה בעת הבקרה, עלה כי לא קיימת שמירת לוגים מ-Active directory לאורך זמן. הדבר לא מאפשר חקירת אירועי אבטחה, ולא עומד בדרישות חוק הגנת הפרטיות.

6.1.6. לא קיימת מדיניות הפעלה שומר מסך עם סיסמא לאחר 30 דקות של אי-פעילות – לא נמסר תיעוד

כיוון שהמדיניות לא קיימת.

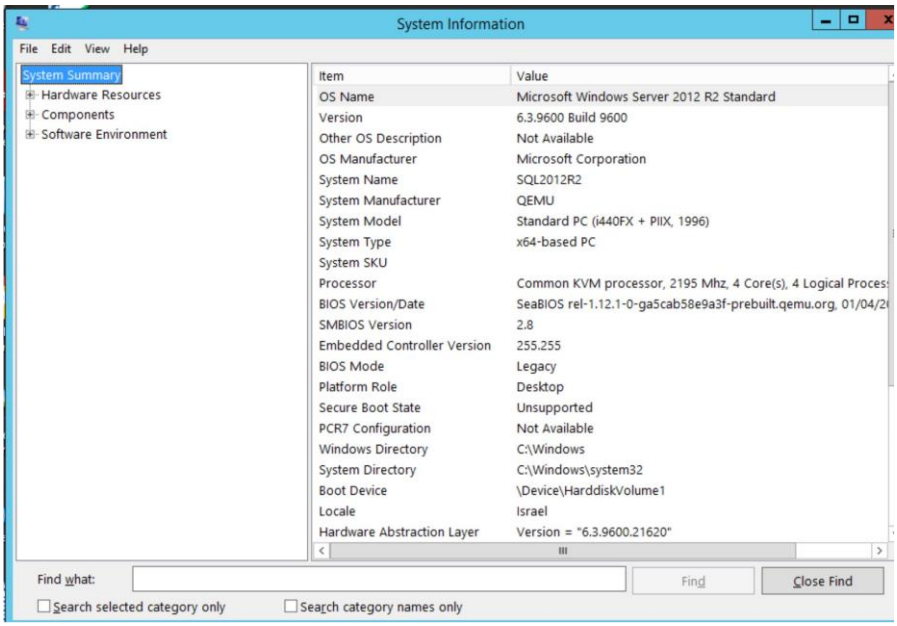
6.1.7. מדיניות נעילת משתמשים - נעילה למשך 30 דקות בלבד.

6.1.8. מדיניות סיסמאות – יש להגדיר Disabled – store password using reversible encryption.



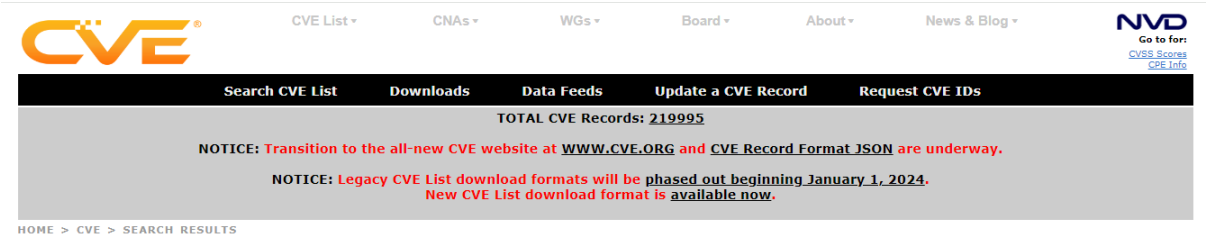
6.2. **שרתים**

6.2.1. מערכת הפעלה בשרת Microsoft Windows Server 2012 R2 Standard – SQL. מערכת ההפעלה הוכרזה כ-End Of Life באוקטובר 2023. היא אינה מקבלת יותר עדכוני אבטחה, עדכוני מערכת הפעלה, תיקון באגים ותמיכה טכנית.

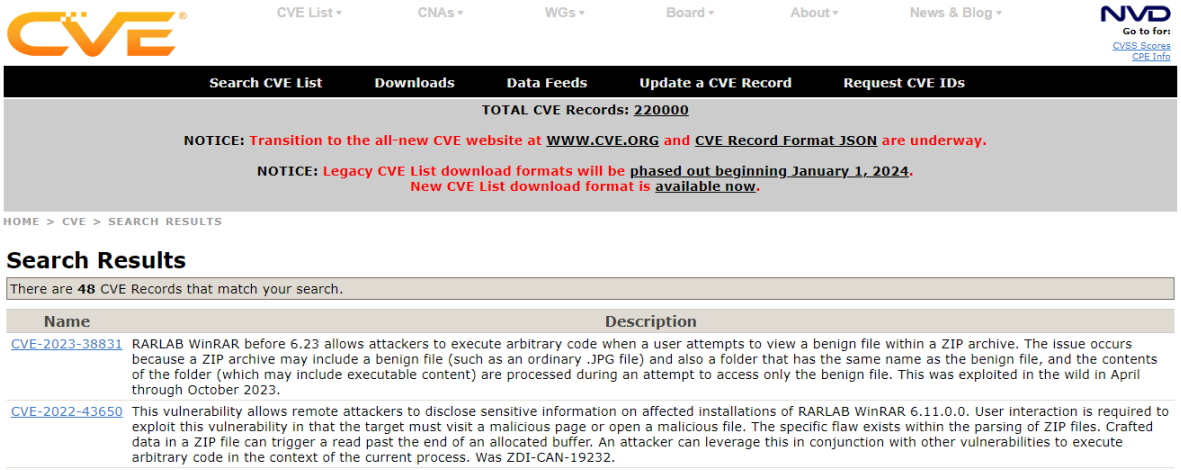


6.2.2. בשרת exchange מותקנות תוכנות לא מעודכנות ובעלות חולשות אבטחה. יש להסיר את WinRAR, ולעדכן את ArcGIS, בכלל השרתים.

:ArcGIS for desktop 10.2.2



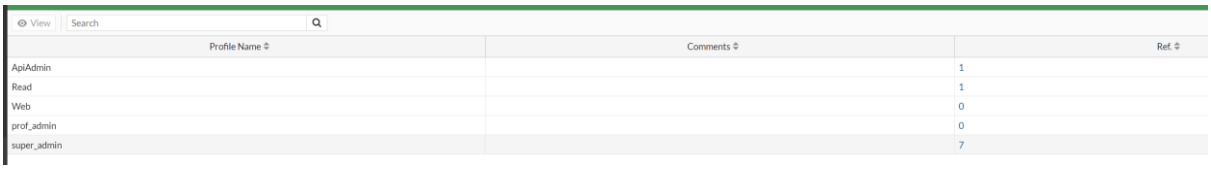
:WinRAR 5.11 .6.2.2.1



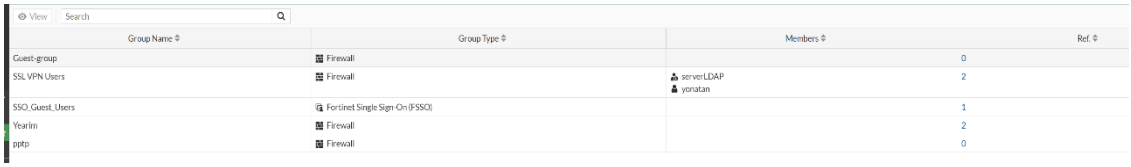
6.2.3. בעת ביצוע הבקרה, הודגמה התחברות לשרת הטרמינל, לאחר התחברות לרשת ה-Wi-Fi המשרדית, ולאחר מכן התחברות באמצעות MFA. תוקף שמבצע Spoofing יוכל להתחבר לשרת ולצפות במידע. יש להוסיף חיבור באמצעות SSL-VPN.

6.3. Firewall

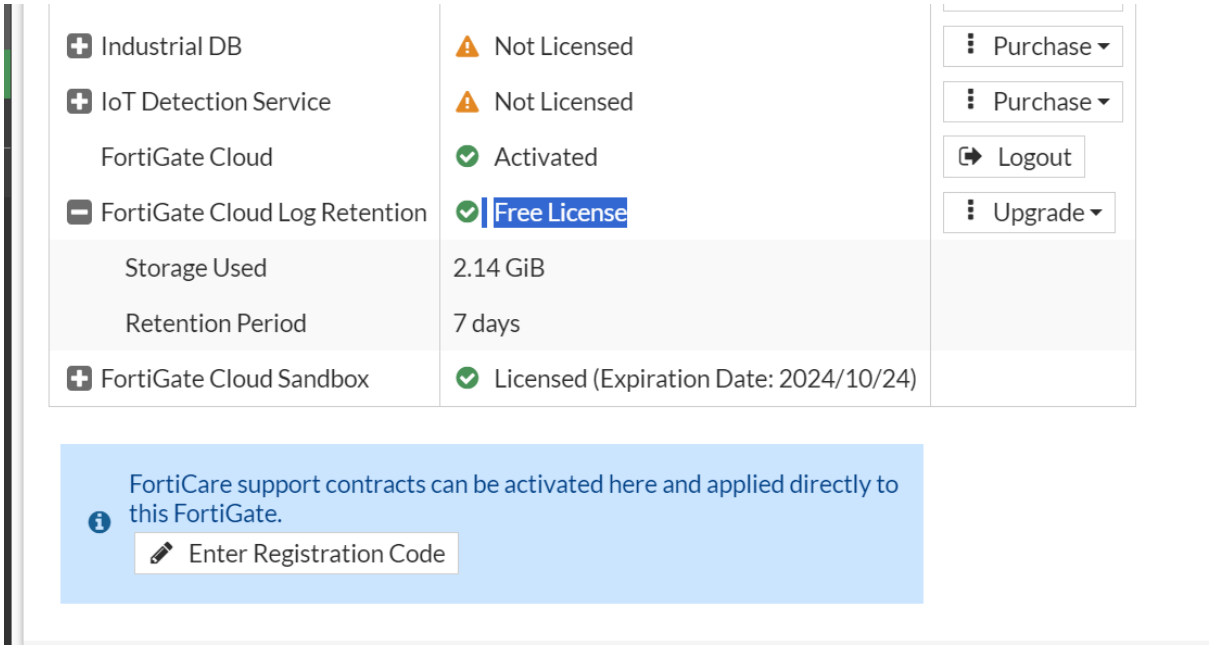
6.3.1. קיימים 7 משתמשי Super Admin, יש לבחון האם כלל משתמשי Adminנצרכים, ולהסיר את המיותרים.



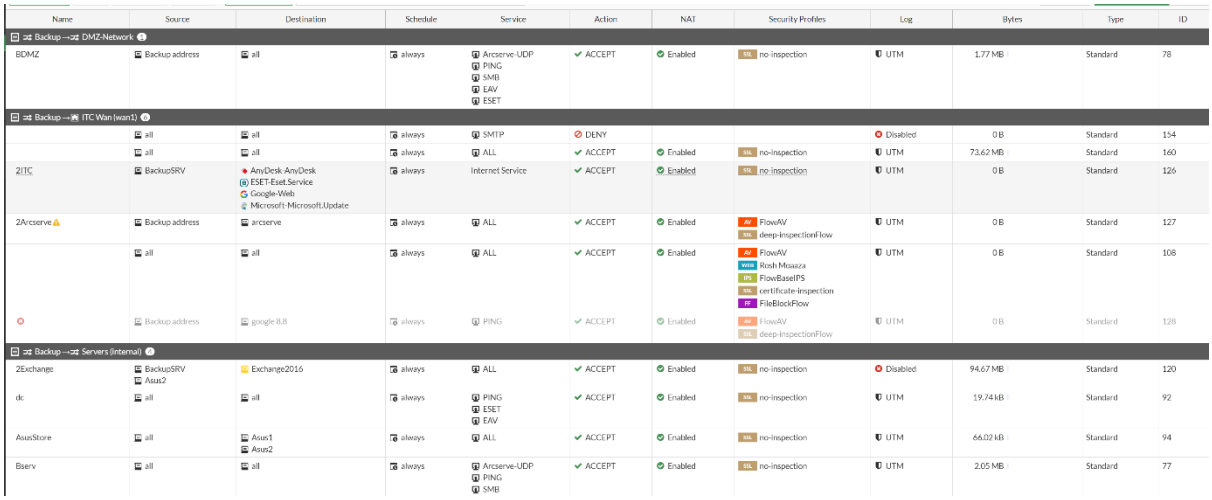
6.3.2. לשני משתמשי ה-SSL-VPN לא מוגדר MFA. המשתמש roy אינו חלק מקבוצת SSL VPN Users.

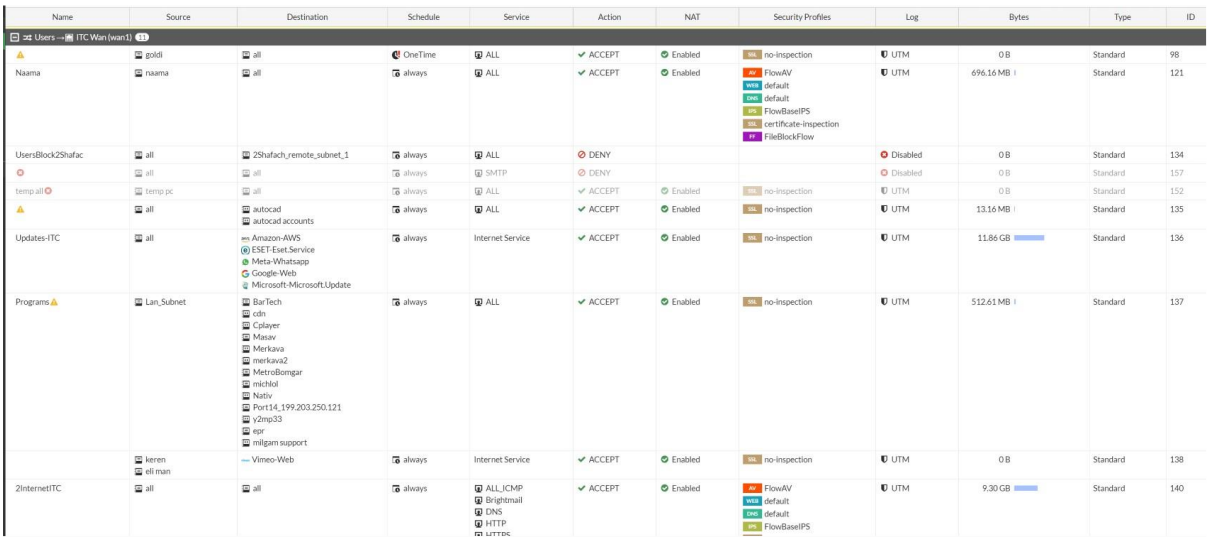


6.3.3. מוגדר רישוי חינמי ל-FortiGuard cloud retention, ועל כן הלוגים נשמרים לשבעה ימים בלבד. במקרה של אירוע אבטחה, לא ניתן יהיה לבצע תחקור אירוע.



6.3.4. חוקת Firewall:





Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes	Type	ID
Users → ITC Wan (wan1) 11											
	goldi	all	OneTime	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B	Standard	98
Naama	naama	all	always	ALL	ACCEPT	Enabled	FlowAV default default FlowBaseIPS certificate-inspection FileBlockFlow	UTM	696.16 MB	Standard	121
UsersBlock2Shafac	all	2Shafach_remote_subnet_1	always	ALL	DENY			Disabled	0 B	Standard	134
	all	all	always	SMTP	DENY			Disabled	0 B	Standard	157
temp all	temp pc	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B	Standard	152
	all	autocad autocad accounts	always	ALL	ACCEPT	Enabled	no-inspection	UTM	13.16 MB	Standard	135
Updates-ITC	all	Amazon-AWS ESET-Eset.Service Meta-Whatsapp Google-Web Microsoft-Microsoft.Update	always	Internet Service	ACCEPT	Enabled	no-inspection	UTM	11.86 GB	Standard	136
Programs	Lan_Subnet	BarTech cdn Cplayer Masav Merkava merkava2 MetroBomgar michlol Nativ Port14_199.203.250.121 y2mp33 epr milgam support	always	ALL	ACCEPT	Enabled	no-inspection	UTM	512.61 MB	Standard	137
	keren eli man	Vimeo-Web	always	Internet Service	ACCEPT	Enabled	no-inspection	UTM	0 B	Standard	138
2InternetITC	all	all	always	ALL_ICMP Brightmail DNS HTTP	ACCEPT	Enabled	FlowAV default default FlowBaseIPS	UTM	9.30 GB	Standard	140

6.3.4.1. לוגים של חוקי ה- Firewall נשמרים על UTM בלבד, ולכן אינם זמינים. בשל כך, לא ניתן לבחון האם חוקים הופעלו ולא ניתן יהיה לתחקר בעת אירוע אילו חוקים הופעלו.

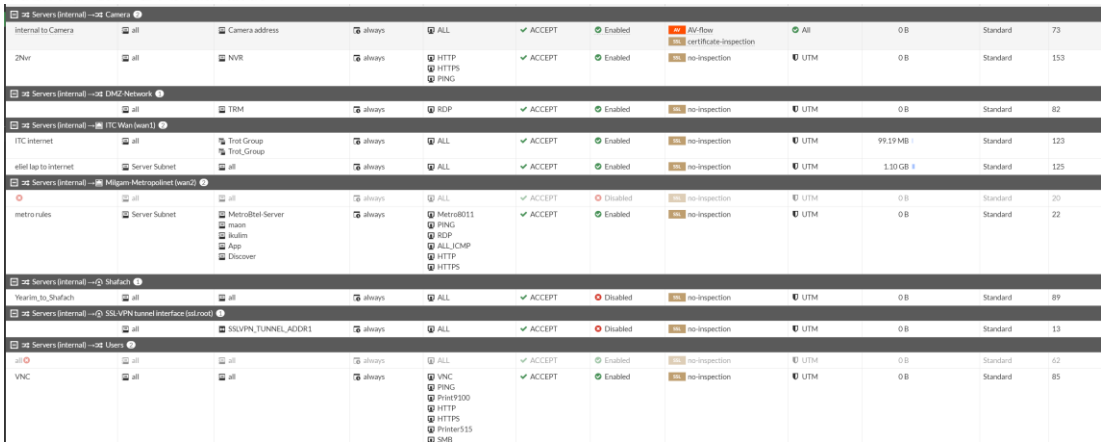
6.3.4.2. קיימים חוקים רבים בהם לא עוברת תעבורת רשת כלל – משמע אין בהם שימוש. יש להסירם מהחוקה. כך לדוגמא חוק 134, 138, 126, 127, 108.

6.3.4.3. בחוקים רבים לא מופעלים שירותי הגנה מתקדמים, ואף מופעל SSL no-inspection, כך שהתעבורה ברשת כלל אינה נבחנת על ידי מערכת ה-Firewall, ולא מתבצעת בדיקה האם הפקטות הנשלחות מכילות נוזקות. כך לדוגמא חוק 136, בעזרתו ניתן לגשת לרשת האינטרנט, תוכן המידע אותו העובר באמצעותו כלל לא נבדק.

6.3.4.4. חוקים רבים מוגדרים כ-Any to Any כך שכל משתמש יוכל להגיע לכל מקום, וניתן להיכנס באמצעות חוקים מהאינטרנט אל שרתים ומערכות המועצה. לדוגמא, חוק מספר 160 המוצג מעלה. כל תוקף בעל גישה לאינטרנט שיצליח להתחבר לשרת הגיבוי יוכל להיחשף לכלל המידע המגובה של הארגון. דוגמא נוספת, חוק 92, לפיו כלל המשתמשים בעלי גישה לשרת ה-DC, על אף שלעובדי הארגון אין צורך להתחבר לשרת.

6.3.4.5. קיימים חוקים ספציפיים שלא נראה שנעשה בהם ולא ברור מה מטרתם – חוק 98, 121, שהמקור שלהם הוא עובדת ספציפית.

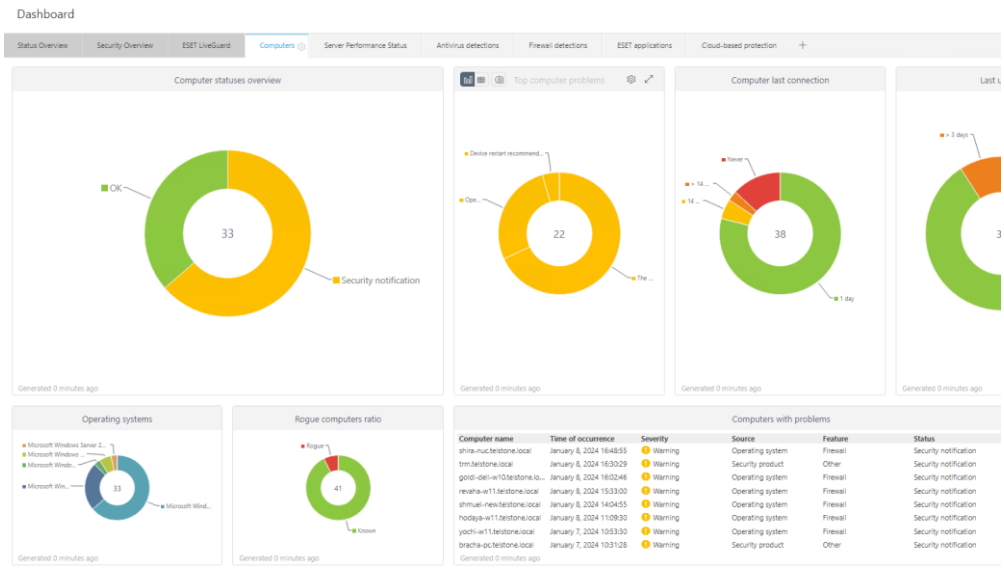
6.3.5. קיימת גישה מהאינטרנט אל רשת מצלמות האבטחה. באמצעות גישה מהאינטרנט, כל תוקף יכול לחדור לרשת המצלמות, לפגוע בפרטיות העובדים ואף להוות איום בטחוני.



6.4. **מערכת הגנה – ESET**

6.4.1. בעת ביצוע הבקרה נעשה ניסיון לחבר DiskOnKey למחשב בחדר ישיבות. אין הגבלת חיבור מדיה נתיקה לתחנות העבודה, אולם מתבצעת סריקה של ההתקן הנייד מחובר למחשב ע"י מערכת ההגנה.

6.4.2. קיימות התראות על 22 תחנות, נראה שחמש תחנות לא התחברו לאחרונה – יש לוודא שכל ההתראות מטופלות.



6.5. **גיבויים**

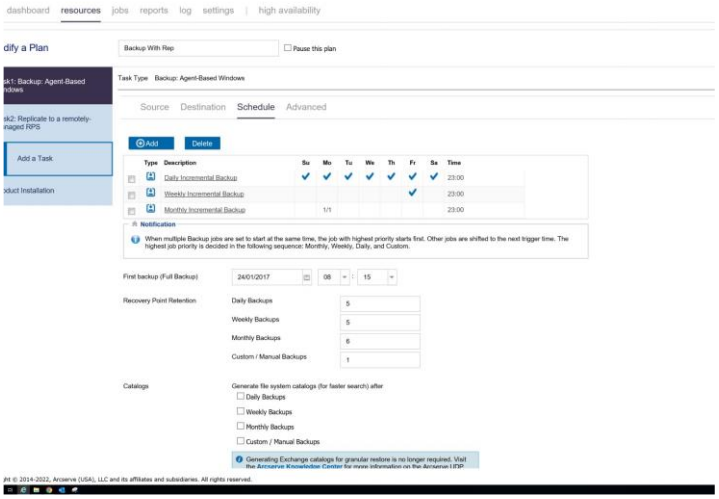
6.5.1. גרסת התוכנה הקודמת של רכיב ASUSTOR DATA MASTER מכילה חולשות אבטחה, העלולות לאפשר לתוקף לפגוע בשלמות, זמינות ואמינות הגיבויים. במהלך הבקרה בוצע שדרוג גרסה.

Search Results

There are **37** CVE Records that match your search.

Name	Description
CVE-2023-4475	An Arbitrary File Movement vulnerability was found in ASUSTOR Data Master (ADM) allows an attacker to exploit the file renaming feature to move files to unintended directories. Affected products and versions include: ADM 4.0.6.RIS1, 4.1.0 and below as well as ADM 4.2.2.RI61 and below.
CVE-2023-3699	An Improper Privilege Management vulnerability was found in ASUSTOR Data Master (ADM) allows an unprivileged local users to modify the storage devices configuration. Affected products and versions include: ADM 4.0.6.RIS1, 4.1.0 and below as well as ADM 4.2.2.RI61 and below.
CVE-2023-30770	A stack-based buffer overflow vulnerability was found in the ASUSTOR Data Master (ADM) due to the lack of data size validation. An attacker can exploit this vulnerability to execute arbitrary code. Affected ADM versions include: 4.0.6.REG2, 4.1.0 and below as well as 4.2.0.RE71 and below.
CVE-2023-2910	Improper neutralization of special elements used in a command ('Command Injection') vulnerability in Printer service functionality in ASUSTOR Data Master (ADM) allows remote unauthorized users to execute arbitrary commands via unspecified vectors. Affected products and versions include: ADM 4.0.6.RIS1, 4.1.0 and below as well as ADM 4.2.2.RI61 and below.
CVE-2019-11689	An issue was discovered in ASUSTOR exFAT Driver through 1.0.0.r20. When conducting license validation, exfat.cgi and exfatctl fail to properly validate server responses and pass unsanitized text to the system shell, resulting in code execution as root.

6.5.2. גיבוי חודשי נשמר לשישה חודשים בלבד. על פי תקנות הגנת הפרטיות, נתונים של אירועי אבטחה יש לשמור ל-24 חודשים.



6.6. **דוא"ל**

6.6.1. מבדיקה שבוצעה במהלך הבקרה, לא קיימות רשומות DKIM ו-DMARC לדוא"ל.

7. נספח תיעודים שנאספו בבקרה

7.1. מסכים pptx.18-12-2023