סיכום והמלצות – רכבי העירייה

1. **בהתאם לתכנית הביקורת לשנת 2024, ערך מבקר העירייה ביקורת בנושא "רכבי העירייה".**
2. **להלן סיכום הממצאים והמלצות הביקורת:**

מבנה ארגוני

1. **מהמבנה הארגוני שהומצא לביקורת עלה כי, מנהל האירועים ממונה, בין היתר, גם על רכזת התחבורה.**
2. **מנהל האירועים כפוף למנכ"לית העירייה.**
3. **העירייה מעסיקה את קצין הבטיחות בתעבורה כנותן שירותים והוא אינו נמנה עם מצבת העובדים של העירייה.**

המלצות:

1. מומלץ לרכז את נושא הטיפול בתחבורה אצל בעל תפקיד אחד = רכזת תחבורה.
2. מומלץ להכפיף את רכזת התחבורה לגזבר העירייה.

הביקורת מוצאת לנכון לציין כי, במהלך הביקורת שונה המבנה הארגוני באופן כזה, שכלל הטיפול במצבת כלי הרכב הועבר ל"רכזת תחבורה". כמו כן, רכזת התחבורה הוכפפה לגזבר העירייה.

וועדת רכב

1. **למרות שלעירייה ניתנה סמכות למנות וועדות נוספות על אלה הקבועות בחוק, העירייה לא מינתה וועדת רכב.**

2. **הביקורת ביקשה לקבל לידיה נתונים על תאונות בהן היו מעורבים רכבים של העירייה בשנים 2022 – 2023. בשל היעדר וועדת רכב, התאונות שהתרחשו לא נחקרו ולא נדונו.**

המלצות

1. לצורך תיעוד קבלת ההחלטות בכל הנוגע למדיניות הקצאת רכבים, ולצורך עמידה בנוהל רכב, ככל שיונהג נוהל כזה, יש למנות וועדת רכב, שתורכב מבעלי תפקידים רלוונטיים בעירייה (מנכ"ל, גזבר, יועמ"ש, מנהל רכש וכד').

2. נוסף על קביעת מדיניות הקצאת רכבים, על הוועדה לנהל מעקבים ודיונים אחר תאונות שהיו מעורבים כלי רכב של העירייה, במטרה להפיק לקחים ולמנוע, ככל האפשר, תאונות עתידיות.

הביקורת מוצאת לנכון לציין, כי במהלך הביקורת ראש העירייה מינה וועדת רכב. הוועדה תדון באישור רכישה/חכירה של רכבים, החלפת רכבים, מעקב אחר תאונות וכיו"ב.

כמו כן, במהלך הביקורת הוכן "נוהל רכב" המגדיר את התפקידים המזכים ברכב צמוד, אופן הגשת הבקשות, מדיניות העירייה, השימוש ברכבי העירייה ועוד.

<u>תקציב וביצוע</u>

למרות שבשנת 2022 אחוז הביצוע חרג בכ-21% מהתקציב, בשנת 2023 גדל תקציב הרכב בכ- 6% בלבד.

המלצה:
בעת הכנת התקציב, הביקורת ממליצה לבחון את הביצוע בגין אותו הסעיף בשנה השוטפת, ולהתאים את התקציב השנתי לצָפי ההוצאה בפועל.

<u>נתונים תוצאתיים</u>

1. **בשנת 2023 ההוצאות בגין שימוש ברכבים שכורים, שלא באמצעות החברה למשק וכלכלה, גדלה בהיקף העולה על 100%.**
2. **סך ההוצאות בגין השכרת רכב בשנת 2023 עלה בכ-62% לעומת שנת 2022.**
3. **הוצאות הדלק בשנת 2023 עמדו על כ-85% לעומת ההוצאות בשנת 2022.**
4. **הוצאות העירייה בגין כבישי אגרה עמדו על כ-23,000 ₪ בכל אחת מהשנים המבוקרות.**
5. **בביקורת נמצא כי כרטיסי הדלק מחולקים לעובדים על ידי שני בעלי תפקידים בעירייה – מזכירת גזבר העירייה ומנהל האירועים של העירייה.**

6. **רישום חלוקת כרטיסי הדלך מנוהל בטבלת אקסל, ממנה ניתן לקבל מידע אודות העובדים שקיבלו את כרטיס הדלק, מועד מתן הכרטיס וסך הכרטיסים שהונפקו לעובד.**

7. **אין מידע מפורט אילו רכבים תודלקו באמצעות כרטיסי הדלק, מועדי התידלוק, מיקום התידלוק וכיו"ב. במצב דברים זה, אין אפשרות לוודא שכרטיסי הדלק שימשו רק את רכבי העירייה.**

המלצות
1. יש להימנע, ככל האפשר, מהנפקת כרטיסי דלק. במקרים בהם העירייה תיאלץ לשכור רכבים לתקופה ממושכת, מומלץ להתקין ברכבים אלה התקן תידלוק.

2. יש לרכז את חלוקת כרטיסי הדלק אצל בעל תפקיד אחד, שינוהל על ידי גזברות העירייה.
3. במועד חלוקת כרטיס דלק חדש, יש לחייב את העובדים לצרף קבלה המפרטת את מועד התדלוק, מקום התדלוק ומספר הרכב.

<u>מערכות מיחשוב</u>

בביקורת נמצא, כי יחידת הרכב מנהלת מעקב אחר קליטה וגריעת רכבים, אך לא מתבצע רישום של יתר הפרטים שעשויים לסייע בהמשך כגון צריכת דלק וכד'.

הביקורת ממליצה להטמיע את מערכת ניהול הרכב "נצר" ולהשלים את כל הנתונים הנחוצים לניהולו התקין של צי הרכב העירוני.

<u>ניהול הבטיחות בתעבורה</u>

1. **בבחינת העסקת מינוי קצין בטיחות בתעבורה נמצא, כי העירייה מעסיקה "קצין בטיחות בתעבורה", באמצעות ספק שירותי. היקף ההעסקה הינו של יומיים בשבוע – <u>תקין</u>.**

2. **הביקורת ביקשה לקבל לידיה עותק מתוכנית לניהול הבטיחות בעירייה, אך תוכנית מעין זו טרם הוגשה לביקורת. משכך, הביקורת יוצאת מנקודת הנחה שהעירייה טרם ערכה ניתוח סיכוני בטיחות, לרבות בתחום הרכב.**

<u>רכבים שאינם צמודים</u>

1. **הביקורת בחנה מספר תיקים. בבדיקה נמצא, כי קצין הבטיחות מנהל מעקב אחר תקינות הרכבים, בכלל זה בדיקה תקופתית ותקינות הרכב - <u>תקין</u>.**
2. **מנתוני מצבת הרכבים שהומצאה לביקורת עלה, כי שמונה (8) רכבים משמשים את עובדי העירייה כרכב עבודה (מאגר) או רכב ביטחון, ומשכך, בגין רכבים אלה העירייה אינה מחייבת בגין שווי שימוש.**
3. **היחידה אינה מנהלת מעקב אחר השארת הרכבים במקום ייעודי בתום יום העבודה. באופן זה, עובדים עלולים לעשות שימוש פרטי ברכב העבודה, תוך הימנעות מתשלום שווי, כמתחייב.**

המלצות

1. יש להגדיר מקומות יעודים אליהם יוחזרו רכבי העבודה בסיום יום העבודה.

2. מומלץ להתקין ברכבי העבודה מכשיר איתור (איתורן וכד'), במטרה לעקוב אחר פעילות הרכב. באופן זה, ניתן יהיה לוודא שברכב נעשה שימוש לצרכי עבודה בלבד.

3. ככלל, יש לחייב את המשתמשים ברכב עבודה למלא "יומן עבודה" מידי יום, במטרה לאתר את הנוהג ברכב במקרים של עבירות תנועה וכד'.

<u>טיפול בתאונות</u>

1. **הביקורת ביקשה לקבל לידיה עותק מנוהל דווח על תאונה בה היה מעורב רכב של העירייה. נכון לסיום הביקורת, נוהל מעין זה לא הוגש לביקורת.**

2. **הביקורת ביקשה לקבל דוח מפורט של התאונות שהיו מעורבים בהן רכבי העירייה בשנים 2022-2023. עד לסיום הביקורת, דוח מעין זה טרם הוגש לביקורת.**

המלצות:

1. יש להכין נוהל מפורט המגדיר את אופן הדווח בכל מקרה בו היה מעורב רכב של העירייה בתאונת דרכים. בנוהל יפורטו הדרכים לדווח, בעלי התפקידים שיש לדווח להם על התאונה וכיו"ב.
2. במטרה למנוע תאונות עתידיות והפקת לקחים, יש לחקור כל תאונה בה היה מעורב רכב של העירייה ולגבש מסקנות אופרטיביות למניעה.

<u>רכבים צמודים</u>

<u>אישור קבלת רכב צמוד</u>

1. **במקרים מסוימים אושר לעובד רכב שאינו כלול ברשימת הרכבים שפרסמה החברה למשק וכלכלה. במקרים מעין אלה, פרק הזמן עד לקבלת הרכב ארוך מהרגיל והעירייה מעמידה לרשות העובד רכב שכור, שעלותו החודשית גבוהה מהעלות ה"רגילה".**

המלצות הביקורת

1. בניסיון להקטין את העלויות השוטפות, בכלל זה דמי הניהול המשולמים לחברה למשק וכלכלה, הביקורת ממליצה לבחון אפשרות להצטרף למכרז מסגרת למתן שירותי רכב בשיטת הליסינג, שפרסמו מספר רשויות מקומיות.

<u>נהיגה ברכב עירוני</u>

1. **מעיון בתיקי הרכב המנוהלים במשרד קצין הרכב עלה, כי מספר עובדים מצומצם הצהיר שהועברה הדרכה לבני המשפחה.**
2. **עותק מרישיונות הנהיגה של בני המשפחה נמצא בשני תיקים בלבד.**
3. **המעקב אחר תוקף רישיונות הנהיגה מנוהל באופן ידני וקצין הרכב בודק, בצורה יזומה, את מסד הנתונים שכאמור, מנוהל בטבלת "אקסל".**
4. **קצין הרכב משלם את אגרת ההפקה למשרד התחבורה ואחת לחודש מגיש לגזברות העירייה החזר התשלומים ששילם. ההחזר מועבר לעובד מ"קופה קטנה".**

המלצות

1. במעמד מסירת הרכב יש להוסיף סעיף בו העובד מצהיר שרק נהגים שיש ברשותם רישיון נהיגה בר תוקף ושעברו הדרכה, יוכלו לנהוג ברכב.

2. יש לנהל את המעקב אחר מועדי פקיעת תוקפם של רישיונות הנהיגה במערכת לניהול צי הרכב (נצר), והמערכת תתריע, באופן אוטומטי, לקצין הרכב על מועד פקיעת תוקף רישיון הנהיגה.

3. לעניין תשלומי האגרה בגין הפקת מידע, מומלץ לבחון עם משרד התחבורה אפשרות של התקשרות גלובלית להנפקת מידע ולמנוע את הצורך של קצין הרכב לשלם מכיסו את האגרה. כמו כן, יש לדרוש לקבל מידע על עובדים שחל שינוי ברישיון הנהיגה שלהם כגון: שינוי סוגי הרכב בהם ניתנה הרשאה, שלילת רישיון נהיגה וכד'.

<u>חוזה התקשרות עם חברת ההשכרה</u>

1. **בביקורת נמצאו מקרים בהם העירייה החזירה את הרכב בטרם חלפו 36 חודשי שכירות.**
2. **נמצא, כי חלק מהרכבים חרגו ממכסת הקילומטרים השנתית והעירייה נשאה בתשלום הנוסף.**
3. **התשלומים בגין החזרת הרכבים לפני תום תקופת ההסכם וחריגת הקילומטרים שולמו מקופת העירייה.**

המלצת הביקורת

1. במקרים בהם הוגשה בקשה להחלפת הרכב בטרם חלפה תקופת ההחכר, יש להשית את תשלום חודשי השכירות על העובד.

2. במעמד אישור הרכב הצמוד יש להעריך את מספר הקילומטרים שהעובד צפוי לנסוע בשנה. אם הצפי עולה על 30,000 ק"מ מומלץ לבחון עם חברה ההשכרה ולקבוע סכום כולל בגין החריגה. אם הצפי אינו עולה על 30,000 ק"מ, מומלץ להחתים את העובד על כתב הרשאה, המאפשר לעירייה לנכות משכרו את הסכומים שהעירייה תיאלץ לשלם לחברת ההשכרה בגין חריגת קילומטרים.

<u>שכירת כלי רכב</u>

1. **בביקורת נמצא כי חסרים נהלים המפרטים את המקרים בהם קיימת הצדקה להתקשרות עם חברות ההשכרה.**
2. **אישור השכרת רכב ניתן על ידי מנכ"לית העירייה ולא על ידי "וועדת רכב".**
3. **התשלום לחברות ההשכרה גבוה מהתשלום שהעירייה משלמת לחברות הליסינג בגין אותם הרכבים.**
4. **בביקורת נמצא כי העירייה שכרה רכבים לתקופות ממושכות, לפעמים תקופה של שנתיים.**
5. **למרות שהעירייה התקשרה עם חברות השכרה לתקופות ממושכות, ברכבים השכורים לא הותקנו מכשירי "פזומט" ותידלוק הרכבים השכורים בוצע באמצעות כרטיסי דלק.**

המלצות הביקורת

1. יש לעגן בנוהל מפורט את המקרים בהם מתעורר הצורך בהתקשרות עם חברת השכרה, את אופן ההתקשרות ומשך התקופה המקסימאלית לשימוש ברכב שכור, עד לקבלת הרכב הרצוי/המבוקש מחברת הליסינג.

2. במקרים חריגים במיוחד בהם מתעורר הצורך להשתמש ברכב שכור לתקופה ממושכת, מומלץ להתקין התקן "פזומט" במטרה לאפשר מעקב אחר תדלוק הרכב השכור.

<u>שווי שימוש – רכב צמוד</u>

מהשוואה בין רשימת העובדים להם העירייה הצמידה רכב לבין זקיפת השווי בשכר העובדים שערכה הביקורת נמצא, כי העירייה לא זקפה שווי לשלושה עובדים (לא כולל רכב עבודה/מאגר/שיטור).

המלצת הביקורת

יש לערוך בדיקה מקיפה של כלל הרכבים הצמודים ולוודא עם מחלקת השכר של העירייה שלכל העובדים שהעירייה הצמידה להם רכב, מדווח שווי שימוש בהתאם להנחיות רשות המיסים.

<u>כבישי אגרה</u>

1. **מנתוני המנויים לכבישי אגרה נמצא כי העירייה רכשה 22 מינויים לכביש 6 חוצה צפון, 10 מינויים למנהרות הכרמל ו-9 מינויים לכביש 6.**
2. **אישור המינויים הינו באחריות גזברות העירייה.**
3. **העירייה שילמה את "דמי הטיפול" לעובדים שעשו שימוש בכבישי אגרה ללא מנוי.**

המלצות

1. יש לקבוע קריטריונים לאישור תשלום השימוש בכבישי אגרה. בכלל זה, יש לפרט את בעלי התפקידים הזכאים להשתתפות.
2. יש להתאים את אחוזי ההשתתפות ואופן התשלום להנחיות המפורטות בהוראת החשב הכללי, בדגש על החזר ההוצאה בשיעור של 70% מהאגרה בלבד, ללא השתתפות בהוצאות אחרות כגון: חובות, דמי טיפול וכד').

ביקורת בנושא "אבטחת מידע" – סיכומים והמלצות

1. מבנה ארגוני

הביקורת ביקשה לקבל מסמכים בנושא מבנה העירייה, כולל ייפוי כוח, בעלי שליטה והגדרת תפקידים בתחום אבטחת המידע, נמסר כי מסמכים אלו חסרים.

המלצת הביקורת

הביקורת בדיעה, כי יש להכין מסמכים מתאימים המסדירים את תחום האחריות והסמכות על אבטחת המידע, כדי לחזק את מערך האבטחה הארגוני ולהבטיח ניהול ברור ואפקטיבי של תחום זה.

2. רשימת בעלי הרשאות, ניהול הרשאות

בהמשך לבקשת הביקורת לקבל רשימה מסודרת של כל בעלי ההרשאות המנהליות ("משתמשי על") באפליקציות הארגוניות, כולל תיאור תפקידם, נמסר כי רשימה כזו אינה קיימת

המלצת הביקורת

הביקורת בדיעה, כי יש לערוך תיעוד וניהול מסודר של הרשאות הניהול, כדי לחזק את הבקרה והפיקוח על משתמשי העל בעירייה.

בהמשך לבקשתנו לקבלת פוליסת ניהול הרשאות לעובדים חדשים, נמסר כי פוליסה כזו אינה קיימת.

המלצת הביקורת

יש להכין פוליסה ברורה לניהול הרשאות לעובדים חדשים, שתבטיח מתן גישה בהתאם לצורכי התפקיד ותסייע לשמור על רמת אבטחת מידע גבוהה.

בהמשך לבקשתנו לקבל פוליסת ניהול הרשאות לעובדים שעוזבים את העירייה, נמסר כי פוליסה כזו אינה קיימת.

המלצת הביקורת

יש לגבש פוליסת עזיבת עובד שתסדיר את תהליך שלילת ההרשאות באופן מסודר כדי למזער סיכוני אבטחה ולשמור על בטיחות מערכות המידע בעירייה.

3. נהלים

בהמשך לבקשת הביקורת לעיין בנוהל אבטחת מידע שמפרט את זיהוי המידע החסוי של העירייה, אמצעי ההגנה עליו ומידור המשתמשים, נמסר כי נוהל כזה אינו קיים. הובהר כי מידור המשתמשים מתבצע באמצעות הרשאות NTFS בשרת הקבצים, בהתאם לקבוצות ולמחלקות.

המלצת הביקורת

6.1.2 הביקורת מורה על הכנת נוהל אבטחת מידע ייעודי אשר יפרט את נהלי ההגנה על המידע החסוי בעירייה ואת עקרונות המידור, כדי לחזק את מערך אבטחת המידע ולהבטיח ניהול נכון של הרשאות וגישה למידע.

בהמשך לבקשת הביקורת לקבל לידיה נוהלי סיסמאות וחיבור מרחוק, כולל מסמכים המתארים את המצב הקיים לעומת המצב הרצוי, נמסר כי מסמכים ונהלים אלו אינם קיימים. הובהר כי מתבצעת החלפת סיסמאות כל חצי שנה, וכי חיבור מרחוק קיים עבור חלק מהעובדים בלבד, עם אפשרות להנפיק רשימת משתמשים בהתאם לצורך.

המלצת הביקורת
יש לפתח נוהלי סיסמאות וחיבור מרחוק והכנת מסמכים שיבחנו את המצב הקיים מול המצב הרצוי, כדי להבטיח אבטחת מידע מיטבית ולהפחית את הסיכונים בגישה למערכות העירייה.

בהמשך לבקשתנו לקבל נוהל שמירה על אבטחת מידע רגיש עבור ספריות קבצים משותפות למחלקות המטפלות במידע רגיש, כגון מחלקת רווחה, נמסר כי נוהל כתוב בנושא אינו קיים.

המלצת הביקורת
מומלץ על פיתוח נוהל כתוב שיסדיר את הגישה לספריות רגישות, כדי להבטיח ניהול אבטחת מידע אפקטיבי והגנה על נתונים רגישים בעירייה.

4. הסכמים עם ספקים וקיום הדרכות

בהמשך לבקשתנו לקבל את ההסכמים עם הספקים המהותיים, כולל סעיפי סודיות, אבטחת מידע וזמני תגובה, נמסר כי ממונה מערכות המידע מועסק באמצעות ספק הענן והתשתיות, אך לא הוצגו הסכמים נוספים בנושא זה.

המלצת הביקורת
אנו ממליצים לעגן בהסכמים עם הספקים המהותיים סעיפים מפורשים בנוגע לאבטחת מידע, סודיות וזמני תגובה כדי לצמצם את הסיכונים ולחזק את מערך האבטחה הארגוני.

הביקורת ביקשה לקבל מידע על קיום הדרכות מודעות שנתיות בנושא אבטחת מידע, כולל נוהל המתייחס לנושא. לביקורת נמסר, כי אין ידוע על הדרכות שבוצעו עד כה. בנוסף, ממונה מערכות המידע המליץ לתאם הדרכות עם חברה חיצונית.

המלצת הביקורת
יש לאמץ נוהל מחייב לביצוע הדרכות מודעות לעובדים לפחות פעם בשנה, ולשקול תיאום הדרכות עם חברה חיצונית המתמחה בתחום, בהתאם להמלצת ממונה מערכות המידע.

הביקורת ביקשה לוודא את קיומו של פורום לניהול איומים וסיכוני אבטחת מידע, כולל פירוט המשתתפים, תפקידיהם ותחומי אחריותם, נמסר כי פורום כזה אינו קיים בעירייה.

המלצת הביקורת
במטרה לחזק את מערך אבטחת המידע הארגוני, מומלץ להקים פורום ייעודי לניהול סיכוני אבטחת מידע, בו ייקחו חלק גורמי מפתח בתחום, ולפרט את תחומי האחריות של כל משתתף.

5. תכנית התאוששות/המשכיות

הביקורת ביקשה לבחון את תהליך קביעתה ואישורה של תוכנית התאוששות מאסון (DR) והמשכיות עסקית, כולל מעורבות מנהל אבטחת מידע. ממנהל מערכות המידע והגורמים הרלוונטיים, נמסר כי תוכנית DR אינה קיימת בעירייה.

המלצות הביקורת

הביקורת ממליצה להתחיל בתהליך גיבוש ואישור תוכנית DR בשיתוף כל הגורמים הרלוונטיים, כדי לחזק את יכולת העירייה להתמודד עם מצבי חירום ולשמור על רציפות תפקודית.

- ✓ גיבוש תהליך קביעת תוכנית DR בשיתוף גורמים בכירים: לקבוע תהליך מוסדר שבו יגובשו נהלי DR בשיתוף פעולה בין מנהל אבטחת מידע, מנהל מערכות המידע והגורמים הרלוונטיים, כדי להבטיח שהתוכנית תואמת את הצרכים האסטרטגיים והאבטחתיים של העירייה.
- ✓ אישור הנהלה וגורמים מוסמכים: לוודא שהתוכנית עוברת תהליך אישור פורמלי, כדי להבטיח את מחויבות הנהלת העירייה ליישום התוכנית.
- ✓ מעקב ועדכון תקופתי: לקיים ביקורות ועדכונים תקופתיים של התוכנית כדי לוודא שהיא עדכנית ומותאמת לשינויים בטכנולוגיה, באיומים ובצרכים של העירייה.
- ✓ הגדרת זמני התאוששות (RTO/RPO): לקבוע זמני התאוששות ותדירות גיבויים עבור כל מערכת קריטית כדי להבטיח עמידה בדרישות העסקיות והאבטחתיות של העירייה.
- ✓ בחינת תרחישים מגוונים: לקיים תרגילים רנדומליים על ספריות שונות ומערכות קריטיות, כדי להבטיח מענה רחב לאירועים מסוגים שונים.
- ✓ תיעוד וניתוח ממצאים: לתעד את ממצאי התרגילים והבחינות כדי לזהות פערים אפשריים ולשפר את התוכנית והנהלים בהתאם לממצאים.

בהמשך לבקשת הביקורת לבחון את טיב תוכנית ההמשכיות העסקית (BCP) והתייחסותה לנושאים הקריטיים לפעילות העירייה, נמסר כי תוכנית BCP אינה קיימת.

המלצת הביקורת

מומלץ להתחיל בגיבוש תוכנית BCP כוללת, כדי להבטיח את יכולת העירייה לשמור על פעילות תקינה ורציפות תפקודית בעת אירועים חריגים.

- ✓ פיתוח תוכנית BCP מקיפה: להכין תוכנית הכוללת את כל התהליכים הקריטיים לפעילות העירייה, תוך הגדרת סדרי עדיפויות להמשכיות הפעילות במצבים של שיבוש.
- ✓ זיהוי נושאים קריטיים: לערוך ניתוח מפורט לזיהוי נושאים קריטיים ולקבוע אמצעים להבטחת תפקוד רציף, כולל גיבויים, מערכות חלופיות וספקים חיצוניים.
- ✓ תרגול ובדיקת התוכנית: לקיים תרגולים תקופתיים ולבצע בדיקות קבועות של התוכנית כדי לוודא את יעילותה ואת מוכנות הצוותים לשעת חירום.

6. ניתוח וניטור סיכונים

הביקורת ביקשה לבחון את תהליך קביעתה ואישורה של תוכנית התאוששות מאסון (DR) והמשכיות עסקית, כולל מעורבות מנהל אבטחת מידע. ממנהל מערכות המידע והגורמים הרלוונטיים, נמסר כי תוכנית DR אינה קיימת בעירייה.

המלצות הביקורת

אנו ממליצים להתחיל בתהליך גיבוש ואישור תוכנית DR בשיתוף כל הגורמים הרלוונטיים, כדי לחזק את יכולת העירייה להתמודד עם מצבי חירום ולשמור על רציפות תפקודית.

- ✓ גיבוש תהליך קביעת תוכנית DR בשיתוף גורמים בכירים: לקבוע תהליך מוסדר שבו יגובשו נהלי DR בשיתוף פעולה בין מנהל אבטחת מידע, מנהל מערכות המידע והגורמים הרלוונטיים, כדי להבטיח שהתוכנית תואמת את הצרכים האסטרטגיים והאבטחתיים של העירייה.

- ✓ אישור הנהלה וגורמים מוסמכים: לוודא שהתוכנית עוברת תהליך אישור פורמלי, כדי להבטיח את מחויבות הנהלת העירייה ליישום התוכנית.
- ✓ מעקב ועדכון תקופתי: לקיים ביקורות ועדכונים תקופתיים של התוכנית כדי לוודא שהיא עדכנית ומותאמת לשינויים בטכנולוגיה, באיומים ובצרכים של העירייה.
- ✓ הגדרת זמני התאוששות (RTO/RPO): לקבוע זמני התאוששות ותדירות גיבויים עבור כל מערכת קריטית כדי להבטיח עמידה בדרישות העסקיות והאבטחתיות של העירייה.
- ✓ בחינת תרחישים מגוונים: לקיים תרגילים רנדומליים על ספריות שונות ומערכות קריטיות, כדי להבטיח מענה רחב לאירועים מסוגים שונים.
- ✓ תיעוד וניתוח ממצאים: לתעד את ממצאי התרגילים והבחינות כדי לזהות פערים אפשריים ולשפר את התוכנית והנהלים בהתאם לממצאים.

בהמשך לבקשת הביקורת לבחון את טיב תוכנית ההמשכיות העסקית (BCP) והתייחסותה לנושאים הקריטיים לפעילות העירייה, נמסר כי תוכנית BCP אינה קיימת.

המלצת הביקורת

מומלץ להתחיל בגיבוש תוכנית BCP כוללת, כדי להבטיח את יכולת העירייה לשמור על פעילות תקינה ורציפות תפקודית בעת אירועים חריגים.

- ✓ פיתוח תוכנית BCP מקיפה: להכין תוכנית הכוללת את כל התהליכים הקריטיים לפעילות העירייה, תוך הגדרת סדרי עדיפויות להמשכיות הפעילות במצבים של שיבוש.
- ✓ זיהוי נושאים קריטיים: לערוך ניתוח מפורט לזיהוי נושאים קריטיים ולקבוע אמצעים להבטחת תפקוד רציף, כולל גיבויים, מערכות חלופיות וספקים חיצוניים.
- ✓ תרגול ובדיקת התוכנית: לקיים תרגולים תקופתיים ולבצע בדיקות קבועות של התוכנית כדי לוודא את יעילותה ואת מוכנות הצוותים לשעת חירום.

7. ניתוח וניטור סיכונים

בהמשך לבקשתנו לבחון את מערך המעקב אחר פעולות חריגות, כולל ניהול לוגים, משך שמירתם וקיום ניטור SOC/SIEM, נמסר כי קיים מעקב יומיומי אחר התחברות של כל מחשב ומשתמש לרשת, ומערך ניטור SOC מבוצע באמצעות חברה חיצונית.

המלצת הביקורת

מומלץ להגדיר מדיניות זמן שמירת לוגים ולהטמיע מערכת SIEM המאפשרת זיהוי התראות אוטומטיות על פעולות חריגות בזמן אמת.

- ✓ שמירת לוגים: לקבוע פרקי זמן ברורים לשמירת הלוגים בהתאם לדרישות רגולטוריות.
- ✓ ניטור SIEM: להטמיע ניטור מלא שיכלול התראות אוטומטיות, לא רק על התחברויות אלא גם על ניסיונות גישה לא מורשים.

בהמשך לבקשתנו לבחון את נוהלי שמירת 'לוגים' ואת מערך המעקב והבקרה עליהם, נמסר כי 'לוגים' נשמרים בשרת הקבצים באופן יומיומי, ללא הגבלת זמן לשמירתם, וכי אין מערך ניטור המיועד למעקב אחריהם.

המלצת הביקורת

מומלץ לגבש נהלים ברורים לשמירה, ניטור ובקרה של הלוגים.

- ✓ מדיניות שמירת לוגים: לקבוע פרקי זמן לשמירת לוגים ולבצע בדיקות תקופתיות לווידוא תקינותם.
- ✓ מערכת ניטור: להטמיע מערכת SIEM לניהול ובקרה אפקטיביים.

בהמשך לבקשתנו לבחון את אמצעי ההגנה מפני תוכנות מזיקות, נמסר כי קיים פתרון EDR מסוג Harmony של חברת צ׳קפוינט להגנה על עמדות קצה.

המלצת הביקורת
מומלץ לבחון את אפקטיביות מערכת ה-EDR ולוודא כיסוי מלא של עמדות הקצה.
- ✓ לוודא שמערכת EDR פועלת בכל עמדות הקצה ומתבצע תחזוקה ועדכונים שוטפים.
- ✓ לבחון את הצורך באנטי-וירוס נוסף בהתאם לסיכונים הקיימים.

בהמשך לבקשתנו לבחון את מיקומם וניהול הגיבויים של שרתי העירייה, נמסר כי חלק מהשרתים ממוקמים בחדר השרתים של העירייה, חלקם בענן של ספק חיצוני, ורק חלקם מגובים באופן קבוע. צוין כי קיימת חוסר אחידות בניהול השרתים ובתהליך הגיבוי.

המלצת הביקורת
מומלץ להסדיר את ניהול השרתים והגיבויים באמצעות תוכנית אחידה וברורה.
- ✓ תיעוד שרתים: להכין רשימה מסודרת של כל השרתים, כולל מיקומם ותפקידם.
- ✓ מדיניות גיבוי: לקבוע מדיניות גיבוי אחידה לכל השרתים, כולל גיבויים שוטפים ובדיקות תקינות.
- ✓ תכנון ניהול שרתים: לגבש תוכנית מרכזית לניהול השרתים, המשלבת בקרה אחידה בין הסביבות המקומיות והעננית.

במסגרת הביקורת נמצא כי בעירייה אין כיום תוכנית רשמית לניהול תרחישים קריטיים בתחום מערכות המידע. מיפוי מקורות איומים, סיכונים ומצבי קיצון טרם בוצע, דבר שמגביל את יכולת העירייה להיערך למצבים משתנים ולהתמודד עם אירועים בלתי צפויים.
בנוסף, העירייה אינה מבצעת כיום ניתוח תרחישים הקשורים לאיומים אפשריים, כגון מתקפות סייבר, כשלים טכנולוגיים, או פגיעות בשירותים לתושבים. נכון להיום, אין גורם מוגדר בעירייה האחראי לניהול תרחישים וניהול סיכונים, וההתמודדות עם אירועים מתבצעת באופן חלקי בלבד ולעיתים תוך הסתמכות על משאבים מוגבלים ושיתוף פעולה עם ספקים חיצוניים.
למרות זאת, הביקורת מצביעה על הצורך הדחוף בהקמת מסגרת עבודה לתכנון תרחישי ייחוס, הכוללת זיהוי איומים מרכזיים, ניתוח סיכונים, והיערכות באמצעות מערכות טכנולוגיות, נהלים, והדרכות ייעודיות. מסגרת זו תסייע לעירייה לצמצם את החשיפה לאיומים ולהבטיח את רציפות השירותים לתושבים גם במצבי חירום.

חומת האש הקיימת היא מדגם FortiGate-E80, שאינו נתמך עוד, וללא רישיון פעיל כשנתיים. כתוצאה מכך, לא ניתן לעדכן את מערך ההגנה מפני איומים חדשים וקיימים, דבר המגביר את חשיפת העירייה לסיכוני אבטחת מידע.
עוד יוער, כי במהלך שנת 2023 האחראי על המחשוב בעירייה (מטעם החברה לאוטומציה) שלח למנכ״לית העירייה ולגזבר העירייה שלוש הודעות בהן התריע על מצב אבטחת המידע ועל הצורך לשדרג את מערכת האבטחה. לדבריו, פניותיו לא זכה למענה ו/או תגובה.
כמו כן ראוי לציין כי, במהלך הביקורת הועברה הצעת מחיר מחודשת לעדכון תוכנת ״חומת אש״.

המלצת הביקורת
יש לשדרג לאלתר(!!) את חומת האש לדגם עדכני הכולל רישיון פעיל, המאפשר עדכון חוקים ופוליסות אבטחת מידע ועדכונים באופן יומיומי שוטף לזיהוי וטיפול באיומים קיימים ומשתנים.

חלק מהשרתים פועלים על מערכות הפעלה ישנות, כמו : Windows Server 2008/2012/2016 שאינן נתמכות עוד על ידי מיקרוסופט. מצב זה חושף את העירייה לסיכוני אבטחה בשל פרצות אבטחה רבות אשר נחשפו בגרסאות שרת אלו. כמו כן גרסאות אלו אינן מקבלות עדכוני אבטחה חשובים וקריטיים.

המלצת הביקורת

מומלץ לעדכן את מערכות ההפעלה בשרתים לגרסאות נתמכות כדי להבטיח קבלת עדכוני אבטחה שוטפים ותמיכה טכנית מלאה.

8. הטמעה

נכון למועד הביקורת, לא מתבצעות הדרכות לעובדים בנושא אבטחת מידע או סימולציות תקופתיות להתמודדות עם איומים פוטנציאליים.

המלצת הביקורת

יש להטמיע תוכנית הדרכות שוטפת לכלל העובדים, עם דגש על עובדים הנחשפים למידע רגיש. התוכנית צריכה לכלול סימולציות תקופתיות להגברת המודעות וההיערכות לאיומים.

למרות שיתופי פעולה חלקיים עם ספקים חיצוניים, אין תוכנית סדורה לניהול ושדרוג המערכות הקיימות, מה שעלול לפגוע ביכולת העירייה לשמור על פעילות רציפה ולהגיב ביעילות לאירועים חריגים.

המלצת הביקורת

מומלץ להסדיר שיתופי פעולה עם ספקים חיצוניים באמצעות הסכמי שירות (SLA) מוגדרים היטב. בנוסף, יש להקים תהליכי עדכון ושדרוג שוטפים של מערכות האבטחה כדי להתמודד עם שינויים טכנולוגיים ורגולטוריים ולהפחית את הסיכונים.

החיבור מרחוק למערכות העירייה מתבצע באמצעות FortiClient, אך ללא יישום של מנגנון אימות דו-שלבי (FA2). חיבור זה מיועד למשתמשים מסוימים בלבד, אך בהיעדר בקרות אבטחה נוספות, קיים סיכון לגישה בלתי מורשית במקרה של הדלפת אישורי התחברות או מתקפות התחזות (phishing). בנוסף, היעדר אימות מחוזק מקשה על זיהוי ונטרול גישה לא חוקית בזמן אמת, במיוחד כאשר אין מדיניות ברורה לניהול חיבורים מרחוק או ניטור פעילויות חריגות. מצב זה מגדיל את הסיכון לחשיפת מידע רגיש ולפגיעה ברציפות התפקודית של מערכות העירייה במקרה של ניסיון חדירה עוין.

המלצת הביקורת

מומלץ להטמיע מנגנון אימות דו-שלבי (FA2) לכל המשתמשים המורשים להתחבר מרחוק, תוך שימוש בפתרון FortiToken, המותאם באופן טבעי לסביבת FortiClient. כמו כן, יש לבחון יישום מדיניות בקרת גישה מוגברת, הכוללת הגבלת כתובות IP מורשות, ניטור חיבורים מרחוק והתראה על ניסיונות כניסה חריגים.

סיכום והמלצות – מוני מים

1. כללי

1.1. במסגרת תכנית העבודה לשנת 2024, ערך מבקר העירייה, בסיוע חברת "גדיר הנדסה" סקר מוני מים, שעיריית יקנעם עילית נושאת בעלות הצריכה השוטפת.

1.2. בסקר, נבדקו כלל מוני המים בגינם משלמת עיריית יקנעם את חשבונות הצריכה השוטפים.

1.3. הסקר נועד לוודא שחשבונות המים המשולמים על ידי העירייה משמשים את העירייה ועובדיה ואת המבנים שבבעלותה/שימושה, לאתר צריכות מים חריגות ולאתר פיצוצים ונזילות ובמטרה להקטין את ההוצאות השוטפות בגין צריכת מים.

2.1 מונים בעלי מחלקה לא מדויקת

בסקר נמצאו 2 מונים בעלי מחלקה לא מדויקת. כלומר, השיוך הנוכחי שלהם בעירייה לא תואם את מה שנמצא בשטח:

2.1.1 דרכי פעולה והמלצות:

העברת רשימת המונים עם שינוי מחלקה לגזברות העירייה על מנת לבחון אפשרות לשינוי מחלקות לחיוב לאותם מונים.

2.2 מונים בעלי כתובת לא מדויקת

במסגרת הסקר אותרו 140 מונים בעלי כתובת לא מדויקת. כלומר, מיקום המונים בשטח נמצא בכתובת אחרת ממה שרשום בכתובת של תאגיד המים:

2.2.1 דרכי פעולה והמלצות:

פנייה מרוכזת לתאגיד המים ע"מ לשנות את כתובות המונים הנ"ל לפי מה שאותר במיפוי בשטח

2.3 מונים בעלי שם אתר לא מדויק:

במסגרת הסקר פורט עבור כל מונה את שם אתר העירייה המוזן מאותו מונה, ע"מ לעקוב אחר צריכת המים של כל אתר מאתרי העירייה.

2.3.1 דרכי פעולה והמלצות:

לבצע פנייה מרוכזת לתאגיד המים ע"מ לשנות את שמות אתרי העירייה הרשומים על אותם מונים.

2.4 מונים שלא אותרו בסקר:

במסגרת הסקר לא אותרו בשטח 40 מונים.

2.4.1 דרכי פעולה והמלצות:

יש לפנות לתאגיד המים ע"מ לתאם סיור משותף עם נציג מטעם העירייה לאיתור המונים שלא אותרו בסקר.

2.5 מונים בעלי חריגות וליקויים:

במסגרת הסקר נמצאו 19 מונים שנמצאו בהם חריגות וליקויים שיש לתקנם.

5 ליקויים הינם ליקויי מונה שבאחריות תאגיד המים לתקנם ו-14 ליקויים הינם מאזור המונה שבאחריות העירייה לדאוג לתיקונם.

2.5.1 דרכי פעולה והמלצות:

א. יש לשלוח את רשימת המונים עם ליקויי המונה לתאגיד המים ע"מ שיטפלו בנושא.

ב. את רשימת המונים עם תקלות מאזור המונה יש לשלוח לאגף תחזוקה בעירייה ע"מ שיטפלו בליקויים שיתגלו במהלך הסקר.

2.6 חשד לחיבור צרכנים זרים:

במסגרת הסקר אותרו 19 חוזים שיש בהם חשד לצרכנים זרים העושים שימוש באתרים שעליהם העירייה משלמת:

2.6.1. המלצות ודרכי פעולה:

יש להעביר את רשימת המונים החשודים בחיבור צרכן זר לגזבר העירייה ע"מ לבדוק את האתרים הנ"ל.

2.7 מונים עם צריכות נמוכות:

במסגרת הסקר אותרו 104 מונים עם צריכה שנתית הקטנה מ-10 קוב בשנה כמפורט בטבלה הבאה:

2.7.1 המלצות ודרכי פעולה:

על העירייה לבדוק את האפשרות לויתור על מונים אלה ע"מ לחסוך בתשלומי קבע על החזקת מונים אלו.

2.8 מונים עם קריאות מונה במיפוי גבוהות מקריאות מונה ברשומה:

במסגרת הסקר אותרו 2 מונים אשר קריאת המונה בשטח היתה נמוכה מקריאת המונה שקיבלנו מתאגיד המים טרם תחילת המיפוי בשטח כמפורטים בטבלה הבאה:

2.8.1 המלצות ודרכי פעולה:

יש לפנות לתאגיד המים לבירור הנושא ולבחון אפשרות של קבלת החזרים רטרו-אקטיביים על הפרשי הקריאות.

סקר מוני חשמל – סיכום והמלצות

1. כללי

במסגרת תכנית העבודה לשנת 2024, הביקורת ערכה סקר מקיף של כלל מוני החשמל בגינם משלמת העירייה את הצריכה החודשית.
הסקר נערך בסיוע חברת "גדיר הנדסה", במטרה למפות את כלל מוני החשמל ולאתר חריגות ו/או חוסר התאמות במידע הניתן על ידי חברת חשמל.

כחלק מהסקר נבדקו ומולאו הנתונים הבאים:

א. קריאת צריכה נוכחית של מוני החשמל.
ב. זיהוי הכתובות של מוני החשמל כולל מיקום מדוייק של כל מונה בקורדינטות GPS.
ג. אימות שמות האתרים אותם מזינים מוני החשמל.
ד. אימות השיוך המחלקתי של המונים למחלקות העירייה השונות (חינוך, רווחה וכדומה).
ה. איתור ליקויים בטיחותיים ואחרים במוני החשמל.
ו. איתור צרכנים זרים העושים שימוש במוני החשמל של העירייה ללא רשות.

2. **ריכוז הממצאים**

2.1 מונים בעלי מחלקה לא מדויקת

בסקר נמצאו 43 מונים עם חשד לשיוך מחלקה לא מדויק. כלומר, יש חשד שהשיוך הנוכחי שלהם בעירייה לא תואם את מה שנמצא בשטח.

2.1.1 דרכי פעולה והמלצות:

העברת רשימת המונים עם שינוי מחלקה לגזברות העירייה על מנת לבחון אפשרות לשינוי מחלקות לחיוב לאותם מונים.

2.2 מונים בעלי כתובת לא מדויקת

בסקר נמצאו 26 מונים בעלי כתובת לא מדויקת. כלומר, מיקום המונים בשטח נמצא בכתובת אחרת ממה שרשום בכתובת של חברת חשמל.

2.2.1 דרך פעולה והמלצות:

פנייה מרוכזת לחברת החשמל, על מנת לשנות את כתובות המונים הנ"ל לכתובות שאותרו בסקר.

2.3 מונים בעלי שם אתר לא מדויק

במסגרת הסקר פורט עבור כל מונה שם אתר העירייה המוזן מאותו מונה, ע״מ לעקוב אחר צריכת כל אתר מאתרי העירייה.

2.3.1 דרכי פעולה והמלצות:

לבצע פנייה מרוכזת לחברת החשמל, על מנת לשנות את שמות אתרי העירייה הרשומים על אותם מונים.

2.4 מונים שלא אותרו בסקר

במסגרת סקר לא אותרו בשטח 12 מונים:

2.4.1 דרכי פעולה והמלצות:

יש לפנות לחברת החשמל, דרך מנהל הלקוח של חברת חשמל בעירייה, ולבקש לאתר את המונים שלא אותרו במהלך הסקר.

2.5 מונים בעלי חריגות וליקויים

בסקר נמצאו 22 מונים שנמצאו בהם חריגות וליקויים שיש לתקנם.

20 מתוכם בעלי לוחית מונה עכורה ועוד שני (2) מונים בעלי ליקויים אחרים.

2.5.1 דרכי פעולה והמלצות:

(1) נמצאו 20 מונים אשר חלון ה״פילר״ בו הם נמצאים עכור, דבר המונע לקיחת קריאה מדויקת. יש לפנות לחברת החשמל על מנת שיטפלו בנושא.
(2) מס׳ חוזה 340607485- מקלט 19 ברח׳ כלניות 8: הדיסק בתוך המונה לא מסתובב למרות שהחשמל במקלט עובד. על העירייה לפנות לחברת חשמל על מנת שהנושא יטופל. ייתכן שהעירייה תידרש לשלם הפרשים בשל צריכות קודמות.
(3) מס׳ חוזה 340824237- בית ספר ארזים ברחוב אלונים 31: אין מסך קריאה למונה, יש לפנות לחח״י ע״מ שיטפלו בנושא.

2.6 חשד לחיבור צרכנים זרים

בסקר אותרו 26 חוזים שיש בהם חשד לצרכנים זרים העושים שימוש באתרים שעליהם העירייה משלמת:

2.6.1. המלצות ודרכי פעולה:

יש להעביר את רשימת המונים החשודים בחיבור צרכן זר לגזבר העירייה ע״מ לבדוק את האתרים החשודים.