דו"ח מבקר המועצה לשנת 2019

בצירוף הערות ראש המועצה

דו"ח ביקורת – תקנות הגנת הפרטיות ואבטחת מידע

ריכוז עיקר הממצאים

1. כללי

התפתחות עולם מערכות המידע במהלך העשורים האחרונים והשימוש ההולך וגובר שנעשה במערכות המידע בכל סוגי הארגונים, הפך מערכות אלו למשאב חיוני בכל ארגון. הגברת שימוש במערכות מידע והגברת השימוש במאגרי מידע תוך הרחבת אספקת שירותים דיגיטליים לתושבים בשנים אחרונות, מגביר את הסיכון כי מידע אישי ייחשף ברבים בזדון או בתום לב ויפגע בפרטיות התושבים והעובדים של המועצה.

ניהול מערכות המידע במועצה נעשה **במיקור חוץ**, שעוסק בכל ההיבטים של ניהול מערכות המידע, לרבות תשתיות ותקשורת, מערכות ליבה, עזר ותחזוקה, וכן הן בהיבט של פיתוח והטמעה והן בהיבט של התפעול השוטף.
חוק הגנת הפרטיות, התשמ"א – 1981 (להלן: "החוק") הגדיר את המונחים "אבטחת מידע", "מאגר מידע", ו"מידע".

בחודש מאי 2017 פורסמו מכוח החוק, תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017 (להלן: "התקנות"). 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.

במועד הביקורת לא היה במועצה ממונה אבטחת מידע כנדרש בתקנות.

להלן עיקר הממצאים:

1.1 מדיניות אבטחת מידע ונהלי אבטחת מידע

סעיף 3 (2) לתקנות קובע כי "הממונה על הבטחה יכין נוהל אבטחת מידע ויביאו לאישור בעל המאגר".
הביקורת מצאה כי, במועצה לא הוגדרו מסמך מדיניות אבטחת וסט נהלים בהיבטי אבטחת מידע. מסמך מדיניות אבטחת מידע ונהלים נדרשים להיות מאושר על ידי המנכ"ל המועצה.

1.2 <u>ממשל תאגידי בהיבטי אבטחת מידע</u>

סעיף 17ב. לחוק הגנת הפרטיות קובע כי המועצה מחויבת כגוף ציבורי למנות אדם בעל הכשרה מתאימה לתפקיד הממונה על אבטחת מידע.

סעיף 3 לתקנות קובע:

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

הביקורת מצאה כי, לא מונה באופן רשמי ממונה אבטחת מידע במועצה. בפועל מנהל מערכות מידע מכהן גם בתפקיד של ממונה אבטחת מידע במועצה אשר אמור לבקר ולפקח על העמידה בדרישות התקנות הגנת הפרטיות. במצב הנוכחי קיימים ניגודי עניינים בין תפקיד מנהל מערכות מידע לממונה אבטחת מידע. מנהל מערכות מידע אחראי ליישום בפועל של תכנית עבודה שוטפת בהיבטי מערכות מידע ובתפקיד הממונה למעשה מבקר ומפקח על פעולותיו.

1.3 <u>תקציב אבטחת מידע</u>

סעיף 3(6) לתקנות קובע כי "בעל מאגר המידע יקצה לממונה את המשאבים הדרושים לו לשם מילוי תפקידו."

החלטה מספר 2443 של רשות התקשוב הממשלתית מ-15.2.15 בנושא "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" קובעת בין היתר, כי "המנכ"לים של משרדי הממשלה ומנהלי יחידות הסמך, במסגרת סמכותם ואחריותם הקיימת, יסדירו את מבנה התקציב השנתי של משרדם כך שלכל הפחות 8% מתקציב תחום טכנולוגיית המידע יופנה להגנת הסייבר"

נמצא כי תקציבי אבטחת מידע אינם מוצגים לאישור הנהלה הבכירה של המועצה ואינם נידונים באופן ייעודי, התקציבים נכללים במסגרת סך תקציב מחלקת מערכות מידע.

1.4 <u>סקרי אבטחת מידע ומבדקי חדירה</u>

בסעיף 5 בתקנות הגנת הפרטיות נקבע כדלקמן:

"(ג) במאגר מידע שחלה עליו רמת האבטחה הגבוהה, בעל המאגר אחראי לכך שייערך סקר לאיתור סיכוני אבטחת מידע (להלן: "סקר סיכונים"); בעל מאגר המידע ידון בתוצאות סקר הסיכונים שיועברו לו, יבחן את הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבותיהן, ויפעל לתיקון הליקויים שהתגלו במסגרת הסקר, ככל שהתגלו; סקר סיכונים כאמור ייערך אחת לשמונה עשר חודשים לפחות..."

מבדיקת הביקורת נמצא כי, טרם בוצע סקר סיכונים להערכת סיכוני אבטחת מידע ומבדקי חדירה לבדיקת אפקטיביות מערך אבטחת מידע. אכן לפי התקנות קיימת חובה לביצוע במאגר ברמת אבטחה גבוהה בפועל מדובר בפרקטיקה מקובלת גם אם מנוהל מאגר ברמות אבטחה נמוכות יותר. המועצה בנוסף לתקנות הגנת הפרטיות מחויבת לספק שירותים כולל שירותי חירום לתושביה וגופים חיצוניים. מתקפת סייבר עלולה להשבית פעילות שוטפת של המועצה ולפגוע ברמת שירות מעבר לפגיעה בפרטיות.

1.5 <u>הדרכות עובדים</u>

סעיף 7 לתקנות 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..."

מבדיקת הביקורת עלה כי, העובדים בכניסתם לעבודה אינם חותמים על מסמך הנחיות אבטחת מידע ולא מקבלים תדריך אבטחת מידע כנדרש בתקנות.

כמו כן, טרם בוצעה הדרכה לכלל העובדים במועצה בנושאי אבטחת מידע והגנת הפרטיות עם מצגת ייעודית המכסה תכנים נדרשים.

1.6 בקרת הרשאות גישה

בסעיף 8 בתקנות ניהול הרשאות גישה נרשם כדלקמן:

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".

נמצא כי, לא קיים טופס בקשת הרשאות הכולל פרטים נדרשים כגון: גישה לאינטרנט, גישה לכונן מחלקתי, דוא"ל, גישה מרחוק, קבוצות הרשאות למסכים במערכות ועוד.

הביקורת מצאה כי, טרם בוצע מיפוי מדויק במועצה של איזה סוגי הרשאות נדרשות ברמת כל תפקיד כנדרש בתקנות. מתן הרשאות באמצעות העתקת הרשאות מעובד אחר עלול לגרום לכך שעובד חדש עלול לקבל הרשאות עודפות שצבר עובד ותיק שלא בהכרח נחוצות לו למילוי תפקידו.

כמו כן, טרם בוצע תהליך תקופתי של תיקוף הרשאות גישה קיימות לכלל מורשי גישה באמצעות סקירת הרשאות על ידי מנהלי המאגרים. במסגרת תהליך תיקוף כזה כל מנהל מאגר נדרש לקבל הרשאות גישה לכל מאגר פר משתמש ולקבוע אם עדיין הרשאה זו נחוצה לכל משתמש או מדובר בהרשאה עודפת.

1.7 בקרה ותיעוד גישה

סעיף 10 לתקנות קובע כי ינוהל מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למערכות המאגר, התיעוד יכלול: זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה. בנוסף, מנגנון הבקרה לא יאפשר ביטול או שינוי של הפעלתו; וכן יקבע נוהל בדיקה שגרתי של נתוני התיעוד של מנגנון הבקרה. נתוני התיעוד של מנגנון הבקרה יישמרו למשך 24 חודשים לפחות.

לביקורת נמסר על ידי מנהל מחלקת מערכות מידע כי, טרם בוצע תהליך מיפוי מקיף ברמת כל מאגר ומערכת מאגר האם אכן מנגנון תיעוד אוטומטי לפעולות משתמשים עומד בדרישות התקנות, לרבות שמירת תיעוד לתקופה של 24 חודש. טרם נקבע נוהל בדיקה שגרתי של נתוני התיעוד כפי שנדרש בתקנות.

בנוסף נמצא כי במערכת שקד של חברת מגע"ר קיים שימוש במשתמש משותף על ידי צוות גבייה. מדובר בהרשאה משותפת שלא מאפשרת בקרה על זהות מבצעי פעולות. למותר לציין כי מדובר במערכת כספית שלכל פעולה בה משמעות כספית למועצה.

1.8 <u>קיום הגנה אפקטיבית כנגד מתקפות מתוחכמות</u>

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."

נמצא כי, במועצה קיים שימוש במערכת חומת אש, אנטי וירוס, מסנני תוכן לדוא"ל. שירותי חומת אש ומסנני תוכן באינטרנט ודוא"ל מסופקים על ידי חברה לאוטומציה בעלת תקן ISO27001.

יחד עם זאת, לדעת הביקורת יש ליישם שכבות הגנה נוספות (ראה פירוט בס' 5.8 בגוף הדוח) .

1.9 <u>אבטחת טלפונים ניידים וטאבלטים</u>

השימוש בטלפונים ניידים של בעלי תפקידים בביצוע עבודתם במועצה חושף את נתוני המידע של המועצה בפני אפליקציות זדוניות.

נמצא כי אין במועצה הגנה על טלפונים ניידים למרות שבארגונים רבים קיים כיום שימוש בטכנולוגיה לניהול ואבטחת התקנים ניידים (MDM) המספקת הגנה מלאה על המידע הנמצא במכשיר, מבלי לפגוע בפרטיות המשתמש.

1.10 אבטחת התקנים ניידים

סעיף 12 לתקנות קובע 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."

נמצא כי, לא מיושמת חסימה למניעת חיבור מדיה נתיקה לתחנות קצה, כיום כלל המשתמשים מורשים לחבר כל מדיה נתיקה וגם בכל מחשבים ניידים פתוחה הגישה. המשמעות היא שקיימת חשיפה רבה להחדרת נוזקה (תוכנה זדונית) שלא תזוהה באמצעות אנטי-וירוס המותקן במערכות המועצה וכן חשיפה לסיכונים נוספים של זליגת מידע רגיש.

1.11 מדיניות בקרת גלישה באינטרנט

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."

כיום הגלישה באינטרנט מבוצעת דרך חומת אש ומופעל מודול סינון אתרים וקבצים. המודול אמור לחסום גישה לקטגוריות של אתרים שמוגדרים כחסומים לגלישה כמו אתרים עם תוכן לא הולם וגם לחסום הורדה של קבצים בפורמטים לא מורשים.

נמצא כי, מדיניות הגלישה מתירנית כאשר לא מיושמת חסימה של כל קטגוריות מסוכנות כמו אתרי דוא"ל חינמי למשל gmail, אתרי שיתופי

ואחסון קבצים כמו google drive , אתרי הפצת תוכנות כמו github. בנוסף לא קיימת חסימה להורדה של קבצי הרצה וסקריפטים.

1.12 הרשאות אדמיניסטרטור

מרבית הנוזקות כיום מנצלות הרשאות של משתמשי קצה על מנת לבצע פעולות זדוניות במערכות מחשב. לאור זאת הבקרה המומלצת כיום הינה כי, למשתמשי קצה יוקצו הרשאות נמוכות ביותר ברמת מערכת ההפעלה.

נמצא כי, בכל תחנות קצה קיימת עדיין הרשאה של לוקל אדמין למשתמש קצה המאפשרת לו לבצע התקנה של תוכנות וביצוע שינויים בהגדרות מחשב. הרשאה זו יכולה להיות מנוצלת על ידי נוזקות זדוניות לרוץ בהרשאות גבוהות ומגבירה את סיכויים לכך שנוזקה תבצע את זממה.

1.13 מערכת מניעת חיבור התקנים זרים לרשת המועצה

בהינתן גישה פיזית של גורם זדוני למשרדי הארגון, הגורם יכול לבצע ניסיון חדירה באמצעות חיבור מחשב או התקן זר לרשת הפנימית תוך קבלת כתובת IP תקינה ברשת. באופן זה למעשה הגורם הזדוני עוקף מנגנוני אבטחה היקפיים המיושמים ברשת לרבות חומת אש.

נמצא כי, לא מיושמת טכנולוגית NAC ברשת הפנימית של המועצה. העדר טכנולוגיה זו לא מנעה מצוות הביקורת לחבר לרשת הפנימית של המועצה מחשב נייד חיצוני ורכיב USB לצורך ביצוע סימולציות של חדירה לרשת הפנימית.

1.14 אבטחת גישה מרחוק

בסעיף 14 (ג) בתקנות 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."

הביקורת מצאה כי, לא מיושמת הזדהות חזקה גישה מרחוק למערכות המועצה. בנוסף נמצא כי כיום למנהל מערכות מידע קיימת שליטה מרחוק לכל המחשבים במועצה דרך מערכת שליטה מרחוק team viewer. מדובר בהרשאה רגישה ביותר ושימוש בהרשאה זו גם לא מחייב שימוש בסיסמה חד פעמית.

1.15 <u>ניטור, דיווח ותגובה לאירועי אבטחת מידע</u>

כאמור, בעל מאגר מידע אחראי לתיעוד כל מקרה שבו התגלה אירוע המעלה חשש לפגיעה בשלמות המידע. בנוסף, יש לקבוע בנוהל האבטחה הוראות לעניין התמודדות עם אירועי אבטחת מידע, לפי חומרת האירוע ומידת רגישות המידע, לרבות לעניין ביטול הרשאות וצעדים מידיים אחרים הנדרשים וכן לעניין דיווח לבעל המאגר על אירועי אבטחה ועל פעולות שננקטו בעקבותיהם.

מבדיקת הביקורת נמצא כי לא קיימים נהלים מפורטים לאיתור, תגובה ותרגול של אירועי סייבר מבוססי תרחישים, לצורך התמודדות עם סוגים שונים של איומים. לא מנוהל מאגר ידני או אוטומטי לתיעוד כלל אירועי אבטחת מידע, לרבות אירועים פוטנציאליים. לא מתקיימים דיונים באירועי האבטחה בפורום מנכ"ל כנדרש בתקנות. לא הוקם צוות תגובה מקצועי אשר ייתן מענה מהיר ואפקטיבי במקרה של התרעה על אירוע סייבר. מנהל מערכות לבדו מקבל התרעות ודיווחים על אירועי אבטחה. לא מתקיימים תרגולים תקופתיים לתרגול תגובה לאירועי סייבר.

1.16 <u>מיקור חוץ</u>

המועצה רוכשת שירותים ממספר ספקי מיקור חוץ הידועים בתחום כגון : חברה לאוטומציה המספקת מערכות ליבה מרכזיות, חברת מגע"ר המספקת מודול לניהול גביית חובות וכו'.

הביקורת מצאה כי חלק מהסכמי ההתקשרות של המועצה אינם מעודכנים בהתאם לתנאים שנקבעו בתקנות הגנת הפרטיות. לדעת הביקורת יש צורך לעדכן את ההסכמים ולהתאימם לדרישות החוק.
בנוסף נמצא כי, טרם בוצע במועצה מיפוי של כלל הספקים של המועצה המחזיקים במידע רגיש או בעלי הרשאת גישה למידע רגיש וזאת על מנת לקבוע דרכי פיקוח ובקרה אליהם.

1.17 <u>רישום וניהול מאגרי מידע</u>

החוק מחייב את בעל מאגר מידע לרשום את המאגר אצל רשם המאגרים במשרד המשפטים.
מבדיקת הביקורת נמצא כי במשרד המשפטים רשומים על שם המועצה שני אגרי מידע בלבד.
עוד נמצא כי אין למועצה מידע על כל מאגרי המידע הקיימים ברשותה הדרושים ניהול ורישום בהתאם לדרישות החוק.

1.18 <u>מבדקים טכנולוגיים לבדיקת אפקטיביות של מערך האבטחה ברשת הפנימית, באתר האינטרנט ובכתובות החיצוניות של המועצה</u>

צוות הביקורת ערך מבדקים שונים במטרה לבחון את יעילות מערך האבטחה של המועצה ולזהות חולשות, במידה שקיימות, תוך דימוי מתקפת סייבר ממוקדת. הבדיקות בוצעו מרשת האינטרנט ומתוך הרשת הפנימית.
מבדיקת הביקורת נמצא כי ההגנות הקיימות כיום אינם מספקות ויש לבצע מספר פעולות נוספות למניעת סיכונים לפעולות זדוניות (ראה פירוט בפרק 5.20 בדוח המפורט).

2. <u>סיכום והמלצות:</u>

הביקורת מצאה כי המועצה אינה ערוכה בהתאם לדרישות החוק בנושא תקנות הגנת הפרטיות ואבטחת מידע.

על המועצה לפעול וליישם את ההמלצות שהוצגו בפירוט בדוח ביקורת זה ולקדם ולהסדיר את נושא אבטחת המידע וניהול מאגרי מידע במועצה האזורית שער הנגב.

להלן ההמלצות:

מדיניות אבטחת מידע ונהלי אבטחת מידע

1. להשלים בהקדם כתיבה, עדכון אשור והטמעה של מסמך מדיניות אבטחת מידע וכל הנהלים וטפסים הנדרשים בהתאם לתקנות הגנת הפרטיות.
2. להגיש את הנהלים ושינויים מהותיים בהם לאישור מנכ"ל המועצה.

ממשל תאגידי בהיבטי אבטחת מידע

3. מומלץ כי, ימונה ממונה אבטחת מידע במועצה בעל הכשרה מתאימה שאינו מנהל מערכות מידע, הממונה לא ימלא תפקיד נוסף שעלול להעמידו בחשש לניגודי עניינים. לצורך המינוי יוכן כתב מינוי שיכלול תפקידיו, אחריותו וסמכויותיו של ממונה וכפיפותו.
4. מומלץ כי הממונה יכין תכנית בקרה שוטפת לעמידה בתקנות, יגיש לאישור ההנהלה וידווח על ביצועה להנהלה ומנהלי מאגרים.
5. 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.

תקציב אבטחת מידע

6. לקבוע מנגנון לקביעת תקציב אבטחת מידע כאחוז אובייקטיבי מסך תקציב מחלקת מערכות מידע.
7. להציג את התקציב אבטחת מידע המפורט לאישור במסגרת ישיבת ועדת היגוי השנתית ברשות מנכ"ל.

סקרי אבטחת מידע ומבדקי חדירה

8. ליזום ביצוע סקרי אבטחת מידע ומבדקי חדירה כנדרש בתקנות במערכות ותשתיות המועצה או בהתאם לתקנים מקובלים כמו תורת הגנת הסייבר בתדירות שתקבע על מנת לספק מענה לתרחישים מגוונים בנוסף לפגיעה בפרטיות.
9. לדרוש מספקי מיקור חוץ של מערכות המשמשות את המועצה להציג בתדירות שתקבע תוצאות סקרי אבטחה ומבדקי חדירה.
10. לקיים דיון בוועדת היגוי בתוצאות סקרים ומבדקי חדירה.
11. לקבוע תכנית עבודה, לו"ז ותיעדוף לתיקון הליקויים שמתגלים ולדווח תקופתית לוועדת היגוי.
12. לקבוע תכנית מפורטת פר מערכת ומאגר לביצוע סקרים ומבדקי חדירה במערכות המאגר כנדרש בתקנות. במסגרת זו יש לקבוע לכל מאגר את רמת האבטחה המתאימה.

הדרכות עובדים

13. לפעול לכך כי, מסמך הצהרת סודיות והנחיות לעובד שיכיל בתוכו כללי אבטחת המידע ייחתם בכניסה לעבודה. המסמך יכלול כללי אבטחת המידע אותם נדרש לקיים העובד, אשר יתייחסו לשימוש נאות במחשבי המועצה, שימוש באינטרנט, היבטי אבטחה פיזית לרבות גריסת ניירת, חוזק סיסמאות, שולחן נקי, נעילה של חומרים רגישים במגירות, ליווי אורחים.
14. לבצע הדרכות מודעות בהיבטי אבטחת מידע והגנת הפרטיות לעובדים חדשים ועובדים קיימים במועצה כנדרש בתקנות כולל הטמעת מנגנון שמבטיח כי כל העובדים, להם יש גישה למערכות המועצה ולמאגרי המידע, יעברו הדרכה לפני קבלת הרשאה ויקבלו הדרכה תקופתית. לדוגמה אפשר ליצור טופס טיולים נכנס שיכיל סעיף לחובת ביצוע תדריך אבטחה ותיעוד לחתימת עובד ועובד מדריך. בנוסף לתעד את דבר ביצוע במערכת כוח אדם לרבות תאריך אחרון של הדרכה וכך ניתן יהיה לעקוב באופן אפקטיבי.

בקרת הרשאות גישה

15. לבצע מיפוי מדויק של סוגי הרשאות נדרשות ברמת כל תפקיד למערכות מאגרים.

16.לבצע תיקוף תקופתי של נאותות הרשאות בכל המאגרים תוך מעורבות כל מנהל המאגר בנוגע להרשאות הגישה למאגר עליו הוא אחראי.

17.להתאים טופס קליטת עובד חדש שיאפשר תיעוד מדויק של סוגי הרשאות שנדרש להגדיר לעובד פר מאגר מידע.

18.לבטל פרקטיקה של מתן הרשאות לעובד חדש כמו לעובד קיים על מנת לא לגרום למצבים של עודף הרשאות.

בקרה ותיעוד גישה

19. להגדיר נוהל בדיקה שגרתי של תקינות נתוני התיעוד בכל המאגרים כולל מערכות מאגרים שמסופקים על ידי ספקי מיקור חוץ ברמת סיכון בינונית וגבוהה ולדווח על תוצאות בדיקה לוועדת היגוי.

20. בהתאם לתוצאות הבדיקה לבצע תיקונים נדרשים בכל מנגנון תיעוד על מנת לעמוד בדרישות התקנות.

21. להגדיר משתמש אישי לכל עובד במערכת שקד של חברת מגע"ר.

קיום הגנה אפקטיבית כנגד מתקפות מתוחכמות

22. להפעיל מודולים והגדרות נוספות במוצרי אבטחה הנמצאים בשימוש המועצה לשיפור אפקטיביות המוצרים להתמודדות עם מתקפות סייבר.

23. יש לבדוק מול חברה לאוטומציה בנוגע להיקף חבילת שירותי אבטחת מידע המתקבלים ממנה.

24. לשקול יישום טכנולוגיות מתקדמות נוספות בהיבטי עלות תועלת על מנת להשיג יכולת נאותה להתמודד עם מתקפות סייבר מתוחכמות.

אבטחת טלפונים ניידים וטאבלטים

25. מומלץ לבחון ליישום הפתרון MDM ועד להשלמת יישום להפעיל מנגנוני אבטחה בסיסיים לצמצום הסיכון.

אבטחת התקנים ניידים

26. מומלץ לבחון לבצע חסימה גורפת של אפשרות חיבור מדיה נתיקה למערכות המועצה.

27. במידה וקיים צורך עסקי להגביל אותו למשתמשים מורשים בלבד תוך שימוש במנגנונים לצמצום הסיכון כתוצאה מחיבור כגון: טכנולוגיה

להצפנת נתונים, הגבלת חיבור התקנים שאושרו מראש בלבד, יישום מנגנון הלבנה לפני חיבור, יישום מודול DLP ועוד.

28. יש לבצע הצפנת דיסקים קשיחים בכל מחשבים ניידים.

מדיניות בקרת גלישה באינטרנט

29. יש לבדוק מחדש את מדיניות הגלישה המתירנית הקיימת כיום במועצה ולהטמיע מדיניות גלישה מחמירה יותר לכל קבוצות העובדים בהתאם לעקרון של אפשרות גלישה לצורכי עבודה בלבד תוך צמצום סיכונים לזליגת מידע רגיש תוך חסימת קטגוריות נוספות, כמו אתרי דוא"ל חינמי, שיתופי קבצים, פרוקסי ועוד.

30. יש לבדוק את הגדרות סינון הקבצים הקיימת כיום במטרה למנוע הורדת קבצי הרצה וסקריפטים מאינטרנט.

31. יש לבדוק תקינות מנגנון DEEP SSL INSPECTION בחומת אש.

הרשאות אדמיניסטרטור

32. לבצע הסרה של הרשאות לוקל אדמין מכל המשתמשים הרגילים בתחנות קצה.

33. להשתמש בכלי LAPS של מיקרוסופט לניהול משתמש לוקל אדמין המשמש את טכנאים בתחנה.

מערכת מניעת חיבור התקנים זרים לרשת המועצה

34. לבחון הטמעה של טכנולוגית NAC ייעודית בכל הרשת הפנימית או לכל הפחות טכנולוגיה NPS הזמינה במערכת הפעלה.

אבטחת גישה מרחוק

35. ליישם בהקדם צורת הזדהות חזקה בגישה מרחוק למערכות המאגרים ברמת אבטחה בינונית וגבוהה לרבות מערכות בספקי מיקור חוץ החשופות לאינטרנט.

ניטור, דיווח ותגובה לאירועי אבטחת מידע

36. מומלץ לבחון יישום טכנולוגיה SIEM ושירות מוקד SOC חיצוניים.

37. מומלץ לבחון שימוש בשירות מודיעין סייבר מקצועי ייעודי למועצה.

38. מומלץ לכתוב נהלים לאיתור, תגובה ודיווח על אירועי סייבר.

39. מומלץ להקים צוות ייעודי לתגובה לאירועי סייבר ולבצע תרגולים תקופתיים של הצוות.
40. מומלץ לנהל מאגר ידני או אוטומטי לתיעוד כלל אירועי אבטחת מידע, לרבות אירועים פוטנציאליים.
41. מומלץ לדווח על אירועי אבטחת מידע לוועדת היגוי בהתאם לנדרש בתקנות.
42. מומלץ לבצע תרגולים תקופתיים לתרגול תגובה לאירועי סייבר.

מיקור חוץ

43. ליישם תהליך ניהול סיכוני אבטחת מידע של ספקי מיקור חוץ בהתאם לנדרש בתקנות.
44. פעם בתקופה לקבל ולבחון את תוצאות סקרי אבטחת מידע שבצעו ספקי מיקור חוץ של המועצה ובהתאם לתוצאות בחינה לבחון בנקיטת צעדים נוספים לבקרה ופיקוח כגון ביצוע ביקורת עצמאית בכותלי הספק.
45. לקבל מספקי מיקור חוץ באופן תקופתי את התקנים ותצהירים המעידים על עמידה בתקנות הגנת הפרטיות.
46. לוודא כי הסכמים עם ספקי מיקור חוץ עומדים בכל דרישות סעיף 15 בתקנות.
47. לבצע מיפוי של כלל ספקים המחזיקים או בעלי הרשאות גישה למידע רגיש של המועצה ולקבוע בקרות פיקוח מתאימות לכל ספק.

רישום וניהול מאגרי מידע

48. מומלץ כי מחלקה משפטית במועצה תוביל ותפקח על יישום כל ההיבטים המשפטיים של יישום חוק הגנת הפרטיות ותקנות.
49. מומלץ כי יבוצע מיפוי מקיף של כלל המאגרים במועצה ועדכון כל הפרטים תוך הסרה של מאגרים שכבר לא קיימים והוספת מאגרים חדשים.
50. מומלץ למנות מנהלי מאגרים שהינם עובדים קיימים לכל המאגרים בהתאם לתפקידם.
51. מומלץ לקיים הדרכות ולהעביר הנחיות למנהלי מאגרים במועצה בנוגע לתפקידם.
52. מומלץ לבצע בחינה של קיום מידע עודף במאגרים בהקדם האפשרי.

53. מומלץ לכתוב מסמכי הגדרות מאגר לכל המאגרים הקיימים במועצה, ולעדכן אותם אחת לשנה .

מבדקים טכנולוגיים לבדיקת אפקטיביות של מערך האבטחה ברשת הפנימית, באתר האינטרנט ובכתובות החיצוניות של המועצה

54. יש לפעול ליישום המלצות לפי דוחות Nessus המצורפים .
55. להגדיר סיסמא לניהול אנטי וירוס כדי למנוע אפשרות להשבית אותו על ידי משתמש קצה.
56. לשדרג גרסאות של כל השירותים ומערכות הפעלה.
57. להפסיק את השימוש בפרוטוקולים פגיעים כמו SMB1, SSL3, SSL2, TELNET, FTP.
58. להחליף את שם מחרוזת ברירת מחדל בשירות SNMP.
59. להפסיק את השימוש בפרוטוקולים LLMNR וNBT-NS.
60. לבצע עדכון גרסה ל- ESXI.
61. לעדכון את גרסת ה -VMware .
62. יש להפעיל חתימה בפרוטוקול singing SMB בתחנות ושרתים.
63. יש להגדיר סיסמאות חזקות לממשקי ניהול של רכיבים ברשת.
64. ליישם סיסמאת BIOS לכל התחנות קצה ומחשבים ניידים.
65. לטפל בחשיפות באתר אינטרנט על ידי חסימת כל הפורטים הפתוחים ושירותים לא נחוצים או הגבלת גישה שירותים דרך חומת אש לכתובות קבועים בלבד תוך שימוש בפרוטוקולים חזקים כמו sftp, ssh.
66. להטמיע תעודת SSL מקצועית באתר אינטרנט בתקן EV.
67. לשקול ליישם מוצר הגנה מתקדם WAF להגנה על אתר אינטרנט.
68. לשקול לבטל שימוש בשירות OWA לגישה לדוא"ל ארגוני מרחוק. במידה וממשיכים להשתמש יש לדרוש ביצוע עדכון גרסאות מחברה לאוטומציה של שרתי Apache ו - OPENSSL וגם לדרוש מנגנון הזדהות חזקה של סיסמה חד פעמית OTP.

דו"ח הביקורת המפורט

3. מבוא

במועצה האזורית שער הנגב פועלות מערכות מידע ממוחשבות ומנוהלים מאגרים מידע שונים לצורך אספקת שירותים מגוונים לתושבים וגופים אחרים.

הגברת שימוש במערכות מידע והגברת השימוש במאגרי מידע תוך הרחבת אספקת שירותים דיגיטליים לתושבים בשנים אחרונות, מגביר את הסיכון כי מידע אישי ייחשף ברבים בזדון או בתום לב ויפגע בפרטיות התושבים והעובדים של המועצה.

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

סיכוני סייבר עלולים להתממש כתוצאה מניצול של חולשות במערכות, תהליכים וגורם אנושי עד כדי לשבש את הפעילות השוטפת, למנוע מהמועצה אספקת שירותים לתושבים, לחשוף את המועצה לתביעות משפטיות ועיצומים רגולטוריים וכד'.

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.

בשנים האחרונות גדל היקף התקיפות באמצעות תוכנות נוזקות (Malware), תוכנות כופרות (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 הארגון. התקיפות הופכות למתוחכמות יותר ויותר תוך אוטומציה שלהן והפצה המונית ושימוש בטכניקות הנדסה חברתית כדי לפתות משתמשים להפעיל אותן.

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.

4. <u>הבסיס החוקי</u>

חוקים ותקנות רלוונטיים בהיבטי הגנת הפרטיות ואבטחת מידע

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..."

מידע - "נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו."

מידע רגיש -

"(1) נתונים על אישיותו של אדם, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו;

(2) מידע ששר המשפטים קבע בצו, באישור ועדת החוקה חוק ומשפט של הכנסת, שהוא מידע רגיש."

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.

המשימות העיקריות בהיבטי הגנת הפרטיות ואבטחת מידע של מועצה כבעלת המאגר:

לקבוע מדיניות ונהלים; לבצע מיפוי מאגרים ונכסי מידע; לקבוע אחריות וסמכויות של בעלי תפקידים; 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

מטרת הביקורת

מטרת הביקורת היינה לבחון את נאותות ניהול היבטי אבטחת מידע במועצה, בהתייחס לדרישות תקנות הגנת הפרטיות, תוך בחינת תהליך יישום תקנות חדשות במועצה ואת אפקטיביות מנגנוני אבטחת מידע הקיימים במועצה להתמודדות עם מתקפות סייבר, תוך זיהוי חולשות אבטחה, פגיעות ופערים.

התחומים העיקריים שנבדקו:

- פעילות מחלקת מערכות מידע
- פעילות ומעורבות הנהלת המועצה
- פעילות בהיבטי משאבי אנוש

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
- קיום תקציבים נאותים
- מדיניות ונהלים בהיבטי הגנת הפרטיות ואבטחת מידע
- קיום אמצעי אבטחה טכנולוגיים נאותים
- פיקוח ובקרה על ספקי מיקור חוץ

מתודולוגיה ורקע

לצורך הביקורת נערכו הפעולות הבאות:

- פגישות עם: מנהל מחלקת מערכות מידע; גזבר, סגן גזבר.
- עיון בחומרים: נהלים, סקרים, מבדקים, תיעוד לפעילות מחלקת מערכות מידע, הסכמים עם ספקים, ועוד.
- 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 המועצה ואתר המועצה.
  - חדירה לרשת העירונית ותחנת קצה במועצה תוך ניצול גישה פיזית, ללא הרשאה, במשרדי מבקר המועצה.
  - 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 הגדרות במוצרי אבטחה.
  - בדיקת הרשאות גישה רגישות, הרשאות חיבור מדיה נתיקה וגלישה באינטרנט

רקע:

הביקורת נערכה בתחילת שנת 2019 ובוצעה בסיוע 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.

ביקורת התבססה על בדיקות מדגמיות ואין הכרח שתחשוף כל ליקוי אם קיים.
יצוין כי המועצה מפעילה מערך אבטחת מידע שכולל שימוש במוצרי אבטחה מקובלים, מנהל מערכות מידע מבצע מעקב אחר ביצוע עדכונים שוטפים, לאחרונה תוכנן מהלך לשדרוג של מערך שרתים ואבטחת מידע במועצה. מערכות ליבה ואבטחת גישה לאינטרנט מנוהלות בספק חיצוני חברה לאוטומציה בעלת הסמכה לתקן מוביל בהיבטי אבטחת מידע.

5. <u>פירוט הממצאים</u>

5.1 מדיניות אבטחת מידע ונהלי אבטחת מידע

סעיף 3 (2) לתקנות קובע 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"

סעיף 4(ג) לתקנות קובע 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...

סעיף 4(ד) קובע 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."

הביקורת מצאה כי, במועצה לא הוגדרו מסמך מדיניות אבטחת וסט נהלים בהיבטי אבטחת מידע. מסמך מדיניות אבטחת מידע ונהלים נדרשים להיות מאושר על ידי המנכ"ל המועצה.

הביקורת מצאה כי, חסרה התייחסות כלל או התייחסות מפורטת להיבטים הבאים במסמכים:

- נוהל ניהול משתמשים והרשאות למערכות המאגרים של מועצה.
- נוהל רישום וניהול מאגרים לפי חוק הגנת הפרטיות
- נוהל ותכנית תגובה מפורטת לאיתור, דיווח ותגובה לאירועי אבטחת מידע וסייבר
- נוהל פעילות ממונה אבטחת מידע לרבות הכנה, ביצוע ודיווח על תכנית בקרה שוטפת לעמידה בדרישות התקנות.
- נוהל לפיקוח ובקרה על ספקי מיקור חוץ
- נוהל לאופן תיעוד ובקרת גישה למערכות מאגר כולל התייחסות לאיזה מידע יישמר בלוגים.

- נוהל ביצוע פעולות פיתוח במאגר ותיעודן
- נוהל אבטחת מידע של מצלמות אבטחה
- נוהל ניהול, הקשחה ועדכון מערכות הגנה ואבטחת מידע
- נוהל ביצוע עדכוני אבטחה ושדרוגי גרסאות של תחנות קצה ושרתים ואפליקציות.
- נוהל גיבוי נתונים – כולל התייחסות לנושא ביצוע ובקרה על שחזורים מנתוני הגיבוי, אבטחת נתוני הגיבוי.
- נוהל אבטחה פיזית – לרבות התייחסות לאופן בקרת גישה לחדר שרתים וחדרי תקשורת לרבות שמירת לוגים של גישות, ניטור במצלמות ועוד.
- נוהל אבטחת מידע למשתמשי קצה – הכולל התייחסות לכללי אבטחת מידע אותם נדרשים לקיים עובדים ומשתמשים במערכות מועצה לרבות שימוש במחשב, דואל, גלישה באינטרנט, מדיה נתיקה, שולחן נקי וכדומה.
- נספח אבטחת מידע וסודיות לספקים המותאם לדרישות סעיף 15 בתקנות הגנת הפרטיות.
- טופס הצהרת סודיות עובד
- טופס בקשת הרשאות

סעיף 17ב. לחוק הגנת הפרטיות קובע כי המועצה מחויבת כגוף ציבורי למנות אדם בעל הכשרה מתאימה לתפקיד הממונה על אבטחת מידע.

סעיף 3 לתקנות קובע:

"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...

(3) הממונה יכין תכנית לבקרה שוטפת על העמידה בדרישות תקנות אלה, יבצע אותה ויודיע לבעל מאגר המידע ולמנהל המאגר על ממצאיו ;
(4) הממונה על אבטחה לא ימלא תפקיד נוסף שעלול להעמידו בחשש לניגוד עניינים במילוי תפקידו לפי תקנות אלה ;
(5) הטיל בעל מאגר המידע על ממונה על אבטחה משימות נוספות על החובות המנויות... לשם ביצוע תקנות אלה, יגדירן בצורה ברורה ;"

תכנית הבקרה תכלול היבטים רבים לרבות בדיקת סטאטוס עדכוני אבטחה, תקינות מוצרי אבטחה, נאותות הרשאות גישה למאגרים, בקרה על חיבור מדיה נתיקה, הפרדת מאגרים, בקרה על אבטחת גישה פיזית לרבות מורשי גישה, חוזק מנגנונים, בקרה על תקינות לוגים במערכות ועוד.

הביקורת מצאה כי, לא מונה באופן רשמי ממונה אבטחת מידע במועצה. בפועל מנהל מערכות מידע מכהן גם בתפקיד של ממונה אבטחת מידע במועצה אשר אמור לבקר ולפקח על העמידה בדרישות התקנות הגנת הפרטיות. במצב הנוכחי קיימים ניגודי עניינים בין תפקיד מנהל מערכות מידע לממונה אבטחת מידע. מנהל מערכות מידע אחראי ליישום בפועל של תכנית עבודה שוטפת בהיבטי מערכות מידע ובתפקיד הממונה למעשה מבקר ומפקח על פעולותיו.

בנוסף לא הוכנה תכנית בקרה שוטפת בשנים 2018 ו- 2019 לצורך עמידה בתקנות.

5.2 ועדת היגוי להיבטי אבטחת מידע

כיום בארגונים רבים לצורך קידום נושאי אבטחת מידע הוקמו ועדות היגוי לנושא אבטחת מידע והגנת הפרטיות, תפקידי ועדת היגוי מקובלים :

- אישור ועדכון בכל הנוגע למדיניות אבטחת המידע ונהלים ;
- לסייע למועצה בכל הקשור לניהול תקין של תחום אבטחת המידע במועצה ;

- 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 המועצה בקבלת החלטות בכל הקשור לתחום אבטחת המידע מתוך ראיה אינטגרטיבית של התחום במועצה.
- קבלת דיווחים תקופתיים ממונה אבטחת מידע והנחיית ממונה אבטחת המידע.

הוועדה תתכנס בתדירות קבועה ומספקת שתקבע ותדווח לראש המועצה ולמנכ"ל, אחת לשנה לכל הפחות, על פעילותה ועל מסקנותיה והמלצותיה בנושאים בהם הוסמכה לעסוק ותערוך פרוטוקולים של ישיבותיה. רצוי כי לפחות בדיון השנתי בו תאושר תכנית העבודה ותקציבים יהיה נוכח מנכ"ל המועצה. כמו כן, חברי הועדה צריכים להיות מתחומים מנהליים ולא רק מערכות מידע לרבות יועץ משפטי, גזבר, קצין הביטחון, מנהל משאבי אנוש, מנהל תפעול, אחראי על גופים חיצוניים כמו מוסדות חינוך.

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

5.3 תקציב אבטחת מידע

סעיף 3(6) לתקנות קובע כי "בעל מאגר המידע יקצה לממונה את המשאבים הדרושים לו לשם מילוי תפקידו."

החלטה מספר 2443 של רשות התקשוב הממשלתית מ-15.2.15 בנושא "קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר" קובעת בין היתר, כי

"המנכ"לים של משרדי הממשלה ומנהלי יחידות הסמך, במסגרת סמכותם ואחריותם הקיימת, יסדירו את מבנה התקציב השנתי של משרדם כך שלכל הפחות 8% מתקציב תחום טכנולוגיית המידע יופנה להגנת הסייבר"

נמצא כי תקציבי אבטחת מידע אינם מוצגים לאישור הנהלה הבכירה של המועצה ואינם נידונים באופן ייעודי, התקציבים נכללים במסגרת סך תקציב מחלקת מערכות מידע.

5.4 סקרי אבטחת מידע ומבדקי חדירה

בסעיף 5 בתקנות הגנת הפרטיות נקבע כדלקמן:

"(ג) במאגר מידע שחלה עליו רמת האבטחה הגבוהה, בעל המאגר אחראי לכך שייערך סקר לאיתור סיכוני אבטחת מידע (להלן - סקר סיכונים); בעל מאגר המידע ידון בתוצאות סקר הסיכונים שיועברו לו, יבחן את הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבותיהן, ויפעל לתיקון הליקויים שהתגלו במסגרת הסקר, ככל שהתגלו; סקר סיכונים כאמור ייערך אחת לשמונה עשר חודשים לפחות.

(ד) במאגר מידע שחלה עליו רמת האבטחה הגבוהה, בעל המאגר אחראי לכך שייערכו מבדקי חדירות למערכות המאגר לבחינת עמידותן בפני סיכונים פנימיים וחיצוניים, אחת לשמונה עשר חודשים לפחות; בעל המאגר ידון בתוצאות מבדקי החדירות ויפעל לתיקון הליקויים שהתגלו, ככל שהתגלו."

מתוך תורת ההגנה בסייבר בארגון:

סעיף 1.2: "יש לאשר אחת לשנה את מפת הסיכונים הנוכחית כפי שהיא עולה מסקר סיכוני סייבר ארגוני"

סעיף 22.3: "הארגון יבצע מבדקי חדירה תשתיתיים ואפליקטיביים למערכות הארגון (בין אם הן פנימיות או חיצוניות אבל מנוהלות על ידו) אחת לתקופה".

מבדיקת הביקורת נמצא כי, טרם בוצע סקר סיכונים להערכת סיכוני אבטחת מידע ומבדקי חדירה לבדיקת אפקטיביות מערך אבטחת מידע. אכן לפי התקנות קיימת חובה לביצוע במאגר ברמת אבטחה גבוהה בפועל מדובר בפרקטיקה מקובלת גם אם מנוהל מאגר ברמות אבטחה נמוכות יותר. המועצה בנוסף לתקנות הגנת הפרטיות מחויבת לספק שירותים כולל שירותי חירום לתושביה וגופים חיצוניים. מתקפת סייבר עלולה להשבית פעילות שוטפת של המועצה ולפגוע ברמת שירות מעבר לפגיעה בפרטיות.

בנוסף נמצא כי, טרם בוצעו מבדקי חדירה תשתיתיים ואפליקטיביים פנימיים וחיצוניים בכל מערכות ותשתיות המאגרים המנוהלים במועצה עצמה לרבות מאגר משרד הפנים. יצוין כי, קיימת חובה לביצוע בנוגע למערכת ברמת אבטחה גבוהה בלבד לפי תקנות. במועד הביקורת לא בוצע תהליך מעמיק לקביעת רמת אבטחה של מאגר. לכן לא ברור אם נדרש או לא מחויב לביצוע. כמו כן, המועצה לא ערכה פיקוח ובקרה בהיבטי אבטחת מידע על המערכות שמסופקות במיקור חוץ לרבות דרישה לקבלת תוצאות מבדקי חדירה מצד ספקי מקור חוץ לרבות חברה לאוטומציה. יש להדגיש כי חוסר מעורבות מנוגד לסעיף 15 בתקנות .

5.5 הדרכות עובדים

סעיף 7 לתקנות 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.."

מבדיקת הביקורת עלה כי, העובדים בכניסתם לעבודה אינם חותמים על מסמך הנחיות אבטחת מידע ולא מקבלים תדריך אבטחת מידע כנדרש בתקנות.
כמו כן, טרם בוצעה הדרכה לכלל העובדים במועצה בנושאי אבטחת מידע והגנת הפרטיות עם מצגת ייעודית המכסה תכנים נדרשים.

5.6 בקרת הרשאות גישה

בסעיף 8 בתקנות ניהול הרשאות גישה נרשם כדלקמן:
"(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)".

בעת קבלת עובד למועצה, הממונה של העובד שולח למחלקת מחשוב דואל לפתיחת משתמש וקבלת הרשאות גישה, בעזיבת עובד התהליך דומה.

נמצא כי, לא קיים טופס בקשת הרשאות הכולל פרטים כמו נדרש אינטרנט, נדרש כונן מחלקתי, אישי, דוא"ל, גישה מרחוק, קבוצות הרשאות למסכים במערכות ועוד.

הביקורת מצאה כי, טרם בוצע מיפוי מדויק במועצה של איזה סוגי הרשאות נדרשות ברמת כל תפקיד כנדרש בתקנות. מתן הרשאות באמצעות העתקת הרשאות מעובד אחר עלול לגרום לכך שעובד חדש עלול לקבל הרשאות עודפות שצבר עובד ותיק שלא בהכרח נחוצות לו למילוי תפקידו.

כמו כן, טרם בוצע תהליך תקופתי של תיקוף הרשאות גישה קיימות לכלל מורשי גישה באמצעות סקירת הרשאות על ידי מנהלי המאגרים. במסגרת תהליך תיקוף כזה כל מנהל מאגר נדרש לקבל הרשאות גישה לכל מאגר פר

משתמש ולקבוע אם עדיין הרשאה זו נחוצה לכל משתמש או מדובר בהרשאה עודפת.

5.7 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.

במהלך הביקורת נמסר על ידי מנהל מחלקת מערכות מידע כי, טרם בוצע תהליך מיפוי מקיף ברמת כל מאגר ומערכת מאגר האם אכן מנגנון תיעוד אוטומטי לפעולות משתמשים עומד בדרישות התקנות, לרבות שמירת תיעוד לתקופה של 24 חודש. טרם נקבע נוהל בדיקה שגרתי של נתוני התיעוד כפי שנדרש בתקנות.
נמסר כי במערכת שקד של חברת מגער קיים שימוש במשתמש משותף על ידי צוות גבייה. מדובר בהרשאה משותפת שלא מאפשרת בקרה על זהות מבצעי פעולות.

5.8 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 (Key On Disk).

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), Honeypots (מלכודת דבש), - EDR Anomaly detection, Behavioral analysis Code Sterilization, (הלבנת קבצים).
ניתן להרחיק את האיום ממשתמשי קצה ולאפשר גלישה מאובטחת באינטרנט באמצעות שימוש במכונות מרוחקות והפרדת רשתות פנים ארגוניות מרשת האינטרנט (Secure browsing).

נמצא כי, במועצה קיים שימוש במערכת חומת אש, אנטי וירוס, מסנני תוכן לדוא"ל. שירותי חומת אש ומסנני תוכן באינטרנט ודוא"ל מסופקים על ידי חברה לאוטומציה בעלת תקן ISO 27001.

יחד עם זאת, הביקורת סבורה כי, קיים מקום להוסיף שכבות הגנה נוספות כמפורט להלן:

- להגדיר מדיניות סיסמאות חזקה ברשת הפנימית ב AD. מדיניות צריכה להיות 8 תווים, 180 יום תדירות החלפה לכל הפחות, מורכבת מאותיות ומספרים כולל אות גדולה לפחות אחת. נעילת חשבון לאחר 5 ניסיונות גישה כושלים, שמירת היסטוריה של 12 דורות אחורה.
- להוסיף במערכת חומת אש מודול SANDBOX FORTI.
- במערכת חומת אש לוודא הפעלה של מודול IPS לחסימת מתקפות מתקדמות.
- במערכת חומת אש במועצה להפעיל מודול DEEP SSL INSPECTION לבחינת תעבורה מוצפנת לאתרי אינטרנט עם SSL.
- להוסיף במערכת חומת אש הקיימת במועצה מודול GEO Protection שמאפשר חסימת גישה למדינות למשל מדינות ערב איתן אין למדינת ישראל יחסים, ומדינות נוספות מסוכנות בהיבטי סייבר לגביהן לא קיים צורך ארגוני לתקשורת מולן כמו צפון קוריאה, רוסיה, סין וכדומה.
- לשקול להפעיל בתחנות קצה מודול EDR לאיתור אנומאליות.
- להפעיל חומת אש אישית במחשבים ניידים הנמצאים מחוץ לארגון ולשקול גם להפעיל חומת אש בתחנות קצה בתוך הרשת הפנימית.
- להפעיל מערכת ״הלבנה״ (סינון רשתי של קבצים) של הלבנת קבצים המועברים בדוא״ל, מורדים מאינטרנט, מועתקים במדיה נתיקה ובממשקים (כספות) לקבלת קבצים מגורמים חיצוניים. מטרת המערכת היא לבצע בחינה וזיהוי של קבצים העלולים לכלול בתוכם קוד זדוני שתול. מערכת זו יכולה אף להסיר את הקוד הזדוני.
- להפעיל טכנולוגיה הקרויה Honeypots המבוססת על רעיון של הצבת מלכודות דבש וירטואליות ברשת הארגון המייצרות אשליה של תחנות קצה ושרתים הכוללים פרצות אבטחה. נוזקות או גורמים זדוניים פועלים לעתים באמצעות התפשטות ברשת תוך איתור רכיבים בהם יש חשיפות. במקרה בו המלכודת מזהה ניסיון פריצה, היא מעבירה התרעה לשרת ניהול מרכזי וגורם בקרה אנושי אמור לבחון את האירוע

ולפעול בהתאם לתכנית תגובה שהוגדרה. יש לציין כי טכנולוגיה זו יעילה בשילוב עם פתרונות נוספים.

- להפעיל מערכת לגלישה מאובטחת באינטרנט, המבוססת על שרתי טרמינל מוקשחים הנמצאים ב"אזור מפורז" (DMZ) החוצץ בין האינטרנט לרשת הפנימית. משתמש הקצה אינו גולש באינטרנט ישירות מתחנה הקצה אלא מתוך השרת, כך שאם נוזקה תקפה במהלך גלישה, התקיפה מכוונת כנגד השרת המוקשח. באופן זה ניתן להגביל הורדה של קבצים לתחנת קצה והקבצים יאוחסנו בשרת ב"אזור המפורז" בלבד ולא יכנסו לרשת. יתרון נוסף בשימוש בטכנולוגיה זו הוא שניתן לחסום העברת קבצים ואף טקסטים מתחנת הקצה ל"אזור המפורז" ובכך למנוע זליגת מידע רגיש דרך אינטרנט.

יצוין כי, מדובר בטכנולוגיות נפוצות כיום בארגונים בסדר גודל של המועצה ואף בארגונים בעלי פעילות פחותה.

5.9 אבטחת טלפונים ניידים וטאבלטים

באמצעות אפליקציות זדוניות שמשתמשים תמימים מורידים למכשירים ניידים שברשותם, ניתן לגנוב מידע רגיש מהטלפון או מהטאבלט, כולל סיסמאות גישה ופרטי דואר אלקטרוני ארגוני שעלולים לכלול נתונים רגישים כולל אישיים.
בארגונים רבים קיים כיום שימוש בטכנולוגיה לניהול ואבטחת התקנים ניידים (MDM) המספקת הגנה מלאה על המידע הנמצא במכשיר, מבלי לפגוע בפרטיות המשתמש.

נמסר כי, טרם הוטמע במועצה פתרון להגנה על טלפונים ניידים מסוג MDM.

נוסף על כך, לא יושמו הגדרות אבטחה בסיסיות, כגון אכיפת הגדרת קוד גישה למכשיר אשר מבצע סנכרון לדוא"ל ארגוני, וחיבור רק ממכשיר מורשה המזוהה לפי פרמטרים של מכשיר.

5.10 אבטחת התקנים ניידים

סעיף 12 לתקנות קובע 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."

נמצא כי, לא מיושמת חסימה למניעת חיבור מדיה נתיקה לתחנות קצה, כיום כלל המשתמשים מורשים לחבר כל מדיה נתיקה וגם בכל מחשבים ניידים פתוחה הגישה. המשמעות היא שקיימת חשיפה רבה להחדרת נוזקה (תוכנה זדונית) שלא תזוהה באמצעות אנטי-וירוס המותקן במערכות המועצה וכן חשיפה לסיכונים נוספים של זליגת מידע רגיש.
עוד נמצא כי לא הופעלה טכנולוגיה להצפנת נתונים במדיה נתיקה ובדיסקים קשיחים של המחשבים הניידים.
בנוסף, הביקרת מצאה כי לא נאכף מנגנון המאפשר חיבור של התקנים ניידים שהוקצה על ידי מחלקת מערכות מידע בלבד ו/או הותרו לשימוש. נוסף על כך, לא נעשה שימוש בטכנולוגיה למניעת זליגת מידע רגיש בזמן העתקת נתונים למדיה נתיקה (מסוג DLP) ולא הוטמע שימוש בטכנולוגיה של "הלבנת" קבצים רשתית לכלל תחנות קצה. קיימת עמדת הלבנה ייעודית במחלקת מערכות מידע אך נמסר כי העובדים לא מקפידים לפעול לפי הנוהל ושימוש בתחנת הלבנה מאוד מצומצם.

5.11 מדיניות בקרת גלישה באינטרנט

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."

כיום הגלישה באינטרנט מבוצעת דרך חומת אש ומופעל מודול סינון אתרים וקבצים. המודול אמור לחסום גישה לקטגוריות של אתרים שמוגדרים כחסומים לגלישה כמו אתרים עם תוכן לא הולם וגם לחסום הורדה של קבצים בפורמטים לא מורשים.

נמצא כי, מדיניות הגלישה מתירנית כאשר לא מיושמת חסימה של כל קטגוריות מסוכנות כמו אתרי דוא"ל חינמי למשל gmail, אתרי שיתופי ואחסון קבצים כמו google drive , אתרי הפצת תוכנות כמו github. בנוסף לא קיימת חסימה להורדה של קבצי הרצה וסקריפטים.
מדיניות מתירנית מדי חושפת לסיכונים של זליגת מידע רגיש מתוך רשת המועצה תוך ניצול פתיחות של אתרים לשיתוף קבצים או חדירת נוזקות זדוניות לרשת תוך ניצול העובדה של כללי סינון לא נוקשים.
צוות הבדיקה בצע הורדה של קובץ טסט דמוי וירוס בשם " eicar. הקובץ נחסם בחומת אש בהורדה בפרוטוקול HTTP שלא כולל הצפנה, אך לא נחסם בחומת אש בהורדה בפרוטוקול HTTPS ורק נחסם באנטי וירוס בתחנת קצה. לכאורה, קיים ליקוי במנגנון DEEP SSL INSPECTION בחומת אש אשר מאפשר בדיקה קבצים העוברים בתווך מוצפן HTTPS .
לפירוט ראה סעיף 4.22.

5.12 הרשאות אדמיניסטרטור

מרבית הנוזקות כיום מנצלות הרשאות של משתמשי קצה על מנת לבצע פעולות זדוניות במערכות מחשב. לאור זאת הבקרה המומלצת כיום הינה כי, למשתמשי קצה יוקצו הרשאות נמוכות ביותר ברמת מערכת ההפעלה.

נמצא כי, בכל תחנות קצה קיימת עדיין הרשאה של לוקל אדמין למשתמש קצה המאפשרת לו לבצע התקנה של תוכנות וביצוע שינויים בהגדרות מחשב. הרשאה זו יכולה להיות מנוצלת על ידי נוזקות זדוניות לרוץ בהרשאות גבוהות ומגבירה את סיכויים לכך שנוזקה תבצע את זממה.

קיים כלי אבטחה LAPS שמסופק על ידי חברת מיקרוסופט המספק מענה לחשיפה זו.

5.13 סגמנטציה של הרשת הפנימית

בתקנות הגנת הפרטיות בסעיף 13 ב(נרשם: "בעל מאגר מידע יפריד, בהיקף ובמידה הסבירים האפשריים , בין מערכות המאגר אשר ניתן לגשת מהן למידע, לבין מערכות מחשוב אחרות המשמשות את בעל המאגר."

ממצאים:

נמצא כי, בנוגע למערכות המסופקות על ידי ספקי מיקור חוץ מתקיימת הפרדה פיזית כאשר מערכות נמצאות ברשתות של הספקים. בנוסף קיימת הפרדה של מוסדות חינוך מרשת המועצה באמצעות חומת אש נוספת.

יחד עם זאת נמצא כי, כיום הרשת הפנימית של המועצה שטוחה וניתן להגיע ברמת תקשורת מכל רכיב לכל רכיב בתוך הרשת הפנימית כולל גישה תקשורתית למאגרי נתונים רגישים.

סגמנטציה מיטבית מושגת באמצעות חומת אש רשתית הממוקמת בתוך הרשת ומחלקת את הרשת באמצעות הפרדה פיזית ולוגית ולכל הפחות הפרדה בין סגמנט של תחנות קצה ושרתים וגם סגמנטציה פנימית לפי מחלקות , מבנים, וכד'.

הביקורת סבורה כי, הנושא צריך לקבל תיעדוף גבוה לאור העובדה כי מדובר בדרישה רגולטורית.

5.14 מערכת מניעת חיבור התקנים זרים לרשת המועצה

בהינתן גישה פיזית של גורם זדוני למשרדי הארגון, הגורם יכול לבצע ניסיון חדירה באמצעות חיבור מחשב או התקן זר לרשת הפנימית תוך קבלת כתובת IP תקינה ברשת. באופן זה למעשה הגורם הזדוני עוקף מנגנוני אבטחה היקפיים המיושמים ברשת לרבות חומת אש. על מנת לספק מענה לחשיפה זו פותחה טכנולוגיה בשם NAC- -NETWORK ACCESS CONTROL בקרת גישה לרשת הפנימית. הטכנולוגיה באמצעות מנגנונים שונים מסוגלת לזהות התקן לא מורשה המנסה להתחבר לרשת הפנימית בארגון ולנתק אותו מהרשת (על ידי ניתוק של נקודת רשת חמה במתג) ובאופן זה למנוע חדירה לרשת הפנימית.

נמצא כי, לא מיושמת טכנולוגית NAC ברשת הפנימית של המועצה. העדר טכנולוגיה זו לא מנעה מצוות הביקורת לחבר לרשת הפנימית של המועצה מחשב נייד חיצוני ורכיב USB לצורך ביצוע סימולציות של חדירה לרשת הפנימית כפי שמפורט בסעיף 5.8.

5.15 אבטחת גישה מרחוק

בסעיף 14 (ג) בתקנות 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."

כיום אמצעי אבטחה מקובל בגישה מרחוק הינו מנגנון הזדהות חזקה הכולל שני שלבים בהזדהות לפחות. 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.

הזדהות חזקה כוללת בד"כ חילול סיסמה חד פעמית ואקראית בכל גישה. במצב נוכחי עלולות סיסמאות קבועות של משתמשים להיחשף בדרכים שונים לגורמים זדוניים ובכך ישיגו גישה מרחוק לנתונים רגישים.

הביקורת מצאה כי, לא מיושמת הזדהות חזקה גישה מרחוק למערכות המועצה. בנוסף נמצא כי כיום למנהל מערכות מידע קיימת שליטה מרחוק לכל המחשבים במועצה דרך מערכת שליטה מרחוק team viewer. מדובר בהרשאה רגישה ביותר ושימוש בהרשאה זו גם לא מחייב שימוש בסיסמה חד פעמית.
יצוין כי, במהלך הביקורת נמסר על ידי מנהל מערכות מידע שהוא הגדיר מנגנון הזדהות OTP של סיסמה חד פעמית לממשק ניהול של team viewer.

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".

הביקורת מצאה כי, מיושמת מדיניות אחידה לביצוע עדכוני אבטחה ברמת מערכת הפעלה WINDOWS בשרתים ותחנות קצה באמצעות עדכוני אבטחה אוטומטיים. לא נמצאו עדכוני אבטחה חסרים ברמת מערכת WINDOWS.

יחד עם זאת עדיין נמצאו עדכוני אבטחה חסרים במערכות הפעלה נוספות כמו VMVARE ESXI , UNIX,CISCO IOS במסגרת מבדקים טכנולוגיים בסעיף 4.21.

כמו כן, קיימות תחנות קצה רבות בהן עדיין מותקן WIN 7, ושרתי WIN 2008 כידוע לפי פרסומי יצרן תיגמר התמיכה במערכת הפעלה זו בינואר 2020.

נמסר כי, כבר לפני הביקורת החל בתהליך רכש ושדרוג מערך השרתים במועצה כך שחלק גדול מהחשיפות אמור להיות מטופל בחודש אפריל במעבר לשרתים מסוג WIN 2016 . כמו כן, יתווסף שרת ניהול מרכזי WSUS.

5.17 ניטור, דיווח ותגובה לאירועי אבטחת מידע

סעיף 11 לתקנות קובע:

"(א) 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 מידיים 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."

להלן תיאור המצב נוכחי:

- חלק מהתרעות אבטחה מתקבלות בדוא"ל למנהל מערכות מידע ממוצרי אבטחת מידע מסוימים.

- מתקבלות התרעות בדוא"ל למנהל מערכות מידע בלבד על מתקפות סייבר המתפרסמות בעולם ועל פרצות אבטחה שמתגלות במוצרי תוכנה וחומרה מ – CERT כללי וגם מנחה סייבר ממשרד הפנים ומחברה לאוטומציה.

יחד עם זאת הביקורת מצאה כי:

- לא קיימים נהלים מפורטים לאיתור, תגובה ותרגול של אירועי סייבר מבוססי תרחישים, לצורך התמודדות עם סוגים שונים של איומים.
- נמצא כי, לא מנוהל מאגר ידני או אוטומטי לתיעוד כלל אירועי אבטחת מידע, לרבות אירועים פוטנציאליים.
- לא מתקיימים דיונים באירועי האבטחה בפורום מנכ"ל כנדרש בתקנות.
- לא הוקם צוות תגובה מקצועי אשר ייתן מענה מהיר ואפקטיבי במקרה של התרעה על אירוע סייבר. מנהל מערכות לבדו מקבל התרעות ודיווחים על אירועי אבטחה.
- לא מתקיימים תרגולים תקופתיים לתרגול תגובה לאירועי סייבר.
- טרם הוטמעה טכנולוגית SIEM ממוכנת המקבלת נתונים ממערכות ארגוניות שונות, מנתחת אותם ומאפשרת בקרה על תהליכים ואירועים, הפקת דוחות בקרה, זיהוי פרצות אבטחה ותגובה למתקפות המתרחשות בזמנים שונים.
- בכל מקרה, עד כה, לא מונה כוח אדם ייעודי לנושא, לרבות הקמת מרכז בקרה המספק מענה אף מעבר לשעות העבודה המקובלות במטרה לאתר אירועי אבטחה בפרק זמן קצר (צוות SOC), כך שנכון למועד איסוף הממצאים, ניטור ובקרה נערכים בהתאם לזמינות כוח אדם במחלקה הטכנולוגיות. ייתכן ואין מקום להקים מוקד פנימי כזה אלא להשתמש בשירותי SOC חיצוני.
- לא מתבצע שימוש שוטף בשירות מודיעין סייבר חיצוני וספציפי לארגון אשר יספק התראות על איומים הרלוונטיים לארגון, על חשש לזליגת

מידע רגיש שמוצג ברשת הציבורית או רשת האפלה, תוקפים ו/או מטרות פוטנציאליות תוך הספקת הנחיות לאופן התמודדות.

5.18 מיקור חוץ

במסגרת תקנות הגנת הפרטיות בסעיף 15 נקבע כי:

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

הביקורת מצא כי, קיים שימוש במספר ספקי מיקור חוץ הידועים בתחום, חברה לאוטומציה המספקת מערכות ליבה מרכזיות, חברת מגער המספקת

מודול לניהול גביית חובות. בנוסף קיים שימוש בספק חיצוני אוטומס המעמיד אתר חיצוני דרכו תושבים יכולים להגיש בקשות לקבל אישור תושבות ובקשות להנחות ארנונה. במסגרת הגשת בקשות התושבים ממלאים פרטים אישיים רבים וגם מצרפים מסמכים לרבות צילום ת.ז.

יצוין כי, אכן נחתם במסגרת מכרז החדש עם חברה לאוטומציה על הסכם חדש העומד בנוסח דרישות סעיף 15. בנוסף הומצא על ידי חברה לאוטומציה לבקשת הביקורת מסמך עמידה בתקן ISO.27001

יחד עם זאת הביקורת מצאה כי, תהליכי פיקוח ובקרה המתבצעים כיום אינם מספקים בנוגע לשירותי מיקור חוץ המתקבלים במועצה.

ההסכם עם חברת מגע״ר הינו משנת 2013 ואינו תואם במלואו לדרישות סעיף 15 בתקנות הגנת הפרטיות.

בנוגע לספק אוטומס קיימת רק הצעת עבודה חתומה אשר איננה כוללת התייחסות להיבטי אבטחת מידע ואינה עומדת בדרישות סעיף 15 בתקנות.

המועצה לא מבצעת פנייה תקופתית לספקיה על מנת לדרוש לקבל מהם סטאטוס עמידה בדרישות תקנות הגנת הפרטיות, אבטחת מידע כנדרש בתקנות.

בנוסף נמצא כי, טרם בוצע במועצה מיפוי של כלל הספקים של המועצה המחזיקים במידע רגיש או בעלי הרשאת גישה למידע רגיש וזאת על מנת לקבוע דרכי פיקוח ובקרה אליהם.

5.19 מסמכי רישום מאגרים, מסמכי הגדרות מאגר ובדיקת מידע רב מן הנדרש

בתקנות הגנת הפרטיות סעיף 2 :

(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;

(3) סוגי המידע השונים הכלולים במאגר המידע, בשים לב לרשימת סוגי המידע שבפרט בתוספת הראשונה;

(4) 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;

(5) פעולות עיבוד מידע באמצעות מחזיק;

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

(7) 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.

לביקורת נמסר כי טרם נכתבו מסמכי הגדרות מאגר.

בנוסף נמסר כי, קיימים מאגרים בהם לא מעודכנים פרטים כמו מנהל המאגר כאשר חלק ממנהלי מאגר כבר אינם עובדים במועצה. בנוסף לא בוצע מיפוי מקיף לתקינות רישום כלל המאגרים.

בהתאם לבדיקה מול אתר משרד המשפטים נמצא כי רשומים שני מאגרים בלבד במועצה:

מספר המאגרזיהוי בעל המאגרשם בעל המאגרשם המאגר

500261375990041135מ. א. שער הנגברישום נולדים

500261375990052870מ. א. שער הנגבתיקי פונים למח"ש לשרותים חברתיים

בפועל נדרש לרשום מאגרים נוספים בהתאם לסוג פעילות לרבות מאגר מרשם אוכלוסין, מאגר שכר ומשאבי אנוש, מאגר גבייה, מאגר דיוור ישיר, מאגר רישוי עסקים, מאגר רישום תלמידים וגנים ועוד.

המחלקה המשפטית במועצה טרם לקחה אחריות לליווי כל ההיבטים המשפטיים של חוק הגנת הפרטיות ותקנות הגנת הפרטיות.

בנוסף מבירור שקיימה הביקורת עלה כי, לא בוצע תהליך בחינה כלשהו אם לא נשמר מידע רב מן הנדרש במאגרים. הביקורת סבורה כי, במידה והיה מתקיים תהליך בחינה הרי היה מתגלה כי, במאגרים השונים מנוהל מידע ישן על תושבים לשעבר, עובדים לשעבר, תלמידים לשעבר וכדומה.

5.20 מבדקים טכנולוגיים לבדיקת אפקטיביות של מערך האבטחה

צוות הביקורת ערך מבדקים שונים במטרה לבחון את יעילות מערך האבטחה של המועצה ולזהות חולשות, במידה שקיימות, תוך דימוי מתקפת סייבר ממוקדת. הבדיקות בוצעו מרשת האינטרנט ומתוך הרשת הפנימית. הצוות השתמש בכלי סריקה מקצועי NESSUS PROFESSIONAL אשר מאפשר סריקה ובדיקה של קונפדרציות, חולשות, פגיעותיו, עדכוני אבטחה חסרים, גרסאות לא עדכניות, שירותים מיותרים ועוד. בנוסף הצוות הריץ בדיקות נוספות כמו סריקת רכיבי ציוד רשת לאיתור סיסמאות ברירת מחדל, ציתות לתעבורת רשת, תפיסת סיסמאות וניסיון פיצוח שלהן, איתור רשתות אלחוטיות פגיעות.

להלן עיקרי הממצאים ברשת הפנימית:

- נמצאה רשת אלחוטית בשם "NOT FOR YOU" עם פרוטוקול הצפנה חלש WEP, הרשת הייתה מחוברת גם לרשת הפנימית. ניתן בקלות לפצח את הסיסמה.

- קיים שימוש בפרוטוקולים LLMNR ו NBT-NS החושפים רשת למתקפות לרבות ציתות וחשיפת סיסמאות משתמשים.
- בוצע ניסיון איסוף סיסמאות מוצפנות של משתמשים ברשת הפנימית. נאספו מספר סיסמאות של משתמשים. סיסמה של משתמש sport2 פוצחה כי הייתה קלה לניחוש.
- קיים שימוש בפרוטוקולים פגיעים בתוך הרשת הפנימית כגון SMBv1 telnet, ftp,ssl3, .
- נמצא שימוש בשירות Dropbear SSH Server בגרסה הפגיעה למתקפות הרצת קוד זדוני מרוחק – RCE.
- נמצא שימוש בשירות VxWorks WDB Debug Agent בגרסה הפגיעה למתקפות הרצת קוד זדוני מרוחק – RCE.
- קיים שימוש בשירות SNMP בציוד תקשורת עם שם ברירת מחדל PUBLIC. ניתן להתחבר לציוד ולדלות פרטי קונפיגורציה פנימיים.
- קיים שימוש בשירות RDP ברשת אשר מיישם פרוטוקולי הצפנה חלשים.
- ESXI VMWARE בגרסה לא מעודכנת אשר פגיעה ל RCE.
- VMware vCenter נמצא בגרסה לא מעודכנת אשר פגיעה ל- RCE.
- לא קיים שימוש בחתימות בפרוטוקול Smb-signing) SMB).
- לא מיושמת סיסמאת BIOS למניעת העלת מערכת הפעלה זרה ושינויים בחומרת מחשב.
- קיים שימוש במערכת הפעלה לא מעודכנת CISCO IOS החושף את הציוד לפריצות.
- צוות הבדיקה בצע בדיקה בתחנה מדגמית בנוגע לבדיקת הקשחת גלישה באינטרנט ומצא כי המדיניות מתירנית מדי המאפשר גישה לאתרים כמו gmail, googledrive, github, winrar, הורדה והתקנה של קבצי הרצה, הורדת קובץ דמוי וירוס ועוד.

- צוות הביקורת הצליח לנטרל אנטי וירוס בתחנת קצה שנבדקה, לא מוגדרת סיסמא לניהול אנטי וירוס.
- נמצאו רכיבי ציוד רשת ללא סיסמאות או סיסמאות ברירת מחדל.

להלן עיקרי הממצאים באתר אינטרנט של המועצה

- בשרת האתר אינטרנט נמצאו שירותים פתוחים לכל האינטרנט עם ממשקי הזדהות כגון FTP, 3 POP החשופים למתקפת brute force.
- קיים שימוש בתעודת SSL של שירות חינמי ורצוי באתר של מועצה להשתמש בתעודה מסוג EV המספקת הגנה מפני התחזות ואמינות. התעודה גם בעלת תוקף של שלושה חודשים בלבד.
- נמצאו פורטים ושירותים שונים פתוחים ולא ברורה נחיצות שלהם כגון 25 SMTP, 53DNS ועוד.
- לא מיושם מוצר הגנה מתקדם חומת אש אפליקטיבית WAF להגנה על אתר אינטרנט.

להלן עיקרי ממצאים בכתובות חיצוניות של מועצה:

יצוין כי, מועצה מקבלת שירותי חומת אש, גלישה, VPN ודוא״ל מחברה לאוטומציה. בצענו סריקה בתיאום עם מנהל מערכות מידע לגבי כתובות חיצוניות המוקצות עבור המועצה.

נמצא כי, שירות OWA המסופק על ידי חברה לאוטומציה לצורך גישה מרחוק לדוא״ל ארגוני כולל חשיפות קריטיות עקב גרסאות ישנות ולא מעודכנות של שרת WEB Apache ושרת OPENSSL .

ככלל שירות OWA מאפשר גישה נוחה לתיבת דוא״ל בארגון באמצעות שם משתמש וסיסמה של המשתמש ברשת בלבד. יחד עם זאת, שירות זה חשוף למתקפות מגוונות ובפרט במקרה של חשיפת סיסמאת משתמש לגורם זדוני

בשיטות שונות כולל שיטות של הנדסה חברתית, נוזקה שמקליטה, מתקפת ניחוש סיסמאות brute force ועוד,שום דבר אינו מונע גישה לתיבת הדוא״ל. כמו בכל שירות גישה מרחוק כיום, הצעד המתבקש לאור הסיכונים כי, תהליך הזדהות יכלול רכיב של זיהוי חזק באמצעות סיסמא חד פעמית למשל.

הערות ראש המועצה

<u>הגנת הפרטיות ומערכות מידע</u>

ראש המועצה מייחס חשיבות רבה לנושא אבטחה ושמירת פרטיות המידע במאגרים הממוחשבים במועצה. בימים אלו נקבעת מדניות המועצה ומסמך המדיניות המפורט בנושא יובא עד לתאריך 30.6.2020 לאישור המליאה. מסמך מדניות המועצה במערכות ואבטחת המידע יהווה בסיס לקביעת תנאי המכרז לרכישת שירותים מקצועיים שוטפים בנושא.

1. **תכנית אסטרטגית** – ראש המועצה רואה חשיבות רבה בהכנת תכנית אסטרטגית למערכות המידע, והנחה את הצוות המקצועי לקדם תכנית אסטרטגית למערכות המידע במועצה.

2. **מבנה ארגוני** – ראש המועצה הנחה את המנכ"לית לבחון את המבנה הארגוני של מחלקת מערכות מידע ואת השירותים הנדרשים לצורך תפקודם התקין וזאת נוכח חשיבותן של מערכות המידע, שלמותן ואיכותן לתפקוד המועצה.

3. **אבטחת מידע** – ראש המועצה הנחה את מנכ"לית המועצה להכין מסמך הכולל עקרונות למדיניות אבטחת המידע בארגון. לאחר אישור המדיניות, על מנהל מערכות המידע להכין תכנית עבודה שנתית ורב שנתית להטמעת המדיניות בארגון, שימורה ועדכונה מעת לעת.

4. **ממונה על אבטחת מידע** - ראש המועצה הנחה את המנכ"לית ואת מנהלת משאבי אנוש לפעול בדחיפות לאיוש תפקיד הממונה על אבטחת המידע, כנדרש בחוק.

5. **תיקון ליקויים** - ראש המועצה הנחה את מנהל המחשוב לפעול בדחיפות לתיקון הליקויים שהעלתה הביקורת, כגון: קביעת נהלי עבודה, הדרכת עובדים, שיפור האבטחה הלוגית והפיזית של מערכות המידע.