

נאותות ניהול סיכוני סייבר והגנת הפרטיות בשגרה ובמהלך משבר נגיף הקורונה

- 1 מבוא
- 4 רישום מאגרים, הגדרות מאגרים וממשל תאגידי בהיבטי אבטחת מידע.....
- 7 הדרכות עובדים ומדיניות בקרת גלישה במרשתת.....
- 8 ניהול משתמשים והרשאות במערכות המחשוב.....
- 12 איתור, דיווח ותגובה לאירועי אבטחת מידע
- 14 התקנים ניידים ואבטחת מכשירי טלפון ניידים ומחשבי לוח.....
- 15 שימוש במערכות הפעלה מעודכנות, הפרדת מערכות המאגרים ואבטחתם הפיזית.....
- 16 קיום הגנה אפקטיבית כנגד מתקפות מתוחכמות.....
- 17 חולשות אבטחה בכתובות חיצוניות של העירייה הנגישות למרשתת ולדוא"ל
- 18 מיקור חוץ
- 20 הערכה וניהול סיכוני סייבר במעבר לעבודה בחירום במשבר נגיף הקורונה
- 21 אבטחת מחשבי הקצה מהן מבוצעת גישה מרחוק לרשת העירייה
- 23 אבטחת גישה מרחוק לרשת הפנימית, לדוא"ל הארגוני של העירייה ולמערכותיה.....
- 26 מבדק סימולציית דיוג (FISHING).....
- 26 סיכום.....

מסמך זה מכיל ממצאי ביקורת של מבקרת העירייה. פרסומו של המסמך או חלק ממנו לפני שחלף המועד שנקבע להגשתו למועצה, ללא נטילת רשות מטעם מבקרת העירייה, אסור עפ"י הוראות סעיף 170ג(ו) ו- 334א לפקודת העיריות.

המפרסם מסמך ביקורת כאמור דינו מאסר שנה.

מבוא

הקצב המהיר של השינויים הטכנולוגיים, הגידול בכמות השירותים הדיגיטליים וזמינותם, הממשק עם מערכות ותיקות והצורך ההולך וגדל בקווי תקשורת עם ספקים, יוצרים כר נרחב להתפתחותם של איומי סייבר ולחשיפתה של העירייה לסיכונים סייבר משמעותיים. בד בבד, חלה בעשור האחרון עלייה מתמדת במספרם של גורמי איום בהיבטים של יכולות, זמינות, כלי תקיפה וקבוצות תקיפה. סיכונים סייבר עלולים להתממש כתוצאה מניצול של חולשות במערכות, בתהליכים ובהתנהלות הגורם האנושי, ומתגבשים לכדי שיבוש בפעילות השוטפת, מניעה של אספקת שירותים לתושבים בשגרה ובחירום, חשיפת העירייה לתביעות משפטיות ולעיצומים רגולטוריים וכיו"ב.

הביקורת בנושא שנערכה בחודשים אפריל – יולי 2020 התבססה על בדיקות מדגמיות רחבות היקף בהתאם למובא להלן. הביקורת מציינת את שיתוף הפעולה של מנהל מערכות מידע בעירייה, והחברה לאוטומציה המעניקה שירותי מחשוב רחבים לעירייה.

מטרת הביקורת והמתודולוגיה - הביקורת פעלה לבחינת הפרמטרים הבאים:

1. הערכת הסיכונים הפוטנציאליים וחשיפת הכשלים הקיימים, באופן יישום אמצעי טכנולוגיה ותהליכים טכנולוגיים החושפים את מערכות המידע של העירייה לפגיעה או לדלף מידע בשל מתקפות סייבר ממוקדות, אשר התגברו במהלך משבר נגיף הקורונה. בחינת אפשרות ניצול מצב החירום המאופיין בעבודה מרחוק, והערכת סיכונים סייבר לעבודה מרחוק בימי החירום.
2. הערכת סיכונים סייבר והגנת הפרטיות בתהליכים טכנולוגיים בעירייה, בהתייחס לדרישות הרגולציה בכלל ולתקנות הגנת הפרטיות בפרט.
3. להלן עיקר ההיבטים שנבחנו בביקורת: בחינה של תהליך הערכת סיכונים ושל תוכנית ניהול סיכונים סייבר במשבר נגיף הקורונה, ובעבודה בחירום ובשגרה; בחינת העמידה בתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017 (להלן - התקנות), לרבות, קיום נהלים; מבנה ארגוני; הדרכות; בקורות טכנולוגיות ומיקור חוץ; בחינת ההיערכות הטכנולוגית של העירייה לעבודה מרחוק בחירום במשבר נגיף הקורונה; בחינת אפקטיביות אמצעי האבטחה למניעת חדירת נזקות למחשבים ניידים, אשר הועמדו לרשות עובדי העירייה לשם ביצוע עבודה מרחוק, ולרשת העירייה באמצעות השימוש בדוא"ל, במדיה נתיקה ובגלישה במרשתת; בחינת אמצעי האבטחה לשם מניעה של זליגת מידע רגיש מהעירייה; בחינת רמת אבטחת המידע במחשבים הביתיים של עובדי העירייה, מהם הוגדרה גישה מרחוק לעבודה בחירום עקב משבר נגיף הקורונה; בדיקת אפקטיביות מנגנוני האבטחה של ממשק גישה דרך דפדפן OWA¹ לדוא"ל הארגוני ושל ממשק VPN² בגישה מרחוק, וחוזק מנגנון ההזדהות לשם כניסה ושימוש במערכות המחשוב בכניסה מרחוק; בחינת אפקטיביות מנגנוני הניטור והתגובה לאירועי סייבר, על ידי עובדי מערכות המידע ומחלקת אבטחת מידע בעירייה; בחינת מודעות עובדי העירייה, להתמודדות עם מתקפות דיוג (Fishing)³; מבדק חדירה לאיתור חשיפות אבטחה

¹ OWA ראשי תיבות של Outlook Web Access - אתר אינטרנט מרוחק אשר באמצעותו מתקבלת גישה לתיבת הדואר האלקטרונית.

² VPN ראשי תיבות של Virtual Private Network בתרגום חופשי: רשת פרטית וירטואלית או רשת פרטית מדומה. שיטה להעברת מידע פרטי על גבי תשתית, שעיקרה או כולה בבעלות ציבורית או בבעלות פרטית עם גישה לכלל הציבור. מטרתו של ה-VPN הינה להעביר מידע מהרשת הארגונית לאדם כלשהו, שנמצא במקום בו לא קיימת תשתית תקשורת פרטית של הארגון, אבל קיימת תשתית ציבורית - מרשתת או טלפוניה.

³ Fishing - דיוג - שיטת הונאה המבוססת על "דיוג" של מידע פרטי וחסוי של הקורבן, על ידי התחזות.

בכתובות IP⁴ חיצוניות של העירייה; איתור חולשות אבטחה ברשת הפנימית של העירייה באמצעות כלי סריקה אוטומטי.

4. בביקורת בוצעו בדיקות טכנולוגיות מדגמיות כדלקמן: נערך שילוב של כלי תוכנה מקצועיים לסריקה אוטומטית לאיתור חולשות אבטחה, ובדיקות ידניות שונות ברשת המחשוב הפנימית והחיצונית; מבדקי חדירה דרך המרשתת בהתאם לכתובות IP חיצוניות שסופקו לביקורת והמזוהות עם העירייה, לשם בחינת אפקטיביות ההגנה בגין ניסיונות תקיפה מהמרשתת בידי גורם זדוני על הממשקים החיצוניים של העירייה⁵; בדיקת מחשב נייד ארגוני לדוגמה של מבקרת העירייה, ומחשב נייד נוסף המשויך לאגף ההנדסה; ביצוע סימולציה של תרגיל דיוג (Fishing) מדגמי, לבחינת מודעות העובדים באמצעות פנייה טלפונית.

חוקים ותקנות בהיבטי הגנת הפרטיות ואבטחת מידע

1. **חוק הגנת הפרטיות, התשמ"א-1981 (להלן – החוק)** מסדיר את סוגיית הזכות לפרטיות. החוק המקיף את תחומי הגנת הפרטיות ונוגע לתחומי משפט שונים, מגדיר מהי פגיעה בפרטיות ובאילו מצבים היא מוצדקת. בנוסף, מסדיר החוק גם את פעילותם של מאגרי מידע הכוללים מידע פרטי ורגיש, וכן קובע, כי ראיות שהושגו תוך כדי פגיעה בפרטיות, לא תהיינה קבילות, אלא באישור בית המשפט. בסעיף 7 בחוק מוגדרים המונחים הבאים:

- **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 אישיותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו".
- **מידע רגיש** - "1) נתונים על אישיותו של אדם, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו; 2) מידע ששר המשפטים קבע בצו, באישור ועדת החוקה חוק ומשפט של הכנסת, שהוא מידע רגיש".

2. ביום 8 במאי 2018 נכנסו לתוקפן **התקנות**, המגדירות את חובותיו של בעל מאגר מידע בו מנוהל מידע אישי, ביישום בקרות תהליכיות וטכנולוגיות לצורך אבטחת המאגר ומניעת הפרת הפרטיות של נשואי המידע. מטרת התקנות, היא לפרט ולקבוע את עקרונות אבטחת המידע הקשורים בניהול ובשימוש במידע אישי, בהתבסס על תקני אבטחת מידע מקובלים בעולם. התקנות מתייחסות בין היתר, לאבטחת הגישה מרחוק למאגרי מידע, ולניטור אוטומטי לאחר אירועי אבטחת מידע.

3. ב-23 במרץ 2020 פרסמה **הרשות להגנת הפרטיות**⁶ מסמך בנושא "הגנת הפרטיות בעקבות התפשטות נגיף הקורונה: שאלות ותשובות להתנהלות הציבור, גופים ציבוריים והשוק הפרטי".

⁴ **כתובת IP** - מזהה מספרי ייחודי שמתפקד כ"כתובת הדיגיטלית" המשמש לזיהוי נקודת קצה, כגון מחשב ברשתות תקשורת.

⁵ VPN, דוא"ל, SMTP, OWA, STMP) ראשי תיבות של Simple Mail Transfer Protocol בתרגום חופשי: פרוטוקול פשוט לשליחת דוא"ל (דרך המרשתת).

⁶ **הרשות להגנת הפרטיות** - הגוף מטעם משרד המשפטים המסדיר, המפקח והאוכף על פי חוק הגנת הפרטיות בישראל. כרגולטור הפועל להגנה על זכות היסוד לפרטיות ולהגנת מידע אישי בישראל, הרשות להגנת הפרטיות מופקדת על הגנת המידע האישי במאגרי מידע דיגיטליים ועל ביצורה של הזכות לפרטיות. לתכלית זו מפעילה רגולציה, לרבות אכיפה מנהלית ופלילית, על כלל הגופים בישראל - פרטיים, עסקיים וציבוריים, המחזיקים/המעבדים מידע אישי דיגיטלי.

המסמך כולל בין היתר, התייחסות לנקיטת אמצעי אבטחה סבירים לעבודה מרחוק של עובדים וקובע, כי על המעסיקים לבחון, כי הם עומדים בהוראות התקנות. הרשות להגנת הפרטיות מכירה בכך, שמצבי חירום, כדוגמת המצב הנוכחי, מחייבים את הגופים השונים לפעול במהירות, וכי לחובה זו עשויה להיות גם השלכה על סוגיות הנוגעות לפרטיות. **עם זאת מבהירה הרשות, כי בכל הנוגע להיבטים של אבטחת מידע, אין במצב חירום בכדי להצדיק אי עמידה של הגופים השונים בהוראות הדין הרלוונטיות לעניין זה.**

4. ב-27 בפברואר 2020 פרסם **מערך הסייבר הלאומי**⁷ התרעה בגין "ניצול הבהלה הציבורית סביב נגיף הקורונה לביצוע מתקפות סייבר". בחודשים מרץ ואפריל 2020 פרסם מערך הסייבר הלאומי מסמכים נוספים בדבר ניצול מגפת הקורונה לביצוע מתקפות סייבר, בהם, מסמך "המלצות הגנה לארגונים ועסקים לעבודה מהבית בעקבות התפשטות הקורונה".

המעבר לעבוד מהבית לשם מזעור המפגשים במקום העבודה, הופך את סביבת העבודה לפגיעה יותר: התוקף מנצל את ריחוקו של המותקף מסביבת עבודתו הטבעית, ואת רמת התקשורת המזערית עם שולח ההודעה. מרבית העובדים מתחברים דרך רשתות Wi-Fi⁸ ברמת אבטחה פחותה מזו של העירייה; עובדים מתפתים לפתוח הודעות דוא"ל בנושא נגיף הקורונה, הצעות להלוואות או מידע כוזב בענייני עבודה; קבלת הודעת דוא"ל מתוקף המתחזה לאישיות בכירה בארגון, בה ביצוע הנחיות שונות ובכלל זה, התקנת תוכנות זדוניות. קבלת הודעות, מידע שגוי או קישורים מושכים, מאפשרים השתלטות על המחשב מרחוק

רישום מאגרים, הגדרות מאגרים וממשל תאגידי בהיבטי אבטחת מידע

1. סעיף 2 בתקנות קובע כך: (א) בעל מאגר מידע יגדיר במסמך הגדרות מאגר 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 עם; (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.

להלן הממצאים והמלצות הביקורת:

א. טרם נכתבו מסמכי הגדרות למאגרים. נדרש לכתוב מסמכי הגדרות לכלל המאגרים הקיימים בעירייה, לעדכןם אחת לשנה ולאשרם מול מנהלי המאגרים.

⁷ **מערך הסייבר הלאומי** - גוף ממלכתי, ביטחוני וטכנולוגי האמון על הגנת מרחב הסייבר הלאומי ועל קידום וביסוס עוצמתה של ישראל בתחום. המערך פועל ברמת המדינה לחיזוק תמידי של רמת ההגנה של הארגונים והאזרחים, לטיפול בתקיפות סייבר ולסילוקן ולהיערכות לחירום.

⁸ **Wi-Fi** - טכנולוגיה המאפשרת למכשירים אלקטרוניים להעביר נתונים אלחוטית באמצעות גלי מיקרו שהם חלק מספקטרום הקרינה האלקטרומגנטית.

- ב. לא בוצע כל תהליך בחינה בו נבדק, האם המידע הנשמר במאגרים רב מן הנדרש למטרות המאגרים. לדעת הביקורת, כי במידה והיה מתקיים תהליך בחינה כאמור, סביר, כי היה מתגלה שבמאגרים השונים מנוהל מידע ישן על תושבים לשעבר, עובדים לשעבר וכיו"ב.
- ג. יש לבצע מיפוי מקיף של כלל המאגרים בעירייה, ועדכון ככל הפרטים בהם תוך הסרת מאגרים שהמידע בהם אינו רלוונטי והוספת מאגרים חדשים.
- ד. יש לקיים הדרכות, ולרענן הנחיות למנהלי מאגרי המידע בעירייה בנוגע לתפקידם.
- ה. יש לבצע בחינה של קיום מידע עודף במאגרים בהקדם האפשרי.
- ו. מומלץ, כי השירות המשפטי בעירייה, יוביל ויפקח אחר יישום כלל היבטיהם המשפטיים של חוק הגנת הפרטיות והתקנות.
- 2. ממשל תאגידי בהיבטי אבטחת מידע**
- על פי סעיף 17 בחוק, החבים באחריות אישית למאגרי המידע בכלל ולאבטחת המידע בפרט, הינם בעל המאגר ומנהל המאגר ביחד ולחוד.
 - סעיף 17(ב)(ב) מוסיף ומטיל אחריות אישית לאבטחת המידע גם על הממונה על אבטחת המידע וקובע, כי עירייה כגוף ציבורי, מחויבת למנות אדם בעל הכשרה מתאימה לתפקיד הממונה על אבטחת מידע.
 - סעיף 3 בתקנות קובע, כי "חלה חובה למנות ממונה על אבטחת מידע, או מונה ממונה על אבטחת מידע במאגר המידע יחולו הוראות אלה: (1) ממונה אבטחה יהיה כפוף ישירות למנהל מאגר המידע או למנהל פעיל של בעל המאגר או המחזיק בו, לפי העניין, או לנושא משרה בכירה אחר הכפוף ישירות למנהל המאגר; (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;
 - על תכנית הבקרה לכלול היבטים רבים, לרבות בדיקת סטטוס עדכוני אבטחה; בקרת תקינות מוצרי אבטחה; נאותות הרשאות גישה למאגרים; חיבור מדיה נתיקה; בקרה על אבטחת גישה פיזית למערכות המאגר, לרבות מורשי הגישה וחוזק מנגנוני הזיהוי; בקרה על תקינות לוגים במערכות, תקינות גיבויים, ניטור אירועי אבטחת מידע ועוד.
- א. בביקורת נמצא, כי מנהל מערכות מידע האחראי ליישום בפועל של תכנית העבודה בהיבטי מערכות מידע, מונה במקביל גם לתפקיד ממונה על אבטחת מידע בעירייה, ולמעשה מבקר ומפקח על פעולותיו שלו עצמו ושל העובדים הכפופים לו בגין העמידה בדרישות התקנות. יודגש בזאת, כי מנהל המאגר אינו יכול לשמש גם כממונה על אבטחת המידע שבמאגר, זאת בהתאם לתקנה 13(1) לתקנות הקובעות, כי ממונה על אבטחת מידע יהיה כפוף ישירות למנהל מאגר המידע או לנושא משרה בכיר אחר הכפוף ישירות למנהל המאגר. בנסיבות אלו, קיים חשש לניגוד עניינים בין התפקידים בהם תיווצר התנגשות בין צורכי מערכות מידע לבין צורכי אבטחת מידע והגנת הפרטיות. בהקשר זה, אפנה לדברי ההסבר בתקנות, לפיהם, הפרדת התפקידים נועדה לאבטחת בכירותו בארגון של הממונה ועצמאות שיקול דעתו.

ב. לביקורת הוצגה תכנית עבודה למערכות מידע לשנת 2020 הכוללת התייחסות לחלק מדרישות תקנות הגנת הפרטיות בלבד כגון: הדרכות לעובדים, סקר סיכונים, ניטור אירועי אבטחה ושדרוג מחשבים. לביקורת נמסר, כי בשנים עברו לא הוכנה תכנית כאמור.

ג. **להלן המלצות הביקורת בנושא:**

- (1) יש למנות ממונה אבטחת מידע בעירייה, אשר אינו מכהן בתפקיד ביצועי במערכות מידע. הממונה לא ימלא תפקיד נוסף העלול להעמידו בחשש לניגוד עניינים.
- (2) על הממונה להכין תכנית בקרה שוטפת לעמידה בכל דרישות התקנות, אשר תוגש לאישור הנהלת העירייה, וידווח על ביצועה להנהלה ולמנהלי המאגרים.
- (3) על הממונה להעביר דיווח תקופתי בכתב במסגרת ועדת היגוי, או ישירות להנהלה הבכירה ולמנהלי המאגרים, בו יוצגו תוצאות פעולות הבקרה שבוצעו על ידו והפערים ככל שימצאו לעמידה בדרישות התקנות. במסגרת זו, על הממונה לתעד באופן מפורט כל פעילות בקרה המבוצעת על ידו.

ד. **ועדת היגוי להיבטי אבטחת מידע:**

לשם קידום תחומי אבטחת מידע והגנת הפרטיות, נעזרים ארגונים רבים בוועדת היגוי אשר מתפקדיה המקובלים: אישור ועדכון מדיניות אבטחת המידע ונהלים; פיקוח ניהול תקין בתחום אבטחת המידע; אישור תכנית העבודה בתחום אבטחת מידע, הקצאת תקציבים ומעקב אחר יישומה; קיום דיונים באירועי אבטחת מידע חריגים; הבטחת קיומם של מנגנוני פיקוח ובקרה נאותים; סיוע להנהלה הבכירה בקבלת החלטות בתחום; קבלת דיווחים תקופתיים והנחיות מממונה אבטחת מידע.

- (1) נמצא, כי לא הוגדרה באופן פורמאלי ועדת היגוי לנושאי אבטחת מידע והגנת הפרטיות באמצעות כתב מינוי או במסגרת נוהל ארגוני לרבות תפקידיה, סמכויותיה וחבריה.
- (2) יש להגדיר באופן פורמאלי ועדת היגוי לנושאי אבטחת מידע והגנת הפרטיות לרבות משתתפיה, תפקידיה וסמכויותיה, וכן יש לכנסה בתדירות קבועה ומספקת כפי שיקבע תוך תיעוד מסודר בפרוטוקולים של הנושאים שנדונו, החלטות ומעקבי ביצוע. חברי הוועדה יהיו מתחומים מנהליים מגוונים מלבד מערכות מידע (לרבות יועץ משפטי, קצין ביטחון, משאבי אנוש, מנהלי מאגרים וכיו"ב). הוועדה תדווח לראש העירייה ולמנכ"ל העירייה אחת לשנה לכל הפחות, על פעילותיה, מסקנותיה והמלצותיה בנושאים בהם הוסמכה. מומלץ, כי הדיון השנתי בו יאושרו תכנית העבודה והתקציב, יהא במעמד מנכ"ל העירייה.

ה. **נהלי אבטחת מידע**

- סעיף 3(2) בתקנות קובע, כי "הממונה על אבטחה יכין נוהל אבטחת מידע ויביאו לאישור בעל המאגר".
- מדריך ליישום התקנות מטעם הרשות להגנת הפרטיות מורה, כי "הממונה על אבטחה יכין נוהל אבטחת מידע ויביאו לאישור הנהלה הבכירה של הארגון".
- סעיף 4(ג) בתקנות דן בתכולת נוהל אבטחת מידע אותו יקבע בעל מאגר מידע. סעיף 4(ד) בהן מוסיף, כי במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, יכלול נוהל אבטחת מידע התייחסות לסעיפים מחמירים נוספים.

(1) **נמצא, כי קיימים נהלי אבטחת מידע המתייחסים למרבית הדרישות בתקנות.**

(2) לביקורת הוצגו המסמכים הבאים: נוהל אבטחת מידע בעירייה (ממאי 2018); נוהל דרישות אבטחת מידע מגורמי חוץ (ממאי 2018); נוהל חוק הגנת הפרטיות (ממאי 2018); טופס הרשאות עובד והתחייבות לאבטחת מידע (מפברואר 2018); נוהל גיבוי מידע (מפברואר 2018); טיוטת נוהל קליטה וסיום עובד (יוני 2020).
הנהלים לא עברו תהליך אשרור ועדכון החל משנת 2018. על מנהל מחלקת מחשוב להגיש את הנהלים לאחר עדכוןם, לאשרורם בידי ועדת ההיגוי ומנכ"ל העירייה.

הדרכות עובדים ומדיניות בקרת גלישה במרשתת

הדרכות עובדים

סעיף 7 בתקנות קובע כדלקמן: (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.

1. מבדיקת הביקורת עולה, כי בעת תחילת העסקה בעירייה, נדרשים העובדים החדשים לחתום על טופס הצהרה לקיום סודיות וכללי אבטחת מידע בארגון. יודגש, כי לא כל העובדים הוותיקים המועסקים בעירייה הוחתמו על מסמך הצהרה כאמור.
2. כחלק מפעילות מנהל מערכות מידע בנושא ההדרכה ניתן למנות: שליחת הודעות ריענון בגין סיכונים אבטחת מידע לכלל העובדים, בפרט בנושא עבודה מרוחקת מהבית בימי משבר הקורונה; שימוש מאובטח בתוכנת Zoom; התרעות על קמפיינים של דיוג (Fishing) ועוד. באוגוסט 2018 התקיימו סדרות של הדרכות לכלל העובדים, וכן תוכנן ביצוע הדרכות חוזרות לעובדים בחודש מרץ 2020 שקיומן נדחה עקב משבר הקורונה.
3. לצורך הגברת מודעות וכושר התמודדות של עובדים עם מתקפות סייבר, ולשם בדיקת תגובת העובדים, נפוץ בארגונים רבים לבצע תהליך של סימולציית מסע פרסומי כוזב (Fishing) באמצעות שליחת דוא"ל לעובדים, ולבחון בכך, האם לדוגמא העובדים יפתחו קישור שצורף.
4. **הביקורת ממליצה כדלקמן:**

- א. יש להחתים את כלל עובדי העירייה להם ניתנת גישה ממוחשבת, על טופס התחייבות לשמירה על סודיות ועל כללי אבטחת מידע, בדומה לעובדים חדשים ועובדים שעברו המנוידיים מתפקידם.
- ב. יש לבצע הדרכות לעובדים להם גישה למערכות ולמאגרי מידע, בהיבטי אבטחת מידע והגנת הפרטיות כפי הנדרש בתקנות, לרבות הטמעת מנגנון לביצוע דרכה תקופתית אחת לשנתיים לכל הפחות.
- ג. יש לשקול לבצע תרגולי סימולציית דיוג (Fishing), להגברת יכולתם של עובדים להתמודד עם אירועי אמת.

מדיניות בקרת גלישה במרשתת

1. סעיף 14(א) בתקנות קובע, כי "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".
 2. כיום, הגלישה במרשתת מבוצעת דרך מערכת "חומת אש"⁹ ומודול סינון אתרים וקבצים. המודול אמור לחסום גישה לקטגוריות של אתרים המוגדרים כחסומים לגלישה, כגון אתרים בעלי תוכן בלתי הולם, לחסום הורדה של קבצים בפורמטים בלתי מורשים ולמנוע זליגה של מידע רגיש לאתרים חיצוניים.
 3. בביקורת נמצא, כי מדיניות הגלישה אינה מגבילה באופן מספק. לא מיושמת חסימה של חלק מקטגוריות ברות סיכון כגון אתרי דוא"ל ללא עלות שימוש; אתרי שיתוף ואחסון קבצים; שירותי גלישה אנונימית; אתרי פצחנות (Hacking)¹⁰; אתרי שיתוף תוכנות בלתי מורשות; אתרי משחקים; אתרי סרטים והזרמת מדיה. בנוסף, לא קיימת חסימה להורדה של קבצי הרצה¹¹ ותסריט (Scripting)¹² מהמרשתת.
- יודגש, כי במצב הנתון, גוברת החשיפה לזליגת מידע רגיש מרשת העירייה דרך המרשתת, ולחדירה של תוכנות זדוניות לרשת העירייה בגלישה לאתרים ברי סיכון.**
4. **המלצות הביקורת הינן כדלקמן:**
 - א. יש לבדוק מחדש את מדיניות הגלישה המתירנית הקיימת כיום בעירייה, ולהטמיע מדיניות גלישה מחמירה יותר לכלל העובדים בהתאם לעקרון של מתן גישת גלישה לצורכי עבודה בלבד, תוך צמצום הסיכונים לזליגת מידע רגיש וחסירת קטגוריות.
 - ב. יש לבדוק את הגדרות סינון הקבצים הקיימת כיום, לשם מניעה של הורדת קבצי הרצה ותסריט מהמרשתת.

ניהול משתמשים והרשאות במערכות המחשוב

- המטרה בניהול משתמשים והרשאות, הינה להבטיח, כי רק לאנשים המתאימים תהיה גישה מתאימה, בזמן המתאים, לכלל המשאבים הטכנולוגיים שנדרשים עבור מילוי תפקידם. האחריות לאבטחת מידע בהתאם לסעיף 17 בחוק הגנת הפרטיות, הינה על בעל מאגר מידע, מחזיק במאגר או מנהלו. הניהול מתבצע על ידי מיפוי ויישום של כל מערך ההרשאות והתפקידים בעירייה, והגבלת הגישה לבעלי התפקידים הזקוקים לכך בלבד, תוך עמידה בעקרונות מידור והפרדת תפקידים למניעת ניצול לרעה של הרשאות. השאיפה היא, שעבור כל משתמש תהיה זהות דיגיטלית יחידה, שמרגע יצירתה, הזהות תנוהל, תתוחזק ותנוטר לכל אורך מחזור חיי הגישה למשאבי העירייה.

⁹ **חומת אש** (באנגלית Firewall): מערכת לניטור וחסירת התקשרויות בלתי רצויות לרשת התקשורת או מחשב יחיד.
¹⁰ **פצחנות (Hacking)** - תהליך בו עושים שימוש במערכות ממוחשבות בכדי להגיע לתוצאות אבטחת מידע טובות יותר מאשר בתכנון המקורי. כיום, למעשה מדובר בתהליך אשר באמצעותו משיגים מידע חסוי ומאובטח, ופורצים מערכות ותוכנות.

¹¹ **קובץ הרצה** - קובץ אשר מכיל נתונים המתורגמים לתוכנית על ידי המחשב.

¹² **תסריט (Scripting)** - תוכנית מחשב הנכתבת על מנת למכן ביצוע משימות, שאחרת היו אולי מבוצעות באופן ידני על ידי משתמש בסביבת תוכנה.

- מדיניות ניהול משתמשים והרשאות למידע ומשאבים, ושיטות לאימות זהותו של המשתמש, כוללת **מתן והסרה של הרשאות** משתמשים במערכות העירייה, **ניטור פעילות משתמשים** מול המידע העירוני, **בקרת סיכונים** בעת גישת משתמשים למידע, איתור **וטיפול בחריגות הרשאות**, **שמירה על עדכניות** המידע האישי והעירוני של המשתמשים וכלים **למימוש בקרות מפצות** במקומות שבהם הבקרה אינה מתאפשרת.
- בסעיף 8 בתקנות הדן בניהול הרשאות גישה נקבע כדלקמן: (א) בעל מאגר מידע יקבע הרשאות גישה של בעלי הרשאות למאגר המידע ולמערכות המאגר בהתאם להגדרות תפקיד; הרשאות הגישה לכל תפקיד תהיה במידה הנדרשת לביצוע התפקיד בלבד (ב) בעל המאגר ינהל רישום מעודכן של תפקידים, הרשאות הגישה שניתנו, ושל בעלי הרשאות הממלאים תפקידים אלה.

בתחילת העסקת עובדים חדשים, וכן בניוד עובדים בין תפקידים ביחידות שונות, קיים תהליך של ניהול הרשאות מחשוב, הכולל טופס הרשאות מובנה הנחתם על ידי מנהלו הישיר של העובד. **יודגש כי, תהליך זה מבוקר באופן חלקי, וגורם לשימוש בלתי ראוי במשאבי העירייה כדלקמן:**

1. במסגרת תהליך תיקוף, כל מנהל מאגר מידע הממונה על מאגר, נדרש לבצע סקירת הרשאות, בה עליו לקבל הרשאות גישה פר משתמש, ולקבוע, באם ההרשאה נחוצה לכל משתמש או שמה קיימת הרשאה עודפת ונדרש להסירה. בפועל, לא מיושם תהליך תקופתי של תיקוף הרשאות גישה קיימות לכלל המשתמשים, ולכלל המאגרים העירוניים.
2. הביקורת מדגישה בזאת, כי נמצאו שני עובדי עירייה לשעבר, להם עדיין הייתה קיימת סיסמא והרשאה למאגרי מידע רגישים חודשים לאחר סיום העסקתם.
3. **חמור מכך נמצא, כי בחודש אוגוסט 2020 ביצעה עובדת עירייה במחלקה לשירותים חברתיים, שימוש אישי פסול מיסודו במידע חסוי ורגיש, זאת תוך ניצול החשיפה לנתונים שאינם תחת טיפולה במאגר מידע אליו היא מורשית לגשת. זאת ועוד, בעת תשאול העובדת, היא הכחישה את הטענות שהופנו כנגדה וטענה דברי כזב. במכלול הנסיבות כמתואר, עברה העובדת על הוראות החוק והפרה את חובת אמונה כלפי העירייה שלא בתום לב. לאחר קיום הליך משמעותי, העובדת הושעתה מעבודתה, ובזאת יודגש כדלקמן:**

א. חוק יסוד: כבוד האדם וחירותו קובע בסעיף 7(א) כי "כל אדם זכאי לפרטיות ולצנעת חייו".
ב. חוק חופש המידע, תשנ"ח – 1998 קובע בסעיף 9(א)(3), כי רשות ציבורית, בכללה עירייה, לא תמסור מידע שגילוי מהווה פגיעה בפרטיות, כמשמעותה בחוק הגנת הפרטיות, אלא אם כן הגילוי מותר על פי דין.

ג. בחוק הגנת הפרטיות נקבע העיקרון הבסיסי לפיו "לא יפגע אדם בפרטיות של זולתו ללא הסכמתו, ומגדיר פגיעה בפרטיות, בין ביתר, כאחת מאלה: העתקת תוכן של מכתב או כתב אחר שלא נועד לפרסום, או שימוש בתכנו, בלי רשות מאת הנמען או הכותב בסייגים; הפרה של חובת סודיות שנקבעה בדין לגבי ענייני הפרטיים של אדם; שימוש בדיעה על ענייני הפרטיים של אדם או מסירתה לאחר, שלא למטרה שלשמה נמסרה; פרסומו או מסירתו של דבר שהושג בדרך פגיעה בפרטיות לפי הסעיפים הקודמים; הפרה של חובת סודיות לגבי ענייני הפרטיים של אדם, שנקבעה בהסכם מפורש או משתמע; פרסומו של ענין הנוגע לצנעת חייו האישיים של אדם, או למצב בריאותו, או להתנהגותו ברשות היחיד.

- ד. חוק הגנת הפרטיות, מוסיף וקובע בסעיף 8 כי לא ישתמש אדם במידע שבמאגר מידע החייב ברישום לפי סעיף זה, אלא למטרה שלשמה הוקם המאגר.
- ה. **חובת הסודיות** שנקבעה בסעיף 16 מורה, כי "לא יגלה אדם מידע שהגיע אליו בתוקף תפקידו כעובד, כמנהל או כמחזיק של מאגר מידע, אלא לצורך ביצוע עבודתו או לביצוע חוק זה או על פי צו בית משפט בקשר להליך משפטי...".
- ו. משמעות הפגיעה בפרטיות והפרת חובת הסודיות בהתאם לחוק, הינה עבירה פלילית שעונשה מאסר ועוולה אזרחית, שבגינה ניתן לתבוע פיצוי כספי.
- ז. חוק העונשין, תשל"ז - 1977 (להלן – חוק העונשין) מורה בסעיף 7.1 משמעות מיוחדת לגבי עובדי ציבור, ובכללם עובדי רשויות מקומיות, מאחר והוא קובע הוראות בדבר מסירת ידיעות רשמיות שהגיעו לעובד בתוקף תפקידו והתרשלות בשמירתן ובהחזקתן; הפרת חוזה ובו התחייבות לשמור בסוד ידיעות שיגיעו אליו עקב ביצוע החוזה; מסירה ללא סמכות כדן, ידיעה כאמור לאדם שלא היה מוסמך לקבלה. החוק מטיל עונשים על העוברים על הוראות אלו (לעניין זה סעיף 117 א' ו - 118 בחוק העונשין).
- ח. יחסי עובד מעסיק נחשבים על פי דיני העבודה ליחסים חוזיים. חוזה עבודה מושתת על יחסי אמון הדדיים. חובת האמון וחובת תום הלב כלפי המעסיק חלות על העובד, מרגע קבלתו לעבודה, במהלך כל תקופת יחסי העבודה ואף לאחר סיומם. יודגש בזאת, כי פעולות מסוימות בהם ניצול של משאבי המעסיק לשימוש פרטי שלא בתום לב, מהוות באופן בולט וברור הפרת חובת אמון מצד העובד.
- ט. על כלל עובדי הרווחה חלה חובת הסודיות מתוקף סעיף 8 ב' בחוק העובדים הסוציאליים, כנאמר, כי הוראות סעיף קטן (א) חלות גם על כל אדם שקיבל מידע לפי הסעיף האמור.
- (1) בהתאם להוראה 1.19 בתע"ס¹³ בנושא מאגר מידע – נתוני יסוד אודות משפחות מטופלות במחלקות לשירותים חברתיים - על עובדי המחלקה לשירותים חברתיים להקפיד בשימוש במידע העומד לרשותם, לבל יפגע חופש הפרט של הלקוח העומד בכל הכללים המפורטים בהוראה 1.17 בתע"ס בנושא חובת הסודיות.
- (2) בהתאם להוראה מספר 1.17 על כל עובדי המחלקות לשירותים חברתיים חלה חובת סודיות בגין מידע המגיע אליהם בתוקף תפקידם, ושימוש בו רק במטרה שלשמה נועד.
- (3) בהוראה מספר 2.13 בתע"ס בנושא כללי התנהגות של עובדי מנהל וזכאות, מוגדרת חובתם של אלו לשמור בסוד על מידע המגיע עליהם במסגרת עיסוקיהם כעובדי רשות מקומית, ולא יגלו אותו, אלא על פי כל דין.
- (4) הגנה על מידע ממוחשב הכולל תיקי משפחה ממוחשבים ודו"חות ממוחשבים, יתבצע על פי אמצעי אבטחת המידע כפי המופיע בהוראה מספר 1.25 בתע"ס, הן באבטחת מידע במחלקות לשירותים חברתיים, לפיה בין היתר: על כל עובד - להגן ולשמור על

¹³ תקנון העבודה הסוציאלית בישראל (להלן - תע"ס), הינו קובץ תקנות מפורט, הבא להסביר ולהסדיר את החוקים הקיימים בענייני רווחה במדינת ישראל. תוקפן החוקי של ההוראות המופיעות בתע"ס, הוא מכוח: התקנות לחוק שירותי הסעד, תשי"ח - 1958; תקנות ארגון לשכת הסעד (תפקידי המנהל וועדת הסעד), התשכ"ד - 1963, הקובע בסעיף 4 (א) (1) "מתן טיפול סוציאלי לנזקקים והגשת סעד על פי דין ובהתאם להוראות נוהל והנחיות המנהל הכללי של משרד העבודה, הרווחה והשירותים החברתיים, וכן מכוח תקנות שירותי הסעד, טיפול בנזקקים התש"מ"ו - 1986.

המידע המצוי ברשותו באמצעים פיזיים בהתאם להנחיות הממונה על אבטחת המידע ברשות המקומית. שימוש במאגרי המידע של הרשות המקומית יהיה אך ורק לצורך מילוי תפקידו של העובד המשתמש בהם ובהתאם להרשאות הגישה הייעודיות שלו. (5) יודגש, כי לעובדת הרשאת כניסה למאגרי מידע חסויים ורגישים, וזאת מבלי שהיא חתומה על טופס התחייבות לשמירת סודיות בניגוד להוראות התע"ס.

מסירת מידע למבקרת העירייה –

(1) סעיף 170 ב(א) בפקודת העיריות {נוסח חדש} קובע בין היתר, כי עובדי העירייה יתנו למבקר העירייה, על פי דרישתו, כל מידע או הסבר שיבקש בתוך התקופה הקבועה בדרישה ובאופן הקבוע בה.

(2) מרמה והפרת אמונים היא עבירה בישראל המופיעה בסעיף 284 לחוק העונשין, בהתאם לו, עובד הציבור העושה במילוי תפקידו מעשה מרמה או הפרת אמונים הפוגע בציבור, אף אם לא היה במעשה משום עבירה אילו נעשה כנגד יחיד, דינו מאסר שלוש שנים. בפסק דין¹⁴ ציין הנשיא ברק, כי האיסור הפלילי על הפרת אמונים בא לשמור בין היתר על הערך המוגן של טוהר המידות של פקידי הציבור, והוא שמירה על התנהגות הוגנת וישרה של עובד ציבור.

4. אבטחת מידע במחלקות לשירותים חברתיים –

א. בהתאם להוראה מספר 1.25 בתע"ס במחלקה לשירותים חברתיים ימונה רפרנט בנושא אבטחת מידע (להלן – הרפרנט) שיהיה מנהל המחלקה או מי מטעמו. הרפרנט יפעל על פי הנחיות הממונה על אבטחת המידע ברשות, ובהתאם לחוק הגנת הפרטיות ותקנותיו.

ב. בהתאם למסמך הנחיות ונוהל אבטחת מידע, במקרים חריגים, כגון תקופת הקורונה, בקשה לקבלת מידע מאת גוף ציבורי (כגון ביטוח לאומי, המשרד לשירותים חברתיים) ניתן למנות בכתב מינוי מסודר, עובד שאינו עובד מחלקה לצורך מתן מענה או סיוע.

ג. בביקורת נמצא, כי מנהלת פרויקט "עיר חכמה" בעירייה, מונתה כרפרנטית בנושא אבטחת מידע. הביקורת מדגישה, כי כל עוד מינויה מאושר על ידי מנהלת המחלקה לשירותים חברתיים, קיים איסור שלרפרנטית תהיה גישה למידע חסוי.

ד. ניהול אבטחת המידע במחלקה לשירותים חברתיים יתבצע בהתאם כדלקמן: אחת לשנה יבצע הרפרנט ריענון של נהלי אבטחת מידע במחלקה לשירותים חברתיים ברשות, וידאג להפצתם בקרב העובדים. כמו גם, הרפרנט יבצע בדיקות אקראיות באשר לביצוע נהלי שמירת אבטחת המידע במחלקה. במסגרת בדיקות אלה יפיק דו"ח בכתב לממונה על אבטחת מידע ברשות ולמנהל המחלקה, בו יציין המלצותיו לטיפול.

יצוין, כי בניגוד להנחיה, לא בוצע ריענון של נהלי אבטחת מידע בקרב עובדי הרווחה, ולא בוצעו בדיקות אקראיות באשר לביצוע שמירת אבטחת המידע במחלקה.

5. יצוין, כי בתקופת משבר נגיף הקורונה, בוצעה הקפאה זמנית של חשבונות המשתמש של העובדים שלא עבדו בחירום.

6. להלן המלצות הביקורת:

¹⁴ דני"פ 1397/03 מדינת ישראל נ' שמעון שבס, ניתן ב-30 בנובמבר 2004.

- א. יש לבצע תיקוף תקופתי של נאותות ההרשאות בכל המאגרים, תוך מעורבות כל מנהל המאגר בגין הרשאות הגישה למאגר שבאחריותו.
- ב. יש להגדיר באופן יסודי לכל עובד בעירייה, ולכל עובד בחברה חיצונית לעירייה לו גישה ממוחשבת למאגר מידע עירוני, את תחום ההרשאה המאושרת (צפיה ו/או שינוי נתונים מלאים או חלקיים) בהתאם למסגרת עבודתם בלבד, ובכך למנוע עודף הרשאות.
- ג. יש להחתים את כלל עובדי העירייה ועובדי חברות חיצוניות המעניקות שירותים לעירייה, על טופס התחייבות לשמירת סודיות כנדרש.

איתור, דיווח ותגובה לאירועי אבטחת מידע

סעיף 11 בתקנות הגנת קובע כדלקמן: (א) בעל מאגר מידע אחראי לתיעוד כל מקרה שבו התגלה אירוע המעלה חשש לפגיעה בשלמות המידע, לשימוש בו בלא הרשאה או לחריגה מהרשאה; 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 בעדכונן של נוהל האבטחה; במאגר מידע שחלה עליו רמת האבטחה הגבוהה, ייערך דיון כאמור אחת לרבעון לפחות; (ד) אירוע אירוע אבטחה חמור – (1) יודיע על כך בעל המאגר לרשם באופן מידי, וכן ידווח לרשם על הצעדים שנקט בעקבות האירוע; (2) רשאי הרשם להורות לבעל מאגר המידע...לאחר שנועץ בראש הרשות הלאומית להגנת הסייבר, להודיע על אירוע האבטחה לנושא מידע שעלול להיפגע מן האירוע.

משבר נגיף הקורונה הביא להתגברות רבת מידות במתקפות סייבר ודיוג מאסיביות כלפי ארגונים, תוך התמקדות בתקיפת מחשבי עובדים אשר עברו לעבוד מהבית. למותר לציין, כי לא ניתן למנוע כל מתקפה, לפיכך קיימת חשיבות משמעותית לקיום תהליכי ניטור וזיהוי אפקטיביים לאירועי אבטחת מידע, ולתגובה מיידית לאירועים אלה ולכל אירוע חריג לשם מניעת התפשטותם.

1. מנהל מערכות מידע מקבל התרעות על אירועים חריגים ברשת הפנימית של העירייה, בדוח יומי אוטומטי, וכן הוא צופה במערכת הקונסול¹⁵ בתדירות שוטפת. הלה בוחן את הרחבת יכולות הניטור באמצעות כלים אוטומטיים, ומבצע בחינה להעלאת רמת אבטחת המידע והסייבר. כמו כן, מקבל לידיו התרעות באמצעות הדוא"ל על מתקפות סייבר המתפרסמות בעולם, ועל פרצות אבטחה המתגלות במוצרי תוכנה וחומרה מהמרכז הארצי לניהול אירועי סייבר ומשרד הפנים.
2. נמצא, כי לחלק מאירועי האבטחה ברמת שרתי ניהול הרשת, מופעלת בקרה על תוכנת מדיניות קבוצתית (GPO)¹⁶ בה נבחנים ניסיונות גישה של משתמשים לרשת הארגונית, אירועים תפעוליים של מערכת ההפעלה ועוד.
3. **לא כל שכן, לדעת הביקורת, הניטור הקיים לאור התגברות מתקפות סייבר בשנה האחרונה, אינו מספק כפי המציין כדלהלן:**

¹⁵ התקן פיזי להצגת והכנסת הודעות טקסט, הקשורות לניהול מערכת ממוחשבת.

¹⁶ **מדיניות קבוצתית** (Group Policy, GPO) - תכונה המאפשרת לנהל קבוצות של מחשבים על פי מדיניות הנקבעת בידי מנהל המחשב ומוחלת על המחשבים המנוהלים. המדיניות הנאכפת על המחשב קובעת הגבלות ואפשרויות שימוש במחשב (כגון: מניעת שינוי השעה בשעון, הגבלה של סמלים בלוח הבקרה והגבלות על שינוי תיקיות במחשב).

- א. בעירייה לא מתקיים דיון שנתי במעמד הנהלת עירייה, בדבר אירועי אבטחת מידע.
- ב. אין בעירייה מידע בגין רמת הניטור המיושמת בחברה לאוטומציה לאחר אירועי אבטחת מידע, וכן לא ידוע מהם שירותי האבטחה ומערכות הליבה המסופקות על ידה לעירייה.
- ג. לאור רגישות המידע המנוהל על ידי החברה לאוטומציה, מן הראוי כי יבוצע על ידה ניטור מוגבר הכולל שימוש בתכנת ניהול אבטחת מידע ואירועים (SIEM)¹⁷ ושימוש במוקד ניטור ותגובה אנושי המופעל בתדירות רציפה בידי צוות מנתחי נתונים.
- ד. לא מוגדרת התרעה מפורטת, האמורה להישלח באופן אוטומטי בעת אירוע גילוי נגיף במחשבים הניידים מהם מבוצעת גישה מרחוק. אין עוררין, כי על אירוע כאמור להיות מטופל בסמיכות לקיומו, לרבות ביטול הרשאת הגישה מרחוק עד לסיום הבדיקה. יצויין, כי במהלך הביקורת מנהל מערכות מידע הגדיר התרעה בנושא.
- ה. מנהל מערכות מידע מסר, כי בוצע פיילוט להטמעת מערכת ניטור אירועי אבטחת מידע ברשת העירייה. רכישת מערכת הניטור נכללה בתוכנית עבודה לשנת 2020 אך רכישתה לא בוצעה, בשל ביטול המימון באמצעות קול קורא על ידי משרד הפנים.
- ו. מספר הגדרות בקרה בגין תוכנת מדיניות קבוצתית (GPO) אינן מופעלות, וקיים מקום להפעילן לשם תיעוד אירועים רגישים נוספים בשרתי ניהול הרשת הארגונית¹⁸.

4. להלן המלצות הביקורת בנושא:

- א. לאור התגברות ניסיונות מתקפות הסייבר בעולם, יש להקשיח את מדיניות התגובה לאירועי אבטחה, וכן להגדיר התרעות ספציפיות לאיתור אירועים חריגים במחשבים הניידים מהם מבוצעת גישה מרחוק.
- ב. יש לעבות את מנגנוני הניטור הקיימים אחר אירועי אבטחת מידע, וכן לבצע תרגולים פנימיים לבדיקת אפקטיביות המנגנונים ותהליכי התגובה לאירועים.
- ג. יש לבחון מול החברה לאוטומציה, את נאותות רמת הניטור המיושמת בה עבור העירייה אחר אירועי אבטחת מידע במערכות הליבה ובשירותי הגישה מרחוק, וכן נאותות מספקת של אבטחת המידע, לרבות קיום שירותי פתרונות אבטחה מתקדמים¹⁹.
- ד. יש להוסיף אירועים נוספים לשם תיעוד ובקרה בתוכנת מדיניות קבוצתית (כגון: גישה למשאבי הרשת על ידי המשתמש; חסימה ומניעת גישה).

¹⁷ SIEM - Security Information and Event Management - ניהול אבטחת מידע ואירועים התקן/תוכנה לניתוח לוגים מרכיבי תקשורת ותוכנות שונות. המערכת מקבלת נתונים ממערכות ארגוניות, מנתחת אותם ומאפשרת בקרה על תהליכים ואירועים, הפקת דוחות, זיהוי פרצות אבטחה ותגובה למתקפות המתרחשות בזמנים שונים.

¹⁸ כגון: בקרה על ניהול חשבונות ועל שינוי מדיניות בקרה (Audit Account management and policy change).

¹⁹ כגון SIEM SOC – SIEM ראשי תיבות באנגלית של Security Information and Event Management : SOC ראשי תיבות באנגלית של Security Operations Center: פתרון אבטחה מתקדם המשלב מערכות טכנולוגיות המנטרות תהליכים ואירועים חשודים במערכות, זיהוי פרצות אבטחה ותגובה בזמן אמת לאירועים. המערכת אוספת נתונים ממקורות רבים: תעבורת רשת, שרתים, בסיסי נתונים ואפליקציות. המערכת מבצעת תיאום נתונים לזיהוי פעילות חשודה, כגון זליגת מידע או הצפתו באופן לא לגיטימי.

התקנים ניידים ואבטחת מכשירי טלפון ניידים ומחשבי לוח

1. **אבטחת התקנים ניידים ומניעת חיבור התקנים זרים לרשת המחשוב העירונית** - סעיף 12 בתקנות 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".

א. מיושמת חסימה למניעת חיבור מדיה נתיקה אל תחנות הקצה. יחד עם זאת, חלק לא מבוטל מהמשתמשים (40 במספר), מורשים לחבר כל מדיה נתיקה למחשבים שבשימושם. נהיר, כי קיימת חשיפה רבה להחדרת נוזקה אשר לא תזוהה באמצעות נוגד נגיפים המותקן במערכות העירייה, וכן קיימת חשיפה לסיכונים נוספים של זליגת מידע רגיש.

ב. יצויין, כי לא הופעלה טכנולוגיה להצפנת נתונים במדיה נתיקה.

ג. לא נאכף מנגנון המאפשר חיבור של התקנים ניידים מטעם מחלקת מערכות מידע בלבד ו/או שהותרו לשימוש על ידה.

ד. נוסף על כך, לא נעשה שימוש בטכנולוגיה למניעת דלף מידע רגיש בזמן העתקת נתונים למדיה נתיקה (מסוג DLP - Data Loss Prevention Software)²⁰, ולא הוטמע שימוש בטכנולוגיה של הלבנת קבצים אל תחנות הקצה או שימוש בעמדות הלבנה ייעודיות.

ה. להלן המלצות הביקורת:

(1) יש לבחון ביצוע חסימה גורפת לאפשרות החיבור של מדיה נתיקה למערכות.

(2) במידה וקיים צורך משמעותי בשימוש בהתקן נייד, יש להגביל את השימוש למשתמשים מורשים בלבד ותחת מנגנונים לצמצום הסיכון כתוצאה מהחיבור כגון: טכנולוגיה להצפנת נתונים, הגבלה לחיבור התקנים שאושרו מראש בלבד, יישום מנגנון הלבנה טרם החיבור, יישום מודול DLP ועוד.

ו. מערכת מניעה לחיבור התקנים זרים לרשת המחשוב העירונית - בהינתן גישה פיזית של גורם זדוני אל משרדי העירייה, יכל הגורם לעקוף מנגנוני אבטחה היקפיים המיושמים ברשת, לרבות מערכת "חומת אש", ולבצע ניסיון חדירה ממחושב באמצעות חיבור למחשב או באמצעות חיבור התקן זר לרשת הפנים עירונית, תוך קבלת כתובת IP תקינה לרשת.

(1) על מנת לספק מענה לחשיפה זו, פותחה טכנולוגיית מערכת בקרת גישה לרשת (Network Access Control - NAC), שבאמצעותה ניתן לזהות ולנתק התקן בלתי מורשה המנסה להתחבר לרשת הפנים עירונית, ובכך למנוע חדירה לרשת לכל הפחות.

²⁰ תוכנה המנטרת, מדווחת ומונעת דליפה של מידע רגיש בתוך הארגון ומחוצה לו. המערכת מנטרת נתונים ובהתאם למדיניות החוקים שנקבעה מראש חוסמת העברת המידע אל גורמים בלתי מורשים.

- (2) בביקורת נמצא, כי לא מיושמת טכנולוגיה של בקרת גישה לרשת המחשוב הפנים עירונית. בתגובה נמסר, כי מתוכנן ביצוע פיילוט למערכת כאמור.
- הביקורת ממליצה לבחון הטמעה של מערכת בקרה, בכל רשת המחשוב הפנימית.
2. **אבטחת מכשירי טלפון ניידים ומחשבי לוח** - באמצעות יישומים זדוניים המועתקים בתם לב להתקנים ניידים, ניתן לגזול מידע רגיש, לרבות סיסמאות גישה ופרטי דוא"ל ארגוני, העשויים לכלול נתונים חסויים ואישיים.
- א. טרם הוטמע בעירייה פתרון להגנה על טלפונים ניידים ומחשבי לוח, מסוג ניהול רשומות אב (MDM - Master Data Services)²¹. יתרה מכך, לא יושמו הגדרות אבטחה בסיסיות, כגון אכיפת הגדרת קוד הגישה למכשיר המבצע סנכרון לדוא"ל ארגוני וחיבור ממכשיר מורשה בלבד מזוהה, יכולת מחיקה מרחוק ועוד.
- ב. הביקורת ממליצה לבחון הטמעה של תשתית MDM בהתקנים ניידים עירוניים, ועד להשלמת ההטמעה, יש להפעיל מנגנוני אבטחה בסיסיים לשם צמצום הסיכון.

שימוש במערכות הפעלה מעודכנות, הפרדת מערכות המאגרים ואבטחתם הפיזית

1. סעיף 13(ג) בתקנות 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".
2. בביקורת נמצא, כי בעירייה מיושמת מדיניות אחידה לביצוע עדכוני אבטחה ברמת מערכת הפעלה בשרתים, ובתחנות הקצה באמצעות כלי לעדכון וניטור מרכזי.
3. יחד עם זאת, במסגרת מבדקי חדירה וסריקות, נמצאו עדכוני אבטחה חסרים במערכות ההפעלה ובתוספי תכולה לתוכנות הקיימות.
4. נמצא, כי קיימות מספר תחנות קצה בהן מותקנת מערכת הפעלה מסוג Windows 7 וכן מספר שרתים בעלי מערכת הפעלה מסוג Windows Server 2008 אשר בהתאם לפרסומי היצרן, התמיכה במערכות הפעלה אלו הסתיימה מזה כבר בינואר 2020.
5. **הביקורת ממליצה כדלקמן:**
- א. יש לתכנן בהקדם שדרוג של תחנות הקצה ושל שרתים בהן מותקנות מערכות הפעלה ישנות וללא תמיכת היצרן.
- ב. יש להפעיל באופן תקופתי כלי סריקה ייעודי, באמצעותו ניתן לבדוק את סטאטוס עדכניות מערכות ההפעלה ותוכנות המותקנות במחשבים ובשרתים ברשת.
- ג. יש להשלים ביצוע עדכוני אבטחה ושדרוגי גרסאות בהתאם לממצאים שעלו בביקורת.
6. **הפרדת מערכות המאגרים** - סעיף 13(ב) בתקנות קובע כדלקמן: "בעל מאגר מידע יפריד, בהיקף ובמידה הסבירים האפשריים, בין מערכות המאגר אשר ניתן לגשת מהן למידע, לבין מערכות מחשוב אחרות המשמשות את בעל המאגר".

²¹ שורה של תהליכים וכלים העוזרים להגדיר ולנהל את אותן רשימות מידע, ולשמור על אותם נתונים מהימנים ומתוקפים.

בביקורת נמצא, כי לא מיושמת הפרדה בין תחנות הקצה ברשת העירונית לבין השרתים, לרבות שרתי ניהול רשת; שרתי קבצים; שרת דוא"ל; שרת גיבוי; שרת מערכת נתוני משרד הפנים ועוד. הואיל וכך, יש להוסיף הפרדה בין רשת תחנות הקצה לרשת השרתים, באמצעות שימוש במערכת "חומת אש" פנימית.

7. אבטחה פיזית של מערכות המאגר - בסעיף 6 בתקנות נקבע כדלקמן: (א) בעל מאגר מידע יבטיח כי המערכות המפורטות בתקנה 5(א)1 (תשתיות ומערכות חומרה, סוגי רכיבי תקשורת ואבטחת מידע) יישמרו במקום מוגן, המונע חדירה וכניסה אליו בלא הרשאה והתואם את אופי פעילות המאגר ורגישות המידע בו. (ב) בעל מאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, ינקוט אמצעים לבקרה ולתיעוד של הכניסה והיציאה מאתרים שבהם מצויות המערכות המפורטות בתקנה 5(א)1 ושל הכנסה והוצאה של ציוד אל מערכות המאגר ומהן. במסגרת יישום תקנה 6(ב) נקבע בתקנה 17 בתקנות בגין שמירת נתוני אבטחה כדלקמן: (א) בעל מאגר מידע ישמור את הנתונים האמורים הנצברים, באופן מאובטח למשך 24 חודשים. (ב) במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, בעל המאגר יגבה את הנתונים שנשמרו באופן שיבטיח שיהיה ניתן, בכל עת, לשחזר את הנתונים האמורים למצבם המקורי.

להלן ממצאי הביקורת:

א. חדר השרתים של העירייה ממוקם במתחם בבניין העירייה הנעול בדלת מחוסמת, לה מפתח הנמצא ברשות מחלקת המחשוב בלבד. המתחם מוגן בשעות היום על ידי שומר ייעודי בכניסה, ולאחר סיום יום העבודה מופעלת מערכת אזעקה המקושרת למוקד חיצוני. מעקב אחר הנכנסים לבניין העירייה, מבוצע בידי המוקד העירוני על ידי מצלמה ראשית. ב. נמצא, כי לא מיושם מנגנון בקרה ותיעוד גישה לחדר השרתים, לרבות רישום של הניגשים אליו לטיפול ולהכנסה או הוצאה של ציוד. יוצא איה, כי אין בעירייה מידע בגין זהות הנגישים ומועד הכניסה אל חדר השרתים.

הביקורת מדגישה, כי יש ליישם מנגנון לבקרת הגישה לחדר השרתים, בהתאם לקבוע בתקנות (כגון בקר זיהוי ביומטרי באמצעותו ניתן לשמור באופן דיגיטלי גישות בהתאם לזיהוי אישי, או כרטיס קירבה אישי). לכל הפחות, יש להתקין מצלמות לניטור ותיעוד גישות לחדר השרתים, אשר נתוניו ישמרו למשך 24 חודשים כנדרש בתקנות.

קיום הגנה אפקטיבית כנגד מתקפות מתוחכמות

1. סעיף 14(א) בתקנות קובע כדלהלן: 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. 2. בשנים אחרונות התגברו מתקפות סייבר מתוחכמות המנצלות פרצות "מתקפת אפס הימים" (Zero-day attack)²², להם טרם הוגדרה תוכנת נוגד נגיפים מתאימה ומוצרי אבטחה נוספים, ומשכך, הן עלולות לא להתגלות ולא להיחסם. לצורך התמודדות עם פרצות אלה, פותחו

²² "מתקפת אפס הימים" (Zero-day attack) - כינוי לשימוש בפרצת אבטחה בלתי מזוהה ע"י גורמי האבטחה ואשר אינה בררת תיקון עד כה.

טכנולוגיות אפקטיביות דרכן ניתן להרחיק את האיום ממשתמשי הקצה, ולאפשר גלישה מאובטחת במרשתת²³.

3. נמצא, כי בעירייה קיים שימוש במערכת "חומת אש" פנימית, לרבות נוגד נגיפים מקצועי בתחנות הקצה והשרתים. יתרה מכך, קיימת מערכת "חומת אש" חיצונית של החברה לאוטומציה לחיבורי ממשק VPN בגישה מרחוק של העובדים ומנגנון לסינון דוא"ל. זאת ועוד, מיושמת מדיניות סיסמאות טובה בגישה לרשת הארגונית ולשרתים.

4. הביקורת סבורה, כי קיים מקום להוסיף שכבות הגנה נוספות, וזאת כפי שפורטו למנהל מערכות מידע.

- א. מומלץ להפעיל מודולים והגדרות נוספות במוצרי האבטחה הקיימים בעירייה, לשם שיפור אפקטיביות המוצרים להתמודדות עם מתקפות סייבר.
- ב. מומלץ לבחון יישום של טכנולוגיות מתקדמות נוספות, לשם השגת יכולת נאותה להתמודד עם מתקפות סייבר מתוחכמות. יודגש, כי הטכנולוגיות שהומלצו, נפוצות כיום בארגונים בקנה מידה כשל העירייה, ואף בארגונים בעלי פעילות פחותה מזו.

חולשות אבטחה בכתובות חיצוניות של העירייה הנגישות למרשתת לדוא"ל
ביצוע מבדק באמצעות כלים אוטומטיים מקצועיים²⁴ לאיתור חשיפות אבטחה בטווח כתובות חיצוניות של העירייה, וניתוח תוצאות סקירות ובדיקות ידניות לתיקוף מדגמי, מעלים את הממצאים הבאים²⁵:

1. על אף שאתר המרשתת העירוני מוגן בידי מערכת "חומת אש", במסגרת הבדיקה נמצאו ממצאים החושפים אותו למתקפות סייבר²⁶. הממצאים הועברו לטיפול החברה לאוטומציה.
2. במסגרת הבדיקה, נמצאו חולשות אבטחה בממשק OWA המספק גישה מרחוק לדוא"ל הארגוני באמצעות הדפדפן. יתרה מכך, רכיבי שרת המערכת אינם מעודכנים²⁷ וקיימת תמיכה בפרוטוקולי תקשורת ישנים²⁸.
3. הואיל ולא מופעלת הגנה על בסיס מיקום גיאוגרפי²⁹, ממשק VPN לגישה מרחוק וממשק OWA פתוחים גלובלית, ובפרט למדינת מצרים. הואיל והעירייה הינה גוף המספק שירותים בישראל בלבד, וממשקים אלו משמשים את עובדי העירייה הנמצאים בארץ וגולשים מכתובות ישראליות בלבד, אין נחיצות כי ממשקים אלו יהיו נגישים מחוץ לישראל.
4. בוצע מבדק לשליחת דוא"ל עם צרופות מסוגים שונים, שמטרתו לבחון את אפקטיביות סינון קבלת דוא"ל זדוני אל שרתי העירייה. בבדיקה נמצא כדלקמן:

²³ באמצעות שימוש מרחוק והפרדת רשתות פנים ארגוניות מרשת האינטרנט (Secure browsing).

²⁴ כלי Nessus Professional - תוכנה מסחרית חוצה פלטפורמות, המשמשת לסריקה ואיתור פגיעויות ברשתות.

²⁵ יצוין כי, לא בוצעו פעולות אקטיביות לניצול חולשות ופריצה מחשש להשבתת פעילות.

²⁶ כגון: מספר רכיבי JavaScript אינם מעודכנים, חלק מקבצי webservices של Sharepoint חשופים לגישה לכל המרשתת.

²⁷ לרבות Openssl ו-Apache.

²⁸ מסוג 2,3 SSL.

²⁹ GEO protection - (GEO-Geostationary earth Orbit) הגנה מפני לוויינים המספקים שירותי תקשורת מתמשכים.

- א. קבצים הכוללים סיסמאות מסוגים שונים, מתקבלים ואינם נחסמים, בהם קבצים בפורמטים המשמשים פצחנים ("האקרים") להסתרת נזקות³⁰. יודגש, כי לא ניתן לבדוק קיום נגיפים בקבצים המוצפנים בסיסמא. לאור זאת מקובל, כי קבצים אלה ייחסמו בפיקוח מחלקת מערכות מידע.
- ב. קבצים מסוימים להם צורף קובץ דמוי נזקה, נחסמו. עם זאת, שני קבצים שכללו פקודות מאקרו³¹ לא נחסמו בדוא"ל, והפעלתם הודגמה על ידי מנהל מערכות מידע.
- ג. מבירור עם החברה לאוטומציה עולה, כי שירות הסינון המסופק לעירייה במכרז הקודם, הינו שירות סינון בסיסי. יתרה מכך, לא הוגדרה חוקה ברורה בגין סוגי הקבצים אותם נדרש לסנן. הביקורת מציינת, כי קיים מקום להרחבת השירות או יישום של סינון פנימי נוסף לכלים הקיימים בעירייה.
5. **להלן המלצות הביקורת:**
- א. יש לפעול לתיקון הפרצות באתר המרשתת העירוני ובממשק OWA של העירייה.
- ב. יש להפעיל שירות חסימה גיאוגרפי להגבלת הגישה בהתאם לצורכי העירייה.
- ג. יש לבחון חוקי סינון לקבצים המתקבלים בדוא"ל הארגוני ולהקשיחם, תוך הוספת מנגנוני סינון נוספים לאור התגברות סיכוני הסייבר.

מיקור חוץ

1. במסגרת התקנות, נקבע בסעיף 15 כי בעל מאגר המתקשר עם גורם חיצוני לצורך קבלת שירות, הכרוך במתן גישה למאגר המידע יבחן, לפני ביצוע ההתקשרות עם הגורם החיצוני המסוים כאמור, את סיכוני אבטחת המידע הכרוכים בהתקשרות, וכן יקבע במפורש בהסכם עם הגורם החיצוני את כל אלה, בשים לב לסיכונים: המידע שהגורם החיצוני רשאי לעבד ומטרות השימוש המותרות בו לצורכי ההתקשרות; מערכות המאגר שהגורם החיצוני רשאי לגשת אליהן; סוג העיבוד או הפעולה שהגורם החיצוני רשאי לעשות; משך ההתקשרות, אופן השבת המידע לידי הבעלים בסיום ההתקשרות, השמדתו מרשותו של הגורם החיצוני ודיווח על כך לבעל מאגר המידע; 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; חובתו של הגורם החיצוני להחתיים את בעלי ההרשאות שלו על התחייבות לשמור על סודיות המידע, להשתמש במידע רק לפי האמור בהסכם, וליישם את אמצעי האבטחה הקבועים בהסכם.
2. במידה והעירייה, כבעלת מאגר המידע, התירה לגורם החיצוני להעניק שירות באמצעות גורם נוסף, חובתו של הגורם החיצוני לכלול בהסכם עם הגורם הנוסף את כל הנושאים המפורטים בתקנה 15.
3. בנוסף, חובתו של הגורם החיצוני לדווח אחת לשנה לפחות לבעל מאגר המידע, אודות אופן ביצוע חובותיו לפי התקנות וההסכם, ולהודיע לבעל המאגר במקרה של אירוע אבטחה.

³⁰ ZIP ו-WAV
³¹ קובץ אקסל וקובץ SLK

- זאת ועוד, יש לנקוט באמצעי בקרה ופיקוח בגין עמידתו של הגורם החיצוני בהוראות ההסכם ובהוראות תקנות אלה, בהיקף הנדרש ובשים לב לסיכונים.
4. בקרה ותיעוד גישה: בהתאם לסעיף 10 בתקנות, במערכות של מאגר מידע אשר חלה עליו רמת האבטחה הבינונית או הגבוהה, ינוהל מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למערכות המאגר, 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. מנגנון הבקרה לא יאפשר, ככל יכולתו, ביטול או שינוי של הפעלתו, ויאתר שינויים או ביטולים בהפעלתו ויפיץ התראות לאחראים.
5. בעל מאגר מידע יקבע נוהל בדיקה שגרתית על נתוני התיעוד של מנגנון הבקרה, ויערוך דוח של הבעיות שהתגלו והצעדים שנקטו בעקבותיהן. נתוני התיעוד של מנגנון הבקרה יישמרו למשך 24 חודשים לכל הפחות.

הביקורת מעלה ממצאים כדלהלן:

העירייה נעזרת במספר ספקי מיקור חוץ, ביניהם, החברה לאוטומציה המספקת מערכות ליבה מרכזיות לעירייה, חברת EPR המספקת מערכת ניהול לשירותי הרווחה וכן בספקים נוספים. **תהליכי הפיקוח והבקרה המחשובים מול ספקי מיקור חוץ, אינם עונים על הדרישות דנן כפי המובא להלן:**

1. העירייה אינה מבצעת פנייה שנתית לכלל ספקיה המעניקים מיקור חוץ, ודורשת מהם נתונים בדבר עמידתם בדרישות תקנות הגנת הפרטיות ואבטחת מידע כנדרש בתקנות.
2. בשנת 2018 פרסמה העירייה נוהל "דרישות אבטחת מידע לגורמי חוץ", עליו חתם בשנת 2019 ספק חוץ אחד בלבד.
3. חלק מהספקים חתומים על התחייבות דרישות אבטחת מידע בנוסח ישן טרם פרסום התקנות.
4. העירייה אינה עורכת לספקי מיקור חוץ, בדיקה לעמידתם בכל הדרישות שנקבעו בסעיף 10 בתקנות בגין מנגנון תיעוד אוטומטי, שיאפשר בקרה לגישה למערכות המאגר על ידם.
5. העירייה מעסיקה את החברה לאוטומציה כספקית מיקור חוץ עיקרית לשירותי מערכות מידע, עימה חתמה על הסכם התקשרות טרם פרסום התקנות. חרף סיכונים אבטחת המידע הכרוכים בהתקשרות, ההסכם בין הצדדים חסר פירוט לתנאים כפי שנקבעו בסעיף 15 בתקנות. לביקורת הוצג מסמך המסביר את עמידתה של החברה לאוטומציה בתקנות, אך אין מדובר בהסכם משפטי על כל המשמעויות הנובעות מכך.
6. מבדיקת הביקורת עולה, כי חברת EPR מחזיקה בתעודת הסכמה לתקן ISO 27001 וכן קיים נספח התחייבות להסכם משנת 2015 המפרט דרישות לאבטחת מידע בהתייחס לחלק מדרישות סעיף 15 בתקנות בלבד. יצויין, כי לא בוצעה בחינה להוספת נספח נוסף אשר יהא תואם לכל דרישות התקנות, לרבות חתימת הספק על הנוהל העירוני שפורסם בשנת 2018.

המלצות הביקורת בנושא הינן כדלהלן:

1. יש ליישם תהליך של ניהול סיכונים אבטחת מידע עבור ספקי מיקור חוץ בהתאם לנדרש בתקנות, ובמסגרת זו, לבחון את העמידה בדרישות סעיף 10 בתקנות, בדבר מנגנון תיעוד אוטומטי שיאפשר בקרה על הגישה למערכות המאגר.

2. יש לקבל ולבחון את תוצאות סקרי אבטחת המידע ומבדקי חדירה שבצעו ספקי מיקור החוץ על ידי מומחים לאבטחת מידע, ובהתאם להן, יש לבחון נקיטת צעדים נוספים לבקרה ולפיקוח, בהם ביצוע ביקורת עצמאית בכותלי הספק.
3. יש לקבל מכל ספקי מיקור החוץ באופן תקופתי, את התקנים והתצהירים המעידים על העמידה בהוראות התקנות.
4. יש לוודא, כי ההסכמים החתומים עם ספקי מיקור החוץ, עומדים בכל דרישות סעיף 15 בתקנות, ובמידת הצורך, יש להחתימם על נוסח התחייבות מעודכן בהתאם.
5. יש להגביר את מעורבותה של מחלקת מערכות מידע, בגין ניהול סיכונים סייבר במערך הרמזורים והמצלמות בעירייה, וכן בפרויקט "עיר חכמה".

הערכה וניהול סיכונים סייבר במעבר לעבודה בחירום במשבר נגיף הקורונה

לאירוע לאומי ואף בינ"ל כשל מגפה, השלכות רחביות על פעילות העירייה. גם מתקפת סייבר מהווה אירוע מיוחד, והיא נמנית כפעולה התקפית לשם חדירה לסביבת הרשת המחשובית במטרה לגנוב מידע, וכן במטרה לשבש את הפעילות בסביבת הרשת ובמערכות המסתמכות בה ולהסב להן נזק. מערך הסייבר הלאומי פרסם מסמך תפיסה לאומי להיערכות ולניהול מצבי משבר, ומסמכים נוספים נלווים, בהם החובה לביצוע סקר היערכות בארגון³².

1. בביקורת נמצא ככלל, כי לעירייה קיימת תכנית התאוששות מאסון (קרי, תכנית המשכיות עסקית), הכוללת תהליכים, מדיניות ונהלים המשמשים להתאוששות מאסון (כגון: שריפה, הצפה, רעידת אדמה, מחיקה מוטעית וכיו"ב) המשבית לזמן ממושך את התשתית הטכנולוגית החיונית לפעילותה של העירייה. בפרט, קיימת תכנית חלופית להפעלת המוקד העירוני ממיקום חלופי. בתוכנית קיימת התייחסות למערכות גיבוי לרבות חשמל, תקשורת וחומרת מחשוב.
2. יצוין, כי התוכנית כוללת התייחסות לאירוע של העדר כוח אדם חיוני המהווה אירוע מקומי בעל השלכה מוגדרת, והיא אינה כוללת התייחסות מפורשת לאירוע לאומי ובנ"ל כמגפה, כמו גם אירוע סייבר, כאירועים העלולים להשבית את פעילות העירייה. לא כל שכן, נדרש לכלול התייחסות נפרדת לאופן התגובה, ההתאוששות וההמשכיות העסקית באירועי מגיפה וסייבר, לרבות תוכניות מגירה מפורטות.
3. באירוע סייבר ישנן השלכות רבות בכללן - פגיעה במוניטין; ניסיון לסחיטה מצד גורמים זדוניים לתשלום כופר; נדרש להוציא דיווחים לרשויות החוק והרגולציה (כגון הרשות להגנת הפרטיות) והודעות לתקשורת ולתושבים; נדרש לבצע חקירה פורנזית תוך שימוש בכלי תחקור מיוחדים, וכן לבצע רכש טכנולוגי במקרה של פגיעה בחומרה ועוד.
 - א. נמצא, כי בוצעו תרגולים לעבודה בחירום, אך ברם, לא בוצע תרגול מפורש להתמודדות עם אירועים מהותיים בעירייה – אירוע סייבר או אירוע מגפה.
 - ב. יצוין, כי לא נרשם תיעוד מפורט לתוצאות תרגולי החירום שבוצעו בעירייה.

<https://www.gov.il/he/Departments/news/cybercrisispreparedness>
<https://www.gov.il/BlobFolder/news/cybercrisispreparedness/he/tfisa.xlsx>

4. סקר סיכונים: בשנת 2018 נערך בעירייה סקר סיכונים, אשר התמקד ברשת המחשוב הפנימית. הסקר לא כלל בחינה של הסיכונים ברשת המחשוב החיצונית, אי לכך, לא בוצע מבדק חדירה לרשת והקשחה של ממשקי הגישה מרחוק לרבות VPN ו-OVA. במידה והיה מתבצע סקר סיכונים סייבר רשמי והיה מוצג להנהלת העירייה, סביר, כי ממצאים שנתגלו בביקורת, היו מטופלים מזה כבר, או לכל הפחות, היו במתווה תכנון לשיפור.
5. יצויין לחיוב, כי יושמו אמצעים לתיקון³³ ולגיבוי תשתיות ותקשורת, בכדי לאפשר במהרה המשך עבודה מרחוק במקרה של פגיעה או השבתה של חומרה, תוכנה וקו תקשורת ראשי בשל אירועים חיצוניים, לרבות אירוע סייבר.
6. נמצא, כי במשבר נגיף הקורונה, שירותי התמיכה הטכנית למשתמשים וכן שירותי התמיכה לחדר השרתים, המשיכו להינתן באמצעות תמיכה מרחוק במתודה המקובלת.
7. על אף פרסום הנחיות מערך הסייבר הלאומי להערכת סיכונים סייבר בגישה מרחוק, נמצא, כי לא בוצע תהליך מתועד ופורמאלי להערכת סיכונים סייבר, וכן לא הוגדרה תכנית עבודה לניהול ולצמצום סיכונים סייבר בגין עבודה בחירום במשבר נגיף הקורונה. יחד עם זאת, מנהל מערכות מידע ביצע מספר צעדים לצמצום הסיכון, כגון ביצוע הקשחת האבטחה במחשב הביתי של העובד במקרים ממנו ניגש העובד לעבודה מרחוק.
8. **להלן המלצת הביקורת בנושא:**

- א. יש לבצע סקר סיכונים סייבר ייעודי לעבודה בחירום במשבר נגיף הקורונה או דומה לו, תוך הערכת השלכות תרחישים שונים על תהליכים תפעוליים וחיוניים בעירייה. הסקר יוגש בצירוף המלצות להנהלת העירייה, ויתקיים בגינו דיון שבסופו יתקבלו החלטות.
- ב. יש לעדכן את התוכנית העירונית להתאוששות מאסון, עקב לקחי הגל הראשון של משבר נגיף הקורונה והנחיות מערך הסייבר הלאומי. במסגרת התוכנית, יש לכלול שלבי פעולה ספציפיים לתגובה ולהתמודדות עם אירוע סייבר.
- ג. יש לבצע תרגול תקופתי להתמודדות עם אירוע סייבר מהותי בעירייה, ואירוע מגיפה.
- ד. יש לתעד בפרוט את תוצאות תרגולי החירום המתבצעים בעירייה, לרבות מסקנות לשיפור.

אבטחת מחשבי הקצה מהן מבוצעת גישה מרחוק לרשת העירייה

- הביקורת בדקה את נאותות אבטחת המידע במחשבי הקצה מהן מבוצעת גישה מרחוק, בהתייחס לחוק, לתקנות ולהנחיות שפורסמו.
- הגישה מרחוק בעירייה מתאפשרת משני סוגי מחשבי קצה - מחשבים ניידים שחולקו על ידי העירייה, ומחשבים ביתיים של עובדים אשר עברו הקשחה³⁴ על ידי מחלקת מערכות מידע. בביקורת בוצעה בדיקה מקצועית במחשב הנייד של מבקרת העירייה, ובמחשב נייד נוסף השייך לעובד במינהל ההנדסה, ולהלן תוצאותיה:
1. במחשב הנייד של מבקרת העירייה, מותקנת גרסה לתוכנת נוגד נגיפים מקצועית בגרסה כמעט אחרונה (קיימת גרסה עדכנית יותר). בבדיקת המחשב נמצא, כי ניתן לשנות את הגדרות התוכנה ואף להסירה לחלוטין. במחשב הנוסף, לא ניתן היה לבטל את התוכנה.

³³ **יתירות** – עודף/כפילות, כגון כפילות של רכיבים במערכות שנועדה למנוע קריסה במקרה כשל באחד מהם.

³⁴ **הקשחה** (באנגלית **Hardening**): תהליך של אבטחת המערכת על ידי הקטנת שטח הפגיעות אשר גדלה ככל שהמערכת מבצעת יותר פעולות. הקטנת אפשרות תקיפת המערכת לרוב כוללת שינוי סיסמאות ברירת מחדל, הסרה של תוכנה מיותרת או התחברויות מקודדות (login) והסרה של שירותים מיותרים.

2. במחשב הנייד של מבקרת העירייה, מותקנת מערכת הפעלה מסדרת Windows 10 המעודכנת לתאריך 12/01/2020. במחשב הנייד הנוסף שנבדק, אותה מערכת ההפעלה מעודכנת לתאריך 24/03/2020. יצויין, כי בחודשים פברואר ועד מאי 2020 פורסמו עדכוני אבטחה חודשיים, אשר לא עודכנו במחשבים שנבדקו.
 3. חשבון המשתמש במחשב הנייד של מבקרת העירייה, מוגדר כבעל הרשאת "מנהל מקומי" המאפשרת למשתמש הקצה לבצע שינויים בהגדרות המחשב, להתקין בו יישומים ללא אישור צוות המחשוב העירוני, ומקלה מאוד על נזקות זדוניות לפעול במחשב בסתר, ללא ידיעת משתמש הקצה. במחשב הנייד הנוסף, לא הייתה הרשאת "מנהל מקומי".
 - יתר על כן, נמצא כי מנגנון Windows PowerShell³⁵ המאפשר להריץ פקודות רגישות במחשב, אינו חסום למשתמשי הקצה בשני המחשבים הניידים שנבדקו.
 4. מתאפשרת שמירה של קבצי עבודה בכונן המקומי במחשבים הניידים, בכלל זה, שמירה של מידע רגיש (כגון מידע אישי ופיננסי של תושבי העיר ועובדיה). נמצא, כי הכוננים הקשיחים של שני המחשבים הניידים אינם מוצפנים. יודגש בזאת, כי במקרה של אובדן, או של גניבת מחשב נייד בעל כונן קשיח שאינו מוצפן על ידי גורם זדוני, ניתן בקלות יתרה לחבר את הכונן הקשיח של המחשב הנייד למחשב אחר, ולהיחשף למידע הרגיש מתוכו.
 - לביקורת נמסר בתגובה, כי נרכש פתרון הצפנה מתאים אשר יוטמע בקרוב.
 5. בשני המחשבים הניידים, לא מיושמת חסימה לחיבור התקני זיכרון חיצוניים ניידים בעלי יציאות אפיק טורי אוניברסלי (USB)³⁶ ולהעתקת חומרים מהתקן החיצוני ואילו. לפיכך במצב זה, מוגברת החשיפה לזליגת מידע מהעירייה ולחדירת נזקות דרך התקנים חיצוניים.
 6. בשני המחשבים הניידים שנבדקו, לא מופעלת מערכת "חומת אש" אישית. רצוי להפעיל מערכת זו, במצב בו המחשב הנייד אינו מחובר לרשת העירייה אלא מחובר לרשת חיצונית (כגון רשת Wi-Fi בבית העובד).
 7. קיימים סוגים רבים של נזקות כגון: תכנת מחשב מזיקה מסוג "סוס טרויאני" החודרת למחשב תוך התחזות לתוכנה תמימה, והמאפשרת לגורמים זדוניים לצפות במתרחש במסך המחשב, להפעיל מצלמה, להקליט, להזיז עכבר וללחוץ על מסכי מערכות. נזקה מסוג "רישום הקשות" (Keylogger) מזהה ומתעדת כל הקשה במקלדת ובעכבר, בהן סיסמאות ונתונים רגישים בזמן החיבור מרחוק לרשת הארגונית.
- א. במסגרת סימולציית השתלטות על המחשב הנייד של מבקרת העירייה, תוך ניצול העובדה שניתן לבטל את תוכנת נוגד נגיפים בו, צלחה הרצת קובץ המזדמה נזקה, המאפשר שליטה מרוחקת והרצת פקודות ממחשב הבדיקה.**
- ב. בדומה להשתלטות על המחשב הנייד של מבקרת העירייה, ניתן לדוגמא לבצע השתלטות על המחשב הנייד של מנהלת החשבונות, בעלת הרשאת גישה לאתרי הבנקים. באופן דומה, יכל גורם זדוני לגנוב את סיסמאות הגישה לחשבונות הבנקים של העירייה, ובשימוש בהרשאתה של העובדת וללא ידיעתה, לבצע העברת כספים לחשבונות בנק יעודים, או לבצע שינוי במספר חשבון הבנק של ספק עירוני, כך שתשלומים בסך של מיליוני שקלים המיועדים לספק, יועברו בפועל לחשבון הבנק שבשליטת הגורם הזדוני.

³⁵ Windows PowerShell - שמה של סביבת עבודה לאוטומטיזציה של משימות של חברת מיקרוסופט, המכילה ממשק שורת פקודה ושפת תסריט, ומאפשרת כלי ניהול במערכות Windows מקומיות ומרוחקות.

³⁶ USB ראשי תיבות של Universal Serial Bus בעברית: אפיק טורי אוניברסלי-תקן לחיבור בין מחשבים להתקני ציוד היקפי.

יודגש, כי הסיכוי למתקפות סייבר גובר משמעותית, במצב בו מחשבים ניידים השייכים לעירייה נמצאים בביתם של העובדים, ואינם מוגנים דרך הרשת הארגונית. העדר הקשחת אבטחה נאותה במחשבים הניידים, עשוי להפוך מידע רגיש וחסוי, ל"טרף קל" עבור גורמים זדוניים, העלולים לעשות בו שימוש אף כדי המשך המתקפות כנגד העירייה.

להלן המלצות הביקורת:

- יש ליישם בהקדם, מדיניות אבטחה והקשחה אחידה בכלל המחשבים הניידים העירוניים מהם מבוצעת גישה מרחוק, תוך התקנה של רכיבי האבטחה הנדרשים והפעלת הצפנה של הכונן הקשיח המקומי. יתר על כן, יש לבצע עדכוני אבטחה שוטפים, חסימה של חיבורי מדיה נתיקה למחשבים הניידים, ביטול הרשאות "מנהל מקומי" למשתמשי הקצה, הפעלת מערכת "חומת אש" אישית וביצוע הקשחות אבטחה נוספות, והכל בהתאם להנחיות מערך הסייבר הלאומי והרשות להגנת הפרטיות.
- יש להגדיר בהקדם בכלל המחשבים ניידים, חסימת גישה לשינוי ההגדרות בתוכנת נוגד נגיפים באמצעות סיסמת ניהול, הגלויה לצוות מערכות המידע בלבד.
- יש לאפשר שימוש בהתקני זיכרון ניידים ייעודים לצורכי עבודה השייכים לעירייה בלבד ואשר עברו הלבנה³⁷, ולהגדיר חיבור של התקן מוגדר בעל מספר סידורי לכל מחשב מאושר.
- יש לשדרג את גרסת תוכנת נוגד נגיפים לגרסה העדכנית ביותר.

אבטחת גישה מרחוק לרשת הפנימית, לדוא"ל הארגוני של העירייה ולמערכותיה

עקב משבר נגיף הקורונה, העירייה כבגופים רבים, נאלצה להעביר את מרבית עובדיה אשר לא הוצאו לחל"ת, לעבודה מרוחקת מבתיים. גם בעתות שגרה, מאפשרת העירייה לחלק מעובדיה לעבוד מרחוק. לשם חיבור מאובטח ומוצפן, נעזרת העירייה ברשת פרטית וירטואלית (VPN) לגישה ממחשב מרוחק אל משאבי הרשת הארגונית הפנימית דרך המרשתת. בנוסף, נעזרת העירייה בממשק גישה מרחוק דרך דפדפן OWA לדוא"ל הארגוני המסופק על ידי חברה לאוטומציה.

- בהתאם לסעיף 14(ג) בתקנות הדן באבטחת תקשורת, 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 ברמת אבטחה בינונית וגבוהה, ייעשה שימוש באמצעי פיזי הנתון לשיטתו הבלעדית של בעל ההרשאה.
- בהנחיות לעבודה מאובטחת מהבית מטעם מערך הסייבר הלאומי ומטעם הרשות להגנת הפרטיות, הדנו בין היתר בהזדהות בגישה מרחוק נקבעו החובות: להתקין רשת וירטואלית פרטית להתחברות מאובטחת בין העובדים לבין משאבי הארגון וכן הפעלת אימות רב גורמי, המהווה מנגנון הזדהות קשיח בכניסה לרשת; להגדיר סיסמת אבטחה מוקשחת; לאכוף אפשרויות העתקה ושמירת מידע רגיש במכשיר הביתי; להגדיר חובת ניתוק וחיבור לאחר פרק זמן של חוסר פעילות בגישה מרחוק; לבטל אפשרות לעבודה עם תוכנות השתלטות מרחוק.

³⁷ הלבנה - תהליך טכנולוגי מתקדם למניעת תוכנות זדוניות באמצעות ביצוע סריקת קבצים ופירוק תוכנות זדוניות עוד לפני כניסתם לרשת הארגונית. תהליך הלבנה אורך שניות בודדות ומנטרל לחלוטין את האיום של החדרת נזקה לארגון.

3. נמצא, כי שיטת ההזדהות בעת הגישה מרחוק של העובדים דרך ממשק VPN, מבוססת על מנגנון סיסמאות קבוע שאינו מתחלף בסיום השימוש, וזאת בניגוד לנדרש בתקנות, בהנחיות מערך הסייבר הלאומי ובהנחיות הרשות להגנת הפרטיות. השימוש המקובל, הינו במנגנון חילול סיסמאות חד פעמי (לדוגמא בדמות ממסר המתקבל בטלפון הנייד של עובד והנתון לשליטתו הבלעדית, או ביישום המחולל סיסמא חד פעמית המותקנת בטלפון הנייד של העובד).
4. הגישה מרחוק לשירות הדוא"ל הארגוני בממשק OWA מחייבת הזנת סיסמא של המשתמש. סיסמא זו קבועה (ומשתנה בתדירות של כל 90 יום) וניתנת לניחוש מושכל, לחשיפה במסגרת תרגיל דיג ולגניבה במידה ומבוצעת גישה ממחשב בלתי מאובטח שקיימת בו נוזקה. במהלך בדיקה בתיאום עם החברה לאוטומציה, נעשה ניסיון לבצע תקיפה כוחנית (Brute Force) על מנת לנחש את סיסמת המשתמש, באמצעות בדיקה של מדגם חשבונות וסיסמאות אפשריים, סבירים או נפוצים. בביקורת נמצא, כי לא ניתן היה לנחש את הסיסמאות, וכן זוהה, כי קיימת הגנה מסוימת המגבילה את הבדיקה. בהינתן חוסר מגבלת של זמן, יוכלו גורמים זדוניים לבצע בדיקה שקטה על כלל החשבונות בעירייה ותרגילי דיג, להשגת סיסמאות מעובדים במרמה והתחזות, לתקוף מחשבי קצה של עובדים בביתם ולדלות משם הסיסמאות.
5. לא מיושמת חסימה להעתקת קבצים בין כונני הרשת, לבין מחשב פרטי ממנו מבוצעת גישה מרחוק על ידי העובד. כמו גם, לא מיושמת חסימה גורפת לאפשרות של העתקת טקסט (Clipboard)³⁸ בין המחשב הפרטי לבין המחשב המרוחק. אין עוררין, כי נוזקות מסוימות במחשב הפרטי עלולות להתפשט גם לרשת הארגונית.
6. לעובדים מתאפשרת אף גישה ישירה ומסוכנת יותר, ממחשבם הפרטי בבית למחשב העובד בעבודה, וזאת בניגוד להנחיות מערך הסייבר הלאומי. גישה מאובטחת יותר, הינה על ידי שימוש והתחברות דרך ממשק כגון שרת טרמינל (Terminal Service). השרת אינו מאפשר גישה ישירה למחשבי העירייה ומשאביה, ומתיר רמת מידור גבוהה בחשיפה ליישומים ותיקיות מוגדרות בהתאם להרשאות שהוגדרו מראש. השרת מהווה סביבת עבודה אחידה וקשיחה למשתמשים, ומסייעת במניעת פגיעה בזדון או בשוגג.
7. לא מיושמת הגנה כנגד מתקפת מניעת שירות מבוזרת (DDOS)³⁹ על ממשק ה-VPN. תקיפה זו מרחוק בידי גורם זדוני, נועדה להשבית את מערכת המחשב על ידי יצירת עומס חריג על הממשק, ועשויה למנוע בכך ממשתמשים מורשים גישה למשאב מחשב מסוים, להאט את שירות הממשק ואף לגרום לקריסה בשירות. בתקופת משבר נגיף הקורונה, עשוי הדבר לפגוע בפעילות העירייה לאור התלות בעבודה מרחוק.
8. מטרת בדיקת תאימות אבטחה (Compliance Security) הינה לוודא, כי מחשב הקצה ממנו מבוצע החיבור מרחוק, אינו מסכן את הרשת הארגונית יתר על המידה. הבדיקה מעלה בין היתר, אם במחשב הקצה מותקנת תוכנת נוגד נגיפים מעודכנת, עדכוני אבטחה נדרשים ועוד,

³⁸ **Clipboard**: בתרגום חופשי: לוח העתקה או לוח עריכה - חלק בזיכרון המחשב בו מאוחסנים נתונים באופן זמני. לוח העריכה מאפשר למשתמשים להעביר ("לגזור") או להעתיק מידע (טקסט, תמונה, קובץ ועוד) מתוכנית אחת הפועלת במחשב באותה עת לתוכנית אחרת הפועלת בו (וכן מתוכנית אל עצמה), או מתיקייה אחת לתיקייה אחרת (להעביר למיקום שונה במערכת הקבצים).

³⁹ **Distributed Denial-Of-Service attack - DDoS**

כמפורט בהנחיות מערך הסייבר הלאומי. רק במקרה ומחשב הקצה עומד ברף התאימות שנקבע בארגון, יתאפשר החיבור מרחוק.

בביקורת נמצא, כי התחברות מרחוק לרשת המחשוב העירונית ע"י העובדים, מתאפשרת מבלי שנבדקים מנגנוני האבטחה הנדרשים.

9. עוד נמצא, כי לא מיושמת חסימה למניעת גישה לממשקי VPN ו- OWA ממדינות מסוימות ובין היתר, מתאפשרת גישה ממדינות ערב כמו מצרים.

10. נעילת המסך במחשבי העירייה מוגדרת לאחר 15 דקות של חוסר בפעילות. יחד עם זאת, לא מוגדר זמן ניתוק התקשורת מהמערכת עקב חוסר פעילות בממשק ה- VPN. הביקורת מתריעה על הסיכון שבהשארת ערוץ תקשורת פתוח.

11. עם הצורך הגובר בקיום פגישות ותקשורת מרחוק, אחת הפלטפורמות שזוכה עתה לפופולריות משמעותית היא אפליקציית Zoom⁴⁰. באפריל 2020 הוציאה ה- FBI התרעה מפני גידול בהיקף הפריצות לפלטפורמות שיתופיות לשיחות וידיאו, שהוא כינה "הפצצת זום (Zoom-bombing)" "על רקע ריבוי השימוש בטכנולוגיות אלו בשל מגיפת הקורונה. הצטרפות בלתי מאושרת של משתתפים שמוצאים את קישורים לשיבות בזום מנצלים זאת כדי לחדור אליהן בזדון מרחוק. **בביקורת נמצא מקרה, בו הותרה הצטרפותו של תושב העיר לישיבה בזום של ועדת משנה לתכנון וסביבה מבלי שהיה בין מוזמניה. יודגש בזאת, כי כפי הנראה הזימון לישיבה נשלח לתושב על ידי אחד המוזמנים. לא למותר לציין ולהדגיש, את הסיכונים שבהשתתפות גורמים בעלי עניין החיצוניים לעירייה בישיבות פנים עירוניות.**

יצוין לחיוב, כי מנהל מערכות מידע הוציא לעובדי העירייה באופן מידי ריענון בנושא.

12. להלן המלצות הביקורת:

א. יש להטמיע מנגנון הזדהות חזק בגישה מרחוק לכלל הממשקים, בתצורת אימות דו שלבי.
ב. יש ליישם מנגנוני מידור נאותים בין מחשבי הקצה מהן מבוצע החיבור מרחוק לבין המשאבים של הרשת הארגונית, לרבות, ביטול האפשרות להעתיק קבצים וכן שימוש בשרת טרמינל.

ג. יש ליישם בדיקת תאימות אבטחה למחשבי הקצה מהם מתבצע חיבור מרחוק לרשת הארגונית, תוך הגדרת רף מזערי סביר לרמת האבטחה בהם (כגון: בדיקת קיום נוגד נגיפים תקף ומעודכן, קיום גרסאות אבטחה עדכניות ביותר ועוד). מחשבים אשר לא יעמדו ברמת האבטחה הקבילה, לא תתאפשר התחברותם לרשת הארגונית.

ד. בזמני משבר קיצוניים או מתקפות סייבר גלובאליות לכל הפחות, יש להגביל את הגישה מרחוק למשאבי העירייה (OWA, VPN ועוד) רק מכתובות IP בתוך מדינת ישראל. כל או אחרת, יש לבצע חסימה גיאוגרפית לגישה ממדינות עוינות.

ה. יש להגדיר מנגנון ניתוק עקב חוסר פעילות בממשקי VPN ו- OWA.

ו. יש לשקול הפעלה של מנגנון הגנה כנגד מתקפת מניעת שירות מבוזרת (Anti DDOS) לממשק ה- VPN.

⁴⁰ Zoom - באפליקציה המאפשרת ביצוע של שיחות ועידה בווידיאו וניהול תקשורת עם ריבוי משתמשים.

מבדק סימולציית דיוג (Fishing)

עקב מעבר לעבודה מרחוק בשל משבר נגיף הקורונה, הוגברו המתקפות כנגד חברות ישראליות על רקע המשבר לשם השגת גישה לרשת הארגונית, ובעיקר הוגברו מתקפות הדיוג; הוקמו אתרי הונאות; הופעלו יישומים זדוניים והופצו כופרות במטרה של מסמכים לגיטימיים לכאורה הנושאים את שם הנגיף. כמו גם, זוהו מתקפות דיוג טלפוניות⁴¹, בהן גורם זדוני מתקשר לעובד ומתחזה במטרה לקבל גישה לסיסמאות המחשב, ומשם לתכולתו ולמערכות המחשב העירונית.

1. **בתיאום עם מנהל מערכות מידע ובאישורי, בוצעה התקשרות טלפונית למספר עובדים. לאחר שהביקורת הציגה עצמה כחברה לתמיכת מחשוב חיצונית העובדת בשיתוף עם מנהל מערכות המידע בעירייה, נדרש מהעובד שענה לשיחה להעניק גישה למחשבו הנייד לשם בדיקת תקלה לכאורה. יצויין בזאת כדלקמן:**

- א. העובד אפשר לביקורת להפעיל במחשבו תכנה לשליטה מרחוק⁴².
- ב. במהלך הבדיקה, נמצא קובץ על שולחן העבודה במחשבו של העובד, שכלל סיסמת גישה לממשק VPN אשר נשמרה באופן גלוי.

2. **להלן המלצות הביקורת לאור ממצאי הבדיקה:**

- א. על העירייה לאמץ את הנחיות מערך הסייבר הלאומי והנחיות הרשות להגנת הפרטיות, בנושא ההתמודדות עם מתקפות דיוג (Fishing).
- ב. יש לערוך ריענון לכלל עובדי העירייה בנושא מתקפות דיוג, תוך פירוט דבר ביצוע בדיקת הביקורת. יש לחדד בפני העובדים את האיסור במתן גישה או מסירת פרטים לגורמים כאלו ואחרים, ללא קבלת אישורו של מנהל מערכות המידע בעירייה.
- ג. יש לבחון ביצוע הקשחה בכלל מחשבי העירייה, לשם מניעה של התקנת תוכנות שליטה מרחוק בהם, ללא אישורו של מנהל מערכות המידע.

סיכום

העירייה משתמשת בטכנולוגיות מידע ותקשורת לשיפור ניהול נכסיה ואיכות החיים של תושביה. מגמה זו, מביאה לגידול חד בכמות הנתונים שבידה ובמספר מאגרי המידע שבבעלותה המשמשים בסיס לעבודתה בעתות רגיעה וחירום, לרבות בתחומי: כספים, תכנון ובנייה, חינוך, רווחה, כוח אדם, רישוי, תחבורה וחניה, תברואה, עיר חכמה ועוד. פגיעה במערכות הממוחשבות ובמאגרי המידע של העירייה, עלולה לגרום לנזקים כבדים, כמו פגיעה בשירותים הניתנים לתושב ובדליפת מידע הפוגעת בצנעת הפרט, ומשכך, מוטלת על העירייה החובה להגן על המידע ולהגביר את חסינותה לצורך הגנה על רציפותה התפקודית לטובת השירות לציבור.

להלן עיקר ממצאי הביקורת אשר נערכה בחודשים אפריל – יולי 2020 והעריכה באופן מדגמי את הסיכונים הפוטנציאליים והכשלים החושפים את מערכות המידע של העירייה לפגיעה או לדליף מידע, בשל מתקפות סייבר בעתות שגרה וחירום, ובהסתמך על דרישות הרגולציה.

1. **רישום מאגרים, הגדרות מאגרים וממשל תאגידי בהיבטי אבטחת מידע - טרם נכתבו מסמכי הגדרות למאגרי המידע בעירייה, וכן לא נבחנה כמות המידע הנשמר בהם באם רב מן הנדרש**

⁴¹ **Vishing (Voice Phishing)** - וקטור תקיפה כנגד הגורם האנושי דרך הטלפון. הונאת הנדסה חברתית בה מנסים האקרים לגרום לקורבן לגלות פרטים אישיים/פיננסיים באמצעות שיחות טלפון זדוניות.

⁴² AnyDesk - תוכנת שליטה מרחוק המקשרת בין המחשב למחשב אחר, במטרה לספק שירותי תמיכה, ביצוע התקנה, או מתן שירות מרחוק ובאופן לא פיזי.

- למטרותיהם; בניגוד לתקנות מנהל מערכות מידע משמש במקביל כממונה על אבטחת מידע, מפקח על פעולותיו שלו ושל עובדיו בגין העמידה בדרישות התקנות, ומעלה בכך חשש לקיומו של ניגוד עניינים; תכנית עבודה למערכות מידע לשנת 2020 אינה עומדת בכל דרישות התקנות; נושאי אבטחת מידע והגנת הפרטיות אינם מנוהלים באמצעות ועדת היגוי; נהלי אבטחת מידע לא עברו תהליך אשרור ועדכון החל משנת 2018.
2. הדרכות עובדים ומדיניות בקרת גלישה במרשתת – לא כל עובדי העירייה הנדרשים, חתומים על טופס הצהרה לקיום סודיות וכללי אבטחת מידע; מדיניות הגלישה במרשתת אינה מגבילה באופן מספק, ולא מיושמת חסימה של חלק מקטגוריות ברות סיכון;
3. ניהול משתמשים והרשאות במערכות המחשוב - לא מיושם תהליך תקופתי של תיקוף הרשאות גישה קיימות לכלל המשתמשים ולכלל המאגרים; נמצאו עובדים לשעבר, להם עדיין הייתה קיימת סיסמא והרשאה למאגרים רגישים, חודשים לאחר סיום העסקתם; חמור מכך נמצא, כי עובדת במחלקה לשירותים חברתיים, ביצעה שימוש אישי פסול מיסודו במידע חסוי ורגיש, תוך ניצול החשיפה לנתונים שאינם תחת טיפולה במאגר מידע לו היא מורשית, ובעת תשאולה טענה דברי כזב. במכלול הנסיבות כמתואר, עברה העובדת על הוראות החוק והפרה את חובת אמונה כלפי העירייה שלא בתום לב. יודגש, כי העובדת הושעתה מעבודתה; לא בוצע ריענון של נוהלי אבטחת מידע בקרב עובדי הרווחה, ולא בוצעו בדיקות אקראיות באשר לביצוע שמירת אבטחת המידע במחלקה לשירותים חברתיים כנדרש.
4. איתור, דיווח ותגובה לאירועי אבטחת מידע – מדיניות התגובה לאירועי אבטחת מידע אינה עונה על הדרישות: לא נרכשה מערכת ניטור; לא מתקיים דיון שנתי בגין אירועי אבטחת מידע; אין מידע בגין רמת הניטור המיושמת בחברה לאוטומציה לאחר אירועי אבטחת מידע, ולא ידוע מהם שירותי האבטחה ומערכות הליבה המסופקות על ידה; לא מוגדרת מערכת התרעה אוטומטית בעת אירוע גילוי נגיף במחשבים הניידים מהם מבוצעת גישה מרחוק. ממצא זה תוקן במהלך הביקורת; הגדרות בקרה על תוכנת מדיניות קבוצתית אינן מופעלות, ומשך אירועים רגישים נוספים בשרתי ניהול הרשת הארגונית, אינם מתועדים.
5. התקנים ניידים ואבטחת מכשירי טלפון נייד ומחשבי לוח-קיימת חשיפה רבה להחדרת נזקה שלא תזוהה על ידי נוגד נגיפים ולזליגת מידע רגיש: 40 משתמשים מורשים לחבר מדיה נתיקה למחשביהם ללא קיום מנגנון סינון לשימוש בהתקנים מאושרים; לא מוטמעות טכנולוגיות רבות: הצפנת נתונים במדיה נתיקה; מניעת דלף מידע רגיש בעת העתקת נתונים מהמחשב/מהרשת למדיה נתיקה; חסימת גישת בלתי מורשים אל רשת המחשוב הפנים עירונית ולטלפונים הניידים ומחשבי הלוח בהם מיושמות הגדרות אבטחה בסיסיות ועוד.
6. שימוש במערכות הפעלה מעודכנות, הפרדת מערכות המאגרים ואבטחתם הפיזית – בניגוד לתקנות: חסרים עדכוני אבטחה במערכות הפעלה ובתוספי תכולה לתוכנות הקיימות; קיים שימוש במערכות הפעלה ישנות ללא תמיכת יצרן; לא מיושמת הפרדה בין מערכות מאגרי המידע לבין מערכות מחשוב אחרות באמצעות מערכת ניטור וחסימת התקשרויות בלתי רצויות; לא קיימים אמצעים לבקרה, לתיעוד ולגיבוי נתוני כניסה ויציאה מחדר השרתים בו מצויות מערכות תשתיות, חומרה וסוגי רכיבי תקשורת, וכן של הכנסה והוצאה של ציוד ממנו;
7. קיום הגנה אפקטיבית כנגד מתקפות – לשם השגת יכולת נאותה להתמודדות עם מתקפות סייבר, הביקורת סבורה, כי קיים מקום להוסיף שכבות הגנה נוספות (מודולים, הגדרות וטכנולוגיות מתקדמות) כפי שפורטו למנהל מערכות מידע.

8. חולשות אבטחה בכתובות חיצוניות של העירייה הנגישות למרשתת ולדוא"ל – על אף ההגנות הקיימות, אתר המרשתת העירוני חשוף למתקפות סייבר; נמצאו חולשות אבטחה בממשק גישה מרחוק לדוא"ל הארגוני; שירות חסימה אל שרתי העירייה על בסיס מיקום גיאוגרפי אינו מופעל, וקיימים ממשקים הפתוחים גלובלית; אפקטיביות סינון וחסימה של קבלת דוא"ל זדוני בצירוף נוזקות אל שרתי העירייה לוקה בחסר.
9. מיקור חוץ - הליך ניהול סיכוני אבטחת מידע עבור ספקי מיקור חוץ לשירותי מחשוב לוקה בחסר: לא נדרשים נתונים בגין עמידתם בהוראות התקנות ואבטחת מידע, ולא נערכת בדיקה לעמידותם בהם; ספקי החוץ אינם חתומים על נוהל דרישות אבטחת מידע, והחוזים עימם אינם כוללים פירוט בגין סיכוני אבטח מידע הכרוכים בהתקשרות כנדרש בתקנות.
10. הערכה וניהול סיכוני סייבר במעבר לעבודה בחירום במשבר נגיף הקורונה – תוכנית עירונית להתאוששות מאסון אינה כוללת התייחסות מפורשת לאירוע מגפה, כמו גם לאירוע סייבר, כאירועים העלולים להשבית את פעילות העירייה, וכן לא בוצע תרגול להתמודדות עם אירועים אלו; תוצאות תרגולי החירום שכן בוצעו לא תועדו; סקר הסיכונים שנערך בשנת 2018 לא כלל בחינה של הסיכונים ברשת המחשוב החיצונית, ומשכך, לא בוצע מבדק חדירה לרשת והקשחה של ממשקי הגישה מרחוק; בוצע הליך חלקי להערכת סיכוני סייבר, ולא הוגדרה תכנית עבודה לניהול סיכוני סייבר בגין עבודה בחירום במשבר נגיף הקורונה;
11. אבטחת מחשבי הקצה מהן מבוצעת גישה מרחוק לרשת העירייה – ממצאי בדיקה מקצועית שבוצעה במחשב הנייד של מבקרת העירייה ובמחשב נייד נוסף, העלתה רמת חשיפה גבוהה לזליגת מידע מהעירייה מהם, לחדירת נוזקות ולשליטה בהם מרחוק כפי שהתאפשר בפועל.
12. אבטחת גישה מרחוק לרשת הפנימית, לדוא"ל העירוני ולמערכותיה - מנגנון הסיסמאות כהזדהות בעת הגישה מרחוק במחשבי העובדים, אינו מתחלף בתום השימוש בניגוד לנדרש; לא מיושמת חסימה להעתקת קבצים בין כונוני הרשת לבין מחשב פרטי ממנו מבוצעת גישה מרחוק, ובין מחשב פרטי לבין מחשב מרוחק, כך שנוזקות מהמחשב הפרטי עלולות להתפשט גם לרשת הארגונית; בניגוד להנחיות לעובדים מתאפשרת גישה ישירה ומסוכנת ממחשבם הפרטי בבית, למחשב בעבודה; לא מיושמת הגנה כנגד מתקפה שנועדה להשבית את מערכת המחשוב; התחברות מרחוק מתאפשרת מבלי שנבדקים מנגנוני האבטחה הנדרשים; לא מופעל שירות חסימה אל ממשקי הגישה מרחוק על בסיס מיקום גיאוגרפי, וקיימים ממשקים הפתוחים גלובלית; קיים סיכון בהשאת ערוץ תקשורת פתוח, בעוד לא מוגדר זמן ניתוק התקשורת מהמערכת עקב חוסר פעילות מרחוק; בביקורת נמצא מקרה, בו הותרה בקשת הצטרפותו של תושב העיר לישיבת ועדה בזום, זאת מבלי שהיה בין מוזמניה.
13. מבדק סימולצית דיג (Fishing) – בתיאום ובאישור מנהל מערכות מידע, בוצע הליך הונאתי על ידי התקשרות טלפונית, באמצעותה עובד עירייה אפשר לביקורת להפעיל במחשבו הנייד תוכנה לשליטה מרחוק, דרכה ניתן היה לדלות נתונים חסויים, אישיים ופיננסיים מהמחשב ומרשתת המחשוב העירונית.

על העירייה לפעול בתכנית מוסדרת לתיקון הממצאים שהועלו בדוח בנוגע לפעולותיה בתחום אבטחת המידע והגנת הפרטיות בהתאם להמלצות, לפעול להעלאת המודעות בקרב עובדיה לחשיבות הנושא ולהעמיד לרשות העובדים את האמצעים למילוי חובותיהם בתחום זה.