אבטחת מידע והגנת הפרטיות

מבוא

1. בעירייה פועלות מערכות מידע ממוחשבות רבות החיוניות להבטחת תקינות פעילותה השוטפת. 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 ומערכי המידע.
2. המחוקק נתן דעתו להיבטים שונים של אבטחת מידע, והדבר בא לידי ביטוי בחוק הגנת הפרטיות, התשמ"א-1981 (להלן - **חוק**) ובחוק המחשבים, התשנ"ה-1995.
3. 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."

מנהל מאגר - **"מנהל פעיל של גוף שבבעלותו או בהחזקתו מאגר מידע או מי שמנהל כאמור הסמיכו לעניין זה."**

שלמות מידע - **"זהות הנתונים במאגר מידע למקור שממנו נשאבו, בלא ששונו, נמסרו או הושמדו ללא רשות כדין."**

4. בדוח מבקר המדינה מספר 62 לשנת 2011 בנושא "אבטחת מידע והגנת הפרטיות ברשויות מקומיות" נאמר בין היתר:

"במשך שנים לא קבע משרד הפנים מדיניות לאבטחת המידע ולהגנת הפרטיות ברשויות המקומיות; לא הניח את התשתית לטיפול בנושא; ולא פעל לקביעת הנחיות בתחום זה, אף שכבר בשנת 1996 תוקן חוק הגנת הפרטיות ונוספו לו סעיפים הנוגעים להגנה על הפרטיות במאגרי מידע.

"הרשות למשפט, טכנולוגיה ומידע שבמשרד המשפטים לא קיימה מאז הקמתה פעולות פיקוח ואכיפה על רישום מאגרי מידע. כמו כן היא לא קבעה נהלים והנחיות ולא הטילה קנסות על רשויות מקומיות שלא קיימו את חובתן זו."

5. האגף הבכיר לביקורת המדינה במשרד ראש הממשלה פרסם בספטמבר 2005 "נוהל מסגרת לאבטחת מידע" הכולל 38 נהלים לאבטחת מידע במשרדי הממשלה, העוסקים בנושאים, כגון: קביעת מדיניות ומיפוי מידע; הגורם האנושי ואבטחת המידע; אבטחה לוגית; אבטחה פיזית; גיבוי, שחזור והתאוששות; אבטחת תקשורת ושימושי אינטרנט;

אבטחת מידע במחשבים המנותקים מרשתות המשרד (להלן יחד - **נוהלי המסגרת**).
בהתייחסות לנוהל בודד יכונה הנוהל לפי מספרו בנוהל המסגרת).
לפי נוהלי המסגרת, על תחום אבטחת מידע בגוף ציבורי יהיה מופקד "הממונה על אבטחת מידע", ובאחריותו לבקר את הפעילויות הממוחשבות כדי לוודא שהמשרד עומד בדרישות אבטחת המידע שמקורן בחוקים, בתקנות ובנהלים. נהלים אלו אמנם אינם מחייבים את הרשויות המקומיות, אולם לדברי אחראית ביקורת אבטחת מידע במשרד ראש הממשלה (שיחה טלפונית שנערכה ב-5.11.14), יש בה כדי ללמד על התשתית הדרושה לאבטחת המידע ולשמירה על הפרטיות בגופים ציבוריים. לפי המבוא לנוהלי המסגרת, יש לשאוף כי **"נוהלי המסגרת יהיו לנגד עיני המשרדים במהלך קביעת הנהלים המחייבים"**.

6. לעירייה שני נהלים בנושאי אבטחת מידע:

- נוהל בנושא "אבטחת מידע בעירייה" שעודכן לאחרונה בנובמבר 2008 (מספר 0402-32) (להלן - **נוהל עירוני לאבטחת מידע**).
- נוהל בנושא "אבטחת חומרה ותוכנה" שעודכן לאחרונה ביולי 2011 (מספר 0403-32) (להלן - **נוהל עירוני לאבטחת חומרה ותוכנה**).

(שני הנהלים ביחד להלן - **נוהלי העירייה**)

עבודת הביקורת

1. מטרת הביקורת הייתה לבחון את נושא אבטחת המידע וההגנה על הפרטיות במערכות המחשוב העירוניות.
2. נושא הביקורת נבחר גם בהתאם להנחיה בנוהל מספר 1 לנוהלי המסגרת בנושא "קביעת מדיניות אבטחת 'מידע רגיש' ומערכי מידע בממשלה ומוסדותיה": **"בפעילות השנתית של יחידת הביקורת הפנימית יש לכלול גם עריכת ביקורת על נושאים בתחום הפיתוח, הניהול, התפעול, התחזוקה והאבטחה של מערכי המידע, השליטה והבקרה הטכנולוגיות, בהיקף שיהיה תואם את הרגישות המרבית של המידע המעובד במערכות, את פרישת מערכי המידע, ואת מורכבותם. פעילות הביקורת תקבל תקציב ראוי.**
"קדימות רבה תינתן לבחינת מערכי המידע והפעילויות הממוחשבות שנמסרו לביצוע על ידי ספק 'מיקור-חוץ' (outsourcing**)."**
3. הביקורת כללה, בין היתר, את הפעולות הבאות:

א. פגישות עם מנהל אגף התקשוב העירוני (להלן - **מנהל האגף**) ועם מנהלת מרכז מידע ומחקר ואתר האינטרנט העירוני.

ב. עיון בדוחות מהמערכת הממוחשבת העירונית ובמסמכים רלוונטיים.

ג. סיור בחדר שרתים הממוקם בבניין העירייה.

ד. ניסיונות כניסה למערכת הממוחשבת.

ה. עיון במסמכים רלוונטיים.

4. הנושא נבדק בעבר ופורסם בדוח ביקורת מספר 28 משנת 2007 בנושא "שירות ואבטחת מידע במערך המחשוב בעירייה" (להלן - **דוח 28**).

לנושאים שנכללו בביקורת הקודמת ונבדקו גם במסגרת הביקורת הנוכחית ניתנה התייחסות בגוף הדוח.

5. הביקורת בוצעה בידי יועצים חיצוניים[1].
6. איסוף ממצאי הביקורת נערך בחודשים יוני עד נובמבר 2014.
7. טיוטות הממצאים הועברו להתייחסות המבוקרים.

לדברי מנהל האגף, עד למועד תחילת עבודת חברה חיצונית מייעצת בתחום אבטחת מידע (להלן - **החברה המייעצת**) (אפריל 2012) לא היו בעירייה אמצעים משמעותיים לאבטחת מידע. משגילה זאת ולצורך מתן מענה ראשוני ומידי, נרכשו והוטמעו מערכות מתקדמות לאבטחת מידע, אולם חלק ניכר מהנהלים והאמצעים הנדרשים טרם יושמו.
הביקורת מודה למנהל האגף על שיתוף הפעולה וסיועו הרב במהלך עבודת הביקורת.

ממצאים

1. מדיניות ונוהלי אבטחת מידע

1.1 נוהל מספר 1 לנוהלי המסגרת בנושא "קביעת מדיניות אבטחת 'מידע רגיש' ומערכי מידע בממשלה ומוסדותיה" קובע כי יש להכין מסמך "מדיניות אבטחת המידע הרגיש ומערכי המידע" ולהטמיעו בקרב כל העובדים.

בנוהל מספר 1 נכתב: **"הניסיון מלמד שהגורמים להלן הם לפעמים קריטיים להצלחת המימוש של אבטחת מידע במשרד: ...מדיניות אבטחת מידע, מטרות ופעילויות המשקפות את מטרת העסק... ההנהלה תקבע מדיניות ברורה לגבי אבטחת מידע ותציג מחויבות לנושא ותמיכה בו, באמצעות פרסום מדיניות וקידומה... ההנהלה תאשר מסמך מדיניות, תפרסם ותפיץ אותו באופן ראוי בין כל העובדים. המסמך יכיל הצהרה בדבר מחויבות ההנהלה ויקבע את גישת המשרד לניהול ואבטחת מידע... התהליך יבטיח שייעשה סקר בתגובה לכל שינוי המשפיע על הבסיס להערכת הסיכונים המקורית...**
"על המנהל הכללי במשרד חלה אחריות מינהלית כוללת להכנת 'מסמך מדיניות לאבטחת מידע רגיש, מערכי מידע, שליטה ובקרה', ולפקח על אופן יישום המדיניות שנקבעה.
"על הממונה על אבטחת המידע (להלן - 'הממונה') חלה אחריות להכנת מסמך המדיניות של המשרד (בהיוועצות עם מנהל מערכות המידע), במסמך אשר לא יגרע מהאמור בנוהל זה, והבאתו לאישור וחתימה של המנהל הכללי."

נמצא כי לא נכתב מסמך מדיניות. לדברי מנהל האגף, קיימת טיוטה שעל עריכתה אחראית החברה המייעצת, אך כתיבתה טרם הסתיימה, משום שניתנה עדיפות גבוהה יותר להתקנת אמצעי אבטחת מידע ולטיפול בבעיות אבטחת מידע דחופות.

[1] רואה חשבון המתמחה בביקורת מערכות מידע וארכיטקט מערכות מידע מוסמך מיקרוסופט עם התמחות באינטרנט (שרת WEB).

1.2 בנוהל מספר 1 נכתב: **"ייזום פיתוח נוהלי אבטחה פנימיים, לשם הסדרת פעילויות אבטחת מידע במשרד..."**

בדוח 28 המליץ מבקר העירייה דאז: "רשות המחשוב תשקול ליזום עריכת טיוטות נוהל בנושאים הבאים ובתיאום עם עורכת הנהלים:

א. נוהל אבטחת חומרה לסוגיה, או להוסיף זאת לנוהל אבטחת מידע בפרק ייחודי בנושא, לרבות אמצעי מנע כלפי גניבות חומרה, כפי שאירעו בעבר וללמוד מלקחיהן.
ב. נוהל בנושא שימוש במשאבי התקשוב.
ג. נוהל המפרט את דרך קבלת שירותי תיקונים באמצעות גורם חוץ.
ד. נוהל המגדיר את אופן גיבוי הנתונים, ושחזורם, אבטחתם מפני אובדן, שינויים בלתי מבוקרים ושימוש שלא על-ידי מורשים לכך.
ה. נוהל המגדיר את אופן ניהול המידע הארגוני ומערכות המידע, כדי להבטיח אבטחת נגישות המשתמשים ליישומים ולנתונים הנדרשים ושימוש בנתונים על-ידי המורשים לכך. ניהול המידע הארגוני יבטיח שימוש אפקטיבי במידע שנאגר, לצורך קביעת מדיניות ותכנון אסטרטגי."

נמצא כי נוהלי העירייה כוללים כיום חלק מהנושאים שנדרשו בדוח 28. עם זאת, הנהלים אינם מקיפים רבים מהיבטי אבטחת המידע, ובכלל זה חלק מההיבטים שנכללו בהמלצות מבקר העירייה. לדוגמה, אין בנהלים התייחסות לעריכת סקרי סיכונים (תדירותם, היקפם, אופן ביצועם והגורם שיבצעם), ועדות היגוי וניהול פרויקטים, אישור מערכות חדשות, בקרת אבטחת מידע והיבטי אבטחת מידע בהתקשרות עם ספקים. לגבי הנושאים גיבויים ותכנית התאוששות מאסון, מנהל האגף מסר כי הנוהל בהכנה.

כמו כן, הנוהל העירוני לאבטחת מידע כולל הוראות שחלקן מיושנות ולא רלוונטיות, כגון שימוש בשיטת "call back"[2] בהפעלת תוכנות ההצפנה.

1.3 בנוהל מס' 1 נכתב: **"לענין בחוזה החלת נוהלי אבטחת מידע על כלל המשתמשים החיצוניים, ועל כל יתר הגורמים אשר יש להם מעורבות... כולל יועצים וספקי 'מיקור חוץ'..."**

מעיון בהסכם ההתקשרות עם החברה המייעצת עולה כי נוהלי העירייה לא צורפו כנספח לחוזה עמה, וכי ההסכם אינו מחייב אותה במפורש לעמוד בהוראות הנהלים הללו (אם כי היא מחויבת, באופן כללי, להיענות להוראותיו והנחיותיו של מנהל האגף).

[2] שיטת "call back" היא שיטת התחברות של ספקים באמצעות ניתוק המודם וחיוג למספר הקבוע בזיכרון של הטלפון. זאת, על מנת לוודא שההתחברות היא רק לטלפון מורשה. כיום, ההתחברות היא באמצעות "חומת אש".

2. בעלי תפקידים בתחום אבטחת מידע

2.1 מבנה ארגוני

א. נוהל מספר 1 ונוהל מספר 4 לנוהלי המסגרת בנושא "גורמי אבטחת מידע - הגדרות ותפקידים" קובעים את המבנה הארגוני של ניהול ויישום אבטחת המידע המושתת על עיקרון "הפרדת הסמכויות":

- גורם ניהולי בכיר - המנכ"ל (או המשנה למנכ"ל או הסמנכ"ל למינהל) - בעל אחריות מינהלית כוללת ליישום נוהלי המסגרת, על-פי החוק ותיקוניו.
- גורם מכוון - ועדת היגוי לאבטחת מידע, שתפקידה, בין היתר, להמליץ בדבר קווים מנחים, לאשר נהלים מוצעים, לכוון מדיניות בדבר הרשאות גישה למידע ולקבוע מהם האירועים והפעילויות החריגים המהווים סיכון לניהול התקין בכוח או בפועל.
- גורם ניהולי אבטחתי - הממונה על אבטחת מידע (להלן - **הממונה**) שיהווה הגורם המקצועי-אבטחתי ויפעל על-פי נוהלי אבטחת המידע במשרד. תפקידו יהיה לכוון את בעלי התפקידים ואת כלל "משתמשי הקצה" לשמור על נוהלי אבטחת מידע.
- גורמי ביצוע - מנהל מערכות המידע, מנהלי מאגרי המידע ועובדי התשתיות יהיו אחראיים בין היתר על יישום הכלים והשיטות לאבטחת מידע על-פי נהלים פנימיים שקבעה הנהלת המשרד, על-פי נוהל המסגרת ועל-פי הנחיה ישירה של הממונה.
- גורם סיוע אבטחתי (נאמני אבטחת מידע) - בעלי תפקיד טכני בתחום הטיפול והתחזוקה של מערכי המידע ביחידות השונות, אשר נוסף לתפקידם הם גם מסייעים לממונה ביישום הנהלים.

ב. הנוהל העירוני לאבטחת מידע אינו מגדיר את תפקידיהם ותחומי אחריותם של בעלי התפקידים כאמור במסגרת המבנה הארגוני.

ג. בניגוד לנדרש בנוהל מספר 1, נמצא כי בעירייה אין "גורם מכוון" (ועדת היגוי לעניין אבטחת מידע), ואף לא הוגדר "גורם ניהולי בכיר" שלו יהיה כפוף הממונה על אבטחת מידע.

2.2 הממונה על אבטחת מידע

א. סעיף 17ב לחוק קובע כי העירייה מחויבת למנות אדם בעל הכשרה מתאימה לתפקיד הממונה על אבטחת מידע.

ב. לפי נוהל מספר 1 לנוהלי המסגרת, הממונה אינו כפוף מינהלית (או באופן אחר) למנהל מערכות המידע, בשל ניגוד עניינים בין שני התפקידים.

ג. לפי נוהל מספר 4, תפקידיו של ממונה אבטחת מידע הם כדלקמן:

1) פיתוח, עדכון, הדרכה, הטמעה, הפצה ובדיקת היישום של נוהלי אבטחת מידע.

2) ייעוץ בנושאי אבטחה ובקרה בעת פיתוח יישומים חדשים, מיפוי ההרשאות ועדכונן באופן שוטף והגדרת פעילויות חריגות.

3) בדיקת יישומים קיימים ומתן ייעוץ לשיפור הבקרות בהם.
4) טיפול שוטף בהרחבת המודעות לסוגיות באבטחת מידע בדרגים השונים.
5) הכנת תכנית פעילות שנתית בנושאי אבטחת מידע במסגרת ועדת היגוי למחשוב. הממונה יכין לקראת כל ישיבה של ועדת היגוי למחשוב דוח מפורט על העשייה למן הישיבה הקודמת והליקויים שנחשפו. כן יכלול הדוח את תכנון הפעילות לתקופה הבאה.
6) סיוע במיפוי וסיווג של מאגרי המידע השונים ואחזקת הרישום המעודכן של כל היישומים וסיווגם.
7) חברות בוועדת ענ"א (עיבוד נתונים אלקטרוני).
8) תיאום עם גורמי הביקורת וביטחון המשרד.
9) מעורבות בהתקשרות עם גורמי חוץ רלוונטיים ומתן הנחיות אבטחת מידע על-פי הצורך, פיקוח על שירותי ספקים רלוונטיים וייעוץ בעת חתימת חוזים רלוונטיים.
10) ריכוז כל סיכומי אירועי ה"וירוסים", תקלות וניסיונות פריצה במשרד.
11) השתתפות בהכנת תכנית התאוששות מאסון והמשכיות עסקית.
12) ייזום בדיקות תקופתיות במחשבים אישיים, ברשת החשמל וציוד מיגון למערכות מחשוב במשרד וייזום תקופתי של בדיקות מומחים של סיכוני האש ומערכת המניעה.
13) קשר עם רשם מאגרי המידע במשרד המשפטים, כולל טיפול בדרישות החוק.
14) אחזקת הרשימות המעודכנות של הגורמים המחזיקים בנוהלי אבטחת מידע.
15) קיום מפגשים תקופתיים עם נאמני אבטחת מידע והנחייתם בהתאם לצורך.

לפי נוהל מספר 10 בנושא "ביקורת של אבטחת מידע", הממונה יבצע ביקורות בתחום אחריותו המקצועית בכל הגופים הממשלתיים שבתחום המשרד.

נוהל מס' 4 מגדיר את תפקידו של מנהל אגף מערכות מידע (מנמ"ר)[3]: **"קיימת חשיבות תפעולית ואבטחתית במינוי אחראי לכל מערכת מידע. מנהל האגף ינחה, יתאם וירכז פעילות האגף. כמו כן, המנהל או מי שהוסמך על ידו, ימנה אחראי לכל מערכת הקיימת במשרד (כגון מערכת כוח אדם, מערכת שכר, מערכת רכש וכד'). אחראי המערכת ירכז את כל המשתמשים ויהיה זה המוסיף או הגורע משתמשים מן המערכת. אחראי המערכת יתודרך תקופתית ע"י הממונה על אבטחת מידע במכלול נושאי האבטחה השוטפים והמתחדשים. ביעור חומר עודף או מיותר יתבצע ע"י אחראי המערכת."**

[3] תפקיד מקביל למנהל האגף.

ד. נמצא כי מנהל האגף משמש גם כממונה על אבטחת מידע בעירייה. לדבריו, בשל היעדר תקן לתפקיד זה בעירייה, הוא מינה את עצמו לתפקיד וקיבל את אישורו של יועץ משפטי חיצוני לעירייה. מנהלת מאגר המידע העירוני דיווחה על מינוי זה למשרד המשפטים.

למנהל האגף, בתפקידו כממונה על אבטחת מידע, מסייעים עובדי האגף וכן רפרנטים של המערכות הממוחשבות ביחידות העירוניות השונות. כמו כן, כאמור, מועסקת באגף חברה מייעצת לצורך ליווי האגף בניהול פרויקטים של אבטחת מידע.

ה. עוד נמצא כי מנהל האגף אינו עורך בקרה על אבטחת המידע ביישומים, אלא מתמקד באבטחת התשתיות בלבד (רשת, חומרה, התקשרות מרחוק, גישה לרשת האינטרנט, גיבויים ועוד). לדבריו, להיבטי אבטחת המידע ביישומים אחראיים הרפרנטים ביחידות השונות המשתמשות באותם יישומים. הרפרנטים כפופים למנהלי היחידות, והוא אינו מפקח עליהם (דוגמאות: מנהלת פרויקטים מחלקת מחשוב ובקרה בגזברות כפופה לגזבר העירייה; רפרנטית המחשוב במינהל לשילוב חברתי כפופה לראשת המינהל).

לדעת מנהל האגף, יש צורך בהידוק שיתוף הפעולה בינו לבין הרפרנטים ביתר היחידות העירוניות (למשל באמצעות ועדות היגוי משותפות) על מנת לתאם את היבטי אבטחת מידע בעת הפיתוח והאפיון של המערכות השונות, לצורך גיבוש מדיניות אחידה בתחומי אבטחת מידע וכיוצא באלה.

2.3 החברה המייעצת

תפקידיה ואחריותה של החברה המייעצת מוגדרים בחוזה ההתקשרות של העירייה עמה. נמצא כי החברה המייעצת ביצעה, לבקשת מנהל האגף, רק חלק קטן מהמשימות הרבות שהתחייבה לבצע. להלן סטטוס ביצוע המשימות לפי דיווח מנהל האגף:

א. המשימות שבוצעו: סיוע בהכנת מכרז לתקשורת ואבטחת מידע, ליווי וניהול פרויקטים בתחום אבטחת מידע, שילוב היבטי אבטחת מידע בפיתוח מערכות, סיוע בקבלת החלטות בבחירת מוצרי אבטחה וביצוע ובחינת חלופות לאמצעי אבטחת מידע.

ב. המשימות שטרם הושלמו: גיבוש מסמך מדיניות אבטחת מידע, מיפוי וסיווג נכסי מידע והטמעה ופילוח של מערכות SIM/SOC[4].

ג. משימות שהחברה טרם החלה לבצע: ליווי בהקמת תקן ISO 27001[5], סקר סיכוני אבטחת מידע, העברת הדרכות והעלאת מודעות בנושאי אבטחת מידע, בדיקת יישומים לזיהוי סיכוני אבטחת מידע, בדיקות קוד מאובטח באפליקציות, ביקורות פיזיות, אִפיון וליווי פרויקטים בתחומי ניהול זהויות וקוד עוין (וירוס).

[4] מערכת לניהול אבטחת מידע.

[5] תקן ישראלי למערכת לניהול אבטחת מידע.

3. סוגיות בנושא אבטחת מידע

3.1 מאגרי מידע

א. סעיף 8(ג) לחוק מחייב את העירייה ברישום של מאגרי מידע בפנקס מאגרי המידע במשרד המשפטים (להלן - **פנקס**).

כאמור, הממונה על אבטחת מידע אחראי לאבטחת המידע במאגרים המוחזקים ברשות העירייה.

ב. נוהל מספר 22 לנוהלי המסגרת בנושא "רישום המאגרים" קובע:

"כל אחראי לתפעול מערכת מידע כלשהי, ידווח על קיומה לממונה על אבטחת המידע במשרד. הדיווח יכלול פרטים אודות המערכת ואת אמצעי האבטחה עליה. הממונה על אבטחת המידע יבדוק אם המאגר מתאים להגדרת החוק. במידה וכן, יפעל לרישומו במשרד המשפטים. יש לדווח כנ"ל על הקמת כל מערכת מידע חדשה.

"לכל מאגר מידע יקבע מנהל מאגר.

"מנהל המאגר יחתום על שאלון הרישום של משרד המשפטים, שנמסר לו ע"י הממונה למערכות המידע במשרד. השאלון יישלח אל רשם מאגרי המידע, ע"י הממונה על אבטחת המידע במשרד... אצל ממונה על אבטחת המידע והממונה על הפעלת חוק חופש המידע יימצא רישום מדוקדק של כל מאגרי המידע של המשרד הרשומים אצל רשם מאגרי המידע במשרד המשפטים, וכן של כל המאגרים הנמצאים בתהליכי רישום כולל עדכון הסטטוס."

הממונה על חוק חופש המידע השיבה לשאלת הביקורת האם הועבר אליה רישום של כל מאגרי המידע של העירייה: "מאגרי המידע הם באחריות... מנהלת אתר האינטרנט העירוני ומר... מנהל התקשוב העירוני [מנהל האגף]."

ג. סעיף 31א(א)(1) לחוק קובע בין היתר כי ניהול, החזקה או שימוש במאגר מידע החייב ברישום ולא נרשם - מהווה עבֵרה פלילית שדינה מאסר שנה. נוסף על כך, בגין עבֵרה זו רשאי רשם מאגרי מידע להטיל קנס מינהלי.[6]

סעיף 8 לנוהל עירוני לאבטחת מידע קובע: **"כל מאגרי המידע בעירייה חייבים ברישום בפנקס מאגרי המידע שבמשרד המשפטים, באחריות מנכ"ל העירייה ובאמצעות מנהל הרשות למחשוב ובקרה."**

נמצא כי מערכת תביעות ביטוח (בר טכנולוגיות) הקיימת בעירייה לא נרשמה בין המאגרים בפנקס.

<u>תגובת מנהלת מרכז מידע ומחקר</u>:

"מדי שנה אני שולחת לכל ראשי המינהלים והיחידות מכתב ובו אני מודיעה להם על:

- סוג המאגרים שחייבים להירשם אצל רשם המאגרים
- רשימת המאגרים הרשומים שבניהולם
- בקשה לדווח על מאגרים שע"פ הקריטריונים חייבים רישום אך לא רשומים.

[6] על-פי תקנות העבירות המנהליות (קנס מינהלי - הגנת הפרטיות), התשס"ד-2004.

השנה צרפתי טופס למילוי עבור מאגרים שאינם רשומים (מצ"ב). לאחר משא ומתן ממושך ואינטנסיבי בכתב ובע"פ במהלך 2014 עם רמו"ט לגבי הקבצים שצריכים לרשום, שלחתי רשימת קבצים לעו"ד... מרמו"ט והיא החזירה לי רשימה של קבצים שצריך לרשום. בחודש האחרון הושלם הרישום של 7 מאגרים חדשים ונותר מאגר אחד שרישומו יושלם מיד לאחר שתנוסח הצהרה שתהיה מקובלת ע"י רמו"ט. להלן רשימת המאגרים החדשים שרישומם הושלם ולבעלי המאגרים נשלח אישור בכתב:...
לא דווח לי על מערכת תביעות הביטוח ולכן היא לא נרשמה."

ד. נוהל מספר 2 בנושא "מיפוי וסיווג 'מידע רגיש' ומערכי מידע" ממליץ לסווג את מאגרי המידע באמצעות "ועדת סיווג" לפי סודיות וחיוניות. רמות הסיווג ינועו בין "בלתי מסווג" (בלמ"ס) לבין "חסוי ביותר". כמו כן, סעיף 12 לנוהל עירוני לאבטחת מידע קובע הוראות מפורטות לעניין סיווג המידע: ארבע דרגות - גלוי, רגיל, מוגבל, רגיש, וכן כי ינוהל רישום של המסמכים הרגישים (רישום זה כשלעצמו יהיה רגיש).

מנהל האגף מסר לביקורת כי אין סיווג של המערכות לפי רגישותן וטרם מונו "בעלים" לכל המערכות. לדבריו, "הנושא בעבודה".

3.2 **סקר סיכונים**

א. לפי נוהל מספר 3 לנוהלי המסגרת בנושא "סקרי סיכונים - ניהול והערכה", "ניהול סיכונים" הוא "**תהליך הזיהוי, הבקרה והמזעור או סילוק של סיכוני אבטחה העלולים להשפיע על מערכות מידע, הנעשה בעלות קבילה. במסגרת ניהול הסיכונים מתבצע סקר סיכונים, שמטרתו לאתר את הסיכונים לארגון ולהעריך את חומרתם, זאת על מנת לאפשר קבלת החלטה מבוססת באיזה סיכונים לטפל, ובאיזה סדר עדיפות, עלות ולוח זמנים**".

הנוהל ממליץ להעריך סיכונים כשלב מקדים בתהליך עיצוב מדיניות אבטחת מידע. תוצאות ההערכה יסייעו לקבוע מהן פעולות האבטחה שראוי לנקוט וישמשו בסיס לקביעת קדימויות להקצאת המשאבים.

האחראיים על יישום נוהל זה הם מנהל אגף מערכות מידע והממונה על אבטחת מידע.

ב. נמצא כי לא נערכו סקרי סיכונים לעניין אבטחת מידע בעירייה. כמו כן, בנוהל העירוני לאבטחת מידע אין התייחסות לעריכת סקרי סיכונים, תדירותם ואופן עריכתם.

ג. כאמור, אף החברה המייעצת שהתחייבה לבצע "סקר סיכוני אבטחת מידע על מערך טכנולוגית המידע של עיריית ראשון לציון" טרם ערכה סקר זה. לדברי מנהל האגף, עריכת הסקר לא הייתה בראש סדר העדיפויות של האגף, ועל כן החברה טרם התבקשה לערכו.

3.3 תצהיר סודיות והדרכות

א. על מנת להפחית טעויות אנוש או שימוש לרעה במידע שנאגר, נושאי אבטחת מידע ושמירת הסודיות צריכים להיות מטופלים כבר בשלב גיוס העובדים ולהיכלל בחוזי העבודה, וכן להיות מנוטרים במשך זמן העסקתו של העובד.

ב. בנוהל מספר 6 לנוהלי המסגרת בנושא "בדיקת מהימנות העובדים, התחייבות לשמירת סודיות" נכתב: **"כל מועמד פוטנציאלי לעבודה יתוחקר כראוי, במיוחד עבור תפקידים רגישים."**
נמצא כי מנהל האגף אינו עורך תחקורים לעובדים חדשים בנושאי אבטחת מידע.

ג. בדוח מבקר העירייה מספר 28 המליץ המבקר דאז "לוודא שכלל עובדי העירייה, לרבות עובדי חברות כוח-אדם, חתמו על תצהיר סודיות".
לדברי מנהלת אגף משאבי אנוש במינהל כוח אדם ואמרכלות, עובדי אגף משאבי אנוש דורשים מהעובדים לחתום על תצהיר סודיות עם קליטתם לעבודה. כמו כן, לדברי מנהל האגף, עם פתיחת הרשאה לגישה למערכות מידע ממוחשבות נדרשים העובדים לחתום באגפו על תצהיר סודיות נוסף.

ד. עוד קובע נוהל מספר 6: **"תנאי ההעסקה יציינו את אחריותו של העובד לאבטחת מידע. אם אפשר, האחריות תהיה תקפה למשך תקופה מוגדרת לאחר גמר העסקתו במשרד. יפורט גם איזו פעולה יש לנקוט במקרה שהעובד אינו מציית לדרישות האבטחה. הזכויות והחובות של העובד בנושא אבטחה, כגון על פי שמירת דיני זכויות יוצרים והחקיקה בנושא הגנת נתונים, יובהרו ויכללו בין תנאי העסקתו... אם אפשר, תנאי ההעסקה יכללו גם הצהרה שאחריות חלה על העובד גם מחוץ לכותלי המשרד וגם מעבר לשעות העבודה הרגילות, כגון במקרה של עבודה בבית."**

מעיון בנוסח האחיד של "תצהיר הסודיות" עליו נדרש לחתום עובד חדש עולה כי מדובר במסמך קצר, לפיו מצהיר העובד ש"הוראות החוקים והתקנות המופיעים מטה הובאו לידיעתי והוסברו לי, לרבות האחריות המוטלת עלי לשנן את הוראותיהם ולפעול לפיהם". עם זאת, אין כל הבהרה או הסבר בדבר ההוראות בכתב, ולדברי מנהל האגף, העובד אף אינו מקבל מידע על אודותם בעל-פה. בתצהיר גם לא נקבעה סנקציה למקרה שעובד לא ציית לדרישות האבטחה, ולא נרשם בו כי אחריותו חלה גם מחוץ לכותלי העירייה.
הביקורת בדקה האם שמונה עובדים שהחלו לעבוד בעירייה בשנים 2013-2014, ושהייתה להם גישה למערכות ממוחשבות עירוניות (נבחרו באופן מדגמי), חתמו על תצהיר סודיות לפני פתיחת הרשאה בעבורם. נמצא כי כל העובדים שנדגמו חתמו על תצהיר סודיות.

ה. בדוח 28 המליץ מבקר העירייה דאז "להקפיד לתדרך ולשנן את נוהל אבטחת מידע לכלל העובדים אחת לשנה ולהפיץ דף מידע, שיכלול את עיקרי הוראות החוק ונהלים הנוגעים למערכות מידע, לפחות אחת לחצי שנה, ולהחתים את העובדים על ספח המאשר כי קראו והבינו את תוכנו".

נוסף על כך, בנוהל מספר 8 לנוהלי המסגרת בנושא "מודעות, הדרכה, הטמעה והסברה" נכתב כי המשתמשים יקבלו הדרכה בנושא נוהלי אבטחה, וכי פעילות ההדרכה תקבל תקציב הולם. הנוהל דן בהדרכה לעובדים חדשים, בהדרכה שנתית וב"פעילות של ריענון": **"ההדרכה תכלול דרישות אבטחה, מחויבויות על פי החוק ובקרות של המשרד, וכן הדרכה לשימוש נכון באפשרות לעיבוד מידע, כגון נהלי כניסה למערכת, שימוש בחבילות תוכנה, כל זאת לפני מתן הרשאת גישה למידע או לשירותים."** כמו כן, **"פעם בשנה תתבצענה פעילויות הדרכה בנושא אבטחת מידע לקבוצות עובדים, משתמשי מחשב ו/או לקבוצות להן נגינה למידע... במהלך השנה תתבצע פעילות של ריענון להגברת המודעות האבטחתית."**

נמצא כי לא מבוצעת כלל הדרכה בנושא אבטחת מידע. כמו כן, אין דף מידע עירוני מפורט העוסק בעיקרי החוק והנהלים לאבטחת מידע.

ו. כאמור, החברה המייעצת התחייבה בחוזה עם העירייה בין היתר ל"העברת הדרכת מודעות לבעלי תפקידים רגישים" ו"לקמפיין להעלאת מודעות אבטחת מידע בקרב כלל העובדים (אמצעים פיזיים ואמצעים אלקטרוניים)". מנהל האגף לא הנחה את החברה לבצע פעולות אלה במהלך שלוש שנות עבודה.

ז. נוהל מספר 7 בנושא "קשר עם גורמי חוץ ב-outsourcing[7]" עוסק ב**"הגדרת אופן קיום הקשר העסקי עם גורמי חוץ, במגמה לצמצם את הסיכון למערכות הממוחשבות ולמאגרי המידע"**. הנוהל ממליץ כי בחוזה עם גורם חוץ ייקבע **"פרק בנושא אבטחה שיכלול את כל הנחיות אבטחת המידע המתייחסות לכלל דרכי הגישה של גורם החוץ למידע... בנוסף לכך יכלול החוזה את הרשימה השמית המדויקת של נציגי גורם החוץ שיורשו לבצע את הפעילות... גישת צד שלישי למידע ולמתקני עיבוד מידע לא תינתן אלא לאחר שיושמו הבקרות הראויות ונחתם חוזה המגדיר את תנאי ההתחברות או הגישה. סידורים הקשורים בגישת צד שלישי למתקני עיבוד מידע של הארגון, יתבססו על חוזה רשמי המכיל את כל דרישות האבטחה, או המתייחס אליהן, כדי להבטיח התאמה לשיטות האבטחה ולתקני האבטחה של הארגון"**.

הביקורת עיינה בשני חוזים לדוגמה: החוזה שנחתם עם החברה המייעצת והחוזה של העירייה עם החברה לאוטומציה. נמצא כי בשני החוזים קיים סעיף "שמירת סודיות" כללי, לפיו חלה על גורם החוץ חובת סודיות לגבי כל מידע שהגיע לידיעתו בקשר עם ביצוע ההסכם. החוזה אינו כולל רשימה שמית של נציגי גורם החוץ כנדרש ולא מוגדרים בו תנאי ההתחברות או הגישה.

4. אבטחה לוגית

4.1 ניהול הרשאות משתמשים

א. בנוהל מספר 13 לנוהלי המסגרת בנושא "מידור, זיהוי והרשאות המשתמשים" נכתב: **"מנהלי המאגרים השונים יהיו אחראים לקביעת ההרשאות של העובדים הכפופים להם. יישום ההרשאות יבוצע בתאום בין מנהלי היישומים לממונים ישירים.**

[7] מיקור חוץ.

למען הסר כל ספק, מודגש כי הרשאה איננה רק אפשרות הגישה למערכת מסוימת, אלא גם הגדרה מדויקת של הפעילויות שרשאי המשתמש לבצע בכל יישום/מסך: אחזור ו/או עדכון ו/או תוספת ו/או מחיקה."

בדוח 28 המליץ מבקר העירייה דאז "להכין נוהל לפתיחת הרשאה למשתמש חדש וביטול הרשאה למשתמש שעזב. הנוהל יפרט את כל התהליכים לפתיחת או סגירת הרשאת משתמש, וזאת על מנת למנוע אפשרות גישה למערכת, שלא בהתאם למדיניות הארגון".

נמצא כי נוהל עירוני אבטחת מידע אינו מפרט תהליכים אלה אלא מסתפק בהוראות כלליות בלבד: **"המנהל יקבע לגבי כל משתמש, את ההבחנה בין הרשאה לשלוף/לעיין במידע ובין ההרשאה לרשום או לתקן מידע קיים. עם העברת עובד לתפקיד אחר או פרישתו, יחליף המנהל מידית את שם המשתמש שהיה ידוע לעובד בתפקידו הקודם."**

ב. עוד נאמר בנוהל מספר 13: **"מנהל מערכות מחשוב ירשום את המערכות שאליהן יהיה העובד מורשה לגשת, יפרט אם העובד מורשה לעדכן את הנתונים או רק להציגם ויאשר בחתימתו על גבי הטופס את מתן הסיסמה ורשות הכניסה למערכת לעובד."**

בדוח 28 המליץ מבקר העירייה דאז גם "ליצור טופס אחיד לבקשה לפתיחת/סגירת הרשאה לעובד חדש, עובד שעזב או נויד מתפקידו".

לדברי מנהל האגף, את ההרשאה פותחים בהתאם לטופס אחיד לעדכון/פתיחת משתמש ברשת העירונית. עם זאת, מנהל האגף אינו מנהל מאגר של הגורמים המורשים לשלוח טופס זה.

כמו כן, בניגוד להמלצת מבקר העירייה, עזיבת עובד אינה מדווחת באמצעות טופס, אלא כהודעה של אגף משאבי אנוש בדואר האלקטרוני.

ג. לפי נוהל מספר 13, **"עזיבת עובד... או העברתו לתפקיד אחר, תועבר מידית לידיעת מנהל היישום, וזה יבטל את הרשאות הגישה של העובד. אחריות הדיווח חלה על הממונה הישיר ו/או מנהל יחידת משאבי אנוש בארגון".**

לפי סעיף 11(4) לנוהל עירוני לאבטחת מידע, **"עם העברת עובד לתפקיד אחר או פרישתו, יחליף המנהל מידית את שם המשתמש שהיה ידוע לעובד בתפקידו הקודם".**

אגף משאבי אנוש הוא האחראי להודיע על עזיבת עובדים. עם זאת, לדברי מנהל האגף, לא בכל המקרים מתקבלות הנחיות ברורות מאגף זה בנוגע להסרת הרשאה. כך לדוגמה, בחלק מהמקרים לא התקבל מידע על אודות המסכים והמערכות שלעובד היו הרשאות גישה אליהן על מנת לבטל את כולן.

הביקורת בדקה לגבי עשרה עובדים שסיימו עבודתם בעירייה בשנת 2013 ונבחרו באופן מדגמי, האם הוסרה הרשאתם מרשת המשתמשים. נמצא כי שמות המשתמש של שלושה מהם לא בוטלו מהרשת:

שם העובד	תאריך עזיבה
צ"א	31.12.13
ל"ו	31.10.13
ד"ש	27.2.13

ד. עוד נכתב בנוהל מספר 13: **"אחת לרבעון תתבצע פעילות ביטול או הקפאת משתמשים שלא עשו שימוש במשאבי המחשוב, במשך תקופה שתוגדר בזמן הבדיקה."** לדברי מנהל האגף, משתמש שלא ביצע כניסה למערכת במשך שלושה חודשים - ננעל.
לביקורת הועבר דוח המציג את המשתמשים האחרונים להם בוצע ביטול/הקפאת משתמש. עם זאת, לא נמצא תיעוד כי אכן בקרה זו בוצעה כל רבעון במהלך שנת 2014.

4.2 מדיניות סיסמאות

א. לפי נוהל מספר 13, **"לא יתאפשר לעבור מיישום ליישום... אלא דרך התפריט הראשי ומערכת הסיסמאות"**. נוהל זה וכן נוהל עירוני לאבטחת מידע מכתיבים מדיניות סיסמאות רצויה.
להלן השוואה בין הוראות הנהלים לבין מדיניות הסיסמאות המוגדרת ברשת וביישומים:

	הנחיות		ממצאי הביקורת		
	נוהל מספר 13	נוהל עירוני לאבטחת מידע	מדיניות סיסמאות ברשת	מדיניות סיסמאות במערכת קומפלוט	מדיניות סיסמאות במערכת נמ"ר לפי איש תמיכה (מינהל לשילוב חברתי)
שמירת סיסמאות קודמות (מספר דורות)	4	אין התייחסות	6	אין שמירה	לא ידוע
כמות תווים בסיסמה	6	6	6	4	6
אילוץ להחלפה (מספר ימים)	60	אין התייחסות	60	אין	אין
מורכבות סיסמה (תווים רצופים, אותיות ומספרים)	כן	כן	כן	אין	יש
הגבלת מספר ניסיונות כניסה עם סיסמה שגויה	3	אין התייחסות	6	אין	אין

הביקורת מצאה כי לאחר 15 דקות ללא עבודה בתחנות העבודה הממוחשבות, תוכנת ניהול הרשת חוסמת את המשתמש ודורשת הזנה חוזרת של שם משתמש וסיסמה.

ב. בנוהל מספר 13 נכתב: **"חל איסור מוחלט למסור/לחשוף סיסמאות. אין לתלות את הסיסמאות על פתקיות בקרבת המחשב"**. הביקורת מעירה כי בעת ביקור בחדר המחשב התגלתה פתקית עם שם משתמש וסיסמה (אם כי בדיעבד הסתבר כי הסיסמה שנרשמה הייתה שגויה).

<u>תגובת מנהל האגף</u>:
"הסיסמה הראשית למחשב הנה הבסיס למדיניות הכניסה למחשב, הסיסמה הנוספת הנה גורם נוסף ולעתים אף מיותר (בלקוחות רבים מיושם פתרון SSO שאינו מצריך סיסמה מעבר לסיסמה הראשונית)."

יש להעיר כי במידה שמנהל האגף יבחר בשיטת SSO (מדיניות סיסמאות מחמירה), יש לעגן את הבחירה במסגרת מסמך מדיניות אבטחת המידע של

העירייה, ובכלל זה התייחסות לסיכונים הטמונים בשיטה זו (לדוגמה: שינוי עתידי במדיניות הסיסמאות לרשת עלול לפגוע בבקרות הגישה למערכת האפליקטיבית).

4.3 טיוב ובקרת הרשאות

א. בנוהל מספר 13 נכתב: **"באחריות מנהלי המאגרים לבדוק כל משתמש פעם בשנה, לצורך עדכון מפת ההרשאות. הביצוע יהיה ביוזמת מנהלי היישומים ובתיאום עם הממונים הישירים."**

בדוח 28 המליץ מבקר העירייה דאז "לבצע בדיקת מורשים ולבטל הרשאות ושמות משתמשים של עובדים שאינם נדרשים לגישה למערכת. לבדוק האם ההרשאות של כל המשתמשים מספק שירותי המחשוב, אושרו כראוי והאם כל הרשאה כזו נחוצה לתפקידם. לבצע בקרה תקופתית אחר פעולות משתמשי העל, גם משום שלמשתמשים אלו יש סמכויות רחבות יותר משאר המשתמשים".

ב. לאור ממצאי הביקורת בדוח מבקר העירייה לשנת 2013 (מספר 34) בנושא "בדיקת פעולות שבוצעו בידי עובדת יחידת אישורים לטאבו למגורים" בנוגע להרשאות לא מתאימות שניתנו לעובדים במינהל הכספים, מסיקה הביקורת כי ההמלצה לא יושמה: "הממונה על הבקרה [במינהל הכספים] מסרה לביקורת כי לא קיים פרופיל מוגדר להרשאות משתמש בהתאם לתפקידו או על-פי היחידה אליה הוא משתייך. לדבריה, עד לשנת 2011 לכל מנהל אגף ניתנה הרשות לבקש הרשאה לעובדיו - הבקשה נמסרה בעל פה וללא תיעוד. החל משנת 2011 רק הממונה על הכנסות העירייה מאשר הקצאת הרשאות נוספות. נמצא כי בקליטת עובד מחליף מועתקות ההרשאות מעובד קיים של אותה יחידה ולא מתבצעת בדיקה מחודשת של נחיצות ההרשאות של העובד אותו החליף בתפקיד. לדברי מנהל אגף גבייה ואכיפה, נכון למועד איסוף ממצאי הביקורת [דוח מספר 34] מבוצעת בדיקה מקיפה של ההרשאות לכל עובד."

ג. לדברי מנהל האגף, מנהלי המערכות ביחידות המקצועיות אחראיים לתחזוקת וטיוב משתמשי היישומים. מנהלת מחלקת מחשוב ובקרה במינהל הכספים נשאלה האם לצורך בקרה וטיוב ההרשאות, היא מעבירה אחת לתקופה לאישור הגזבר או גורם אחר במינהל את קובץ ההרשאות במערכות הכספים. כאסמכתא, היא התבקשה להעביר לביקורת את הקובץ, אם שלחה אותו, לצורך בחינת ההרשאות לפי עקרון "הצורך לדעת ולעשות"[8]. מנהלת מחלקת מחשוב ובקרה השיבה לביקורת: "לא קיבלתי הנחיה בנושא ולא מידע שהדבר נעשה בעבר. יזמתי ניהול קובץ מעקב באקסל על הרשאות במג"ע, רכש ופיננסית, קוגנוס

[8] בנוהל מספר 1 נכתב:

"א. על פי עקרון 'הצורך לדעת ולעשות' (במידע, ובמערכי המידע, השליטה והבקרה) ימדר המשרד את המידע ומערכות המידע, השליטה והבקרה ואת המורשים להשתמש או לטפל בהם, ויעניק הרשאות גישה רק לפרטי מידע ומערכות מידע, שליטה ובקרה, הנדרשים [על פי קביעת גורם מינהלי בכיר במשרד], לצורך ביצוע תפקידים במשרד.

ב. המידור ייעשה על ידי חלוקת המשתמשים לקבוצות שייכות או נושא כשבכל הרשאה יוגדר גם מה מותר לעובד לעשות (מידע/נתונים - קריאה, כתיבה, מחיקה, העברה וכיוצא בכך. מערכי מידע, תקשורת, שליטה ובקרה - הפעלה, כיבוי, תחזוקה, הוספת חומרה וכו').

ג. עקרונות המידור יוגדרו על ידי 'הממונה', תוך היוועצות מוקדמת עם גורמי המטה המקצועיים לכל תחום פעילות במשרד ולכל מאגר מידע, ויובאו לאישור ועדת המשנה לאבטחת מידע, שתמונה על ידי ועדת ההיגוי למחשוב."

ורישיונות סריקה שכולל "שם מאשר", תאריך והרשאה למספר מסך...." הקובץ שהתבקש לא צורף לתגובתה.

ד. נמצא כי מנהל האגף אינו בודק באמצעות הפקת דוח הרשאות מכל היישומים כי אכן ניתנו הרשאות משתמשי-העל רק לרפרנטים של המערכות על בסיס עקרון "הצורך לדעת". כלומר, הוא אינו מפקח על הרשאות-העל בכל אפליקציה, שהן בעלות הסיכון הרב ביותר משום שהן מאפשרות למשתמש לעקוף את בקרות המערכת.
כמו כן, מנהל האגף אינו מפיק דוח הרשאות לרשת ואינו מפיץ את הדוח הנ"ל לאישור הממונים הישירים, על מנת שיאשרו כי ההרשאות הקיימות ברשת תואמות את עקרון "הצורך לדעת".

4.4 בקרה ופיקוח לוגי על פעולות ברשת

א. נוהל מספר 15 בנושא "בקרה ופיקוח לוגי" מגדיר "בקרה לוגית" כ"**ניטור שוטף ממוחשב אחר הפעילות במערכת הממוחשבת, תוך התמקדות באירועים חריגים או רגישים**". "פיקוח לוגי" מוגדר כ"**מעקב אחר פעילויות במחשב גם לאחר ביצוע הפעילות ובהשהיית זמן כלשהו**". נוהל זה ממליץ כי "**יוגדרו במערכת פעולות חריגות או רגישות... ההגדרה הנ"ל תכלול ניסיונות סרק לכניסה למערכת וכן ניסיונות לבצע פעולות בלתי מורשות אחרות... הגדרת הפעילויות החריגות תיבדק ותתעדכן לפחות אחת לשנה**".
נמצא כי אין הגדרה לאירועי אבטחה/פעילויות חריגות (טעויות חוזרות בכניסה למערכת, פעילות בשעות הלילה וכדומה). עם זאת, לדברי מנהל האגף, "העירייה משלימה בימים אלה נוהל מקיף המגדיר את תהליך הטיפול באירועי אבטחת מידע".

ב. עוד נכתב בנוהל מספר 15, כי במערכת יישמר יומן (LOG) של כל הפעילויות שבוצעו באמצעות תוכנה ייעודית. ה"לוגים" ינותחו אחת לשבוע באמצעות כלים ממופנים והממצאים החריגים יועברו באופן מידי לממונה על אבטחת מידע שיערוך בירור דחוף לגבי הממצאים החריגים.
נמצא כי לא נשמרים בעירייה לוגים (לרבות על פעולות של עובדי התמיכה שהם בעלי הרשאות-על). מנהל האגף מסר לביקורת: "אנו בתהליך מיכון נושא הטיפול באירועי אבטחת מידע. במסגרת זו ייכלל גם בסיס נתונים היסטורי אשר יתעד את כלל אירועי המידע בארגון... אנו עומדים ליישם טכנולוגיה לזיהוי אירועי אבטחת מידע SIEM." הוא צופה שהמערכת תחל לפעול עד סוף שנת 2014.

5. אבטחה פיזית וסביבתית

5.1 ניהול מלאי חומרה ותוכנה

נוהל מספר 23 לנוהלי המסגרת בנושא "ניהול מלאי חומרה ותוכנה" קובע כי תנוהל, תבוקר ותתוחזק מצבת חומרה ותוכנה. זאת, משום ש"**רשימת מצאי של נכסים עוזרת להבטיח שתהיה הגנה אפקטיבית על הנכסים... תהליך הכנת מצאי נכסים הוא היבט חשוב בניהול סיכונים. משרד צריך להיות מסוגל לזהות את נכסיו ואת הערך והחשיבות היחסיים**

שלהם... צוות מרכז התמיכה ינהל יומן רישום ומעקב... מעת לעת יבצע צוות מרכז תמיכה וצוות סיוע טכני בדיקה".

נמצא כי קיימת רשימת מצאי הכוללת את הנכסים הקשורים למערכות המידע, וכי כל מחשב מזוהה באופן חד-ערכי, עם ציון שם העובד, שם המשתמש וכתובת.

5.2 **בקרת גישה פיזית**

א. בנוהל מספר 12 בנושא "בקרת גישה למחשב המרכזי ולמחשבים האישיים" נכתב: **"הימצאות בעלי תפקידים ביחידת המחשב המרכזי תהיה באזורים הנדרשים להם מחוקף תפקידם בלבד. בעלי תפקיד ומוזמנים אחרים, שאינם עובדי המשרד, יהיו מלווים מרגע כניסתם לאזור הממודר של מערך המידע, בכל משך שהותם בו, עד צאתם מאזור זה!"**

לבקשת הביקורת, מסר מנהל בניין העירייה, הממונה על מערכת כרטיסי הדלתות, רשימה של 34 מורשים להיכנס לחדר השרתים. רבים מהם בעלי הרשאת "מאסטר" לכל הבניין.

לדוגמה, עובד עירייה ה"ממונה על תחום מים ומירסים חירום", שישה עובדי רכש ואספקה, וכן מורשית זמנית שאינה נמצאת במצבת עובדים הם בעלי הרשאת "מאסטר".

<u>תגובת מנהל האגף</u>:

"בעקבות הערת הביקורת הנחיתי את הגורם האחראי למתן הרשאות לחדר המחשב כי יש לאפשר הרשאות ל-6 מתוך 34 עובדים בלבד."

ב. סעיף 14 לנוהל עירוני לאבטחת מידע קובע: **"עובד היוצא מחדר עבודתו יסגור את תחנת העבודה בה הוא משתמש, ואם לא נוכח בחדר עובד אחר, ינעל את החדר."**

נמצא כי, על אף שלחדר השרתים בבניין העירייה יש בקרת גישה באמצעות כרטיסים מגנטיים, יועצי הביקורת הצליחו להיכנס אליו ללא כרטיס מגנטי וללא מלווים, משום שדלת החדר הייתה פתוחה לרווחה, בלא ששהו בו עובדי האגף.

ג. על ארונות התקשורת להיות נעולים, למניעת פגיעה או התחברות של גורם לא מורשה. אף על פי כן, בעת סיור נציגי הביקורת, ארון התקשורת בקומה הרביעית בבניין העירייה לא היה נעול.

5.3 **סיכוני אש, חשמל ומים בחדר המחשב המרכזי**

א. בנוהל מספר 27 לנוהלי המסגרת בנושא "סיכוני אש, חשמל ומים בחדר המחשב" נכתב כי **"המחשב המרכזי יהיה מחובר אל מקור המתח באמצעות יחידת UPS מסוג** ONLINE". לביקורת הועברה חשבונית המאשרת רכישת אל-פסק חדש בינואר 2014.

ב. סעיף 6(ז) לנוהל עירוני לאבטחת חומרה ותוכנה קובע: **"יש לשמור על סביבת עבודה נקייה ולהימנע ממצבים קיצוניים של אבק, טמפרטורה, הפרעות מתח חשמל..."**

נמצא כי בחדר המחשב המרכזי מותקן מד טמפרטורה ושני מזגנים הנדרשים לצורך שמירת ובקרת הטמפרטורה בחדר, כנדרש בנוהל.

ג. עוד נכתב בנוהל מספר 27: **"מחשבים הניצבים על הרצפה יוצבו על משטח מוגבה יציב בגובה של 10 ס"מ לפחות. זאת כדי למנוע פגיעת רטיבות ונוזלים."** כמו כן, לפי נוהל זה, בחדר המחשב המרכזי יוצבו מטפי גז הלון.
בסיור במקום נמצא כי מותקנת בחדר המחשב המרכזי רצפה צפה להגנת הציוד מפני הצפה. כמו כן, בחדר הוצבו מטפי גז הלון.

ד. על מנת להימנע מהפרעות מתח חשמל ולשמור על הטמפרטורה קיים גנרטור לגיבוי מערכת החשמל. לביקורת הועבר אישור בדיקת תקינות הגנרטור מ-27.4.14, אולם באישור צוין כי "הבדיקה בוצעה לגנראטור ללא בדיקת עומס וללא בדיקת מערכת ההחלפה והמערכות הנלוות והנתמכות על ידי הגנרטור". כלומר, חרף חשיבותה של בדיקת העומס ובדיקת מערכת ההחלפה והמערכות הנלוות - הן לא נבדקו. לדברי מנהל אחזקת בניין העירייה, מתבצעות בדיקות עומס, אך לא צורף לכך תיעוד. הביקורת מצאה כי בעת הפסקת חשמל שהייתה בבניין באוקטובר 2014, הגנרטור לא פעל, וכתוצאה מכך, התחמם חדר השרתים.

5.4 ניהול ואבטחה של אמצעי אחסון

בעירייה אין נהלים או הנחיות לאחסון ולטיפול במצעים (media), למעט ההוראה שבסעיף 6(א) לנוהל עירוני לאבטחת חומרה ותוכנה, לפיה **"אין להשתמש בתקליטור או ב-**DISK ON KEY **להעברת מידע אלא באישור ממונה מקצועי ישיר"**. העובדים אמנם הונחו בדבר האיסור להשתמש בהתקן נייד להעברת מידע, אך נמצא כי לא קיים ניטור על שימוש בהחסן נייד על מנת לוודא את יישום ההוראה בפועל.

6. גיבוי, שחזור והתאוששות מאסון

6.1 גיבוי ושחזור

א. בנוהל מספר 28 בנושא "גיבוי ושחזור מידע" מוגדר "גיבוי" כ**"עותק זהה של המידע, שנכתב על גבי מצע נוסף"** וכן **"פעולת ההעתקה של המידע למצע נוסף"**.
נוהל זה ממליץ כי **"האחראי על גיבוי ושחזור יכין נוהל עבור כל סוג גיבוי"**.
נמצא כי אין בעירייה נוהל בנושא גיבויים. לדברי מנהל האגף, הנוהל נמצא בהכנה.

ב. בדיקת הביקורת העלתה כי המערכות הממוחשבות מגובות באופן יומי, ומדי שבוע נשלחות קלטות הגיבוי לאתר מרוחק.

6.2 התאוששות מאסון

א. נוהל מספר 29 לנוהלי המסגרת בנושא "תכניות התאוששות מאסון" (DRP-Disaster Recovery Planning) עוסק בהגנה על תהליכים קריטיים מהשפעת כשלים רציניים או מקרי אסון. המטרה היא להקטין נזקים במקרה אסון, להקטין הוצאות ביטוח ולהגביר מודעות להגנת המערכות.

לפי נוהל זה, תכנית התאוששות תתייחס בין היתר לכך ש"**ממונה אבטחת מידע, בתאום עם מנהל יחידת מחשב, להכין תכנית כתובות מפורטות לתפעול והתאוששות. "העתקי תכנית ההתאוששות יימצאו אצל מנהל יחידת המחשב ואצל ממונה אבטחת המידע.**

"תכנית ההתאוששות תיקח בחשבון את הערכות יחידות המשרד כולן ואת הקשר בין המחשב המרכזי ליחידות השונות אחרי פגיעה חמורה. ההתייחסות לא תהיה רק ליחידת המחשב, אלא גם לאופן הפעילות הרלוונטית ביחידות המשרד מאז הפגיעה ועד לפתרון הקבע."

הנוהל ממליץ על הכנת תכניות התאוששות שיפותחו על ידי צוות היגוי.
נמצא כי העירייה טרם הכינה תכנית להתאוששות מאסון.

ב. לפי נוהל מספר 29, יוגדר אתר חלופי כתשובה לתרחיש של אסון מלא שלא יאפשר כלל להשתמש באתר הקבוע.
לדברי מנהל האגף, קיים אתר חלופי ל-25 שרתים בחברה לביטחון וסדר ציבורי, אליו מועבר מידע מדי יום, הכולל את כל המערכות, מלבד מערכת גבייה ודואר אלקטרוני.

ג. עוד נכתב בנוהל כי אחת לשנה ייערך תרגול מקיף של **כלל** היבטי התכנית ותחומיה: "**מהלכו של התרגיל יתועד על ידי ממונה אבטחת מידע, אשר בסופו של התרגיל יפיק דוח סיכום תרגיל. ממצאיו יועברו לדיון בישיבת ההיגוי בנושא אבטחת מידע, המסקנות יתועדו, יוטמעו ויתורגלו כנדרש**".
לדברי מנהל האגף, נערך תרגיל התאוששות מאסון. נכון למועד הפצת טיוטת הממצאים, בקשת הביקורת לקבל העתק מתיעוד התרגילים שנערכו בשנים 2013-2014 נענתה בסיכומי דיונים ממאי 2014 שערכו עובדי האגף בנוגע להכנת התרגיל. לא נתקבל תיעוד למידע ששוחזר, מועד השחזור והשרתים ששוחזרו. נוסף על כך, מהסיכומים עולה כי לא בוצעה השבתה הלכה למעשה של שרתים לשם בחינה כי מערך הגיבוי אכן פועל כנדרש.

6.3 אבטחת מידע במחשבים ניידים ובמחשבים אישיים

א. נוהל מספר 30 לנוהלי המסגרת בנושא "אבטחת תוכנה וחומרה במחשבים אישיים" קובע כי יש לשמור את הקבצים השונים במחיצות היחידתיות והאישיות שהוקצו לכל משתמש ברשת המחשבים.
יועץ הביקורת הצליח להתחבר למחשב אישי בסמוך לאגף המחשוב, באמצעות חיבור ישיר לכונן הקשיח ולהדפיס מסמכים שונים. זאת, היות שהעובד המשתמש בתחנה שמר מסמכים על הכונן המקומי, ולא רק בשרתי העירייה, כפי שנדרש בנוהל.

ב. נוהל מספר 31 לנוהלי המסגרת בנושא "אבטחת מידע במחשבים ניידים, palm pilot ודיסקים נתיקים" ממליץ בין היתר כי מחשב נייד יהיה מוגן (מבחינת הפעלה) בסיסמאות בהתאם לנוהל העוסק בסיסמאות. חיבור המחשב לרשת התקשורת של המשרד יתבצע רק לאחר וידוא קיום מתמשך של אמצעי הגנה הולמים במחשב וברשת המשרד.

נמצא כי במחשבים הניידים של בכירי העירייה נדרשת סיסמה בעת ההתחברות.
כמו כן, למשתמשים קיימת חסימה (מערכת F5) להעברת נתונים מקומיים מהמחשב אל התחנה המרוחקת. נכון למועד הפצת טיוטת הממצאים, בקשת הביקורת לקבל צילום מסך ממערכת המציגה את החסימה הנ"ל טרם נענתה.

7. אבטחת תקשורת ושימושי אינטרנט

7.1 אבטחת תוכנה ברשתות מקומיות

א. לפי נוהל מספר 32 בנושא "אבטחת תוכנה ברשתות מקומיות", יש צורך למנות מנהל רשת שתפקידו יהיה לנהל ולתפעל בין היתר, את כלי האבטחה של הרשת.
נמצא כי מונה אחראי רשת בעירייה.

ב. ברשת המקומית (שרתי ניהול הרשת ובתחנות) של העירייה מותקנת מערכת NAC אשר מונעת גישה של מחשבים שאינם מוגדרים כמחשבי העירייה. כמו כן, קיימת בקרה האחראית על כך שבמקרה של חיבור מחשב לא מורשה לרשת, נקודת הרשת תתנתק, ולמנהל הרשת ידווח כי בוצע ניסיון לחיבור מחשב שאינו מורשה. הנקודה תחזור להיות פעילה אך ורק לאחר שמנהל הרשת יבצע תיקוף לנקודה.
כמו כן, מותקנת מערכת שמטרתה חסימת ניסיון כניסה לרשת ללא הרשאה מתאימה, ושליחת הודעה אוטומטית לממונה על אודות התחברויות וניסיונות התחברות לרשת.
שני ניסיונות יועץ הביקורת להתחבר לנקודות תקשורת (בבניין העירייה ובמשרדי המינהל לשילוב חברתי הממוקמים מחוץ לבניין העירייה) באמצעות מחשב נייד לא צלחו - כשלוש דקות לאחר חיבור המחשב לנקודות בוצע ניתוק אוטומטי של התקשורת, ומעמדות המחשב מהן נעשו ניסיונות החדירה לא ניתן היה להתחבר לרשת המקומית.

ג. יועץ הביקורת ביצע סריקה חיצונית שטחית של כתובות הרשת החיצוניות של העירייה על מנת לזהות פגיעות אפשריות מבחוץ ללא גרימת נזק או מניעת שירות.
להלן הממצאים:

1) בבדיקה חיצונית ללא ידע מוקדם התגלו פרטים בסיסיים על מבנה התקשורת והשרתים בעירייה. מתוך הנתונים הראשוניים שהתגלו ניתן היה להמשיך בבדיקות מעמיקות יותר ולגלות את שרתי הדואר, נותני שירותים חיצוניים ואת הכתובות החיצוניות של העירייה כולה. ניתן להסיק כי מבנה התקשורת והשרתים בעירייה הוא מורכב ובנוי במתודה היגיונית עם התייחסות לסיכונים חיצוניים ושימוש בהגנות רלוונטיות ברמת חומרה ותוכנה. נגישות המערכות הפנים-ארגוניות של העירייה אינה מידית ונדרש מאמץ ותכנון מכוון על מנת להיכנס ולהגיע למידע. עם זאת, נמצאו פרצות הן ברמת אתר האינטרנט והן ברמת גישה חיצונית לתקשורת של מערכות העירייה עצמה שדרכן יש יכולות להעמיק ולהגיע אל תוך הארגון. יועץ

הביקורת לא המשיך בניסיונות החדירה משלב זה על מנת שלא לגרום נזק למערכות הממוחשבות (ניתוק המערכת).

<u>תגובת מנהלת מרכז מידע ומחקר</u>:

"אתר האינטרנט אינו יושב בשרתי העירייה אלא בשרתי החברה לאוטומציה, לכן אבטחת האתר באחריותה. עלי לציין שמאז שאני מנהלת את האתר (2009) לשמחתנו לא הייתה פריצה כלשהי. החברה לאוטומציה נוקטת באמצעים מקדימים לטיפול בהאקרים כולל השבתה של האתר. עם זאת, אעביר את המידע הזה לחברה לאוטומציה."

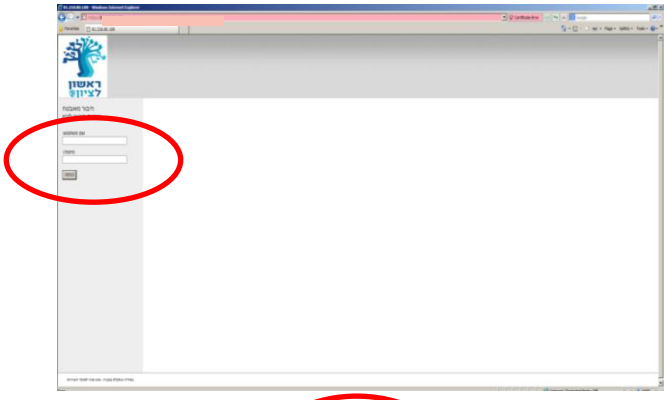
2) התגלה קישור מחוץ למערכת הפנימית של העירייה:

המשמעות היא שהתגלה מידע רב על אודות הרשת העירונית שרצוי שלא יהיה גלוי.

כמו כן, התגלה קישור חיצוני למערכת הדואר העירוני:

יש לציין כי במצב בו הגישה לדואר מתאפשרת מחוץ לארגון, קיימת אפשרות לפצחנים (האקרים) עם כוונת זדון לחדור לתיבת דואר אלקטרוני של עובד כלשהו.

להלן המסכים של המערכת הפנימית אליהם נחשפה הביקורת באמצעות כניסה ממערכת חיצונית:



להלן המקרים אליהם נחשף יועץ הביקורת (כתובות ה-IP[9] של כל אחד מהמקרים שבלוח הוצגו למנהל האגף):

	זיהוי מצבו בסריקה	שם פרוטוקול	פרוטוקול
	open	http	tcp
Checkpoint	open	fw1-topology	tcp
	open	https	tcp
	closed	isakmp	tcp
	open	http	tcp
Checkpoint	open	fw1-topology	tcp
	closed	isakmp	tcp
	open	https	tcp
	closed	isakmp	tcp
Checkpoint	open	fw1-topology	tcp
	open	https	tcp
	open	http	tcp
SMTP error	open	smtp	tcp
SMTP error	open	smtp	tcp
	open	http	tcp
	open	http	tcp
Microsoft	open	http	tcp
	filtered	rmiactivation	tcp
ISC BIND 9	open	domain	tcp
Apache htt	open	http	tcp
	open	snmp	tcp
Apache htt	open	http	tcp
	filtered	ams	tcp
	filtered	cplscrambler-al	tcp
OpenSSH 4.	open	ssh	tcp
	filtered	rmiregistry	tcp
	filtered	caspssl	tcp
	filtered	sddp	tcp
	filtered	ms-sql-s	tcp

[9] זיהוי מחשבים ברשת העירונית.

פרוטוקול	שם פרוטוקול	זיהוי מצבו בסריקה	
tcp	dectalk	filtered	
tcp	amiganetfs	filtered	
tcp	tvbus	filtered	
tcp	deslogin	filtered	
tcp	mysql	filtered	
tcp	nati-svrloc	filtered	
tcp	unknown	filtered	
tcp	parsec-master	filtered	
tcp	imqbrokerd	filtered	
tcp	http	filtered	
tcp	simplifymedia	filtered	
tcp	unknown	filtered	
tcp	msgsys	filtered	
tcp	unknown	filtered	
tcp	unknown	filtered	
tcp	unknown	filtered	

משמעות המידע המופיע בלוח היא שברשות הפצחן יש נתונים על אודות כתובות מחשבי העירייה העלולים לסייע לו בניסיונות פריצה.

<u>תגובת מנהל האגף</u>:

"הכתובות המוצגות בטבלה הנן חיצוניות ואפשרות הפריצה דרך כתובות אלו הנה קלושה. בכל מקרה פנינו ליצרן לחשיפה מוקטנת של הנתונים המוצגים.

"...האתר של העירייה ממוקם בחברה לאוטומציה והוא מנותק מהרשת העירונית.

"הקישור למערכות הפנימיות בעירייה מאובטח באמצעות SSLVPN של מוצר F5 כולל גישה רק לאחר קבלת SMS למכשיר העובד - אין סיכון בחשיפת הכתובת המצורפת, זו כתובת חיצונית בלבד.

"הקישור למערכות הדואר הנו מפורסם עבור כלל עובדי העירייה לגישה לתיבת הדואר לאחר שעות העבודה, והנו חלק ממדיניות העירייה. אנו מגבילים את ניסיונות הגישה לתיבה אשר מגבילים את אפשרות 'הפצחנים' לפריצה באופן משמעותי."

לדעת הביקורת, האחריות לאבטחת האתר היא בראש ובראשונה של מנהל האגף, אף אם הכתובות ממוקמות בחברה לאוטומציה. חשיפת הכתובות מקלה על גורם עוין בפריצה למאגרי העירייה וניתן למנוע זאת באמצעות

חסימת גישה לכתובות IP. הגבלת ניסיונות הגישה היא אכן בקרה מהותית, אך יש לשקול מניעת גישה כאמור לגורם חיצוני.

3) באתר האינטרנט של העירייה נמצאו פרצות המאפשרות גישה לאזורים מסוימים. יועץ הביקורת לא ביצע ניסיונות פריצה בפועל, אך לפי רמת המוגנות, ההערכה היא כי פריצה הייתה מתאפשרת במהירות יחסית גבוהה.

4) יועץ הביקורת שלח למספר מנהלים בעירייה דואר אלקטרוני שכלל קובץ המכיל תוכנה זדונית המאפשרת לקבל שליטה מרחוק על מחשבי הארגון. נמצא כי הקבצים אמנם נפתחו, אך התוכנה הזדונית נחסמה באמצעות מערכת סינון הדואר.

7.2 אבטחת מידע בשימוש באינטרנט

א. קישור לא מאובטח לאינטרנט טומן בחובו סכנות חמורות לתפקודם התקין של מערכי המידע. לדברי מנהל האגף, במערכות העירייה הותקנו כלים טכנולוגיים חדישים עליהם המליצה החברה המייעצת לאבטחת הגלישה באינטרנט ולהגנת הדואר האלקטרוני: מערכת "חומת אש", WEBSENSE, מערכת אנטי-וירוס ועוד.

ב. לביקורת הועבר צילום מסך ממערכת אנטי-וירוס, ונמצא כי הוא מעודכן ליום הבדיקה. עדכון התוכנה חיוני היות שבכל יום מעדכן ספק שירותי האנטי-וירוס את מלאי הוירוסים אותם התוכנה מסוגלת לגלות/למנוע.

ג. תפקיד מערכת "חומת אש" הוא למנוע חדירה לרשת של גורמים מחוץ לארגון, לרבות באמצעות רשת האינטרנט. מערכת זו מונעת את הכניסה הבלתי-מורשית באמצעות כללים שיש להגדירם למערכת. בנוהל מספר 34 בנושא "אבטחת מידע בשימוש באינטרנט" נכתב כי השימוש במערכת "חומת האש" צריך להתבצע ביוזמת מנהל האגף ובסיוע של יועץ מקצועי בכיר.
נכון למועד הפצת טיוטת הממצאים, טרם נענתה בקשת הביקורת לקבל אסמכתא לכך שמנהל האגף אישר את הכללים שהוגדרו למערכת "חומת האש".

<u>תגובת מנהל האגף</u>:
"הקמת מערכת 'חומת אש' הייתה ביוזמת מנהל האגף תוך שיתוף פעולה מלא עם החברה המייעצת לנושא החוקים המתופעלים בשוטף על ידם. הקמה וביטול של חוקים במערכת 'חומת אש' הנם של החברה המייעצת מול האינטגרטור שמתחזק את המכונה. כל חוק עובר לידיעתי."

יש להעיר כי לביקורת לא הועבר תיעוד לבקרה הנעשית בידי מנהל האגף. מומלץ כי תיערך ותתועד בחינה תקופתית של כלל החוקים במערכת.

7.3 השתלטות מרחוק

בנוהל מספר 36 בנושא "התקנה ואבטחה של תוכנות השתלטות מרחוק" נכתב:
"לצורך השתלטות על המחשב המארח חייבים להפעיל את אפשרויות האבטחה הקיימות בתוכנת השתלטות מרחוק... שם משתמש... סיסמא בת 6 תווים לפחות, עפ"י ההנחיות שיוגדרו... הפעלת אפשרות ניתוק לאחר חוסר פעילות של פרק זמן שיקבע ע"י הממונה אבטחת מידע... הפעלת יומן LOG של פעילות המתבצעת באמצעות תוכנת ההשתלטות."

הוראות דומות נקבעו בנוהל עירוני לאבטחת מידע.

נמצא כי לכל התחברות של ספק מרחוק נדרש אישור עובד טכני של האגף וכן הזנת שם משתמש וסיסמה. כמו כן, המערכת מבצעת ניטור על התקשרויות מרחוק של ספקים, כך שבגין כל התקשרות מרחוק נשלח דואר אלקטרוני למנהל האגף.
הביקורת קיבלה דוח ניטור ספקים מחוץ לעירייה עבור חודש אוקטובר, המכיל 298 כניסות של ספקים ועובדים. מדוח הניטור עולה כי מרבית כניסות הספקים שייכות לחברת מ.ל.מ. ולחברת טלדור המעניקות תמיכות למערכות העירייה.

עיקרי הממצאים[10] ומסקנות

1. נוהלי העבודה העירוניים אינם כוללים את כל תהליכי העבודה המומלצים לפי נוהלי המסגרת ואת המלצות מבקר העירייה בדוח 28. כמו כן, הם אינם מעודכנים בהתאם לתהליכים המבוצעים בפועל.
2. התנהלות האגף בתחום אבטחת המידע ללא מסמך "מדיניות אבטחת מידע רגיש" וללא נהלים מקיפים ומעודכנים, אף לאחר כשנתיים מתחילת עבודה עם חברה מייעצת לנושא, פוגעים בהטמעת נושא אבטחת המידע, הן בקרב עובדי האגף והן בקרב המשתמשים. בהסכם שנחתם עם החברה המייעצת פורטו התחייבויותיה, אך בפועל היא טרם נדרשה לבצע את כל המשימות.
3. לא מונתה ועדת היגוי לעניין אבטחת מידע ולא הוגדר גורם ניהולי בכיר בעירייה האחראי על הממונה על אבטחת מידע. הביקורת רואה חשיבות בהגדרת גורמים אלו הן בקביעת מדיניות ושיתוף פעולה כלל עירוני (באמצעות השתתפות הרפרנטים ליישומים השונים ביחידות העירוניות בוועדת היגוי) והן בבקרה ופיקוח על הגורמים המעורבים בתהליך ופיקוח על יישום המדיניות שתיקבע.
4. אחד ממאגרי המידע העירוניים לא דווח למנהלת מרכז מידע ומחקר, וכתוצאה מכך לא נרשם אצל רשם מאגרי המידע במשרד המשפטים, בניגוד לסעיף 8ג לחוק הגנת הפרטיות.
5. לא בוצעו סקרי אבטחת מידע שמטרתם להעריך את הסיכונים כשלב מקדים בעיצוב מדיניות אבטחת המידע.
6. עובדי העירייה לא עברו הדרכות בנושא אבטחת מידע. אי-ביצוע הדרכות תקופתיות למשתמשים ו/או העלאת המודעות לנושא באמצעות שימוש בכלים הקיימים כדוגמת הפורטל העירוני היו מסייעים בהטמעת נושא אבטחת המידע בקרב המשתמשים.
7. נוסח תצהיר הסודיות עליו חותם עובד חדש אינו כולל הסברים בדבר הוראות החוק הרלוונטיות ואינו כולל סנקציות במקרה של אי-ציות להוראות התצהיר עליו חתם.
8. מנהל האגף אינו מנהל רשימת גורמים המורשים להגיש בקשה לעדכון/פתיחת משתמש ברשת העירונית. הליך הסרת פרטי עובד מהמערכות מתבסס על קבלת דואר אלקטרוני הכולל את פרטי העובד, ללא פירוט ההרשאות שיש להסיר. כמו כן, לא נערך מיפוי של כל

[10] בגוף הדוח מובאים ממצאים נוספים שלדעת הביקורת על מנהל האגף ליישם כחלק ממדיניות אבטחת מידע בעירייה, כגון: ניטור שימוש בהחסן ניייד, סיווג המערכות לפי רמת סודיות וחיוניות ומינוי "בעלים" למערכות וביצוע תחקירים לעובדים בתפקידים שיוגדרו "רגישים".

ההרשאות שניתנו למשתמשים במערכות העירוניות, לרבות משתמשי-על. בקרה תקופתית אחר תקינות ההרשאות תקטין את הסיכון לביצוע פעולות בידי לא מורשים.

9. לדעת הביקורת, מדיניות הסיסמאות הקיימת בחלק מהמערכות (כגון: מערכת קומפלוט ונמ"ר) היא קלה לפיצוח וקיים סיכון ממשי לכניסת משתמשים לא מורשים למערכות רגישות אלו.

10. לא הוגדרו אירועי אבטחת מידע חריגים ולא נשמרו "לוגים" לתנועות. המשמעות היא שיש פגם בבקרה על איתור ותחקור אירועי אבטחת מידע.

11. לא קיימת הקפדה על הגנת אמצעי המחשוב: סגירת דלת חדר השרתים, סגירת ארון תקשורת ובדיקה כי הגנרטור בחדר השרתים נותן מענה במקרה של הפסקת חשמל.
הליך מלא של השבתת שרתים והעלאת הגיבויים מאתר מרוחק לא התבצע בשנת 2014.
תרגיל שנתי של תכנית התאוששות מאסון הוא חיוני לבחינת תקינות כלל גורמי הגיבוי/השחזור הקיימים בעירייה.

<u>תגובת מנהל האגף</u>:
"דלת חדר השרתים סגורה ומאופשרת ע"י כרטיס עובד עירייה בלבד.
חדרי התקשורת הקומתיים נעולים ואין גישה מעבר לעובדי התקשורת בתקשוב ואנשי תחזוקת הבניין.
גנרטור הבניין נכנס לפעולה באופן אוטומטי - הנושא נבדק מספר פעמים.
לא בוצע הליך מלא של השבתת שרתים היות ואתר ה-DR הוקם רק ב-2014, תרגיל מקיף מתוכנן רק לאמצע 2015."

12. ניסיונות הביקורת לחדור למערכת העירונית מחוץ לעירייה לא צלחו. עם זאת, פעולות הביקורת העלו כי גורם המבצע חדירה למערכות העירייה מחוץ למחשבי העירייה חשוף למידע רב על מבנה רשת המשתמשים. מידע זה עשוי לסייע לפצחן בחדירה לרשת העירונית (הביקורת לא המשיכה בניסיונות החדירה על מנת שלא לגרום נזק למערכות העירייה).

המלצות

1. יש לסיים את כתיבת הנהלים העירוניים ולעדכן את הקיימים. הנהלים יתייחסו בין היתר לגיבויים, לשימוש בנתונים, לבעלי תפקידים ותחומי אחריותם, לעריכת סקרי סיכונים לעניין אבטחת מידע, למדיניות סיסמאות, לאחסון וטיפול במצעים, לבקרות אבטחה פיזיות ולטיפול באירוע אבטחת מידע.

   ✓ בישיבת הצוות לתיקון ליקויים דווח כי ההמלצה מבוצעת.

2. הממונה על אבטחת מידע יעמוד בראש ועדת היגוי לנושא אבטחת המידע אשר תגדיר את בעלי התפקידים העיקריים לניהול הנושא בעירייה ותדון בנתונים, כדוגמת ממצאי סקר סיכונים ותקבע מדיניות. בהתאם לצורך, ישתתפו בישיבות הוועדה גם הרפרנטים ליישומים השונים ביחידות העירוניות. הממונה על אבטחת מידע יעביר את המלצותיו

לידיעת ראש העירייה והמנכ"ל, וידווח על אודות התהליכים המבוצעים ואלו שיבוצעו, כולל לו"ז לביצוע.

- ✓ בישיבת הצוות לתיקון ליקויים דווח כי ההמלצה תבוצע.

3. יש לוודא כי כל מאגרי המידע ידווחו ויירשמו אצל רשם מאגרי המידע במשרד המשפטים.

- ✓ בישיבת הצוות לתיקון ליקויים דווח כי ההמלצה מבוצעת.

4. מנהל האגף יקבע לו"ז לביצוע כל המשימות שהתחייבה החברה המייעצת לבצע לפי ההסכם וטרם נדרשה לבצען. לדעת הביקורת, יש לייחס חשיבות לביצוע סקר סיכונים שימפה את התהליכים ואת סיכויי ההיקרות של כל אחד מהם והנזק העלול להיגרם עקב כך, וכן לגיבוש מדיניות אבטחת מידע וכתיבת מסמך "מדיניות אבטחת מידע" שיוטמע בקרב העובדים.

- ✓ בישיבת הצוות לתיקון ליקויים דווח כי ההמלצה מבוצעת.

5. יש להוסיף לנוסח תצהיר הסודיות עליו חותם עובד חדש את סעיפי החוק הרלוונטיים, הנחיה כי חובותיו חלות גם מחוץ לכותלי העירייה וכן סנקציות שיוטלו עליו בגין אי-עמידה בדרישות אבטחה אלו.

- ✓ בישיבת הצוות לתיקון ליקויים דווח כי ההמלצה תבוצע.

6. יש להעביר הדרכות תקופתיות בנושא אבטחת מידע לכלל עובדי העירייה, או לחילופין, יפורסמו בפורטל העירוני הנחיות בכתב לשימוש במערכת.

- ✓ בישיבת הצוות לתיקון ליקויים דווח כי ההמלצה מבוצעת.

7. יש לשקול פנייה לבתי התוכנה האחראיים על יישומי תוכנה לשם התאמת מדיניות סיסמאות ליישומים השונים לדרישות נוהלי המסגרת.

- ✓ בישיבת הצוות לתיקון ליקויים דווח כי ההמלצה בוצעה.

8. מנהל האגף ינהל רשימת גורמים המורשים להגיש אליו בקשה לעדכון/פתיחת משתמש ברשת העירונית וכן מאגר מידע ממוחשב של הרשאות למסכים ולמערכות עבור כל משתמש. הרפרנטים של המערכות ימפו את המשתמשים, לרבות משתמשי-על, כך שלאגף תועבר רשימה מעודכנת לאחר אישור הממונים הישירים. לאחר מכן, יופק דוח הרשאות תקופתי שיועבר לאישור הממונים הישירים בהתאם לעקרון "הצורך לדעת".

- ✓ בישיבת הצוות לתיקון ליקויים דווח כי ההמלצה מבוצעת.

9. מנהל האגף ואגף משאבי אנוש במינהל כוח אדם ואמרכלות יבחנו את הליך הדיווח בנוגע להסרת הרשאות משתמשים שסיימו עבודתם בעירייה, לרבות התייחסות לבקרות הנדרשות על מנת לוודא שאכן הוסרו כל ההרשאות שניתנו לעובדים אלו.

- ✓ בישיבת הצוות לתיקון ליקויים דווח כי ההמלצה תבוצע, וכן ש"אחת לשנה תיערך בדיקת חריגים".

10. מנהל האגף והחברה המייעצת יגדירו מהו אירוע אבטחת מידע ויפעלו ליישום כלי אבטחת מידע שיבטיחו תחקור מלא של אירוע כזה. כמו כן, יוגדרו המערכות כך שישמרו יומן תנועות (LOG) שינותח אחת לשבוע באמצעות כלים ממופנים. ממצאים חריגים מהניתוח, לפי ההגדרה הנ"ל, יועברו לבירור הממונה על אבטחת מידע.

- ✓ בישיבת הצוות לתיקון ליקויים דווח כי ההמלצה תבוצע.

11. יש לערוך תכנית התאוששות מאסון ולערוך תרגול לנושא זה שיתייחס להשבתת שרתים מרכזיים, העלאת מידע מקלטות ועבודת משתמשים לאורך זמן מהאתר המרוחק.

- ✓ בישיבת הצוות לתיקון ליקויים דווח כי ההמלצה תבוצע.

12. מנהל האגף והחברה המייעצת יבחנו את החשיפה לחדירה למערכות העירוניות מחוץ למחשבי העירייה ואת הדרכים למניעתה.

- ✓ בישיבת הצוות לתיקון ליקויים דווח כי "יבוצעו בדיקות באמצעות חברה חיצונית נוספת".