אבטחת מידע

כללי

1. דוח זה הוא דוח מעקב אחר יישום החלטות שהתקבלו בדו"ח ביקורת, מס' 35, לשנת 2006 שעסק בנושא אבטחת מידע (להלן דו"ח ביקורת 2006).

2. מטרת הביקורת:

   א. מעקב יישום החלטות שהתקבלו על סמך דו"ח הביקורת שנערך בשנים 2006/7;

   ב. בדיקה מעמיקה של יחידת אבטחת המידע - תכניות, משימות, סמכויות, שיטת ביצוע, בקרה וכו';

   ג. ביקורת על פעילות הערכת סיכונים;

   ד. ביקורת על תחקור אירועי אבטחת מידע - שיטות ויישומים;

   ה. בדיקת אופן תיעוד נהלי סיווג מידע ואבטחתו;

   ו. תיעוד מערכות קיימות- חומרות, תוכנות, גיבויים וכו'.

3. איסוף הממצאים לדוח הביקורת כלל: עיון בנתונים ומסמכים שונים, ראיונות עם בעלי תפקידים באגף המחשוב.

4. איסוף הממצאים לדוח הביקורת בוצע במהלך שנת 2011.

ממצאים

העלאת נושא אבטחת מידע בסדר הקדימויות הארגוני

בדיון שהתקיים בנושא בחודש אפריל 2007, קבע מנכ"ל העירייה כי "**אבטחת מערכות מידע הוא נושא בעל חשיבות עליונה ויש להעלות את רמת הקדימות שלו בסדר העדיפויות העירוני**", לצורך בחינת יישום המלצה זו מדו"ח קודם, הביקורת בחנה את היקף התקציב שהוקצה לאבטחת מידע ואת היקף כ"א העוסק באבטחת מידע.

תקצוב אבטחת מידע

5. על פי דו"ח אבטחת מערכות מידע, מס' 35, לשנת 2006, התקציב הישיר לצורך אבטחת מידע היווה בשנת 2006, כ 1.8% מהתקציב הכולל של האגף לאותה שנה. המלצת הביקורת היתה כי יש להפריד בין תקציב אבטחת מידע לבין התקציב הכולל של האגף. ממידע שנמסר לביקורת על ידי בוחן תקציבים באגף תקציבים וכלכלה בתאריך 13.6.11 עולה כי במסגרת התקציב השוטף והתקציב הבלתי רגיל נקבעו סעיפי תקציב ייעודיים לאבטחת מידע, כדלקמן:

במסגרת התקציב הרגיל (שנת 2010)

א.

סעיף התקציב	פירוט	תקציב מקורי	תקציב מעודכן
01-99341-751-2	"אבטחת מידע"	560,000	816,000

הסעיף הנ"ל מיועד להעסקת נש"מים ויועצים בתחום זה.

ב.

סעיף התקציב	פירוט	תקציב מקורי	תקציב מעודכן
01-99328-754-1	"אבטחת מידע"	350,000	350,000

הסעיף הנ"ל מיועד בעיקר להעסקת נש"מים ויועצים בתחום זה במסגרת פרויקט המחו"ג.

ג. בנוסף כלל התקציב הקצבה לנושא שכירות ואחזקת תוכנה בשנה זו (סעיף 01-99331782), על פי הפירוט להלן:

שם החברה	נושא/ציוד	אומדן להוצאה בשנה"ע 2010 (בש"ח כולל מעמ)
טו בי סקיור	FIREWALL	23,000
משרד המשפטים	אגרה לבעלי מאגרי מידע	5,000
מכון התקנים הישראלי	תקליטור א"מ	1,000
טו בי סקיור	ESAFE	89,000

ד. כמו כן כלל התקציב הקצבה לנושא שכירות ואחזקת ציוד בשנה זו (סעיף 01-99331783), על פי הפירוט להלן:

שם החברה	נושא/ציוד	אומדן להוצאה בשנה"ע 2010 (בש"ח כולל מעמ)
טו בי סקיור	קופסא לא"מ	23,000
טו בי סקיור	קופסת פרוטגריטי לא"מ	26,000
טו בי סקיור	צ'קפוינט אדג' 16	1,000

ה. במסגרת התקציב הרגיל מתוקצבים עובדי עירייה. [1] עלות עובדי אחזקת מידע, כפי שהיא מופיעה בספר התקציב, נכללת בעלות השכר הכולל של ענף ארכיטקטורה.

<u>במסגרת התקציב הבלתי רגיל (שנת 2010)</u>

ו.

סעיף התקציב	פירוט	מקורי	תוספת בשנת 2010
02-009312-200-3	"אבטחת מידע"	145,921	755,000

הסעיף הנ"ל מיועד לרכישת חומרה, תוכנה ולהעסקת יועצים לפיתוח בתחום זה.

כמו כן, במסגרת סעיף תקציב בלתי רגיל 02-009316-220-5, המיועד לפיתוח המחו"ג, נכלל סכום כספי שיועד למימון אבטחת מידע בפרויקט זה. רכזת פיקוח תב"ר מסרה לביקורת כי בשנת 2010 הוצא מתוך תב"ר שת"פ ארנונה סכום של 697,325 ₪ לטובת פיתוחים בנושאי אבטחת מידע בפרויקט מחו"ג.

6. הביקורת בחנה את סעיפי התקציב לתקופה: 2008 - 2011 להלן עיקרי הממצאים:

7. אגף מחשוב ומערכות מידע (פרק מס' 993 בהצעת התקציב הרגיל)

שנה	תקציב מתוכנן	אחוז הגידול בכל שנה ביחס לשנה קודמת
2008	65,880,000	
2009	72,800,000	10.50 %
2010	86,270,000	18.50 %
2011	94,290,000	9.29%

א. ענף ארכיטקטורה באגף מיחשוב ומערכות מידע (פרק מס' 9934 בתקציב הרגיל):

שנה	תקציב מקורי	אחוז הגידול בכל שנה ביחס לשנה קודמת
2008	8,520,000	
2009	8,870,000	4.10%
2010	9,550,000	7.66%
2011	10,998,000	15.16%

[1] לביקורת לא נמסרו נתונים לגבי עלות המשכורת הכוללת של עובדי אבטחת מידע בין השנים 2008-2011.

ב. אבטחת מידע בסעיף ארכיטקטורה (פרק מס' 2-751 בתקציב הרגיל):[2]

שנה	תקציב מקורי	אחוז הגידול בכל שנה ביחס לשנה קודמת
2008	657,000	
2009	665,000	1.2%
2010	560,000	-15.79%
2011	980,000	75%

ג. אבטחת מידע בסעיף מערכת חיוב וגביה (פרק מס' 1-754 בתקציב הרגיל):

שנה	תקציב מקורי	אחוז הגידול בכל שנה ביחס לשנה קודמת
2008	סעיף לא קיים בתקציב	
2009	סעיף לא קיים בתקציב	
2010	350,000	
2011	530,000	51.42%

כח אדם ביחידת אבטחת מידע

על פי נתוני דו"ח מס' 35, בנושא אבטחת מידע משנת 2006, ליחידת אבטחת מידע נקבעו שישה תקני כ"א שאוישו על ידי חמישה עובדים קבועים ויועץ חיצוני. בשנת 2010 נוספו ליחידה 3 עובדים, אחד מהם פועל בפרויקט המחו"ג בלבד.

כמו כן, על פי מידע שנמסר לביקורת על ידי מנהל יחידת אבטחת מידע בתאריך 29.6.11, נוספו כ- 500 שעות עבור עבודת יועצים חיצוניים.

ממידע שנמסר על ידי מנהל אבטחת מידע נמצא כי נכון לחודש יולי 2011, בהשוואה לשנת 2010 חל גידול בהיקפי העבודה של אבטחת מידע, להלן:

נתונים השוואתיים	2010	עד יולי 2011	שיעור גידול
מספר קריאות שטופלו ע"י אבטחת מידע	698	776	11%
כמות פניות בדוא"ל		5712	
טפסים (BPM בלבד)		1897	
רכיבים מכוסים ב AV	3,810	4515	19%
חיבורי OWA בו זמנית		כ- 500 ליום	
הנפקת טוקנים	360	420	17%
יישומים שנבדקו	20	21	5%

[2] לנתונים אלו יש להוסיף את נתוני כ"א אבטחת מידע.

נתונים השוואתיים	2010	עד יולי 2011	שיעור גידול
מערכות אבטחת מידע	30	36	20%
קווי תקשורת מחוברים דרך היחידה	31	35	13%
בקרות שבוצעו על ידי היחידה	10	18	80%

מדיניות ועקרונות שימוש מאובטח במערכות מידע

8. אחת ההמלצות בדו"ח הביקורת בנושא אבטחת מידע משנת 2006, שהתקבלה על ידי הנהלת העירייה היתה כי: "**על העירייה להגדיר עקרונות שימוש מאובטח במערכות המידע שברשותה. עקרונות אלה מגדירים את אופן השימוש בשרתים, מחשבים ניידים, מחשבים נישאים, ציוד תקשורת וכל ציוד מחשובי אחר המשמש את העירייה לצרכי עיבוד או שמירת מידע**". מבדיקת הביקורת עולה כי נושא אבטחת מידע עוגן במסמך מדיניות בנושא אבטחת מידע, הוגדרו נהלים בנושא, הוגדר תפקידו של ממונה אבטחת מידע, הוגדרו סמכויות ואחריות ליישום המדיניות והוקמה ועדת היגוי.

9. מסמך 'מדיניות אבטחת מידע' אושר באפריל 2007. מטרתו של מסמך מדיניות אבטחת המידע להציג את המדיניות שאושרה על ידי הנהלת העירייה בנושא אבטחת מידע.

במסמך המדיניות פירוט של תחומים שונים והוא כולל, בין היתר, פירוט תחומי האבטחה; מבנה ארגוני לניהול וליישום אבטחת מידע; הגדרה של רמה מחייבת של אבטחת מידע; סמכות ואחריות ועוד.

10. מבדיקת הביקורת עולה כי לא כל התחומים המוגדרים במסמך המדיניות יושמו בתקופת הביקורת. לדוגמה: מבחינת סעיף 5.6 במסמך עולה כי רכזי המחשוב ישמשו כנאמני אבטחת מידע יסייעו לממונה על אבטחת מידע במטלות אבטחת המידע ויונחו על ידו. מבדיקת הביקורת עולה כי נכון לתקופת הביקורת סעיף זה לא מיושם. בתקופת הביקורת (בשנת 2011) נעשה פיילוט במחלקה אחת, בענף פיתוח באגף המחשוב.

ועדת היגוי

11. ועדת ההיגוי לאבטחת מידע מייעצת למנכ"ל העירייה אודות מדיניות אבטחת המידע ומנחה את הממונה על אבטחת המידע בהתאם למדיניות זו.

12. לבקשת הביקורת נמסרו לה פרוטוקולים של ועדת ההיגוי. הפרוטוקול האחרון שנמסר לידי הביקורת הוא מחודש יוני 2009.

בתגובה לממצאים נמסר לביקורת על ידי מנהלת אגף המחשוב ומ"מ כי: **"התקיים כינוס נוסף של הוועדה ב – 14.09.11."**.

נהלים

13. במסמך 'מדיניות אבטחת מידע' נקבע כי הממונה על אבטחת מידע אחראי לפיתוח נהלי עבודה לשם הסדרת פעילות אבטחת מידע, יהיה מעורב בפיתוח כל הנהלים שיש להם השלכה על אבטחת מידע. בנוסף, על העירייה לעגן בחוזה את החלת תנאי אבטחת מידע על כלל המשתמשים החיצוניים, ועל כל יתר הגורמים אשר יש להם מעורבות בפיתוח, תפעול ותחזוקת מערכות מידע בעירייה, לרבות מיקור חוץ.

14. על פי דו"ח הביקורת, מס' 35, בנושא אבטחת מידע משנת 2006 מרבית הנהלים היו בסטטוס של כתיבה, בדיקה ו/או המתנה לאישור. באופן כללי התחייב האגף בעקבות הדו"ח הנ"ל לפרסום 16 - 21 נהלים ועוד כ 30 הוראות עבודה באתר האינטראנט העירוני עד סוף שנת 2007.

15. תהליך אישור הנהלים: הביקורת המליצה כי במקרים בהם הנוהל דורש מספר רב ולא סביר של גורמים מאשרים, יש להבחין בין נהלי מיקרו המתייחסים לתהליכי עבודה נקודתיים ובין נהלי מאקרו המתייחסים לתהליכים כלל מערכתיים ומהותיים יותר, ובהתאם לזאת לקבוע את הגורמים הרלונטיים לאישור הנוהל. לביקורת נמסר על ידי הארכיטקט הראשי כי המלצה זו יושמה.

16. מבדיקת הפורטל העירוני בתאריך 9.6.11 נמצא כי בפורטל אגף המחשוב קיימים נהלים, הנחיות עבודה וטפסים בנושא אבטחת מידע, על פי הפירוט להלן:

כתיבה מאובטחת של מערכות אינטרנט ואינטראנט; נוהל הגדרת משתמש חיצוני ברשת העירונית; הצהרת סודיות; הנחיות לצפייה בדואר עירוני מהבית; העברת קבצים לגורם חיצוני; הרשאות גישה למאגרי מידע; נוהל הגדרת משתמש חיצוני ברשת העירונית; ניהול ותפעול מערך הסיסמאות; נוהל להפעלת עובדים חיצוניים; בקשה לפתיחת תיבת דואר יחידתית; נוהל אבטחת מצעי אחסון; נוהל אבטחת מחשבים נישאים; אבטחת אינטרנט ודואל; נוהל אבטחה לוגית; מודעות הדרכה והסברה; דיווח על אירועים חריגים; אבטחת תקשורת ותשתיות; נוהל גיבוי; נוהל ניקוי

תחנה החשודה כנגועה; נוהל אבטחת יישומים; נוהל בדיקתFIREWALL; אבטחה פיזית; מדיניות חיבור גורמים חיצוניים לרשת העירונית; מסמך מדיניות אבטחת מידע עירונית; מסמך מדיניות הנפקת טוקן; טופס הצהרת סודיות; הצהרת סודיות; בקשה מרוכזת להרשאות גישה למאגר.

17. על פי דו"ח הביקורת, מס' 35, בנושא אבטחת מידע משנת 2006 מספר הנהלים הקשורים לאבטחת מידע כלל:

נוהל לשעת חרום למקרה של קריסת מערכות; נוהל הכנסת תוכנה חיצונית ע"י ספק תוכנה רלוונטי; נוהל אבטחת מידע המטפל בניהול, הכנסה, תפעול והוצאה של מידע מהעירייה, כולל מערכות המכילות זכרון נייד כדוגמת מחשבים ניידים וכרטיסי זכרון.

18. הביקורת בחנה 21 נהלים המופיעים בפורטל ולהלן עיקרי הממצאים:

א. בחלק מהמקרים לא ניתן לדעת את תאריכי כתיבת הנוהל ותאריך התוקף שלו משום שהמידע אינו רשום על הנוהל: רק ב- 3 נהלים מתוך 21 נרשם תאריך פרסום ורק ב- 7 נרשם תאריך התוקף של הנוהל.

ב. חלק מהנהלים אינם כתובים בתבנית קבועה לכתיבת נהלים.

ג. חלק מהנהלים אינם עדכניים ו/או אינם מיושמים במלואם. להלן מספר דוגמאות:

הנוהל	**פירוט הפעילות הנדרשת על פי הנוהל**
ניהול ותפעול מערך הסיסמאות העירוני	פקידי משאבי אנוש ורכזי מחשוב ידווחו על עזיבת עובד על מנת לחסום את הגדרות הלקוח שלו.
סעיף 5.3 לנוהל אבטחת אמצעי איחסון	באחריות ממונה אבטחת מידע לנהל רישום של כל האמצעים העירוניים המכילים נתונים עירוניים שהועברו לגורמים חיצוניים.
סעיף 4.4 בנוהל בקשה לפתיחת תיבת דוא"ל יחידתית.	מנהל צוות התמיכה וממונה על אבטחת מידע יפקחו יבקרו ויאכפו את היישום
סעיף 6.1 בנוהל בקשה לפתיחת תיבת דוא"ל יחידתית.	באופן שוטף תיערכנה ביקורות מדגמיות לבחינת יישום ההנחיות המפורטות בנוהל זה.
סעיף 3.3 בנוהל אבטחה לוגית	בנוהל מוגדר כי סביבת העבודה העירונית מורכבת, בין היתר ממחשב מרכזי, mainframe.
נספח א' בנוהל אבטחה	קובע בין היתר כי נוהל זה מטפל בשימוש בקוד לקוח בזמן

הנוהל	פירוט הפעילות הנדרשת על פי הנוהל
לוגית	העדרות עובד. מבדיקת הביקורת עולה כי אין מערכת אשר עושה הצלבה בין שעות עבודה לבין כניסה למערכות העירייה ולכן לא ניתן לאתר פעולות רגישות או חריגות, אלא רק בבדיקה ידנית.
מודעות הדרכה והסברה	בנוהל נקבע כי תפורסמנה הנחיות אבטחת מידע בתלוש המשכורת אחת לשנה.

אחריות מנהלים

19. על פי סעיף 8.3.2 במסמך 'מדיניות אבטחת מידע' מנהלים ישאו באחריות לוודא נקיטת אמצעים לקיום דרישות החוק והתקנות הנלוות, ולוודא יישום ואכיפת הנהלים במערכות שבאחריותם. מבדיקת הביקורת עולה כי לא נעשות פעולות הדרכה ובקרה לבחינת היבט זה.

בתגובה לממצאים מסר מנהל אבטחת מידע לביקורת כי: **"בוצעו מגוון של פעולות הדרכה, לדוגמא – בהנחיית המנכ"ל התקיים כנס מנהלי מחלקות בכנס הוצג נושא אבטחת המידע למנהלים. נושא אבטחת המידע הוצג בפורום מנכ"ל וגם בפורומים אגפיים ומחלקתיים שונים."**.

מודעות והדרכה

20. על פי המלצות דו"ח הביקורת, מס' 35, בנושא אבטחת מידע לשנת 2006 נדרש טיפול מערכתי תוך שילוב מודעות, אחריות מנהלים לאורך המדרג העירוני, לצורך הטמעת החשיבות בקרב העובדים.

21. בנוהל מודעות הדרכה והסברה הנמצא בפורטל אגף המחשוב נקבע בסעיף 3 כי פעם בשנה תתבצענה פעילויות הדרכה בנושא אבטחת מידע לקבוצות עובדים, משתמשי מחשב ו/או לקבוצות שיש להן נגיעה למידע. סעיף זה אף קובע כי הפעילות תתבצע באופן קבוצתי בחלוקה לבעלי תפקידים שונים: מנהלים בכירים, עובדי האגפים השונים וכו'.

22. ממידע שנמסר לביקורת על ידי מנהל אבטחת מידע עולה כי כחלק מיישום המלצות על פי דו"ח, הביקורת, מס' 35, בנושא אבטחת מידע משנת 2006, נעשו פעולות שונות על פי הפירוט הבא:

א. בוצעה הדרכה אחת למנהלי מחלקות והנושא הוצג במספר פורומים של מנהלי מחלקות.

ב. ניתנה הרצאה אחת לפורום מנכ"ל.

ג. נציג מטעם אבטחת מידע נותן הרצאה בכל קורס של העירייה.

ד. הוקם פורטל מידע בנושא.

ה. <u>הדרכת עובדים חדשים</u> – בנוסף, על פי דו"ח סטטוס מיום 5.8.07 לגבי "**איתור אוכלוסיית עובדים שהתחילו עבודתם אחרי 1.1.07 לצורך תיאום הדרכה וביצועה. הדרכה תקופתית לעובדים חדשים**" נכתב כי "**האוכלוסייה אותרה. משאבי אנוש התחייבו לביצוע ההדרכה בנובמבר 2007. ההדרכה הראשונה בדצמבר 2007 ואח"כ כל 4 חודשים.**".

לביקורת נמסר על ידי הארכיטקט הראשי כי כל עובד חדש הנקלט באגף המחשוב עובר הדרכה בנושא אבטחת מידע בטווח של חצי שנה.

בתגובה לממצאים מסר מנהל אבטחת מידע לביקורת כי: "**מהיבט ההדרכה התבצע שינוי גדול: נציג אבטחת מידע מדריך בכל קורס עירוני. בקורס לעובדי חיוב וגביה חדשים משולבת דרך קבע הרצאה של אבטחת מידע. מתוכננים 2 קורסים באבטחת מידע (קורס אבטחת מידע כללי וקורס נאמני אבטחת מידע למפתחים). היתה תוכנית יחד עם מחלקת תכנון ופתוח משאבי אנוש העירונית לחייב כל עובד חדש להגיע לקורס אבטחת מידע אולם לא יצא לפועל. באגף מיחשוב מתבצעת הדרכה בנושא לעובדים חדשים. בוצעו מספר הדרכות לצוותי הפיתוח באגף, למפעילים, לרכזי המיחשוב ולצוות המזכירות.**

מבחינת המודעות יש שינוי גדול לטובה, יחד עם זאת נדרשת עבודה נוספת נוכח הסיכונים הגדלים בתחום. בועדת היגוי לאבטחת מידע הנחה הסמנכ"ל שתתבצע עבודה בנושא יחד עם מנהל הידע העירוני.

מבחינת הכשרת עובדי מחלקת אבטחת מידע – כיום מתנהל קורס Cissp ייחודי בלמידה עצמית לכל עובדי המחלקה. הקורס מקיף את כל תחומי אבטחת המידע באופן מעמיק. בסיום הקורס העובדים יוכלו לגשת לבחינה לצורך קבלת התואר.".

23. עובדים חדשים הנקלטים בעירייה באגפים אחרים אינם עוברים הכשרה ייעודית בנושא אבטחת מידע.

24. הכשרת עובדי אבטחת מידע – בדו"ח הביקורת מס' 35, לשנת 2006, הביקורת המליצה כי תתבצע הכשרה ייעודית בנושא אבטחת מידע לעובדי אבטחת מידע, הכוללת השתלמויות וקורסים בתדירות גבוהה, מתוך הנחה כי החידושים בעולם אבטחת המידע מתעדכנים ומתחדשים בקצב מסחרר.

בקרה ואכיפה

25. בעקבות דו"ח הביקורת, מס' 35 בנושא אבטחת מידע לשנת 2006 גובשה תוכנית עבודה לביצוע בקרות ברמה יומית, חודשית, רבעונית, חצי שנתית ושנתית. תוכנית העבודה מגדירה פעילות וגורם אחראי.

26. מניתוח של תכנית העבודה אל מול ביצוע בפועל, נכון לחודש מרץ 2011, עולים הממצאים הבאים:

א. בקרה יומית:

לביקורת נמסרה טבלה שאינה כוללת פירוט ברמה יומית של ביצוע, אלא ברמה חודשית בלבד. מניתוח נתונים אלו הביקורת לא יכולה לקבוע באם כל הבקרות המתוכננות לבדיקה יומית מבוצעות מדי יום. בנוסף נמצא כי הפעילות לבדיקת תשובות מוקד השירות av אינה מבוצעת כלל.

ב. בקרה חודשית:

מבדיקת הביקורת נמצא כי:

1) חלק מהבקרות שהוגדרו בשנת 2009 בעקבות דו"ח הביקורת מס' 35, לשנת 2006, בוטלו ולא בוצעו כלל, על פי הפירוט להלן: בדיקה ה- wsadmin (ריקה) ו- NotInGpo (ריקה), בדיקת תשובות מוקד השירות לגבי תחנות ללא av, נוכחות מורשים בחדר מחשב.

2) בשנת 2011 הוכנסה בקרה אחת, שלא נכללה בביקורות החודשיות בשנים קודמות: הכנת דיסק אנטי וירוס עבור pcs.

3) להלן פירוט הנתונים כפי שנמסרו לביקורת:

סוג הבקרה	2009	2010	2011
בדיקה ה wsadmin (ריקה) ו NotInGpo (ריקה)	V	X	X
ביצוע בדיקת FW - האם עונה ל PING	V	V	V
דו"ח למחשבים ושרתים ללא אנטיוירוס	V	V	V
ביצוע פעולות נדרשות לפי הדו"ח הנ"ל	V	X	X
בדיקת תשובות מוקד השירות לגבי תחנות ללא av	V	X	X
נוכחות מורשים בחדר מחשב	V	X	X
גיבוי סביבת FireWall	V	V	V
בדיקת ou בשם users	V	V	V
הכנת דיסק אנטי וירוס עבור pcs	X	V	V

*V=בוצע X=לא בוצע

ג. בקרה רבעונית:

תוכנית הבקרה המתוכננת כוללת שני סוגי בקרות, אשר אמורות להתבצע אחת לרבעון. מניתוח הבקרות שנערכו בשנים 2009, 2010 עולה כי הבקרות לא בוצעו כלל, או בוצעו באופן חלקי ולא כמתוכנן. להלן פירוט הממצאים:

ביקורת שתוכננה לשנים 2008 - 2010	**ביצוע בפועל**
ארבע פעמים בשנה- נעילה וביטול משתמשים בסביבות עבודה	2008 - בוצע פעמיים. 2009 - לא בוצע כלל. 2010 - בוצע שלוש פעמים. נכון ליום בדיקת הביקורת בחודש מרץ 2011 הביקורת האחרונה שבוצעה הייתה בתאריך 1.10.10.
ארבע פעמים בשנה - נעילה וביטול מחשבים	2008 - לא בוצע כלל. 2009 - לא בוצע כלל. 2010 - בוצע שלוש פעמים. נכון ליום בדיקת הביקורת בחודש מרץ 2011 הביקורת האחרונה שבוצעה הייתה בתאריך 1.10.10.

להלן פירוט הנתונים כפי שנמסרו לביקורת:

פעילות	1.06.08	1.09.08	01.01.09	1.04.09	1.08.09	1.12.09	1.02.10	1.06.10	01.10.10
נעילה וביטול משתמשים בסביבות עבודה	v	v	x	x	x	x	v	v	v
נעילה וביטול מחשבים				x	x	x	v	v	v

*V=בוצע X=לא בוצע

ד. בקרה חצי שנתית:

תוכנית הבקרה המתוכננת כוללת ארבע סוגים של בקרות, אשר אמורות להתבצע אחת לחצי שנה. להלן עיקרי הממצאים:

ביקורת שתוכננה לשנים 2008 - 2010	ביצוע בפועל
בקרה חצי שנתית - החלפת סיסמא של כל ה Domain Administrators	בוצע פעם אחת
בקרה חצי שנתית - החלפת סיסמת compadd	לא בוצע כלל
בקרה חצי שנתית - שינוי סיסמת קודן	לא בוצע כלל- אין קודן
בקרה חצי שנתית - קו IpVpn - בדיקת Ipsec בנתב המרכזי	בוצע פעמיים ב 2010

להלן סיכום פירוט הנתונים כפי שנמסרו לביקורת:

פעילות	1.01.09	1.06.09	22.12.09	01.06.10
החלפת סיסמא של כל ה Domain Administrators			v	
החלפת סיסמת compadd				
שינוי סיסמת קודן	אין קודן	אין קודן	אין קודן	
קו IpVpn - בדיקת Ipsec בנתב המרכזי			v	v

*V=בוצע

ה. בקרה שנתית:

תוכנית הבקרה המתוכננת כוללת 5 סוגי בקרות, אשר אמורות להתבצע אחת לשנה-שנתיים. מניתוח הבקרות שנערכו בשנים 2009 - 2010 עולה כי הבקרות לא בוצעו כלל, או בוצעו באופן חלקי ולא כמתוכנן. להלן עיקרי הממצאים:

ביקורת המתוכננת לשנים 2008 - 2010	ביצוע בפועל
ביצוע בקרה אחת לשנה - אבטחת הקישור לנתיבי איילון	בוצע פעם אחת, יוני 2008.
ביצוע בקרה אחת לשנה - החלפת סיסמת dom001\administrator	בוצע בכל התקופה שלוש פעמים. פעם אחת בוצע לאחר חצי שנה בלבד, במקום לאחר שנה. נכון ליום בדיקת הביקורת בחודש מרץ 2011 הביקורת האחרונה שבוצעה הייתה ב- 12.2009.
ביצוע בקרה אחת לשנה - רענון תקופתי של קובץ מנהלי המאגרים - בעירייה ובמשרד המשפטים	לא בוצע כלל
ביצוע בקרה אחת לשנתיים - בקורת פיזית באתרים עירוניים	לא בוצע כלל

ביקורת המתוכננת לשנים 2008 - 2010	ביצוע בפועל
ביצוע בקרה אחת לשנתיים - להזמין נסיון פריצה לרשת מבחוץ	בטבלה לא נרשם ביצוע בפועל אולם לביקורת נמסר כי בקרה זו בוצעה כמתוכנן.

להלן פירוט הנתונים כפי שנמסרו לביקורת:

פעילות		1.06.08	1.06.09	12.2009	12.2010
ביצוע בקרה אחת לשנה - אבטחת הקישור לנתיבי איילון		v			
ביצוע בקרה אחת לשנה - החלפת סיסמת dom001\administrator		v	v	v	
ביצוע בקרה אחת לשנה - רענון תקופתי של קובץ מנהלי המאגרים – בעירייה ובמשרד המשפטים					
ביצוע בקרה אחת לשנתיים - בקורת פיזית באתרים עירוניים	אחת לשנתיים				
ביצוע בקרה אחת לשנתיים - להזמין נסיון פריצה לרשת מבחוץ	אחת לשנתיים				

*V=בוצע

ו. ניתוח בקרות - בדיקת סביבת FIRE WALL

בנוהל בדיקת סביבת FIRE WALL נקבע כי:

יש לבצע את הבדיקות הבאות: גלישה מתחנה בתוך הרשת העירונית לאתרים חיצוניים, גלישה מתחנה בתוך הרשת לאתר האינטראנט העירוני, שליחת דואר החוצה, קבלת דואר מבחוץ, ביצוע PING לשרת שב"א, בדיקת קישוריות והתחברות לאתר המחובר ב IP/VPN, התחברות מתחנה מחוץ לרשת העירונית לעירייה באמצעות VPN, התחברות מתחנה מחוץ לרשת העירונית לעירייה על ידי TS, התחברות מתחנה מחוץ לרשת העירונית לעירייה על ידי OWA, התחברות מתחנה מחוץ לרשת העירונית לעירייה בערוץ בזק עסקי (כיבוי, תברואה), התחברות מתחנה מחוץ לרשת העירונית לעירייה בערוץ IP/VPN.

את הבדיקות יש לתעד בטבלה הכוללת את הפירוט הבא: סוג הבדיקה, שם מבצע, תאריך ושעה, סטטוס וחתימה.

מבדיקת הביקורת עולה כי לא כל הוראות הנוהל מבוצעות על ידי היחידה לאבטחת מידע.

בתגובה לממצאים מסר מנהל אבטחת מידע לביקורת כי:

"א. הוכנה תוכנית בקרות, מצ"ב קובץ הבקרות. הוא מכיל בקרות יומיות, חודשיות, רבעוניות, חצי שנתיות ושנתיות.

ב. מבחינת הביצוע: מפורט בטבלה גם הביצוע בפועל (שלא תמיד נרשם). חלק מהבקרות לא מתבצעות עקב קשיי כ"א.

ג. בקרה היומית – בקרת אנטי וירוס מבוצעת ע"י אבטחת מידע במלואה, מתוכננת לעבור לספק החדש של שירותי מוקד התמיכה מ-4/2012.

ד. הבקרות על שינוי סיסמת קודן ובקרת הקו לנתיבי איילון - בוטלו, עקב ביטול הצורך בהם.

ה. ב - 2012 ימונה עובד שחלק מהמטלות שלו תהיינה אחריות על הבקרות.".

אבטחה פיזית

27. במסמך 'מדיניות אבטחת מידע' נקבע כי אחת הפעולות הנדרשות לאבטחת מידע היא הגנה פיזית על מאגרי מידע ונתונים או גיבויים, מפני מכלול אפשרויות הפגיעה הפיזית בהם או גנבתם.

על פי נוהל אבטחה פיזית מנהל אבטחת מידע אחראי לביצוע בקרות תקופתיות על מאגרי מידע ונתונים או גיבויים ומנהל אבטחת מידע או מי מטעמו אחראי לבצע ביקורת אבטחת מידע פיזית, אחת לשנתיים וממצאיה יוגשו למנהלי היחידה ולמנהל אגף המחשוב.

נספח 2 לנוהל אבטחת מידע מגדיר 23 סעיפים לבדיקה פיזית, מתוכם 9 סעיפים הוגדרו כחובה.

מממצאי הביקורת עולה כי היחידה לאבטחת מידע לא מבצעת ביקורות על אבטחה פיזית.

28. אזורים מאובטחים: על פי המלצת הביקורת על ממונה אבטחת המידע לחלק את סביבת העבודה שלו למעגלי אבטחה/אזורים מאובטחים לפי רמות רגישות, לקבוע את רגישות אזורי העבודה ואופי ההגנה עליהם וליישם מספר מעגלים של בקרות גישה פיזית, הגדרת בקרות, מידור אזורים ועוד. מבדיקת הביקורת הדבר לא נעשה.

29. שימוש בקודנים לנעילת דלתות אוטומטית: עד לתקופת הביקורת לא נעשתה בדיקה שיטתית, גורפת לצורך הכנסת קודנים במקומות רגישים, אשר יבטיחו נעילה אוטומטית של דלתות.

מנהל אבטחת מידע מסר לביקורת בתגובה לממצאים כי: **"בוצעה חלוקה של סביבת העבודה למעגלי האבטחה.**

א. <u>חדר מחשב ומרכז התקשורת בבניין הראשי</u> - במסגרת הבינוי שהתבצע בבנין הראשי נסגרו כל הכניסות, הכניסה מתבצעת באמצעות כרטיס מגנטי לפי רשימת מורשים. קיים ומיושם נוהל בקרה לנוכחים בחדר מחשב. קיים גם נוהל לליווי עובדים חיצוניים החייבים לעבוד בחדר מחשב. החדרים מבוקרים ע"י מצלמות.

ב. <u>חדר המחשב ומרכז התקשורת במנהל הנדסה</u> - התבצעה ומתבצעת פעילות של העברת השרתים לחדר מחשב בבנין המרכזי. חדר זה נעול והמפתחות נמצאים בהנהלת הבית ואצל מנהל הרשת.

ג. <u>מרכזי התקשורת והחשמל בבנין הראשי נעולים</u>.

ד. <u>חדר מנהלי הרשת</u> (אזור רגיש) נעול בקודן.

ה.<u>חדר מנהלי הרשת</u> במנהל הנדסה – נעול.

ו.<u>חדרי אבטחת מידע</u> בצייטלין נמצאים במתחם נעול (אינו נגיש לעובדים לא מורשים).

התבצעו מספר בקרות אבטחה פיזית. העובד שבצע את העבודה עבר לתפקיד אחר. הבעיה היתה שהיחידות ביקשו, בסיום כל ביקורת, שאבטחת מידע יממנו את תיקון הממצאים. לאחר מספר בקרות כשהבנו שאין תועלת בבקרות – הן הופסקו.".

נתיב בקרה (audit trail)

30. במסמך 'מדיניות אבטחת מידע' נקבע כי במסגרת הבקרה ייקבע נתיב בקרה, במערכות המחשוב. כלומר ייושמו כלים המאפשרים זיהוי חד ערכי של משתמשים אשר ביצעו שינויים במידע או בתכנה, או ניגשו למידע רגיש, תוך פירוט ורישום של כל סוג פעילות שבוצעה, מועד ביצועה ופרטי המבצע. לשאלת הביקורת מסר מנהל אבטחת מידע ביום ה- 28.8.2011 כי **"הפעילות בנושא זה נעשית ברבדים שונים: מודעות, מתודולוגיות עבודה, בקרת הפרוייקטים ועוד. במסגרת מערכת מחו"ג שפיתוחה הסתיים לא מכבר – הוטמע בתהליכים הנושא של רישום המבצעים שינויים בנתונים. במבגרת מתודולוגיית הפיתוח המאובטח – המפתחים נדרשים לבצע רישום שינויים. במסגרת בדיקות אבטחה של המערכות לפני עליה לאויר – הנושא נבדק.**

למרות השיפור העצום בנושא - הוא עדיין איננו מתבצע לשביעות רצוני המלאה ואפשר להכניס בו עוד שינויים ושיפורים.".

מנהל אבטחת מידע מסר לביקורת בתגובה למצאים כי:

"אין לי ספק שהמצב השתפר מבחינת המודעות לנושא והפעילות המתבצעת בהקשר זה".

נתיב הבקרה נדרש לכל פעילות (ברמת מערכת הפעלה, ברמת התשתית, ביישומים). בנוסף נדרשת בקרה על הרישום בכל נתיבי הבקרה. הרישום הוא בהיקף של מליוני תנועות ביממה ואין אפשרות אנושית לקרוא את כל הלוגים ובמיוחד לא לעשות קורלציה בין הלוגים השונים.

<u>מבחינת מערכת ההפעלה</u> – הרישום מתבצע באופן שוטף בכל המערכות (בשרתים, ברכיבי האבטחה השונים...). הוטמעה מערכת mom מתוצרת מיקרוסופט שמדווחת לגורמים שונים באגף על אירועים ספציפיים במערכות ההפעלה (אני מקבל מיילים על אירועי אבטחה – למשל הוספת לקוח לקבוצת Domain Admins).

<u>מבחינת התשתיות</u> – בסיסי הנתונים – הנושא מטופל ע"י צוות ה - DBA.

מערכת נת"ע שהוטמעה ע"י מחלקת אינטגרציה באגף מכילה רישום מפורט של כל הפניות אליה.

<u>מבחינת יישומים</u> - מתודולוגית הכתיבה המאובטחת ובדיקות אבטחה של היישומים מתייחסים בקפדנות לנושא זה .

(הדבר אינו נכון לגבי יישומים קנויים). המערכות האחרונות שעלו, מחו"ג וחות"ם, עונות על דרישה זו.".

כרטיס חכם

31. בסעיף 18 בהערות ראש העירייה לדו"ח הביקורת בנושא אבטחת מידע משנת, מס' 35, נכתב: **"המנכ"ל יקיים דיון לגבי אופן שילוב כרטיס חכם בת"ע 2008."**. מבדיקת הביקורת עולה כי התקיים דיון בנושא כרטיס חכם והוא אושר להפעלה בשנת 2008 ל- 1000 יחידות. ממנהל אבטחת מידע נמסר לביקורת בתאריך 23.3.11 כי נעשה שימוש בכרטיס חכם בפרויקטים ובמאגרים מיוחדים בלבד, בנושא טפסי אבטחת מידע בלבד.

32. על פי מידע שנמסר לביקורת על ידי מנהל היחידה לאבטחת מידע, השימוש בכרטיסים חכמים נעשה בצורה מצומצמת בלבד בגלל שיקולים כלכליים.

33. מבדיקת הביקורת עולה כי לא נעשה תהליך של בחינת הכדאיות/עלויות לאור הניסיון הקיים בשימוש בכרטיסים חכמים ולא נבחנו העלויות ביחס לסיכונים.

מחשבים ניידים ו- DOK

34. על פי סעיף 18 בהערות ראש העירייה לדו"ח הביקורת, מס' 35, בנושא אבטחת מידע משנת 2006 נקבע כי יתקיים דיון לגבי עקרונות השימוש במחשבים ניידים ו- DOK (disk on key).

35. על פי דו"ח סטטוס מתאריך - 5.8.07, שנמסר לביקורת על ידי מנהל אבטחת מידע קיים נוהל למחשבים ניידים.

36. לביקורת נמסר על ידי מנהל אבטחת מידע כי התקיים דיון מנכ"ל בנושא המשך טיפול בהיבטים הקשורים ב- DOK, שבו סוכם כי קומה 12 תהווה פיילוט לבדיקת היתכנות 'תחנות הלבנה', נכון למועד עריכת הביקורת לא בוצע פיילוט זה.

מנהלי מאגר

37. מממצאי דו"ח הביקורת, מס' 35, בנושא אבטחת מידע לשנת 2006 בנושא קביעת הרשאות על ידי מנהלי המאגרים נמצא כי: למנהלי המאגרים אין כלים המתאימים לקביעת רמת ההרשאות שאמורה להינתן לעובדים. מבדיקת הביקורת עולה כי הנושא טופל על ידי מעבר לשימוש בטופס ממוחשב למתן הרשאות.

38. בדו"ח הביקורת, מס' 35, בנושא אבטחת מידע לשנת 2006 בנושא פעולות חריגות במאגרים נכתב כי מנהלי המאגרים אינם מקבלים חיווי שוטף על פעולות חריגות שמבוצעות במאגרים עליהם הם אחראים, למרות שעל פי הוראות חוק הגנת הפרטיות האחריות מוטלת על מנהל המאגר ומנהל אבטחת מידע ביחד ולחוד.

39. בסעיף 12 ב' בהערות ראש העירייה, בדו"ח הביקורת, מס' 35, בנושא אבטחת מידע לשנת 2006 נכתב כי **"תיבנה תוכנית ייעודית קבועה ושיטתית של מנהלי מאגרי המידע העירוניים. ימוסד פורום לעדכונים שוטפים."**. משיחה של הביקורת עם מנהל אבטחת מידע בתאריך 22.3.11, עולה כי לא נבנתה תוכנית ייעודית לנושא זה. מנהל אבטחת מידע מסר לביקורת כי הוא אמור להוציא אחת לשנה עדכונים שוטפים למנהלי המאגרים, אולם הדבר לא נעשה בשנה האחרונה.

בתגובה לממצאים מסר מנהל אבטחת מידע לביקורת כי: **"במשך מספר שנים אחרי הדו"ח הקודם, הופץ לכל מנהלי המאגרים מכתב המפרט את מחויבויותיהם על פי החוק. עקב עליית המודעות לאבטחת מידע בכלל אנו רואים הקפדה רבה יותר מבעבר על אישור ההרשאות."**.

טיפול במתן הרשאות ו'הקמת משתמש'

40. בדו"ח הביקורת, מס' 35, בנושא אבטחת מידע לשנת 2006 נכתב כי הטיפול בהרשאות הינו תחום טיפול מרכזי של עובדי אבטחת מידע, על פי הממצאים בדו"ח זה נהוג היה לתת לעובדים הרשאות בצורה פרטנית, על פי דרישות יחידות העירייה. כמו כן נמצא כי בתהליך מתן ההרשאות שולבו תהליכי עבודה ידניים ארוכים, הדורשים ניירת מרובה. מבדיקת הביקורת נמצא כי נכון לתקופת הביקורת נבנה מנגנון ממוחשב להעברת טפסים בין הגורמים השונים.

41. אנשי יחידת אבטחת מידע עוסקים בטיפול בהרשאות.

42. הגדרת ההרשאות ניתנת לעובד ולא לתפקיד. במערכות המחשוב החדשות משייכים עובד לתפקיד ובמערכות המחשוב הישנות לא ניתן לעשות כן.

43. בדו"ח הביקורת, מס' 35, בנושא אבטחת מידע משנת 2006 נכתב כי על אבטחת מידע לוודא שהרשאות גישה למערכות מידע ולשירותים, מוקצות ומתוחזקות כראוי ולכן נדרשת הגדרה של תהליך רישום וביטול להרשאות גישה למערכות מידע ולשירותים. נכון למועד עריכת הביקורת המלצה זו יושמה.

44. נכון לתקופת איסוף הממצאים לדו"ח הביקורת מתן ההרשאות לגישה למאגרי מידע נעשה באמצעות שימוש בטופס ממוחשב. טופס זה כולל הצהרת סודיות, חתימות של מאשרי הבקשה, פירוט הרשאות מבוקשות ועוד. מבדיקת הביקורת עולה כי השימוש בטופס זה מאפשר ניהול יעיל ומבוקר של מתן הרשאות.

45. על פי מידע שנמסר לביקורת על ידי מנהל יחידת אבטחת מידע נמצא כי היחידה מטפלת בכ- 500 טפסי בקשה למתן הרשאות, מדי חודש. כלומר כ 20 - 25 טפסים ליום עבודה בממוצע.

46. מנהל יחידת אבטחת מידע מסר לביקורת כי הטיפול במתן הרשאות והקמת משתמש ('יוזר'), הוא לעיתים תהליך ארוך הדורש פתיחת הרשאות במערכות שונות כגון: רשת, מחשב מרכזי, מרשם תושבים, מחו"ג ומשרד הפנים. אורכו של תהליך פתיחת משתמש במערכת הוא כ- 15 - 20 דקות לעובד חדש וכ- 30 דקות לעובד שצריך לקבל הרשאה למחשב המרכזי. על בסיס נתונים אלו נמצא כי כ- 125 - 250 שעות עבודה בכל חודש מוקדשות על ידי עובדים באבטחת מידע לטיפול בהרשאות.

47. מבדיקת הביקורת עולה כי אין מיפוי של הרשאות לקוחות, ולא ניתן למצוא בצורה קלה ופשוטה את כל ההרשאות של משתמש אחד, אלא רק לאחר חיפוש במספר מערכות. כלומר יכול להיות מצב שבו המשתמש נעול לכניסה לרשת, אולם יש לו הרשאות שימוש במערכות שונות שלא נחסמו ולעיתים השימוש במערכות אלו מחייב תשלום עבור רישיון שימוש.

בתוגבה לממצאים מסר מנהל אבטחת מידע לביקורת כי "**לגבי משך הטיפול בהרשאות, הערכת הזמן תלויה בבקשת ההרשאה עצמה. כך לדוגמא יש טפסים רבים שעוברים 4 תחנות באבטחת מידע (אישור הבקשה, הגדרת הרשאות בסביבה המבוזרת, הגדרת הרשאות במחשב המרכזי, הגדרת הרשאות ביישום למשל מחו"ג או חות"ם).**

מתבצעת פעילות פיתוח חדשה לביצוע הגדרות בצורה ממוחשבת ואוטומטית בסביבה המבוזרת עם אינטגרטור חיצוני. התוכנה מתוכננת גם לענות על הצורך במיפוי מדויק יותר של הרשאות הלקוח.

מתבצעת בקרה רבעונית לנעילת משתמשים שבמסגרתה עובד שהפסיק את עבודתו ננעל, מבוטלות הרשאותיו ברשת, ומבוטלות הרשאותיו במערכת מחו"ג – שבה עלות הרשיון היא כ 800 יורו.".

DBA

48. על פי מידע שנמסר לביקורת על ידי מנהלת מסדי הנתונים עולה כי שלושה בעלי תפקידים ביחידה עובדים עם 'יוזר גנרי' אחד. לשאלת הביקורת נמסר כי כיום לא ניתן לזהות מי מבין בעלי התפקידים עשה שימוש ב'יוזר הגנרי' ומתי, ובמקרה שיתעורר צורך בניטור המידע, לא ניתן יהיה לעשות זאת בדיעבד.

49. בתגובה לממצאי דו"ח הביקורת, מס' 35, בנושא אבטחת מידע לשנת 2006 נמסר על ידי הנהלת האגף כי ביצוע בקרה וניטור מדגמי של היחידה נכללת במשימות אבטחת מידע. מבדיקת הביקורת את פירוט הבקרות הנערכות על ידי יחידת אבטחת מידע נמצא כי נכון למועד עריכת הביקורת לא בוצעו בקרות כלל. בוצעה החלפת סיסמא של כל ה Domain Administrators פעם אחת בשנת 2009 .

בתגובה לממצאים מסר מנהל אבטחת מידע לביקורת כי:"**מחלקת ה Dba מבצעת בקרות משלה על בסיסי הנתונים.**

מוצר סנטריגו שהוטמע בחלק מבסיסי הנתונים משפר את מצב האבטחה של בסיסי הנתונים.

המשתמש הגנרי הבעייתי הוא משתמש Sa המשמש את עובדי מחלקת dba לצרכים רבים.

עבודת משתמש זה הוגבלה ל 4 מחשבים נקבע שהסיסמא תהיה שונה בין הדומיינים השונים ובחלק מהסביבות. שונתה פעם אחת הסיסמא.

במסגרת הניטור השוטף של סנטריגו נרשמות פעולות חריגות אבטחתית בבסיסי הנתונים שבהם מוטמע הסנטריגו.

נשכר עובד בהיקף 500 שעות לשנה שתפקידו לבצע "אבטחת בסיסי נתונים". נכתבה טיוטת מתודולוגיה לאבטחת בסיסי נתונים.

בקרת היישומים כוללת כמובן גם היבטי אבטחה של בסיסי הנתונים מבחינה אפליקטיבית.".

פרויקט ה- DRP

50. במסגרת פרויקט ה DRP נערך מיפוי של מערכות העירייה והגדרת רמות הקריטיות של כל מערכת. על פי מסמך סטטוס של אגף המחשוב מיום 5.8.2007 שנמסר לידי הביקורת על ידי מנהל אבטחת מידע עולה כי:

א. הוחלט על מיפוי המידע העירוני מבחינה אבטחתית, להוסיף את רמת הסיכון לכל מערכת בטבלת מערכות שהוכנה ל- DRP.

ב. מתבצעת הכנה של רשימת מערכות ע"י רכזי המחשוב. יבוצע טיוב בין רשימה זו לרשימה הקיימת באבטחת מידע. לרשימה יוכנס הסיכון האבטחתי. הרשימה תוכנס לדיון בפורום מטה. המועד המעודכן לביצוע היה ספטמבר 2007.

ג. מנהל אבטחת מידע מסר לביקורת בתאריך 28 באוגוסט 2011 כי **"הפעילות בנושא ה** drp **יצאה מידי אבטחת מידע לפני כ- 8 שנים והועברה לתפעול. מתפעול הועברה לפרוייקטור במטה חטיבת תכנון.".**

גיבוי

51. גיבוי מערכות המידע וביצוע בקרה על איכות הגיבויים. מבדיקת הביקורת עולה כי הגיבויים נעשים על ידי מנהלי הרשת.

סקר סיכונים

52. בסעיף 15 בהערות ראש העירייה בדו"ח הביקורת, מס' 35, בנושא אבטחת מידע לשנת 2006 נכתב: **"המנכ"ל אישר לבצע סקר ניהול סיכוני אבטחת מידע במערכות המידע והממשקים הפועלים בעירייה. לצורך ביצועו ויישום ההמלצות אושר תקציב ייעודי.".**

53. לביקורת נמסר על ידי מנהל היחידה לביטוח וניהול סיכונים בתאריך 9.2.11, כי בעבר התקיימו דיונים עם בעלי תפקידים באגף המחשוב לצורך בחינה של סוגיות שונות בנושא אבטחת מידע ובחינת כדאיות הביטוח, אולם לא מתקיימת עבודה שיטתית וקבועה בנושא.

54. על פי מסמך 'מדיניות אבטחת מידע' נקבע כי באחריות ממונה אבטחת מידע להכין הערכת סיכונים ולבצע סקר סיכונים תקופתי המבוסס על פעילות העירייה ומערכות המידע שברשותה.

55. מבדיקת הביקורת עולה כי בדצמבר 2007 בוצעה **'הערכת סיכוני אבטחת מידע'** על ידי חברה חיצונית. במסגרת בחינה זו התקבלה תמונת האיומים הכוללת. ניתוח הממצאים כלל דירוג כמותי של דרגות הסיכון ומדרוג רמות הסיכון, מסקנות והמלצות.

56. בסעיף יא' לדו"ח **'הערכת סיכוני אבטחת מידע'**, נכתב כי **"מומלץ לבצע בדיקת סיכונים (בדומה לבדיקה זו) לאחר גמר ביצוע התיקונים לאחר פרק זמן של מספר חודשים על מנת לקבל תמונת מצב עדכנית של סיכוני אבטחת המידע ברשת המחשוב, בדיקה ומעקב אחר יישום התיקונים שנדרשו בבדיקה הנוכחית וקבלת רשימת פעולות לביצוע על מנת לסגור את הפרצות הקריטיות בארגון."**.

57. לא בוצע סקר סיכונים נוסף, נכון לחודש יוני 2011.

58. בתגובה לממצאים מסר מנהל אבטחת מידע לביקורת כי: **"בעקבות החלטה של מנהלת האגף מותנע בימים אלו סקר סיכונים, הכולל אף הקצאת שעות לבדיקת התיקון. סקר הסיכונים מתבצע על 3 דומיינים (רשת העירייה, אתר האינטרנט העירוני, רשת ארגון העובדים). לדומיין החדש שהוקם לאחרונה (חוות תקשוב החינוך) התבצע נסיון פריצה, נסיונות אלו מסייעים באישוש/תיקוף הסיכונים שהוגדרו, בת"ע 2012 תוקצבו 2 נסיונות פריצה לרשת, שיסייעו באיתור הסיכונים."**

יכולת הניטור והמעקב

59. בסעיף 16 בהערות ראש העירייה בדו"ח הביקורת, מס' 35, בנושא אבטחת מידע לשנת 2006 נכתב: **"נושא שיפור יכולת הניטור והמעקב יקבל עדיפות בת"ע 2008, כולל הביטוי התקציבי לכך."**

60. לשאלת הביקורת נמסר על ידי מנהל יחידת אבטחת מידע כי ברשותם כלים טכנולוגיים למניעת זליגת מידע, אולם הדבר דורש החלטה ניהולית והקצאה של שעות הטמעה, פיקוח ובקרה, וביצוע ניטור מדגמי של בעלי הרשאות לנושא זה.

61. ניטור אבטחתי:

לשאלת הביקורת נמסר כי נעשית פעילות אבטחת מידע רשתית הכוללת ips פנימי, אולם אין בדיקה פרטנית של כל מסוף, בדיקה טכנולוגית לאיתור תוכנות מאיימות ופוגעניות בנקודות קצה ובנוסף אין בדיקה פיזית של אתרים חדשים.

בתגובה לממצאים מסר מנהל אבטחת מידע לביקורת כי: "**<u>חיוויים</u> - יחידת אבטחת מידע מקבלת כיום חיוויים מ 4 תוכנות מרכזיות: מערכת האנטי וירוס (**Symantec Endpoint Protection**), מערכת** Mom**, מערכת** setntrigo **(בסיסי נתונים) ומערכת ה** spectrum **לשליטה ובקרה.**

<u>ניטור אתרי האינטרנט העירוניים</u> - במהלך 2011 נרכש מוצר לניטור וגיבוי אתרי אינטרנט. המוצר כולל ביצוע גיבוי שבועי של אתר האינטרנט העירוני, ניטור האתר (אנושי – בשעות העבודה) ויכולת מעבר לאתר חלופי בענן מיקרוסופט. בימים אלה נרכשת גירסא מתקדמת יותר של המוצר.

ל 2012 מתוכננת רכישת שירות siem\soc **לשיפור יכולות הניטור והתגובה לאירועי אבטחה.**".

62. בקרה על בסיס הנתונים:

קיימת תוכנה לבקרה על בסיס הנתונים, המופעלת כיום, על פי מנהל אבטחת מידע, בהיקף של 600 שעות שנתיות. התוכנה מבצעת בקרות ברמת הניטור בלבד, אולם לא מבוצעות בקרות באופן כללי.

טיפול בענייני משמעת

לביקורת נמסר על ידי התובע לענייני משמעת כי לא טופלו עבירות הקשורות באבטחת מידע במהלך השנים 2008 – 2010.

מיקום ארגוני

63. יחידת אבטחת מידע ממוקמת בכפיפות לארכיטקט הראשי. על פי המלצות דו"ח ביקורת, מס' 35, בנושא אבטחת מידע לשנת 2006 המנכ"ל הנחה את אגף ארגון ותקינה לבצע בחינה ארגונית לגבי כפיפות היחידה בתוך אגף המחשוב, תוצאות הבחינה אמורות היו להיות מוצגות עד 15 ביולי 2007.

64. מבדיקת הביקורת עולה כי לא התקבלה החלטה בנושא למרות שנערכו מספר דיונים והוצגו מספר חלופות.

היערכות למצב חירום

65. בדו"ח אבטחת מערכות מידע, מס' 35, לשנת 2006, נכתב כי נדרש נוהל לשעת חירום למקרה של קריסת מערכות.

66. בסעיף 7 בהערות ראש העירייה בדו"ח אבטחת מערכות מידע, מס' 35, לשנת 2006, נכתב כי תוכן תוכנית היערכות למצב חירום, הכוללת צעדים אופרטיביים ליישום עד סוף שנת 2007.

67. ממידע שנמסר לביקורת על ידי הארכיטקט הראשי עולה כי התקציב לכך התקבל בשנת 2011 ובתקופת הביקורת התבצעה עבודה ברמה עירונית בנושא.

רכזי המחשוב

68. על פי דו"ח מס' 35, לשנת 2006 בתקופת הביקורת בוצעה עבודה בהובלת ארגון ותקינה להגדרת תפקיד רכז המחשוב ותפקידו בהקשר של אבטחת מידע.

69. מבדיקה שנערכה על ידי הביקורת, נכון לחודש יוני 2011 עולה כי במהלך השנים נבחנו מספר הצעות בנוגע לתפקיד רכז המחשוב, אולם עד לתקופת איסוף הממצאים לדוח ביקורת זה לא התקבלה החלטה בנושא.

70. מבדיקת הביקורת עולה כי לרכז המחשוב משימות בנושא אבטחת מידע המוגדרות במספר נהלים המופיעים בפורטל אגף המחשוב. מבדיקת הביקורת עולה כי קיימת שונות ביישום ובביצוע התפקיד כפי שהוא מוגדר בנהלים אלו על ידי רכזי המחשוב ביחידות השונות.

בתגובה לממצאים מסר מנהל אבטחת מידע לביקורת כי: "**מנקודת מבטה של יחידת אבטחת מידע, רכזי המחשוב הם שותפים מרכזיים, וככאלה מקבלים שירות בהתאם. חלק מפניות הלקוחות לאבטחת מידע מחויבות במעורבות רכז המחשוב (למשל מתן הרשאה). התקיימו אף 2 ישיבות עם רכזי המיחשוב לליבון סוגיות שונות באבטחת מידע.**".

קליטת עובד חדש

71. מסמך 'מדיניות אבטחת מידע' המגדיר כי המידע יסווג לפי אופיו וכללי האבטחה שיחולו עליו יהיו לפי סיווגו. להלן פירוט הסיווגים: מערכת בלתי מסווגת, מערכת תפעולית, מערכת כספית ומערכת המכילה נתוני צנעת הפרט. כהחלטה אסטרטגית החליטה העירייה לקטלג את כלל המידע ברמה ביטחונית "נתוני צנעת הפרט". בסעיף 8.1.2 למסמך זה נכתב כי "**כל עובד עירייה וכל קבלן חיצוני אשר תורשה לו גישה למערכות המחשב של העירייה יעבור בדיקה בטרם תאושר הגישה למערכות.**".

72. מבדיקת הביקורת עולה כי בעת קליטת עובד חדש לא נעשית בדיקה מעמיקה אודות העובד, גם במקרים שבהם הוא מיועד לתפקיד שיש בו גישה למאגרי מידע רבים ורגישים, כדוגמת מנהלי רשתות.

תחומי אחריות וסמכות במערך התפקידים באבטחת מידע

73. בדו"ח הביקורת מס' 35, בנושא אבטחת מידע לשנת 2006, נמצא כי אבטחת מידע בעירייה עוסקת בעיקר במישור התפעולי, המתבטא בעיקר בנושא הטיפול בהרשאות. בדו"ח זה נמצא כי הטיפול במישור התורה ובנהלי העבודה נעשה בצורה חלקית ועל ידי מנהל היחידה בלבד. לשאלת הביקורת נמסר על ידי מנהל אבטחת מידע כי נכון לתקופת איסוף הממצאים לדוח זה, מספר בעלי תפקידים ביחידה עוסקים במישור התורה וקביעת מדיניות אבטחת מידע אבל עדיין מרבית בעלי התפקידים עוסקים בעיקר במישור התפעול.

בתגובה לממצאים מסר מנהל אבטחת מידע לביקורת כי: **"העבודה התפעולית מתחלקת היום בין 2 תחומים (סביבת ה perimitter והסביבה הפנימית) ומתבצעת העברת משאבים לצרכים שוטפים ולצרכי התמקצעות.**

<u>בתחום המתודולוגי</u> מתבצעת העבודה ע"י 3-4 אנשים. נכתבו (הורחבו) לאחרונה 3 רכיבי מתודולוגיה: מתודולוגיית אבטחת בסיסי נתונים, מתודולוגיית כתיבה מאובטחת, ריכוז דרישות אבטחה למוצרי תוכנה נרכשים (מוצרי מדף או מוצרים המפותחים במיוחד עבור העירייה).

<u>תוכניות העבודה השנתיות</u> מגובשות במחלקה בשיתוף אותם גורמים.

<u>בתחום התכנון ארוך הטווח</u> (אסטרטגי) מתבצעת עבודה עם חברת יישוץ (קיוריטי) שבה משתתפים מצד העיריה שני נציגים.".

שחזור חסימה

74. נכון לתקופת הביקורת תהליך שחזור סיסמא אמור להעשות על ידי מוקד התמיכה והשירות, על פי נוהל זיהוי משתמש. מבדיקת הביקורת עולה כי נוהל זה אינו מיושם ואינו מבוקר. מנתונים שנמסרו לביקורת על ידי מנהלת מרכז השירות והתמיכה עולה כי כ- 30% מהפניות אל מרכז השירות נעשות בנושא סיסמאות. מבדיקת הביקורת עולה כי לא נעשות פעולות יזומות לרענון הנוהל ו/או על ביצוע בקרה על יישומו על ידי יחידת אבטחת המידע.

75. מבדיקת הביקורת עולה כי קיימת הנחיית עבודה לאופן שחזור סיסמת משתמש. על פי הנחיית העבודה לצורך אימות נתונים יש לבצע מספר פעולות כגון: לבקש שם משתמש ומספר ת.ז, לשאול מספר שאלות לגבי זהות המשתמש ועוד. הנחיית העבודה אינה מיושמת במלואה ואינה מבוקרת בצורה ראויה.

76. הביקורת בחנה הנחיית עבודה ולהלן פירוט הממצאים: אחת ההוראות המופיעות בהנחיית העבודה לשחזור סיסמא היא כי אסור לאפס סיסמאות למשתמשים נעולים ב Disabled או להחזיר ל Enable, אלא רק משתמשים ב Locked Out כלומר ננעלו כתוצאה מהקשת סיסמא שגויה ניתן לשחרר. מבדיקת הביקורת עולה כי לא קיימים כלים טכנולוגיים שיאפשרו בדיקה של שחזור סיסמא בניגוד להנחיות והנושא אינו מבוקר כלל.

בתגובה לממצאים מסר מנהל אבטחת מידע לביקורת כי: **"מוקד השירות אינו מורשה ואינו מבצע שחרור משתמשים הנעולים ב** disabled.

אין מעקב אחר קיום/אי קיום הנוהל.

במהלך 2011 התקיים פיילוט למימוש האפשרות של שחרור סיסמא ע"י משתמש הקצה (ע"י התחברות לפורטל הפנימי, מענה על שאלות שתשובותיהן קיימות במערך משאבי אנוש ובחירת סיסמא חדשה). הפיילוט נערך בשיתוף מחלקת אינטגרציה והוקצה תקציב לפעילות זו במהלך 2012.".

טיפול בתקלות על ידי מרכז תמיכה ושירות

77. טיפול בתקלות מחשב נעשה מרחוק באמצעות תוכנה, על ידי עובדי מרכז השירות, הטיפול מרחוק נעשה אך ורק לאחר שהלקוח מאשר את ההשתלטות בזמן אמת על המחשב שלו.

בתגובה לממצאים נמסר על ידי מנהלת מחלקת שירות וקשרי לקוחות כי: **"השימוש בכלי ה-**damware **מבוצע באישור ובידיעת מנהלת האגף, מתוך הבנת המצוקה הקיימת בצורך במתן שירות ללקוחות, כאשר קיים פער בתשתיות הקיימות לצורך כך. מפעילי המוקד הונחו לבקש תחילה את אישור הלקוח להשתלטות על התחנה."**.

78. על פי מנהלת מרכז השירות והתפעול הם מטפלים בכ- 4,500 לקוחות. אולם לכ- 500 לקוחות מתוכם אין אפשרות גישה מרחוק באמצעים הרגילים משום שלא מותקנת בהם המערכת המאפשרת השתלטות מרחוק לצורך מתן שירות. במקרים אלו נעשה שימוש בתוכנת demwear. השימוש בתוכנה זו אינו מחייב קבלת אישור להשתלטות מהלקוח בזמן אמת, ולפיכך ניתן לכאורה להשתלט על המחשב מרחוק מבלי ידיעת הלקוח.

79. מבדיקת הביקורת עולה כי בעיה זו מוכרת ומטופלת על ידי אגף המחשוב, ואמורה להגיע לפתרונה עד סוף שנת 2011.

הגדרת סמכות

80. על פי הערות ראש העירייה בדו"ח מס' 35, בנושא אבטחת מערכות מידע, לשנת 2006, נדרשת אכיפה של שימוש בסיסמאות והרכבת הסיסמה משילוב של סימן מיוחד אחד ולפחות 5 ספרות.

81. בהמלצות בדו"ח נכתב בין היתר כי:

א. תוגדר מדיניות סיסמאות, בהתאם לרגישות המערכת על ידי מנהל אבטחת מידע.

ב. במידה וסיסמא נמסרת למשתמש: הסיסמא לא תימסר דרך רשת האינטרנט, או דרך תשתית לה נדרשת הסיסמא להזדהות, יש לאמת תחילה את זהות המשתמש, המשתמש יחויב לשנות סיסמא בהתחברות ראשונית למערכת.

ג. הסיסמאות לא יישמרו באופן גלוי, או באופן הניתן לשחזור ברשומות, בזכרון, או במאגרי מידע.

ד. סיסמא תבוטל מיידית בכל מקרה של חשש לחשאיותה.

ה. אי שימוש בחשבון למשך תקופה של חצי שנה יביא לביטול הסיסמא הנדרשת בתהליך ההזדהות לאותו חשבון.

82. מבחינת הביקורת עולה כי המלצות יושמו בתהליכי העבודה ובנהלים שהוגדרו. לביקורת אין כלים לבחון את יישומם בפועל.

מוקד תמיכת משתמשים

83. מוקד תמיכת משתמשים באגף המחשוב, מופעל על ידי חברה חיצונית החל משנת 2006. הביקורת בחנה את חוזה ההתקשרות ולהלן הממצאים: במפרט הטכני לחוזה **'הקמה ניהול ותפעול של מרכז שרות'** משנת 2006, נקבע כי על הספק ועובדיו לנהוג על פי כללי ונהלי ומדיניות אבטחת המידע הנהוגים בעירייה, ולהבטיח קיום מנגנוני אבטחת מידע באמצעות נהלים ברורים, כולל מידע שמופץ ברשת האינטרנט, עפ"י נהלי העבודה לאבטחת המידע הנהוגים בעירייה.

84. לביקורת נמסר הן על ידי מנהל אבטחת מידע והן על ידי מנהלת המוקד כי הנהלים הקשורים לשחזור סיסמאות אינן מיושמות כהלכה. מניתוח דו"ח הקשבות במוקד תמיכת משתמשים מיום 10.1.10 עולה כי 35% מהפניות למוקד הן בנושא סיסמאות: שינוי סיסמא, איפוס סיסמא. והזמן הממוצע לטיפול בפנייה בנושא סיסמאות, על בסיס הנתונים המופיעים בדו"ח זה, עמד על 4.2 דקות.

מנגנונים לניהול בקרות גישה במערכות חדשות

85. על פי דו"ח מס' 35, בנושא אבטחת מערכות מידע, לשנת 2006, יש לכלול במערכות המחשוב החדשות את מיטב המנגנונים לניהול בקרות גישה.

86. בדו"ח סטטוס מיום 5.8.07 צוין כי נכון ל- 7.9.2008 מתבצעת בקרה מפורטת של כל מערכת בשלבי הפיתוח לצורך עמידה בהנחיות אבטחת מידע ובוצעה הדרכה לחלק מהצוות, כמו כן אמורה היתה להיות הדרכה נוספת בסוף שנת 2007.

87. משיחה שהתקיימה עם מנהל אבטחת מידע עולה כי מערכת המחו"ג מהווה דוגמה ליישום החלטה זו ובשלב פיתוחה היתה מעורבת חברה המתמחה באבטחת מידע.

שרתי האנטי וירוס

88. בדו"ח מס' 35, בנושא אבטחת מערכות מידע, לשנת 2006, נמצא כי מצב תחזוקת שרתי האנטי וירוס, אינו יעיל דיו בהגנה בפני וירוס עבור כל קישור לרשת עירונית ולכן הביקורת המליצה ליישם מנגנונים ממוכנים לניהול בקרות גישה במערכות מידע וביישומים (אפליקציות).

לשאלת הביקורת מסר מנהל אבטחת מידע ביום ה 28.8.2011 כי **"מערכות האנטי וירוס השונות מספקות יכולות ניהול של המוצר. יכולות המוצר הם כרגע המנגנונים הממוכנים לניהול הבקרות במוצר. הדיווחים המתקבלים נוגעים למחשבים שנדבקו, מחשבים שיש קשיים כלשהם מערכת האנטי וירוס שלהם. בנוסף הוגדר נוהל לטיפול בשירות האנטי וירוס. תכננו לתקציב 2012 מוצר אכיפת מדיניות הכולל אופציית מניעת התחברות לרשת ללא אנטי וירוס מעודכן, אבל התקציב לא אושר."**.

על פי דו"ח סטטוס מיום 5.8.07, אשר נמסר לידי הביקורת על ידי מנהל אבטחת מידע עולה כי נכון ל- 7.9.2008 (התאריך הנ"ל במקור) הם מטפלים בחסימה. החסימה נתקלת בקשיים תפעוליים ומתבצעת עבודה לתיקון תקלות (יחד עם יצרן הציוד וספק הציוד). מבצעים הגנה בתחנת עבודה, סורקים כל שבוע באופן יזום, עורכים בדיקה שבועית על קיום/אי קיום אנטי וירוס מעודכן בת"ע ושרתים ותיקון תקלות. בנוסף מתבצע ניטור שוטף על כל הרשת וכל מחשב או שרת ללא אנטי וירוס מטופל.

בדו"ח סטטוס זה נכתב כי החלפת התוכנה שמתבצעת אמורה לפתור את הבעיה. עד סוף השנה יוחלפו כולם עד כה הוחלפו כ- 200 כפיילוט. לשאלת הביקורת מסר מנהל אבטחת מידע ביום ה 28.8.2011 כי **"מנהלת האגף הנחתה להתקדם עם הפרוייקט. יש תוכנית עבודה להמשך הפריסה המתבצעת בימים אלה. סטטוס ההפצה – נכון לרגע זה כ 750 תחנות ושרתים. התהליך יסתיים לקראת סוף אוקטובר השנה."**.

בתגובה לממצאים מסר מנהל אבטחת מידע לביקורת כי: **"שירותי האנטי וירוס העירוניים מבוצעים בכל הרשתות (עירייה, ארגון, אתר האינטרנט העירוני, אתר תקשוב החינוך).**

שירותי האנטי וירוס מורכבים מ: אנטי וירוס ב perimitter **מתוצרת** safenet **שמבקר כל מה שנכנס ויוצא מהרשת העירונית (תקין), אנטי וירוס בתוך ה** exchange **מתוצרת** Microsoft **ומורכב מ 4 מנועים שונים (תקין), אנטי וירוס בתחנות ובשרתים (ראה פירוט להלן), ואנטי וירוס** forfront **מתוצרת** Microsoft **בשרתי ה -** mos **(לא מוטמע באופן מלא).**

ב 3 שנים האחרונות השתמשה העירייה ב trendmicro **כמוצר האנטי וירוס בתחנות ובשרתים. המוצר לקה בחסר ב3 תחומים: יכולות ניהול גרועות, התנתקות תחנה או מעבודה מול השרת (שמשמעותה הפסקת קבלת עידכונים ופקודות משרת הניהול) ויכולות תמיכה גרועות. הוחלט לעבור למוצר אחר ובוצע פיילוט עם חברת מיקרוסופט להטמעת** Forefront **כאנטי וירוס העירוני. הפיילוט נכשל והוחלט לעבור ל** sep **המספק אנטי וירוס ויכולות נוספות. נכון לחודש נובמבר 2011 בוצע מעבר לכ- 4050 תחנות עבודה ושרתים. לקראת סוף השנה תעבור כל העירייה למוצר החדש.".**

<u>לתשומת לב:</u>

התייחסויות המבוקרים ואחרים לטיוטת ממצאי הביקורת בשלב אימות הממצאים, מצורפות לדוח בפרק הנספחים, ומהוות חלק בלתי נפרד מדוח הביקורת. הנספחים להתייחסויות (אם צורפו) שמורים במשרד מבקר העירייה.

נספח א – התייחסות אגף מחשוב ומ"מ, מתאריך 28.11.11.

מסקנות

כללי

89. מרבית המלצות דוח הביקורת בהיבטים של ניהול, קביעת מדיניות, קביעת נהלים ותהליכי עבודה יושמו על ידי אגף המחשוב ומ"מ, בעוד שהמלצות הקשורות בנושאים הנוגעים לביצוע מעקב, בקרה והטמעה של נושא אבטחת מידע בוצעו בצורה חלקית ולא מספקת.

90. היקפי העבודה של היחידה גדלו, גידול אשר קיבל ביטוי בהגדלת התקציב ובהגדלת כ"א. ההשקעה התקציבית הגדלה כמו גם הגדלת כ"א בנושא אבטחת מידע מעידה, לדעת הביקורת, על תפיסת החשיבות של נושא אבטחת מידע בעיני הנהלת העירייה.

91. המידע אודות ההשקעה התקציבית ביחידה הינו מבוזר ולביקורת נדרש תהליך של איסוף מידע ממקורות שונים לצורך קבלת תמונה מדויקת של ההשקעה התקציבית.

92. הביקורת סבורה כי יחידת אבטחת מידע משקיעה משאבים רבים במשימות תפעוליות כגון מתן הרשאות בעוד שהיא משמשת כגוף מטה מתכנן, מנהל ומבקר את הביצוע של נושא אבטחת מידע בעירייה. לדעת הביקורת מצב שבו אותה יחידה מבצעת משימות תפעוליות ובקרה כאחד אינו מיטבי.

93. לדעת הביקורת אחד התפקידים החשובים של אבטחת מידע הוא ביצוע בקרות שוטפות על אופן יישום המדיניות בנושא, אולם לדעת הביקורת נושא זה מטופל בצורה לא מספקת.

תקציב וכ"א

94. יש הפרדה בין תקציב אבטחת מידע לבין התקציב הכולל של האגף. במסגרת התקציב השוטף והתקציב הבלתי רגיל נקבעו סעיפי תקציב ייעודיים לאבטחת מידע, אולם אין הבחנה בין עלות עובדי אבטחת מידע לבין עלות השכר הכולל של ענף ארכיטקטורה, בספר התקציב.

מדיניות, נהלים ותהליכי עבודה

95. נושא אבטחת מידע עוגן במסמך מדיניות בנושא אבטחת מידע, הוגדרו נהלים בנושא, הוגדר תפקידו של ממונה אבטחת מידע, הוגדרו סמכויות ואחריות ליישום המדיניות והוקמה ועדת היגוי:

א. לא כל התחומים המוגדרים במסמך המדיניות יושמו בתקופת הביקורת - מסמך 'מדיניות אבטחת מידע' כולל פירוט של תחומים שונים, ובין היתר פירוט תחומי האבטחה; מבנה ארגוני לניהול וליישום אבטחת מידע; הגדרה של רמה מחייבת של אבטחת מידע; סמכות ואחריות ועוד.

ב. ועדת היגוי לנושא אבטחת מידע אמורה לייעץ למנכ"ל העירייה אודות מדיניות אבטחת המידע ולהנחות את הממונה על אבטחת המידע בהתאם למדיניות זו, אולם ועדה זו לא מתכנסת בצורה סדירה וקבועה.

ג. תהליך אישור הנהלים שונה וקוצר על פי המלצות דוח קודם.

ד. המלצות דוח קודם בנושא הגדרת נהלים יושמו. בפורטל אגף המחשוב יש נהלים, הנחיות עבודה וטפסים, אולם אין אחידות באופן כתיבת הנהלים וחלק מהנהלים אינן עדכניים ו/או אינם מיושמים במלואם.

96. מודעות והדרכה

א. הביקורת סבורה כי נעשות פעולות רבות של הגברת המודעות ומתן הנחיות לעובדים אולם לא מתקיימות מספיק פעולות המיועדות לדרג הניהולי. לדעת הביקורת פעולות אלו נעשות יותר בהיבט של תפעול ותחזוקה ופחות כמהלך שמטרתו עידוד חשיבה ולקיחת אחריות.

ב. הביקורת סבורה כי לא נעשות הדרכות מקצועיות מספיקות לעובדים באבטחת מידע.

ג. עובדים חדשים הנקלטים בעירייה באגפים אחרים אינם עוברים הכשרה ייעודית בנושא אבטחת מידע.

97. בקרה

חל שינוי משמעותי בהיקף ובסוג הבקרות המבוצעות על ידי אבטחת מידע. הבקרות הנדרשות הוגדרו על ידי אבטחת מידע בתוכנית עבודה שיטתית ומקיפה, אולם למרות זאת חלק מן הבקרות אינן מבוצעות או שהמידע על ביצועם אינו מתועד.

98. אבטחה

א. היחידה לאבטחת מידע לא מבצעת מספיק ביקורות על אבטחה פיזית למרות שעל פי נוהל אבטחה פיזית מנהל אבטחת מידע אחראי לביצוע בקרות תקופתיות על מאגרי מידע ונתונים או גיבויים ומנהל אבטחת מידע או מי מטעמו אחראי לבצע ביקורת אבטחת מידע פיזית, אחת לשנתיים ולהגיש את ממצאיה למנהלי היחידה ולמנהל אגף המחשוב.

ב. יישום כלים המאפשרים זיהוי חד ערכי של משתמשים אשר ביצעו שינויים במידע או בתכנה, או ניגשו למידע רגיש, תוך פירוט ורישום של כל סוג פעילות שבוצעה, מועד ביצועה ופרטי המבצע מתבצע בעיקר במערכות חדשות, משום שהרישום הוא בהיקף של מיליוני תנועות ביממה. המלצה זו מדוח קודם אינה ניתנת ליישום נרחב ואוטמטי במערכות הישנות של העירייה. לאור ממצא זה יש לבחון את הסיכונים הקיימים בכל מערכת.

99. כרטיס חכם

לא נעשה תהליך של בחינת הכדאיות/עלויות לאור הניסיון הקיים בשימוש בכרטיסים חכמים ולא נבחנו העלויות ביחס לסיכונים.

100. מחשבים ניידים ו DOK

א. נכתב נוהל בנושא המחשבים הניידים.

ב. בנושא ה DOK (disk on key) לא חל כל שינוי בנושא זה למרות בחינת השימוש ב'תחנות הלבנה'.

101. מנהלי מאגר

א. נושא ההרשאות טופל על ידי מעבר לשימוש בטופס ממוחשב למתן הרשאות.

ב. מנהלי המאגרים אינם מקבלים חיווי שוטף על פעולות חריגות שמבוצעות במאגרים עליהם הם אחראים, למרות שעל פי הוראות חוק הגנת הפרטיות האחריות מוטלת על מנהל המאגר ומנהל אבטחת מידע ביחד ולחוד. לא נבנתה תוכנית ייעודית לנושא זה.

102. טיפול במתן הרשאות ו'הקמת משתמש'

א. בנושא הטיפול במתן הרשאות ו'הקמת משתמש' חל שינוי מהותי ונושא זה מנוהל, לדעת הביקורת, בצורה טובה.

ב. נבנה מנגנון ממוחשב להעברת טפסים בין הגורמים השונים לצורך טיפול בהרשאות.

ג. אנשי יחידת אבטחת מידע עוסקים בטיפול בהרשאות. היקף העבודה המוטל על יחידת אבטחת מידע, בטיפול בטפסי בקשה למתן הרשאות הוא גדול מאוד. תהליך זה גוזל שעות עבודה רבות של עובדי היחידה.

ד. הגדרת ההרשאות ניתנת לעובד ולא לתפקיד. במערכות המחשוב החדשות משייכים עובד לתפקיד ובמערכות המחשוב הישנות לא ניתן לעשות כן ולפיכך יכולים להיווצר מקרים שבהם לא מתבטלות באופן מיידי הרשאות של אדם שעוזב תפקיד מסוים.

ה. יש הגדרה של תהליך רישום וביטול להרשאות גישה למערכות מידע ולשירותים.

ו. עדיין לא ניתן מענה למיפוי הרשאות לקוח על מנת שניתן יהיה למצוא בצורה קלה ופשוטה את כל ההרשאות של משתמש אחד, אלא רק לאחר חיפוש במספר מערכות.

103. DBA

בקרות על בסיסי הנתונים מבוצעות על ידי מחלקת ה DBA.

104. פרויקט ה- DRP

במסגרת פרויקט ה DRP נערך מיפוי של מערכות העירייה והגדרת רמות הקריטיות של כל מערכת, הפעילות בתחום זה הועברה לפרויקטור במטה חטיבת התכנון.

105. גיבוי

הגיבויים נעשים על ידי מנהלי הרשת.

106. סקר סיכונים

לא מתבצעת הערכת סיכונים וסקר סיכונים תקופתי המבוסס על פעילות העירייה ומערכות המידע שברשותה, מלבד סקר חד פעמי שבוצע בדצמבר 2007.

107. יכולת הניטור והמעקב

א. ברשות אבטחת מידע יש כלים טכנולוגיים למניעת זליגת מידע, אולם לא התקבלה החלטה ניהולית לצורך הקצאה של שעות הטמעה, פיקוח ובקרה, וביצוע ניטור מדגמי של בעלי הרשאות לנושא זה.

ב. ניטור אבטחתי: נעשית פעילות אבטחת מידע רשתית הכוללת ips פנימי, אולם אין בדיקה פרטנית של כל מסוף, בדיקה טכנולוגית לאיתור תוכנות מאיימות ופוגעניות בנקודות קצה ובנוסף אין בדיקה פיזית של אתרים חדשים.

ג. בקרה על בסיס הנתונים: קיימת תוכנה לבקרה על בסיס הנתונים, התוכנה מבצעת בקרות ברמת הניטור בלבד, אולם לא מבוצעות בקרות באופן כללי.

108. טיפול בענייני משמעת

הביקורת סבורה כי העובדה שאין עבירות משמעת בנושא אבטחת מידע אינה סבירה ויכולה להעיד על חוסר אכיפה/בקרה בנושא זה.

109. מיקום ארגוני

יחידת אבטחת מידע כפופה לארכיטקט הראשי, כפיפות זו מבטאת לדעת הביקורת את תפקידה של היחידה כגוף מעצב ומטמיע של מתודולוגיה, מנהל ועורך בקרות.

110. רכזי המחשוב

רכזי המחשוב נתפסים על ידי יחידת אבטחת מידע כשותפים מרכזיים להטמעת הנושא והדבר בא לידי ביטוי בנהלי עבודה של היחידה. הביקורת סבורה כי קיימת שונות בהגדרה ובביצוע תפקיד רכז המחשוב ביחידות השונות ולכן לא מומלץ להגדיר אותם כשותפים מרכזיים, אלא רק לאחר שתפקידם יוגדר ויבוקר בצורה שיטתית.

111. קליטת עובד חדש

בנושא קליטת עובד חדש ומתן הרשאות למערכת לא נעשית בדיקה מעמיקה אודות העובד, גם במקרים שבהם הוא מיועד לתפקיד שיש בו גישה למאגרי מידע רבים ורגישים, כדוגמת מנהלי רשתות.

112. תפקידי היחידה

מספר בעלי תפקידים ביחידה עוסקים במישור התורה וקביעת מדיניות אבטחת מידע אבל עדיין מרבית בעלי התפקידים עוסקים בעיקר במישור התפעול ובעיקר במתן הרשאות.

113. שחזור חסימה

בנושא שחזור סיסמא נקבע נוהל אך נוהל זה מיושם בצורה חלקית ואינו מבוקר.

114. טיפול בתקלות על ידי מרכז תמיכה ושירות

א. טיפול בתקלות מחשב נעשה מרחוק באמצעות תוכנה, על ידי עובדי מרכז השירות, הטיפול מרחוק נעשה אך ורק לאחר שהלקוח מאשר את ההשתלטות בזמן אמת על המחשב שלו.

ב. יש מקרים שבהם נעשה שימוש בתוכנת demwear. השימוש בתוכנה זו אינו מחייב קבלת אישור להשתלטות מהלקוח בזמן אמת, ולפיכך ניתן לכאורה להשתלט על המחשב מרחוק מבלי ידיעת הלקוח.

115. הגדרת סיסמאות

כל ההמלצות בנושא הגדרת סיסמא יושמו בנהלים ובתהליכי עבודה.

116. מנגנונים לניהול בקרות גישה במערכות חדשות

המלצת דוח קודם לגבי הכללת מיטב המנגנונים לניהול בקרות גישה במערכות המחשב מיושמת.

117. שרתי האנטי וירוס

מתקיים תהליך של החלפת תוכנת אנטי וירוס בכל העירייה.

המלצות

118. הביקורת סבורה כי השינויים שחלו בהיקפי העבודה של אבטחת מידע ובאופייה מחייבים את אגף המחשוב ומ"מ בחינת הפרדת פעילות הקשורה בתפעול מפעילות הקשורה בבקרה.

119. המידע אודות ההשקעה התקציבית ביחידה הינו מבוזר וקיים קושי לקבל מידע המאפשר בחינה והשוואה לאורך מספר שנים. מומלץ כי מידע מרוכז יהיה בידי גורם אחד מאגף התקציבים/אגף המחשוב.

120. באחריות הנהלת האגף לבצע מעקב אחר יישום התחומים שהוגדרו במסמך מדיניות אבטחת מידע ולקיים את ישיבות ועדת ההיגוי בקביעות ובתדירות סבירה.

121. באחריות מנהל אבטחת מידע לערוך בחינה של כל הנהלים לצורך ביצוע סטנדרטיזציה ותיקוף מחודש. מומלץ להגדיר בכל נוהל תהליכי בקרה לבחינת יישומו בפועל.

122. הביקורת סבורה כי נדרשות פעולות ייעודיות לדרג הניהולי, שיעודדו חשיבה ולקיחת אחריות. מומלץ לשקול הקמתו של פורום חשיבה שיתכנס אחת לשנה לדיון בנושא, שמטרתו שיפור תהליכי עבודה והגברת תחושת האחריות. נושא זה נמצא בתחום האחריות של יחידת אבטחת מידע.

123. יש לקיים הכשרה ייעודית בנושא אבטחת מידע לעובדי אבטחת מידע, הכוללת השתלמויות וקורסים בתדירות גבוהה, מתוך הנחה כי החידושים בעולם אבטחת המידע מתעדכנים ומתחדשים בתדירות גבוהה. נושא זה נמצא בתחום האחריות של יחידת אבטחת מידע.

124. באחריות אגף משאבי אנוש לשלב בתהליך הקליטה של עובד חדש בעירייה הכשרה ייעודית בנושא אבטחת מידע.

125. באחריות ועדת ההיגוי לנושא אבטחת מידע לוודא כי תוכנית הבקרות מעודכנת ושכל פעולות הבקרה המוגדרות בה מבוצעות ומתועדות.

126. הביקורת סבורה כי כל פעילות שינוי הנעשית בצורה מצומצמת כפיילוט ראוי שתבחן בסיומה לצורך הפקת לקחים על ידי היחידה המבצעת. במקרה של כרטיסים חכמים לא נעשה תהליך של בחינת הכדאיות/עלויות לאור הניסיון הקיים בשימוש בכרטיסים חכמים ולא נבחנו העלויות ביחס לסיכונים.

127. באחריות יחידת אבטחת מידע לבנות תוכנית ייעודית בנושא עדכון מנהלי המאגרים בפעילות חריגה.

128. נדרש עדכון מיידי של המערכות במקרה שמישהו עוזב את העירייה או מחליף תפקיד, באחריות אבטחת מידע להגדיר תהליכי עבודה בהתאמה לאגף משאבי אנוש, כך שהתהליך יהיה אוטומטי מול מרכז התמיכה.

129. באחריות אבטחת מידע למצוא מענה למיפוי הרשאות לקוח על מנת שניתן יהיה למצוא בצורה קלה ופשוטה את כל ההרשאות של משתמש אחד, מבלי לערוך חיפוש במספר מערכות.

130. הביקורת רואה חשיבות רבה בביצוע סקר סיכונים, כאמצעי שיאפשר קבלת החלטות טובה יותר. באחריות ועדת ההיגוי לנושא אבטחת מידע לבצע מעקב אחר נושא זה.

131. באחריות ועדת ההיגוי לנושא אבטחת מידע לקבל החלטה ניהולית בנושא השימוש בכלים טכנולוגיים לצורך מניעת זליגת מידע ובקרה על בסיס נתונים. הביקורת ממליצה כי החלטה זו תתקבל לאחר ביצוע תהליך של מיפוי הסיכונים.

132. יש לבחון את תפקיד רכזי המחשוב במשימות הקשורות באבטחת מידע רק לאחר שתפקיד הרכז יוגדר ויוטמע בצורה אחידה.

133. הביקורת סבורה כי מתן גישה לעובד חדש למאגרי מידע מסווגים ורגישים מחייב קביעת מדיניות לגבי אופי והיקף בדיקת הרקע של העובד, לאחר הפעלת שיקול דעת לגבי הסיכונים. באחריות ועדת ההיגוי לפעול לקידום הנושא בשיתוף משאבי אנוש.

134. הביקורת ממליצה להנהלת האגף לבחון הוספת כוח אדם ו/או העברת המשימות התפעוליות, על מנת שהיחידה תפעל בצורה מיטבית. לדעת הביקורת תפקידי היחידה צריכים להיות בעיקר במישור התכנון, בקרה והכשרה ולכן מרבית הפעילות של עובדי היחידה צריכה להיות קשורה בהיבטים אלו.

135. בנושא שחזור סיסמא – באחריות יחידת אבטחת מידע לבצע בקרות על אופן יישום הנוהל והכשרות ייעודיות של מרכז השירות והתמיכה. כמו כן הביקורת סבורה כי יש לבחון אפשרות של מתן מענה טכנולוגי שיאפשר שדרוג תוכנה בצורה עצמאית, על ידי העובד, ללא צורך בסיוע של מרכז התמיכה.