אבטחת מערכות מידע

כללי

פרק א - מבוא

1. אבטחת מידע - **"מכלול הפעולות והאמצעים הננקטים והמיושמים במערכת מידע המתופעלת באופן עצמאי או במשולב עם מערכות אחרות כדי להגן עליה מפני פגיעה בזמינותה, ובשרידותה, מפני חשיפה ושינוי במזיד או בשוגג של המידע ומפני פגיעה בשלמות המידע ובאמינותו"** (תקן ישראלי מס' 1495 חלק 6 סעיף 3.10).

2. השימוש במערכות מידע הינו מחוייב המציאות כיום, ולא ניתן לדמיין כיצד ניתן לתפעל ארגון כמו עיריית תל-אביב-יפו בלעדיהן. התפתחות המערך הטכנולוגי התומך בפעילות הארגונית ו/או העסקית, הכולל בתוכו את מערכות המידע, יוצר הזדמנויות עסקיות חדשות ומאפשר התייעלות בפעילות העירייה הכוללת.

3. יחד עם זאת, שימוש במערכות מידע חושף את העירייה לסיכונים המאיימים על שלמות המידע האגור בהם, אשר עלולים לפגוע בפעילותה. הסיכונים יכולים להיווצר החל מפגיעות אשר יש בהן כדי לשבש את הפעילות השוטפת ולמנוע מהעירייה להציג את התוצאות להן היא מחוייבת, חדירות העלולות לחשוף את העירייה לתביעות משפטיות או לחילופין לשתקה באופן חלקי ו/או זמני, ועד כדי פגיעות אשר יש בהן כדי למוטט אותה, לדוגמה:

   א. חדירה למערכות המחשב מחוץ לעירייה או מתוכה, למטרות חשיפת פרטים אישיים של עובדים ולקוחות;

   ב. פגיעה במסדי הנתונים על ידי מחיקה או שיבוש אחר שאינו מאפשר שימוש בהם;

   ג. פגיעה בחומרה, במערכות ההפעלה או בתוכנה, הפוגעת בזמינות המערכת.

   לפיכך, על הנהלת העירייה להגן על המידע אודות לקוחותיה, עובדיה וכל הגורמים הבאים במגע עימה.

4. לצורך כך, על העירייה להקצות משאבים (כספיים, אנושיים וטכנולוגיים) ליישום מערכי אבטחת מידע יעילים, הכוללים מנגנונים ותהליכי בקרה המסוגלים לספק את המענה הנדרש לצרכיה.

5. בקרות ומנגנוני אבטחת מידע מטפלים במניעה, גילוי, תיעוד והתרעה של חשיפה ואירועי אבטחת מידע. אבטחת המידע מטפלת בנושאי זמינות (Availability), אמינות (Integrity) וחשאיות (Confidentiality).

   הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"אבטחת מידע להערכתנו אינה מטפלת בזמינות (בזמינות מטפל תפעול). אנו פנינו למספר חברות וארגונים גדולים במשק**

הישראלי לקבל תמונת מצב כיצד הנושא מטופל בארגונם (בזק, סלקום, קופ"ח, חברת חשמל, מקורות, בנק, מי עדן, וכו'). עד כה התקבלו תשובות מבזק ומבנק לאומי למשכנתאות ובשניהם DRP אינו קשור לאבטחת מידע.".

הביקורת מציינת בהתייחס לתגובת הנהלת אגף המחשוב כי זמינות הנתונים מהווה מרכיב חשוב ועיקרי בנושא אבטחת מידע. זמינות הנתונים באה להבטיח שהמידע בעירייה יהיה נגיש וזמין לכל הגורמים הרלוונטיים, בכל נקודת זמן. זמינות אינה עוסקת אך ורק בנושא ה- DRP.

6. על העירייה להגדיר עקרונות שימוש מאובטח במערכות המידע שברשותה. עקרונות אלה מגדירים את אופן השימוש בשרתים, מחשבים נייחים, מחשבים נישאים, ציוד תקשורת וכל ציוד מחשובי אחר המשמש את העירייה לצורכי עיבוד או שמירת מידע.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"הוכן מסמך מדיניות והתקבלה התייחסותו והערות סמנכ"ל תכנון. מנהל אבטחת מידע לא הגיע להטמעת השנויים והמשך התהליך. השינויים יוטמעו בנוהל ע"י מנהל אבטחת מידע עד ה- 15.12. מתוך מטרה שעד ה- 1.1 המסמך המתוקן יועבר לאישור הנהלת העירייה".**

7. על עקרונות אלו להתייחס לנושאים כגון שימוש ברשת האינטרנט, שימוש בדואר אלקטרוני, שמירה וטיפול במידע, הרשאות גישה לוגיות ופיזיות, שמירה ושימוש בסיסמאות, נעילת המחשב בפני גישה כאשר אינו בשימוש וכדומה.

8. יישום מדיניות אבטחת המידע הינו תהליך מורכב הדורש תכנון קפדני בהתאם לאופי העירייה. לשם יישום המדיניות יש לפעול באופן הבא:

   א. הקמה והטמעה של נושאי ניהול אבטחת המידע בעירייה;

   ב. בניית תוכנית עבודה ליישום המדיניות;

   ג. עדכון הגדרת מדיניות אבטחת מידע, סיווג נכסים וביצוע הערכת סיכונים;

   ד. תכנון אופן יישום בקרות אבטחת המידע, כולל כתיבת נהלים;

   ה. יישום בקרות ומנגנוני אבטחת מידע.

קווים כלליים לשימוש במערכות מידע בעיריית תל-אביב-יפו

9. עיריית תל-אביב-יפו מנהלת ומחזיקה ברשותה 147 מאגרי מידע שונים, חלקם בעלי רגישות גבוהה. מאגרי המידע מנוהלים על ידי 97 מנהלי מאגרים שונים אשר ממלאים בנוסף תפקידים בכירים בעירייה.

10. נכון למועד עריכת הביקורת מערכות המידע משמשות תחליף כמעט מושלם, לחלק מהמסמכים שאוחסנו בקלסרים וארכיבים.

11. לרוב, הנתונים המצויים במערכות המידע הינם רגישים ובעלי ערך רב, על כן יש לשמור עליהם הן מבחינת השחתה והן מבחינת גניבה.

12. לאור מה שצויין לעיל וחשיבות הנושא, החליטה הביקורת לבצע בדיקותיה בתחום אבטחת מידע בעיריית תל-אביב-יפו. הביקורת התמקדה בבדיקת מידת יישום מנגנונים ובקרות נדרשות, בחינת המבנה הארגוני, מערך התפקידים, תחומי אחריות ומבני סמכויות, פעילויות, תהליכי עבודה ותקציבים.

13. הבדיקה כללה:

א. ביצוע ראיונות עומק עם מנהלים ועובדים באגף המחשוב, כולל כל עובדי היחידה לאבטחת מידע.

ב. עיון וניתוח מסמכי עבודה, פרוטוקולים, דוחות תקציב ואחרים, תרשומות פנימיות, נהלים ועוד.

ג. ביצוע תצפיות ובדיקות אבטחה פיזית, לוגית, אנושית.

ד. בחינת החוקים והתקנות בתחום אבטחת מידע ומידת יישומם במערך אבטחת מידע בעיריית תל-אביב-יפו.

ה. בחינת הסיכונים.

14. הביקורת לא בדקה את פעילות אבטחת המידע ברמת מאגרי המידע, והשימוש שנעשה בתחום ברמת משתמש קצה, אלא רק את אופן פעילותה ותיפקודה של יחידת האבטחה העירונית.

15. הביקורת נערכה במהלך החודשים אפריל 2006 עד ספטמבר 2006.

16. מילון מונחים מקצועיים מצורף לדוח ביקורת זה כנספח א'

פרק ב - הוראות החוק ותקני ISO

17. תקן ISO 17799 נועד לקבוע בסיס משותף לפיתוח של תקני אבטחה ארגוניים ושל שיטות אפקטיביות לניהול אבטחה, וכן לספק בטחון (בכל הנוגע לאבטחת מידע) בעסקים בין - ארגוניים. התקן פורסם בדצמבר 2000, והינו אימוץ של התקן הבריטי BS 7799 (חלק שני).

18. הרשויות המקומיות והחברות בארץ מחוייבות לעמוד בדרישות החוק להגנת הפרטיות בנושא אבטחת מידע אולם אינן מחוייבות לעבוד על פי כללי תקני ה-ISO. למרות האמור, מרבית הארגונים פועלים על פי הקווים המנחים המוגדרים בתקן, גם אם אינם מוסמכים באופן רשמי על ידי גוף הסמכה חיצוני. הסיבה לכך נובעת מהעובדה שהתקן מהווה מסגרת ברורה, מספק הנחיות שיטתיות לעבודה וטומן בחובו את הבסיס לאבטחת מידע. כיום, (נכון למועד עריכת הביקורת),

מקובלת התפיסה כי ארגונים אשר לא פועלים על פי הכללים המנחים שמוגדרים בתקן, חושפים את עצמם לאיומים שונים העלולים לפגוע במערכות המידע שלהם.

19. התקן מפרט 10 קריטריונים:

א. מדיניות אבטחת מידע – נהלים או הנחיות עבודה כתובים המהווים בסיס לניהול השוטף ולקידום יעדים.

ב. ארגון אבטחת מידע – חלוקת תפקידים נכונה והיררכית בין כל עובדי מחלקת אבטחת מידע, תוך כדי רישום נהלים ברורים לשם הגנה על אבטחת המידע וביצוע פעולות במצב חירום.

ג. בקרת המידע וסיווגו – סיווג המידע על פי רמתו המתאימה.

ד. אבטחת הסגל – תדריכים לעובדי מחלקת אבטחת המידע אשר תכלול: דגשים על חשיבות מערך האבטחה, דוגמאות לתקריות בנושא ויצירת מנגנוני דוחות.

ה. אבטחת סביבת העבודה ואבטחה במישור הפיזי – נורמות התנהגות הכוללות שמירה על אזורים מסווגים ובטיחות מתקנים.

ו. ניהול וכללי עבודה עם המידע – מזעור הסיכון הנוצר בעקבות קריסת המערכת.

ז. בקרת הגישה – פיקוח ובקרה על גישה לרשת או נספחיה.

ח. יצירת מערכות ותמיכה – עמידה בסטנדרטים שיובילו את הטמעתם של פרויקטים עתידיים.

ט. אבטחת פעילות תקינה של המערכות – יכולת לשמור על מכלול התהליכים המכריעים במצב חרום או בעת אסון.

י. תאום – מידת התיאום בין תקן ISO 1779 לבין הנורמות והתקנים המשפטיים.

מממצאי הביקורת, כמפורט בפרקים ז'-כא', עולה כי העירייה אינה עומדת באופן מלא בכל קריטריונים המפורטים בתקן.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"העירייה אינה עובדת לפי ISO, מכאן שהתקן אינו מחייב את העירייה וההשוואה אליו יכולה להיות רק בנקודת התייחסות כמסגרת כוללת או מנחה. אבטחת מידע עושה בו שימוש כמסגרת של כללים."**.

בהתייחס לתגובת הנהלת אגף המחשוב מפנה הביקורת לסעיף 18 לעיל.

20. הוראות חוק מאגרי מידע

א. מאגר מידע לפי הגדרתו בחוק הגנת הפרטיות (להלן:"החוק") הינו **"אוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב".**

ב. בעבר, כשהיה נגנב מידע מארכיון או ממשרד, תוך פרק זמן קצר הייתה מתגלה ונחקרת הגניבה. כיום, בעידן של מאגרי המידע, קשה מאוד לדעת כשנגנב מידע. מסיבות אלו ואחרות נחקק חוק הגנת הפרטיות הדן בין היתר באופן שבו צריך לאבטח מאגרי מידע.

ג. חוק הגנת הפרטיות הוא חוק כללי, העוסק בהגנת פרטיותו של אדם. פרקים ב' וד' לחוק עוסקים בהגנת הפרטיות במאגרי מידע ממוחשבים. החוק מחייב רישומו של כל מאגר מידע המכיל מידע אישי אצל רשם מאגרי המידע במשרד המשפטים. המחזיקים, המנהלים ובעלי מאגרי המידע נדרשים להגן עליו לבל יועבר ממנו מידע למי שאינו מורשה לכך. החוק דורש הגנה למידע רגיש, המוגדר כ- **"נתונים על אישיותו של אדם, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו".**

ד. כחלק אינטגראלי מתפקידו של מנהל מאגר, עליו ליישם את הוראות חוק הגנת הפרטיות במאגרי מידע.

סעיף 17 לחוק קובע כי **"בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע".**

ה. בסעיף 17ב לחוק, שעוסק בתקנות למינוי ממונה על אבטחת מידע, נקבע כי:

"(א) הגופים המפורטים להלן חייבים במינוי אדם בעל הכשרה מתאימה שיהיה ממונה על אבטחת מידע (להלן – הממונה) :

(1) מחזיק בחמישה מאגרי מידע החייבים ברישום לפי סעיף 8;

(2) גוף ציבורי כהגדרתו בסעיף 23;

(3) בנק, חברת ביטוח, חברה העוסקת בדירוג או בהערכה של אשראי "

ו. סעיף 17ב(ב) לחוק קובע, כי **"בלי לגרוע מהוראות סעיף 17, הממונה יהיה אחראי לאבטחת המידע במאגרים המוחזקים ברשות הגופים כאמור בסעיף (א)".**

ז. מהוראות החוק עולה כי יש למנות גוף אשר יבצע את אבטחת המידע, אף על פי כן חלה אחריות משותפת להגנה על מידע רגיש במאגר על מנהל המאגר וממונה אבטחת המידע ביחד ולחוד.

פרק ג - מבנה ארגוני ומערך תפקידים

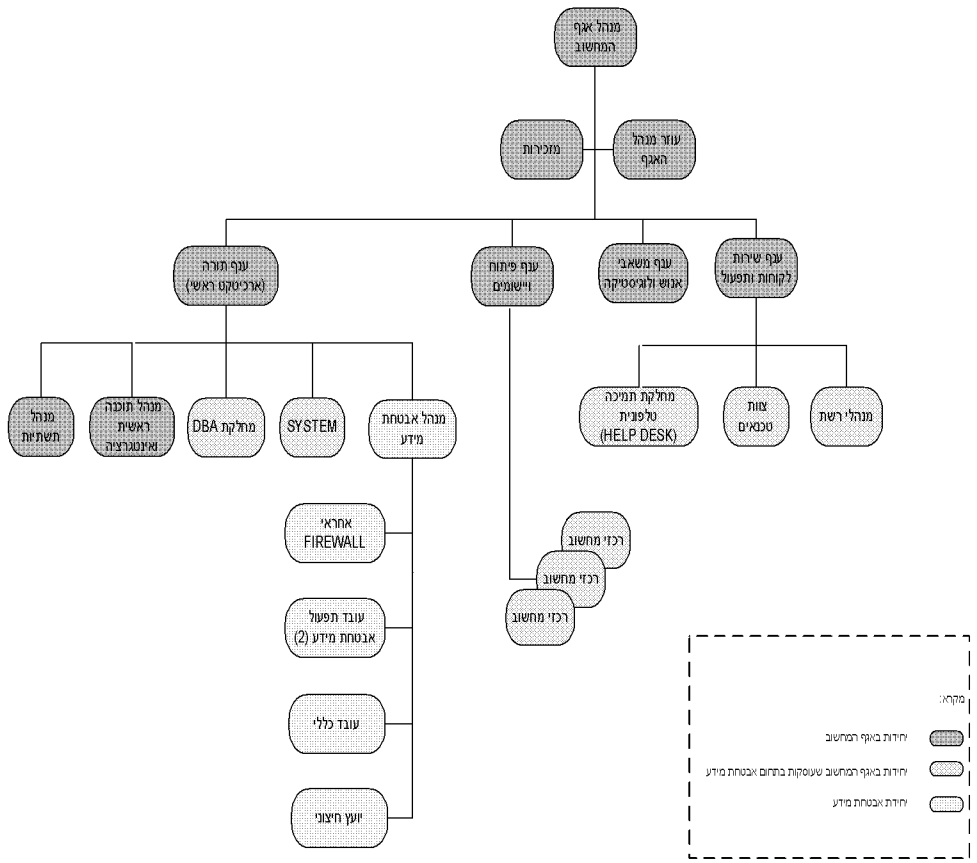
21. יחידת אבטחת מידע הינה הגוף המקצועי בעיריית תל-אביב-יפו, האמון הן על התורה והן על תפעול תחום אבטחת מידע. היחידה כפופה לאגף המחשוב כאשר מנהל היחידה כפוף לארכיטקט הראשי (מנהל ענף תורה), הכפוף ישירות למנהל אגף המחשוב (ראה תרשים: מערך אבטחת מידע – מבנה ארגוני קיים).

22. תאור מבנה היחידה:

23. יחידת אבטחת מידע מונה חמישה עובדים קבועים ויועץ חיצוני, על פי הפירוט הבא:

מנהל היחידה:	ניהול וריכוז פעילות יחידת אבטחת מידע.
עובדי התפעול ביחידה:	עובד האחראי על מתן הרשאות ופתרון תקלות ברשת המקומית. (נש"מ).
	עובד האחראי על כל הקשור לתכנות (נש"מ). נכון למועד עריכת הביקורת עובד יום בשבוע בתחום ובשאר מלוא משרתו מייצג את תחום אבטחת מידע בפרוייקט מחו"ג.
	עובד האחראי על מתן הרשאות ופתרון תקלות ברשת המקומית. (סטודנט בחצי משרה).
מנהל רשת אבטחת מידע:	עובד האחראי על כל הנושאים הטכניים והתפעוליים, ובהם: שרתי חומת האש (Fire Wall), שער הגישה, הזדהות חיצונית, וקישורים חיצוניים. Login script, אנטי וירוס, GPO. (עובד עירייה במשרה מלאה).
יועץ חיצוני:	יועץ חיצוני המסייע למנהל היחידה ולעובדיה (בהיקף של 650 שעות לשנה).

להלן תרשים מערך אבטחת המידע - מבנה ארגוני קיים:



ממצאים

24. בעיריית תל-אביב-יפו קיימים מספר גורמים העוסקים בתחום אבטחת המידע, אם באופן ישיר ואם באופן עקיף, חלקם כפופים לאגף המחשוב וליחידת אבטחת מידע, וחלקם משוייכים לאגפי העירייה השונים.

25. ייעוד ומטרות - תפקידה העיקרי של יחידת אבטחת מידע הוא להגן על נכסי העירייה הכוללים מידע על פעולותיה, עובדיה ולקוחותיה (תושבים ואזרחים), מפני גורמים חיצוניים וגורמים פנים ארגוניים. הגנה על מערכות המידע משמעותה, שמירה על שלמות ותקינות המידע ומניעת הצגת המידע בפני גורמים לא מורשים. על מנת למלא את ייעודה אחראית היחידה, בין היתר, על שרת ה– Fire Wall, גיבוי המערכת, מתן הרשאות למשתמשים, אנטי וירוס, הקשחת תחנות ושרתים, אבטחת רשת התקשורת, יישום והטמעת בקרות האבטחה השונות ותחזוקה שוטפת שלהן.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"היחידה אחראית על נוהל הגבויים. הגבויים בפועל מבוצעים ע"י התפעול. קיימים שני נהלים לנושא הגבוי, הראשון: נוהל גבוי רשתות חיצוניות שפורסם ופעיל, וקיים נוהל שני לגבוי הנתונים ברשת הפנימית והוא כתוב ונמצא בתהליכי אישור בתוך אגף המחשוב. הנוהל יאושר ע"י אבטחת מידע עד ה- 15.12 ויופץ פנימית בתוך אגף המחשוב להתייחסות. הנוהל יפורסם עד ה- 15.2. אם זאת, מתבצע היום גבוי של השרתים בהתאם לנוהל קיים באגף שצבר עם הזמן שנויים ועדכונים ומטרת הנוהל החדש לעשות סדר בהוראות ובעדכוני הנוהל לכדי נוהל ברור ונעים ולקחת בחשבון עדכונים טכנולוגיים קיימים ועתידיים (כדוגמת ספריית הגבוי שתיכנס לשימוש במהלך דצמבר-ינואר). בינתיים מתבצע הגבוי בהתאם לנוהל החדש למרות שלא פורסם."**.

26. על פי הממצאים מרבית שותפי התפקיד, הגורמים העוסקים בנוסף באבטחת מידע, שייכים לאגף המחשוב. קבוצה ראשונה של שותפי תפקיד כפופה (על פי החלוקה למחלקות) לארכיטקט הראשי מנהל ענף תורה. המשמעות הינה כי מקור הסמכות לפעולה וביצוע של הגורמים הללו הינו הארכיטקט הראשי. מנהל יחידת אבטחת מידע ממוקם במיקום ארגוני נמוך מבחינת מדרג סמכויות לגורמים הללו, וכמו כן אין ברשותו כל סמכות ניהולית ו/או מקצועית לאכוף את דרישות הביצוע בתחום אבטחת מידע.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"מנהל יחידת אבטחת מידע ממוקם במקביל למדרג סמכויות אלו ובכפיפות לארכיטקט הראשי. למנהל אבטחת מידע אין סמכות ניהולית אך יש סמכות מקצועית מלאה וכל עובדי הענף והאגף מחוייבים למלא אחר הנחיותיו. סמכות מקצועית אינה נגזרת ממיקום הירדכי כזה או אחר. לגבי הסמכות הניהולית מכיוון שתחום אבטחת מידע הינו מקביל לשאר שותפי התפקיד בענף, הסמכות המקצועית נגזרת מהיות כל היחידות באותו ענף. בענף חסרות המחלקות: (1) תשתיות תוכנה, (2) אינטגרציה, ו- (3) ארכיטקטורת תשתיות."**.

א. <u>מחלקת DBA</u> - מחלקה זו כפופה לארכיטקט הראשי והיא מונה 3 עובדים קבועים. עיקר תפקידיה של מחלקה זו הינם:

1) התקנת בסיסי הנתונים;

2) תחזוקת בסיסי הנתונים;

3) תפעול ואופטימיזציה של מסדי הנתונים;

4) תמיכה במפתחים בפיתוח מסד הנתונים;

5) גיבוי בסיסי הנתונים;

6) שחזור טבלאות;

7) מתן הרשאות לשימוש בבסיסי הנתונים.

משיחה שניהלה הביקורת עם אנשי מחלקת ה - DBA נמצא כי יש ברשותם הרשאות מנהל רשת לביצוע פעולות כגון: שינוי סיסמאות, מתן הרשאות משתמשים, מחיקה והוספה של משתמשים וכו'. לאור עובדה זו קיים קושי רב מצידה של יחידת אבטחת המידע לשלוט על תקינות פעילותם של אנשי ה - DBA, וזאת בעקבות חוסר סמכות וחוסר יכולת להפעיל את מרותה כלפי מחלקת DBA.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"היקף הפעילות של המחלקה בנושא ההרשאות הוא פחות מאחוז אחד מכלל פעילותה, ולכן אין קשר של כפיפות ניהולית או מקצועית למנהל אבטחת מידע, אלא הגוף נותן שירותים עפ"י הצורך למנהל אבטחת מידע. הרשאות מנהלי הרשת אינן נמצאות אצל כל ה- DBA-ים, אלא רק ל- DBA הראשי, וזאת בכדי לאפשר לו להגדיר תקשורת ולטפל בתקלות בכל השרתים מהם יש קשר למסדי הנתונים. אופי העבודה מחייב בסיכומו של דבר לתת הרשאות ע"י ובתאום אבטחת מידע לאותם אנשים העוסקים במלאכה אחרת לא יוכלו לבצע את עבודתם. 'קיים קושי רב מצידה של אבטחת מידע לשלוט על תקינות פעילותם של אנשי ה – DBA – בבואנו לנתח את משמעות המשפט אנו יכולים להבחין בכמה מישורים: מישור המעקב אחר פעילות אנשי ה- DBA: אכן לדעתנו יש מקום לתת כלי למעקב של אנשי אבטחת מידע ו/או אחרים אחר פעילות בעלי הרשאות "מנהל רשת" בכלל וה- DBA בפרט, מעקב כזה מתאפשר ע"י כלי מעקב וניטור הקיימים בשוק ומבצעים רישום של כל פעילות (איתרנו כלי כזה אותו מייצגת בארץ ... והמאפשר הקלטה של הפעילות המבוצעת בשרתים ובעמדות בעלי הרשאת מנהל רשת ועלותו 93 אלף דולר לא כולל מע"מ). לצערנו נושא זה לא נכלל בתוכנית העבודה של אגף המחשוב לתקופה הקרובה. כלי נוסף הנדרש למניעת זליגת מידע ע"י הגורמים המורשים אותר ע"י אגף המחשוב, עלותו כ- 130 אלף ₪ וייושמו הינו חלק מתוכנית העבודה לשנת 2007. מישור שני הוא פיקוח על מי מותר לעשות מה, והנחיות אלו ניתנות ע"י אבטחת מידע**

ומבוצעות באופן מדוייק ע"י ה- DBA-ים. מישור נוסף הינו ביצוע בקרה וניטור מדגמי של ה- DBA-ים שנכללת במשימות יחידת אבטחת מידע. 'חוסר סמכות וחוסר יכולת להפעיל את מרותה': אחד מהיתרונות של הכפפת יחידת אבטחת מידע לארכיטקט הראשי ביחד עם ה- DBA כיחידה הומוגנית אחת עם מנהל ישיר אחד, מאפשרת עבודה מתואמת, משולבת בה בפועל הן הסמכות והן המרות מופעלים הלכה למעשה. עם זאת, סמכות הינה פועל יוצא של מקצועיות, ניסיון, ידע, אוטוריטה מקצועית, שליטה בחומר, ויכולת אישית.".

הביקורת מציינת בהתייחס לתגובת הנהלת אגף המחשוב כי ה- DBA הראשי מאפשר לשאר עובדי מחלקת ה- DBA להשתמש בהרשאות מנהל הרשת הנמצאות ברשותו.

ב. <u>מחלקת SYSTEM</u> - מחלקה זו כפופה לארכיטקט הראשי. תפקיד המחלקה הוא טיפול בחומרת המחשב המרכזי, במערכת ההפעלה של המחשב המרכזי, ברכיבי התשתית של המחשב המרכזי, ומתן הרשאות במחשב המרכזי. משיחה שניהלה הביקורת עם אנשי מחלקת ה- SYSTEM נמצא כי יש ברשותם הרשאות מנהל רשת לביצוע פעולות במחשב המרכזי בלבד. לאור עובדה זו קיים קושי רב מצידה של יחידת אבטחת המידע לשלוט על תקינות פעילותם של אנשי ה- SYSTEM, וזאת בעקבות חוסר סמכות וחוסר יכולת להפעיל את מרותה כלפי מחלקת SYSTEM. יש לציין כי אנשי ה- SYSTEM אחראים בין היתר על השמדת מדיות מגנטיות שיצאו מכלל שימוש. מנהל אבטחת מידע אינו מפקח על פעולה זו המבוצעת על ידי אנשי ה- SYSTEM, כתוצאה מכך יכול להיווצר מצב שבו מדיות מגנטיות המכילות חומר רגיש לא יושמדו כהלכה.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות למצאים כי: **"לאף אחד מאנשי ה- SYSTEM אין הרשאת מנהל רשת. בעבר למנהל המחלקה בלבד הייתה הרשאה שהוסרה בעקבות פעילות אגפית לצמצום בעלי הרשאת "מנהל רשת". אנשי ה- SYSTEM אינם אחראים על השמדת מדיות מגנטיות. קלטות ברשת המבוזרת מושמדות ע"י אבטחת מידע. במחשב המרכזי לא מבוצעת השמדת קלטות באופן שוטף. כאשר מוחלפת מדיה מתבצעת השמדה של המדיה הישנה בחירייה באמצעות דריסה עם טרקטור ושריפה.".**

הביקורת מציינת בהתייחס לתגובת הנהלת אגף המחשוב כי מברור נוסף שערכה עם מנהל אבטחת מידע, עולה כי לאנשי ה- SYSTEM יש הרשאות מלאות במחשב המרכזי וכי יחידת אבטחת מידע לא מעורבת כלל בהשמדת מדיות מגנטיות במחשב המרכזי.

27. קבוצה שנייה של שותפי תפקיד עיקריים נוספים העוסקים בנוסף באבטחת מידע, שייכת לאגף המחשוב אך אינה כפופה לענף תורה שאליו כפופה יחידת אבטחת מידע. גורמים אלו כפופים (על פי החלוקה למחלקות) לענף שירות לקוחות ותפעול ולענף פיתוח המקבילים במדרג הארגוני לענף

תורה. במקרה זה הקושי באכיפת הביצוע בתחום אבטחת מידע מתעצם לאור ההבדל המהותי בהגדרת הייעוד והמטרות של תחום שירות לקוחות ותפעול לעומת תחום אבטחת מידע ותורה אשר לעיתים נתפס כגורם מעכב ואף מנוגד לפעילות המקצועית ולזרימת העבודה השוטפת.

א. <u>אנשי פיתוח ורכזי מחשוב</u> - כפופים לענף פיתוח ויישומים באגף המחשוב וחלק מעבודתם מתואם ע"י ענף שירות לקוחות ותפעול. רכזי המחשוב מהווים הגורם המקשר בין אגף המחשוב לבין לקוחות האגף וחלק מעבודתם מתואם אף ע"י ענף שירות לקוחות ותפעול. ברוב המקרים הרכזים כפופים לאגף המחשוב, אך ישנם רכזים הכפופים לאגפי עירייה שונים. הרכזים ממוקמים באגפים ובמחלקות השונות, תפקידם העיקרי הוא העלאת דרישות מחשוב של לקוחות האגף לטיפול המחלקה הרלוונטית באגף המחשוב ומעקב אחר סטאטוס הטיפול בדרישות. הנהלת אגף המחשוב מסרה לביקורת כי נכון למועד מתן ההתייחסות לממצאים מבוצעת עבודה בהובלת או"ת להגדרת תפקיד הרכז ומכאן שיתכן ותהיה השלכה גם על אופן טיפולו בנושא אבטחת המידע. כחלק מתפקידו השוטף של רכז המחשוב הוא משמש כנאמן אבטחת מידע. באחריותו לרכז את נושא ההרשאות, על סמך דרישות מנהלי המחלקות, להחתים את מנהל המאגר הרלוונטי ולהעביר את הטופס ליחידת אבטחת מידע (הטפסים נשמרים במחלקת אבטחת מידע). במקרים בהם רכזי המחשוב אינם כפופים לאגף המחשוב סוגיית הסמכויות והקושי באכיפת הביצוע בולטים עוד יותר מאחר ועלול להיווצר ניגוד עניינים מעצם תפקידם. קיים קושי רב מצדה של יחידת אבטחת המידע לשלוט על תקינות פעילותם של רכזי המחשוב, עקב חוסר סמכות וחוסר יכולת להפעיל את מרותה כלפי רכזי המחשוב. לדוגמא: למנהל יחידת אבטחת מידע אין סמכות מוגדרת המאפשרת לו לבטל את האישורים שניתנו על ידי רכז המחשוב ומנהל המאגר על בסיס שיקולים מקצועיים.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"נאמן אבטחת מידע אינו חלק פורמאלי מתפקידו של רכז המחשוב, עם זאת קיימת הבנה ואף למעלה מכך שפעילות בפורמט זה בין אבטחת מידע לבין הרכזים, נושא אשר הובל והוטמע ע"י מנהל אבטחת מידע. במסגרת הגדרת תפקידו של רכז המחשוב, פעילות המתבצעת בתקופה זאת ע"י או"ת, נחייחס גם לנושא זה. למנהל אבטחת מידע סמכות לבטל את האישורים שניתנו ע"י מנהלי המאגרים והרכזים עם זאת מנהל אבטחת מידע אינו סבור כי הוא נדרש לסמכות כזאת כלל ועיקר אלא במקרים יוצאי דופן והמנוגדים לחוק."**.

ב. <u>אנשי פיתוח</u> - בדומה לעובדי ה- SYSTEM אנשי הפיתוח עושים שימוש נרחב בהרשאות במהלך הפעילות השוטפת במסגרת תפקידם. גם ביחס ליחידה זו קיים קושי רב מצידה של יחידת אבטחת מידע לשלוט על תקינות פעילותה. דבר זה מחריף אף יותר לאור העובדה כי מדובר בכמות גדולה של עובדים.

ג. <u>מנהלי רשת</u> - מנהלי הרשת כפופים לענף שירות לקוחות ותפעול באגף המחשוב. תפקידם של מנהלי הרשת כולל:

1) תחזוקת רשת התקשורת – תחזוקת הנתבים, מתגים וציודי תמסורת;

2) תחזוקת השרתים השונים בעירייה, בין השרתים שעליהם אחראים מנהלי הרשת נמצא גם שרת האנטי וירוס.

חלקם של מנהלי הרשת באבטחת המידע הוא מניעת גישה (פיזית ולוגית) של גורמים לא מורשים לציודי התקשורת ולשרתים.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"תפקידו של מנהל הרשת הוא ביצוע מדיניות אבטחת המידע באופן מלא, אין למנהלי הרשת חלק בקביעת המדיניות של אבטחת מידע."**.

מחלקת מנהלי הרשת בעיריית תל-אביב-יפו אינה כפופה ליחידת אבטחת המידע, יתרה מכך ליחידת אבטחת המידע בעיריית תל-אביב-יפו אין כל פיקוח על נושא תחזוקת שרת האנטי וירוס ובכל הנוגע לפעילות מחלקת מנהלי הרשת בנושא אבטחת המידע. במצב הקיים, מחד שרת האנטי וירוס אינו באחריותה של יחידת אבטחת מידע, אולם מאידך האחריות על הטיפול ופתרון תקלות מוטלת על יחידת אבטחת מידע"...

"יחידת אבטחת מידע מתחזקת את כל השרתים הקשורים לאבטחת מידע ולפיכך מוקצה לה מנהל רשת ייעודי. לפני כחודשיים התחילה פעילות העברת תחזוקת שרת האנטי וירוס למנהל רשת אבטחת מידע. כרגע אנו בונים מנגנון שיבטיח התנהלות תקינה בהיבטים של אבטחת מידע וניהול הרשת.".

ד. <u>מחלקת תמיכה טלפונית</u> - מחלקה זו כפופה לענף שירות לקוחות ותפעול באגף המחשוב.

תפקידה של המחלקה הוא:

1) קבלת פניות לשירות ממשתמשי המערכות השונות;

2) פתרון תקלות באמצעות מסוף מרוחק;

3) הדרכת המשתמשים;

4) הזמנת טכנאים.

בין היתר, כחלק אינטגראלי מתפקידי צוות התמיכה, אחראית מחלקה זו על שיחזור סיסמאות ופתיחת חשבונות נעולים הן במחשב המרכזי והן בשרתי הרשת. פעולות אלו הינן קריטיות לשמירה על מערך אבטחת המידע. מנהל יחידת אבטחת מידע אינו מדווח על פעולות אלו ואינו מעודכן כלל, לפיכך אין באפשרותה של יחידת אבטחת המידע לפקח ולבקר את תקינות דרכי פעילותה של מחלקת התמיכה. עפ"י דיווחי מנהל היחידה נעשו על ידו ניסיונות לחייב את עובדי מחלקת תמיכה טלפונית לאמת את זהות המשתמשים טרם

פתיחת סיסמה נעולה, אולם ניסיונות אלו כשלו משום שאין לו את הסמכות לאכוף זאת עליהם.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"קיימים שני סוגים של פתיחת חשבונות נעולים: חשבונות שננעלו ע"י אבטחת מידע – לא מתבצע ע"י צוות התמיכה אלא רק ע"י אבטחת מידע, ופתיחת חשבונות שננעלו בעקבות טעות משתמש – מתבצע ע"י מחלקת התמיכה והינם חלק מתפקידה. טיפול שוטף ושגרתי זה אינו מעניינו של אבטחת מידע. על פעילות איפוס/שנוי סיסמאות מעקב מלא באמצעות תוכנת MOM של מיקרוסופט."**.

הביקורת עומדת על דעתה כי טיפול בפתיחת חשבונות נעולים מכל סיבה שהיא הינה בתחום אחריות אבטחת מידע. המשך תגובת אגף המחשוב, כפי שתובא להלן, תומכת בעמדת הביקורת:

"אין ברשותנו היום כלי המאפשר זהוי חד חד ערכי של הלקוח המתקשר למרכז התמיכה לפתוח חשבון נשול. במהלך שנת 2007 (עד מאי) תתבצע עבודה בתחום אבטחת מידע לאימות הפונה ע"י קבלת נתונים המופיעים במאגר העובדים העירוניים והשוואה אליהם. מנהל מחלקת שירות לקוחות תנחה את המוקדניות כי בכל מקרה שכזה יש לאמת את נתוני הפונה ע"י צלצול חוזר לטלפון כפי שמופיע ברישומי אגף המחשוב. פעילות זאת תיכנס לעבודה החל מה- 1.1 ותיבדק ע"י תחום אבטחת מידע באופן אקראי מידי חודש.".

ה. <u>צוות טכנאים</u> - כפוף לענף שירות לקוחות ותפעול ומשמש כזרוע המבצעת של מחלקת התמיכה. כאשר נדרש פתרון לבעיה מחישובית שאינה יכולה להיפתר בצורה מרוחקת, פותחים אנשי התמיכה קריאה לצוות הטכנאים, המתייצבים אצל המשתמש לטיפול וסגירת הקריאה. בדומה לסוגיה שפורטה לעיל מול מחלקת התמיכה הטלפונית, גם במקרה זה אין באפשרותה של יחידת אבטחת המידע לפקח ולבקר את תקינות דרכי פעילותה של מחלקת הטכנאים. למחלקת הטכנאים קיימת רמת הרשאות גבוהה מזו הנדרשת לה לביצוע תפקידה. כמו כן, במהות עיסוקם הטכנאים נגישים לרכיבי חומרה העלולים להכיל מידע רגיש וליחידת אבטחת מידע אין דרך לפקח על דרך טיפולם של הטכנאים ברכיבי החומרה והמידע המצוי עליהם. בנוסף, יש באפשרות הטכנאים לעסוק בנושא ההרשאות למרות שאינם אמורים לעשות זאת ואין זה מתוקף תפקידם.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"אין באגף מחשוב מחלקת טכנאים, שירות זה נקנה היום מחברה חיצונית על בסיס תשומות. בימים אלו אנו נמצאים בתהליך מכרז של החלפת שירות זה מבסיס תשומות לבסיס תפוקות. במכרז הוגדר שהחברה הזוכה תהיה כפופה לנהלי אבטחת המידע של העירייה. עם ההכרזה על זוכה וכניסתו לעבודה אנו נוודא כי הוא פועל עפ"י הנהלים ואינו חורג מסמכותו. הטכנאים אינם מבצעים פעילות אבטחת מידע. נושא הרשאות הטכנאים מהווה דילמה מקצועית.**

הרשאות אלו נדרשות בכדי לבצע את עבודת הטכנאי לצורך מתן שירות מהיר ופתרון הבעיה במקום. קיימות שתי חלופות: האחת שלטכנאים יש את ההרשאה ואז יש לבצע ביקורות של אבטחת מידע לוודא עמידה בנהלים, והשניה שהרשאות אלו ינתנו ויוסרו אד-הוק ע"י אבטחת מידע. החלופה השניה אינה פותרת את הבעיה כי עדיין אין כל שליטה על מה שעושה הטכנאי בתחנה מחד, ומסרבלת את מתן השירות מאידך. לפיכך הבחירה של אגף המחשוב הינה בחלופה הראשונה. אם זאת, כאמור לעיל עם בחירת זכיין אנו נוודא עמידה בנהלים. לאחרונה ביצענו מיפוי של ההרשאות הקיימות בידי הטכנאים, הרשאות מנהלי הרשת ילקחו מכל הטכנאים וינתנו להם הרשאות לניהול תחנות העבודה בלבד. כאשר ידרשו הרשאות מעבר לכך, הרשאות אלו ינתנו אד-הוק ע"י אבטחת מידע. עבודה בתצורה זו תבוצע החל מה- 1.1.

אנשי הפיתוח באגף המחשוב הינם גם שותפי תפקיד השייכים לקבוצה זו".

28. קבוצה שלישית של שותפי תפקיד עיקריים העוסקים בנוסף באבטחת מידע הינם מנהלי מאגרים. מנהלי המאגרים כפופים לאגפי העירייה השונים, ואינם כפופים לאגף המחשוב כלל. למנהלי המאגרים חלק מהותי באבטחת המידע, מתוקף אחריותם על מאגר המידע. חוק הגנת הפרטיות תשמ"א 1981 כולל פרק שלם הדן בהגנה על הפרטיות במאגרי מידע. החוק מפרט את כל חובותיו ואחריותו של מנהל המאגר, כל העובר על חוק זה, עובר עבירה פלילית וצפוי לעד שנת מאסר.

לקבוצה זו ממשק העבודה המרוחק ביותר יחסית, מבחינת מיקום ארגוני, ליחידת אבטחת מידע. פעולותיהם כמו גם סדרי העדיפויות ומקור סמכויותיהם נגזרים ישירות ממטרות ויעדי הפעילות המקצועית של יחידות העירייה השונות. קיימים מקרים בהם נושאי אבטחת מידע מקשים על הפעילות המקצועית השוטפת מנקודת ראותם של עובדי היחידות. במקרים הללו מעדיפים העובדים להתעלם מהוראות הביצוע של אבטחת המידע. לפיכך, בקבוצה זו בולט הקושי באכיפת ביצוע בנושא אבטחת מידע יחסית לכל הקבוצות שפורטו לעיל. לדבריו של ממונה אבטחת המידע אין ברשות מנהלי המאגרים הכלים המתאימים לקביעת רמת ההרשאות שאמורה להינתן לכל עובד. לעיתים מנהלי המאגרים מסתמכים על שיקול דעתם של רכזי המחשוב הממוקמים במחלקות השונות. בנוסף, מובאת לידיעתם של מנהלי המאגרים כל הרשאה שאמורה להינתן לעובדים. למרות האמור, כאשר עובד מסיים את תפקידו או לחילופין עובר לתפקיד אחר אין נוהל דיווח המיידע את מנהל המאגר בגין ביטול ההרשאה. משיחה עם אחד ממנהלי המאגרים בעירייה עולה כי הוא אינו מקבל חיווי שוטף על פעולות חריגות שמבוצעות במאגר עליו הוא אמון, על כן הוא שם את מבטחו בממונה אבטחת המידע. ראוי להדגיש שהאחריות על אבטחת המידע במאגר, על פי חוק הגנת הפרטיות, מוטלת על מנהל המאגר ומנהל אבטחת מידע ביחד ולחוד.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"במהלך הרבעון הראשון של 2007 אנו נכניס לעבודה טופס אבטחת מידע אלקטרוני. כחלק מהתהליך הוקם מאגר של מאגרי מידע ומנהליהם. לאחר סיום הטמעת השימוש בטופס האלקטרוני נוכל לאפשר למנהלי המאגרים**

לקבל נתונים בזמן אמת אודות רמות ההרשאה שניתנו לעובדים במאגרים אלו. למרות שמנהלי המאגרים מתבססים לעיתים על שיקול דעתם של רכזי המחשוב, הם אינם מאשרים ללא חתימת ממונה ישיר ומנהל אגף.".

29. במסגרת יישום שינוי המבנה הארגוני של אגף המחשוב חל פיחות במיצוב היחידה לאבטחת מידע במדרג הארגוני של אגף המחשוב. היחידה מוקמה נמוך יותר במדרג יחסית לעבר, דבר אשר לו משמעויות ארגוניות שונות כדוגמת פיחות ביוקרה ובמוניטין המקצועי, בסמכויות ובמידת קבלת עובדי העירייה את היחידה כסמכות מקצועית בתחומה.

התייחסות מנהל אבטחת מידע: **"מקבל באופן מלא את עמדת הביקורת בסעיף זה".**

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **המיקום הנוכחי של היחידה הינו תחת ראש ענף תורה עובדה שלהערכתנו מאפשרת עבודה אינטגרטיבית רבה יותר עם שאר הגורמים בענף זה כפי שהביקורת ציינה בסעיף 26, גורמי הענף בכלל וראש הענף, הארכיטקט הראשי בפרט, נותנים מעטפת מקצועית לאבטחת מידע ומאפשרים "סגירת" נושאים במעגלים קצרים בתוך ענף ארכיטקטורה. מנהל האגף אינו בעל סמכות מקצועית טהורה וספציפית בתחום אבטחת מידע ולכן מהווה סמכות ערעור ניהולית ולא מקצועית. עם זאת, מיצוב של יחידה בכלל ויחידת אבטחת מידע בפרט הינו פונקציה של אוטוריטה מקצועית, ידע, רמת שירות, קשר לליבה העסקית של הארגון, ועוד פרמטרים רבים שהמדרג הארגוני הינו בטל בשישים מולם. בעבר הרחוק נושא אבטחת המידע לא זכה להתייחסות מספקת בשולם ולכן החשיבות של מיקומו במדרג הארגוני הביעה את הרצון של הארגונים להבלטת הנושא. כיום עם חדירת המודעות של אבטחת המידע, מיקומו הטבעי הוא בסביבה המקצועית כפי שבא לידי ביטוי במבנה הארגוני של אגף המחשוב. בשנים האחרונות הנושא עלה על סדר היום, ולראיה החוקים והתקנות המחייבים את כלל הארגונים בתחום זה, ולכן נושא אבטחת מידע באגף המחשוב יכול לחזור למקומו הטבעי בכפוף לסמכות מקצועית לצורך השגת מטרותיו באופן מיטבי.בנוסף, למנהל אבטחת מידע, כחלק מהמבנה הארגוני, יכולת של קשר ישיר עם מנהל האגף ללא צורך במעבר בהיראכיה הניהולית בכל עניין ונושא בהתאם לראות עיניו.".**

30. היעדר הגדרה ארגונית ברורה של תחום אבטחת מידע - מנהל היחידה שווה לדרגת מנהל מחלקה לצרכי הגדרת הזכויות הסוציאליות ותנאי העבודה, אולם אין הדבר בעל משמעות במובן הארגוני של הגדרת התפקיד.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"המושג תחום אינו למיטב ידיעתנו תואר עמום אלא מושג תקניתי עירוני, ולראיה רק באגף המחשוב קיימים מספר לא מועט של תחומים חשובים ביותר: תחום גביה, תחום הנהלת חשבונות, תחום משאבי אנוש, תחום מתודולוגיה וארכיטקטורת תוכנה, ועוד. בעירייה קיימים תחומים: זיקנה, נכויות, יישומים, משאבי קהילה, ילד ונוער, פרוייקטים, וכו'. ושוב כאמור בסעיפים הקודמים, סמכותו של תחום מקצועי אינה נקבעת עפ"י התואר אלא עפ"י מקצועיות, אוטוריטה, וכו' ".**

ההגדרה הארגונית של יחידת אבטחת מידע עמומה ואינה ברורה באופן חד משמעי לכל הגורמים הרלונטיים. קיימים מקרים בהם אבטחת מידע מוגדרת כתחום ובמקרים אחרים מוגדרת כיחידה. יתרה מזו, לטענת מנהל אבטחת מידע היחידה מוגדרת כמחלקה וכך התייחסות לנושא בכל ישיבות הנהלת האגף. לעומת זאת בשיחות עם הביקורת הגדירה הנהלת האגף את יחידת אבטחת מידע כתחום, המהווה יחידה ארגונית נמוכה ממחלקה במדרג הארגוני (מספר תחומים מהווים מחלקה). דבר זה תומך בטענת הביקורת כפי שבאה לידי ביטוי בסעיף 29 הקודם, כי במסגרת השינוי המבני שבוצע באגף חל פיחות במיצוב יחידת אבטחת מידע במדרג הארגוני של אגף המחשוב.

תחומי אחריות וסמכות במערך התפקידים ביחידת אבטחת מידע

31. מנהל יחידת אבטחת מידע

תפקידיו העיקריים כוללים:

א. אחריות מקצועית וניהולית כוללת על עובדי היחידה ופעילות היחידה;

ב. גיבוש וריכוז המידע הנדרש בתחום אבטחת מידע למתודולוגיה הפיתוח של העירייה (עליה אחראי הארכיטקט הראשי ומנהלו הישיר של מנהל היחידה);

ג. איתור פערים וצרכים באבטחת מידע - העלאת סדרי עדיפויות לביצוע בתחום לאישור תקציבי וביצועי של הארכיטקט הראשי;

ד. אישור של כל מערכת חדשה המוכנסת לעירייה, חומרה ותוכנה.

ה. ביצוע אבטחה פיזית ולוגית/ניהול משתמשים - תפעול וטיפול יומיומי מרגע קליטת העובד ועד פרישתו ו/או עזיבתו;

ו. מתן הרשאות - טיפול ואישור טפסי החתימה על הרשאות (כ- 50 טפסים ביום);

ז. ניתוב הבקשות לעדכון פרטים בין עובדי היחידה (כ- 300 בקשות בשבוע);

ח. ביצוע מעקב ובקרה בנושא שרתי אבטחת מידע (Fire Wall, שער הגישה, אימות משתמשים, וכו');

ט. טיפול מול עובדי DBA - בניית הגדרות והרשאות;

י. אבטחת אפליקציות;

יא. אבטחת נקודות חמות;

יב. הדרכות עובדי העירייה בנושאי אבטחת מידע;

יג. ניהול הקשר ומו"מ עם ספקים;

יד. בדיקת מוצרים חדשים טרם רכישתם;

טו. ליווי והטמעת פרוייקטים אד - הוק;

טז. כתיבה ובקרת נהלים;

יז. בקרה על שרת האנטי וירוס.

32. מנהל רשת אבטחת מידע האחראי על שרתי אבטחת המידע של העירייה (האחראים על כניסה ויציאה של מידע ברשת). כחלק מעבודתו השוטפת אחראי על הטיפול בנושאים הבאים:

א. אחראי על תפעול, תחזוקה (בקרה על גישה מרחוק ואתרים חיצוניים) והגדרת נהלים בתחום שרתי אבטחת המידע (Fire Wall, שער הגישה (eSafe), אימות משתמשים, וכו') של העירייה;

ב. טיפול שוטף ב – GPO, מערכת האחראית על ניהול המשתמשים ברשת;

ג. ליווי טכנולוגיות חדשות המופעלות בעירייה;

ד. אבטחת אתר בזק בינלאומי;

ה. העברת השרתים לבניין העירייה הראשי;

ו. טיפול בשרת ה – Proxy, שרת המתווך בין המשתמשים לבין רשת האינטרנט;

ז. טיפול בשרת ה – Reverse Proxy, שרת המאפשר גישה לדואר האלקטורני מרשת האינטרנט;

ח. טיפול ב – FTP, פרוטוקול העברת ושיתוף קבצים.

33. עובד האחראי על הטיפול בהרשאות עובדים. כחלק מעבודתו השוטפת אחראי על:

א. טיפול בהרשאות עובדים והתאמה להגדרת התפקיד;

ב. פתרון תקלות ברשת המקומית (מול האקטיב דירקטורי);

ג. מתן סיוע לעובד האחראי על שרתי Fire Wall.

34. עובד המטפל בכל הקשור לתכנות. כחלק מעבודתו השוטפת אחראי על:

סיוע לעבודה השוטפת ביחידה על פי חלוקת המטלות של מנהל המחלקה בעיקר הגדרת משתמשים, הרשאות וכרטיסי טוקן.

35. עובד שעיקר תפקידו מתן הרשאות ופתרון תקלות ברשת המקומית. כחלק מעבודתו השוטפת אחראי על:

סיוע לעבודה השוטפת ביחידה על פי חלוקת המטלות של מנהל המחלקה.

ממצאים

36. יחידת אבטחת מידע נדרשת לקבוע הן את התורה ונהלי העבודה בתחום אבטחת מידע, הן את התפעול של תהליכי העבודה והמנגנונים בשטח וכן לבצע מעקב ובקרה. על פי ממצאי הביקורת

יחידת אבטחת מידע בעירייה עוסקת בעיקר במישור התפעול המתבטא בעיקר בנושא הטיפול בהרשאות. הטיפול במישור התורה ונהלי עבודה חלקי ונעשה על ידי מנהל היחידה בלבד. לא קיימת מדיניות אבטחת מידע מפורטת, רשמית ומתועדת, אין מדריכי משתמשים לאפליקציות וכן לא קיים בפועל נוהל אבטחת מידע כולל המפרט באופן שיטתי את כל הנדרש בתחום אלא מספר מועט של נהלים בנושאים נפרדים.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות למצאים כי: **"חלק מהתפעול מתבצע בשם אבטחת מידע ועפ"י הנחיותיו ע"י מנהלי הרשת, הטכנאים, מוקד התמיכה, וה- DBA-ים. הטיפול במישור התורה מתבצע ע"י היקף של כשתי משרות ולא רק ע"י מנהל היחידה בלבד. אין מקום לדעתנו לנוהל אבטחת מידע כולל אחד, קיים מסמך מדיניות המפרט את הנדרש (ראה התייחסות בסעיף 6) וקיימים מספר נהלים והוראות עבודה כמפורט בהמשך הביקורת."**.

37. תחום DRP הינו תחום טיפול השייך במהותו לתחום אבטחת מידע. זהו תחום המהווה חלק אינטגרלי ומובן מאליו של נושא אבטחת מידע, בדומה לתחומים אחרים השייכים לתחום, ולכן ממוקם באופן טבעי בארגונים השונים ביחידות העוסקות בנושא. במסגרת פרוייקט ה – DRP אמורים לזהות את כל הפעולות והמשאבים הקריטיים לפעילות העירייה. הביקורת מצאה כי בעיריית תל-אביב-יפו פרוייקט ה-DRP מנוהל על ידי מנהל שהוגדר באופן ספציפי כ"אחראי DRP, שליטה ובקרה" ואינו שייך ליחידת אבטחת מידע.

מנהל אבטחת מידע מסר לביקורת כי DRP צריך להיכלל במסגרת תפקידו.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות למצאים כי: **"DRP מטפל בהמשכיות עסקית של הארגון ואין לזה, להערכתנו (ראה התייחסות לסעיף 5) כל קשר לאבטחת מידע (כמובן מעבר למה שיש לכל מערכת אחרת). למיטב ידעתנו גם בארגונים אחרים DRP אינו חלק מאבטחת מידע. אם זאת, אגף המחשוב נמצא בתחילתו של הכנת מסמך DRP שיגדיר את המדיניות העירונית, יגדיר את רמת הסיכון המשתמעת ממנו, והמשאבים הנדרשים. במקביל במסגרת תוכנית העבודה ב- 2006 ו- 2007 התחלנו להיערך למספר נושאים הקשורים ליישום DRP כגון: הכפלת שרתים למניעת נקודת כשל, כאשר שרתי אבטחת המידע היו הראשונים שטופלו. עצם העובדה שהגדרנו תפקיד ספציפי כאחראי DRP שליטה ובקרה מראה כי בכוונתנו לא להרפות מנושא זה."**.

38. נושא האנטיוירוס אשר מהווה חלק בלתי נפרד ומרכזי בתחום אבטחת מידע אינו בתחום אחריותו של ממונה אבטחת המידע, אלא נתון באחריות מנהלי הרשתות הכפופים לענף שירות לקוחות ותפעול. דבר זה מקשה על היחידה באבטחת התפעול היעיל הנדרש של נושא האנטיוירוס בכל המחשבים המצויים בעירייה כולל עדכון תוכנות האנטיוירוס. יתרה מכך, אין באפשרותו לוודא באופן מוחלט שאכן פועלת תוכנת אנטיוירוס בכל התחנות בעירייה.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"נושא תחזוקת שרת האנטי וירוס יועבר לאחריות מנהל רשת אבטחת מידע בהתאם להתייחסותנו לעיל. אגף המחשוב נמצא בתהליך רכש של מערכת שכחלק מתפקידיה מניעת האפשרות של תחנה ללא אנטי וירוס או שהאנטי וירוס אינו מעודכן מלהתחבר לרשת. סיום הטמעת המערכת עד תום הרבעון הראשון 2007."**.

39. תהליך קבלת הרשאות גישה למאגרי המידע - הטיפול בהרשאות (הגדרה, אישור, ביטול וכו') הינו תחום הטיפול המרכזי של עובדי יחידת אבטחת מידע. ממצאי הביקורת העלו מספר נושאים בעייתיים בתהליכי הטיפול:

א. הגדרת ההרשאות ניתנת לעובד ולא לתפקיד אותו הוא ממלא. לא קיים מיפוי של כלל התפקידים בעירייה הכולל פירוט לגבי המידע או רמת ההרשאות הרלוונטיות לכל תפקיד ותפקיד.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"הרשאות אמורות להינתן לתפקיד ולא לעובד ואכן במערכות החדשות המפותחות באגף המחשוב וכאלו הנרכשות מבחוץ ניתן דגש על יישום הרשאות באופן זה. המערכות הישנות של העירייה אינן תומכות באפשרות זאת והשינו אינו ריאלי בהיבטי עלות תועלת. מיפוי כלל התפקידים בעירייה אמור להיעשות ע"י או"ת, כיום לא קיים מיפוי כנ"ל."**.

ב. אישור מתן הרשאות מבוצע על טופס פתיחת הרשאות. הטפסים אינם ממוחשבים ואופן העבודה ידני. נוהל העבודה דורש עבודת ניירת רבה וגורם לתהליכי עבודה ארוכים ומסובכים. כתוצאה מכך נוצר עומס עבודה גדול על כל הגורמים המעורבים בתהליך, כולל על היחידה לאבטחת מידע, דבר אשר גורם לעיכובים בעבודת עובדי העירייה.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"יחידת אבטחת מידע נמצאת בעיצומו של תהליך לבניית מנגנון ממוחשב להעברת טפסים בין הגורמים תוך שימוש בכרטיס חכם להזדהות וחתימה. תהליך זה יושם מבחינה תקציבית בשנים 2007 ו- 2008."**.

ג. נכון למועד עריכת הביקורת, הטופס דורש שורה ארוכה של חתימות וגורמים מאשרים. הדבר גורם לכך שעל טופס לעבור דרך תחנות רבות, עד לאישור ההרשאה. כתוצאה מכך נוצרים עיכובים במתן האישורים וזמן טיפול ארוך.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"החוק מחייב חתימת מנהל מאגר בלבד. אם זאת מנהלי המאגרים דורשים חתימה של ממונה ישיר ומנהל אגף טרם חתימתם."**.

ד. קיים חוסר בהירות ועמימות ביחס לתפקידו של מנהל אבטחת המידע במתן אישור להרשאות. לא ברור האם תפקידו הינו ביצועי בלבד והוא נדרש לבצע באופן אוטומטי את

מתן ההרשאה על פי אישורי מנהל האגף ומנהל המאגר, או שמא חלה עליו חובת בדיקה אחרונה טרם מתן האישור, כאשר בסמכותו לפסול אישור מתן הרשאות על פי שיקול דעתו.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"מנהל אבטחת מידע ימליץ להנהלת העירייה עד תאריך 1.1.2007 על תפקידו בנושא ההרשאות."**.

פרק ד – הון אנושי והכשרה

40. החידושים בעולם אבטחת המידע מתעדכנים ומתחדשים בקצב מסחרר, על כן יש לבצע השתלמויות וקורסים בנושא, זאת בכדי לתת מענה טוב לכל האיומים המאיימים לפגוע במערכות הממוחשבות, שמתחדשים גם הם.

ממצאים

41. יחידת אבטחת מידע מורכבת כאמור מחמישה עובדים אשר את עיקר הכשרתם וניסיונם בתחום אבטחת מידע צברו במסגרת תפקידם הנוכחי ביחידה לאבטחת מידע בעירייה. מנהל היחידה שימש בתפקידו הקודם כמנהל רשת (איש SYSTEM). העובד הבכיר הנוסף ביחידה השתתף בקורס מנהלי רשתות MCSE והחל לעבוד בעירייה דרך חברה קבלנית (כיום עובד עירייה). עובד נוסף שימש בתפקידו הקודם כטכנאי מחשבים, לאחר מכן עבר קורס MCSC של מייקרוסופט, ניהל מוקד תמיכה של חברת start-up ושימש כרכז מחשוב בעירייה טרם תפקידו הנוכחי. עובד נוסף בעברו היה מאבטח בתחנת משטרה, החל קורס מייקרוסופט בתכנות, התקבל למשרה זמנית בעירייה וביצע פרוייקטים נוספים עד אשר הפך לנש"מ. העובד האחרון הינו סטודנט בעיסוקו. אין במצוין לעיל בכדי להפחית במקצועיותם של עובדי המחלקה אולם יש לציין שמרבית הידע הנצבר בקרב עובדי המחלקה בנושא אבטחת מידע מתבסס על הניסיון בעבודתם בתפקידם הנוכחי ביחידת אבטחת מידע בעירייה, ומהסתייעות ביועצים החיצוניים המלווים אותם בתחום.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"כל העובדים מקבלים הכשרות במסגרת קורסים ייעודיים הנתפרים עבור אבטחת מידע ובהתאם לצרכיה."**.

42. באגף המחשוב קיימת מודעות למתן הכשרה מקצועית וארגונית לעובדי האגף. מראיונות שהתקיימו עם עובדי יחידת אבטחת מידע, עולה כי הקורסים וההשתלמויות אליהם נשלחים העובדים אינם קשורים באופן ישיר לנושא אבטחת מידע.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"הכשרה מקצועית וארגונית לעובדי אבטחת מידע הינה באחריותו הישירה של מנהל אבטחת המידע. עובדי אבטחת מידע יוצאים לקורסים והכשרות יעודיים לנושא עפ"י תוכנית מנהל אבטחת המידע. כמו כן, כאשר יש**

הכשרות אגפיות שיכולות לתרום לידע המקצועי הכללי של עובדי אבטחת מידע, הם משולבים בהכשרות אלו. בנוסף כאמור בהתייחסותנו לסעיף הקודם התבצע כבר קורס אחד התפור לצרכי היחידה ואנו כרגע בהכנת הסילבוס לקורס ההמשך..".

43. ההדרכות הניתנות לכלל עובדי העירייה בנושא אבטחת מידע, ניתנות כנספח קצר המשולב בסדנאות וקורסים העוסקים בנושאים מקצועיים ואחרים הניתנים לעובדים. לעובדי העירייה לא ניתנות הדרכות מסודרות ומלאות בתחום אבטחת מידע. לא קיימת חובת נוכחות בהרצאות המקוצרות שאכן ניתנות. לא מתבצע מעקב ורישום מסודר של נוכחות עובדים. ממונה אבטחת המידע מסר לביקורת כי לדעתו כי יש לקיים סדנאות בנושא, ברשותו מערכי שיעור מסודרים והוא אף מרצה בתחום לפי הזמנה ברשויות מקומיות שונות וגופים אחרים.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"מנהל אבטחת מידע הרצה בכנס מקצועי אחד ולא ברשויות מקומיות אחרות או גופים אחרים.".**

44. מודעות לנושא אבטחת מידע בעיריית תל-אביב-יפו – מנהל אבטחת מידע מסר לביקורת כי רמת המודעות לנושא אבטחת מידע בעירייה נמוכה. עובדי העירייה אינם בקיאים בנדרש מהם לביצוע כמו גם אינם מודעים די הצורך לחשיבות ולסכנות הטמונות באי אכיפת הוראות העבודה של אבטחת מידע. בשיחות עם עובדי עירייה ניכר חוסר מודעות בולט לתחום וחשיבותו עד לכדי זלזול. הדבר ניכר ביחס להרשאות וסיסמאות, הוצאת חומר רגיש, יכולת החדירה הקלה למערכות העירייה, נקודות הפרצה הרבות הקיימות ועוד.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"המודעות כמעט אינה קיימת, והיא בעייתית גם בהיבטים של אבטחה פיסית: נעילת דלתות, דלתות במסדרונות שאין בהם קבלת קהל, דוחות מסווגים שמסתובבים חופשי, וכו'. מכיוון שנקודה זו זוהתה כבעייתית מתבצעות פעולות הדרכה ע"י מנהל אבטחת מידע בכל פורום רלוונטי. בנוסף היה פרסום בתלוש המשכורת להדגשת חשיבות הנושא.".**

פרק ה - ניהול

45. בתפיסת הניהול של הנהלת אגף המחשוב תחום אבטחת מידע נתפס כנושא חורג מהעיסוק המרכזי של האגף. אבטחת מידע נתפס כגורם מפריע ומעכב ליישום מטרות והשגת יעדי האגף במתן שירות מיטבי בתחום המחשוב לכל המשתמשים ומענה לכל דרישות הנהלת העירייה.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"ההתייחסות לאבטחת מידע אינה חורג מהעיסוק המרכזי אלא עוד נושא שווה לכל הנושאים האחרים המטופלים ע"י האגף.".**

46. בראיונות שקוימו עם הביקורת טען הארכיטקט הראשי כי מצבו של תחום אבטחת מידע בעירייה הינו בכי רע בשל הזנחת הנושא במשך מספר רב של שנים על ידי מספר מנהלים. עוד טען כי הגישה שרווחה בקרב קודמיו בתפקיד ראתה באבטחת מידע גורם מפריע. ממצאי הביקורת נראה כי גישה זו לא השתנתה גם היום.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"התייחסות זאת השתנתה באופן קיצוני: היום אבטחת מידע מעורבת בכלל פעילות האגף באופן יזום החל משלב ייזום הפעילות. אבטחת מידע משולבת בישיבות העלאה לאויר, בפורום הטכני, בתהליכי אישור תוכנה, בתהליך אפיון תוכנה, ועוד (מה שלא היה בעבר). כמו כן תקציבי אבטחת המידע הישירים והעקיפים הוכפלו בשנה הראשונה ושולשו בשנה השניה (ממה שהיה בשנה הראשונה, כלומר פי שש ממה שהיה). לעניות דעתנו הכפלת התקציב פי שש בשנתיים על חשבון פעילויות אחרות היא פעולה קיצונית ללא אח ורע המצביע בהכרח על רמת ההתייחסות לנושא בהנהלת האגף."**.

47. ניהול יחידת אבטחת מידע - מן הדיווחים לביקורת עולה כי מנהל היחידה מפנה את עיקר זמנו לטיפול במשימות תפעוליות שוטפות (בעיקר תחום הרשאות) ופחות בטיפול בנושאים מערכתיים כוללים וניהול מסודר ושיטתי של התחום. לטענת מנהל היחידה אין לרשותו די הצורך משאבי זמן וכח אדם לטיפול מסודר בגיבוש וכתיבת מדיניות, תפיסה ומתודולוגית אבטחת מידע, הכנת מסמכי עבודה ונהלים מסודרים, בניית תוכנית עבודה מתוך ראייה מערכתית כוללת, כולל תוכנית עבודה מסודרת בנושא רכש על פי סדרי עדיפויות, המספקת מענה נדרש לצרכי השטח.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"מנהל אבטחת המידע מחלק את זמנו בהתאם למרות וליעדים מחד ולמשאבים המוקצים לו מאידך. חלוקת הזמן היה כ- 50% למשימות תפעוליות ו- 50% למשימות ניהוליות ותכנוניות. אם זאת, החובה המוטלת על כולנו היא לנסות ולהתייעל לאורך הדרך, למצוא פתרונות יצירתיים לבעיות הצצות חדשות לבקרים, ונסיון באופן מתמיד להגדלת השוגה העומדת לרשותנו."**.

48. תפקידו של מנהל יחידת אבטחת מידע בעירייה הינו תפקיד מורכב ואינו עשוי מקשה אחת. על ממונה אבטחת המידע לטפל בנושאים הבאים: יישום מוצלח של אבטחת המידע בעירייה, ניהול יחידת אבטחת מידע, אחריות ניהולית ומקצועית לביצוע מיטבי של המשימות על ידי עובדיו, ואחריות על שותפי התפקיד באופן מקצועי. כמו כן, על ממונה אבטחת המידע לאכוף ביצוע הנחיותיו המקצועיות על ידי שותפי התפקיד וכן הוא אחראי על יישום נהלי אבטחת מידע והנחיות הניתנות על ידו של כל משתמשי הקצה בעירייה. ממונה אבטחת המידע נדרש לבצע באופן מיטבי את כל מכלול התפקיד, דבר זה דורש ממנו להיות בעל מעמד מקצועי בכיר ואיתן, בעל ידע ויכולות ניהוליות. על פי ממצאי הביקורת ממונה אבטחת המידע מתקשה להפעיל את סמכותו המקצועית ולאכוף ביצוע על שותפי התפקיד שפורטו ועל משתמשי הקצה בעירייה. לדוגמה, מנהל יחידת אבטחת מידע ביקש להטמיע נוהל לפיו יחידת אבטחת מידע תהיה מעורבת בקליטת עובדים

חדשים באמצעות מתן תדריך באבטחת מידע. ניסיון זה לא צלח בעקבות חוסר שיתוף פעולה מצד הגורמים הרלוונטיים בעירייה. יחד עם זאת, הצליח מנהל היחידה להנהיג קבלה מסודרת של דרישה לכניסת עובד בעת קליטת עובד חדש, דבר המאפשר לו לספק הרשאה מסודרת לעובד מיד עם קליטתו. כמו כן, מנהל אבטחת מידע הצליח להנחיל נוהל לפיו הוא מקבל דיווח על כל עובד שפרש מהעירייה. למרות האמור מנהל אבטחת מידע אינו מקבל דיווח על עובדים שעברו תפקיד בעירייה.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"עדיין לא ניסיון אמיתי לפעול מול הגורמים בעירייה, כך שלא ניתן להגדיר "ניסיון לא צלח""**

49. תוכנית עבודה - תוכנית העבודה בתחום אבטחת מידע אינה נקבעת בשיתוף עם מנהל יחידת אבטחת מידע כי אם על ידי הנהלת אגף המחשוב ומוצגת לאחר קביעתה. לא קיים תהליך מסודר ומובנה לקביעת תוכנית העבודה האמורה לבטא נאמנה את סדרי העדיפויות וצרכי העבודה של תחום אבטחת מידע. לא מתקיים דו שיח ו/או דיונים משותפים של תהליך הדדי לפיו מועלות הצעות מהשטח ומתקבלות הסתייגויות מההנהלה. תוכנית העבודה מונחתת מהדרגים הגבוהים יותר באגף המחשוב והינה בעיקר תולדה של אילוצים תקציביים.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"מצב זה היה נהוג בעבר. החל מהכנת תוכנית העבודה של 2007 שבוצעה במהלך השנה שעברה התהליך שונה. התהליך בהכנת תוכנית העבודה הוא הכנת רשימת צרכים מתועדפת ע"י אבטחת מידע. ההחלטה על גובה התקציב התבצעה ע"י מנכ"ל העירייה והדברים שמתבצעים הם אלו שאבטחת מידע הגדירה ונכנסים לפי עדיפותם למסגרת התקציב. על נושאים אלו אנו מוסיפים ברמת ענף תורה פעילויות שנראות נחוצות מתוך תקציבים שאינם אבטחת מידע כדוגמת שדרוג השרתים של אבטחת מידע (מתקציב שדרוג שרתים) הכפלת שרתים להגברת יתירות (מתקציב שדרוג שרתים), וכדומה. התערבות הארכיטקט הראשי חלה ברמת מדיניות מאקרו ללא כל התערבות במיקרו. לדוגמא: החלטה שאנו מאפשרים לגורמים התומכים בעירייה בתוכנות קריטיות, בחומרה קריטית או בציוד תקשורת קריטי להתחבר לעירייה מרחוק למתן שירות היא של הארכיטקט הראשי, איך זה מבוצע בפועל ומהם נהלי העבודה זאת החלטה בלעדית של אבטחת מידע ללא התערבות. המדיניות של "איך כן" במקום "לא גורף" היא מדיניות של אגף המחשוב, היישום הוא של אבטחת מידע ללא כל התערבות."**.

50. מהראיונות שבוצעו עולה כי מחד קיימת מעורבות רבה יחסית של הארכיטקט הראשי בנושאים תפעוליים ושוטפים בתחום אבטחת מידע אולם מאידך, הוא אינו מספק את הסיוע המקצועי והניהולי הנדרש למנהל יחידת אבטחת מידע ברמה המערכתית הכללית האסטרטגית ממנהלו הישיר, לדוגמא שיתוף בהכנת תוכניות עבודה, בניית תקציב, קביעת סדרי עדיפויות נכונים לביצוע, גיבוש מדיניות וכו'.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות למצאים כי: **"הארכיטקט הראשי מספק סיוע מקצועי וניהולי נדרש ברמה מערכתית ואסטרטגית בעבודה השותפת."**

התייחסות מנהל אבטחת המידע: **"הארכיטקט הראשי הוא היועץ המקצועי שלי."**.

הביקורת מציינת בהתייחס לתגובת הנהלת אגף המחשוב כי הממצאים המצויינים בסעיף נכונים למועד ביצוע הראיונות ואיסוף הממצאים. הביקורת רואה באור חיוב את השינוי בגישה ובמצב כפי שדווחה במהלך ביצוע הביקורת.

פרק ו - תקציב

51. כאמור, על פי המבנה הארגוני בעירייה, יחידת אבטחת מידע כפופה לאגף מחשוב, על כן תקציבה של היחידה מתוקצב מאגף המחשוב.

ממצאים

52. על פי הצעת התקציב לשנת הכספים 2006, תקציבו הכולל של אגף המחשוב הסתכם לכ – 90,000,000 ש"ח. סכום של כ- 57,610,000 ש"ח נקבע במסגרת התקציב הרגיל וסכום של 32,200,000 ש"ח נקבע במסגרת התקציב הבלתי רגיל.

הנהלת אגף המחשוב מסרה לביקורת כי: **"החלוקה היא קצת פחות מ- 50% לשכר עובדי עירייה וקצת יותר מ- 50% לשאר."**

אגף המחשוב בעירייה מונה 250 משרות בעוד שיחידת אבטחת מידע מונה בין 3.5 ל – 4 משרות (כ- 1.5% מסך כל המשרות באגף).

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות למצאים כי: **"אגף המחשוב מונה 250 עובדים מתוכם כ- 125 משרות מתוך ה- 250 הם של עובדי עירייה, יתרת העובדים הם נש"מים ויועצים ורק מיעוטם עובדי עירייה."**

53. על סמך הנתונים שהציג לביקורת מנהל אבטחת מידע, תקציב יחידת אבטחת מידע לשנת הכספים 2006 חולק באופן הבא:

יעוץ חיצוני:	200,000 ש"ח
רכש:	200,000 ש"ח
אחזקות	200,000 ש"ח
שכר עובדים	700,000 ש"ח
שכר נשמ"ים:	280,000 ש"ח

54. תקציב יחידת אבטחת מידע לשנת 2006, הסתכם לסך של כ- 1,600,000, והיווה כ – 1.8% מתקציב האגף הכולל לאותה שנה.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"מעבר לתקציבים הישירים הנמצאים תחת הכותרת "אבטחת מידע" קיימים תקציבים בסעיפים אחרים כדוגמה: שדרוג שרתים – נרכשו שש שרתים לאבטחת מידע בעלות כוללת של 210 אלף ₪."**.

55. לא ניתן לציין כלל אצבע ברור אשר קובע מהו התקציב הדרוש לכל רשות מקומית, על מנת למלא את אחריותה לאבטחת מידע, על כן לא ניתן לקבוע באופן חד משמעי מהו התקציב הנדרש ליחידת אבטחת מידע בעיריית תל-אביב- יפו. כעקרון, תקציב אבטחת המידע אמור להיגזר מצרכי הרשות, מאגרי המידע אותם מנהלת הרשות, דרישות וסדרי עדיפויות שקובעת הנהלת הרשות וזאת לאחר שבוצע סקר סיכונים מקיף בנושא.

56. מנהל אבטחת מידע אינו מעורב בהכנת התקציב וקביעת היקפו וסעיפיו. הדבר פוגע ביכולתו לפתח ולקדם את נושאי אבטחת מידע עפ"י צרכי התחום, בהתאם לתפיסתו וסדרי עדיפויותיו.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"מנהל אבטחת המידע קובע באופן בלעדי את הנושאים שברצונו לבצע בשנת העבודה הבאה. במסגרת הסכום שהוקצה לו מתעדף מנהל אבטחת המידע את הנושאים, אין כל התערבות בסדרי העדיפות שנקבעים ע"י אבטחת מידע."**

התייחסות מנהל אבטחת מידע: **"בתקציב ותוכנית עבודה 2007 מנהל אבטחת מידע קבע בלעדית את התוכנית."**.

57. כמו כן, לא קיימת תוכנית עבודה שנתית מסודרת המתייחסת לתחום אבטחת המידע. באגף המחשוב לא נקבעה תוכנית של יעדים ומדדים על פיה פועל מנהל אבטחת מידע וממנה נגזרים ביצועיו. לטענת הארכיטקט הראשי בתוכנית העבודה השנתית בעירייה אין התייחסות לנושא אבטחת המידע, לכן לא ניתן להכין תוכנית של יעדים ומדדים המתייחסת לפעילות אבטחת המידע.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"מנהל אבטחת מידע יכין עד לתאריך 15.2.2007 הכוללת יעדים ומדדים לאישור הנהלת האגף."**. (הטעות במקור).

מברור שערכה הביקורת לאחר קבלת התגובות מאגף המחשוב, נמסר על ידי מנהל אבטחת מידע כי עליו להכין תוכנית עבודה שנתית מסודרת הכוללת קביעת יעדים ומדדים.

פרק ז - הערכת סיכונים

58. מערכות אבטחת מידע אמורות להתבסס על הנחות יסוד המגדירות איומים, נקודות חולשה ונקודות חזקות במערכת. על ממונה אבטחת המידע לבחון ולהצדיק את הנחותיו.

59. הנהלת העירייה אחראית (עד כדי אחריות אישית) לנקוט בפעולות מניעה אשר יש בהן כדי לזהות את הסיכונים הקיימים ולהפחית משמעותית את החשיפה להם. אחת מפעולות המניעה החשובות בנושא זה היא עריכת סקר סיכונים (Risk Analysis) בנושא אבטחת מערכות מידע.

60. הערכת הסיכונים מגדירה את רמת הרגישות של המערכות ומתייחסת למכלול סיכוני אבטחת המידע הפוטנציאלים הנובעים ממערכות המידע ומההתנהלות השוטפת של העירייה. סיווג רמת הרגישות של כל מערכת נקבעת לפי רגישות המידע בו היא מטפלת.

61. תהליך זה מתבסס על סיווג הנכסים, אופי פעילות העירייה ומהות העבודה ביחידות ובאגפים השונים.

62. מתפקידו של מנהל יחידת אבטחת מידע לעדכן את הערכת הסיכונים בעת ביצוע שינויים משמעותיים בתהליכי העבודה, במערכות המידע או באיומי אבטחת מידע.

63. סקר סיכונים מקיף נועד לבחון את אופי, יעילות ורמת אבטחת המידע בעירייה, ולהשגת היעדים הבאים:

א. לאתר את הסיכונים והאיומים להם חשופה מערכת המחשב;

ב. לזהות את מערכות המידע הרגישות בעירייה;

ג. להציג את הסיכונים שנמצאו על פי משקלם היחסי;

ד. להציג את הפעולות המתקנות שיאפשרו להקטין את הסיכונים.

פרק ח - מדיניות אבטחת מידע

64. הגדרת מדיניות אבטחת מידע איננה פעולה חד פעמית של כתיבת מסמך, אלא תהליך מתמשך ומתחדש בהתאם לאיומים וסיכונים. מדיניות אבטחת המידע כוללת: קווי מדיניות, סטנדרטים, הנחיות ונהלים, כללי גישה, מתן הרשאות וסיווג מידע לפי רגישותו. בנוסף, מדיניות אבטחת המידע מאפשרת להנהלת העירייה להשיג את מטרותיה, בכל הקשור לאבטחת מידע, ביתר קלות. להלן עקרונות מדיניות אבטחת מידע:

א. ניתוח סיכונים - בחינת תשתיות ופעילויות העירייה, תוך זיהוי איומים, הערכת חשיפות וקביעת מוקדי סיכון.

ב. בחינת עיסוקים - זיהוי תחומי העיסוק של בעלי התפקידים בעירייה הקובעים סמכויות גישה ושימוש במערכות המידע הממוחשבות.

ג. עקרון "הצורך לדעת"(Need to Know) - הגבלת תפוצת המידע לבעלי התפקידים הזקוקים לו.

ד. מידור המידע - פעילויות המחלקות את מערכות המידע הממוחשבות לתחומים לוגיים ופיזיים.

ה. זיהוי "בעלי המידע" (Owners of Data) - הגורמים המאשרים שימוש במידע מסוים על ידי אנשים בעירייה או מחוצה לה.

ו. הגדרת הגורמים האחראים על יישום מדיניות אבטחת המידע ומערכת הרשאות.

ז. סיווג המידע מבחינת רגישותו וחשיבותו לעירייה, באופן בלתי תלוי במשתמשים (התועלת לגורם זר לגרום נזק לעירייה כתוצאה מחשיפת המידע). ניתן להגדיר גם רמת סיווג למשתמשים.

ח. עיצוב מערכת הרשאות - עקרון "הצורך לדעת" קובע את הרשאות הגישה והשימוש במידע. רמת רגישות המידע קובעת את כללי הגישה ואמצעי ההגנה והבקרה הנדרשים עבור כל הרשאת גישה.

ט. בקרה שוטפת – המדיניות מהווה בסיס לבקרה והערכה שוטפת בתחום אבטחת המידע.

65. על המדיניות להיות מתועדת במסמך המופץ בכל העירייה ומהווה בסיס לפיתוח בקרות אבטחת מידע ולכתיבת נהלי אבטחת מידע.

66. תהליך בניית המדיניות כולל שלושה שלבים עיקריים, העוסקים בשתי רמות שונות של המדיניות:

א. קביעת עקרונות אבטחת מידע כלליים – אלו קווים מנחים כללים המגדירים ברמה כללית מהם עיקרי מדיניות אבטחת המידע;

ב. קביעת מדיניות מפורטת על בסיס העקרונות הכלליים – אלו הם נהלים והנחיות פרטניים הנבנים על מנת ליישם את מדיניות אבטחת המידע בעירייה כולה.

יישום המדיניות

67. דוגמאות לעקרונות אבטחת מידע כלליים:

א. מנגנוני זיהוי ואימות הזיהוי;

ב. שמירת מידע אך ורק ברשת (אי שמירת נתונים בדיסק המקומי);

ג. רישום ותיעוד אירועים חריגים;

ד. כיבוי מחשבים בסוף כל יום;

ה. דיווח על כל אירוע חריג לממונה אבטחת המידע.

68. דוגמאות למדיניות מפורטת:

א. בניית ארכיטקטורת רשת מאובטחת בהתאם לאיומים הרלבנטיים;

ב. ביצוע הקשחה של השרתים בעירייה;

ג. ביצוע הקשחה של רכיבי התקשורת (נתבים, מתגים וכד');

ד. התקנת אנטי וירוס לשרתים ולתחנות קצה;

ה. התקנה שוטפת של עדכוני תוכנה;

ו. שימוש במוצר להצפנת תעבורת דואר אלקטרוני מול ספקים רגישים;

ז. קביעת מדיניות לגבי סוג האימות של המשתמשים (סיסמה, כרטיס חכם וכד');

ח. נטרול כונני הדיסקטים וכונני ה- CD במחשבים;

ט. גיבוש הנחיות עבודה לשימוש במחשב נייד;

י. שימוש במנגנוני אבטחה באפליקציות ומסדי נתונים.

69. שלבי יישום המדיניות הינם:

א. כתיבת נהלים ברורים והפצתם לכלל עובדי העירייה.

ב. בדיקות אבטחה.

ג. איתור חולשות אבטחה:

1) ניתוח התוצאות מבדיקת האבטחה;

2) ביצוע בדיקת חדירה לרשת;

3) שינויים והוספת מערכות ורכיבים חדשים;

4) גילוי חולשות אבטחה בעולם;

5) עדכון מדיניות האבטחה הקיימת.

ממצאים

70. מבדיקת הביקורת עולה כי מדיניות אבטחת מידע בעירייה עודכנה לאחרונה בשנת 2004. במדיניות אבטחת המידע נרשמו עקרונות אבטחת מידע כלליים בלבד. לא נמצאה כל התייחסות למדיניות אבטחת מידע מפורטת, יתרה מכך הטיוטה למדיניות הכללית שהוכנה, לא אושרה עד ליום כתיבת דוח הביקורת.

הנהלת אגף המחשוב: מסרה לביקורת בהתייחסות לממצאים כי: **"לעניין אישור מסמך המדיניות, ראה התייחסותנו לסעיף 6 (1.1.2007) מדיניות אבטחת מידע מפורטת – הינה למעשה אוסף של**

נהלים והוראות עבודה כפועל יוצא ממסמך המדיניות. לנושא זה התייחסותינו בהמשך בסעיף 77.".

71. ישנם מעט נהלים כתובים והנחיות עבודה המתועדות באופן חלקי, המשמשים את העירייה. בנוסף, מבדיקת הביקורת עולה כי מרבית העובדים אינם מודעים לנהלים ולהנחיות אלו.

72. יחידת אבטחת מידע בעיריית תל-אביב-יפו קיבלה רשימת נהלי אבטחת מידע מסודרת מעיריית ירושלים ותכננה ליישם נהלים אלו. עד למועד עריכת הביקורת נהלים אלו לא יושמו, בטענה כי לא הוקצה כוח אדם ראוי ביחידת אבטחת מידע שיכול לטפל בנושא התאמת הנהלים לצרכי העירייה.

73. להלן רשימת הנהלים הקיימים בעירייה, המתייחסים לנושא אבטחת המידע, כפי שעולה ממצאי הביקורת:

שם הנוהל	תיאור הנוהל	סטאטוס	הערות מנהל אבטחת מידע
מדיניות אבטחת מידע	מסמך מדיניות שיאושר על ידי הנהלת העירייה.	התקבלו הערות סמנכ"ל לתיקון	בטיפול
אבטחה פיזית	אבטחה פיזית של יחידות המחשב אבטחת תחנות קצה	נוהל פנימי המגדיר את עבודת יחידת אבטחת מידע בלבד	הנוהל מתייחס לבקורת פיזית. משמש את מבצע הביקורת. מסקנות (מרוכזות) הועברו לסמנכ"ל רלוונטי
גיבוי	הוכן על ידי ק	בתהליך בדיקה עם חברה חיצונית	יש 2 נהלים. גיבוי אתר חיצוני – עובדים לפיו בשטח. גיבוי בתוך העירייה – עדיין בעבודה
אבטחת יישומים	תהליך בדיקה וסיווג אבטחתי של פרויקט. הפקת הנחיות אבטחה לפרויקט.	נוהל פנימי המגדיר את עבודת יחידת אבטחת מידע בלבד	הוא רלוונטי לכל עבודת האגף. על פיו מסווגות המערכות החדשות – וניתנות הנחיות אבטחה לאפליקציה (לדוגמא קופת מחו"ג)
נוהל בדיקות סביבת FIREWALL	סדרת בדיקות שיש לבצע בסיום כל שינוי בסביבת ה-FW לפני חזרה לעבודה	נוהל פנימי המגדיר את עבודת יחידת אבטחת מידע בלבד	מבוצע בכל שינוי בסביבת השרתים המדוברת. זה נוהל חשוב מאוד
בדיקות לתחנה נגועה	סדרת בדיקות שיש לבצע בתחנה שיש חשש שנגועה	בתהליך בדיקה עם חברה חיצונית	נוהל קיים שאמור להיות מבוצע ע"י עובדי אבטחת מידע או טכנאים בכל פעם שמתעורר חשש לוירוס או לתוכנה פוגענית

שם הנהל	תיאור הנהל	סטאטוס	הערות מנהל אבטחת מידע
	בתוכנה עוינת		אחרת. הנוהל ייושם עד ה-15.3.07
אבטחת תקשורת ותשתיות		בתהליך הכנה על ידי חברה חיצונית	הנוהל נכתב וסוכם. לאחר עיון נוסף הוא יועבר להתייחסות הגורמים הטכניים באגף המחשוב ובהמשך לאישור ההנהלה

74. על פי הממצאים, מרבית הנהלים המפורטים בטבלה נמצאים בסטאטוס של בדיקה ו/או המתנה לאישור.

75. בנוסף לנהלים האמורים לעיל, קיימים כ-38 נהלים שונים המצויים בשלב טיוטה ראשוני. על פי דיווחי מנהל אבטחת מידע הנהלים הללו מעוכבים זמן רב בשלב הטיוטה מהסיבות הבאות: היעדר המשאבים הנדרשים לנושא, חוסר בכח אדם לכתיבת הנהלים, עיכוב של אישור הנהלים על ידי הארכיטקט הראשי, גורמים מקצועיים, סמנכ"ל, מנהל האגף ומועצת העירייה.

התייחסות מנהל אבטחת מידע: **"העיכוב נגרם אך ורק ע"י מנהל אבטחת מידע".**

76. להלן תהליך אישור נוהל בנושא אבטחת מידע בעיריית תל-אביב- יפו:

א. כתיבת הנוהל על ידי יחידת אבטחת המידע;

ב. אישור הנוהל על ידי הארכיטקט הראשי;

ג. אישור הנוהל על ידי הצוות הטכני המטפל בנושא כגון: מנהלי רשת, עובדי מחלקת DBA וכ"ו;

ד. אישור הנוהל על ידי מנהל המחלקה המקצועית;

ה. אישור הנוהל על ידי מנהל האגף;

ו. אישור הנוהל על ידי סמנכ"ל תיכנון;

ז. אישור הנוהל על ידי מועצת העירייה.

77. משיחה עם ממונה יחידת אבטחת המידע נמצא כי, ברוב המקרים נוצרת "סחבת בירוקרטית", הגורמת לעיכוב הטיפול בנוהל.

הנהלת אגף המחשוב: מסרה לביקורת בהתייחסות לממצאים כי: **"כיום ישנם שבעה נהלים סגורים, שלושה נהלים בתהליכי טיפול, ועוד שלושים הנחיות עבודה שהן פועל יוצא של מסמך המדיניות. נהלים והוראות עבודה אלו הועברו לידיעת הגורמים התפעוליים כולל אלו שמחוץ לאגף המחשוב. עד לתאריך 15.12 נהלים והוראות עבודה אלו יפורסמו באתר האינטראנט/הפורטל העירוני כולל הודעה לכל פורום אגף המחשוב על עצם פרסום זה. עד ה-**

15.2 יתפרסמו שלושת הנהלים שבתהליך טיפול. להערכתו של מנהל אבטחת מידע חסרים עדיין בין עשר לחמש עשרה נהלים בכדי לכסות את מגוון הפעילויות כפועל יוצא של מסמך המדיניות. מנהל אבטחת מידע יכין עד 1.1 את רשימת הנהלים החסרים הנ"ל. אגף המחשוב יסיים להכין טיוטות לנהלים אלו עד ה- 1.6.2007 מתוך מטרה להביא לאישורם ופרסומם באתר האינטראנט/פורטל העירוני במהלך הרבעון האחרון של 2007. בטבלה המופיעה בסעיף 73 תוקנו טעויות שנפלו בהכנת הטבלה. לנושא תהליך אישור הנוהל בעיריית ת"א, מכיוון שהנוהל מערב גורמים רבים ואמור להתבצע ע"י אותם גורמים, מצאנו לנכון לקבל התייחסות לנוהל והערות מכל אותם גורמים מעורבים. מכיוון שלדעת הביקורת אישור הנוהל דורש מספר רב ולא סביר של גורמים נשמח לקבל את הצעת הביקורת לסבב קצר יותר. יתרה מכך הביקורת לא ציינה את אגף ארגון ותקינה כעוד גורם בתהליך אישור הנוהל (נוהל חיצוני לאגף).".

פרק ט - ארגון אבטחת המידע

78. יחידת אבטחת מידע בעירייה כפופה לאגף המחשוב, כתוצאה מכך קיימים מקרים בהם נוצרים מעין "ניגודי אינטרסים" סמויים בין מטרות אבטחת המידע ובין מטרות אגף המחשוב, התופס עצמו כמי שאמור לסייע למשתמשים לבצע עבודתם ביעילות ובמהירות, ולספק את כל הכלים המחשובים האפשריים לביצוע יעיל של העבודה, לעתים תוך כדי קיצורי דרך ואי הקפדה בנושאי אבטחת מידע.

79. בפני צוות הביקורת הוצג מקרה שבו עובד ביקש לקבל הרשאה למערכת מסויימת הפועלת בעירייה, הדורשת את אישורם של שישה מנהלי מאגרים שונים. לטענת הארכיטקט הראשי מצב זה אינו סביר, לאור עיכובים שנוצרים בזמן ההמתנה לחתימת מנהלי המאגרים. בעקבות כך הורה הארכיטקט הראשי לממונה אבטחת המידע לקצר את תהליך קבלת ההרשאה למערכת על ידי צמצום מספר הגורמים המאשרים את ההרשאה. מבחינת ממונה אבטחת המידע בקשה זו אינה סבירה ופוגעת במערך אבטחת המידע בעירייה, לאור העובדה כי המערכת מציגה נתונים הקשורים למאגרי מידע הנמצאים תחת אחריותם של ששת מנהלי המאגרים.

80. במצב הקיים ישנה עמימות ואי בהירות ביחס לחלוקת סמכויות, קבלת החלטות בנושא אבטחת מידע והגדרת מקור סמכות אחד לקבלת החלטות בתחום. כמו כן, קיימים מקרים בהם מנהלי אגפים בעירייה עוקפים את סמכותו של מנהל אבטחת מידע ופונים בנושאי אבטחת מידע ישירות לארכיטקט הראשי ו/או למנהל אגף המחשוב. כך נוצר מצב שבו הארכיטקט הראשי ומנהל האגף מקבלים החלטות מבלי לערב את מנהל אבטחת המידע. לדוגמה: לפני כשנתיים הועלתה לרשת של עיריית תל-אביב-יפו מערכת המכילה בבסיס הנתונים מספרי כרטיסי אשראי. המערכת הותקנה ללא ידיעתו של מנהל אבטחת מידע. כעבור תקופה ארוכה שבה פעלה המערכת, הופנתה בקשה בנושא הרשאות המערכת במאגרי המידע למנהל אבטחת המידע. יש לציין כי רק בשלב זה נחשף

מנהל אבטחת מידע למערכת ולבסיס הנתונים שלה. בבדיקה שערך ממונה אבטחת המידע נמצא כי מספרי כרטיסי האשראי אינם מוצפנים וזאת בניגוד לכללים שהנחילו אנשי אבטחת מידע בעירייה ובכלל.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים הרשומים בפרק זה כי: **"לא קיימת שום עמימות או אי בהירות. קבלת ההחלטות היא אך ורק ע"י מנהל אבטחת המידע. הצעת הנוהל המדובר שונתה כתוצאה מסיכום דיון בהשתתפות מנהל אבטחת המידע, והסיכום היה על דעת כל המשתתפים בדיון (ולבסוף הנוהל לא שונה כתוצאה מהתנגדות מנהלי המאגרים). כל שיפורי התהליך שהוצעו ולהם הסכימו גורמים אחרים אך מנהל אבטחת המידע התנגד - לא יושמו וסיכום הפגישה כלל רק את המוסכם. דוגמא לנושא שלא בוצע: מתן ההרשאות עפ"י הנהלים ע"י צוות מוקד התמיכה כפי שקיים בארגונים אחרים. השיפור הוא מהותי בהיבט זמני התגובה ואין לו כל בעיה בהיבט אבטחת מידע היות וברגע שהנוהל מקויים (יש את כל החתימות על הטופס) גם צוות אבטחת מידע פועל באופן אוטומטי לחלוטין. ולפיכך האמור בסעיף אינו נכון."**.

עוד מסרה הנהלת אגף המחשוב כי: **"מנהל אגף המחשוב והארכיטקט הראשי מעולם לא עקפו את מנהל אבטחת המידע. גם כאשר הייתה פניה ישירה – ההחלטה הייתה בתאום, בשיתוף ובהסכמת אבטחת מידע. לגבי המערכת המדוברת (קופת מחו"ג), המערכת התחילה את פיתוחה בשנת 92 לפי אפיון ותוכנית שאושרה בעבר, כאשר אין לאגף מנדט לעשות שינויים בשלב הנוכחי. למרות זאת המערכת הועברה לאישור אבטחת מידע ולא עלתה לאויר לפני ביצוע השינויים שדרשה אבטחת מידע וזאת בניגוד לתוכנית העבודה המאושרת של האגף. אין ולא היתה מעולם העלאה של מערכת חדשה ו/או רכישה של מערכת חדשה מאז מנוי ההנהלה החדשה של האגף ללא אישור ומעורבות של אבטחת מידע. עפ"י החלטת המנכ"ל משנה שעברה, לאגף המחשוב אין מנדט לבצע שינויים במערכות קיימות מבלי אישור ועדת שוש"ים העירונית. בגלל חשיבות נושא אבטחת המידע לא פעם הנהלת האגף החליטה לאשר שינויים ופיתוחים בהקשר אבטחת מידע, כדוגמת השנוי במערכת ה-** IVR **(שעלתה לאויר בקיץ 2004) באשר להצפנת כרטיסי האשראי."**.

פרק י - אבטחה פיזית

81. גישה פיזית למחשב (או לנתב) בדרך כלל נותנת למשתמש מתוחכם, במידה מספקת, שליטה מלאה על אותו מחשב. גישה פיזית לעורק רשת בדרך כלל מאפשרת לאדם לצותת לאותו עורק, לשבש אותו, או להזרים אליו תנועה. אין טעם בהתקנת אמצעי אבטחת תוכנה מסובכים, כאשר הגישה לחומרה אינה מבוקרת.

82. במטרה למנוע גישה לא מורשית, נזק למידע והפרעה לתהליכים הארגוניים, יש ליישם אבטחה פיזית בעיקר באזורים רגישים ולצורך הגנה על ציוד רגיש.

83. עיקרי האבטחה הפיזית כוללים:

א. מניעת גישה פיזית למערכות המידע, מפני גורמים לא מורשים על ידי שימוש במנעולים, קודנים וכו';

ב. חלוקת סביבת העבודה למעגלי אבטחה/אזורים מאובטחים לפי רמות רגישות. להלן דוגמא לאופן חלוקת אזורים לפי רמת רגישות: גבוהה (חדרי שרתים), עסקית (אזור עבודה לעובדי משרד אחורי – Back Office), ציבורית (הקהל הרחב רשאי להסתובב באזור זה);

ג. תחזוקה ובקרה שוטפת של שירותים תומכים, שתפקידם למנוע את קריסת המערכת;

ד. היבט נוסף של אבטחה פיזית המיועד למנוע פגיעה לא מכוונת בציוד רגיש של העירייה, כגון שריפות, הצפות וכדומה, העלולות לגרום לנזק בלתי הפיך למערכות העירייה וכתוצאה מכך איבוד מידע יקר;

ה. הגנה על המערכות של העירייה מפני יירוט של מידע. בעזרת הטכניקה של יירוט מידע יכול גורם זר לראות את תעבורת המידע בתוך הרשת;

ו. הגנה על המערכות הניידות של העירייה כגון מחשבים ניידים, מדיה ניידת (דיסקים, DISK ON KEY) מפני גניבות (גניבה פיזית של המערכות הניידות או גניבת מידע מתוכן) ושימוש לא מורשה;

ז. כחלק מההגנה על המידע בעירייה יש להגן על ציוד וניירת המכילים מידע רגיש.

ממצאים

84. על מנת לתחקר אירוע אבטחת מידע שהתרחש באחד מן המתקנים הרגישים, יש למצוא למי הייתה נגישות למתקן בתקופה שבסמוך לאירוע. מבדיקות הביקורת ומשיחות שהתקיימו עם העובדים האמונים על המתקנים הרגישים, עולה כי לא קיים רישום המתעד כל כניסה של המבקרים החיצוניים למתקנים הרגישים בעירייה.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"נוהל אבטחה פיזית יעודכן כך שיכלול את הדברים הבאים: (1) הגדרה של מתקן רגיש, (2) מיפוי מתקנים רגישים בעירייה המאושרים ע"י מנהלי האגפים הרלוונטיים, (3) מנגנון עדכון הטבלה, (4) סעיף המחייב את מנהל האגף הרלוונטי לוודא כי קיים רישום המתעד כל כניסה כנדרש. הנוהל ירוענן לכל מנהלי האגפים והגורמים המקצועיים בכל אגף אחת לחצי שנה. הנוהל יהיה נוהל עירוני ופרסומו יהיה עפ"י התהליך ולוח הזמנים העירוני."**.

85. לא מתבצעת בחינה שוטפת של הגורמים בעלי גישה למתקנים רגישים, זאת על מנת לבדוק האם הגורמים להם יש גישה למתקנים עדיין זקוקים לכך לצורך ביצוע עבודתם השוטפת. לדוגמה,

לצוות המס"פ ישנה גישה לחדר השרתים והגיבויים המרכזי, למרות שבפועל אין הם צריכים גישה לחדר זה על מנת לבצע את עבודתם.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"נוהל אבטחה פיזית יעודכן ויכלול הנחיות לגבי בעלי גישה למתקנים רגישים כולל מנגנון בקרה לעדכון הרשימה. בכלל זה ישונו ההנחיות לצוות המס"פ ותיאסר הגישה לחדר השרתים למי שאינו מורשה. שינוי זה יכנס לתוקף החל מה- 15.12".**

86. לדבריו של ממונה אבטחת המידע ישנו נוהל כתוב, המחייב כי כל הפקדה או השאלה של מדיית אחסון תאושר על ידי גורם מתאים ותרשם. רכזי המחשוב אמורים לאכוף נוהל זה. מראיונות שהתקיימו עם רכזי המחשוב עולה כי הם אינם מודעים כלל לנוהל האמור.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"באחריות אבטחת מידע להפיץ נוהל זה מחדש עד ה- 1.12 ומידי חצי שנה לרענן את הנוהל אצל הרכזים. כמו כן, בפגישה הבאה של רכזי המחשוב עם הנהלת האגף הנושא יוצג ויוסבר באופן פרטני.".**

87. הקודן של חדר השרתים גלוי, באופן שבו כל עובר אורח יכול לראות את הקוד בזמן שעובד מבצע כניסה לחדר השרתים. בנוסף, הקוד ידוע גם לעובדים אשר ביצעו פרוייקט זמני בחדר השרתים. מבדיקות הביקורת מול אנשי אגף המחשוב עולה כי קוד הכניסה לאזורים הרגישים אינו משתנה מידי תקופה.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"מנהל תחום אבטחת מידע יפנה להנהלת הבית להזמין כבוי לשלושת הקודנים הקיימים מתוך מטרה לנסות ולרכוש עוד השנה. הפניה תבוצע עד ה- 10.12. מנהל אבטחת מידע יהיה אחראי על שנוי הקוד בקודנים אחת לחצי שנה ומסירת הקוד למורשים. ההחלפה הראשונה תתבצע במהלך דצמבר 2006.".**

88. משיחות עם גורמים שונים שנערכו במהלך הביקורת, עולה כי החדרים בהם נמצא מידע רגיש כגון חדרי שרתים, לעיתים נשארים פתוחים. מצב זה חושף את העירייה בפני סיכון של חדירת גורם עוין וגניבת מידע.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"מנהל ענף שירות לקוחות ותפעול יוציא הנחיה עד 1.12 כי אין להשאיר חדרים פתוחים. אחריות מנהל אבטחת מידע אחת לתקופה (יחד עם שנוי הקוד) לרענן הנחיה זו בקרב דיירי החדרים.".**

89. חדרי השרתים מכילים ציוד אלקטרוני ושרתים בעלי יכולות טכנולוגיות גבוהות. על מנת להבטיח את עבודתם התקינה יש לדאוג שהטמפרטורה בחדר השרתים לא תעלה על 20 מעלות. בדיקות הביקורת העלו כי מערכת מיזוג האוויר בחדרי השרתים אינה מתוחזקת בצורה ראויה ואף נמצא כי באחד מחדרי השרתים לא נמצא כלל מיזוג.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"בימים אלו מותקן מזגן נוסף בחדר השרתים שבבניין העירייה. ב- 15.11 סיימנו "ניקיון" של כבלים רבים ישנים ומיותרים מתחת הרצפה הצפה שהיוו חסימה לזרימת אויר תקינה. מנהל מחלקת תפעול יזמין את ממונה המיזוג העירוני לבדיקה של מערכות המיזוג בחדרי השרתים. אם זאת נשמח לקבל התייחסות ספציפית של הביקורת למקום הבעיה."**.

90. מערכת הצנרת בבניין אינה ידועה לגורמים האמונים על נושא אבטחת מידע ועל כן עלולה לסכן את חדרי השרתים, במצב של התפוצצות אחד הצינורות. בדרך כלל נהוג למקם את חדרי השרתים בחדר שבו לא עוברת צנרת הבניין. מבדיקת הביקורת עולה כי לא קיים בעירייה ציוד המתריע בפני הצפות או רטיבות בחדרי התקשורת או השרתים.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"מנהל אבטחת מידע יפנה עד ה-15.12 להנהלת הבית בכדי לקבל את מיפוי הצנרת בחדרי השרתים העירוניים. בחדר השרתים המרכזי (בניין העירייה) קיימת מערכת לגלוי והתרעה על הצפה. לא קיימת מערכת כזאת בחדר השרתים של מנהל הנדסה. מנהל מחלקת תפעול יערך לרכוש מערכת כזאת במהלך הרבעון הראשון של 2007 לחוות השרתים שבמנהל הנדסה."**.

91. לעיתים, חדר השרתים משמש כמקום אחסון לציוד של המנקות בעירייה המחזיקות ברשותם מפתחות לחדרי השרתים.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"האמור בסעיף זה מתייחס אך ורק לחדרים הנמצאים באתרים חיצוניים בלבד. מנהל אבטחת מידע יתייחס לנושא בנוהל אבטחה פיזית ובנוסף יפנה בכתב עד ה- 15.12 לכל מנהלי האתרים המתריע על תופעה חמורה זו ודורש להפסיקה לאלתר."**.

92. ישנה האפשרות לגנוב מידע על ידי האזנה באמצעות ציוד אלקטרוני לתווך התקשורת שעליו עובר המידע. בעירייה אין אמצעי התרעה על האזנה לא מורשית לרשת התקשורת ולכן ניתן לבצע יירוט מידע.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"סעיף זה מתייחס לשני סוגי האזנה לתווך התקשורת: (1) האזנה ע"י התחברות פיזית לרשת – נושא זה יפתר באמצעות תוכנה וחומרה הנמצאים בתהליך רכש ואמורים להיות מותקנים ומפועלים באופן מלא עד סוף הרבעון הראשון של 2007, (2) האזנה באמצעות ציוד אלחוטי ומרוחק – מניעת אפשרות זאת כרוכה בעלויות רבות ומתבצעת בארגונים צבאיים, לדעת האגף ביחס עלות תועלת אין מקום להשקעות מסוג זה."**.

פרק יא - אבטחה לוגית

93. מטרתה של האבטחה הלוגית היא בעצם זיהוי ואימות המונע מאנשים שאינם מורשים (או תהליכים שאינם מורשים) להיכנס למאגרי המידע השונים.

94. כדי שהמערכת תוכל לזהות ולהבדיל בין המשתמשים השונים יש צורך באימות וזיהוי המשתמשים.

95. בנוסף לכך, באמצעות הבקרות המיושמות על הגישה הלוגית ניתן לדעת את זהות המשתמש שניגש למשאב מסוים במערכת ואלו פעולות הוא ביצע באותו משאב. האבטחה הלוגית משמשת את מנהלי מערכת האבטחה בסינון גישתם של המשתמשים לכלל המידע המצוי במערכת.

96. כיום, גובר הצורך בגישה אל משאבי העירייה מרחוק לטובת ביצוע פעולות על ידי העובדים מחוצה לה, תחזוקה מהירה וזולה יותר מגורמי תמיכה או אפילו רק בכדי לאפשר עבודה על הדואר האלקטרוני לעובדים שנמצאים מחוץ לעירייה.

97. עם פתיחת דלתות העירייה כלפי חוץ, על יחידת אבטחת מידע להתמודד מול איום נוסף שנוצר עקב האפשרות להתחברות של תחנות קצה לא מוגנות מחוץ לעירייה.

98. על מנת להתמודד מול איום זה יחידת אבטחת מידע מנפיקה התקני טוקן (token) המשמשים לזיהוי ודאי של המשתמש, על ידי כך נמנעת התחברות של משתמשים לא מורשים למערכות העירייה.

99. בנוסף להתקן הטוקן המזהה את המשתמש באופן ודאי, נפתח קו VPN מאובטח ומוצפן באמצאות פרוטוקול SSL, שדרכו מתקשר המחשב המרוחק עם השרת.

100. עיקרי האבטחה הלוגית כוללים:

א. זיהוי ואימות של המשתמשים באופן אינדיבידואלי באמצעות סיסמאות, tokens, או אמצעים אחרים.

ב. בקרות לגישה הלוגית- מעקב מתמשך על ניהול סיסמאות (עדכון ושינוי באופן שוטף), הרשאות ובקרה על ניסיונות גישה לא מורשים למערכת (קבצי LOG של מערכת ההפעלה).

ממצאים

101. המשתמשים אינם מחויבים בהחלפת סיסמה בכל פרק זמן קבוע. החלפת הסיסמאות נועדה למזער מצבים של שימוש לא מורשה בסיסמאות. כך לדוגמה, במידה ואדם זר חשף סיסמה של אחד

העובדים בעירייה הוא יוכל להיכנס למערכות ולבסיס הנתונים בהתאם להרשאות שניתנו לעובד. במידה וניתן תוקף לסיסמה הוא יוכל להשתמש בסיסמה לכל היותר במשך התוקף שהוגדר.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"שנוי סיסמאות אוטומטי כנדרש יוכל להתבצע רק לאחר השלמת המעבר לסוג שרתים אחד בלבד (ביטול שרתי נובל) במהלך שנת 2006 צומצם מספר שרתי הנובל בכ- 50% ונשארו כשלושים שרתים בלבד. צפי לסיום התהליך – סוף 2007. למרות האמור לעיל מנהל אבטחת מידע נקט במספר פעולות: (1) הטמעת מערכת לשנוי סיסמאות שהופעלה ע"י 2000 משתמשים עד כה, (2) הגברת המודעות של העובדים לנושא הסיסמאות, (3) הנחיית צוות ההתקנות על שנוי סיסמה בכל התקנה חדשה, (4) משלוח הודעה למשתמשים שלא שינו סיסמה במשך זמן רב על הצורך בשנוי סיסמה."**.

102. הקישור לבסיסי הנתונים השונים נעשה דרך האפליקציות השונות. לכן, על מנת לראות או לשנות את בסיסי הנתונים, לא מספיק שלעובד תהיה הרשאת כניסה למערכת הוא יזדקק בנוסף גם להרשאה בבסיס הנתונים. עובדים אשר עזבו את מקום העבודה נחסמים ב – ACTIVE DIRECTORY אך אינם נחסמים באפליקציות עצמן.

103. בעיה זו נוצרת כתוצאה מכך שהתוכניתנים הממונים על מתן סיסמאות לאפליקציות השונות אינם מקבלים דיווח לגבי עובדים שעזבו את העירייה או החליפו תפקיד בעירייה. אי לכך, ההרשאות שניתנו בעבר לאותם עובדים, אינן נחסמות. לאור האמור, נוצרת פרצה במערך אבטחת המידע, כך שעובדים שסיימו את תפקידם במחלקה מסויימת, תעמוד בפניהם אפשרות השימוש במערכות המידע בהן השתמשו בעבר, זאת למרות שכיום לעובדים האמורים אין צורך בשימוש באותן מערכות מידע.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"הפתרון לסוגיה זו הינו שימוש במתודולוגיית** single sign on (SSO) **שמשמעותה כניסה באמצעות סיסמה אחת במקום אחד למכלול השרותים. בעירייה קיימות חמש סביבות עבודה שונות: (1) סביבת המחשב המרכזי – בסביבה זאת בעיה זו אינה קיימת היות וכאשר עובד עוזב אבטחת מידע מבטלת/נועלת את סיסמת הגישה למחשב המרכזי, (2) סביבת פיתוח מחולל יישומים מג'יק – בסביבה זו אין יכולת כיום לעבוד במתודולוגיה זאת. עד מחצית 2008 מתוכננת החלפת סביבה זו בסביבה עדכנית (ע"י חברת מלם שזכתה במכרז לנושא) הכוללת בתוכה יישום מתודולוגיה זאת ואז ברגע שהעובד נחסם ב- AD הוא אינו יכול להיכנס למערכת, (3) סביבת** VB6 **– בסביבה זאת מתוכננת הסבה למתדולוגית** SSO **במהלך הרבעון הראשון של 2007, (4) סביבת** ASP.Net **– הפיתוח בסביבה זאת הינו עפ"י מתודולוגיית** SSO **מאז ומעולם, (5) סביבת** SAP **– הדרישות של העירייה מהחברה שזכתה במכרז השת"פ לפיתוח מחו"ג (נס) הינו פיתוח עפ"י מתודולוגיית** SSO."**.**

104. בעירייה ניתן לקבוע סיסמאות שאינן קשות לפיצוח (דוגמא לסיסמה: 123456), תבנית מסוג זה מקלה בצורה משמעותית על פורצים בגילוי הסיסמה.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"הנושא נדון בעבר באגף המחשוב והוחלט על השארת הפורמט הנוכחי. הסיבה היא יכולת ההתמודדות של מקצת משובדי העירייה עם התפעול היומיומי של סיסמה מסובכת כדוגמת זיהוי מצב המקדלת עברית/אנגלית/CAPS LOCK, הקלדת תוים מיוחדים, וכדומה. שנוי הפורמט יגרור תקלות תפעול רבות ויפגע ברמת השירות שהעירייה מספקת ללקוחותיה ועובדיה."**.

התייחסות מנהל אבטחת מידע: **"מורכבות נוכחית: הסטוריה – 5 דורות. מינימום 6 תוים.אין חיוב סיבוכיות (complexity). מורכבות אפשרית: יש אפשרות להוסיף סיבוכיות – לא בוצע מסיבות תפעוליות. סיבוכיות מחייבת הכללת תוים וסימנים מיוחדים. בגלל בעיית השפה, להערכתי, לא נוכל לעמוד בזה."**.

105. בכל הארגונים מתרחשים מקרים שבהם עובד שוכח סיסמה או לחילופין סיסמתו ננעלת עקב ניסיונות חוזרים וכושלים של כניסה למערכת. לרוב, מקרים אלו אינם חריגים ולא אמורים להיבדק, אך ישנן נסיבות חריגות האמורות להיבדק לגופן. בעירייה אין פרוצדורה מובנית לטיפול במקרים בהם סיסמה של עובד ננעלת, בדיקה והפקת לקחים, דבר העלול לגרום לכשל באבטחת המידע.

על פי נוהג העבודה הקיים היום בעירייה, צוות התמיכה הטלפונית מאפשר לשחרר סיסמאות דרך קווי טלפון לא בטוחים או בדואר אלקטרוני, מבלי לברר את זהות מבקש הסיסמה.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"מנהל אבטחת מידע יכין נוהל לטיפול בנושא עד ה- 1.2. על מנת לזהות את אותן נסיבות חריגות יש לבצע קישור בין מערכת ניהול פניות לקוחות הקיימת לבין ה- AD-(active dierectory) פעילות המבוצעת בימים אלו ומתוכננת להסתיים עד סוף 2007."**.

106. הסיסמאות בעירייה אינן נמסרות למשתמש בצורה מאובטחת אלא בשיחת טלפון, דבר העלול ליצור פגיעה ברמת אבטחת המידע בעירייה.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"לקוחות אגף המחשוב מפוזרים על פני העיר ת"א ועל כן אין דרך אחרת להעביר את הסיסמאות זולת הטלפון."**.

107. מהביקורת עולה כי ישנם מספר רב של עובדים המחזיקים ברשותם הרשאות שלא על פי צרכיהם כגון: עובדי מחלקת DBA, מחלקת תמיכה טלפונית ועוד כפי שפורט בפרק ג'.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"באגף המחושב מתבצעת עבודה של הורדת כמות המשתמשים בעלי הרשאות מנהלי רשת למינמום האפשרי על בסיס תוכנית שהכין מנהל אבטחת מידע ואושרה במטה האגף. סיום הפעילות יהיה עד תום 2007. מעבר לכך ראה התייחסותנו לפרק ג'."**.

108. בעיריית תל-אביב- יפו לא מבוצעת סקירה תקופתית של אישורי הגישה למערכות המידע. כדי להגביר את הבקרה על שימושים שלא לצורך במשאבי המחשב או לחילופין במאגרי המידע הממוחשבים, יש לבצע מעת לעת סריקה של אישורי הגישה למערכות המידע או למשאבי המערכת וזאת בכדי לקבוע אם הם עדיין מתאימים.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"בהיקף הלקוחות של אגף המחשוב מצד אחד מול המשאבים לנושא אבטחת מידע והמשימות מהצד השני, נושא זה אינו ישים. אם זאת, מידי חצי שנה בודק מנהל אבטחת המידע את כל אותם בעלי הרשאות שלא עשו שימוש כלל במערכות בחצי השנה שעברה ומתחיל בתהליך לנעילתם והסרת ההרשאה. מעבר לכך, אנו במהלך של פיתוח "כלי שירות" (utility) שמבצע הצלבה בין מערכת משאבי אנוש ל-** active directory **על בסיס מספר ת.ז. בכדי לבטל עובדים שעזבו."**.

109. לעיתים נוצר מצב שבו עובד במהלך עבודתו אינו נמצא בקרבת המחשב. נקודת זמן זו, היא הזמן האידיאלי לדלות פרטים ממחשבו של העובד. במידה והעובד ערני ומודע לחשיבות אבטחת המידע, בעת עזיבתו הוא ינעל את מחשבו, אך אם העובד אינו ערני לסיכונים הקיימים הוא ישאיר את מחשבו פתוח לעיני כל. חלק לא מבוטל העובדים בעיריית תל-אביב- יפו משאירים את מחשביהם פתוחים מבלי לבצע פעולת LOG OUT.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"בכל העמדות הפועלות עם מערכת הפעלה** XP **יש נעילה אוטומטית לאחר 20 דקות של אי שימוש במחשב. במהלך 2005-2006 הוסבו כ- 90% מתחנות העבודה למערכת הפעלה** XP**, יתרת ההסבה מתבצעת עקב בצד אגודל עם הסבת מערכות המג'ק לגרסה מתקדמת ע"י חברת מלם. הסבת מערכות המג'יק תסתיים עד סוף 2008 ובהתאם לכך סיום ההסבה ל-** XP**."**

110. נקודות הגישה לרשת בעיריית תל אביב –יפו מאופשרות באופן קבוע, כך נוצר מצב שבו כל אדם המחזיק ברשותו מחשב נייד וכבל רשת יכול להתחבר לרשת המידע בעירייה.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: "נושא זה יפתר באמצעות תוכנה וחומרה הנמצאים בתהליך רכש ואמורים להיות מותקנים ומפועלים באופן מלא עד סוף הרבעון הראשון של 2007.".

111. המשתמשים המרוחקים מאומתים בצורה קפדנית ביותר, כל מידע המועבר מהמחשב המרוחק לשרת מוצפן ומאובטח ועל כן כמעט בלתי אפשרי לחדור לרשת על ידי התחזות או להאזין למידע המועבר בין השרת למשתמש. יחד עם זאת, אין מעקב אחר אופן האבטחה במחשב המרוחק. כתוצאה מכך ישנה סבירות שוירוס שנמצא על המחשב המרוחק יעבור באמצעות הקו המאובטח (VPN) ויגיע לשרתי העירייה.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"חלקם של המחשבים המרוחקים הם מחשבים עירוניים והם נבדקים ומטופלים ע"י האגף. החלק האחר של המחשבים הם מחשבים פרטיים ואין יכולת לאגף לכפות על בעלי המחשב רכישה של תוכנות הגנה והקשחה של המחשב. אם זאת, כל קישור לרשת העירונית עובר דרך שרת האנטי וירוס העירוני שמגן בפני כל וירוס ללא קשר לאופן הגעתו (מחשב בייתי או האינטרנט)."**.

פרק יב - שרידות וגיבוי מערכת המידע

112. כחלק מתהליך האבטחה יש לשמור גיבוי של המידע לפני השינויים ואחריהם, על מנת לאפשר שחזור של המידע.

113. לכן, במערכות מידע זקוקים לתוכנית חלופית על מנת להתמודד עם מצבים לא מתוכננים, כגון: אסון שהרס את מתקני אחסון המידע או במקרה שמערכת המידע נפגעת כתוצאה מווירוס או נזק לא מכוון.

114. על מנת לנהל את מערכת הגיבוי בצורה היעילה ביותר יש לבצע את הפעולות הבאות:

א. זיהוי הפעולות הקריטיות והרגישות ביותר למערכת המידע (מידע שחשוב מאוד לשמר ושקשה לשחזרו ללא מחשב);

ב. הכנת תוכנית חילופית מקיפה ומתועדת לשחזור הנתונים הקריטיים למערכת המידע;

ג. ניהול תוכנית גיבוי תקופתית ושמירת המידע בצורה מתוזמנת וקבועה.

ממצאים

115. בכדי להחליט אלו משאבים לשמור ולגבות, יש לזהות את כל הפעולות הקריטיות והרגישות ביותר המשמשות את העירייה לעבודתה. בעירייה לא זוהו כל הפעולות הקריטיות והרגישות ביותר. לפני כ – 3 שנים החלו בבניית DRP, במסגרת פרוייקט זה אמורים לזהות את כל הפעולות והמשאבים הקריטיים. חשוב לציין כי את פרוייקט ה – DRP מוביל עובד אשר אינו נמנה על עובדי יחידת אבטחת המידע בעירייה.

116. לא פותחה תוכנית חלופית מקיפה. תוכנית חלופית משמשת את העירייה בזמן אסון כלומר, לאחר קריסת המערכת או בזמן שנוצרת תקלה. התוכנית החלופית אמורה להדריך כיצד ניתן לאפשר למערכות הקריטיות בעירייה להמשיך לעבוד.

117. על מנת שהעירייה תוכל לשוב לפעילות מלאה לאחר אסון בדרך המהירה והיעילה ביותר יש להגדיר תפקידים ברורים כך שכל עובד ידע בדיוק מהו תפקידו בזמן אסון. בדרך זו יכולה

העירייה להימנע ממצב של בלבול וחוסר וודאות בזמן ההתאוששות מאסון. בעירייה לא מונו אחראים להתאוששות מאסון.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"במסגרת המבנה הארגוני החדש של אגף המחשוב מונה אחראי DRP ושו"ב כשמיקומו בענף שירות לקוחות ותפעול. ראה התייחסותנו לנושא זה בסעיף 37. במסגרת פרויקט ה- DRP, הסתיים שלב א' שכלל מיפוי המערכות והגדרת רמת הקריטיות של כל מערכת. השלב הבא (ייושם בשנת 2007) הוא מתן מענה למערכות הקריטיות ביותר."**.

118. בעירייה מבוצעים גיבויים תקופתיים, זאת בכדי לאפשר את שחזור מערכותיה בזמן אסון. מסיבה זו הגיבויים אמורים להימצא בכספות, כך שגם בזמן שריפה תוכל העירייה לבצע שחזורים. בעירייה עורכים מספר גיבויים המבוצעים על פי נוהל גיבויי פנימי. להלן פרוט הגיבויים התקופתיים הקיימים:

א. גיבויים יומיים;

ב. גיבויים שבועיים;

ג. גיבויים חודשיים;

ד. גיבויים שנתיים.

119. גיבויים יומיים הנשמרים בעירייה, אינם מאופסנים בתוך כספות חסינות אש.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"גיבויים יומיים מאוחסנים בחדר מחשב ואין העברה לחדר בטחון, קלטות שבועיות מועברות לחדר בטחון (כספת חסינת אש) פעם בשבוע בימים אלו אנו מכניסים לפעולה גיבוי באמצעות רובוט (סיום משוער – אפריל 2007) לאחר מכן, כמות הקלטות תופחת משמעותית וכל הקלטות תיכנסנה לכספות חסינות אש. מדיניות הגבוי העירוני היא כדלקמן: ביצוע גבוי יומי ושמירתו במשך 30 דורות, גבוי חודשי נשמר למשך 24 דורות וגבוי שנתי נשמר 7 דורות."**.

פרק יג - בקרות הנהלה

120. בקרות ההנהלה מתמקדות בניהול אבטחה טכנולוגיית במערכת המידע וניהול סיכוני המערכת בצורה מחזורית. בקרות אלו מאפשרות להנהלה לתכנן תוכנית אבטחה מערכתית.

121. בקרות ההנהלה כוללות בתוכן:

א. ניהול סיכונים - סיכון הינו ההסתברות שיתרחש מאורע אשר יגרום לפגיעה במערכת המידע. ניהול הסיכונים הוא תהליך של הערכת הסיכונים, נקיטת צעדים על מנת להוריד

את הסיכון למידה סבירה ושמירה על רמה סיכון נמוכה. להלן השלבים לעריכת ניהול הסיכונים:

1) מדידת הסיכון באופן מחזורי;

2) הכנת רשימה של ליקויים וחולשות של המערכת;

3) החלטה על מידת הסיכון ואישורו על ידי ההנהלה.

ב. סקירת בקרות אבטחה - הערכות שגרתיות ותגובות לנקודות חולשה שזוהו הינם אלמנטים חשובים בזיהוי סיכוני המערכת. על מנת לבדוק את מידת הקריטיות של אלמנטים שונים נבחנים ההיבטים הבאים:

1) סקירת בקרות האבטחה של המערכת ומערכות מקושרות לה;

2) בקרת ההנהלה על קיום הפעולות המתקנות.

ג. מחזור חיים - על מנת לנהל את מערך האבטחה בצורה הטובה ביותר יש לבדוק את תכנונו לכל אורך מחזור החיים של המערכת. מחזור החיים של המערכת כולל 5 שלבים בסיסיים: החלטה, פיתוח/רכישה, יישום/תחזוקה, הפעלה, הפסקת עבודה.

ד. מחזור קליטת מערכת חדשה או שינוי מהותי במערכת קיימת יכלול בין היתר את השלבים הבאים:

1) אפיון המערכת: אפיון פרמטרים של אבטחת מידע, כגון סיסמאות, הרשאות, הצפנות, נפח וטיפול בזיכרון וכדומה;

2) בניית המערכת: מימוש דרישות אבטחת המידע המופיעות באפיון המערכת;

3) בדיקת המערכת: בדיקות במהלך הפיתוח ובדיקות קבלה בהיבטי אבטחת מידע;

4) קליטת המערכת: קבלה והתקנה מאובטחת ומאושרת של המערכת על ידי הגורמים המוסמכים לכך בעירייה, תוך שילוב אנשי אבטחת המידע בעת ההתקנה;

5) שינויים במערכת: יש לקחת בחשבון שיקולי אבטחת מידע בעת כל שינוי הנעשה במערכת ולהעביר שינוי זה למנהל אבטחת המידע;

ה. עיבוד מורשה (אישור וייפוי כוח) - עיבוד מורשה מהווה באופן מסוים מעין ביטוח לגבי רמת האבטחה של המערכת. אי לכך, יש צורך בכתב אמנה המאפשר לכל אפליקציה לפעול בתוך המערכת. על מנת לבצע ייפוי כוח בצורה נכונה יש להכין את המסמכים הבאים:

1) כל מערכת מחויבת באישור על ידי כתב אמנה;

2) המערכת צריכה לפעול בהתאם לנהלים ספציפיים של החברה.

ממצאים

122. בשנים האחרונות לא נערך סקר סיכונים בעירייה. בעבר הייתה דרישה לסקר, התקבלה הצעת מחיר אך לא אושר התקציב הנדרש.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"עלות ביצוע סקר סיכונים מוערכת בכ- 150 אלף ₪. אין טעם בביצוע סקר שכזה (שאורך כחצי שנה) ללא הקצאה מראש של תקציב למימוש המלצות הסקר, לפחות בחלקן. הערכה שלנו שהתקציב שיידרש לשלב הראשון של יישום ההמלצות הוא אותו סדר גודל של תקציב."**.

123. יש סיווג של רגישות מערכות המידע בעירייה, אך אין רישום מסודר של המערכות. כמו כן, אין התייחסות שונה לכל מערכת בהתאם לסיווגה, כל מערכת מקבלת התייחסות שווה ממחלקת אבטחת מידע.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"במסגרת סיום שלב א' של ה-DRP הוכנה טבלה של רגישות כל מערכות המידע בעיריה. טבלה זאת תאפשר התייחסות מתאימה לכל מערכת בהתאם לסיווגה ע"י אבטחת מידע."**.

124. מתבצע איתור של האיומים אליהם חשופות מערכות המידע, אך אין התייחסות לסיכון שטמון בכל איום ואיום.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"בהמשך לביצוע איתור האיומים קיימת התייחסות לכל איום."**.

125. בקרות האבטחה הקיימות אינן נבדקות מידי תקופה. עקב כך נוצר מצב שבו הבקרות לא עונות על הדרישות ומגלות זאת בזמן היווצרות הבעיה.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"לא ברורה לנו כוונת הסעיף. אם זאת מנהל אבטחת המידע מבצע פעולות באופן שוטף כדוגמה: ניסיון פריצה מבחוץ מידי תקופה, הפעלת תוכנות לזיהוי נקודות חולשה, הפעלת תוכנה לאיתור פרצות במסד נתונים, וכדומה."**.

הביקורת אימתה את תגובת אגף המיחשוב וממצאיה מעלים כי בוצע נסיון פריצה אחד ייזום, מחוץ לעירייה, על ידי מנהל אבטחת מידע. לגבי נסיונות פריצה מתוך העירייה, לא בוצעו נסיונות פריצה כלל וכלל וזאת לאור מצבה העגום של העירייה בנושא. לאחר נסיון הפריצה שביצעה הביקורת הוחלט באגף לרכוש תוכנה לזיהוי נקודות חולשה ואיתור פרצות במסדי הנתונים. תוכנה זו טרם נכנסה לשימוש.

126. לא קיימת רשימה מסודרת של פעולות מתקנות שיש לבצע על מנת להקטין סיכון ספציפי. כמו כן, לא ידוע בכמה אחוזים יקטן הסיכון בעקבות הפעולה המתקנת.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"חלק ניכר מעבודתו השוטפת של מנהל אבטחת מידע הינו זיהוי ואיתור סיכונים פוטנציאליים. מול כל סיכון שכזה מנהל אבטחת מידע, במסגרת המשאבים העומדים לרשותו מכין פעולות מתקנות. מנהל אבטחת מידע יכין רשימה של סיכונים צפויים ופעולות מתקנות עד סוף הרבעון הראשון של 2007."**.

127. לא פותחה מתודולוגיית התפתחות מחזור חיים למערכות הפועלות בעירייה.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"אגף המחשוב אימץ את נוהל מפת"ח (נוהל ממשלתי) לניהול מחזור החיים וכל המערכות החדשות מפותחות על בסיס הנוהל.."**

מברור שערכה הביקורת עם מנהל אבטחת מידע, לאחר קבלת תגובת אגף מחשוב לדוח, עולה כי עובדי אבטחת מידע מודעים לכך שאגף המחשוב אימץ נוהל מפת"ח, אך נוהל זה לא הגיע לידיהם והם אינם מודעים למשמעויות והשלכות הנוהל לגבי עבודתם השוטפת.

128. לאנשי יחידת אבטחת מידע בעיריית תל-אביב-יפו ידועה רמת הסיווג (סודי ביותר, סודי, שמור וכדומה) של כל מידע המצוי במערכות השונות. למרות זאת, לא קיים מסמך כלשהו המתעד את סיווג המידע ודרכי הטיפול בו.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"מנהל אבטחת מידע יוסיף את רמת הסיווג לכל מערכת על גבי טבלת המערכות שהוכנה במסגרת פרויקט ה- DRP עד לסוף הרבעון הראשון של 2007."**.

פרק יד - בקרת חומרה ותוכנה

129. מערכת האבטחה של העירייה לא צריכה להסתמך על ההנחה שכל תוכנה או חומרה מנוטרלות מבאגים, לכן על מנהלי הרשת לדעת בדיוק על איזה תוכנה ואיזו חומרה הם יכולים לסמוך.

130. בקרות אלו משמשות כדי לפקח על התקנתם ועדכונם של רכיבי חומרה ותוכנה, על מנת להבטיח שהמערכת תפעל כפי שמצופה ממנה, ולא תגרם לה פגיעה בעקבות עדכונים אלו.

131. על מנת לפקח על בקרה זו יש לבצע מספר פעולות:

א. הגבלת הגישה הפיזית לחומרה ולתוכנות המערכת;

ב. בדיקתה ואישורה של כל חומרה ותוכנה חדשה לפני הכנסתה למעגל המערכת, כמו גם בדיקתו של כל עדכון לפני ביצועו;

ג. בדיקה האם מערכות האבטחה מצליחות להקטין את הפגיעות במערכת המידע.

ממצאים

132. בכדי להבטיח באופן מרבי כי מידע מהעירייה לא יזלוג מחוצה לה, יש לשמור על חומרת העירייה. כידוע, דיסקים קשיחים, זיכרונות למיניהם ומחשבים ניידים עלולים לטמון בחובם מידע רב, על כן יש לשומרם. בעירייה לא קיים נוהל אחזקת מחשבים ניידים, ליווי אנשי מקצוע וכדומה, בכל הנוגע להיבטי אבטחת המידע.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"קיים נוהל ליווי אנשי מקצוע. מנהל אבטחת מידע יכין נוהל אבטחת מחשבים ניידים כחלק מאוסף הנהלים הכולל."**.

133. תוכנות העושות שימוש במשאבי המערכת בעירייה, מקבלות הרשאות פעולה בעירייה וזאת על מנת למלא את יעודן. קודם למתן ההרשאות יש לבצע מספר בדיקות:

א. במקרה שמדובר בתוכנה, יש לבדוק לאלו מאגרי מידע צריכה התוכנה להיות נגישה ומהי רמת אבטחת המידע בתוכנה;

ב. במקרה שמדובר בחומרה, יש לבצע בדיקת תאימות למערכות העירייה.

מהביקורת עולה כי ישנן תוכנות וחומרות חדשות אשר אינן נבדקות ומאושרות על ידי יחידת אבטחת מידע, בטרם מבצעים בהם שימוש, כגון תוכנת הגביה, שהוזכרה בתחילת הדוח, החושפת מידע רגיש אודות כרטיסי האשראי המופיעים במערכת המידע.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"אישור אבטחת מידע הוא חלק מובנה מתהליך פיתוח ורכש מערכות. אין הכנסה של תוכנה או חומרה חדשה ללא אישור ומעורבות בתהליך באותם מקרים שאישור זה נדרש. לגבי תוכנת הגביה בבדיקה שבוצעה כחלק מתהליך העבודה השגרתי ע"י אבטחת מידע התגלו בעיות בתחום האבטחה בניגוד להנחיות שהתקבלו מאבטחת מידע, ובעקבות כך המערכת לא עלתה לאוויר עד לתיקון התקלות לשביעות רצונו של מנהל אבטחת מידע."**.

הביקורת מציינת בתגובה להנהלת אגף המחשוב כי משיחה שנערכה עם מנהל יחידת אבטחת מידע עולה כי הוא אינו מעורב באישור הכנסת תוכנה ו/או חומרה חדשה לעירייה. למרות קיומו של טופס אישור של אבטחת מידע בנושא, אין באפשרות אבטחת מידע לטפל בנושא לעומק, מאחר ואין באפשרותם להקצות כח אדם היכול להתפנות לטיפול בנושא. במצב הקיים הנושא אינו מטופל.

134. ככל שמשתכללות טכנולוגיות אבטחת המידע כך משתכללים האיומים על מאגרי המידע. חברות התוכנה מפיצות עדכוני תוכנה שוטפים על מנת ליעל את עבודת התוכנה ובכדי להגביר את רמת אבטחת המידע. בעירייה לא קיימת בקרת גרסאות ועדכוני תוכנה שוטפים.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"אנו נמצאים לקראת סוף בדיקת היתכנות (פיילוט) של מוצר WSUS של מיקרוסופט להפצה אוטומטית של עדכוני גרסה. בתום בדיקת ההיתכנות יחוברו כל עמדות המחשב בעירייה למערכת."**.

135. התוכנות לא רשומות ברשימת המצאי באופן מסודר.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"כל תחנות העבודה עליהן פועלת מערכת ההפעלה XP ומחוברות לרשת העירונית מחוברים למערכת SMS של מיקרוסופט הכוללת בין השאר ניהול מצאי תוכנה של מוצרי מדף. לכל המערכות העירוניות קיימת רשימה כולל הרשאות גישה של הלקוחות לכל מערכת ומערכת."**.

בנוסף לכך, מסרה הנהלת אגף המחשוב לביקורת כי: **"רשימת המערכות מופתה במסגרת שלב א' של ה-** DRP."**.**

פרק טו - שלמות המידע

136. בקרות שלמות המידע משמשות להגנת המידע משינוי או מחיקה במקרה או בזדון. בנוסף, הבקרה מספקת למשתמש את הביטחון כי המידע עומד בציפיות בכל הנוגע לאיכותו ושלמותו.

137. על מנת להבטיח את שלמות המידע יש לבצע את הפעולות הבאות:

א. התקנת תוכנת אנטי-וירוס ועדכונה מעת לעת;

ב. התקנת תוכנת בקרה לצורך בדיקת שלמות המידע ותקינותו.

ממצאים

138. כיום, רשת האינטרנט היא חלק אינטגראלי ובלתי נפרד מהעירייה. למרות יתרונותיה הרבים של רשת האינטרנט ישנם מאות איומים חדשים המופיעים מידי חודש ומופצים דרך רשת האינטרנט, על כן יש לעדכן את תוכנת האנטי וירוס באופן שוטף. בעירייה פועלים, בין השאר, מחשבים בעלי WIN 98 בהם לא מעודכן באופן שוטף קובץ חסימת הוירוסים ולכן רמת הסיכון לחדירת וירוס למערכת, דרך מחשבים אלו, גדל.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"ממועד הפגישות להכנת הדוח בוצעה סקירה מקיפה ונכון להיום תוכנת האנטי וירוס מעודכנת באופן מקסימאלי. אגף המחשוב התחיל לאחרונה בתהליך רכש של תוכנה שאינה מאפשרת התחברות לרשת העירונית למחשב שאינו מכיל אנטי וירוס מעודכן. תוכנה זו תותקן ברשת העירונית עד אמצע 2007 (עקב הצורך להטמיע אופציה זו בכל הרשת העירונית)."**.

139. סריקה תקופתית של הרשת מפני וירוסים יכולה להתריע בפני וירוסים או חשדות לוירוסים גם אם תוכנת האנטי וירוס אינה מעודכנת. סריקת וירוסים מבוצעת בשרתים באופן שוטף אך סריקת וירוסים תקופתית אינה מבוצעת במחשבי המשתמשים.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"לא מבוצעת סריקה יומית בתחנות. ניתן להכניס סריקה שבועית שתתבצע במהלך סופשבוע. אם המחשב כבוי הסריקה תתבצע בהדלקת המחשב. ההשלכות התפעוליות ברורות."**.

140. בכדי לבדוק אם רשומות הושחתו, נמחקו או שונו יש ליישם בקרות לבדיקת שלמות ותקינות המידע. בעירייה לא מיושמות בקרות תקינות ושלמות מידע.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"בסביבת הפיתוח העדכנית של אגף המחשוב (דוט נט ו- SAP) קיימת תשתית טכנולוגית ומחוייבות של כל פרויקט ליישם בקרת תקינות ושלמות המידע. במסגרת נהלי האיכות המיושמים באגף ינתן דגש מחודש לנושא. לגבי מערכות שפותחו בעבר, אכן לא קיים מנגנון שכזה."**.

פרק טז - תיעוד ורישום נהלים

141. מערכת המידע של העירייה הינה מערכת מסועפת ורבת תחומים. מפעילי מערכת האבטחה צריכים להיות מעורים בכל חלקיה ולדעת את נהליה על בוריים.

142. כידוע, עירייה אינה מנוהלת באופן קבוע וסטאטי וישנם שינויים רבים במצבת כוח האדם שלה.

143. כל עובד העוזב את יחידת אבטחת המידע עלול להותיר חלל ריק ולקחת עימו ידע מקצועי ומידע שצבר בהקשר לפעילויות ולתהליכי עבודה שונים מבלי שהונחל לעובדים אחרים. בכדי למלא חלל זה יצטרכו עובדי היחידה שימלאו את מקומו, לשחזר תהליכים ושיטות עבודה ולהגיע בסופו של דבר לרמת התפעול הנדרשת. מניעת אובדן מידע וידע נצבר הינו המניע הראשוני לתיעוד תהליכים תפעוליים ביחידת אבטחת המידע ובכל יחידה ארגונית אחרת.

144. תיעוד נכון פירושו סדר ושיטתיות בביצוע, כך שפרטים אינם הולכים לאיבוד וניתן לבצע בקרת תהליכים נאותה.

145. התיעוד מכיל תיאור של החומרה, תוכנה, נהלים סטנדרטיים, פרוצדורות ואישורים הקשורים למערכת אשר נותנים תוקף לבקרות מערכת האבטחה.

ממצאים

146. לא קיים תיעוד יצרן – ספק לתוכנות שנרכשו;

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"לחלק ניכר מהתוכנות הנרכשות ע"י העירייה אין תיעוד מודפס וכל המידע זמין ונגיש באמצעות רשת האינטרנט. בנוהל הכנסת תוכנה חיצונית יתווסף סעיף המחייב את היצרן לספק תיעוד הרלוונטי (באינטרנט, מדיה מגנית או ספרות פיזית)."**.

147. קיימים מספר מדריכי משתמש אך העובדים אינם מודעים לקיומם;

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"לכל פרטי החומרה הנרכשת ע"י העירייה קיים תיעוד ברשת האינטרנט ו/או מסופק עם החומרה.מנהלי הפרויקטים הרלוונטיים ירעננו אצל לקוחותיהם את המידע בדבר קיום מדריכי משתמש."**.

148. לא קיימת תוכנית אבטחה מערכתית;

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"לא ברורה כוונת הביקורת. להערכתנו מסמך מדיניות אבטחה שהוזכר בתחילת ההתייחסות מהווה תוכנית אבטחה מערכתית."**.

149. אין נוהל גיבוי רשום ומתועד;

התייחסות אגף המחשוב: **"ראה התייחסותנו לסעיף 24."**.

150. אין נוהל מוכן לשעת חירום למקרה של קריסת המערכות.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"נוהל כזה יוכן בשלבים הבאים של פרויקט ה- DRP."**.

פרק יז - ערנות, הכשרה וחינוך לאבטחה

151. כל משתמש ברשת המחשבים לוקח חלק ממערך אבטחת המידע, על כן, על כל משתמשי המחשבים בעירייה לגלות ערנות בכל הקשור לאבטחת מידע. במידה והמשתמשים מבינים את חשיבות תפקידים בנושא אבטחת מידע והסיבות לאמצעי האבטחה הנקטים בעירייה, ניתן יהיה להיעזר בהם לצורך מניעת ניסיונות פריצה למערכת המידע.

152. עובדים המשאירים מחשב פתוח, כאשר הם עוזבים את חדרם לא נעול, משאירים פרצה באבטחת המידע. במצב זה יכול גורם זר לחדור ולהשתמש ב- OUTLOOK, אפליקציות וכל תוכנה אחרת שפתוחה על המסך.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"נושא זה קיבל התייחסות ופתרון בתשובתנו לסעיף 105. סיסמה הכשרה וחינוך מגבירים את האבטחה, על ידי הגברת הערנות**

להגן על משאבי המערכת. בנוסף, ההכשרה מפתחת מיומנויות וידע על מנת שהמשתמשים יוכלו לבצע את עבודתם בצורה יותר מאובטחת."

ממצאים

153. בעירייה לא מבוצעות הדרכות המתמקדות אך ורק בנושא אבטחת המידע.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"מנהל אבטחת מידע יפנה לד"ר ר ג לצורך מחשבה משותפת לבניית קורס עירוני ייעודי בנושא אבטחת מידע."**.

154. מנהל אבטחת מידע מצטרף להדרכות הנערכות בנושאים שונים, ובסוף כל הדרכה הוא מציג לעובדי העירייה את נושא אבטחת המידע.

155. ההדרכות המבוצעות אינן מתועדות ומבוקרות, דבר המקשה על ביצוע הדרכות בצורה יעילה ומקיפה של כלל העובדים.

156. בכדי להבטיח כי כל עובדי העירייה עברו הדרכות ומודעים לסיכונים הגלומים באבטחת המידע, יש לחייב אותם להגיע להדרכות. בפועל העובדים אינם מחוייבים להשתתף בהדרכות.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"מנהל אבטחת מידע יפנה לאגף משאבי אנוש ויציע להם לערוך אחת לחודש כנס קצר של כל העובדים החדשים שנתקבלו לעירייה בחודש שעבר לצורך הסבר על אבטחת מידע (מפגש זה יכול להוות פלטפורמה להעברת מסרים נוספים לאותה אוכלוסיה)."**.

פרק יח - אבטחה אנושית

157. מערכות המידע נועדו לשרת משתמשים רבים. בכדי לשמור על המידע המצוי במערכות השונות, יש לבצע מספר פעולות על מנת לנטרל כל בסיס לזליגת מידע מחוץ לעירייה על ידי גורם פנים ארגוני. להלן הפעולות שיש לבצע:

א. הפרדת סמכויות על מנת להבטיח אחריות אישית של כל משתמש ומשתמש. יש לתחם את הסמכויות הניתנות לכל משתמש, בכדי למנוע ריבוי סמכויות בידי משתמש יחיד;

ב. הענקת סמכויות והרשאות רבות מידי למשתמש יחיד עלולה לגרום לכך שבמידה ואותו משתמש יבצע פעולות לא מורשות, תהיה זו משימה מורכבת מאוד לאתר את אותן פעולות;

ג. ביצוע בדיקת רקע מקיפה על מנת לאפשר סינון ממוקד של מועמדים, טרם קבלתם לעבודה.

ממצאים

158. לא קיימת הפרדת סמכויות על מנת להבטיח אחריות אישית לכל עובד ועובד;

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"סמכויות של עובדי העירייה נקבעות בהתאם להגדרת התפקיד אותו הם ממלאים. אגף המחשוב מאפשר הרשאות במערכות המידע אך ורק בהתאם להגדרות תפקיד אלו."**.

159. ידוע על רמת הרגישות של תפקידים ומשרות מסויימות, אך לא קיימת סקירה מסודרת אשר תקבע את רמת הרגישות ודרך ההתייחסות לאותה משרה או תפקיד;

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"האחריות על מתן ההרשאות הינה של מנהלי המאגרים. אם זאת, בעת ביצוע ההרשאות שנתבקשו ע"י מנהל המאגר, אבטחת מידע בודקת את סבירות הבקשות. במידה ונראה לה כי התבקשה רמת הרשאה שאינה תואמת את רמת רגישות התפקיד, לא מתבעת מתן ההרשאה אלא לאחר בירור עם מנהל המאגר."**.

160. באופן כללי ידועות ליחידת אבטחת המידע מהן ההרשאות להן זקוק כל משתמש, על מנת לבצע את תפקידו. למרות זאת לא קיים מסמך המפרט את דרישות העבודה בכל משרה ומשרה;

161. לא מבוצעת בדיקת רקע למועמדים טרם קבלת ההרשאות למערכת המידע;

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"מנהל אבטחת מידע יקבע פגישה עם מנהל אגף משאבי אנוש לצורך מחשבה משותפת על נושא זה."**.

162. לא קיים מנגנון יציאת עובדים לחופשות מאולצות ורוטציית תפקידים.

התייחסות אגף המחשוב: **"כנ"ל."**.

פרק יט - בקרות ייצור קלט/פלט

163. קיימים אספקטים רבים לתמיכה בפעולות ה- IT. טווח הנושאים רחב וכולל עזרה למשתמשי קצה לנוהל אחסון וטיפול בהשמדת מידע. במערכות המידע של העירייה קיים מידע רב המועבר באופן יום יומי להתקנים חיצוניים, כגון: דיסקים, DISK ON KEY ופלטי מדפסת. מטרתה של מערכת אבטחת המידע היא למנוע העברת נתונים רגישים מחוץ לגבולות העירייה ללא אישור מתאים.

ממצאים

164. לא קיימת בקרה המבטיחה כי אנשים לא מורשים, לא יוכלו להוציא מידע באמצעות התקן חיצוני (צורב, מחשב נייד או DISK ON KEY);

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"אגף המחשוב נמצא בתהליך בחינה של מערכת העונה לדרישות הנ"ל (אוניגמה). המערכת מאפשרת חסימה של התקנים**

ומשאבי מחשב (עד רמת printscreen) עפ"י סיווג החומר, מיקומו, מילות מפתח, ועוד, בכוונה לרכוש מוצר שכזה בשנת 2007.".

165. לא קיימות בקרות המונעות שליחת נתונים רגישים להדפסה;

התייחסות אגף המחשוב: **"כנ"ל.".**

166. על מנת לטפל בכל מידע בצורה הראויה לו יש לבצע תיוג של המידע לפי רמת רגישותו ובהתאם לכך לטפל בו. בעירייה קיים תיוג חלקי בלבד של רגישות המידע;

התייחסות אגף המחשוב: **"כנ"ל.".**

167. בכדי לוודא שמדיה שצריכה לעבור מעובד אחד למשנהו, אינה מועברת עם מידע, יש לבצע חיטוי למדיה טרם העברתה. ביצוע חיטוי למדיה שאמור להיעשות בה שימוש חוזר אינו באחריות יחידת אבטחת מידע, כמו גם הבקרה על ביצוע החיטוי;

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"נושא זה אינו מקבל ביטוי כיום בעירייה כלל. להערכתנו חיוב כל עובדי העירייה לבצע חיטוי למדיה טרם העברתה אינו בבחינת גזירה שהציבור יכול לעמוד בה. אם זאת, אבטחת מידע נוקטת במגוון כלים ומתודולוגיות למנוע את התוצאות היכולות לנבוע מאי חיטוי שכזה כפי שבא לידי ביטוי בהתייחסותנו לסעיפי הדוח (אנטי וירוס, מניעת התקנות ב- GPO, וכו').".**

168. בעירייה, המדיה הפגומה לא תמיד מועברת להשמדה ביחידת אבטחת מידע ולכן אין אפשרות לפקח על תהליך זה.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"ירוענן נוהל השמדת מדיה מגנטית כולל הפצתו במסגרת כלל נהלי אבטחת מידע.".**

פרק כ - בקרה על איומי רשת

169. רשת ה- TCP/IP הגדולה בעולם, האינטרנט, מאפשרת כיום לחבר אינספור רשתות מחשב מקומיות זו לזו. בכך נוצרת קישוריות גלובלית בין מחשבים. ואולם, לקישוריות זו יש מחיר: חיבורה של הרשת המקומית אל האינטרנט חושף אותה גם לסכנה של פגיעה מצד גורמים עויינים ברשת.

170. האינטרנט יצר אתגר אלקטרוני לגנבים שתרים אחר דלתות וירטואליות פתוחות. מנהלי המאגרים נדרשים להבין את האיומים העומדים בפניהם, מידת הסיכון והמחיר שעלולים האיומים לגבות. כמו כן, על מנהלי מאגרי המידע להחליט באילו פעולות עליהם לנקוט על מנת להקטין ככל הניתן את רמת הסיכון לדליפה, זמינות או שינוי מידע השמור על המדיות המגנטיות של הארגונים.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"מנהל אבטחת מידע יזום פעילות במהלך המחצית הראשונה של 2007 לסייע למנהלי מאגרי המידע בעזרת אינפורמציה וידע לגבי פעולות המוזכרות בסעיף. בנוסף במסגרת הפגישות עם ד"ר ר ג יעלה מנהל אבטחת מידע את הרעיון להכנת סדנה/השתלמות ייעודית למנהלי המאגרים."**.

171. ניתן לחלק את הסכנות האורבות למידע באינטרנט לשתי קבוצות עיקריות:

א. תקיפה של הרשת המקומית - סכנות לרשת המקומית. הארכיטקטורה הפתוחה שבבסיס פרוטוקול ה-TCP/IP עלולה לאפשר גם לגורמים לא רצויים להתחבר אל הרשת המקומית ולגרום נזק לא מבוטל. הדוגמה הנפוצה מכולן למידע לא רצוי המוצא את דרכו למחשבים הוא וירוס המחשב, העשוי לגרום לנזקים ניכרים, הן למידע המאוחסן על מחשבי הרשת והן לשרתים השונים בהם משתמשים המחשבים;

ב. פגיעה בפרטיות - כפועל יוצא מאופיין המבוזר של רשתות TCP/IP ובמיוחד לאור מבנה רשת האינטרנט, חבילות הנשלחות ממחשב אל מחשב עשויות לעבור דרך מספר גדול של תחנות ביניים עד שיגיעו ליעדן. לצד הגמישות הגדולה שמקנה מבנה הרשת, מצב זה גם טומן בחובו סכנה. המידע אותו שולח המשתמש עשוי ליפול בדרכו אל הידיים הלא נכונות, בדרכים שונות.

172. על מנת למנוע איומים מסוג זה, יש לבצע מספר פעולות:

א. הקמת מערך הגנה בפני התקפות פאסיביות ואקטיביות;

ב. הקמת FIREWALL;

ג. קידוד (חתימות אלקטרוניות);

ד. התקנת תוכנת אנטי-וירוס ועדכונה באופן שוטף.

ממצאים

173. תוכנת האנטי וירוס אינה מתעדכנת באופן שוטף;

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"ראה התייחסותנו לסעיף 138."**.

174. אין וודאות מלאה שבכל המחשבים פועלת תוכנת האנטיוירוס;

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"ראה התייחסותנו לסעיף 139."**.

175. נושא החתימות האלקטרוניות נמצא, נכון למועד עריכת הביקורת, בשלב הפיילוט;

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"בוצע פיילוט לשימוש בכרטיס עובד חכם לצורך הזדהות וחתימה דיגיטאלית. עד כה הופצו חמישים כרטיסים לצורך בדיקת**

ההיתכנות. הפיילוט הסתיים בהצלחה. המשך הפרויקט והרחבתו לשאר עובדי העירייה אינו מתוקצב.".

התייחסות אגף המחשוב: **"ראה התייחסותנו לסעיף 139."**.

פרק כא - מעקב ביקורת

176. מעקב ביקורת יכול לספק אחריות אישית, אמצעי לשחזור אירוע, זיהוי חדירות וזיהוי בעיות. על מנת לבצע את המעקב יש לבצע רישום של כל פעילות המעורבת בגישה ושינוי של קבצים רגישים או קריטיים וחקירת פעילות זו.

ממצאים

177. לא קיימת הפרדת סמכויות בין עובדי יחידת אבטחת המידע האחראי על בקרת הגישה לרשת לבין העובד האחראי על מעקב הביקורת. במצב זה יכול עובד יחידת אבטחת המידע לבצע פעילות אסורה ו/או שגויה ולאחר מכן לבקר את פעולותיו;

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"בשל היקף כוח האדם באבטחת מידע והפעילות הנדרשת, לא מצאנו לנכון לבצע הפרדה שכזאת."**.

178. על מנת לבדוק אירועי אבטחת מידע שהתרחשו בעבר יש לבדוק רישומי יומן היסטוריים ולנתחם. רישומי היומן אינם נשמרים לאורך תקופת זמן ממושכת;

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"קיימת פעילות באגף שמטרתה לקבוע מדיניות למשך זמן שמירת סוגי מידע שונים. אנו נצרף סוג מידע זה (רישומי יומן היסטוריים) לעבודה זאת. עבודה זאת צפויה להסתיים במהלך מחצית 2007. ברשות העירייה קיים מוצר (MOM) המטפל באופן חלקי בנושא המעקב אחר שינויים לפי סוג השנוי ומעביר הודעות לבעלי תפקידים שונים באגף. כמו כן, במהלך 2007 תוכנס לשימוש מערכת יוניסנטר (המכרז נמצא בחתימות לקראת פרסום) שתאפשר בין השאר ריכוז מידע מכל מרכיזי הרשת והשרתים."**.

179. לדברי מנהל יחידת אבטחת מידע אין רישום מלא ושיטתי ביומן אירועים (קובץ LOG) של שינויים במידע רגיש במאגר הנתונים ולכן לא מתבצע מעקב מסודר אחר השינויים. בנוסף, אין אפשרות לאתר מי ביצע את השינויים במקרה של פגיעה או שינוי של נתונים במאגרי המידע.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: "בסביבות הפיתוח העדכניות של האגף (דוט נט ו- SAP) קיים פתרון מובנה לנושא. במערכות הישנות נושא זה אינו מיושם.".

פרק כב - בדיקות שטח של הביקורת

בבדיקות שנערכו במהלך הביקורת בעיריה, בתחומי אבטחת המידע השונים, עלו הממצאים הבאים:

180. חוסר מודעות וערנות לאבטחת מידע

א. ביום 18 ביולי, 2006 בשעה 12 בצהרים הגיע צוות הביקורת לקומת המרתף שבבניין העירייה, ללא תאום מראש עם גורם כלשהו, בניסיון לחדור לחדר השרתים המרכזי. צוות הביקורת נכנס לחדר מס"ב, מבלי להזדהות. לאחר שצוות הביקורת הציג עצמו כעובדים מטעם מבקרת העירייה, עובדי המס"ב הפנו את חברי הצוות, מבלי לאמת כי אנשי הצוות הינם עובדי הביקורת, לחדר השרתים המרכזי. יש לציין כי באותה העת לא נמצאו בחדר השרתים עובדים. צוות הביקורת איתר בחדר השרתים את כל קלטות הגיבויים היומיים והשבועיים של הבניין המרכזי בעיריית תל אביב - יפו. ראוי להדגיש כי מתוך קלטות אלו ניתן לדלות כל מידע המשמש ונמצא במאגרי המידע של העירייה, כגון: פרטים כספיים, פרטים בנוגע למכרזים, פרטי אישיים על התושבים וכדומה. כמו כן, יש לציין כי באפשרות אנשי הביקורת היה לגרום לנזק בלתי הפיך, מבלי שגורם כלשהו יפקח ויבדוק את מעשיהם.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"עובדי המס"פ והמפעילים קיבלו הנחיות ברורות וחד משמעיות כי אין להכניס לחדר השרתים המרכזי אנשים שאינם מזוהים באופן מיידי. כמו כן, ראה התייחסותנו לסעיף 87 ו- 84."**.

ב. הביקורת הצליחה לדלות מאחראי הגיבויים מידע לגבי כל סוג גיבוי: היכן הוא מאוחסן, מתי הוא מועבר ומהי פרוצדורת השחזור. בנוסף, צוות הביקורת זכה לסיור קצר ומודרך בחוות השרתים, על ידי אחד העובדים, וזאת מבלי שהאחרון יאמת הפרטים ומטרת הביקור של חברי צוות הביקורת.

התייחסות אגף המחשוב: **"כנ"ל."**.

181. אבטחה פיזית

א. לכל אחד מעובדי מחלקת המס"ב ישנה גישה חופשית לחדר השרתים והגיבויים. משמעות הדבר היא שלעובדים שעל פי הגדרת תפקידם אינם זקוקים לגישה לחדר השרתים, קיימת האפשרות להכנס לחדר השרתים והגיבויים ולדלות מידע ממנו, באין מפריע.

ב. מבדיקה שערכה הביקורת עולה כי צוות ניקיון אחראי על ניקיון חדר השרתים והגיבויים. ככל שליותר גורמים קיימת גישת הכניסה לאזורים רגישים, כך מצטמצמת האפשרות לבקר את הכניסה לאזורים אלו ולהתחקות אחר גורמים עוינים שחדרו לאזורים אלו.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"ראה התייחסותנו בסעיף 84, 85, 87."**

ג. משהייה של מספר דקות הצליחה הביקורת לדלות את הקוד של דלת הכניסה של חדר השרתים. יש לציין שכל אדם העובר במסדרונות העירייה יכול לראות את הקוד לדלת הכניסה ללא מאמץ רב (הקודן מופנה כלפי העוברים והשבים ללא כיסויי המונע הסתכלות על הקוד בזמן ההקשה).

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"ראה התייחסותנו בסעיף 87."**

182. אבטחה לוגית

א. משיחה שערכה הביקורת עם מנהל צוות המס"ב, עולה כי על מנת לקבל סיסמת גישה לרשת או ל MAIN FRAME יש להצטייד בשם פרטי ומשפחה של אחד מעובדי העירייה. באמצעות פרטים אלו ניתן לקבל סיסמה חדשה לרשת או למחשב המרכזי. באמצעות קבלת סיסמת רשת של משתמש מוגדר מקבל הפורץ את אותן הגדרות שניתנו על ידי מנהל הרשת לאותו משתמש, בנוסף יקבל הפורץ כרטיס כניסה לכל מאגרי המידע שאליהם היה רשאי אותו משתמש להכנס.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"ראה התייחסותנו בסעיף 101."**

ב. ביום 20 ביולי, 2006, התחזה צוות הביקורת למר ד ח, סגן מבקר העירייה, והתקשר למס"ב, על מנת לקבל סיסמת כניסה למערכת. ללא שום קושי מיוחד וללא מסירת פרטים מלבד שם פרטי, שם משפחה ופרטי המחשב ממנו אנו רוצים להתחבר, הצליח צוות הביקורת לקבל סיסמה ולהיכנס למערכת.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"ראה התייחסותנו בסעיף 26."**

183. אבטחה אנושית

א. משיחות שערכה הביקורת עם אנשי מחלקת DBA, עולה כי על מנת לעבוד בצורה יותר מהירה משתמשים אנשי מחלקת DBA בסיסמת מנהל רשת (הסיסמה ידועה לכל אנשי הצוות) כל אחד לפי צרכיו.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"ראה התייחסותנו בסעיף 25."**

ב. מבדיקות ומשיחות שערכה הביקורת, עלה כי בפני אנשי מחלקת המס"ב עומדת היכולת לעדכן הרשאות ברשת למרות שעל מנת למלא את תפקידם אין הם זקוקים להרשאה זו. הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"ראה התייחסותנו בסעיף 26."**.

ג. בפני כל משתמש המחזיק בהרשאת מנהל רשת ישנה האפשרות לחסום משתמשים (גם את העובד המוגדר כמנהל רשת), ליצור הרשאות, למחוק משתמשים, לשתף מידע, לצפות בכל מידע שיחפוץ ולשנות כל מידע שמצוי על השרתים.

ד. מבדיקה שערכה הביקורת עולה כי באמצעות תוכנה שיתופית הניתנת להורדה דרך רשת האינטרנט, ללא כל תשלום, ניתן להאזין לתעבורת המידע ברשת ולדלות סיסמאותיהם של משתמשי הרשת.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"הדבר נכון רק לגבי עמדות המפעילות חלונות 98, תחנות אלו נמצאות בתהליכי החלפה. פעילות שתסתיים במהלך 2007."**.

ה. באמצעות מחשב נישא וכבל רשת הצליחה הביקורת לדלות סיסמה של עובד במחלקת מכרזים ובאמצעותה לחדור לשרת app12803 המכיל מאגרי מידע ומערכות כגון: מערכת חוזים, מערכת שקילות, מערכת הזמנות ותיקיית table המכילה מידע רב ורגיש. ברגע שקיבל צוות הביקורת את אותן הרשאות היה באפשרותו לשנות, למחוק ולהוסיף נתונים למערכות השונות. באמצעות רשת האינטראנט של העירייה הצליח צוות הביקורת להתחבר לתיבת הדואר האלקטרוני של אותו עובד. בעזרת תיבת הדואר ניתן לדלות מידע לגבי מספרי העובד של כל עובדי העירייה ולקבל את הרשאותיהם. בדרך זו ניתן היה לקבל סיסמאות של כל עובד המתחבר לעירייה ובאמצעות הסיסמאות לקבל את ההרשאות שניתנו לעובד. באמצעות הרשאות אלו ניתן להתחבר לבסיסי הנתונים, לדלות נתונים, לשנות נתונים, למחוק נתונים ולהוסיף נתונים וזאת מבלי שגורם כלשהו יבחין בכך.

הנהלת אגף המחשוב מסרה לביקורת בהתייחסות לממצאים כי: **"מוצר לפתרון הבעיה נמצא בתהליכי רכש."**.

פרק כב - מסקנות והמלצות

כללי

184. על פי ממצאי הדוח מסקנת הביקורת באופן כללי הינה כי קיים קושי רב בהשגת המטרות ויעדי יחידת אבטחת מידע כמו גם ביכולתה לאכוף את הנושא על כל מחלקות ואגפי העירייה. בין היתר

עקב היעדר תקציבים, אמצעים וכח אדם מספקים. דבר זה מתחדד במקרים בהם היא מייצגת פעילות הנמצאת בסדר עדיפות נמוך יחסית לפעילות הליבה של האגף אליו היא משויכת. ובנוסף קושי זה מתעצם כאשר הגורם האחראי על הנושא הינו בעל סמכות מקצועית בלבד, ממוקם במיקום נמוך יחסית במדרג הארגוני, מרוחק ממוקד קבלת ההחלטות ואינו בעל סמכויות החלטה ברורות ובלעדיות בתחום עליו הוא אחראי.

185. למרות טענת אגף מיחשוב, הביקורת סבורה כי במצב הקיים ישנה עמימות ואי בהירות ביחס לחלוקת סמכויות, קבלת החלטות בנושא אבטחת מידע והגדרת מקור סמכות אחד לקבלת החלטות בתחום.

מדיניות

186. אגף המחשוב התחייב להטמיע את מסמך המדיניות שגובש לאחרונה בנוהל עד לתאריך 15/12/06 ולהעבירו לאישור הנהלת העירייה עד למועד 01/01/07. הביקורת הצביעה על חיוניות הנושא ורואה בחיוב את שבוצע. בשלב כתיבת מסקנות והמלצות הביקורת דווח לביקורת על סיום הכנת המסמך, הכולל משימות לביצוע עם הגדרת אחריות ולוחות זמנים לביצוע (Action's Item). נמסר כי המסמך עבר את אישורו של מנהל אגף המחשוב ושובץ בתוכנית העבודה השוטפת. יחד עם זאת יש לבצע מעקב ובקרה ולוודא הטמעת הנושא ברבעון השלישי של שנת 2007.

ייעוד ומטרות

187. בעירייה קיימים מספר גורמים העוסקים בתחום אבטחת מידע, אם באופן ישיר ואם באופן עקיף, חלקם כפופים לאגף המחשוב וליחידת אבטחת מידע, וחלקם משוייכים לאגפי העירייה השונים. ליחידה שותפי תפקיד רבים העוסקים כחלק מתפקידם בנושא אבטחת מידע, אולם אין ברשותה את הסמכות הפורמלית, המנגנונים והאמצעים הנדרשים לקידום ואכיפת מדיניותה. במצב זה ליחידת אבטחת מידע קיים קושי רב לנהל, לאכוף וליישם את המדיניות וההוראות בתחום אבטחת מידע. באופן כללי מצב זה מקשה על היחידה במילוי יעודה והשגת מטרותיה. דבר זה אף בא לידי ביטוי בהתייחסות אגף המחשוב שהיחידה אחראית על נוהל גיבויים אולם הם מבוצעים בפועל על ידי התפעול. בכל אופן הביקורת מקבלת בברכה את התחייבויות אגף המחשוב ואת לוחות הזמנים לאישור שני נהלי הגיבוי עד ה-15/12/06 ופרסומם עד 15/02/07. וממליצה לבצע מעקב ובקרה במהלך הרבעון הראשון של שנת 2007.

מבנה ארגוני ומערך תפקידים

188. במסגרת יישום שינוי המבנה הארגוני של אגף המחשוב חל פיחות במיצוב היחידה לאבטחת מידע במדרג הארגוני של אגף המחשוב והוא מוגדר על ידי מנהלת האגף כתחום. היחידה מוקמה נמוך יותר במדרג יחסית לעבר, דבר אשר לו משמעויות ארגוניות שונות כדוגמת פיחות ביוקרה

ובמוניטין המקצועי, בסמכויות ובמידת קבלת עובדי העירייה את היחידה כסמכות מקצועית בתחומה.

189. למרות שמנהל אבטחת מידע ממוקם בכפיפות לארכיטקט הראשי, במקביל לגורמי סמכות אחרים באגף, אין לו הסמכות הפורמלית המאפשרת לו לחייב את עובדי האגף בפרט ואת עובדי העירייה בכלל למלא אחר הנחיותיו ולאכוף נושאי אבטחת מידע כנדרש. יש להקנות למנהל אבטחת מידע סמכויות פורמליות שיאפשרו לו לאכוף ולקדם את הפעילות בתחום אבטחת מידע. דבר זה רצוי לבצע בערוצים/מנגנונים ארגוניים שונים כדוגמת מיקום נכון במבנה/המערך הארגוני העירוני או האגפי, מבנה ארגוני יחידתי הולם הכולל תחומים נוספים המבוצעים כיום ע"י יחידות שאינן כלולות ביחידת אבטחת מידע, סמכויות פורמליות רשמיות, מוגדרות וברורות לכל הגורמים, סמכות החלטה ו/או אישור מוחלטים בנושאים מרכזיים כגורם המקצועי בתחום.

190. בהתבסס על ממצאי הביקורת במישורים השונים בתחום אבטחת מידע, מצב התחום בעיריית תל אביב-יפו לקוי וטעון שיפור. הביקורת מבקשת לציין כי במהלך ביצוע הביקורת הנהלת אגף המיחשוב ומנהל אבטחת מידע שיתפו פעולה עם הביקורת, ביצעו שינויים ויישמו המלצות, עוד לפני שלב ההמלצות הסופיות. נכון לשלב זה סוגיות בנושאים שונים טופלו ותמונת המצב בתחום אבטחת המידע השתפרה. הביקורת קיבלה מסמך המפרט סטאטוס ביצוע לתיקון הליקויים שעלו במהלך הביקורת, של אגף המיחשוב ומנהל אבטחת מידע. יחד עם זאת, מודעות הגורמים השונים בעירייה לנושא ולחשיבותו הינה מועטה כמו גם התקציבים, המשאבים והאמצעים העומדים לרשות עובדי היחידה לקידום פעילות אבטחת מידע. דבר זה נכון אף בהשוואה לחברות וארגונים עסקיים במשק הישראלי. במקרים חריגים כגון זה, למבנה הארגוני ולמיקום היחידה במדרג הארגוני הכללי, יש משקל רב במעמד ובחשיבות ששואפים להקנות לנושא ולמידת ההצלחה בהטמעתו. מצב נושא אבטחת מידע בעיריית תל אביב יפו אינו תואם כלל את תמונת המצב המתקדמת ברחבי העולם אותה מצייר אגף המחשוב, כמו גם החשיבות והמודעות הניתנות כיום לנושא. לפיכך אין מקום לטענות כגון **"כיום עם חדירת המודעות של אבטחת מידע, מיקומו הטבעי הוא בסביבה המקצועית...ולכן נושא אבטחת מידע באגף המחשוב יכול לחזור למקומו הטבעי....."** מצב אבטחת מידע בעיריית תל אביב- יפו ירוד מבחינת משאבים, מערך ארגוני, סמכויות פורמליות ולפיכך גם מבחינת מיצובו. כך שנכון יהיה לקבוע כי ההיפך הוא הנכון. לעיריית תל אביב- יפו יש מקום רב עוד מבחינת הקצאת תשומת לב ניהולית, סדר עדיפויות לטיפול, תקציב ואמצעים על מנת להביא את התחום למקומו הטבעי מהמקום הנמוך בו נמצא למעלה, ולא להשיבו למקומו הטבעי כפי שנטען ע"י אגף המחשוב. עפ"י המלצת הביקורת יש לשקול מיקום יחידת אבטחת מידע בכפוף לתחום ניהול סיכונים הכפוף ישירות למנכ"ל העירייה. בניגוד לתגובת אגף המחשוב, דווקא מיקום זה מבטא "קשר לליבה העסקית של הארגון".

191. באם אין אפשרות ארגונית להוציא את תחום אבטחת מידע מאגף המחשוב מומלץ להכפיפו ישירות למנהל האגף.

192. פרוייקט מחו"ג - הביקורת סבורה כי מהותי לכלול עובד אבטחת מידע בפרוייקט מחו"ג. אולם דבר זה צריך להיעשות, להערכת הביקורת, על ידי עובד נוסף מבלי לפגוע עוד יותר במערך כח האדם ובפעילות השוטפת של יחידת אבטחת מידע, אשר ממילא אינם מספקים דיים לטיפול מקצועי ויעיל בתחום אבטחת מידע בעיריית תל-אביב- יפו

193. מחלקת DBA

א. ממצאי הביקורת מעלים כי הנחיות אבטחת מידע אינן נאכפות כנדרש ע"י עובדי ה- DBA. ליחידת אבטחת מידע קושי רב לשלוט על תקינות פעילותם של אנשי ה- DBA בתחום אבטחת מידע.

ב. ממצאי הביקורת מצביעים על כך כי בפועל הרשאות מנהלי הרשת נמצאות אצל ה- DBA-ים ולא רק אצל ה- DBA הראשי. מצב זה אינו תקין.

ג. לא מבוצעות די הצורך בקרות מדגמיות אחר פעילות עובדי ה-DBA ע"י מנהל אבטחת מידע. ממולץ לאפשר למנהל אבטחת מידע האמצעים הטכנולוגיים והתקציבים הנדרשים לצורך ניתור ומעקב אחר פעולות עובדי ה- DBA, כדוגמת הגדלת אחוזי משרת עובדים יעודיים לנושא כלי לניתור פעולות העובדים וכו'. באמצעים אלו תבוצענה בנוסף, בקרות מדגמיות על אנשי ה- SYSTEM.

ד. מחלקת DBA שולטת על צמתים מרכזיים ואחראית על נושאים מהותיים בלב ליבה של אבטחת מידע. זאת בלי קשר להיקף פעילותה בנושא זה מתוך כלל פעילות המחלקה. לפיכך, הביקורת רואה בהפרדה בין ה- DBA לאבטחת מידע פיצול מלאכותי הפוגע בכל תחום אבטחת המידע ובתפקודו של מנהל אבטחת מידע. לדעת הביקורת במצב הקיים, מיקום יחידת אבטחת מידע במקביל ליחידת ה- DBA בכפוף לארכיטקט הראשי לא תורם די הצורך לעבודה מתואמת ומשולבת המאפשרת את האכיפה הנדרשת של נושאי אבטחת מידע. באם אגף המחשוב סבור שחלק ניכר מתפקידי ה- DBA אינם קשורים לתחום אבטחת מידע, דבר המצדיק לשיטתו פיצול ארגוני מאבטחת מידע. מוצע כי הפיצול הארגוני יתבצע ברמת ה- DBA ולא ברמת אבטחת מידע. כלומר במקרה כזה, מוצע להכפיף חלק מעובדי ה- DBA לאבטחת מידע.

ה. באשר לביצוע מעקב אחר פעילות עובדי ה-DBA באמצעות כלי מעקב וניטור- מבלי לבצע ביקורת מעמיקה ביחס לאפקטיביות כלי המעקב ובקרה המצויינים בתגובת אגף המחשוב, הערכת הביקורת הינה כי כלים אלו אכן יכולים לסייע בביצוע הבקרה הנדרשת. הביקורת רואה בחיוב הטמעת כלי למניעת זליגת מידע, במסגרת תוכנית העבודה לשנת

2007. מוצע לבצע מעקב ובקרה על הטמעת הנושא ואפקטיביות הכלי במהלך הרבעון האחרון של שנת 2007 ו/או הרבעון הראשון של שנת 2008.

194. רכזי מחשוב - הביקורת מבקשת להדגיש במסקנותיה את חשיבות תפקיד רכז המחשוב לנושא אבטחת מידע. לאור דיווחי אגף המחשוב לביקורת כי מבוצעת כיום עבודה בהובלת או"ת להגדרת תפקיד הרכז, מומלץ להדגיש את חשיבותו של רכז המחשוב לקידום נושא אבטחת מידע בגיבוש המסמך ותיעודו. כמו כן מומלץ להגדיר באופן רשמי, ברור ומחייב את רשימת משימות אבטחת מידע הכלולות בתפקיד רכז המחשוב, כולל הגדרת כתובת ברורה לסמכות, אחריות וחובת דיווח בנושא אבטחת מידע.

195. אנשי פיתוח – מנהל אבטחת מידע לא מבצע בקרות אחר פעולותיהם של אנשי הפיתוח. לטענת מנהל אבטחת מידע לאנשי הפיתוח אין צורך ברמת הרשאות הניתנת להם, לכן הביקורת ממליצה למנוע מאנשי הפיתוח האפשרות לבצע פעולות שאינן נכללות במסגרת תפקידם.

196. תחזוקת שרתי אנטי וירוס - הביקורת בממצאיה הצביעה על ליקוי ארגוני בכך שנושא האנטי וירוס אינו כפוף למנהל אבטחת מידע. לאור תגובת אגף המחשוב, הביקורת רואה בחיוב את העברת תחזוקת שרתי האנטי וירוס למנהל רשת אבטחת מידע, כמו גם את רכישת המערכת אשר מונעת אפשרות של התחברות לרשת העירונית למחשבים שאינם מכילים אנטי וירוס מעודכן. מוצע לבצע מעקב ובקרה ולוודא אכיפה והטמעת הנושא בהצלחה במהלך הרבעון השני של 2007.

197. מחלקת תמיכה טלפונית - אגף המחשוב מסר לביקורת כי עד חודש מאי 2007 תתבצע עבודה בתחום אבטחת מידע לאימות זהות הפונה למרכז התמיכה לפתיחת חשבון נעול, ע"י קבלת נתונים המופיעים במאגר העובדים העירוניים. כמו כן נמסר כי מנהלת שירות לקוחות תנחה את המוקדניות כי בכל מקרה שכזה יש לאמת את נתוני הפונה ע"י צלצול חוזר לטלפון כפי שמופיע ברישומי אגף המחשוב. פעילות זאת תיכנס לעבודה החל מה-1/1/07 ותיבדק ע"י תחום אבטחת מידע באופן אקראי מדי חודש. הביקורת ממליצה לבצע מעקב ובקרה ולוודא אכיפת הפעילות במהלך הרבעון הראשון של שנת 2007.

198. צוות טכנאים - פעילות תקינה של הטכנאים הינה משמעותית לתקינות הפעילות בתחום אבטחת מידע. לפיכך ישנה חשיבות להגדרת פעילותם בכפוף לנהלי אבטחת מידע. יישום הנושא בהתקשרות עם החברה החיצונית החדשה מהווה צעד מרכזי לאבטחת תקינות פעילות הטכנאים בכלל ובנושאי אבטחת מידע בפרט, כמו גם התאמת ההרשאות הניתנות לטכנאים. לפיכך מוצע לבצע מעקב ובקרה במסגרת ההתקשרות עם החברה החדשה לשרות טכנאים ואכיפת נושא עמידה בנהלי אבטחת מידע לאחר בחירת הזכיין החדש לשרות טכנאים במהלך שנת 2007. כמו כן, יש

לבצע מעקב ובקרה והטמעת שיטת העבודה החדשה של ניהול הרשאות מנהלי רשת עבור טכנאים ע"י אבטחת מידע, ברבעון הראשון של שנת 2007.

199. מנהלי מאגרים - למנהלי המאגרים חלק מהותי באבטחת מידע. בקבוצה זו הקושי הגדול ביותר לאכוף ביצוע בנושא אבטחת מידע. הקושי בא לידי ביטוי באופן מרכזי בתפקידם במתן הרשאות לעובדים לכניסה למאגר המידע אשר באחריותם, כאשר אין להם הכלים המתאימים לקביעת רמת ההרשאות שאמורה להינתן לכל עובד. שימוש בטופס אבטחת מידע אלקטרוני ויכולת לקבל נתונים בזמן אמת אודות רמות ההרשאה הניתנות לעובדים במאגרי מידע שונים הינם מנגנונים משמעותיים להבטחת פעילות תקינה של מנהלי מאגרים במישור אבטחת מידע. לפיכך מומלץ לבצע מעקב ובקרה על הטמעת טופס אבטחת מידע האלקטרוני בשגרת העבודה וזמינות נתונים דרושים למתן הרשאות בזמן אמת למנהלי המאגרים. יש לבצע בדיקה במהלך הרבעון השלישי של שנת 2007.

200. תחום DRP - הטיפול במיפוי המערכות בעירייה והגדרת רמות הקריטיות של כל מערכת כחלק מתפקידי ה- DRP, מחזק את עמדת הביקורת כי מקום ה- DRP בחלקו או במלואו הינו בתחום אבטחת מידע ולא בענף שירות לקוחות ותפעול. יחד עם זאת מוצע לבצע מעקב ובקרה ולוודא אכיפת הפעולות, כפי שהתחייב אגף המחשוב, במהלך שנת 2007, בהתאם למועדים שנמסרו ע"י אגף המחשוב.

תהליך קבלת הרשאות גישה למאגרי המידע וניהול סיסמאות

201. הטיפול בהרשאות (הגדרה, אישור, ביטול וכו') הינו תחום הטיפול המרכזי של עובדי יחידת אבטחת מידע ומהווה נתח נכבד מפעילות אבטחת מידע בעירייה ככלל. ישנה חשיבות רבה לטיפול בבעיות הקיימות בתהליך הטיפול, לשפר ולהטמיע השינויים הנדרשים.

202. בעיריית תל אביב-יפו נהוג לתת לעובדים הרשאות בצורה פרטנית, על פי דרישת יחידות העירייה. דרך עבודה זו יוצרת פתח למתן הרשאות באופן בלתי תקין. כך לדוגמא, יתכן כי עובד יקבל הרשאות החורגות מתחום עסוקו ו/או מאפשרות לו לבצע פעולות ללא בקרות מתאימות.

203. לא קיים מיפוי של כלל התפקידים בעירייה הכולל הגדרת תפקיד, סמכויות, הרשאות וכיוב'. דבר זה חיוני למתן הרשאות נכון ותקין ומהותי לתקינותו של התחום באופן כללי. בהתאם לתגובת אגף המחשוב לממצאי הביקורת, מיפוי כלל התפקידים אמור להיעשות ע"י או"ת ועדיין לא בוצע. לפיכך מומלץ לכלול את המיפוי האמור כבר בתוכנית העבודה של אגף או"ת בשנת 2007.

204. בהתאם לממצאי הביקורת בתהליך מתן ההרשאות משולבים תהליכי עבודה ידניים, ארוכים, הדורשים ניירת מרובה. כך לדוגמא אישור מתן הרשאות מבוצע על גבי טופס פתיחת הרשאות ידני. דבר זה יוצר עומס רב ומיותר על עבודת יחידת אבטחת מידע וגורם לעיכובים בעבודת עובדי

העירייה. הביקורת סבורה כי הטיפול בנושא זה חיוני ויש לבצע זאת בסדר עדיפות גבוה. עפ"י תגובת אגף המחשוב יחידת אבטחת מידע נמצאת בעיצומו של תהליך לבניית מנגנון ממוחשב להעברת טפסים בין הגורמים תוך שימוש בכרטיס חכם להזדהות וחתימה. תהליך זה יושם מבחינה תקציבית בשנים 2007-2008. לפיכך ממליצה הביקורת לבצע מעקב במספר אבני בוחן לאורך השנים 2007 ו-2008 לבקרת ביצוע והטמעת הנושא.

205. לאור מסקנת הביקורת כי קיים חוסר בהירות ועמימות ביחס לתפקידו של מנהל אבטחת מידע במתן אישור להרשאות, התחייב אגף המחשוב כי מנהל אבטחת המידע ימליץ להנהלת העירייה עד תאריך 1/1/07 על תפקידו בנושא ההרשאות. לפיכך מומלץ לבצע מעקב ביצוע בנושא תפקיד מנהל אבטחת מידע במתן אישור להרשאות במהלך הרבעון השני של שנת 2007.

206. הביקורת סבורה כי על אבטחת מידע לוודא שהרשאות גישה למערכות מידע מאושרות, מוקצות ומתוחזקות כראוי. לצורך כך, יש לבצע הפעולות הבאות:

א. להגדיר תהליך רישום וביטול רישום להרשאות גישה למערכות מידע ולשירותים;

ב. להגביל או לפקח אחר מתן הרשאות גישה למערכות ושירותים, בהתאם לרגישות המערכות;

ג. רצוי כי ניהול ההרשאות ייעשה על ידי מנגנון ממוכן לניהול הרשאות.

207. הביקורת סבורה כי בכדי לאכוף שימוש בסיסמאות שתמנענה גישה של משתמשים לא מורשים אל מערכות מידע, יש לבצע הפעולות הבאות:

א. מנהל אבטחת המידע יגדיר מדיניות סיסמאות, בהתאם לרגישות המערכת;

ב. הסיסמה תהיה ידועה אך ורק למשתמש;

ג. הסיסמה הראשונית תוגדר על ידי המשתמש או תימסר לידיו באופן חסוי. בכל מקרה, הסיסמה לא תימסר דרך רשת האינטרנט או דרך התשתית לה נדרשת הסיסמה להזדהות;

ד. במידה וסיסמה נמסרת למשתמש, יש לאמת ראשית את זהות המשתמש. המשתמש יחויב לשנות את הסיסמה בהתחברות הראשונה למערכת;

ה. סיסמאות לא ישמרו באופן גלוי (Clear Text) או באופן הניתן לשחזור ברשומות, בזיכרון או במאגרי מידע.

ו. סיסמה תבוטל מיידית בכל מקרה של חשש לפגיעה בחשאיותה;

ז. אי שימוש בחשבון למשך תקופה של חצי שנה יביא לביטול הסיסמה הנדרשת בתהליך ההזדהות לאותו חשבון;

ח. מורכבות הסיסמה, תוקפה ותחולתה, ייקבעו בהתאם לתקנים מקובלים (כגון תקן ישראלי 1495). לדוגמא: הסיסמה תורכב משילוב של אותיות וספרות, לא יאופשר שימוש בתווים

זהים רצופים, תוקפה יפוג לאחר 60 יום, המערכת תינעל לגישה לאחר 4 ניסיונות גישה כושלים וכדומה.

אבטחה אנושית, מודעות והדרכות עובדים

208. המודעות לנושא אבטחת מידע בעיריית תל אביב יפו מועטה. ניכר חוסר מודעות בולט לתחום ולחשיבותו עד כדי זלזול. כך לדוגמא, לא ניתן כלל לדעת מי מעובדי העירייה עבר הדרכות בנושא אבטחת המידע. הביקורת סבורה שישנה חשיבות רבה בטיפול מערכתי במישור זה לשיפור רמתו בעירייה בכלל, להעלאת המקצועיות, לפעילות יעילה וליכולת האכיפה. להערכת הביקורת יש לתת תשומת לב ניהולית כלל עירונית גבוהה לנושא העלאת המודעות בנושא אבטחת מידע. יש לקבוע מדיניות ותוכנית עבודה מסודרת למהלך העלאת המודעות שתכלול יעדים ומשימות ברורות וממוקדות במישורים ובערוצי פעילות שונים. כמו כן, יש להחיל נוהל עבודה של ביצוע הדרכות שנתיות מסודרות בנושא אבטחת מידע ולנהל מעקב אחר העובדים המשתתפים בהדרכות אלו. מוצע להוביל מהלך כולל זה כמהלך של אגף המחשוב בהנהגתו ומחוייבותו המלאה של מנהל האגף ולא רק ברמה נקודתית של מנהל אבטחת מידע.

209. הביקורת סבורה כי המודעות לנושא אבטחת מידע צריך ללוות את עובדי העירייה עוד בשלב קבלתם לעבודה, דרך התפקידים השונים אותם הם ממלאים בעירייה ועד לעזיבתם. על מנהל אבטחת מידע להגדיר את אופי הטיפול בכל עובד לפי הסטאטוס ואופי התפקיד שלו בעירייה.

ניהול

210. בתפיסת הניהול של הנהלת אגף המחשוב תחום אבטחת מידע נתפס כנושא חורג מהעיסוק המרכזי של האגף. אבטחת מידע נתפס לרוב כגורם מעכב ליישום מטרות והשגת יעדי האגף במתן שירות מיטבי בתחום המחשוב לכל הלקוחות ומענה לכל דרישות הנהלת העירייה. במצב הקיים באגף המחשוב, הביקורת סבורה כי נושא אבטחת מידע אינו יכול ואינו צריך להיות כפוף לאגף המחשוב בעיריית תל אביב יפו. כל עוד הוא כפוף לאגף זה הוא מתגמד ואינו מקבל את המקום הנדרש על מנת לקדם באופן מהותי את מעמדו וחשיבותו הראויים לעירייה ככלל.

211. הביקורת סבורה כי מנהל אבטחת מידע מפנה מזמנו חלק גדול מדי למשימות תפעוליות שוטפות ופחות מהרצוי לטיפול בנושאים מערכתיים כוללים, תכנוננים וניהול מסודר ושיטתי של התחום. יחד עם זאת, להערכת הביקורת לא עומדים לרשות מנהל אבטחת מידע המשאבים הנדרשים (תקציב, כח אדם, משאבי זמן, אמצעים, סמכויות) לעשות זאת.

212. הביקורת סבורה כי אל לעובדי אבטחת מידע לעסוק רק בתחומים ביצועיים ותפעולים. עליהם להיות אחראיים גם על:

א. יישום מדיניות אבטחת מידע;

ב. הפעלת בקרות הקשורות לאבטחת מידע;

ג. החדרה והטמעה של פתרונות אבטחת מידע בכל הרמות, הכוללות: תשתיות, יישומים, נהלים וכו'.

ד. הנחייה מקצועית של עובדי העירייה והנהלת העירייה, בכל הנוגע לתחום אבטחת מידע.

213. כמו כן, הביקורת סבורה כי על עובדי אבטחת מידע להיות בעלי הכישורים והניסיון בתחום וזאת בכדי שיוכלו לתת מענה לדרישות אבטחת המידע בעירייה.

תקציב ותוכנית עבודה

214. התקציב הישיר של נושא אבטחת מידע מהווה כ- 1.8% מהתקציב הכולל של אגף המחשוב. זהו תקציב נמוך ביותר המבטא את החשיבות המועטת הניתנת לנושא באגף המחשוב. באשר לטענת המחשוב כי קיימים תקציבים עקיפים בנושא אבטחת מידע, עמדת הביקורת הינה כי תקציב אבטחת מידע צריך להיות מבודד ולעמוד בפני עצמו. העובדה כי הוא פרוס על פני מספר תחומים מקשה על השליטה בתקציב וכמו כן מלמדת כי התקציב לא נמצא בשליטתו של מנהל אבטחת מידע.

215. לאור הדיווחים באשר לשינוי בשיטת העבודה בהכנת התקציב, מציינת הביקורת כי יש לראות באור חיובי את השינוי בתפיסה ובשיטת העבודה ואת המקום הראוי הניתן למנהל אבטחת מידע בקביעת התקציב ותוכנית העבודה. בהתאם לדיווחי אגף המחשוב כי מנהל אבטחת מידע יכין עד לתאריך 15/02/07 תכנית עבודה הכוללת יעדים ומדדים לאישור הנהלת האגף, מומלץ לוודא ביצוע בנושא תוכנית יעדים ומדדים באבטחת מידע במהלך הרבעון השני של שנת 2007.

נהלים

216. נושא אבטחת מידע אינו מתועד ומיושם כראוי בנהלי עבודה רשמיים ומסודרים. קיים מספר מועט של נהלים כתובים, חלקם כתובים באופן חלקי ובלתי מספק. מרבית הנהלים נמצאים בסטטוס של כתיבה, בדיקה ו/או המתנה לאישור. בתגובה אגף המחשוב העביר לביקורת פירוט של הנהלים על פי סטטוס ביצוע כולל פירוט לוחות זמנים לאישור ופרסום. באופן כללי התחייב האגף לפרסם 3 נהלים ועוד כ-30 הוראות עבודה באתר האינטראנט העירוני עד לתאריך 15/12/06 ו- 3 נהלים נוספים עד לתאריך 15/02/07. כמו כן התחייב האגף להכין טיוטות לאישור של עוד כ 10-15 נהלים החסרים עד ה- 1/06/07 ולפרסמם באתר האינטראנט במהלך הרבעון האחרון של 2007. לפיכך מומלץ לבצע מעקב ביצוע בנושא נהלים והוראות אבטחת מידע במהלך שנת 2007 בהתאם ללוחות הזמנים לביצוע שניתנו ע"י אגף המחשוב.

217. לנושא תהליך אישור הנהלים, אכן הביקורת סבורה כי קיימים מקרים בהם הנוהל דורש מספר רב ולא סביר של גורמים לאישור. הביקורת מציעה להבחין בין נהלי מיקרו המתייחסים לתהליכי

עבודה נקודתיים ובין נהלי מאקרו המתייחסים לתהליכים כלל מערכתיים ומהותיים יותר. בהתאם לזאת לקבוע את הגורמים הרלוונטיים לאישור הנוהל.

218. בנוסף, יש לבצע מעקב לביצוע והטמעה של הנהלים הבאים:

א. נוהל הכנסת תוכנה חיצונית ע"י ספק תוכנה רלוונטי;

ב. נוהל לשעת חרום למקרה של קריסת מערכות;

ג. נוהל אבטחת מידע המטפל בניהול, הכנסה, תפעול והוצאה של מידע מהעירייה, כולל מערכות המכילות זיכרון נייד כדוגמת מחשבים ניידים וכרטיסי זיכרון.

219. הנהלים יעברו תהליך בדיקה ועדכון בהתאם לצורך, עם שינוי משמעותי בסביבה הטכנולוגית או לאחר אירוע אבטחת מידע.

הון אנושי והכשרה

220. למרות שבאגף מיחשוב מתבצעות הכשרות רבות בתחומים שונים, אין הכשרה יעודית מספקת בנושא אבטחת מידע לעובדי יחידת אבטחת המידע. דבר זה משמעותי אף יותר לאור העובדה כי עובדי יחידת אבטחת מידע רכשו את עיקר הכשרתם ונסיונם בתחום במסגרת תפקידם הנוכחי בעירייה. יש לציין כי עד למועד ביצוע הביקורת עובדי היחידה עברו קורס אחד בלבד שהותאם לצרכי היחידה באופן מיוחד.

221. החידושים בעולם אבטחת המידע מתעדכנים ומתחדשים בקצב מסחרר. בכדי לתת מענה מקצועי הולם באבטחת מידע יש לבצע השתלמויות וקורסים בתדירות גבוהה.

אבטחה פיזית

222. נושא האבטחה הפיזית בעיריית תל אביב-יפו טעון שיפור. הביקורת קיבלה את התייחסות אגף המחשוב והתחייבות לתיקונים ושיפורים. בהתאם לזאת יש לבצע מעקב ביצוע של התחייבויות האגף בנושא כמפורט:

א. נוהל אבטחה פיזית- יש לבצע מעקב ביצוע הטמעה לפי התחייבות אגף המחשוב במהלך הרבעון הראשון של שנת 2007.

ב. יש לבצע מעקב ביצוע רענון והפצת נוהל הפקדה או השאלה של מדיית אחסון במהלך הרבעון הראשון של שנת 2007.

ג. יש לבצע מעקב ביצוע בנושא קודנים: הזמנת כיבוי קודנים ושינוי הקוד אחת לחצי שנה ע"י מנהל אבטחת מידע ברבעון הראשון של שנת 2007 ו/או רבעון שלישי של שנת 2007.

223. הביקורת סבורה כי בכדי לחזק את מערך האבטחה הפיזית ובכדי למנוע גישה לגורמים לא מורשים העלולים לגנוב או לגרום לנזק למידע המצוי בעירייה, יש לנקוט בפעולות הבאות:

א. אזורים מאובטחים

1) ממונה אבטחת המידע יחלק את סביבת העבודה למעגלי אבטחה/אזורים מאובטחים לפי רמות רגישות. להלן דוגמא לאופן חלוקת אזורים לפי רמת רגישות: גבוהה (כגון חדרי שרתים), עסקית (אזור עבודה לעובדי משרד אחורי – Back Office, ציבורית (הקהל הרחב רשאי להסתובב באזור זה);

2) על יחידת אבטחת המידע לקבע את רגישות אזורי עבודה ואופי ההגנה עליהם, על סמך המידע הנשמר בכל אזור וסוגי הקהל;

3) על יחידת אבטחת המידע ליישם מספר מעגלים של בקרות גישה פיזית. אם אין ביכולת יחידת אבטחת מידע ליישם בקרת גישה פיזית, עליה ליישם לכל הפחות בקרות ניטור בכל אחד מאתריו. רגישות המידע ומערכות המידע ייבחנו לכל אזור ויוגדרו מורשי גישה לכל אזור.

ב. בהתאם להערכת הסיכונים יוגדרו בקרות פיזיות לאבטחת המידע.

ג. על בקרת הגישה באזורים המוגדרים ברגישות גבוהה לכלול לפחות שער כניסה אחד הנפתח על ידי אמצעי זיהוי חזק. דוגמא לאזור ברגישות גבוהה: חדר השרתים.

ד. מחלקות המעניקות שירותי קבלת קהל במשרדיהם, ישקלו הפרדה בין האזור בו ניתנים שירותים אלו, לבין אזורי העבודה השוטפים בעירייה. בכל מקרה, לא יתאפשר לגורם, שאינו מורשה, להסתובב במשרדי העירייה ללא פיקוח.

ה. האזורים הציבוריים המכילים מידע המסווג כרגיש יוגנו וימודרו בפני גישה של אנשים שאינם בעלי הרשאה למידע. אזורים אלה כוללים בין השאר משרדים, תאי הדואר של העובדים וארכיונים.

אבטחה לוגית

224. על מנת לשפר את רמת אבטחת המידע בעיריית תל אביב יפו, יש לשמור על סודיות הסמאות שניתנות לכל עובד ולטפל בהן כפי שמטפלים בהכנת משכורת או בכל אינפורמציה אישית של עובדים. מצב האבטחה הלוגית בעיריית תל אביב טעון שיפור. אגף המחשוב מסר התחייבויותיו לביקורת לביצוע שינויים ושיפורים. בהתאם לזאת מוצע לבצע מעקב ביצוע במהלך שנת 2007.

225. באשר לנושא מתן סיסמאות באמצעות הטלפון, מוצע לשקול האפשרות לבצע זאת באמצעות רכז המחשוב, לדוגמא, ולא באמצעות הטלפון.

226. באשר לנושא אבטחת משתמשים- הביקורת סבורה כי מצב תחזוקת שרתי האנטי וירוס בעיריית תל אביב יפו אינו יעיל דיו בהגנה בפני וירוס עבור כל קישור לרשת העירונית.

227. הביקורת ממליצה ליישם מנגנונים ממוכנים לניהול בקרות גישה במערכות מידע וביישומים (אפליקציות). בקרות גישה יורכבו מאמצעי זיהוי ובקרת הנתיב בין תחנת הקצה לשירות/שרת.

שרידות וגיבוי מערכות המידע

228. מצב נושא שרידות וגיבוי מערכות המידע בעיריית תל אביב יפו סביר יחד עם זאת מומלץ לבצע מעקב שיפורים ותיקונים בהתאם להתחייבויות אגף המחשוב בנושאים:

א. על אגף המחשוב להגדיר דרישות גיבוי למערכות המידע השונות, בהתאם לרמת הרגישות שתקבע בהערכת הסיכונים.

ב. ממונה אבטחת המידע יהיה אחראי על בקרת איכות הגיבויים.

ג. מוצע לקיים מעקב ביצוע במתן מענה למערכות קריטיות ולטיפול בהתאוששות מאסון במהלך שנת 2007.

ד. מומלץ לקיים מעקב ביצוע באפסון קלטות גיבוי יומי בתוך כספות חסינות אש במהלך שנת 2007.

בקרות הנהלה

229. הביקורת אתרה ליקויים בנושא בקרות ההנהלה, בתחום אבטחת המידע הדורשים תיקון. יש לציין כי ליקויים אלו נמצאים בטיפול אגף המחשוב במסגרת פרוייקט ה-DRP.

230. בנושא סיכונים צפויים ופעולות מתקנות- מוצע לקיים מעקב ביצוע במהלך שנת 2007 ולוודא הכנת רשימת סיכונים צפויים ופעולות מתקנות בהתאם ע"י מנהל אבטחת מידע.

231. כמו כן מוצע לקיים מעקב ביצוע במהלך שנת 2007 בנושא קביעת רמת סיווג לכל מערכת ע"י מנהל אבטחת מידע.

232. הביקורת סבורה כי על אבטחת מידע ליצור רשימת מלאי של כל נכסי המידע העיקריים של כל המערכות, לסווג נכסים אלו לפי רמת הרגישות ולהגדיר בקרות אבטחת המידע הנדרשות.

233. הביקורת ממליצה לקיים הערכת סיכוני אבטחת מידע במערכות המידע והממשקים הפועלים בעירייה, באופן הבא:

א. הערכת הסיכונים תגדיר את רמת הרגישות של המערכות ותתייחס למכלול סיכוני אבטחת המידע הפוטנציאלים הנובעים ממערכות המידע ומההתנהלות העסקית השוטפת של העירייה. סיווג רמת הרגישות של כל מערכת תיקבע לפי המידע בעל הרגישות הגבוהה ביותר בו היא מטפלת.

ב. תהליך זה יתבסס על סיווג הנכסים, אופי העבודה במערכים והאגפים השונים בעירייה והאופי העסקי של העירייה.

ג. העירייה תעדכן את הערכת הסיכונים עם שינויים משמעותיים בתהליכים העסקיים, במערכות המידע או באיומי אבטחת מידע.

ד. תוצר הערכת הסיכונים ינחה את הנהלת העירייה בהפניית משאבים נאותים להטמעת אמצעי אבטחת מידע ולמיקוד בסקרי סיכוני אבטחת המידע במערכות השונות בעירייה.

ה. תוצר הערכת הסיכונים, יחד עם תוצר סיווג הנכסים, יספק מדרג רגישות של מערכות שונות בעירייה.

ו. המערכות הבאות והממשקים הבאים יסווגו בכל מקרה כמערכות בעלות סיווג גבוה:

1) מערכות המכילות מידע רפואי;

2) קישור נותני שירות מחוץ לעירייה לרשת העירייה;

3) תקשורת דרך רשת ציבורית אל תוך רשת המידע בעירייה המכילה מידע רגיש;

4) מאגרי כוח אדם/עובדים/תושבים – פרטים אישיים הקשורים בצנעת פרט;

5) סקרי סיכוני אבטחת מידע ומבחני חדירה מבוקרים.

ז. הביקורת ממליצה לבצע סקר סיכונים בנושא אבטחת מידע, בכדי להבטיח עמידת מערכות המידע בדרישות מדיניות אבטחת המידע של העירייה ושל מתודולוגיות אבטחת מידע מקובלות בעולם.

ח. ממונה אבטחת המידע ייזום סקרי אבטחת מידע של מערך טכנולוגיית המידע של העירייה.

ט. מערכות בעלות סיווג גבוה ייסקרו לפחות אחת ל – 12 חודש.

י. לגבי מערכות אחרות ההנהלה תקבע את תדירות הסקרים בהתאם לרגישות המערך.

יא. הסקרים יבחנו את נושאי הניהול ואת יעילות אמצעי ההגנה (כולל אמצעים פיזיים ולוגיים) שיושמו בעירייה ואת רמת הגדרות אבטחת המידע במערכות המידע הן ברמת התשתית (ציוד ותווך תקשורת, מערכות הפעלה, בסיסי נתונים) והן ברמת האפליקציה (ברמת קוד מקור או חבילות תוכנה).

יב. ממונה אבטחת המידע יערוך סקרי אבטחת מידע לפני הטמעת שינויים משמעותיים במערכות שהוגדרו על ידי העירייה כבעלות סיכון גבוה לפי הערכת הסיכונים, כלומר כאשר חלים שינויים משמעותיים במערכות אלו או לפני הכנסת מערכות אלו לשימוש תפעולי (Production).

יג. ממונה אבטחת המידע ייזום מבחני חדירה (Penetration Tests) הן ברמת התשתית והן ברמת היישום (אפליקציה), המדמים ניסיונות פריצה על ידי פורצים מתוך ומחוץ לעירייה,

הן כמשתמש קיים והן כפורץ ללא חשבון קיים, למערך הטכנולוגי. תדירות מבחני החדירה תיקח בחשבון את רגישות המערך.

יד. סקרי אבטחת המידע ומבחני החדירה ייערכו על ידי גורם מקצועי, עצמאי, בלתי תלוי וחיצוני לעירייה.

טו. הנהלת העירייה תקיים דיונים על תוצאות סקרי אבטחת המידע ומבחני החדירה ותפעל למימוש המלצותיהם תוך פרק זמן סביר.

בקרת חומרה ותוכנה

234. מצב נושא בקרת חומרה ותוכנה סביר. אם כי מוצע לקיים מעקב ביצוע בנושאים:

א. הכנת נוהל אבטחת מחשבים ניידים ע"י מנהל אבטחת מידע בהתאם להתחייבות אגף המחשוב. יש להגדיר בנוהל מה הם השימושים המותרים שניתן לבצע במחשבים ניידים ואופן אבטחת המחשבים הניידים

ב. במידה והמחשבים הניידים מחוברים לרשת העירייה, יש לאבטח את הרשת ואת האמצעים בפני פגיעה הדדית ברמת אבטחת מידע.

ג. מעקב ביצוע של בדיקת התכנות למוצר WSUS של מיקרוסופט להפצה אוטומטית של עדכוני גרסה במהלך שנת 2007.

הגנה מפני ניסיונות פגיעה

235. הביקורת סבורה כי על מנת להגן על רשת העירייה ומשתמשיה, על מנהל אבטחת מידע לנקוט באמצעים מקובלים ונאותים המצמצמים את החשיפה לניסיונות פגיעה (כולל איתור, זיהוי ומניעת ניסיונות אלה). אמצעים אלו יגנו מפני שימוש לא תקין במידע, במערכות המידע ובבסיסי הנתונים. דוגמא לאמצעים המצמצמים את החשיפה לניסיונות פגיעה הינה קיומן של מערכות לאיתור ניסיונות חדירה מהאינטרנט ומתוך הארגון (IDS), מערכות לסינון תכנים (Content Filtering) וכדומה.

236. על ממונה אבטחת המידע להתאים את האמצעים המקובלים והנאותים בהתאם להתפתחויות הטכנולוגיות שישררו באותה עת, ולאיומים ולחשיפות הרלוונטיים לאותה תקופה.

זמינות נתונים

237. על ממונה אבטחת המידע ליישם כלים להבטחת זמינות הנתונים של מידע שהוגדר כחיוני בתהליך הערכת הסיכונים. לצורך כך, יש לשקול שימוש בכפילות ויתירות של מערכות, במערכות לחלוקת עומסים, בכלים לייצוב מתח חשמלי וכדומה.

ניהול רשת

238. ממולץ כי קישור גורמים חיצוניים מ/אל רשת העירייה תתבצע באופן ריכוזי, דרך מספר נקודות כניסה מאובטחות. לא תאושר כל התחברות "עצמאית", שאינה דרך נקודות כניסה מאובטחות אלה.

239. יש ליישם מידור בין החלקים השונים ברשת באמצעות חלוקה לוגית ופיזית של הרשת והגבלת אפשרות הקישור בין הרשתות השונות. רמת המידור תיקבע בהתאם לרמת הרגישות של המערכות.

240. יש ליישם בקרה וסינון של תקשורת יוצאת ונכנסת על פי הגדרות העירייה ובקרה על הפעילויות המתבצעות במערכות לאיתור אירועים חריגים. בנוסף לבקרה בדיעבד, תיושם בקרה בזמן אמת.

תגובה לאירועי אבטחת מידע

241. הביקורת סבורה כי על ממונה אבטחת המידע להגדיר מה הם אירועי אבטחת מידע ולשקול על איזה מהם יש להגיב. כמו כן, יש להגדיר מנגנון דיווח על אירועי אבטחת מידע שיהיה נגיש לעובדים ואופן התגובה לכל אירוע שכזה.

הצפנה (Encryption)

242. יש לשקול יישום מנגנוני הצפנה להגנה על חיסיון מידע בעל סיווג גבוה האגור באמצעי אחסון (קובץ, בסיס נתונים וכדומה).

243. על ממונה אבטחת המידע ליישם הצפנה להגנה על חיסיון מידע בעל סיווג גבוה בתווך התקשורת אל מחוץ לארגון.

פיתוח ותחזוקה של מערכות

244. בכדי להבטיח הטמעת בקרות אבטחת מידע בתהליך פיתוח מערכות מידע יש לבצע הפעולות הבאות:

א. בתהליך קליטה של מערכות מידע חדשות או בעת שדרוג מהותי של מערכות מידע קיימות, יילקחו בחשבון שיקולי אבטחת מידע;

ב. דרישות אבטחת מידע יוגדרו לתהליך פיתוח של מערכות חדשות או שדרוג של מערכות קיימות;

ג. יישומו מנגנונים קריפטוגרפים על מנת להבטיח חשאיות (Confidentiality) ואמינות (Integrity) של נתונים בעלי סיווג גבוה;

ד. אבטחת מידע תוטמע ברמת היישום (האפליקציה) כולל וידוא קלטים, וידוא פלטים, אימות שדרים, אישור אמיתות נתונים וכדומה;

ה. כאשר פיתוח מערכת נעשה על ידי גורם חיצוני, יש להבטיח בהתקשרות הגנה על נושאים רגישים.

נתיב בקרה (Audit Trail)

245. בכדי שמנהל אבטחת מידע יוכל לגלות פעילויות לא מורשות ולזהות את מקורן, עליו לבצע הפעולות הבאות:

א. לקיים נתיב בקרה לניטור ומעקב אחר ביצוע פעולות ושאילתות במערכות השונות, הן מתוך העירייה והן מחוצה לה. יש להחיל מנגנון נתיב בקרה על כל מערכת.

ב. תכולת נתיב הבקרה תיקבע בהתאם לרמת רגישות המערכת. על ה - Log להכיל את הנתונים הרלוונטיים, כך שיתאפשר לגלות ניסיונות גישה ופעולות לא מורשות ולזהות את מקורן. נתיב הבקרה יכלול מידע לפחות על ניסיונות של מורשים ולא מורשים, מוצלחים ולא מוצלחים, מהות הפעולה, מקור הגישה וזמן הגישה.

ג. פרק הזמן לשמירת קבצי התיעוד ייקבע בהתאם לרגישות המערכת.

ד. כל ניסיון גישה כושל וחריג למערכת ינוטר ויתועד במנגנון אירועים.

ה. העירייה תיידע את עובדיה בדבר ביצוע רישום פעילויותיהם בקובץ LOG.

ו. על שעון מנגנון הניטור להיות מסונכרן עם מקור שעון מדויק לצורך דיוק התיעוד.

ז. קבצי ה – LOG יאובטחו בפני מחיקה, שינוי או קריאה בלתי מורשים.

שירותים מקוונים

246. בכדי למנוע חשיפת מידע הקשור בצנעת פרט לגורמים לא מורשים ולצמצם יכולת פריצה של גורמים לא מורשים אל רשת העירייה, על מנהל אבטחת מידע לבצע הפעולות הבאות:

א. מידע רגיש, המועבר דרך תשתית תקשורת ציבורית (לדוגמא, דרך אתר העירייה באינטרנט) ודרך תקשורת טלפוניה יאובטח באופן המצמצם את הסיכון לחשיפתו.

ב. בכל מקרה כזה, יידרשו אמצעי הצפנה, שמירה על מהימנות נתונים, זיהוי אישי חד ערכי ואמצעי מניעת התכחשות. יש לעשות שימוש באמצעים מקובלים.

ג. התקשורת Session)) תהיה מאובטחת לכל אורך חייה. במידת הצורך, במהלך התקשורת Session)) תידרש הזדהות חוזרת גם לאחר הזדהות ראשונית.

ד. לא תותר גישה ישירה מבחוץ (אתר העירייה) למערכות מידע ברשת הפנימית (קישור ישיר ל – LAN) של העירייה, אלא דרך מערכת שער (Gateway) מאובטחת, הממוקמת באזור מפורז מחוץ לרשת הפנימית (DMZ Demilitarized Zone), שתיזום את ההתקשרות לרשת הפנימית.

ה. בסיסי נתונים המכילים מידע רגיש, לא יהיו נגישים למשתמשים מהאינטרנט ולא ימוקמו ברשת המפורזת DMZ. הגישה לבסיסי הנתונים תתאפשר אך ורק דרך מחשבי העירייה המשמשים כמתווכים באופן מאובטח.

ו. יוגדרו הרשאות כך שכל משתמש יוכל לבצע אך ורק את הפעולות שהוגדרו לו כמותרות.

בקרות קלט

247. מוצע לקיים מעקב ביצוע בנושאים הבאים:

א. הוצאת חומר ע"י התקן חיצוני;

ב. שליחת נתונים רגישים להדפסה;

ג. תיוג המידע לפי רמת רגישותו;

ד. חיטוי למדיה טרם העברתה;

ה. רענון נוהל השמדת מדיות מגנטיות.

איומי רשת

248. על הנהלת אגף המחשוב לבצע מעקב אחר הפעולות אליהם התחייב אגף המיחשוב, בנושא בקרות קלט. כמו כן, הביקורת ממליצה להמשיך את פרויקט כרטיס עובד חכם.

מעקב ביקורת

249. על הנהלת אגף המחשוב לבצע מעקב בנושא פעילות אגף המיחשוב, בכל הנוגע לשמירת סוגי המידע השונים.

הערת הביקורת

250. בתאריך 27/2/07 לאחר סיום עבודת הביקורת הועבר מאת אגף המיחשוב המסמך שלהלן המפרט את הפעולות שביצע האגף בעקבות מסקנות והמלצות הביקורת.

משימות לביצוע:

מענה לטיוטת דו"ח ביקורת בנושא אבטחת מידע

	משימות לביצוע	סעיף	אחראי	מועד מתוכנן	מועד מעודכן	סטאטוס	הערות
1	לברר את נושא הזמינות בחברות אחרות	5	א	מיידי			לבדוק מייל של א
2	עריכת שינויים סופיים במסמך מדיניות קיים-	6	ח	15.12.06		בוצע	
3	העברת מסמך מדיניות לאישור הנהלת העירייה	6	ח	1.1.07	15.3.07	בעבודה	27.2. אושר ע"י ע–
4	סיום כתיבת נוהל גיבוי מערכות פנימיות- והעברתו להתייחסות לכל הנוגעים בדבר.	24	ח	15.2.06	15.4.07	לא התחיל	
5	לבדוק האם נוהל השמדת מדיות מופיע בתוך נוהל גיבוי-	24	ח	15.2.06		בוצע	

	משימות לביצוע	סעיף	אחראי	מועד מתוכנן	מועד מעודכן	סטאטוס	הערות
6	העברת הטיפול בשרת אנטי וירוס לאבטחת מידע- לדבר עם ד	24	א	מיידי		בוצע	
7	זיהוי משתמש (בתמיכה) ע"פ נתונים עירוניים במ"א	26	ח	מאי 2007	יוני 2007	בעבודה	6.2.07 נשלחה בקשה לע לשימוש בכתובת לקוח. 27.2 ע לא אישר- ידון בפ"ע ח- ע 15.4.07
8	להודיע לא על הנחיית עבודה חדשה (בתמיכה) בעניין זיהוי משתמשים ע"פ צלצול חוזר. כולל בדיקה חודשית	26	א	1.12.06		בוצע	
9	שינוי הרשאות לטכנאים ממנהלי רשת למנהלי תחנות עבודה	26	ח	1.1.07		בוצע	
10	טופס אבטחת מידע אלקטרוני (כולל מיפוי מאגרי מידע ומנהליהם)	27	ח	עד מרץ 2007	יולי 2007	בעבודה	הטופס קיים, צריך תוכניתן
11	התייחסות מנהל האגף לסעיף 28	28	א	מיידי		בוצע	

	משימות לביצוע	סעיף	אחראי	מועד מתוכנן	מועד מעודכן	סטאטוס	הערות
12	מניעת כניסה לרשת ללא אנטי וירוס		ח	עד מרץ 2007		בעבודה	23.01.07 הציוד נרכש. נקבעה ישיבת התקנה והתנעה ל 31.01.07. 6.2.07 תקלות בהתקנה
13	הגדרת תפקיד ממונה אבטחת מידע בנושא הרשאות	28-29	ח	1.12.06	15.4.07	לא התחיל	
14	בדיקת התואר "תחום" עם א וא	29	א	מיידי		בוצע.	
15	לבדוק הוצאות נוספות (כמו שרתים) ב2006 ולהוסיף לסעיף 53	53	א	מיידי		בוצע	
16	תוכנית עבודה (יעדים ומדדים)- אבטחת מידע	46	ח	15.2.06	15.3.07	לא התחיל	
17	פרסום נהלים קיימים באינטראנט ובהמשך בפורטל האירגוני+ שליחת הודעה על הפרסום בפורום אגף מחשוב	77	ח/ ר	15.12.06		בוצע	עבור כל הנהלים הקיימים
18	פרסום נהלים חדשים בפורטל	77	ח/ ר	מרץ 2007		בוצע	

	משימות לביצוע	סעיף	אחראי	מועד מתוכנן	מועד מעודכן	סטאטוס	הערות
19	רשימת נהלים שיש לכתוב	77	ח	1.1.07		בוצע	
20	הכנת טיוטות לנהלים	77	ח	1.6.07		בעבודה	
21	מיפוי מתקנים רגישים (בטבלה ראשונית) והעברתה למנהלי האגפים להתייחסות. לאחר מכן יש לצרפה לנוהל ולהפיצו אחת לחצי שנה בכל פורום מנהלי האגפים לרענון.	85	ח	1.3.06	1.6	בעבודה	6.2.07 יש רשימה, אין סיווג
22	הנחייה לאיסור כניסה של צוות המס״ב לחדר שרתים	26	א/ א	מיידי		בוצע	
23	הפצת נוהל הפקדה או השאלה של מדיות אחסון	77	ח	1.12.06		בוצע	נוהל 12
24	הזמנת כיסוי ל-3 קודנים של חדרי השרתים	88	ח	15.12.06		בוצע	נערכה בדיקה- אין מוצר כזה בחברה שהתקינה את הקודנים.
25	שינוי קוד בקודנים- אחת לחצי שנה.	88	ח	החל מ-15.12.06		בוצע	החלפה ראשונה 1.2.07, מעכשיו כל חודש.
26	הנחייה לנעול חדרי שרתים- לשלוח בפורום מנהלי אגפים	89	ד	1.12.06		בוצע	

	משימות לביצוע	סעיף	אחראי	מועד מתוכנן	מועד מעודכן	סטאטוס	הערות
27	בקשה לקבלת תוכניות צנרת בסביבת חדרי השרתים (מהנהלת הבית)	91	ח	15.12.06		בוצע	אין תוכנית צנרת בעירייה, יוציאו בשיפוץ את הצינורות מחדר מחשב.
28	רכישת מערכת התרעה בפני הצפות	91	ד	עד מרץ 07		בוצע	הועבר לידיעתו של ד.
29	לבדוק מול דני מתי מתוכננת ירידה משרתי נובל		ר	מיידי		בוצע	עד סוף 2007
30	בדיקה לגבי מורכבות הסיסמאות היום	102	ח	מיידי		בוצע	
31	נוהל שינוי סיסמא (עבור מוקד 8025)	102	ח	1.107		בוצע	
32	251. להכניס בנוהל הכנסת תוכנה חיצונית סעיף המחייב את היצרן לספק תיעוד הרלוונטי (באינטרנט, מדיה מגנית או ספרות פיזית)	149	א			?	
33	לפנות למנהלי פרויקטים לרענן את הנהלים אודות קיומם של מדריכים למשתמש	151	א	מטה מורחב הבא		בוצע	

	משימות לביצוע	סעיף	אחראי	מועד מתוכנן	מועד מעודכן	סטאטוס	הערות
34	ממונה אבטחת מידע יפנה לד"ר ר ג לצורך מחשבה משותפת לבניית קורס עירוני ייעודי בנושא אבטחת מידע.	160	ח	2007		בוצע	בפגישה עם ר ג סוכם כי אין מקום לבניית קורס מלא לאבטחת מידע. תבוצענה פעילויות בשת"פ לעידוד המודעות.
35	מנהל אבטחת מידע יקיים פגישה עם עובדים חדשים (טרם כניסת לתפקיד ובתיאום עם משאבי אנוש) בנושא אבטחת מידע- אחת לחודש	163	ח	2007		בעבודה	נקבעה פגישה ל 21.02.07 עם ע בנושא. במידה ו מבטל יש להצטרף לפ"ע של א. 27.2 מבקש להצטרף לפ"ע א
36	מנהל אבטחת מידע יזום פגישה עם מנהל אגף משאבי אנוש במטרה לגבש קריטריונים לבדיקה בתהליך קליטת עובד חדש.	168	ח	2007		בעבודה	נשלחה בקשה 6.2.07
37	יציאת עובדים לחופשות מאולצות ורוטציית תפקידים- כנ"ל	169	ח	2007		לא התחיל	
38	התייחסות של דני	120	א			בוצע	
39	הכנת רשימת סיכונים צפויים+ פעילויות מתקנות רלוונטיות	128	ח	עד מרץ 2007	מאי 2007	לא התחיל	

	משימות לביצוע	סעיף	אחראי	מועד מתוכנן	מועד מעודכן	סטאטוס	הערות
40	להוסיף את רמת הסיכון לכל מערכת בטבלת מערכות שהוכנה ל- DRP	130	ח	עד מרץ 2007	יולי 2007	בעבודה	
41	בדיקת נוהל ליווי אנשי מקצוע (חיצוניים)	135	ר- ח	מיידי		בוצע	
42	להכין נוהל אחזקת מחשבים ניידים כחלק מרשימת הנהלים	135	ח		אפריל 2007	לא התחיל	
43	לבדוק האם מתבצעת סריקת וירוסים לכל המחשבים כל לילה בחצות	142	ח	מיידי		בוצע	מתבצעת סריקה שבועית על כל המחשבים והשרתים ברשת.
44	בקרת תקינות ושלמות מידע	143	ח			בוצע	
45	לרענן נוהל מדיה מגנטית, כולל הפצתו במסגרת כל הנהלים	175	ח			בוצע	
46	יזום פעילות סיוע למנהלי המאגרים בעזרת אינפורמציה וידע לגבי פעילויות המוזכרות בסעיף. בנוסף פגישות עם ד"ר ר ג- להעלאת	177	ח	עד יוני 2007		בעבודה	ביקשתי מרן ג לדבר בפורום מנהלי אגפים בנושא. מחכה לזימון.

	משימות לביצוע	סעיף	אחראי	מועד מתוכנן	מועד מעודכן	סטאטוס	הערות
	רעיון להכנת סדנא/ השתלמות ייעודית למנהלי מאגרים.					בוצע	
47	להתייחס לנושא הלוגים בפגישות שלמדיניות שמירת קבצים		א			בוצע?	
48	להוציא מייל ל ולמ לגבי איסור כניסה לחדר שרתים שיעבירו למנהלים שלהם.		ר- ח	מיידי		בוצע	

נספח א – מילון מונחים

פרק זה מפרש מונחים שונים בהם נעשה שימוש לאורך הדוח. מונחים אלה מוסברים בהקשר של אבטחת מידע.

252. **איום – Threat**: אפשרות פוטנציאלית לפגיעה בשלמות, זמינות או חשאיות המידע.

253. **מתקן רגיש** : כל חדר אשר מכיל בתוכו מידע רגיש.

254. **אמצעי זיהוי**: אמצעי המספק פרטים לגבי זהותו של אדם או מערכת בעת ניסיון כניסה ואישור ביצוע פעולות מטעמם למערכת מידע.

255. **הערכת סיכונים:** תהליך של הערכת רמת הסיכון של המערכות השונות בארגון. התהליך ממפה את האיומים השונים הנובעים מהפעילות במערכות השונות. תוצר הערכת הסיכונים הנו מסמך המדרג את רמת הרגישות של המערכות השונות בארגון. מסקנות מסמך זה משמשות לגזירת פעילויות אבטחת המידע השונות.

256. **הצפנה:** יישום של קריפטוגרפיה הממירה מידע גלוי (Clear Text) למידע מקודד (Cipher Text) באופן שיוכל להיות מפוענח ומובן אך ורק לגורמים מורשים.

257. **חומת אש – Firewall:** רכיב (תוכנה על שרת או רכיב חומרה) המבקר את התעבורה הנכנסת והיוצאת מרשת תקשורת על פי מדיניות אבטחה מוגדרת.

258. **חשיפה – Vulnerability:** חולשה במערכת העלולה להוביל להתממשות איום.

259. **חתימה דיגיטאלית (Digital Signature):** פריט מידע ייחודי הנוצר כפונקציה קריפטוגרפית של פריט מידע אחר, כך שהוא מזהה את התוכן בצורה מדוייקת ומאפשר לזהות שינוי בו.

260. **לוג – Log:** קובץ התיעוד של נתיב בקרה.

261. **מדיניות אבטחת מידע:** מסמך המציג את תפיסת ההנהלה בנושא אבטחת המידע בארגון, מביע את מחוייבותה לנושא ומגדיר את המבנה הארגוני וחלוקת הסמכויות בתחום. במסמך זה נקבעים עקרונות מנחים ליישום ולבקרה של אבטחת מידע, תוך יצירת תשתית ממנה ייגזרו נהלי עבודה בתחומים השונים.

262. **מידע רגיש:** מידע שהארגון סיווג כבעל סיווג הדורש אמצעי אבטחת מידע נאותים. בכל מקרה מידע בעל סיווג גבוה, יוגדר כמידע רגיש, תכולת מידע זה נתונה לפרשנותו של הארגון.

263. **מערכת מידע**: מערכת מידע היא חבילת תוכנה המאפשרת לנהל מידע בצורה ממוחשבת. המערכת מיועדת לארגון או ליחיד. היא מאפשרת אחסון מידע, ניהולו, עיבודו ושליפתו מאוחר יותר, בחתכים מסוימים. ניתן לנהל מערכות מידע בכל תחום: פיננסי, תעשייתי ,גיאוגרפי, וכדומה. הציוד הממוכן התומך בעיבוד מידע של הארגון הכולל בין השאר: שרתים, מחשבים נייחים וניידים, ציוד תקשורת, ציוד אבטחת מידע, מהווה חלק חשוב במערכת המידע.

264. **סיכון:** הינו ההסתברות שיקרה דבר עוין.

265. **סקר סיכונים:** סקר המאתר איומים/חשיפות הקשורות באבטחת מידע במערכות שונות והמעריך את רמת הסיכון שלהם לארגון.

266. **קריפטוגרפיה:** שימוש בכלים מדעיים ואלגוריתמים לצורך הגנה על מידע. המטרות העיקריות של קריפטוגרפיה הינן שמירה על חשאיות ואמינות המידע, מתן פתרון למניעת הכחשה של פעולות ומתן מנגנון לאימות זהות משתמשים.

267. **שימוש באמצעים מקובלים:** שימוש בטכנולוגיה לאבטחת מידע, שאומצו על ידי מומחי אבטחת המידע. אמצעים אלו יותאמו בהתאם להתפתחויות בנושא ולסיכונים הרלוונטיים באותה עת.

268. **רשת פנימית - LAN) Local Area Network):** קבוצת מחשבים המקושרים זה לזה בעזרת ציוד תקשורת ונגישים למשאבים (משתמשים ומחשבים אחרים) בתוך הארגון.

269. **בסיס נתונים (או מסד נתונים):** הוא תוכנה המשמשת לאחסון מסודר של אינפורמציה מכל סוג שהוא במחשב, לשם אחזורה ועיבודה. לתוכנה זו יש מודלים תכנותיים קבועים מראש, שמקילים על העבודה עם המידע, כמו מנגנונים פנימיים למיון וחיפוש.

270. **מערכת הפעלה:** היא תוכנה המגשרת בין המשתמש, החומרה ויישומי התוכנה.

271. **חומרה:** היא אוסף כל הרכיבים הפיזיים במחשב או בהתקן אלקטרוני אחר.

272. **אבטחת מערכות מידע:** הוא תחום פעילות העוסק בהגנה על מערכות מחשב מפני סיכונים המאיימים עליהן.

273. **שרת:** מחשב ותוכנה המותקנת בו המחוברים לרשת מחשבים ותפקידם לספק שירותים שונים למחשבים ברשת. דוגמה לשרתים: שרת קבצים, שרת דואר.

274. **נקודה חמה**Hot spot)): אזור ציבורי או מסחרי בו מוצעת גישה אלחוטית לאינטרנט, בין אם בחינם או בתעריף לפי שעות או ימים.

275. **טבלה:** בבסיס נתונים יחסי, טבלה היא אוסף כל הרשומות בנושא מסוים. טבלת כתובות במרשם התושבים, למשל, תכיל את כל רשומות הכתובת של כל התושבים.

276. **זמינות שרת:** כל נפילה או תקלה בתהליך או ישום על גבי השרת פירושה השבתה של השרת (כל השבתה בעצם גורמת לחוסר זמינות של המידע המצוי על השרת).

277. **חיסיון המידע:** מידע יהיה נגיש לגורם שהורשה לו בלבד.

278. **זמינות המידע (והמערכת):** מערכת המידע והמידע האגור בה יהיו זמינים בהתאם לרמת הזמינות שהוגדרה על ידי לקוחות המערכת.

279. **שלמות ואמינות המידע:** הגנה על כך שהמידע במערכת יכיל את כל שהוגדר מלכתחילה וכי הנתונים עצמם לא עברו שינוי על ידי גורם שאינו מורשה.

280. **מערך הרשאות:** מתבסס על הזדהות כתנאי מקדים, שכן המערכת נדרשת לקשר בין משתמש לפעולה.

281. **גיבוי (Backup):** הנו שם כללי המציין את מכלול התהליכים אותם יש לבצע בכדי ליצור העתק של מידע השמור מפני שינויים.

282. **תהליך הגיבוי:** הנו חלק מתהליך אבטחת המידע, בו נשמר העתק של המידע לפני השינויים ואחריהם על מנת לאפשר שחזור של המידע במקרה של כשל. כמו כן, נשמרות גרסאות השינויים שנעשו במידע בכדי לאפשר חזרה לגרסה תקינה במקרה של שיבוש.

283. **נתב - (Router):** הוא רכיב ברשת מחשבים שמבצע החלטות לגבי העברת חבילות נתונים על פי מערכת כתובות לוגיות (כתובות IP) ופרמטרים אחרים.

284. **מתג - (Switch):** הוא רכיב ברשת מחשבים המאפשר שליטה על התעבורה ברשת בהתבסס על כתובות MAC, ומחבר בין שניים או יותר חלקים של הרשת.

285. **אנטי וירוס:** היא תוכנה ייחודית שנכתבת להגנה על המחשב מפני פעילות של וירוסים במחשב.

286. **וירוס מחשב:** הוא תוכנת מחשב, שחודרת למחשב ללא ידיעת המשתמש, וגורמת על פי רוב לשיבושים ולתקלות שונים בהפעלת המחשב, מתוך כוונת מכוון.

287. **תקשורת מחשבים או "תקשוב":** שם כללי לשני מחשבים (או יותר) המעבירים ביניהם מידע מבלי להעביר אמצעי אחסון פיזי (כגון: תקליטון - דיסקט, תקליטור וכו') כלשהו ביניהם. הקשר בין המחשבים מתקיים באמצעות תווך תקשורת כלשהו.

288. **אפליקציה:** קבוצת פקודות הנכתבות על ידי משתמש ומכילות רצף הגיוני בעל מטרה.