נספח א

עיריית תל-אביב-יפו
אגף מחשוב ומערכות מידע

ב' בכסלו, התשע"ב
28-נובמבר-11
סימוכין : 42009511

לכבוד : מבקרת העירייה

הנדון: טיוטת ממצאים לדוח ביקורת בנושא אבטחת מידע

סימוכין מס' 37383511, מיום 25 אוקטובר 2011

מצ"ב התייחסות בעלי התפקידים השונים באגף מחשוב ומ"מ לטיוטת ממצאי דו"ח ביקורת בנושא אבטחת מידע :

א. התייחסות מנהלת אגף מחשוב :

פרק וועדת היגוי, סעיף 12,עמוד 6 , התקיים כינוס נוסף של הוועדה ב – 14.09.11.

ב. התייחסות מנהל יחידת אבטח מידע :

1. פרק אחריות מנהלים, סעיף 19,עמוד 8
בוצעו מגוון של פעולות הדרכה, לדוגמא – בהנחיית המנכ"ל התקיים כנס מנהלי מחלקות בכנס הוצג נושא אבטחת המידע למנהלים. נושא אבטחת המידע הוצג בפורום מנכ"ל וגם בפורומים אגפיים ומחלקתיים שונים.

2. פרק: מודעות והדרכה. סעיף:20-24. עמוד: 8-9
מהיבט ההדרכה התבצע שינוי גדול : נציג אבטחת מידע מדריך בכל קורס עירוני. בקורס לעובדי חיוב וגביה חדשים משולבת דרך קבע הרצאה של אבטחת מידע. מתוכננים 2 קורסים באבטחת מידע (קורס אבטחת מידע כללי וקורס נאמני אבטחת מידע למפתחים). היתה תוכנית יחד עם מחלקת תכנון ופתוח משאבי אנוש העירונית לחייב כל עובד חדש להגיע לקורס אבטחת מידע אולם לא יצא לפועל. באגף מיחשוב מתבצעת הדרכה בנושא לעובדים חדשים. בוצעו מספר הדרכות לצוותי הפיתוח באגף, למפעילים, לרכזי המיחשוב ולצוות המזכירות.
מבחינת המודעות יש שינוי גדול לטובה, יחד עם זאת נדרשת עבודה נוספת נוכח הסיכונים הגדלים בתחום. בועדת היגוי לאבטחת מידע הנחה הסמנכ"ל שתתבצע עבודה בנושא יחד עם מנהל הידע העירוני.
מבחינת הכשרת עובדי מחלקת אבטחת מידע – כיום מתנהל קורס Cissp ייחודי בלמידה עצמית לכל עובדי המחלקה. הקורס מקיף את כל תחומי אבטחת המידע באופן מעמיק . בסיום הקורס העובדים יוכלו לגשת לבחינה לצורך קבלת התואר.

3. פרק: בקרה ואכיפה. סעיף:25-26. עמוד: 9-13.
א. הוכנה תוכנית בקרות, מצ"ב קובץ הבקרות. הוא מכיל בקרות יומיות, חודשיות, רבעוניות, חצי שנתיות ושנתיות.
ב. מבחינת הביצוע: מפורט בטבלה גם הביצוע בפועל (שלא תמיד נרשם). חלק מהבקרות לא מתבצעות עקב קשיי כ"א.
ג. בקרה היומית – בקרת אנטי וירוס מבוצעת ע"י אבטחת מידע במלואה, מתוכננת לעבור לספק החדש של שירותי מוקד התמיכה מ-4/2012.
ד. הבקרות על שינוי סיסמת קודן ובקרת הקו לנתיבי איילון - בוטלו, עקב ביטול הצורך בהם.
ה. ב - 2012 ימונה עובד שחלק מהמטלות שלו תהיינה אחריות על הבקרות.

4. פרק: אבטחה פיזית. סעיף:27-29. עמוד: 13-14.
בוצעה חלוקה של סביבת העבודה למעגלי האבטחה.

רחוב אבן גבירול 69, תל-אביב-יפו 64162 טלפון מנהל האגף: 03-5218505, פקס: 03-5216424

א. חדר מחשב ומרכז התקשורת בבנין הראשי - במסגרת הבינוי שהתבצע בבנין הראשי נסגרו כל הכניסות, הכניסה מתבצעת באמצעות כרטיס מגנטי לפי רשימת מורשים. קיים ומיושם נוהל בקרה לנוכחים בחדר מחשב. קיים גם נוהל לליווי עובדים חיצוניים החייבים לעבוד בחדר מחשב. החדרים מבוקרים ע"י מצלמות.
ב. חדר המחשב ומרכז התקשורת במנהל הנדסה – התבצעה ומתבצעת פעילות של העברת השרתים לחדר מחשב בבנין המרכזי. חדר זה נעול והמפתחות נמצאים בהנהלת הבית ואצל מנהל הרשת.
ג. מרכזי התקשורת והחשמל בבנין הראשי נעולים.
ד. חדר מנהלי הרשת (אזור רגיש) נעול בקודן.
ה. חדר מנהלי הרשת במנהל הנדסה – נעול.
ו. חדרי אבטחת מידע בצייטלין נמצאים במתחם נעול (אינו נגיש לעובדים לא מורשים).
התבצעו מספר בקרות אבטחה פיזית. העובד שבצע את העבודה עבר לתפקיד אחר. הבעיה היתה שהיחידות ביקשו, בסיום כל ביקורת, שאבטחת מידע יממנו את תיקון הממצאים. לאחר מספר בקרות כשהבנו שאין תועלת בבקרות – הן הופסקו.

5. פרק: נתיב בקרה. סעיף:30 עמוד: 14.

"אין לי ספק שהמצב השתפר מבחינת המודעות לנושא והפעילות המתבצעת בהקשר זה".
נתיב הבקרה נדרש לכל פעילות (ברמת מערכת הפעלה, ברמת התשתית, ביישומים). בנוסף נדרשת בקרה על הרישום בכל נתיבי הבקרה. הרישום הוא בהיקף של מליוני תנועות ביממה ואין אפשרות אנושית לקרוא את כל הלוגים ובמיוחד לא לעשות קורלציה בין הלוגים השונים.
מבחינת מערכת ההפעלה – הרישום מתבצע באופן שוטף בכל המערכות (בשרתים, ברכיבי האבטחה השונים...).
הוטמעה מערכת mom מתוצרת מיקרוסופט שמדווחת לגורמים שונים באגף על אירועים ספציפיים במערכות ההפעלה (אני מקבל מיילים על אירועי אבטחה – למשל הוספת לקוח לקבוצת Domain Admins).
מבחינת התשתיות – בסיסי הנתונים – הנושא מטופל ע"י צוות ה - DBA.
מערכת נת"ע שהוטמעה ע"י מחלקת אינטגרציה באגף מכילה רישום מפורט של כל הפניות אליה.
מבחינת יישומים - מתודולוגית הכתיבה המאובטחת ובדיקות אבטחה של היישומים מתייחסים בקפדנות לנושא זה .
(הדבר אינו נכון לגבי יישומים קנויים). המערכות האחרונות שעלו, מחו"ג וחות"ם, עונות על דרישה זו.

6. פרק: מנהלי מאגר. סעיף:37-39 עמוד: 15.
במשך מספר שנים אחרי הדו"ח הקודם, הופץ לכל מנהלי המאגרים מכתב המפרט את מחויבויותיהם על פי החוק. עקב עליית המודעות לאבטחת מידע בכלל אנו רואים הקפדה רבה יותר מבעבר על אישור ההרשאות (לדוגמא גב' ע. ס.).

7. פרק: טיפול במתן הרשאות. סעיף:40-47 עמוד: 16-15.
לגבי משך הטיפול בהרשאות, הערכת הזמן תלויה בבקשת ההרשאה עצמה. כך לדוגמא יש טפסים רבים שעוברים 4 תחנות באבטחת מידע (אישור הבקשה, הגדרת הרשאות בסביבה המבוזרת, הגדרת הרשאות במחשב המרכזי, הגדרת הרשאות ביישום למשל מחו"ג או חות"ם).
מתבצעת פעילות פיתוח חדשה לביצוע הגדרות בצורה ממוחשבת ואוטומטית בסביבה המבוזרת עם אינטגרטור חיצוני. התוכנה מתוכננת גם לענות על הצורך במיפוי מדויק יותר של הרשאות הלקוח.
מתבצעת בקרה רבעונית לנעילת משתמשים שבמסגרתה עובד שהפסיק את עבודתו ננעל, מבוטלות הרשאותיו ברשת, ומבוטלות הרשאותיו במערכת מחו"ג – שבה עלות הרשיון היא כ 800 יורו.

8. פרק: Dba סעיף:48-49 עמוד: 17.
מחלקת ה Dba מבצעת בקרות משלה על בסיסי הנתונים.
מוצר סנטריגו שהוטמע בחלק מבסיסי הנתונים משפר את מצב האבטחה של בסיסי הנתונים.
המשתמש הגנרי הבעייתי הוא משתמש Sa המשמש את עובדי מחלקת dba לצרכים רבים.
עבודת משתמש זה הוגבלה ל 4 מחשבים (ח., י., א. וא.), נקבע שהסיסמא תהיה שונה בין הדומיינים השונים ובחלק מהסביבות. שונתה פעם אחת הסיסמא.
במסגרת הניטור השוטף של סנטריגו נרשמות פעולות חריגות אבטחתית בבסיסי הנתונים שבהם מוטמע הסנטריגו.
נשכר עובד בהיקף 500 שעות לשנה שתפקידו לבצע " אבטחת בסיסי נתונים ". נכתבה טיוטת מתודולוגיה לאבטחת בסיסי נתונים.
בקרת היישומים כוללת כמובן גם היבטי אבטחה של בסיסי הנתונים מבחינה אפליקטיבית.

9. פרק: סקר סיכונים. סעיף:52-57
בעקבות החלטה של מנהלת האגף מותנע בימים אלו סקר סיכונים, הכולל אף הקצאת שעות לבדיקת התיקון. סקר הסיכונים מתבצע על 3 דומיינים (רשת העירייה, אתר האינטרנט העירוני, רשת ארגון העובדים). לדומיין החדש שהוקם לאחרונה (חוות תקשוב החינוך) התבצע נסיון פריצה, נסיונות אלו מסייעים באישוש / תיקוף הסיכונים שהוגדרו, בת"ע 2012 תוקצבו 2 נסיונות פריצה לרשת, שיסייעו באיתור הסיכונים.

10. פרק: יכולת הניטור והמעקב. סעיף:58-61 עמוד: 18-19.
ראו התייחסות בסעיף 8 לעיל.
<u>חיוויים</u> - יחידת אבטחת מידע מקבלת כיום חיוויים מ 4 תוכנות מרכזיות: מערכת האנטי וירוס (Symantec Endpoint Protection), מערכת Mom, מערכת setntrigo (בסיסי נתונים) ומערכת ה spectrum לשליטה ובקרה.
<u>ניטור אתרי האינטרנט העירוניים</u> - במהלך 2011 נרכש מוצר לניטור וגיבוי אתרי אינטרנט.
המוצר כולל ביצוע גיבוי שבועי של אתר האינטרנט העירוני, ניטור האתר (אנושי – בשעות העבודה) ויכולת מעבר לאתר חלופי בענן מיקרוסופט. בימים אלה נרכשת גירסא מתקדמת יותר של המוצר.
ל 2012 מתוכננת רכישת שירות siem\soc לשיפור יכולות הניטור והתגובה לאירועי אבטחה.

11. פרק: רכזי המיחשוב סעיף:67-69 עמוד: 20.
מנקודת מבטה של יחידת אבטחת מידע, רכזי המיחשוב הם שותפים מרכזיים, וככאלה מקבלים שירות בהתאם. חלק מפניות הלקוחות לאבטחת מידע מחויבות במעורבות רכז המיחשוב (למשל מתן הרשאה). התקיימו אף 2 ישיבות עם רכזי המיחשוב לליבון סוגיות שונות באבטחת מידע.

12. פרק: תחומי אחריות וסמכות...באבטחת מידע. סעיף 72 עמוד 20.
העבודה התפעולית מתחלקת היום בין 2 תחומים (סביבת ה perimitter והסביבה הפנימית) ומתבצעת העברת משאבים לצרכים שוטפים ולצרכי התמקצעות.
<u>בתחום המתודולוגי</u> מתבצעת העבודה ע"י 3-4 אנשים: ח. נ.., י.. ח.., מ.. מ.. ובנושאים ספציפיים – מ.. ק... נכתבו (הורחבו) לאחרונה 3 רכיבי מתודולוגיה: מתודולוגיית אבטחת בסיסי נתונים, מתודולוגיית כתיבה מאובטחת, ריכוז דרישות אבטחה למוצרי תוכנה נרכשים (מוצרי מדף או מוצרים המפותחים במיוחד עבור העירייה).
<u>תוכניות העבודה השנתיות</u> מגובשות במחלקה בשיתוף אותם גורמים.
<u>בתחום התכנון ארוך הטווח</u> (אסטרטגי) מתבצעת עבודה עם חברת ייעוץ (קיוריטי) שבה משתתפים מצד העיריה ח.. ומ...

13. פרק: שחזור סיסמא. סעיף 75-73 עמוד 21
מוקד השירות אינו מורשה ואינו מבצע שחרור משתמשים הנעולים ב disabled.
אין מעקב אחר קיום/אי קיום הנוהל.
במהלך 2011 התקיים פיילוט למימוש האפשרות של שחרור סיסמא **ע"י משתמש הקצה** (ע"י התחברות לפורטל הפנימי, מענה על שאלות שתשובותיהן קיימות במערך משאבי אנוש ובחירת סיסמא חדשה). הפיילוט נערך בשיתוף מחלקת אינטגרציה והוקצה תקציב לפעילות זו במהלך 2012.

14. פרק: שירותי האנטי וירוס סעיף 78-76 עמוד 21
שירותי האנטי וירוס העירוניים מבוצעים בכל הרשתות (עירייה, ארגון, אתר האינטרנט העירוני, אתר תקשוב החינוך).
שירותי האנטי וירוס מורכבים מ: אנטי וירוס ב perimitter מתוצרת safenet שמבקר כל מה שנכנס ויוצא מהרשת העירונית (תקין), אנטי וירוס בתוך ה exchange מתוצרת Microsoft ומורכב מ 4 מנועים שונים (תקין), אנטי וירוס בתחנות ובשרתים (ראה פירוט להלן), ואנטי וירוס forfront מתוצרת Microsoft בשרתי ה - mos (לא מוטמע באופן מלא).
ב 3 שנים האחרונות השתמשה העירייה ב trendmicro כמוצר האנטי וירוס בתחנות ובשרתים. המוצר לקה בחסר ב3 תחומים: יכולות ניהול גרועות, התנתקות תחנה או מעבודה מול השרת (שמשמעותה הפסקת קבלת עידכונים ופקודות משרת הניהול) ויכולות תמיכה גרועות. הוחלט לעבור למוצר אחר ובוצע פיילוט עם חברת מיקרוסופט להטמעת Forefront כאנטי וירוס העירוני. הפיילוט נכשל והוחלט לעבור ל sep המספק אנטי וירוס ויכולות נוספות. נכון לחודש נובמבר 2011 בוצע מעבר לכ -4050 תחנות עבודה ושרתים. לקראת סוף השנה תעבור כל העירייה למוצר החדש.

ג. התייחסות מנהלת מחלקת שרות וקשרי לקוחות :

1. עמ' 9 סע' 26 א' בנושא בקרה יומית: נכתב כי "..בנוסף נמצא כי הפעילות לבדיקת תשובות מוקד השירות av אינה מבוצעת כלל".אבקש לקבל הסבר למשפט זה. על איזה שירות שמבצע המוקד מדובר?

2.עמ' 21 סע' 73 בנושא שחזור חסימה: יש לשנות את המשפט "כ 30% בממוצע מהפניות אל מרכז השירות עוסקות בנושא סיסמאות". (ולא בשחזור סיסמא).

3. עמ' 21 סע' 77- יציין כי השימוש בכלי ה- damware מבוצע באישור ובידיעת מנהלת האגף, מתוך הבנת המצוקה הקיימת בצורך במתן שירות ללקוחות, כאשר קיים פער בתשתיות הקיימות לצורך כך. מפעילי המוקד הונחו לבקש תחילה את אישור הלקוח להשתלטות על התחנה.

העתק :
מנהלת מחלקת שרות לקוחות ותפעול .
מנהל אבטחת מידע

רחוב אבן גבירול 69, תל-אביב-יפו 64162 טלפון מנהל האגף: 03-5218505, פקס: 03-5216424

סודר	ממצא	עמוד	פעולה	לו"ז	הערות
1	מדיניות ועקרונות - סעיף 9 - מדיניות אבטחת מידע	5	יעודכן מסמך מדיניות אבטחת מידע בהתאם לשינויים הטכנולוגיים ויועבר לאישור הנהלת העירייה	30.4.2012	
2	מדיניות ועקרונות - סעיף 10 - נאמני אבטחה	5	מתוכנן קורס לגמל לנאמני אבטחת מיע בפיתוח.		
3	נהלים - סעיף 18-14 - כמות הנהלים והוראות העבודה המפורסמים באתר	6	תוגדל כמות הנהלים והוראות העבודה ל 35. הנהלים הקיימים יעברו ריענון.הנהלים יוסבו לתבנית נוהל סטנדרטית של האגף.יעודכן תאריך הכתיבה ותאריך התוקף.	31.8.2012	
4	אחריות מנהלים - סעיף 19	8	תוכנה 2 פניות: האחת למנהלי המאגרים והשניה פניה למנהלים בעירייה.	1.3.2012	
5	מודעות והדרכה - סעיף 22 ה. הדרכת עובדים חדשים	9			
6	מודעות והדרכה - סעיף 24 - לעובדי אבטחת מידע	9	כמעט כל חברי הצוות משתלבים בקורס ייחודי - cissp. תוכן תוכנית הדרכה למחצית השניה של 2012	30.6.2012	
7	בקרה ואכיפה - 26 א + ב	9	תוספת כ"א המאושרת ל 2012 תפנה משאבים לביצוע קפדני יותר של הבקרות והוספת בקרות. לגבי פעילות המוקד בנושא av - ההסכם החדש מחייב ביצוע בקרה זו על ידיהם.	1.2.2012	
8	בקרה ואכיפה - סעיף 26	10			
9	אבטחה פיזית - סעיף 27	13			
10	נתיב בקרה - סעיף 30	14	במהלך 2012 חוטמע שירות siem\soc שינטר וידווח על אירועי אבטחת מידע ברשתות העירוניות. תגבור יכולות אבטחת היישומים יתרום רבות לשיפור המצב במערכות החדשות.	31.8.2012	
11	כרטיס חכם - סעיף 31	14	ההטמעה בצמוד לפרוייקטים.		
12	מחשבים ניידים ו dok - סעיף 34	15	אנחנו קרובים לסיום הפיילוט הכולל: מניעת שימוש ב dok+ הפעלת עמדת הלבנה. היכולת למניעת שימוש ב dok+cd+dvd קיימת ולא מופעלת. יש תקמיב לעמדות הלבנה. בסיום הפיילוט יוכן מתווה להטמעה.	31.12.2011	
13	מנהלי מאגר - סעיף 37	15	יוקם פורום מנהלי מאגרים שדרכו תופצנה הודעות שוטפות למנהלי המאגרים. תמשך הפצת האגרת השנתית למנהלי המאגר. בכל פניה כזו יקבל מנהל המאגר את שמות כלל המורשים למערכות שבאחריותו.	31.5.2012	
14	טיפול במתן הרשאות - סעיף 47	16	במסגרת העבודה עם חברת איירוקס על ביצוע אוטומטי של טפסי אבטחת מידע, מתוכנן מודול דיווח המציג את הרשאות הלקוח למערכות (ולא לספריות). זה יאפשר הצגה קלה של הרשאות הלקוח בצורה מובנת.	30.6.2012	
15	צוות ה dba - סעיף 48	17	יקבע נוהל להחלפת סיסמת המשתמש הגנרי. יקבע נוהל בקרות על ניהול בסיסי הנתונים.		
16	פרוייקט ה - odrpסעיף 50	17	אבטחת מידע ישתלבו בפרויקט ה cmdb להוספת שדה רגישות אבטחתית במערכת		
17	סקר סיכונים - סעיף 52	18	מתבצע כיום סקר סיכונים ע"י חברה חיצונית. בסיומו יוגש דו"ח ויתבצעו תיקונים לפי המימצאים.	31.3.2012	

18	יכולת ניטור ומעקב - סעיף 58	18	תותקן מערכת forsigh air לניטור וגיבוי אתרי האינטרנט העירוניים. ירכש שירות siem\soc שידווח (דרך רכיבי ניטור שונים) על אירועים חריגים במערכת.	28.2.2012	
19	יכולת ניטור ומעקב - סעיף 59 - זליגת מידע	18	נבחן יישום sep כרכיב מניעת זליגת מידע בתחנות הקצה. במהלך 2012 יבחנו מוצרים למניעת הזליגה ב perimitter.	1.7.2012	
20	יכולת ניטור ומעקב - סעיף 60 - ניטור אבטחתי	19	ירכש שירות siem\soc שידווח (דרך רכיבי ניטור שונים) על אירועים חריגים במערכת.	1.9.2012	
21	יכולת ניטור ומעקב - סעיף 61 - בקרה על בסיס הנתונים	19	תורחב הבקרה על בסיסי הנתונים באמצעות מוצר שנרכש	1.6.2012	
22	תחומי אחריות - סעיף 72	20	בתהליך הכנה תוכנית אסטרטגית לאבטחת מידע	30.4.2012	בשיתוף חברת קיוריטי
	שיחזור סיסמא - סעיף 73	21	אושר לביצוע פרוייקט החלפת סיסמא (שנשכחה) ל 2012. ירוענן הנוהל מול מוקד השירות.יוכנס נוהל בקרה תקופתית לאימות ביצוע הנוהל ע"י מוקד השירות.	1.9.2012	
	אנטי וירוס - סעיף 87	23	כרגע בביצוע החלפה לתוכנת סימנטק המאפשרת הגנה וניהולה בצורה טובה יותר. תתבצע במהלך 2012 השלמת הטמעת forefront בכל שרתי mos.		