12 דצמבר 2024
י״א כסלו תשפ״ה
סימוכין: 2024-0103-1106

<u>דו״ח מישיבה מס׳ 12 של ועדת ביקורת</u>
<u>שהתקיימה ביום שלישי, ז׳ באלול התשפ״ד (10.9.2024)</u>

השתתפו: מר אלדד רבינוביץ, חבר מועצה ויו״ר ועדת ביקורת

נכחו: גב׳ עופרה ברכה, מבקרת העירייה והמורשה לטיפול בתלונות
עו״ד דני ליבמן, משנה ליועמ״ש לנושאים מיוחדים
מר ציון סמולר, מנהל אגף הגנת סייבר
מר דודו אמזלג, סגן מנהל אגף התקציבים וממונה על ההוצאות
מר ינון נוימן, מנהל אגף לביקורת ובקרת יועצים
גב׳ אורטל אריה, מנהלת מחלקה בכירה, לפיתוח תכנון ובקרה
רו״ח שלומי בני, יועץ הביקורת
מר צבי עבו, מזכיר ועדת ביקורת

<u>על סדר היום נדון הנושא הבא:</u>
דוח מבקרת העירייה לשנת 2023 בנושא: אבטחת מידע וסייבר

<u>פתיחת הדיון:</u>
<u>מר אלדד רבינוביץ, יו״ר הוועדה</u>: מתכבד לפתוח את הדיון בוועדת ביקורת מספר 12- אבטחת מידע וסייבר.
חלמנו כשנגיע לארץ אבותינו נגיע למנוחה ונחלה. ברוך השם הגענו לכאן, אבל מנוחה ונחלה עדיין אין לנו.
יש הרבה איומים בסביבתנו, לצערי כולנו חווים אותם יום יום. יש איום משמעותי מאוד שקצת פחות מכירים אותו- איומי מחשב. אלו איומים ממשיים ומשמעותיים, עם הרבה מאוד השלכות לעולם הפיסי שלנו. כולנו שומעים קצת בחדשות על מה שאנחנו עושים לאחרים ועל מה שאחרים שעושים לנו, זה אירוע משמעותי וצריך להיערך לו.
זה תחום שקשה להבין בו, הוא מאוד מקצועי, משתנה מהר ולא מספיק מוחשי. לא תמיד תוכל לדעת שהותקפת ולא תמיד תוכל לדעת מה מצבך. הביקורת נעשתה כדי שתחום חשוב זה לא יוזנח והעירייה משקיעה הרבה מאוד כדי שזה לא יוזנח.

<u>גב׳ עופרה ברכה, מבקרת העירייה</u>: מדובר בנושא רלוונטי ועדכני לתקופתנו והמלצותיו מחייבות תיקון ומניעת הישנותם.

<u>דיון הוועדה:</u>

<u>פרק 1 - בדיקת רגולציה, מדיניות, נהלים ותהליכים בתחום אבטחת מידע וסייבר</u>

<u>המלצת המבקרת:</u>

- לסיים את מסמך המדיניות, להציגו ולאשרו בהנהלת העירייה ולפקח על יישומו.
- לעדכן את נוהלי אבטחת המידע ולכלול את כל ההיבטים שהשתנו מאז כתיבתם, לאשרם בהנהלת העירייה, לדאוג לתקף אותם אחת לשנה (או בעת שינוי בתהליכי העבודה של העירייה, המוקדם מביניהם), ולוודא תאימות מלאה לפורטל העירייה.
- להקים ועדת היגוי שתורכב מכמה גורמים מדיסציפלינות שונות, אשר תתכנס אחת לתקופה, תתווה מדיניות, תפקח, תעדכן ותייעץ להנהלת העירייה בקבלת החלטות בנושא אבטחת מידע וסייבר.

<u>תגובת המבוקר:</u>

קיים נוהל לא רשמי, כיוון שוועדת ההיגוי טרם הוקמה. לאחר שהיא תוקם, היא תבחן את הנוהל, תשנה ותשלח לתיקוף.

על מנת שהוועדה תוקם בצורה מיטבית, יש להתייעץ עם ממונה על טכנולוגיות מידע בנוגע לאיוש התפקידים בה והגדרות עבודתה.

<u>המלצת ועדת ביקורת:</u>

לקבל את המלצת הביקורת.

הקמת ועדת ההיגוי משמעותית מאוד ויש להקימה בהקדם בהתייעצות עם גורמי המקצוע בעירייה.

<u>המלצת המבקרת:</u>

- לעדכן את נוהל הגיבויים והשחזורים של העירייה לרבות כל ההיבטים שהשתנו בתהליך הגיבויים והשחזורים משנת 2016 ועד היום, לאשרו בהנהלת העירייה ולדאוג לתקף אותו אחת לשנה או בעת שינוי בתהליכים האמורים, המוקדם מביניהם.
- לעבות את הצוות ביחידת אבטחת המידע ולספק לה את המשאבים הדרושים למילוי תפקידיה.
- להפריד את חדרו של מנהל יחידת אבטחת המידע ולהתקין מנגנון נעילה לדלת.

<u>תגובת המבוקר:</u>

נעשו כבר מספר שינויים ויש תכנית עבודה למשך. מדובר באירוע יקר מאוד ונדרש תקציב ייעודי.

<u>המלצת ועדת ביקורת:</u>

לקבל את המלצות הביקורת תוך בחינת אופן היישום בצוות לתיקון ליקויים בראשות המנכ"ל ותקצוב האגף בהתאם.

<u>המלצת המבקרת:</u>

- לקיים תהליך הערכת סיכונים לעירייה - לרבות מיפוי הסיכונים שאליהם היא חשופה, רמת הקריטיות של כל סיכון, העוצמה הסבירות וכו', ובהתאם לתוצאותיו להכין תוכנית עבודה לצמצום הסיכונים שזוהו.
- לבצע סקר טכנולוגי אחת ל-18 חודשים לפחות במאגרי מידע שחלה עליהם רמת אבטחה גבוהה. סקר כזה יאפשר לעירייה לאתר חולשות וסיכוני אבטחת מידע ברשת ובמערכות העירייה, ולבצע תכנון נכון של תקציב אבטחת המידע וחלוקת המשאבים לטיפול בחשיפות.

תגובת המבוקר:
במקביל לתהליך הביקורת נעשה סקר יחד עם חברה מובילה ומקצועית וניתן דו"ח בהתאם לכללי ניסט.

המלצת ועדת ביקורת:
לקבל את המלצות הביקורת.

המלצת המבקרת:
- לא להעלות מערכות לאוויר ללא ביצוע מבדקי חדירה ותיקון הליקויים שנמצאו.
- להכין תוכנית עבודה לטיפול בממצאים בהתאם למבדקי החדירה בתוך פרק זמן סביר בהתאם לדרגת הסיכון.
- לבצע תהליך הערכת סיכונים אשר יכלול את סיווג רמת האבטחה הנדרשת בהתאם לתקנות הגנת הפרטיות, ובהתאם לכך לבחור את המערכות הרלוונטיות לביצוע מבדקי חדירה אחת ל-18 חודשים לפחות.
- בהתאם לתהליך הערכת הסיכונים, להגדיל באופן ניכר את כמות מבדקי החדירה המבוצעים מדי שנה גם למערכות נוספות מעבר לדרישה של תקנות הגנת הפרטיות.

תגובת המבוקר:
התקיימה ישיבה עם מנהלת הפיתוח שכפופה למנמ"רית החדשה בנוגע למערכות. הועברה הנחייה שכל מערכת חדשה שעולה לאוויר מחויבת מבדק חדירה. ישנן מערכות אופציונאליות נוספות. אציין שאנו מקדמים הסכם לבדיקות קבועות דרך חברת משכ"ל במימון של המרכז לשלטון המקומי.

המלצת ועדת ביקורת:
לקבל את המלצת הביקורת.

המלצת המבקרת:
- שירותי בדיקות אבטחת מידע, לרבות מבדקי חדירה, יינתנו על ידי ספקים חיצוניים אשר אינם קשורים באופן ישיר או עקיף לחברת נס. ספקים אלו ייבחרו על ידי העירייה ואף את התשלום עבור שירותיהם תבצע העירייה.

תגובת המבוקר:
ההמלצות מקובלות.

המלצת ועדת ביקורת:
לקבל את המלצת הביקורת.
בנוסף, להמליץ למנכ"ל ולצוות לתיקון ליקויים לבחון עם הייעוץ המשפטי לעירייה את הצורך בהחתמת הבודקים וחברת נס על מסמך ניגוד עניינים הדדי.

המלצות המבקרת:
- לבחון את אחריות העירייה בדבר יישום תקנות PCIDSS. בהתאם לאחריות העירייה למפות את הפערים בין המצב הקיים לדרישות התקן וליישמן בהתאם עד לסגירת הפערים. נוסף על כך לפקח על יישום הוראות התקן של צד ג' שבו נעזרת העירייה לסליקת כרטיסי האשראי.

תגובת המבוקר:
העירייה עומדת בכל הדרישות והתקנים בנוגע לרשת PCI.

כיכר ספרא 1, ירושלים 9100707 | טל: 02-6295723 פקס: 02-6297153 :Fax Tel
mazkir_haeir@jerusalem.muni.il

המלצת ועדת ביקורת:
לקבל את המלצת הביקורת.

המלצות המבקרת:
- להחליף סיסמה למשתמשים האפליקטיביים אחת לתקופה בהתאם למדיניות שתיקבע.
- לערוך סקירה תקופתית לרשימת המורשים להשתמש במכשירים ניידים.
- להעריך את היקף הנזקים הכלכליים הצפויים מאירוע סייבר ולאחר מכן לבחון את כיסוי פוליסת הביטוח בגינם.

תגובת המבוקר:
הטיפול במשתמשים האפליקטיביים קיים בתוכנית העבודה, כבר בוצע הרבה.

המלצת ועדת ביקורת:
לקבל את המלצת הביקורת תוך בחינת אופן היישום בצוות לתיקון ליקויים בראשות המנכ"ל ובחינה של הסוגיה הביטוחית עם מומחי ביטוח.

המלצות המבקרת:
- לבצע שחזורים יזומים לפי סבב שרתים, מערכות ובסיסי נתונים אחת לתקופה שתיקבע מראש, לצורך בדיקת זמינות, שלמות ודיוק הגיבויים.
- להחליף את המערכות שהוגדרו EOL במערכות חדשות הנתמכות על ידי היצרנים. עד להחלפת המערכות הנ"ל לבצע מבדקי חדירה במטרה לזהות פגיעויות ברמת סיכון קריטית וגבוהה ולאתר בקרות מפצות כנגד פגיעויות אלו.

תגובת המבוקר:
ההמלצות מקובלות, בכפוף לתקציב. יש מערכת אוטומטית עם גיבוי ושחזור, עובדים על שיפור והגדלה שלה.

המלצת ועדת ביקורת:
לקבל את המלצת הביקורת.

פרק 2 - מבדק מערכות אבטחת מידע

המלצת המבקרת:
- להסיר את החוקים שאינם בשימוש.
- לוודא כי כל החוקים של ה-FW יירשמו בלוג.
- להגדיר במערכת ה-FW פעולה לשליחת דוחות שבועיים למנהל אבטחת המידע.
- להגדיר במערכת ה-FW שמירת לוג אירועים לתקופה של 24 חודשים לפחות.
- להקשיח את פרוטוקול LDAP ולשנות את הפורטים ל-686 בצורה מוצפנת.
- לבחון חיבור כלל המשתמשים במערכת ל-AD הארגוני.
- להגדיר במערכת ה-FW שינוי סיסמאות המשתמשים אחת לתקופה.
- להסב מערכות הפעלה אשר אינן נתמכות על ידי היצרן למערכות הפעלה נתמכות (וכן למחוק מערכות אשר אינן בשימוש).
- להגדיר הקשחות במחשבים בהתאם לשיטות עבודה מקובלות ולהסיר פרוטוקול ישן.
- לבצע שינוי הגדרות מידע ולהחליף סיסמאות לפחות אחת ל-180 יום.

כיכר ספרא 1, ירושלים 9100707 | טל: 02-6295723 Tel פקס: 02-6297153 :Fax
mazkir_haeir@jerusalem.muni.il

- ליישם בקרה בכלל השירותים לפי שיטות עבודה מקובלות באופן הבא:
- Account Logon / Kerberos Service Ticket Operations– Success & Failure
- Detailed Tracking / DPAPI Activity– Success & Failure
- Privilege Use / Sensitive Privilege Use– Success & Failure
- לבצע שינוי הגדרות ולא לשמור סיסמאות בתוך קובצי ה-GPO.
- לקבוע מדיניות סיסמאות ב-Default GPO לפי המדיניות המומלצת:
- https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc770842(v=ws.10)?redirectedfrom=MSDN
- למחוק GPO אשר אינו בשימוש.
- לבטל את האובייקטים אשר אינם בשימוש יותר מחצי שנה.
- להגדיר מדיניות סיסמאות נאותה לכל המשתמשים במערכת.
- לתת הרשאה לאובייקטים.
- לבצע הקשחה לחשבונות האדמיניסטרטורים באמצעות דרישת אישור בעת הענקת הרשאות.
- לשקול יישום ההגדרה ב-AD כדלהלן: "Account is sensitive and cannot be delegated".
- לבדוק אחת לחודש לפחות, אם קיימים עדכונים לשרתי ה-SQL. לכשיימצאו עדכוני אבטחת מידע בעלי חשיבות גבוהה, יש לבצע עדכון ללא דיחוי.
- להגדיר במערכת שליחת דוחות תקופתיים למנהל אבטחת המידע לגבי סטטוס עדכוני האבטחה בעירייה.

<u>תגובת המבוקר:</u>
המלצות הביקורת מקובלות, חלק בוצע וחלק בתהליך.

<u>המלצת ועדת ביקורת:</u>
לקבל את המלצות הביקורת.

<u>פרק 3 - מבדקי חדירה למערכות</u>
<u>המלצת המבקרת:</u>

- להגביל את הקלט שניתן להקליד במערכת מצבת הנכסים, במטרה למנוע הזרקות SQL. הסינון הטוב ביותר הוא להגדיר רשימת ביטויים ספציפיים שניתן להכניס לקלט. לחלופין ניתן להגדיר הזנה מרבית של אותיות ללא סימנים מיוחדים (לדוגמה עד 8 אותיות ללא מספרים או תווים מיוחדים - גרש סימון שווה, מירכאות וכדומה). סינון כזה ימנע את רוב התקפות ה-SQL. הטמעת מערכת WAF תמנע הזרקות SQL למיניהן. נקיטת צעדים לסניטיזציה (חיטוי קוד) בצד הלקוח תשמש שכבת הגנה נוספת מפני הזרקות.
- לעדכן את הרכיבים הישנים במערכת מצבת הנכסים כדי למנוע ניצול של הפגיעויות.
- ליישם מנגנוני הגנה שונים מפני התקפה מסוג XSS במערכת מצבת הנכסים. העיקריים שבהם: אימות קלט: וידוא כי ניתן להזין רק תווים רלוונטיים בשדות הרלוונטיים. הטמעה של מערכת WAF יכולה לסייע בבלימת התקפות Cross-Site Scripting ולהוסיף שכבות הגנה ברמה היישומית.

- ליישם מנגנוני הגנה שונים מפני התקפה מסוג XSS במערכת מצבת הנכסים. העיקריים שבהם: אימות קלט; וידוא כי ניתן להזין רק תווים רלוונטיים בשדות הרלוונטיים. הטמעה של WAF יכולה לסייע בבלימת התקפות Cross-Site Scripting ולהוסיף שכבות הגנה ברמה היישומית.
- להשתמש בהצפנה ברמת התעבורה (SSL/TLS) כדי להגן על כל התקשורת העוברת בין הלקוח לשרת במערכת מצבת נכסים.
- להשתמש בכותרת ה-HTTP Strict-Transport-Security כדי לוודא שלא יבוצע חיבור לא מאובטח של מערכת מצבת נכסים.
- להחיל את ה-HttpOnly flag + Secure על כל העוגיות במידת האפשר במערכת מצבת נכסים.
- לעדכן את הרכיבים הישנים במערכת מצבת תלמידים כדי למנוע ניצול של הפגיעויות.
- ליישם את הנחיות האבטחה כדלהלן במערכת מצבת תלמידים:
- להשתמש בהצפנה ברמת התעבורה (SSL/TLS) כדי להגן על כל התקשורת העוברת בין הלקוח לשרת.
- להשתמש בכותרת ה-HTTP Strict-Transport-Security כדי להבטיח שלא יבוצע חיבור לא מאובטח של המערכת.
- להחיל את ה-HttpOnly flag + Secure על כל העוגיות במידת האפשר במערכת מצבת תלמידים.
- כדי לחסום את מצב debug יש ליישם את ההנחיות המפורטות להלן:
  - לערוך את קובץ Web.config עבור האפלקציה.
  - לאתר את הרכיב <compilation> בקטע <system.web>.
  - להגדיר את ערך ה debugging ל-"false".
  - לוודא שתכונת ה-debug ברכיב <compilation> לא הוגדרה ל-"true" בקובץ Machine.config.
- להגביל את מספר הבקשות האפשרי לשליחה בשירותי שליחת SMS ואימייל למספר קבוע בשעה. מעבר לכך מומלץ לחסום את השימוש.
- לתעד את הלוגים באתר האינטרנט ולבצע ניטור ומעקב אחר פעולות לא שגרתיות כמו ריבוי בקשות ו/או ניצול רכיבים במערכת.
- לעדכן את הרכיבים המיושנים באתר האינטרנט כדי למנוע ניצול של הפגיעויות.
- להחיל את ה-HttpOnly flag + Secure על כל העוגיות באתר האינטרנט.
- לבצע הקשחה ברמת ה-Headers שצוינו. כמו כן, אין לחשוף מידע על אודות התשתית/הטכנולוגיה שבשימוש אתר האינטרנט.

<u>תגובת המבוקר:</u>
חלק מהמערכות מאוד ישנות וצריכות עבודה רבה, במיוחד המערכת הכספית. הפיתוח נכנס כבר לתוכנית העבודה.

<u>המלצת ועדת ביקורת:</u>
לקבל את המלצת הביקורת תוך בחינת אופן היישום בצוות לתיקון ליקויים בראשות המנכ"ל ושקילת מתן דגש פיתוחי ותקציבי על המערכת הכספית.

כיכר ספרא 1, ירושלים 9100707 | טל: 02-6295723 פקס: 02-6297153 Tel Fax:
mazkir_haeir@jerusalem.muni.il

<u>סיכום:</u>
מר אלדד רבינוביץ, יו"ר הוועדה: דנו בדו"ח חשוב מאוד בנושא שנראה שלא טופל כהלכה עד לכתיבת הדוח. נראה כי כעת יש שיפור גדול, מקווה שהשיפור ימשיך ומסקנות הדו"ח ייושמו.
מזכיר כי זה עתה דנו בדו"ח על מיגון תושבי העיר. בשנת 2021 יצא דו"ח חמור שהצביע על כשלים רבים. הדו"ח לא יושם והממצאים בו לא תוקנו, כך שאת המלחמה הזו התחלנו במצב טוב פחות ממה שהיינו אמורים להיות בו. גם בדיון שם הערנו שחייבים ליישם את הדוחות ולהכניס אותם לתוך תוכניות העבודה.
משמח לראות שמנהלי העירייה מתייחסים לביקורת וצמאים לתיקון. בסוף, דוח הביקורת הוא כלי עזר למנהלים. בע"ה מתקדמים.

הוועדה לענייני ביקורת ממליצה למועצת העירייה לאמץ את המלצות הביקורת כמפורט בדוח זה ותוך בחינת אופן היישום בצוות לתיקון ליקויים בראשות המנכ"ל.

הישיבה נעולה.

בברכה,

אלדד רבינוביץ
חבר מועצת העיר ירושלים
יו"ר ועדת ביקורת

Audit Committee | ועדה לענייני ביקורת | لجنة المراجعة
כיכר ספרא 1, ירושלים 9100707 | טל: 02-6295723 פקס: 02-6297153 :Fax
mazkir_haeir@jerusalem.muni.il