



ועדה לענייני ביקורת

26 נובמבר 2024
כ"ה חשון תשפ"ה
סימוכין: 2024-0103-1106

דו"ח משיבה מס' 12 של ועדת ביקורת שהתקיימה ביום שלישי, ז' באלול התשפ"ד (10.9.2024)

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

נכחו: גבי 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
גבי אורטל אריה, מנהלת מחלקה בכירה, לפיתוח תכנון ובקרה
רו"ח שלומי בני, יועץ הביקורת
מר צבי עבו, מזכיר ועדת ביקורת

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

פתיחת הדיון:
מר אלדד רבינוביץ, יו"ר הוועדה: 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 עושים 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.

גבי עופרה ברכה, מבקרת העירייה: מדובר בנושא רלוונטי ועדכני לתקופתנו והמלצותיו מחייבות תיקון ומניעת הישנותם.



ועדה לענייני ביקורת

דיון הוועדה:

פרק 1 - בדיקת רגולציה, מדיניות, נהלים ותהליכים בתחום אבטחת מידע וסייבר

המלצת המבקרת:

- 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.

תגובת המבוקר:

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.

המלצת ועדת ביקורת:

לקבל את המלצת הביקורת.

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

המלצת המבקרת:

- 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 תפקידה.
- להפריד את חדרו של מנהל יחידת אבטחת המידע ולהתקין מנגנון נעילה לדלת.

תגובת המבוקר:

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

המלצת ועדת ביקורת:

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

המלצת המבקרת:

- 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 וסיכונים אבטחת מידע ברשת ובמערכות העירייה, ולבצע תכנון נכון של תקציב אבטחת המידע וחלוקת המשאבים לטיפול בחשיפות.



ועדה לענייני ביקורת

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 המבקר:

- 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 המבקר:

- 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 המבקר:

- 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.

Audit Committee | ועדה לענייני ביקורת | لجنة المراجعة

כיכר ספרא 1, ירושלים 9100707 | טל: 02-6295723 Tel פקס: 02-6297153 Fax:

mazkir_haeir@jerusalem.muni.il



ועדה לענייני ביקורת

המלצת ועדת ביקורת:
לקבל את המלצת הביקורת.

המלצות המבוקרות:

- 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 המבוקרות:

- 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 ולאחר בקורות 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

המלצות המבוקרות:

- 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.

Audit Committee | ועדה לענייני ביקורת | لجنة المراجعة

כיכר ספרא 1, ירושלים 9100707 | טל: 02-6295723 Tel פקס: 02-6297153 Fax:

mazkir_haeir@jerusalem.muni.il



ועדה לענייני ביקורת

- 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](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. לכשימצאו עדכוני אבטחת מידע בעלי חשיבות גבוהה, יש לבצע עדכון ללא דיחוי.
- להגדיר במערכת שליחת דוחות תקופתיים למנהל אבטחת המידע לגבי סטטוס עדכוני האבטחה בעירייה.

תגובת המבוקר :

המלצות הביקורת מקובלות, חלק בוצע וחלק בתהליך.

המלצת ועדת ביקורת :

לקבל את המלצות הביקורת.

פרק 3 - מבדקי חדירה למערכות

המלצת המבקר :

- 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 לסניטזציה (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.



ועדה לענייני ביקורת

- 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 האפליקציה.
 - 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.

תגובת המבוקר:

חלק מהמערכות מאוד ישנות וצריכות עבודה רבה, במיוחד המערכת הכספית. הפיתוח נכנס כבר לתוכנית העבודה.

המלצת ועדת ביקורת:

לקבל את המלצת הביקורת תוך בחינת אופן היישום בצוות לתיקון ליקויים בראשות המנכ"ל ושקילת מתן דגש פיתוחי ותקציבי על המערכת הכספית.



ועדה לענייני ביקורת

סיכום:

מר אלדד רבינוביץ, יו"ר הוועדה: דנו בדו"ח חשוב מאוד בנושא שנראה שלא טופל כהלכה עד לכתובת 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

פרק שני

אבטחת מידע וסייבר

תוכן העניינים

בדוח זה הושמטו קטעים או צוינו פרטים באופן כללי ולא פרטני וזאת מטעמים של אבטחת מידע.

יצוין כי חשיפת הנתונים שהושמטו עלולה להביא לפגיעה באינטרס הציבורי וכי אין בהשמטתם כדי לשנות את ממצאי הדוח או את המלצות הביקורת.

תקציר // 3

מבוא // 9

פירוט הממצאים

פרק ראשון:

בדיקת רגולציה, מדיניות, נהלים ותהליכים בתחום אבטחת מידע וסייבר // 29

פרק שני:

מבדק מערכות אבטחת המידע // 49

פרק שלישי:

מבדקי חדירה למערכות // **הושמט**

סיכום // 54

תקציר

רקע

אבטחת מידע והגנת סייבר נועדו להגן על הארגון מפני גישות לא מורשות, חשיפת מידע, שיבוש פעילות, העתקה או השמדה של המידע ומערכות המידע - על ידי גורמים עוינים או בשוגג. אבטחת מידע והגנת סייבר נאותים פירושם הגנה על כלל השכבות, הכלים, הטכנולוגיות, רכיבי האחסון, קווי התקשורת, תחנות הקצה ועוד.

אבטחת מידע והגנת סייבר הם נושאים מורכבים ומאתגרים. אחד האתגרים המרכזיים בתחום זה הוא המהלך המובנה בו - שכלל שמוגברת רמת האבטחה של הארגון, כך גדל הקושי של המשתמש הפשוט (העובד) לבצע את המטלות הכרוכות בעבודה מול מחשב. לכן יש לשקול ולתכנן היטב את מבנה מערכות המידע וההגנה עליהן, גם אם מתוך הבנה ברורה שאין דרך לספק בתחום זה ביטחון והגנה מוחלטים.

הביקורת בדקה את המדיניות והנהלים בנושא אבטחת המידע, ביצעה מבדק טכנולוגי לבחינת רמת האבטחה הקיימת ביישומי אבטחת המידע (אנטי-וירוס, FW (חומת אש), AD (מערכת לניהול משתמשים) ומערכת עדכוני אבטחת מידע), בדיקה פיזית לאבטחת המידע, מבדקי חדירה לשתי מערכות ולאתר האינטרנט של העירייה.

הביקורת העלתה ליקויים מהותיים לגבי המדיניות ונוהלי אבטחת המידע, יישום הוראות חוק הגנת הפרטיות ותקנותיו; ניהול מערכת ה-AD ומערכת ה-FW, ליקויי אבטחת מידע בעלי חשיבות גבוהה במערכות אלו ובאתר האינטרנט של העירייה.

להלן רמת האבטחה כפי שהעריכה הביקורת לפי נושאי הדוח (ציון 5 הוא הגבוה ביותר):

תמונה 1: רמת אבטחה בעירייה על פי תוצאות הביקורת



עיקרי הממצאים

בדיקת רגולציה, מדיניות, נהלים ותהליכים בתחום אבטחת מידע וסייבר

1. בידי העירייה לא קיים מסמך מדיניות אבטחת מידע, ונוהלי אבטחת המידע לא עודכנו בה זה שנים רבות. נוסף על כך, חלק מהנהלים אינם מעודכנים וחלקם אף אינם מופיעים כלל בפורטל העירייה.
2. יחידת אבטחת המידע, האחראית לפיקוח בנושא אבטחת מידע בעירייה, מתקשה למלא כראוי את תפקידה בגלל תקציב נמוך באופן יחסי ומגבלות כוח אדם.
3. לא קיים תהליך הערכת סיכונים לבחינת הסיכונים הפוטנציאליים שאליהם חשופה העירייה בנושא אבטחת מידע ולא בוצע סקר סיכונים טכנולוגי זה שנים רבות.
4. לא קיימת בעירייה ועדת היגוי בנושא אבטחת מידע וסייבר אשר תתווה מדיניות, תפקח על יישומה ותסייע להנהלת העירייה בקבלת החלטות בתחום.
5. מערכת מסוימת, עלתה לאוויר ברמת אבטחת מידע נמוכה. ליקויים שנמצאו במבדק חדירה שבוצע לאחר העלייה לאוויר לא טופלו, נכון למועד הביקורת.
6. מבדקי חדירה מבוצעים מדי שנה לשיעור נמוך מאוד של מערכות ביחס למספר המערכות הקיימות בעירייה.
7. קיים ניגוד עניינים מובהק של חברת נס (ספק המחשוב העיקרי של העירייה). שירותים אשר נועדו לבחון את רמת אבטחת המידע של מערכות שפיתחה החברה (לדוגמה: מבדקי חדירה למערכת) וכן את מתן שירותי אבטחת המידע של החברה לעירייה באופן כללי, ניתנים על ידי ספק שעליו המליצה חברת נס עצמה, והתשלום עבור שירותיו מתבצע אף הוא דרך אותה החברה.
8. העירייה אינה עומדת בהוראות תקנות הגנת הפרטיות, לא בחנה את אחריותה בדבר יישום הוראות תקן PCI-DSS של חברות כרטיסי האשראי, ואינה מפקחת על יישום ההוראות הנ"ל של ספק צד ג', שבו נעזרת העירייה לסליקת כרטיסי האשראי.
9. נמצאו 35 משתמשים מסוימים שלא החליפו סיסמה יותר מ-3 שנים!
10. העירייה אינה מבצעת שחזורים יזומים במטרה לבדוק כי אכן ניתן לשחזר את המידע המגובה באופן שלם, מדויק ובזמן סביר.

מבדק מערכות אבטחת מידע

11. רמת התחזוקה של מערכת ה-FW (מערכת חומת האש) מתבצעת באופן חלקי ואינה מספקת.
12. רמת אבטחת המידע של מערכת ה-AD (מערכת מרכזית של העירייה לניהול המשתמשים) אינה תואמת את הסטנדרטים המקובלים של רמת אבטחת מידע, ובשל כך העירייה חשופה לסיכוני הדבקה ופגיעה פוטנציאליים.

מבדקי חדירה

13. נמצאו 6 ליקויי אבטחת מידע במערכת מסוימת, מהם 5 ליקויים בעלי חשיבות גבוהה. המערכת הוגדרה ברמת סיכון בינונית-גבוהה על ידי צוות הביקורת.
14. נמצאו 4 ליקויי אבטחת מידע במערכת נוספת, מהם 2 ליקויים בעלי חשיבות גבוהה.
15. נמצאו 4 ליקויי אבטחת מידע באתר האינטרנט של העירייה, מהם ליקוי אחד בעל חשיבות גבוהה.

המלצות מרכזיות

בדיקת רגולציה, מדיניות, נהלים ותהליכים בתחום אבטחת מידע וסייבר

1. לגבש מדיניות אבטחת מידע, להציגה ולאשרה בהנהלת העירייה ולפקח על יישומה.
2. לעדכן את נוהלי אבטחת המידע ונוהלי הגיבויים והשחזורים של העירייה, לכלול את כל ההיבטים שהשתנו מאז כתיבת הנהלים, לאשרם בהנהלת העירייה, לפקח על יישומם ולטעון את הנהלים המעודכנים לפורטל העירייה.
3. לעבות את הצוות ביחידת אבטחת המידע ולספק לה את המשאבים הדרושים למילוי תפקידיה.
4. לקיים תהליך הערכת סיכונים בתחום מערכות המידע בעירייה - לרבות מיפוי הסיכונים שאליהם היא חשופה, רמת הקריטיות של כל סיכון, העוצמה הסבירות וכו' - ובהתאם לתוצאותיו להכין תוכנית עבודה לצמצום הסיכונים שזוהו. נוסף על כך, לבצע סקר סיכונים טכנולוגי בעירייה, וממנו לגזור תוכנית עבודה.
5. להקים ועדת היגוי שתורכב מכמה גורמים מדיסיפלינות שונות, אשר תתווה מדיניות, תפקח, תדווח ותייעץ להנהלת העירייה בקבלת החלטות בעלות משקל בנושא אבטחת מידע וסייבר.
6. לטפל בדחיפות בממצאים שעלו במבדק החדירה למערכת מסוימת, שחלקם אף ברמת סיכון קריטית וגבוהה.
7. להגדיל באופן ניכר את מספר מבדקי החדירה למערכות המבוצעים מדי שנה.
8. 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.
9. למפות את הפערים בין הדרישות בתקנות הגנת הפרטיות ותקן PCIDSS (תקן אבטחת מידע של חברות כרטיסי האשראי) ובין המצב הקיים בעירייה ולטפל בפערים בהקדם.
10. להחליף בהקדם את הסיסמאות למשתמשים מסוימים שלא החליפו סיסמאות במשך 3 שנים, ולוודא שהדבר ייעשה מדי פרק זמן מוגדר מראש לכל המשתמשים האלה.
11. לבצע שחזורים יזומים לפי תוכנית עבודה שתיקבע מראש.

מבדק מערכות אבטחת מידע

12. לטפל בהקדם בממצאים שנמצאו בהגדרות של מערכת ה-FW ומערכת ה-AD.

מבדקי חדירה

13. לטפל ללא דיחוי בממצאים בעלי החשיבות הגבוהה, ובתוך פרק זמן סביר - בממצאים בעלי החשיבות הבינונית שנמצאו בשתי מערכות מסוימות ובאתר האינטרנט של העירייה.

תמצית זו אינה כוללת את כל הממצאים שעלו וגם אינה מוסרת את כל ההמלצות והפרטים המופיעים בגוף הדוח. לקבלת מידע זה יש לקרוא את הדוח המפורט.

תגובת המבוקרים

מנהל אגף מחשוב ומערכות מידע

ב-26.10.2023, הועברו הסמכות והאחריות בתחום הסייבר של עיריית ירושלים מראש מינהל משאבי אנוש והמינהל העירוני, למנהל אגף המחשוב. במסגרת העברת התחום, הוסכם על איש תכן נוסף שיאשר עד סוף שנת התקציב הנוכחית (2023) וכן תכן נוסף שעתיד להיות מאושר בשנת תקציב 2024.

בחודשים נובמבר 2023 – אוגוסט 2023 בוצע סקר סיכונים על ידי חברת BDO. ממצאי הסקר מעובדים ונלמדים בימים אלה, במטרה לייצר תמונת מצב עדכנית על חוסנה של העירייה כיום בתחום אבטחת המידע והסייבר ועל רמת הבשלות שלה בהתאם למתודולוגיית NIST.

מערכת מסוימת נמצאת ברשת העירונית ועל כן מאובטחת בדומה ליתר מערכות המידע העירוניות. לאור ממצאי הסקר פועלת חברת מ' בימים אלו כדי להתאים את רמת אבטחת המידע במערכת לממצאי הסקר.

אגף המחשוב אמון על כ-400 מערכות מידע. מתוך הבנה כי לא ניתן לבצע בדיקות חדירה ייעודיות עבור כל מערכת בתדירות שנתית, העירייה עושה שימוש במערכות ממוכנות כדוגמת 'xm cyber' ו-'bright' לביצוע בדיקות חדירה, ככלי משלים לבדיקות התקופתיות שהוגדרו במכרז מיקור החוץ.

חברת נס תפעל לטיפול בממצאים שהועלו במסגרת מבדקי החדירה למערכות, בהתאם לחומרתם ובמסגרת תוכניות העבודה.

הממונה על אבטחת המידע

מסמך מדיניות נכתב והוצג ברמת טיטה בפני הביקורת. צוין כי המסמך הוא ברמת טיטה וטרם אושר על ידי ועדת ההיגוי העירונית.

נוהלי אבטחת מידע הקיימים מנוסחים מחדש בימים אלה ויובאו בפני הוועדה לאישור עד לסוף שנת 2023. בנוסף יובאו לאישור מספר נהלים חדשים לאישור.

החל תהליך מיפוי מחדש של כלל המאגרים מתוך מחשבה לצמצם את כמות המאגרים (איחוד). במהלך שנת העבודה 2024 יבוצע סקר על כלל המאגרים ומערכות המידע כולל מבדקי חדירה, אשר להערכת יושלם בתוך כשנה.

סיכום

בשנים האחרונות ישנה עלייה מתמדת בהיקף ובעוצמת תקיפות הסייבר בארץ ובעולם. בין המותקפים ניתן למנות בתי חולים, אוניברסיטאות, עיריות, חברות ביטוח, תשתיות, אתרי אינטרנט ועוד. המתקפות עלולות לערער את היציבות הארגונית, לפגוע בנכסי הארגון, במוניטין שלו ובלקוחותיו, ולעיתים אף לסכן חיי אדם.

הגורמים הפוטנציאליים לתקיפות ברשויות המקומיות יכולים להיות בעלי אינטרס כלכלי, גורמים אנטי-ישראליים, גורמים פנימיים להשגת רווח או גרימת נזק מכוון ואף גורמים מדינתיים כחלק ממאבק אידיאולוגי.

עיריית ירושלים היא יעד מרכזי לניסיון תקיפות סייבר, וזאת בין היתר בשל היותה עיר הבירה ואחד הסמלים החשובים של מדינת ישראל. ניסיונות חדירה למאגרי המידע, תקיפה והשחתה של אתר האינטרנט ומניעת שימוש במערכות, הם רק חלק מהסיכונים הקיימים במרחב הסייבר של העירייה.

תקיפה של מערכות העירייה עלולה לשבש מערכות קריטיות של כריזה, גבייה, ניהול וסיוע לתושבים ועוד.

האחריות ליישום מנגנוני אבטחת המידע בעירייה היא של אגף מחשוב ומערכות מידע במינהל אסטרטגיה וחדשנות, המונה כ-200 עובדים, אשר רובם עובדי מיקור חוץ. האחריות להתוויית המדיניות והפיקוח על יישום מנגנונים אלו מוטלת על יחידת אבטחת מידע הכפופה למינהל משאבי אנוש ומינהל עירוני, יחידה הדלה במשאבים תקציביים ובכוח אדם.

כדי לצמצם ככל האפשר את הסיכונים במרחב הסייבר נדרש למפות ולהעריך את הסיכונים הקיימים, להתוות מדיניות הגנה ברורה ולפקח על יישומה באופן שוטף.

הביקורת בדקה את המדיניות והנהלים בנושא אבטחת המידע, בחנה את מנגנוני האבטחה הקיימים והמופעלים בעירייה ואף ביצעה מבדקי חדירה למערכות של העירייה כדי להעריך את רמת אבטחת המידע בהן.

הביקורת העלתה ליקויים מהותיים לגבי התוויית המדיניות ונוהלי אבטחת המידע של העירייה, העמידה בהוראות החוק, בתקנים ובסטנדרטים המקובלים, העמדת המשאבים המוקצים לפיקוח על אבטחת המידע והסייבר ועוד. מכלול הממצאים שצוינו בדוח מגבירים את הסיכון לתקיפה של מערכות העירייה.

על העירייה לטפל בממצאים שהועלו בהקדם, בדגש על גיבוש מסמך מדיניות ועדכון הנהלים, ביצוע תהליך הערכת סיכונים, טיפול בפקרים הטכנולוגיים שנמצאו - לרבות במבחני החדירה - והקמת ועדת היגוי אשר תפקח, תדווח ותייעץ להנהלת העירייה בקבלת החלטות בעלות משקל בתחום אבטחת המידע.

אף שלא ניתן למנוע באופן מוחלט אירועי אבטחת מידע וסייבר, אירועים שבשנים האחרונות התגברו והפכו מוחשיים וקריטיים יותר, היערכות נכונה לקראתם תהפוך את ההתמודדות עימם למוצלחת יותר וקלה יותר. היערכות נכונה מראש יכולה לקצר את זמני התגובה, לאפשר להנהלה לקבל החלטות מושכלות ונכונות יותר, לאפשר לעירייה לעמוד בחובותיה הרגולטוריות וכפועל יוצא להפחית את הסיכונים למיניהם מעצם התרחשות האירוע.

מבוא

בעיריית ירושלים פועלות מערכות מידע ממוחשבות ומנוהלים מאגרי מידע רבים לצורך אספקת שירותים מגוונים לתושבים ולייעול תהליכי העבודה.

שימוש במערכות ובמאגרים אלה תוך הרחבת אספקת השירותים הדיגיטליים לתושבים, מגביר את הסיכון שמידע אישי/רגיש ייחשף ברבים, בזדון או בתום לב, ויפגע בפרטיות של התושבים ושל העובדים.

כמו כן שימוש זה חושף את העירייה לסיכונים במרחב הסייבר העלולים לפגוע ולשבש את פעילותה השוטפת, למנוע אספקת שירותים לתושבים וכן לחשוף את העירייה לתביעות משפטיות ולעיצומים רגולטוריים.

בשנים האחרונות יש עלייה מתמדת בהיקף ובעוצמת האיומים במרחב הסייבר בעולם כולו ובישראל בפרט, באמצעות תוכנות זדוניות (נוזקות וכופרות) המתפשטות דרך רשת האינטרנט, הדואר האלקטרוני או באמצעות חיבור פיזי של התקני זיכרון למיניהם למחשבים ברשת הארגונית. התקיפות הופכות למתוחכמות יותר ויותר על ידי אוטומציה שלהן והפצה המונית. הגורמים הפוטנציאליים לפגיעה במערכות העירוניות יכולים להיות גורמים מדינתיים, גורמים אנטי-ישראליים, תוקפים בעלי אינטרס כלכלי או אינטרס בירוקרטי וכן גורמים פנימיים. לכן, אבטחת המידע – מכלול האמצעים במערכת ובארגון שתפקידם להבטיח שהמידע האגור בה מוגן וממודר - הפכה לצורך בסיסי.

במהלך השנים נמצאו כמה חולשות במערך ההגנה של העירייה ואף בוצעו כמה תקיפות כלפי מערכות העירייה. כך לדוגמה, ביולי 2023 נמצאה פרצת אבטחה חמורה אשר אפשרה לצפות בחומרים שתיעדו כמאה מצלמות הפזורות ברחבי בעיר. ביולי 2022, האקרים פרו-איראנים השביתו את אתר האינטרנט של העירייה ובכך מנעו מתן שירותים למאות אלפי תושבי העיר. בשנת 2020 פרצה חמורה באתר האינטרנט של העירייה אפשרה לצפות בקלות במידע רגיש כגון: דוחות אישיים, תיקי בניין, בקשות לארנונה, ערעורים ועוד.

הזכות לפרטיות וחובת השמירה על צנעת הפרט עוגנו בחקיקה. חוק הגנת הפרטיות, השתמ"א-1981 קובע כי "לא יפגע אדם בפרטיות של זולתו ללא הסכמתו". החוק מגדיר, בין היתר, "מידע" כ"נתונים על אישיותו של אדם, מעמדו האישי, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו", ו"מאגר מידע" כ"אוסף נתוני מידע המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב".

עוד קובע החוק כי "בעל מאגר מידע, מחזיק מאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע". כמו כן, במאי 2017 פורסמו תקנות הגנת הפרטיות ואבטחת מידע, התשע"ז-2017. התקנות מגדירות בפירוט את החובות של בעל מאגר מידע ליישום בקרות תהליכיות וטכנולוגיות לצורך אבטחת המאגר.

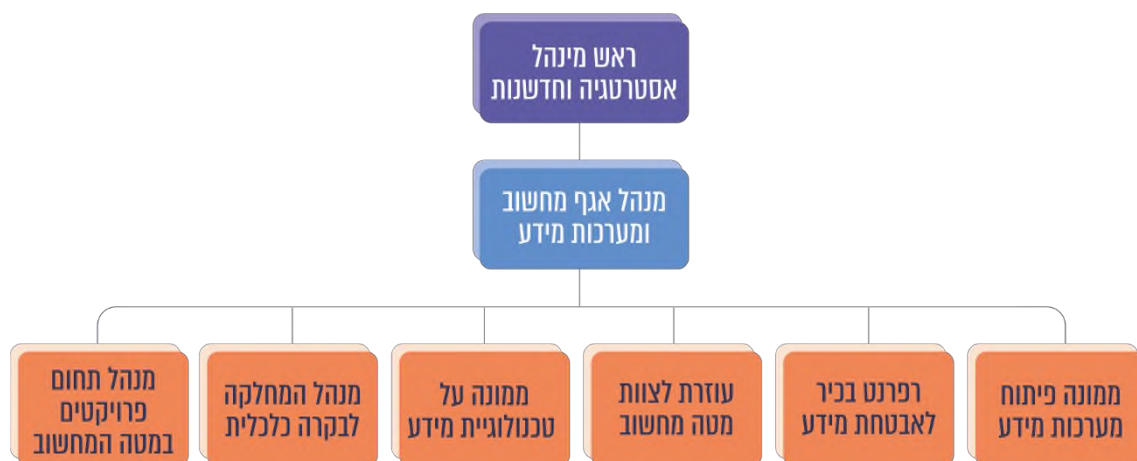
כאמור, לשם שמירה על צנעת הפרט ועל הוראות החוק יש לנקוט אמצעים לאבטחת המידע ומערכי המידע ולהגן עליהם מפני פגיעה, חשיפה ושינוי במזיד או בשוגג. יש לעשות זאת באופן שיישמרו הזמינות, השלמות, המהימנות, הסודיות והשרידות של המידע ומערכות המידע.

העירייה מחויבת לקיים את הוראות החוק להגנת הפרטיות, התשמ"א-1981, ותקנותיו ובעלת הסמכה ל-ISO 27001 (תקן המגדיר את עקרונות הקמת ניהול ותחזוקה של מערכת אבטחת מידע המתאימה לארגון). הביקורת בדקה נושאים מחייבים בהתאם לחוק ולהסמכה כאמור, ועם זאת מצאה לנכון להרחיב בנושאים אחרים בעלי חשיבות גבוהה, בהתאם לתורת ההגנה בסייבר 2.0 מאת מערך הסייבר הלאומי וה-NIST (המכון הלאומי האמריקני לתקנים וטכנולוגיה המפרסם תקנים בתחום הגנת המידע).

הביקורת ערכה גם מבדקי חדירה לאתר האינטרנט ולשתי מערכות מסוימות.

אגף מחשוב ומערכות מידע במינהל אסטרטגיה וחדשנות אחראי למערכות המחשוב של העירייה ומונה כ-200 עובדים אשר רובם עובדי מיקור חוץ (מחברת נס). האגף אחראי גם ליישום מערכות אבטחת מידע בעירייה. להלן תרשים ארגוני של האגף:

תרשים 1: מבנה ארגוני של אגף מחשוב ומערכות מידע



תקציב מערכות אבטחת מידע בעירייה גדל באופן ניכר בשנת 2022 ביחס לשנים עברו. להלן התקציב בחלוקה למערכות ותחזוקה משנת 2019 ועד לשנת 2022:

לוח 1: פילוח תקציב אבטחת מידע בעירייה בשנים 2022-2019 (ש"ח)

שנה	2019		2020		2021		2022	
	תחזוקה	מערכות	תחזוקה	מערכות	תחזוקה	מערכות	תחזוקה	מערכות
סה"כ	145,551	1,973,798	739,663	675,694	732,370	995,104	2,580,172	1,790,866
סה"כ מערכות + תחזוקה	2,119,349		1,415,357		1,727,474		4,371,038	

תקנה 3 לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, קובעות בין היתר כי גוף ציבורי או מי שמחזיק בחמישה מאגרי מידע (החייבים ברישום לפי החוק) נדרשים למנות ממונה אבטחת מידע. בהתאם לכך התקנה חלה על עיריית ירושלים. נוסף על יישום מערכות אבטחת מידע, בעירייה קיימת יחידת אבטחת המידע הכפופה למינהל משאבי אנוש והמינהל העירוני, האחראית להתוויית מדיניות אבטחת המידע והפיקוח על הנעשה בנושא אבטחת מידע וסייבר בעירייה. ביחידה עובד

איש אבטחת מידע אחד בלבד (המוגדר כממונה אבטחת המידע של העירייה), אשר אינו נתמך על ידי מיקור חוץ (לאחרונה מקבל סיוע מועט לצורכי עדכון נהלים ותקנות הגנת הפרטיות). תקציב אבטחת המידע של היחידה נמוך (כמיליון ש"ח בשנה) ומנוהל באגף מחשוב ומערכות מידע.

בעקבות ביקורת בנושא אבטחת מידע שבוצעה במהלך 2019 שיפרה העירייה במעט את מערך אבטחת המידע והחלה בהקמה של אתר DR (התאוששות מאסון) להמשך הפעילות התפקודית של העירייה בקורות אירוע אסון. עם זאת, נמצא מספר רב של ליקויים שעלו במהלך הביקורת הקודמת וטרם טופלו למועד ביקורת זו, וכן נמצאו ליקויים שעלו במהלך הביקורת הנוכחית (בנושאים שלא נבדקו בביקורת הקודמת) הדורשים טיפול, חלקם אף טיפול מיידי.

מטרת הבדיקה

מטרת הביקורת היא לבחון את נאותות התנהלות העירייה בהיבטי אבטחת המידע וצמצום הסיכון לתקיפות סייבר כנגד רשתות העירייה ומערכות המידע שלה, על ידי:

- בחינת היבטי ניהול מערכות המידע ומימוש אבטחת המידע בעירייה.
- בחינת שילוב אבטחת המידע בניהול מאגרי המידע, העלאת מודעות העובדים, ניהול התקציב, עדכון המערכות הלא-נתמכות.
- בחינת עמידת העירייה בהוראות חוק הגנת הפרטיות ותקנותיו.
- בחינת רמת אבטחת המידע על ידי ביצוע מבדק טכנולוגי.

היקף הבדיקה

בדיקת מדיניות ונהלים בנושא אבטחת המידע, מבדק טכנולוגי לבחינת רמת האבטחה הקיימת ביישומי אבטחת המידע (אנטי-וירוס, FW, AD ומערכת עדכוני אבטחת מידע).

מבדקי חדירה לשתי מערכות מסוימות ולאתר האינטרנט של העירייה.

הביקורת לא בדקה את מערך אבטחת המידע של החברות העירוניות.

דוחות קודמים בנושא

- דוח מבקרת העירייה בנושא ניהול מערך אבטחת המידע בעירייה, 2019.
- דוח מבקרת העירייה בנושא המשכיות תפקודית בעת חירום, 2020.
- דוח מבקר המדינה, ניהול מערכות מידע ברשויות המקומיות, מתוך דוחות על הביקורת בשלטון המקומי לשנת 2022.
- דוח מבקר המדינה, אבטחת מידע והגנת הפרטיות ברשויות מקומיות, מתוך דוחות על הביקורת בשלטון המקומי לשנת 2017.

תקופת הביקורת

הביקורת נערכה בחודשים אפריל - ספטמבר 2023.

פירוט הממצאים

פרק ראשון

בדיקת רגולציה, מדיניות, נהלים ותהליכים בתחום אבטחת מידע וסייבר

מדיניות ונהלים

הבסיס לפעילות אבטחת המידע הארגוני הוא מסמך מדיניות אבטחת המידע. מסמך זה אמור לשקף את תפיסת מדיניות האבטחה הארגונית, לתאר את התקן לפעילות, את שיטות העבודה והעקרונות המנחים; ההנהלה נדרשת לאשר את מסמך המדיניות ולפקח על יישומו.

המסמך הוא כתב הצהרת ההנהלה בדבר מחויבותה לאבטחת המידע ותפיסתה לגבי אופן יישום אבטחת המידע בעירייה.

מדיניות אבטחת מידע

בידי העירייה לא קיים מסמך מדיניות אבטחת מידע. הביקורת סקרה מסמך שטרם אושר על ידי הנהלת העירייה ועריכתו טרם הסתיימה עוד מינואר 2021.

המסמך מכיל בין היתר התייחסות לנושאים האלה:

- אופן השימוש בנכסי המידע של העירייה
- מדיניות בקרה וכניסה לעירייה
- מדיניות המשכיות עסקית
- מדיניות העברת מידע וגיבויים
- מדיניות עבודה מרחוק
- מדיניות שימוש בדואר אלקטרוני

מסקנות

1. ללא מסמך מדיניות מעודכן ומאושר על ידי הנהלת העירייה, הגורמים האחראים ליישום אבטחת המידע בעירייה ופיקוח עליה אינם יכולים ליישם באופן נאות את המדיניות המותווית, את העקרונות ואת שיטות העבודה, ולפקח עליהן.

המלצות

1. לסיים את מסמך המדיניות, להציגו ולאשרו בהנהלת העירייה ולפקח על יישומו.

תגובת המבוקרים

הממונה על אבטחת המידע

מסמך מדיניות נכתב והוצג ברמת טיטה בפני הביקורת. צוין כי המסמך הוא ברמת טיטה וטרם אושר על ידי ועדת ההיגוי העירונית.

נוהלי אבטחת מידע

תקנה 4 (ה) תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, קובעת כי "בעל מאגר מידע יבחן, אחת לשנה, את הצורך בעדכון הנוהל, ובלי לגרוע מן האמור, יבחן אם יש צורך בעדכון של הנוהל במקרים אלה: (1) נעשים שינויים מהותיים במערכות המאגר או בתהליכי עיבוד מידע (2) נודע על סיכונים טכנולוגיים חדשים הנוגעים למערכות המאגר".

הביקורת סקרה את הנהלים הקשורים באופן ישיר ועקיף לאבטחת המידע של העירייה (סה"כ 29 נהלים) כפי שהתקבלו מאגף מחשוב ומערכות מידע ומנהל אבטחת המידע בעירייה. הנהלים כוללים בין היתר את האחריות לניהול מערכות המידע, ניהול ההרשאות, ניהול הסיסמאות, גישה מרחוק, שימוש באינטרנט, אבטחת פלט נייר ועוד. בבדיקת הנהלים נמצא כי 25 מתוכם לא עודכנו יותר מ-3 שנים (ישנם נהלים שלא עודכנו זה 7 שנים!). עוד עלה כי קיים שוני מהותי בין הנהלים שקיבלה הביקורת לבין אלה המפורסמים בפורטל העירייה. כך לדוגמה, ישנם נהלים בפורטל שעודכנו לאחרונה בשנת 2001 ואילו הביקורת קיבלה נוהל שעודכן לאחרונה בשנת 2016; ישנם נהלים שלהם שם זהה אולם התוכן של הנוהל שהתקבל בביקורת שונה מזה של הנוהל בפורטל העירייה. כן נמצאו מקרים שבהם הנוהל שהתקבל במהלך הביקורת כלל אינו קיים בפורטל העירייה, ולהפך, נהלים הקיימים בפורטל ולא הועברו במהלך הביקורת. להלן בטבלה פירוט הנהלים, מועד עדכון האחרון והשוני בהשוואה לפורטל העירייה:

לוח 2: פירוט נוהלי אבטחת המידע ותאריך עדכון בעירייה

מס"ד	מספר נוהל	תיאור נוהל שהתקבל במהלך הביקורת	תאריך עדכון אחרון	הנוהל בפורטל העירייה
1.	08.04.15	ניהול מאגרי מידע	מאי 2022	לא קיים
2.	08.04.01	הודעה יזומה בדבר הפסקת שירותי מחשוב עירוניים	מרץ 2016	נוהל משנת 2002
3.	08.04.02	קבלת שירותי מחשוב במקרי חירום - לאחר שעות העבודה	מרץ 2016	נוהל משנת 2001
4.	08.04.03	הפעלת מערכת מידע נפגעים	מרץ 2016	נוהל משנת 2001

מס"ד	מספר נוהל	תיאור נוהל שהתקבל במהלך הביקורת	תאריך עדכון אחרון	הנוהל בפורטל העירייה
5.	08.04.04	מטה המחשוב העירוני	מרץ 2016	נוהל משנת 2004
6.	08.04.05	מילון מונחים מעודכן	אוגוסט 2016	נוהל משנת 2006
7.	08.04.06	אחריות לניהול וליישום אבטחת מידע	מרץ 2016	נוהל משנת 2013
8.	08.04.07	מנהל מערכות מידע - הגדרות ותפקידים	אפריל 2016	נוהל משנת 2013
9.	08.04.08	מודעות הדרכה והסברה	אפריל 2016	נוהל משנת 2013
10.	08.04.10	יישום חוק הגנת הפרטיות - מתוקן	נובמבר 2016	לא קיים
11.	08.04.11	דיווחים על אירועים חריגים	אפריל 2015	נוהל משנת 2013
12.	08.04.12	זיהוי והרשאות משתמשים - חדש 1	אוגוסט 2022	נוהל משנת 2013
13.	08.04.13	תפעול מערך הסיסמאות	דצמבר 2013	תאריך עדכון זהה, אולם התוכן שונה
14.	08.04.14	שימוש בדואר אלקטרוני	אפריל 2016	נוהל משנת 2013
15.	08.04.15	שימוש באינטרנט	דצמבר 2013	תאריך עדכון זהה, אולם עם תוכן שונה
16.	08.04.16	שימוש ברשת העירונית הפנימית	אפריל 2015	נוהל משנת 2013
17.	08.04.17	גישה מרחוק	אפריל 2014	נוהל משנת 2013
18.	08.04.18	אבטחת אמצעי מחשוב ניידים	אפריל 2016	נוהל משנת 2013
19.	08.04.19	אבטחת פעילות פיתוח ותחזוקה	אפריל 2016	נוהל משנת 2013
20.	08.04.20	אבטחת פלט נייר	אפריל 2016	נוהל משנת 2013
21.	08.04.21	סדרי העברת מידע והוועדה להעברת מידע בין גופים ציבוריים	אפריל 2016	נוהל משנת 2017
22.	08.04.22	ניהול ואבטחת אמצעי אחסון	אפריל 2016	נוהל משנת 2013
23.	08.04.23	בקרה ופיקוח לוגי	אפריל 2016	נוהל משנת 2001
24.	08.04.25	בטיחות פיזית ומניעת גניבה	אפריל 2016	נוהל משנת 2001
25.	08.04.32	טלפונים חוץ כיכריים	אפריל 2016	נוהל משנת 2009
26.	08.04.33	שימוש ביישומי ענן	מרץ 2016	לא קיים
27.	08.04.34	פעולות למתקפת סייבר מתוכננת	יוני 2016	לא קיים
28.	A	מדיניות סיסמאות במערכת העירונית	יולי 2021	לא קיים
29.	B	מדיניות אבטחת מידע	ינואר 2021	לא קיים

מסקנות

2. בשל נהלים שאינם מעודכנים באופן שוטף, אינם רלוונטיים לתקופה ואינם מעודכנים בפורטל העירייה, קיים קושי ביישום אבטחת המידע ובפיקוח עליה, וכן העירייה אינה עומדת בתקנות הגנת הפרטיות.

המלצות

2. לעדכן את נוהלי אבטחת המידע ולכלול את כל ההיבטים שהשתנו מאז כתיבתם, לאשרם בהנהלת העירייה, לדאוג לתקף אותם אחת לשנתיים (או בעת שינוי בתהליכי העבודה של העירייה, המוקדם מביניהם) ולוודא תאימות מלאה לפורטל העירייה.

תגובת המבוקרים

הממונה על אבטחת המידע

נוהלי אבטחת המידע הקיימים מנוסחים מחדש בימים אלה ויובאו בפני הוועדה לאישור עד לסוף שנת 2023. בנוסף, יובאו לאישור מספר נהלים חדשים לאישור. בפורטל העירוני פורסמו אך ורק נהלים אשר אושרו בעבר ולא נהלים שהיו בהליכי ניסוח ולא עברו אישור סופי. אחריות לתחום הסייבר הועברה לאגף מחשוב ולפיכך ממונה אבטחת המידע יסייע לאגף בגיבוש נהלים אלו.

מנהל אגף מחשוב ומערכות מידע

ב-26.10.2023 הועברו הסמכות והאחריות בתחום הסייבר של עיריית ירושלים מראש מינהל משאבי אנוש והמינהל העירוני, למנהל אגף המחשוב. ההחלטה התקבלה על ידי מנכ"ל העירייה וזאת בהתאם לחוות הדעת של היועץ המשפטי. במסגרת העברת התחום הוסכם על איש תכן נוסף שיאושר עד סוף שנת התקציב הנוכחית (2023) וכן תכן נוסף שעתיד להיות מאושר בשנת תקציב 2024.

נוהל גיבויים ושחזורים

בעירייה קיים נוהל 08.04.24 בנושא גיבויים ושחזורים. הנוהל כולל התייחסות לקביעת תדירות הגיבויים, אופן שמירתם, מיקום שמירת התיעוד, אופן השמדת גיבוי וביצוע שחזורים יומיים לבדיקת הגיבויים. עם זאת נמצא כי העדכון האחרון של הנוהל היה באפריל 2016 והוא אינו מאושר על ידי הנהלת העירייה.

מסקנות

3. נוהל גיבויים ושחזורים לא מעודכן אינו רלוונטי לתקופה וחושף את העירייה לסיכון שהתהליכים המפורטים בו לא יבוצעו כנדרש.

המלצות

3. 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.

תגובת המבוקרים

מנהל אגף מחשוב ומערכות מידע

נוהל גיבויים יכתב עד לסוף שנת העבודה הנוכחית.

יחידת אבטחת מידע

מנהל אבטחת מידע בארגונים הפך להיות תפקיד חיוני, בשל תחומי האחריות שלו, להגן על המידע הקיים במערכות הארגון מפני גישה לא מורשית, שימוש לרעה, חשיפה, שיבוש מידע, העתקה, השמדה ועוד.

בעירייה מוגדר מנהל אבטחת מידע (CISO) המנהל את יחידת אבטחת המידע בעירייה. היחידה כפופה למנהל משאבי אנוש ומנהל עירוני, והיא אחראית להתוויית מדיניות אבטחת המידע והפיקוח על הנעשה בנושא אבטחת מידע וסייבר בעירייה. תקציב היחידה בשנת 2023 עמד על כמיליון ש"ח כולל פרויקטים ייחודיים (הסבר מטה).

מלבד מנהל היחידה, ישנו תקן למשרה חלקית (כ-120 שעות בחודש) של סטודנט/ית לצורכי תמיכה ועזרה בעבודה השוטפת.

לצורך ביצוע פרויקטים ייחודיים בשנת 2023 קיבל מנהל היחידה סיוע במיקור חוץ כדלהלן:

- עובדת שגויסה בתחילת השנה לתקופה בת חצי שנה, לסיוע בפרויקט יישום בקורות בהתאם לחוק הגנת הפרטיות.
 - עובד שגויס לתקופה של שלושה חודשים לסיוע בפרויקט התאוששות מאסון.
- היקף כוח האדם והתקציב של יחידת אבטחת המידע של העירייה אינו מספק למילוי תפקידי היחידה.

בארגונים מסוימים, לרבות עיריות ומשרדי ממשלה, קובעים את תקציב יחידת אבטחת המידע בשיעור מסוים מהכנסות הארגון, כך שהשיעור הממוצע נע בין 0.15% ל-0.8%. להלן טבלה המציגה את שיעור תקציב היחידה מסך הכנסות העירייה:

לוח 3: בדיקת תקציב אבטחת המידע בעירייה ביחס להכנסות בשנים 2022-2019

שנה	הכנסות העירייה (אלפי ש"ח)	תקציב היחידה (אלפי ש"ח)	אחוז מההכנסות
2019	8,845,553	500	0.006%
2020	11,147,593	840	0.008%
2021	10,791,994	1,000	0.009%
2022*	12,031,597	1,000	0.008%

* הכנסות לשנת 2022 נלקחו כממוצע אחוז גידול בהכנסות לשנים 2018-2021.

מהנתונים בטבלה עולה כי תקציב היחידה בעירייה נמוך באופן ניכר מהמקובל.

יצוין עוד כי מנהל יחידת אבטחת המידע, אשר נושא תפקיד רגיש, חולק את החדר עם גורם נוסף בעירייה (לעיתים מדובר בגורם המיישם אבטחת מידע ולעיתים בגורם שכלל אינו עוסק בתחום זה), דלת הכניסה לחדר אינה עונה על הצרכים, לא ניתן לסגור אותה כלל ואין מנגנון של סיסמה או אבטחה כלשהי שימנע כניסת לא מורשים.

מסקנות

4. יחידת אבטחת המידע האחראית לפיקוח בנושא אבטחת המידע בעירייה, מתקשה למלא כראוי את תפקידה בגלל תקציב נמוך באופן יחסי ומגבלות כוח אדם.
5. בחדרו של מנהל אבטחת המידע נמצא בדרך כלל מידע רגיש. שיתוף מרחב זה עם עובדים שאינם קשורים לתחום מסכן את אבטחת המידע בעירייה.

המלצות

4. לעבות את הצוות ביחידת אבטחת המידע ולספק לה את המשאבים הדרושים למילוי תפקידה.
5. להפריד את חדרו של מנהל יחידת אבטחת המידע ולהתקין מנגנון נעילה לדלת.

1 בהתאם למחקר שנערך ע"י חברת AT&T במאי 2020 בנושא: "תקציב אבטחת מידע וסייבר" - <https://cybersecurity.att.com/blogs/security-essentials/how-to-justify-your-cybersecurity-budget>

תגובת המבוקרים

ראש מינהל משאבי אנוש והמינהל העירוני

המלצה 4: בהתאם לבקשת הממונה על אבטחת המידע, ובעת בקשתו, ניתן תקציב נוסף לטובת המחלקה והוגדרו צורכי כוח אדם של המחלקה לרבות פרסום מכרז מספר פעמים, ברם המכרז לא צלח ולא נמצא מועמד לתפקיד.

עם העברת האחריות על ההיערכות והטיפול באירועי סייבר לאגף המחשוב ומערכות מידע במינהל אסטרטגיה וחדשנות, סוכם שמינהל אסטרטגיה וחדשנות יציג צרכים ויתקיים דיון שבסופו יוחלט על כוח האדם שיש להקצות לטובת הסייבר ולטובת אבטחת המידע.

המלצה 5: משרדו של הממונה על אבטחת המידע מצוי בחדר ולא בעמדה ולצידו מועסקת סטודנטית מטעמו בתחום אבטחת מידע ואין המדובר בעובד מתחום אחר. באשר לנעילת הדלת, מהמידע שנמסר לי היה מדובר בתקלה טכנית ותו לא. התקלה טופלה וניתן לנעול את החדר. הקצאת חדר אחר תיבחן בהתאם לאפשרויות הקיימות בנסיבות העניין.

ניהול סיכוני אבטחת מידע

הערכת סיכונים וסקר סיכוני אבטחת מידע טכנולוגי

הערכת סיכונים הוא תהליך המאפשר הגעה לרמת הגנה סבירה על מערכות המחשוב של הארגון תוך שמירה על איוון ההוצאות התפעוליות הנובעות מיישום אמצעי הגנה על מערכות אלה. תהליך הערכת סיכונים הוא תהליך מורכב, וכולל: זיהוי והערכת נכסי מידע ארגוניים, זיהוי סיכוני אבטחת מידע, ניתוח הסיכונים, דירוג הסיכונים ועוד.

סקר סיכוני אבטחת מידע טכנולוגי הוא אוסף מבדקים בנושאים טכנולוגיים, שמטרתם לגלות חשיפות פוטנציאליות של נכסי המידע הקריטיים בארגון לפגיעה בהיבטי סודיות (Confidentiality), שלמות (Integrity) וזמינות (Availability).

תקנה 5 (ג) לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, קובעת כי "במאגר מידע שחלה עליו רמת האבטחה הגבוהה, בעל המאגר אחראי לכך שייערך סקר לאיתור סיכוני אבטחת מידע (להלן: סקר סיכונים); בעל מאגר המידע ידון בתוצאות סקר הסיכונים שיועברו לו, יבחן את הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבותיהן, ויפעל לתיקון הליקויים שהתגלו במסגרת הסקר, ככל שהתגלו; סקר סיכונים כאמור ייערך אחת לשמונה עשר חודשים לפחות".

הביקורת מצאה כי לא קיים תהליך הערכת סיכונים לבחינת הסיכונים הפוטנציאליים שאליהם חשופה העירייה בנושא אבטחת המידע ולא בוצע במערכת סקר סיכונים טכנולוגי זה שנים רבות.

מסקנות

6. תהליך הערכת סיכונים בנושא אבטחת מידע בעירייה הכרחי להבנת הסיכונים שאליהם חשופה העירייה ולקבלת החלטה על האמצעים הנדרשים לצמצומם.

7. אי ביצוע סקר סיכונים טכנולוגי מעמיד את העירייה במצב שבו אין היא יודעת מהם החולשות וסיכוני אבטחת המידע ברשת ובמערכות העירייה, ונוסף על כך היא איננה עומדת בתקנות הגנת הפרטיות תקנה 5 (ג).

המלצות

6. 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.
7. 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 המבוקרים

מנהל אגף מחשוב ומערכות מידע

בימים אלו מתבצע סקר של חברת BDS אשר מטרתו היא שיפור התהליכים העסקיים כדי לייצר המשכיות תפקודית בריאה ובטוחה של הארגון.

מבדקי חדירה לרשת ולמערכות העירייה

מבדקי חדירה הם שיטת בדיקה להעריך את רמת האבטחה של מערכות, אפליקציות, שירותי מובייל ותשתיות. מטרת הבדיקה היא לאתר את החולשות והפגיעויות ולתת את הדגשים וההמלצות לתיקונם, וזאת על ידי איסוף המידע וניתוח המידע. במהלך הבדיקה הבוחן שואף לדמות את מאמציו של תוקף זדוני בצורה אותנטית על מנת לקבל מבט מציאותי על רמות ההגנה של הארגון.

תקנה 5 (ד) לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, קובעת כי "במאגר מידע שחלה עליו רמת האבטחה הגבוהה, בעל המאגר אחראי לכך שייערכו מבדקי חדירות למערכות המאגר לבחינת עמידותן בפני סיכונים פנימיים וחיצוניים, אחת לשמונה עשר חודשים לפחות; בעל המאגר ידון בתוצאות מבדקי החדירות ויפעל לתיקון הליקויים שהתגלו, ככל שהתגלו."

בעירייה מבצעים מבדקי חדירה ל-2-3 מערכות בלבד מדי שנה (וללא קשר לרמת האבטחה של מאגר המידע). הביקורת סקרה את מבדקי החדירה שבוצעו משנת 2021 ועד למועד הביקורת, הממצאים שעלו וסטטוס הטיפול בהם, כדלהלן:

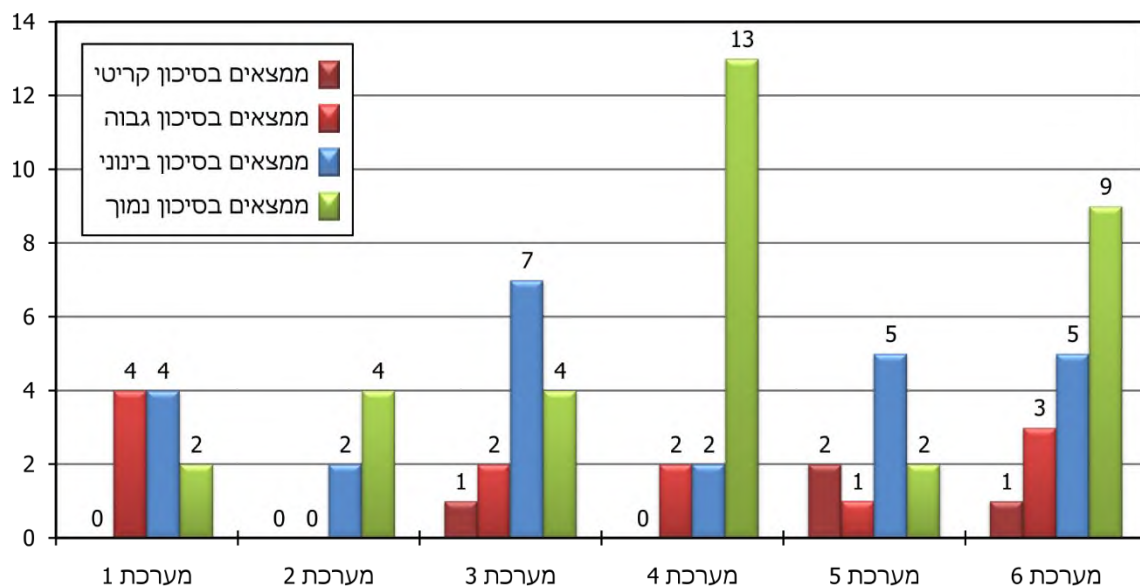
לוח 4: סיכום ממצאי מבדקי חדירה שבוצעו בעירייה בשנים 2021-2023 וסטטוס הטיפול בהם

שנה	מספר ממצאים	מספר ממצאים בדרגת סיכון גבוהה / קריטית	טיפול בממצאים
2021	10	4	כל הממצאים טופלו
2021	6	0	הממצאים טרם טופלו
2022	17	2	כל הממצאים טופלו
2022	10	3	7 ממצאים טופלו, 3 ממצאים טרם טופלו (אחד ברמת סיכון בינונית ושניים נמוכה)
2023	14	3	הממצאים טרם טופלו
2023	18	4	הממצאים טרם טופלו

* מערכת הגבייה החדשה עלתה לאוויר בתחילת שנת 2023.

להלן התפלגות הממצאים עבור כל מבדק:

תרשים 2: ממצאי המבדקים לפי סוג המערכת ורמת הסיכון של הממצאים



מערכת מסוימת - הביקורת מצאה כי המערכת, שהיא מערכת ליבה של העירייה, עלתה לאוויר ללא ביצוע מבדקי חדירה וטיפול בממצאים. מבדק החדירה למערכת בוצע במהלך חודש ינואר 2023, והעלה כי רמת אבטחת המידע שלה נמוכה. עוד עלה כי ממצא בדרגת סיכון קריטית ו-2 ממצאים בדרגת סיכון גבוהה שנמצאו במבדק טרם טופלו, נכון למועד הביקורת (כ-8 חודשים לאחר שהתגלו הממצאים), כלומר המערכת עלתה לאוויר ברמת אבטחת מידע נמוכה.

מערכות אחרות - הביקורת בדקה את סטטוס הטיפול בממצאי המבדקים של המערכות האחרות ונמצא כי ישנם ממצאים בדרגת סיכון בינונית (ונמוכה) שטרם טופלו משנת 2021.

עוד נמצא כי:

- א. לא בוצעה הערכת סיכונים טרם בחירת המערכות.
- ב. נבדקו מעט מאוד מערכות ביחס למספר המערכות הקיימות בעירייה (כ-200).

מסקנות

8. העלאה לאוויר של מערכת ליבה ללא ביצוע מבדקי חדירה וטיפול בממצאים שנמצאו במבדק, או לחלופין אי טיפול בתוך פרק זמן סביר בממצאים שנמצאו במערכות שכבר פועלות בעירייה, חושפים את העירייה לניצול חולשות על ידי תוקף פוטנציאלי, במיוחד במערכת בעלת סיכון מובנה גבוה.
9. ביצוע מבדקי חדירה מעת לעת חיוני ביותר לאבטחת המידע בארגון. ללא ביצוע הערכת סיכונים טרם בחירת המערכות אין למקבלי ההחלטות אפשרות לבחור את המערכות הרלוונטיות ביותר לביצוע מבדקי החדירה.
10. במצב הנוכחי שבו מתבצעים מבדקי חדירה למעט מאוד מערכות בשנה יוצא שמרבית המערכות אינן נבדקות מכלל במשך כל התקופה שהן משמשות בעירייה. לצורך ההמחשה: בעירייה קיימות כ-200 מערכות ובממוצע מערכת מידע מוחלפת מדי 15 שנים. במהלך אותן שנים מבוצעים כ-40 מבדקי חדירה (2-3 מבדקים מדי שנה), ולכן נוצר מצב שבו לא יבוצעו מבדקי חדירה כלל ל-160 מערכות.
11. העירייה אינה עומדת בתקנות הגנת הפרטיות, המחייבות ביצוע סקר ומבחני חדירה אחת ל-18 חודשים במאגר מידע שחלה עליו רמת אבטחה גבוהה.

המלצות

8. לא להעלות מערכות לאוויר ללא ביצוע מבדקי חדירה ותיקון הליקויים שנמצאו.
9. להכין תוכנית עבודה לטיפול בממצאים בהתאם למבדקי החדירה בתוך פרק זמן סביר בהתאם לדרגת הסיכון.
10. 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.
11. בהתאם לתהליך הערכת הסיכונים, להגדיל באופן ניכר את כמות מבדקי החדירה המבוצעים מדי שנה גם למערכות נוספות מעבר לדרישה של תקנות הגנת הפרטיות.

תגובת המבוקרים

מנהל אגף מחשוב ומערכות מידע

המלצה 8: בדיקות אלו מתבצעות באמצעות כלים ממוכנים כדוגמת bright וכן מתבצע טיפול בממצאים בהתאם.

המלצה 9: הערת הביקורת מקובלת. טיפול בממצאי בדיקות החדירה מוגדר בתהליכי העבודה ומבוצע בהתאם. יבוצע חידוד בנהלים אודות הכנת תוכנית עבודה לטיפול בממצאים.

המלצה 10: אגף המחשוב מבצע את בדיקות החדירה למאגרי המידע, בהתאם להנחיות ממונה אבטחת המידע.

המלצה 11: במכרז מיקור החוץ שיחודש בשנת 2024 עלתה בקשה להרחבה משמעותית של בנק השעות לצורכי בדיקות חדירה, שיעמוד על שעות בדיקה רבות.

הממונה על אבטחת המידע

המלצה 10: החל תהליך מיפוי מחדש של כלל המאגרים מתוך מחשבה לצמצם את כמות המאגרים (איחוד). במהלך שנת העבודה 2024 יבוצע סקר על כלל המאגרים ומערכות המידע כולל מבדקי חדירה, אשר להערכת יושלם בתוך כשנה.

ועדת היגוי בנושא אבטחת מידע וסייבר

תפקידה של ועדת היגוי בנושא אבטחת מידע וסייבר בארגונים כולל אישור ועדכון קווים מנחים למדיניות אבטחת המידע וסייבר, קבלת דיווחים תקופתיים מהממונה על אבטחת המידע, "פיקוח-על" בנושא אבטחת המידע וסייבר, הבטחת קיומם של מנגנוני פיקוח ובקרה נאותים, דיווח להנהלת הארגון, סיוע בקבלת החלטות בתחום ועוד. הוועדה אמורה להתכנס באופן קבוע ובתדירות מספקת, ומורכבת בדרך כלל מגורמים מדיסציפלינות שונות כגון: משאבי אנוש, כספים וכו' (ולא רק מתחומי המחשוב או אבטחת המידע).

באגף מחשוב ומערכות מידע גובשה ועדת אבטחת מידע. זו מתכנסת אחת לשבועיים ודנה בנושאי אבטחת מידע (דיווח על אירועים חריגים, רכישה של מוצרים חדשים, מעקב אחר יישום מוצרי אבטחת מידע ועוד). עם זאת, מדובר בוועדת אבטחת מידע המורכבת מאנשי אגף המחשוב בלבד (ואף אינה כוללת את אחראי אבטחת המידע של העירייה) ואינה משמשת כוועדת ההיגוי של העירייה.

מסקנות

12. בעירייה לא קיימת ועדת היגוי בנושא אבטחת מידע וסייבר, וכתוצאה מכך אין גוף או ועדה המתווים מדיניות ומפקחים על יישומה, מדווחים ומסייעים להנהלת העירייה בקבלת החלטות בעלות משקל בתחום אבטחת מידע וסייבר.

המלצות

12. 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.

תגובת המבוקרים

מנהל אגף מחשוב ומערכות מידע

מרגע העברת התחום לאחריות מנהל אגף המחשוב נקבעו ועדות היגוי מקצועיות בתדירות שבועית, וכן, ייקבעו בעתיד הקרוב ועדות היגוי עליונות בהתאם לתקנות בנושא זה.

ראש מינהל משאבי אנוש והמינהל העירוני

לאור התארכות ההליך להעברת האחריות להיערכות ולטיפול באירועי סייבר לאגף המחשוב ומערכות מידע במינהל אסטרטגיה וחדשנות, הדבר התעכב. עם זאת, כפי שעולה מתגובתו של מנהל אגף המחשוב ומערכות המידע להמלצה, הנושא טופל.

תחומי אחריות והתקשרות עם חברת נס

ארגונים רבים מקבלים שירותי מערכות מידע ואבטחת מידע מספקי מיקור חוץ. במקרים אלו, הארגון נדרש לפקח על איכות העבודה וזמינות מתן השירות של הספקים. כמו כן, הארגון חייב לוודא כי לא מתקיימים ניגודי עניינים בין מגוון השירותים שמבצע אותו ספק כמיקור חוץ.

חברת נס נשכרה על ידי העירייה לספק שירותי מערכות מידע ואבטחת מידע. ההסכם עימה נחתם במאי 2016. תחומי האחריות של חברת נס בהתאם להסכם, הם אחריות כוללת על מערך המחשוב, יישום מנגנוני בקורות אבטחת מידע, פיתוחים ושינויים במערכות, שמירה על עדכניות טכנולוגית ובחירת פתרונות ומוצרים טכנולוגיים מתאימים מבחינת תקציב ודרישות העירייה.

הביקורת סקרה עניינים מקצועיים עיקריים (ולא היבטים מסחריים) בהסכם שנחתם מול חברת נס ונמצא כי:

- לחברת נס הסמכה ל-ISO27001 (תקן העוסק באבטחת מידע).
- תחומי האחריות של חברת נס הם אלה: אחריות כוללת על מערך המחשוב, יישום מנגנוני בקורות אבטחת מידע, פיתוחים ושינויים במערכות, שמירה על עדכניות טכנולוגית ובחירת פתרונות ומוצרים טכנולוגיים מתאימים מבחינת תקציב ודרישות העירייה.
- רציפות במתן שירות בין העירייה לבין חברת נס עקב חשיבות השירות הניתן במקרה חירום, מחלוקת בין שני הצדדים או מקרים אחרים (סעיף 6).

- קיימת התייחסות לספק שירותים בתקופת המעבר בין הספק הקודם לבין חברת נס כך שחברת נס תספק את השירותים בתקופה הנ"ל (סעיף 7).

בנושא רכש שירותים (שאינם ניתנים על ידי חברת נס), מוצרי מדף או מדף עם התאמות (לדוגמה: כספות, FW וכו'), בחירת השירות/המוצר מתבצעת על ידי העירייה, אולם הייעוץ, ההמלצה, ההסכם והתשלום מול הספק מבוצעים כולם על ידי חברת נס, כך שלמעשה, הבחירה של העירייה היא נגזרת מחוות הדעת של חברת הנס.

מסקנות

13. במקרים רבים שירותים אשר נועדו לבחון את רמת אבטחת המידע של מערכות שפיתחה חברת נס (לדוגמה: מבדקי חדירה למערכת) וכן את מתן שירותי אבטחת המידע של חברת נס לעירייה באופן כללי, ניתנים על ידי ספק שעליו המליצה חברת נס, וגם התשלום בעבור השירות מתבצע דרך חברת נס, דבר שהוא בגדר ניגוד עניינים מובהק.

המלצות

13. 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 המבוקרים

מנהל אגף מחשוב ומערכות מידע

על פי המכרז, החברה מחויבת לקיים 4 בדיקות חדירה שנתיות, שמבוצעות על ידי ספקים חיצוניים ותכולתן נכתבות ומאושרות על ידי אגף המחשוב.

עמידה בהוראות PCIDSS

בשנת 2006 הועבר תקן PCIDSS על ידי כלל חברות האשראי בעולם והוא נאכף על ידי חברות האשראי בישראל. התקן קובע כי כל ארגון **המעביר, מעבד, מכבד** או שומר נתוני כרטיסי אשראי חייב לעמוד ב-12 דרישות אבטחת המידע. חברות האשראי בישראל המפקחות על יישום תקן ה-PCIDSS דורשות בין היתר כי ימונה גורם מטעם הארגון האחראי לפיקוח על יישום התקן.

לביקורת נמסר כי העירייה אינה שומרת, מעבדת או מעבירה נתוני כרטיסי אשראי. עם זאת, העירייה "מכבדת" כרטיסי אשראי ולכן, לדעת הביקורת, עליה לעמוד בהוראות התקן. יתר על כן, העירייה

נעזרת בצד ג' לסליקת כרטיסי האשראי ולכן מוטלת עליה האחריות לפיקוח וליישום הוראות התקן הן בעירייה והן בצד ג'.

מסקנות

14. אי קיום הדרישות בתקן PCIDSS חושף את העירייה לקנסות מצד חברות האשראי ואף במצב קיצוני, לשלילת כיבוד כרטיסי אשראי על ידי העירייה.

המלצות

14. לבחון את אחריות העירייה ליישום תקן 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 המבוקרים

מנהל אגף מחשוב ומערכות מידע

ההמלצה מקובלת.

מדיניות סיסמאות ברשת למשתמשים מסוימים

מדיניות סיסמאות מחמירה יותר לרשת הארגון, תצמצם את הסיכון לגישה של גורמים בלתי מורשים לרשת או למערכות המידע בארגון.

מדיניות הסיסמאות נדרשת לחול על משתמשים של עובדים (נבדק בפרק שני בסעיף 3 בהמשך הדוח) ועל משתמשים אלה.

בבדיקת מדיניות הסיסמאות החלה על משתמשים אלו נמצאו 35 משתמשים אשר לא החליפו סיסמה למעלה מ-3 שנים.

מסקנות

15. אי החלפת סיסמה, אחת לתקופה, מגבירה את הסיכון לשימוש בלתי מורשה במשתמשים האמורים.

המלצות

15. להחליף סיסמה למשתמשים אלו אחת לתקופה בהתאם למדיניות שתיקבע.

תגובת המבוקרים

מנהל אגף מחשוב ומערכות מידע

לאחר אירוע הסייבר שחוותה עיריית ירושלים בחודש יולי אשתקד, צוות ה-System של חברת נס, בהתאם להנחיית, ביצע איפוס סיסמאות עבור כל המשתמשים המסוימים במערכות המידע. הליך זה ארך כשנה והסתיים לאחרונה. איפוס הסיסמאות יתבצע אחת לשנה, כהגדרת מדיניות החלפת סיסמאות לסוג זה של משתמשים.

ניהול מכשירים ניידים וגישה מרחוק

בשנים האחרונות, מאז מגיפת הקורונה, עבודה באמצעות גישה מרחוק למערכות ושרתי הארגונים נעשתה נפוצה מאוד.

קביעת מדיניות לגבי גישה מרחוק ומכשירים ניידים כגון: טלפונים חכמים, טאבלטים ועוד המתחברים לרשת הארגונית או למשאבי הארגון (כגון: דוא"ל ארגוני) חשובה מאוד לרמת ההגנה הקיימת בארגון. ללא מדיניות וניהול מוסדר עלול להיווצר מצב שבו מכשיר של עובד יגדיל את משטח התקיפה של התוקף.

בעירייה ישנם מכשירים ניידים הנשלטים ונמצאים ברשת העירונית, והחיבור לרשת מתבצע דרך VPN עם שם משתמש וסיסמה.

לצורכי הביקורת הופקה רשימת המורשים להשתמש במכשירים הניידים. נמצא כי הרשימה כוללת 190 מחשבים ניידים ו-323 טלפונים חכמים לשימושי הפקחים.

בבדיקה נמצא כי הרשימה מפורטת וכוללת את סוג המכשיר, שם המשתמש, קוד המכשיר וגרסת מערכת ההפעלה. הביקורת בדקה מדגמית כמה מכשירים כדי לוודא כי מערכות ההפעלה עדכניות (מערכות הפעלה שאינן עדכניות מגבירות את הסיכון לניצול חולשות על ידי תוקף) ולא נמצאו ממצאים חריגים.

עם זאת, הביקורת לא קיבלה תיעוד של סקירת הרשימה על ידי גורם מורשה מטעם העירייה, שמטרתו לוודא שאכן כל המכשירים ברשימה קיימים בפועל ונמצאים בשימוש על ידי עובדי העירייה הנדרשים לכך מתוקף תפקידם.

מסקנות

16. חיבור העובדים מרחוק לרשת העירונית נועד לתמוך בצורכי העבודה של המשתמשים, אולם הדבר טומן בחובו סיכונים, כגון: גישה בלתי מורשית לרשת הארגונית, גישה מרחוק בלתי מאובטחת וכיוצ"ב. אי ביצוע סקירה של רשימה המכילה מאות מכשירים ניידים המתחברים מרחוק לעירייה, מגביר את הסיכון לכך שיהיו עובדים המופיעים ברשימה אך בפועל אינם נדרשים להשתמש במכשיר נייד כחלק מתפקידם, או לחלופין, מכשירים שכבר אינם ברשות העירייה ועדיין מורשים להתחבר לרשת שלה מרחוק.

המלצות

16. לערוך סקירה תקופתית לרשימת המורשים להשתמש במכשירים ניידים.

תגובת המבוקרים

מנהל אגף מחשוב ומערכות מידע

בקרה על רשימת המורשים לשימוש במכשירים ניידים מתבצעת באמצעות מערכת ה-idm.

פוליסת סייבר

לאור עלייה ניכרת בהיקף ובמורכבות תקיפות הסייבר, תלות הארגונים במערכות מידע ורגולציה התגברה. בתחום אבטחת המידע והסייבר קיים ביטוח הניתן לרכישה מחברות הביטוח. ביטוח זה אמור לסייע במקרים כדלהלן:

- תשלום נזקים לצד שלישי – בגין אובדן מידע אישי, מידע תאגידי והפרת אבטחת מידע
- תשלום קנסות הניתנים לביטוח – בעקבות הפרת הפרטיות ופגיעה בחופש המידע
- תשלום הוצאות מומחי סייבר ויועצי מדיה – במקרה של משבר
- תשלום הוצאות דיווח ללקוחות – במקרה של אירוע סייבר המחייב יידוע נשואי המידע
- כיסוי לסחיטה – פיצוי בגין כספים ששולמו בעקבות סחיטה ונזקים הנלווים לה, לרבות תשלום כופר, הוצאות מומחה והוצאות ניהול המשבר
- פגיעה ברשת/ אובדן רווחים – תשלום אובדן רווחים בעקבות פגיעה מתמשכת ברשת כתוצאה ישירה מכשל באבטחת מידע

העירייה מחזיקה בפוליסת כיסוי לאירועי סייבר. בבדיקת הפוליסה נמצא כי היא נרכשה מחברת הביטוח הפניקס (מספר פוליסה 1000379/23/115/740) לתקופה מ-23.2.2023 עד 22.2.2024. להלן חלק מסוגי הכיסויים בהתאם לפוליסה:

- התחייבות על הפרטיות – עד 5 מיליון דולר
- כיסוי בגין פריצת אבטחה – עד מיליון דולר
- התחייבות אבטחת מידע – עד 5 מיליון דולר
- התחייבות מולטימדיה – עד מיליון דולר

עם זאת, לא נערכו בדיקה והערכה של הנזקים הכלכליים הצפויים מאירועי סייבר, לדוגמה: תשלום ליועצי סייבר במקרה של תקיפה, נזקים בגין תביעות משפטיות על הפרות חוק, אובדן הכנסות, פגיעה במוניטין, שיקום מערכות המחשוב לאחר אירוע וכו'.

מסקנות

17. לא נערכה בדיקה של הנזק הכלכלי הצפוי מאירוע סייבר טרם רכישת פוליסת הביטוח, וכתוצאה מכך לא ניתן להעריך מהו כיסוי הפוליסה הרצוי.

המלצות

17. להעריך את היקף הנזקים הכלכליים הצפויים מאירוע סייבר ולאחר מכן לבחון את כיסוי פוליסת הביטוח בגינם.

תגובת המבוקרים

מנהל אגף מחשוב ומערכות מידע

לעירייה קיים ביטוח סייבר.

גיבויים ושחזורים

קיימים גורמי סיכון רבים על מערכות המידע, כגון: הגורם האנושי (אם בשוגג ואם בזדון), תקלות, וירוסים, נזקי טבע, וכו'. גורמים אלו עלולים לגרום לפגיעה בנתונים המנוהלים במערכות המידע ואף להפסקת פעילות מערכות אלו. על מנת להבטיח את המשך פעילות מערכות המידע על הארגון לנקוט פעולות למיניהן - בין השאר עריכת גיבויים וביצוע שחזורים יזומים לבדיקתם.

בבדיקתנו נמצא כי קיימים שלושה סוגי גיבויים בעירייה:

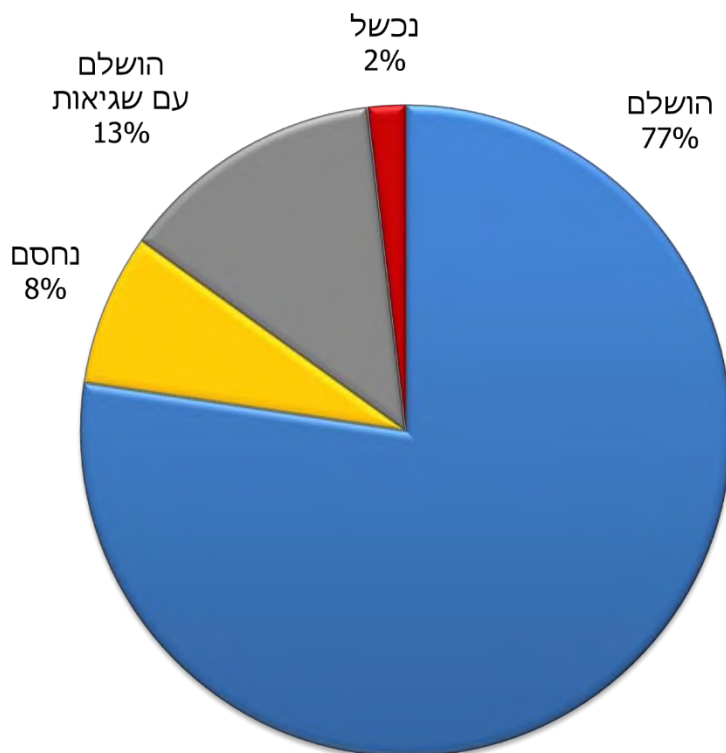
- מערכת גיבויים של חברת Commvault לניהול מערך הגיבויים בעירייה.
- גיבוי במיקרוסופט Azure למוצרי מיקרוסופט בענן כגון CRM ו-BI.
- גיבוי בקלטות למחשבי AS400 אשר הוחלפו לאחרונה.

גיבויים דרך מערכת Commvault מתוזמנים באופן יומי קבוע כגיבוי מלא לכל הרשת, למעט חלק מתיבות הדואר האלקטרוני.

נוסף על אלה, בעת כישלון של גיבוי נשלח מייל אוטומטי מהמערכת לצוות התמיכה לצורכי טיפול. צפינו במייל דוגמה שנשלח ב-17.7.2023 בגין נפילת ג'וב לריצת גיבוי (ג'וב מספר 528426). הגיבוי הוא עבור בסיסי הנתונים של מערכת אורקל. נמצא כי הגיבוי תוקן על ידי הרצה חוזרת של הג'וב.

הביקורת בדקה את תהליך השחזורים בעירייה, ונמצא כי לא מבוצעים שחזורים יזומים של מערכות או מידע, אלו מבוצעים רק לפי הדרישה. שלפנו את לוג הג'וב של השחזור במערכת לתקופה שבין אפריל 2021 ליולי 2023 ונמצא כי בממוצע מבוצעים שני שחזורים לחודש. בדיקת סטטוס ביצוע השחזורים העלתה את התוצאות כדלהלן:

תרשים 3: תוצאות השחזורים שבוצעו בתקופה אפריל 2021 עד יולי 2023



מסקנות

18. ללא ביצוע שחזורים יזומים אין אפשרות לוודא כי הגיבויים אכן מבוצעים כראוי.

המלצות

18. לבצע שחזורים יזומים לפי סבב שרתים, מערכות ובסיסי נתונים אחת לתקופה שתקבע מראש, לצורך בדיקת זמינות, שלמות ודיוק הגיבויים.

תגובת המבוקרים

מנהל אגף מחשוב ומערכות מידע

עיריית ירושלים מבצעת כ-3,000 שחזורים בשנה מכל הסוגים בצורה תקינה. לאור כמות השחזורים, לדעת מנהל אגף המחשוב אין צורך בבדיקה תקופתית.

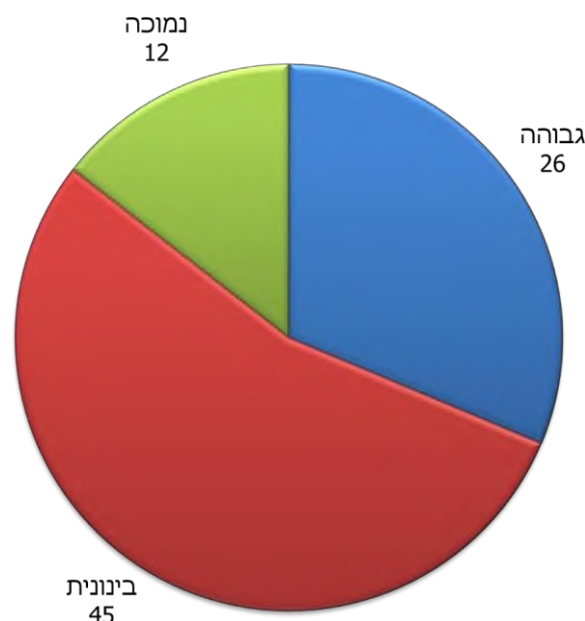
מערכות לא נתמכות על ידי יצרן התוכנה

עם סיום מחזור החיים של מערכת, יצרני המערכת מפסיקים להעניק תמיכה, תיקוני באגים ועדכוני אבטחת מידע. הדבר חושף את המערכת למתקפות סייבר שכן גורמים עוינים עלולים לזהות במערכות אלה חולשות ולנצלן לפריצה אליהן.

בעירייה קיימות 83 מערכות במצב EOL (End Of Life), כלומר היצרנים של אותן מערכות הפסיקו לתמוך בהן. בבדיקת מסמך שהתקבל מהעירייה ראינו כי המערכות הנ"ל מחולקות ל-3 רמות כלהלן:

- מערכות בעדיפות גבוהה להחלפה: מערכות המספקות שירותי רוחב עם טכנולוגיה מיושנת מאוד ולא נתמכת. מדובר במערכת עם שימושיות גבוהה.
 - מערכות בעדיפות בינונית להחלפה: מערכות עם טכנולוגיה מיושנת עם שימושיות בינונית.
 - מערכות בעדיפות נמוכה להחלפה: מערכות מתקדמות יחסית עם שימושיות נמוכה.
- להלן פילוח המערכות לפי רמת החשיבות:

תרשים 4: רמת החשיבות של מערכות לא נתמכות לפי מספר המערכות



מסקנות

19. עם סיום מחזור החיים של מערכת, יצרני המערכת מפסיקים, בין היתר, מתן עדכוני אבטחת מידע למערכת, ולכן מערכות אלה בעלות סיכון גבוה יותר לתקיפה של גורמים עוינים.

המלצות

19. 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 ולאחר בקורות מפצות כנגד פגיעויות אלו.

תגובת המבוקרים

מנהל אגף מחשוב ומערכות מידע

עיריית ירושלים התחילה פרויקט של שדרוג מערכות המידע.

פרק שני

מבדק מערכות אבטחת המידע

תשתית מערכת האנטי-וירוס

בעירייה קיימת מערכת אנטי-וירוס מרכזית של חברת Kaspersky אשר מנהלת את כל עמדות הקצה והשרתים בעירייה. נוסף עליה קיימת מערכת EDR³ של חברת מייקרוסופט אשר מנהלת בענן. מתודולוגיית בדיקת הביקורת התבססה על בדיקות תצפית וקבלת תיעוד שבו נבחנה רמת ההגנה. להלן ממצאי הבדיקה:

- כל התחנות מנוהלות על ידי מערכת אנטי-וירוס מרכזית ומעודכנת.
- המערכת שולחת התרעות במייל על אירועי הדבקה.
- המערכת שולחת דוחות סטטוס באופן שוטף.
- המערכת שומרת לוגים למשך 24 חודשים.
- המערכת מכילה תוסף EDR לחסימת הצפנה.
- המערכת מכילה מדיניות חסימת USB בעמדות קצה.
- המערכת מכילה מדיניות לבקרת גלישה בעמדות קצה.
- המערכת תואמת את הרישוי הקיים.

מסקנות

1. רמת התחזוקה של המערכת תקינה ומתבצעת בהתאם לסטנדרטים המקובלים של רמת אבטחת מידע.

תשתית מערכת ה-Firewall

מערכת Firewall היא מערכת לניטור ולחסימת תקשורת בין הרשת הארגונית לרשתות חיצוניות (כגון: רשת האינטרנט). מערכת זו היא חלק חשוב במערך אבטחת המידע של הארגונים. מתודולוגיית בדיקת הביקורת התבססה על בדיקות תצפית וקבלת תיעוד שבו נבחנה רמת ההגנה.

3 (Endpoint Detection & Response) EDR – פלטפורמת אבטחה, זיהוי ותגובה של נקודות הקצה, המספקת לארגונים את האמצעים לפקח, לאתר ולהגיב לאיומי נקודות קצה.

מסקנות

2. התחזוקה של מערכת ה-FW מתבצעת באופן חלקי.
3. ללא הגדרות מתאימות במערכת לשליחת דוחות ולשמירת לוגים לפרק זמן ארוך, העירייה תתקשה לתחקר אירועי אבטחת מידע שהחלו בצורת "זחילה" מהעבר. זאת ועוד בתנאים אלה העירייה אינה עומדת בתקנות הגנת הפרטיות.

המלצות

1. להסיר את החוקים שאינם בשימוש.
2. לוודא כי כל החוקים של ה-FW יירשמו בלוג.
3. להגדיר במערכת ה-FW פעולה לשליחת דוחות שבועיים למנהל אבטחת המידע.
4. להגדיר במערכת ה-FW שמירת לוג אירועים לתקופה של 24 חודשים לפחות.
5. להקשיח פרוטוקול מסוים.
6. לבחון חיבור כלל המשתמשים במערכת ל-AD הארגוני.
7. להגדיר במערכת ה-FW שינוי סיסמאות המשתמשים אחת לתקופה.

תגובת המבוקרים

מנהל אגף מחשוב ומערכות מידע

- המלצה 1:** מתבצע בשוטף. כדי לייעל את תחזוקת ה-FW הומלץ לרכוש ולהטמיע מערכת TUFIN.
- המלצה 2:** כדי לשמור לוגים ל-24 חודשים כנדרש, יש לבצע היערכות ורכש של תשתית שמירת לוגים בממדים אלו.
- המלצה 3+4:** הנושאים הועלו בתוכניות העבודה של שנת 2024 ויבוצעו בכפוף לתקציב שיאושר.
- המלצה 5:** הקשחת פרוטוקול מסוים תתבצע באופן מיידי.
- המלצה 6:** כלל המשתמשים המתחברים ל-FW מחוברים דרך AD – TACACS.
- המלצה 7:** שינוי סיסמאות מוגדר בהתאם להחלפת סיסמה ב-AD.

תשתית מערכת ה-Active Directory

מתודולוגיית הבדיקות של ה-AD כוללת בדיקות רחבות בכל הנוגע לרכיבי התשתית הקיימים. מתודולוגיית בדיקת הביקורת התבססה על בדיקות תצפית וקבלת תיעוד שבו נבחנה רמת ההגנה.

בבדיקה זו ניתן לקבוע באיזו מידת סיכון נמצאת הרשת ברמה הלוגית לפגיעה בסודיות, באמינות או בזמינות המידע. הבדיקה בוצעה על ידי כלי Ping Castle.

להלן ממצאי הבדיקה:

- מערכות ההפעלה בתחנות הקצה והשרתים - נמצאו גרסאות מערכות הפעלה אשר אינן נתמכות על ידי היצרן. מדובר במערכות הפעלה ישנות של שרתים ועמדות קצה אשר אינן נתמכות.
- מערכות הפעלה שאינן נתמכות על ידי היצרן מוגדרות כבעלות סיכון גבוה יותר לתקיפה של גורמים עוינים, כיוון שיצרני המערכות מפסיקים את מתן עדכוני אבטחת המידע.
- פרוטוקולים מוגדרים ברשת - על ארבעה שרתי AD מופעל פרוטוקול ישן ולא מאובטח בגרסאות smb1.
- הגדרות רישום ובקרה - מערכות הרישום והבקרה בשרתים מיושמות בצורה חלקית.
- חשבונות משתמשים - נמצאו חשבונות משתמשים המוגדרים כלא פעילים וכאלה שהסיסמה שלהם לא השתנתה זמן רב.
- נמצאו אובייקטים שיש להם הרשאות עודפות.
- אדמיניסטרטורים ברשת - נמצא כי לחלק מהאדמיניסטרטורים קיימת אפשרות לבצע דלגציה לא מאושרת, כלומר לתת הרשאות נוספות למשתמשים אחרים.

מסקנות

4. רמת התחזוקה של המערכת בינונית ואינה תואמת את הסטנדרטים המקובלים של רמת אבטחת מידע. בשל כך העירייה חשופה לסיכונים הדבקה ופגיעה פוטנציאליים במערכת המרכזית.

המלצות

8. להסב מערכות הפעלה אשר אינן נתמכות על ידי היצרן למערכות הפעלה נתמכות (וכן למחוק מערכות אשר אינן בשימוש).
9. להגדיר הקשחות במחשבים בהתאם לשיטות עבודה מקובלות ולהסיר פרוטוקול ישן.
10. לבצע שינוי הגדרות מידע ולהחליף סיסמאות לפחות אחת ל-180 יום.
11. ליישם בקרה בכלל השירותים לפי שיטות עבודה מקובלות.
12. לבצע את הפעולות האלה:
- 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](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".

תגובת המבוקרים

מנהל אגף מחשוב ומערכות מידע

הסבת מערכות הפעלה מתבצעת בהתאם לתוכנית שדרוג המערכות. הסרת פרוטוקולים ישנים תבוצע לכשיתאפשר, לאחר שדרוג מערכות ישנות כגון מערכת חנייה, ניהול פרויקטים, ועדות ועוד.

טיוב GPO יתבצע במהלך שנת 2024.

נדרש פירוט הממצאים בכלל בנושאי Active Directory.

תשתית מערכת עדכוני אבטחת מידע

קיימת מערכת מרכזית SSCM אשר מנהלת את כל עמדות הקצה והשרתים בארגון. כמו כן, קיימת מערכת INTUNE, אשר מנהלת את עמדות הקצה והשרתים בארגון והתאמתם למדיניות אבטחת המידע בארגון.

להלן ממצאי הבדיקה:

- קיימים עדכוני אבטחת מידע ברמה גבוהה אשר לא הוחלו בזמן על שרתי ה-SQL.
- המערכת לא הוגדרה לשלוח דוחות תקופתיים למנהל אבטחת המידע לגבי סטטוס עדכוני האבטחה בעירייה.

מסקנות

5. רמת התחזוקה של המערכת תקינה ובהתאם לסטנדרטים מקובלים של רמת אבטחת מידע. עם זאת שתי הגדרות דורשות שינוי, ובשל כך העירייה חשופה במעט לסיכוני הדבקה ופגיעה פוטנציאליים.

המלצות

13. לבדוק אחת לחודש לפחות אם קיימים עדכונים לשרתי ה-SQL. לכשיימצאו עדכוני אבטחת מידע בעלי חשיבות גבוהה יש לבצע עדכון ללא דיחוי.
14. להגדיר במערכת שליחת דוחות תקופתיים למנהל אבטחת המידע לגבי סטטוס עדכוני האבטחה בעירייה.

תגובת המבוקרים

מנהל אגף מחשוב ומערכות מידע

המלצה 13: קיים נוהל הטמעת עדכונים וחברת נס עובדת על פיו.

המלצה 14: חברת נס תפעל לטיפול בממצאים אלו, בהתאם לחומרתם ובמסגרת תוכניות העבודה.

סיכום

בשנים האחרונות ישנה עלייה מתמדת בהיקף ובעוצמת תקיפות הסייבר בארץ ובעולם. בין המותקפים ניתן למנות בתי חולים, אוניברסיטאות, עיריות, חברות ביטוח, תשתיות, אתרי אינטרנט ועוד. המתקפות עלולות לערער את היציבות הארגונית, לפגוע בנכסי הארגון, במוניטין שלו ובלקוחותיו, ולעיתים אף לסכן חיי אדם.

הגורמים הפוטנציאליים לתקיפות ברשויות המקומיות יכולים להיות בעלי אינטרס כלכלי, גורמים אנטי-ישראליים, גורמים פנימיים להשגת רווח או גרימת נזק מכוון ואף גורמים מדינתיים כחלק ממאבק אידיאולוגי.

עיריית ירושלים היא יעד מרכזי לניסיון תקיפות סייבר, וזאת בין היתר בשל היותה עיר הבירה ואחד הסמלים החשובים של מדינת ישראל. ניסיונות חדירה למאגרי המידע, תקיפה והשחתה של אתר האינטרנט ומניעת שימוש במערכות, הן רק חלק מהסיכונים הקיימים במרחב הסייבר של העירייה.

תקיפה של מערכות העירייה עלולה לשבש מערכות קריטיות של כריזה, גבייה, ניהול וסיוע לתושבים ועוד.

האחריות ליישום מנגנוני אבטחת המידע בעירייה היא של אגף מחשוב ומערכות מידע במינהל אסטרטגיה וחדשנות, המונה כ-200 עובדים, אשר רובם עובדי מיקור חוץ. האחריות להתוויית המדיניות והפיקוח על יישום מנגנונים אלו מוטלת על יחידת אבטחת מידע הכפופה למינהל משאבי אנוש ומינהל עירוני, יחידה הדלה במשאבים תקציביים ובכוח אדם.

כדי לצמצם ככל האפשר את הסיכונים במרחב הסייבר נדרש למפות ולהעריך את הסיכונים הקיימים, להתוות מדיניות הגנה ברורה ולפקח על יישומה באופן שוטף.

הביקורת בדקה את המדיניות והנהלים בנושא אבטחת המידע, בחנה את מנגנוני האבטחה הקיימים והמופעלים בעירייה ואף ביצעה מבדקי חדירה למערכות של העירייה כדי להעריך את רמת אבטחת המידע בהן.

הביקורת העלתה ליקויים מהותיים לגבי התוויית המדיניות ונוהלי אבטחת המידע של העירייה, העמידה בהוראות חוק, בתקנים ובסטנדרטים המקובלים, העמדת המשאבים המוקצים לפיקוח על אבטחת המידע והסייבר ועוד. מכלול הממצאים שצוינו בדוח מגבירים את הסיכון לתקיפה של מערכות העירייה.

על העירייה לטפל בממצאים שהועלו בהקדם, בדגש על גיבוש מסמך מדיניות ועדכון הנהלים, ביצוע תהליך הערכת סיכונים, טיפול בפערים הטכנולוגיים שנמצאו - לרבות במבחני החדירה - והקמת ועדת היגוי אשר תפקח, תדווח ותייעץ להנהלת העירייה בקבלת החלטות בעלות משקל בתחום אבטחת המידע.

אף שלא ניתן למנוע באופן מוחלט אירועי אבטחת מידע וסייבר, אירועים שבשנים האחרונות התגברו והפכו מוחשיים וקריטיים יותר, היערכות נכונה לקראתם תהפוך את ההתמודדות עימם למוצלחת יותר וקלה יותר. היערכות נכונה מראש יכולה לקצר את זמני התגובה, לאפשר להנהלה לקבל החלטות מושכלות ונכונות יותר, לאפשר לעירייה לעמוד בחובותיה הרגולטוריות, וכפועל יוצא להפחית את הסיכונים למיניהם מעצם התרחשות האירוע.

דוח שנתי 2023

אבטחת מידע וסייבר

אני מבקש להודות למבקרת העירייה על עריכת דוח מפורט בנושא זה, אשר פרט לפירוט הממצאים בו, כולל סקירה מעמיקה לגבי נושא אבטחת מידע וסייבר שהוא נושא חשוב ומהותי בעל השלכות על העירייה ועל תושביה.

החשיבות הרבה של הדוח טמונה בכך שאבטחת מידע הפכה לצורך בסיסי לאור העלייה המתמדת בהיקף ובעוצמת האיומים במרחב הסייבר בעולם כולו ובישראל בפרט. רשויות מקומיות מהוות לצערי כר פורה למתקפות סייבר, בשל היקף השימוש שלהן במערכות מידע, בשל השימוש הרב באמצעים טכנולוגיים, בשל המידע הרגיש והרב שהן מחזיקות ובשל רמת המוכנות וההגנה הנמוכות יחסית בחלק מן הרשויות.

בהתאם, במהלך השנים האחרונות היינו עדים למספר מתקפות סייבר על גופים ציבוריים לרבות עיריות, ואף עיריית ירושלים הייתה חשופה בעבר למספר ניסיונות למתקפה כפי שמוזכר בדוח. העירייה בראשותי מתייחסת לאיום הסייבר ברצינות מלאה וביצעה פעולות רבות בהשקעת משאבים לא מבוטלת (כמפורט בדוח, תקציב העירייה בתחום אבטחת המידע הכפיל את עצמו בין השנים 2019 ל-2022), בכדי לוודא כי העירייה תהיה במוכנות מספקת למתקפה.

על אף שנראה כי חל שיפור מתמיד בהתנהלות העירייה בתחום זה (וניתן לראות אותו ביחס לדוח מבקרת העירייה שנערך בעניין זה בשנת 2019), עולה מהדוח כי עדיין קיימים פערים ומקומות שבהם העירייה נדרשת לשפר את פעילותה.

אני רואה חשיבות גדולה בטיפול מהיר בליקויים שנמצאו. אבטחת מידע וסייבר נועדו להגן על העירייה וכפועל יוצא מכך על הציבור. ניתן רק לתאר את הכאוס האפשרי שעלול להיגרם כתוצאה מהשבתת תשתיות תחבורה כמו רמזורים או השמדה של מאגרי מידע עירוניים על ידי גורמים עוינים או בשוגג. על העירייה להתייחס לאיומי הסייבר כאיום על פעילותה הרציפה והסדירה לכל דבר ועניין.

הביקורת גילתה ליקויים רבים בהתנהלות העירייה בעניין זה. מספר רב של ליקויים נגעו לנושא רגולציה, מדיניות, נהלים ותהליכים בתחום אבטחת מידע וסייבר. כך לדוגמה, נמצא כי בידי העירייה לא קיים מסמך מדיניות אבטחת מידע וכי נוהלי אבטחת המידע של העירייה לא עודכנו לאחרונה. כמו כן, נראה כי לא קיים תהליך הערכת סיכונים בנושא זה וכי לא קיימת ועדת היגוי בנושא אשר תתווה מדיניות ותפקח על יישומה. הביקורת הצביעה גם על ליקויים בנושא יחידת אבטחת המידע, אשר לדעת הביקורת מתקשה למלא כראוי את תפקידה בגלל תקציב נמוך יחסית ומגבלות כוח אדם. בנוסף, נמצאו ליקויים ובעיות במבדקי חדירה, וניגוד עניינים אפשרי שבו עלול להימצא ספק המחשוב העיקרי של העירייה.

מעיון בדוח מבקרת העירייה בנושא זה, עולה כי גם הגורמים המקצועיים בעירייה הסכימו עם רובם ככולם של ממצאי הדוח, מה שמעיד על כך כי הצורך בשיפור התנהלות העירייה בנושא זה אינו מוטל בספק. אין ספק שקיים בראש ובראשונה צורך בגיבוש מדיניות אבטחת מידע ופיקוח על יישומה, בעדכון נוהלי אבטחת המידע ונוהלי הגיבויים והשחזורים של העירייה, פיקוח על יישומם והעלאת הנהלים המעודכנים לפורטל העירייה. כמו כן, בכפוף למגבלות תקציביות כמובן, יש לעבות את הצוות הרלוונטי ביחידת אבטחת המידע ולספק לה את המשאבים הדרושים למילוי תפקידיה. בנוסף, יש צורך בקיום תהליך הערכת סיכונים בתחום מערכות המידע בעירייה ובטיפול בליקויים שנמצאו בקשר עם ממצאי מבדקי החדירה השונים. יש גם צורך במיפוי הפערים בין הדרישות בתקנות הגנת הפרטיות והתקנים הרלוונטיים לבין המצב הקיים בעירייה, ובטיפול בפערים בהקדם.

עיינתי בתגובת גורמי המקצוע השונים, ובכלל זה מנהל אגף מחשוב ומערכות מידע והממונה על אבטחת מידע. אני מברך על תגובת גורמי המקצוע מהם עולה כי הם מקבלים את רובן של ההמלצות, לרבות ההמלצות בדבר הכנת מסמך מדיניות ועדכון נוהלי אבטחת מידע, ואף החלו ליישמן. כמו כן, גורמי המקצוע התחייבו לפעול בכובד ראש על מנת לאמץ את שאר המלצות הביקורת. תגובתם מעידה על רצון אמיתי לשיפור וטיוב את התנהלות העירייה בנושא זה לטובת הציבור.

עיריית ירושלים בראשותי תמשיך להשקיע ולקדם את נושא אבטחת המידע, בוודאי לאור המצב הביטחוני ולאור הגידול בכמות אירועי הסייבר והתגברות הסיכון הנשקף לרשויות המקומיות, והכול בכדי להיות מוכנים למתקפה הבאה ולהגן על העירייה ועל תושבי העיר באופן המיטבי.

הנחתי את מנכ"ל העירייה לבצע מעקב על יישום המלצות הביקורת על ידי הגורמים המקצועיים הרלוונטיים, לרבות בחינת האפשרות לטיפול בפערים הטכנולוגיים שנמצאו – לרבות במבחני החדירה – וקידום תהליך הקמת ועדת היגוי אשר תפקח, תדווח ותייעץ להנהלת העירייה בתחום אבטחת המידע.



הוועדה לביקורת – תמליל

מספר הוועדה : 12

מקום ההתכנסות : אולם הנהלה 2

תאריך הוועדה : ז' באלול תשפ"ד (10.9.2024)

מזכיר הוועדה בדיון : צבי עבו

שעת תחילת הוועדה : 13: 53

שעות סיום הוועדה : 14: 47

התמליל נכתב ע"י חברת גולד וורק בע"מ ולא עבר בדיקה או הגהה ע"י גורם כל שהוא בעיריית ירושלים

עיריית ירושלים וחברת גולד וורק בע"מ עושים כל שביכולתם על מנת לייצר תמליל איכותי ובעל ערך. עם זאת מודגש כי קריאה בתמליל צריכה להיעשות באופן מושכל תוך הבנה שיתכנו טעויות ו/או השמטות מסיבות אובייקטיביות שונות.



גולד וורק תמלול והקלטה

גולד-וורק ת M ג R ים

יו"ר אלדד רבינוביץ:

אני מתכבד לפתוח דיון וועדת ביקורת מספר 13, אבטחת מידע לסייבר. אנחנו חלמנו כשנגיע לארץ אבותינו, נגיע למנוחה ונחלה. ברוך השם אנחנו הגענו לכאן, אבל מנוחה ונחלה, הם קצת פחות. יש הרבה מאוד איומים מסביבות, אנחנו חווים אותם, אנחנו מרגישים, יש איום מאוד משמעותי שאנחנו פחות מדברים עליו, פחות מכירים אותו איום דיגיטלי. לא יודע אם דיגיטלי זה המושג הנכון, אבל איום, איום ברשת, איומים ממשיים, איומים משמעותיים, עם הרבה מאוד השלכות בעולם הפיסי שלנו, מתחילים לאט לאט להבין, שומעים קצת בחדשות, שומעים קצת את מה שאנחנו עושים, מה שעושים לנו, זה אירוע שהוא מאוד משמעותי וצריך להיערך לו. תחום שמאוד קשה להבין בו, מאוד מאוד מקצועי, תחום שמשנתה מאוד מהר, כבר לא מספיק מוחשי, אתה לא תמיד רואה כשהותקפת, אתה לא תמיד מבין, מה יש לך מה אין לך, לפעמים זה מוזנח. אנחנו כאן הביקורת נעשתה, כדי שזה לא יוזנח, והעירייה משקיעה הרבה מאוד, כדי שזה לא יוזנח, ובשביל זה אנחנו כאן, בעזרת השם נשתפר תמיד.

עפרה ברכה:

זהו, אז הביקורת באמת ביצעה את הנושא הזה מאוד מאוד חשוב, מאחוריו רואה חשבון שלומי בני, שזה הוא התחום ההתמחות שלו, לערוך את הביקורת, ואני מאוד מקווה שנשמע שהעירייה באמת נקטה בצעדים, כי מצאנו באמת שיש צורך לעשות, לאץ מספר המלצות, כדי שהעירייה תהיה מוגנת ככל שניתן, ערוכה, לכל חלילה קטסטרופה שתגיע גם מההיבט הזה חס וחלילה. אני מעבירה לך את זה שלומי, בבקשה.

שלומי בני:

אוקי, תודה, אז אני אציג את עצמי, כולכם מכירים, אז שמי שלומי בני, כמו שעפרה ציינה, אני רואה חשבון במקצועי, אבל תחום ההתמחות שלי זה מערכות מידע וסייבר, רואה חשבון בא מעולם ניהול הסיכונים, אז איפה שהוא מתחבר. אני שותף במשרד RSM שיף הזנפרץ ושות', זה פירמה בינלאומית, מאוד מאוד גדולה, שמספקת בין היתר שירותי אבטחת מידע וסייבר. ואחת ההתמחויות שלי, זה בעצם ביקורות פנימיות בתחום הסייבר, גם בעירויות, בארגונים גדולים, מכונים, בנקים, וכולה. ופה בעצם נתבקשתי לסייע בביקורת פנימית בתחום אבטחת המידע והסייבר של העירייה. בעצם כללנו את רוב הנושאים בתחום של אבטחת מידע וסייבר, כמו שניתן לראות. אם יש שאלות, תרגישו בנוח, באמת נושא יותר טכני, יותר טכנולוגי, אבל תרגישו בנוח, אם אני מדבר בגיבריש, תעצרו אותי.

אלדד רבינוביץ:

אני לא מתחייב להבין הכול, אני אנסה.

שלומי בני:

אני אדאג שאתם תבינו את הדברים החשובים. בסדר? טוב, אז קודם כל עיריית ירושלים, יש לה מספר רב של מערכות מידע, אני אומר בין 200 ל – 400, תלוי את מה סופרים בתור מערכת או לא, תלוי את מי שואלים, אז בגדול יש הרבה מאוד מערכות נקרא לזה. יש חוקים שהעירייה צריכה לעמוד בהם, כמו כל גוף בישראל, יש את חוק הגנת הפרטיות, תקנות אבטחת המידע הגנת הפרטיות. ויש דברים שהם וולונטוריים, כמו איזואים, כמו כל מיני כאלה. אנחנו בעצם התמקדנו בנושא של אבטחת מידע, בהתאם לתקנות הגנת הפרטיות, בהתאם לתקנים, מובילים, מערך הסייבר הלאומי ניסט וכולה, באמת לראות איפה העירייה עומדת, ביחס לתקנים, ולבסס פרקטיס מה שנקרא. הביקורת שלנו בעצם, אם אני מחלק אותה, לסבר את האוזן, אז היא התחלקה לשלושה נושאים, הנושא הראשון בדקנו את כל הצד הרך, כל הנושא של מדיניות, של נהלים, כל הנושא של וועדת היגוי באבטחת מידע וסייבר, כל העולם הזה של הנהלים והמדיניות. הנושא השני זה מבדק טכנולוגי שבאנו ובדקנו את המערכות אבטחת מידע של העירייה, איך הן פועלות, אנטי - וירוס, בטח כולכם מכירים, חומת אש מי שאולי לא מכיר, זה איזה שהוא כלי שמפריד בינך לבין, בין המערכות לבין האינטרנט, עוד כל מיני מערכות אבטחת מידע, איך בעצם הגדירו אותם, האם הגדירו אותם נכון, האם לא הגדירו אותם נכון, האם יש,

אלדד רבינוביץ:

האם הן קיימות.

שלומי בני:

האם הן קיימות, נכון שאלה, הערה מצוינת, מעולה. והחלק האחרון עשינו מבחני חדירה לשתי מערכות שבחרנו מתוך, כמו שצינתי 200 או 400 מערכות, איך שאנחנו לא מסתכלים על זה. אז זה בעצם שלושת החלקים של ה - . הממצא הראשון זה בעצם שבעירייה לא קיים מסמך מדיניות אבטחת מידע, ונהלי אבטחת המידע לא עודכנו שנים רבות. בנוסף חלק מהנהלים, בכלל הם לא מופיעים בפורטל העירייה. אז אני מסתכל רגע מהצד שלי, אני אגיד לכם עד כמה, עד כמה אני רואה את זה בחומרה נקרא לזה, בסדר? אני אומר גוף כזה שהוא באמת סמל, הייתי מצפה שבאמת יהיה מדיניות, שיהיו נהלים, שתהיה וועדת היגוי, זה צריך להיות מאוד מאוד ממוסד, אני מגיע לחברות שהן יותר קטנות, חברות קטנות מאוד, שכבר אצלם יש מדיניות, שמכילים אותה, ונהלים, ומעדכנים אותה. אז בטח ובטח בגוף כזה שיש לו מאגרי מידע מאוד מאוד רגישים, ולכן כמובן שזה, זה משהו שצריך לעמוד לנגד עיניכם, כנגד העירייה, ולגבש את המדיניות, לעדכן את הנהלים, לתקשר אותם, וכולה. אני חייב לציין אולי עוד איזה שהיא הערה, לגבי גן כל הדו"ח ייאמר לזכות העירייה לזכות הגורמים שקיבלו את ההמלצות, קיבלו את הממצאים, קיבלו את ההמלצות, לא היה ויכוחים, יש כאלה מבקרים מתחילים להתווכח שלושה חודשים, בסוף את הרוב מקבלים. באמת קיבלו פה את הרוב, ויאמר לזכותם שלא היה יותר מידי דיונים, באמת מה שרשמנו מה שהעלינו באמת,

אלדד רבינוביץ:

רוצה להגיב? ציון.

ציון סמולר:

כן, בעיקרון הוועדה לצערי עדיין לא הוקמה, זה דבר אחד, לא הוקם הוועדה, אבל הנוהל קיים, זאת אומרת יש נוהל, לא שם ברמה הפורמאלית, זאת אומרת צריכה לקום הוועדה, מבחינת ההיגוי שתיתן באמת את האישור הראסמי. חוץ מזה יש כבר טיוטה, טיוטה של נוהל, שזה בצורה מאוד מאוד (לא ברור), רק צריך לאשר אותה.

אלדד רבינוביץ:

תגובות, לפני כמה חודשים טובים, שהיא מוקמת ו –

ציון סמולר:

נכון, זה שני ראשי מנהלים, ברמת העיקרון יש שמה, את רני שהוא עוזב, רני רוזנהיים, ולגבי כוח צריך פשוט לראות, צריך לגבש את זה, צריך שזה יקרה.

אלדד רבינוביץ:

מי אחראי שזה יקרה?

ציון סמולר:

לא אכפת לי להיות אחראי להוביל, אבל,

אלדד רבינוביץ:

הוסמכת. טוב חשוב שיהיה מישהו שידחוף את זה קדימה, אחרת זה יישאר באותו סטאטוס עוד כמה חודשים. אז זה מצוין.

ציון סמולר:

בשמחה.

אלדד רבינוביץ:

אתה ראית את הטיוטה שלהם?

שלומי בני:

כן, הייתה איזה טיוטה שאנחנו קיבלנו, אבל באמת היא ברמת טיוטה, עם הערות וסימונים בצהוב, כך שמבחינתי זה לא, זה אפילו לא הגיע לשלב של טיוטה סופית, נקרא לזה לפני שאושרה.

אלדד רבינוביץ:

אולי כדאי להראות?

שלומי בני :

כן,

אלדד רבינוביץ :

כן?

שלומי בני :

בטח, בוודאי הערה 2 אולי זה מצוין, כן, בהחלט, בשביל זה אנחנו פה.

אלדד רבינוביץ :

לא חלילה מתוך זלזול וזה, תמיד עין, עין נוספת מבחוץ זה תמיד,

ציון סמולר :

חד-משמעית.

אלדד רבינוביץ :

מאוד מועיל בכל דבר. מצוין.

שלומי בני :

אוקי, אז דבר נוסף. בדרך כלל אנחנו רואים יחידות אבטחת מידע בארגונים בסדר גודל הזה, נאורות בכוח אדם, אז אני לא מצפה שיהיה פה 50 אנשים, אבל אני מצפה שיהיה איזה שהוא תקציב סביר, הולם, לנושא אבטחת מידע וסייבר, ובאמת ראינו משהו פה, שיש פה בחור מאוד נחמד, מוכשר, אבל זה עדיין זה בחור, בחור וחצי אני קורא לזה, שמנסים לעשות איזה שהוא משהו עם תקציב מאוד מאוד דל, אנחנו חושבים שצריך לעבות אותו, לסדר אותו, אולי לשנע, אני לא יודע, אני לא, אני לא מתערב כרגע מאיפה להביא את הכסף, אבל אולי מ - , מאגף מחשוב, אני לא יודע, אבל צריך פה,

אלדד רבינוביץ :

כסף,

דודו אמזלג :

אפשר לשאול?

שלומי בני :

איד?

דודו אמזלג:

מה ההיקף שהוא לא דל? אנחנו מדברים,

ציון סמולר:

אני רק אגיד שנמצא בתל – אביב.

עפרה ברכה:

אבל נעשו עוד כמה דברים מאז, נדמה לי שגם הוא תוקצב קצת או משהו.

דודו אמזלג:

לכן אני שואל, מה, שנבין מה, מאיפה אנחנו, כמה אנחנו רחוקים,

עפרה ברכה:

מאפס לכמה?

דודו אמזלג:

ההליך,

עפרה ברכה:

היינו במצב שאין לו תקצוב.

דודו אמזלג:

לא תקצוב,

שלומי בני:

כן, כן, כמעט אין תקצוב.

ציון סמולר:

לא, הוא כתב, הוא כתב.

עפרה ברכה:

היה מצב מאוד,

ציון סמולר:

הוא כתב באופן כללי שמכל התקציב העירוני צריך להיות 0.8% שנמצא בתקצוב,

עפרה ברכה:

כן,

ציון סמולר:

בתקציב מטורף, זה פי 100.

שלומי בני:

כן,

עפרה ברכה:

הוא היה במצב,

שלומי בני:

בוא נהיה פי 10 ממה שיש היום,

ציון סמולר:

כן,

שלומי בני:

אז אנחנו כבר נהיה במקום טוב.

ציון סמולר:

אנחנו הכי,

אלדד רבינוביץ:

ראיתי שכתוב שיש שני תקנים.

ציון סמולר:

זה לא התקנים, עכשיו הוא מדבר על הכסף. עכשיו לגבי התקנים, בעיריית תל – אביב יש 20 תקנים, אבטחת מידע ארגון שהוא חצי מאיתנו.

אלדד רבינוביץ:

חצי גודל, כן,

ציון סמולר:

חצי גודל,

שלומי בני :

אני רק אחדד, כי אני גם מכיר את עיריית,

עפרה ברכה :

קודם כל עשו כמה שינויים גדולים, אולי תתייחס לזה.

ציון סמולר :

כן,

עפרה ברכה :

לא, זהו, אז אני אומרת אולי כדאי להתייחס לזה, בהתייחסות.

ציון סמולר :

הוקם האגף, הוקם, יש גם פיבה מאוד משמעותי, שהם הייתה צריכה להיות פה, אני לא יודע מה זה, ה – DPO, שהוא בעצם קצין המחשוב, שזה התייחסות מעמיקה,

עפרה ברכה :

האגף לאבטחה,

שלומי בני :

אז עקפת את הנושא של פרטיות בצורה רצינית.

ציון סמולר :

האגף הסייבר הוקם,

עפרה ברכה :

זה כן,

ציון סמולר :

במקביל, הוא צריך להיות כפוף, יש פה לפי החוק, יש יצא חוק חדש של הגנת הפרטיות, ממש מתעדכן בימים האחרונים.

שלומי בני :

יצא, אושר?

ציון סמולר:

יצא אושר, בסדר.

שלומי בני:

כן,

דודו אמזלג:

לפי מה שבדקת, צריך לשים 100 מיליון שקל, אז,

ציון סמולר:

כן, זה מה שכתוב באומדן.

שלומי בני:

לשים 10 מיליון, אנחנו כבר נהיה במקום טוב.

עפרה ברכה:

זה לא 10.

שלומי בני:

עזוב, שלא לפרוטוקול. קיבלת הנחה, קיבלת הנחה.

ציון סמולר:

חשבון אני יודע לעשות,

דודו אמזלג:

צריך לעבוד,

ציון סמולר:

ככה שזה לדיון פנימי. ככה זה דיון פנימי, אני מאז,

שלומי בני:

טוב.

ציון סמולר:

ובעצם הפיבה מאוד מאוד משמעותית, כי הנקודה היא של הגנה על הפרטיות, מידע עירוני זה משהו שהוא מאוד מאוד משמעותי, יש וועדת דווקא בנושא הזה יש וועדה, זה שאברוס כבר נכנס לזה בצורה מאוד מאוד חזקה.

עפרה ברכה :

מיכאל היה מנהל, אחראי על אבטחת מידע,

ציון סמולר :

מיכאל אחראי על הכול, היה את מיכאל מזרחי,

עפרה ברכה :

זהו.

ציון סמולר :

שאחראי באמת על כל מה שקורה (לא ברור).

עפרה ברכה :

בדיוק, אז עכשיו יש לנו את הבחור שהיה פה היום.

ציון סמולר :

אברוס, כן, הוא היה בבוקר.

עפרה ברכה :

הוא ממונה אבטחת מידע?

ציון סמולר :

הוא הגנת הפרטיות.

עפרה ברכה :

זהו, רציתי להסביר.

ציון סמולר :

מבחינת החוק צריך למנות,

עפרה ברכה :

זהו,

ציון סמולר:

פיבה כזאתי,

עפרה ברכה:

נכון,

ציון סמולר:

אנחנו הגדלנו,

עפרה ברכה:

נכון,

ציון סמולר:

את (לא ברור) בסשן הזה. מה שכן צריך כן להגדיל משאבים, דודו דווקא כן יודע לסיים, אחרי שהוא מבין את הנקודות הוא נרתם ועוזר פה בצורה בלתי רגילה, לפחות בכובע הקודם שהיה לי. אנחנו פה נמצאים באמת דו"ח ביקורת שהיא דבר ראשון תודה רבה עליו, אני קראתי אותו, והתחלתי לקבל סוג של ראייה מה קיים, מה צריך לעשות, זה גם נכנס כחלק מהתוכנית עבודה גם לתקצוב.

שלומי בני:

אוקי,

אלדד רבינוביץ:

אז רגע, אז מבחינת תקצוב מה יש לנו עכשיו בתקציב הנוכחי?

ציון סמולר:

תענה.

דודו אמזלג:

שנתנו איזה שהוא פלסטרים, היה את האירוע עם מייקרוספט.

ציון סמולר:

תמיד, תמיד כשהיה צריך משהו, בנקודה של חלון צפות, כל דבר, גם הייעוץ פה, זה סכומים אחרים, זה סכומים של אנשים מאוד מאוד מקצועיים, אתה יכול לחזק אותי בנקודות האלה, כל דבר פה הוא באמת יוניק, בצורה, יש שבעה רבדים שצריך להגן עליהם, בארגון שלנו והם מעבר לזה. בסדר? עכשיו לכל דבר פה, נדרש התייחסות, נדרשת תוכנית עבודה מסודרת. כמוכן שהתקציב עכשיו לא

יכול להישאר כמו התקציב שקיים היום. הכנתי תוכנית ראשונית בשביל להקים, נתחיל לעשות פה גם ברמה של המבנה של הכוח אדם, גם במבנה של התקציב הנדרש פה, בשביל לתת מענה לדוח מבקרת, יש פה דו"ח של סקר סיכונים שערכנו אותו, של BDO, עשיתי אותו במקביל בכובע השני שלי וזה משרת אותי עכשיו,

דודו אמזלג:

אנחנו גם בדיוק בתקופת,

ציון סמולר:

תקציב.

דודו אמזלג:

דיוני תקציב, אז,

אלדד רבינוביץ:

הגשת את זה, הגשת את זה שם בעצם.

דודו אמזלג:

כן,

ציון סמולר:

היום בבוקר היה סבב א', אצלנו, אנחנו כבר רפרנטים בתקציבים, הצגתי להם אותה, את ה - ,

עפרה ברכה:

אני שואלת, כי אני באמת רוצה להבין, הנושא של מיכה של אבטחת מידע, הוא מתוקצב? של - .

דודו אמזלג:

של מה?

עפרה ברכה:

של מיכה הוא אבטחת מידע, בסדר, ציון אתה מנהל אגף אתה, אני שומעת שאתה גם יודע לדאוג לדברים שלך, אתה עשית תוכנית עבודה, תיכף גם תגיע, מישהי שתחליף את,

ציון סמולר:

איתמר.

עפרה ברכה:

מנמ"רית חדשה, כן, שנבחרה במכרז. אבל מיכה בעצמו, שהוא כבר עכשיו כפוף גם כן לאותו מינהל שלכם, נכון?

ציון סמולר:

הוא כרגע כפוף לאגף המחשוב בשלב הזה,

עפרה ברכה:

והוא מקבל תקצוב שהוא צריך כדי לנהל את כל נושא,

דודו אמזלג:

שוב, בגלל שהוא כפוף לאגף המחשוב, אז התקציבים, אנחנו די נותנים שם גמישות בתקציב המחשוב, האם נקבע בהתאם לדרישות תקציב, למשל שהיו שנה שעברה, אוקי, הוגשה לשנת תקציב,

עפרה ברכה:

טוב.

דודו אמזלג:

תוקצב מה שתוקצב, אבל לא ספציפית, כמובן שלקחו בחשבון גם את הדרישות של ה - , של הסייבר מה שהוא העלה אז, ניתן תקציב כלשהו, לשחק בו, עוד פעם אני אומר, גם כשנדרש במהלך השנה שנתיים האחרונות תקציב נוסף עבור אירועים ספציפיים, עבור יועצים, עבור,

ציון סמולר:

תמיד עוזרים, נעזרים.

דודו אמזלג:

ניסו לעזור אחד לשני,

שלומי בני:

אבל זה נשמע,

עפרה ברכה:

אני רוצה להיות במצב,

שלומי בני:

זה בדיוק העניין,

עפרה ברכה:

שאנחנו לא (לא ברור).

דודו אמזלג:

עוזרים, זה נשמע כאילו עושים, עושים טובה (לא ברור).

ציון סמולר:

לא, לא,

עפרה ברכה:

אני רוצה להיות במצב שאנחנו נערכים,

דודו אמזלג:

(לא ברור) שאגף התקציבים מסייע במהלך השנה, צריך להבין שהנהלת העירייה קבעה את תקציב האגף לא משנה, כרגע זה מחשוב, או כל אחד אחר, שבתוך הסייבר, אוקי, נקבע תקציב בתחילת שנה, זה לא שבמהלך שנה עכשיו יש לי פתרונות קסם למצוא פה מיליונים,

שלומי בני:

ברור, ברור.

דודו אמזלג:

אוקי, אז אנחנו מסייעים, זה אומר אנחנו עושים מאמצים,

שלומי בני:

כן, אבל אני חושב שצריך לטפל בזה מהשורש, צריך להיות תקציב.

דודו אמזלג:

השורש,

אלדד רבינוביץ:

זה מה שעכשיו מה שבדיוני התקציב בעצם יש, מאה אחוז התייחסות,

דודו אמזלג:

דיני תקציב מגיעים ההחלטות של מה שלא סוכם, להנהלת העירייה, ומנסים שם, לכן אני אומר קודם כל זה מתודה, מה שנקבע שנה שעברה הוא נקבע, אז אני לא יכול, לא מקבלת החלטות לבד בסוף אז אני בסופו של דבר אומר, שגם למרות שנקבע אתה עוזר, ואתה משנע ממקום למקום, או,

עפרה ברכה:

כן, אם יש בעיה,

דודו אמזלג:

בשנים הבאות הולך תקציב ייעודי לאבטחת מידע,

ציון סמולר:

כן, בעזרת השם.

דודו אמזלג:

אבטחת מידע או לסייבר, דיוני תקציב, ציון יגיע הדרישות שלו נראה מה החלטת, החלטת העירייה.

עפרה ברכה:

טוב.

אלדד רבינוביץ:

מצוין.

שלומי בני:

לא קיים, או לא בוצע, תהליך הערכת סיכונים לבחינת הסיכונים הפוטנציאליים, אליהם חשופה העירייה בנושא אבטחת מידע, ולא בוצע סקר סיכונים טכנולוגי, מזה שנים רבות.

ציון סמולר:

אז אני חייב לתקן פה, כי אין לנו לא איתמר, ולא עשיתי את זה במקביל, אני ראיתי שזה צוין בדו"ח, היה, ב – 2023 עשיתי פה סקר עם חברת BDO, חברה מובילה היא חברה מאוד מקצועית שהיא סקרה, יש לה, יש דו"ח אני יכול להעביר לך אותו, אתה יכול לראות, סקר סיכונים כמו שצריך לפי ניסט, אז הכול שמה.

שלומי בני:

אבל איך זה שאיתמר ומיכה הם לא מעודכנים בכזה, סקר? זאת אומרת מנהל האגף המחשוב ומנהל אבטחת מידע.

ציון סמולר:

אני לא יודע מה היה פה במענה, נראה לי שראיתי דווקא שהם כן התייחסו.

אלדד רבינוביץ:

כתוב משהו מוזר - זה סקר שיפור תהליכים עסקיים, כתבו שיש, זה אותו דבר? זה קשור זה משהו?

שלומי בני:

לא,

ציון סמולר:

אם זה שיפור תהליכים עסקיים, זה נכון.

אלדד רבינוביץ:

בעמוד 36 כאילו זה, אני לא קשור ל - , זה התשובה ל - ,

שלומי בני:

זה התשובה אל (לא ברור)?

אלדד רבינוביץ:

זה הייתה התשובה להמלצה הזו, ולא הבנתי מה הקשר.

שלומי בני:

כן, תראה, אני מצפה שאם יש, ויכול להיות אגב שיש, והוא באמת היה אצלך, והוא שואל אותך בתור CEO אם הבנתי נכון, זה מה שהיית, נכון?

ציון סמולר:

קיים, אני רואה פה את ההמלצות, ההמלצות מאוד מקובלות לחלוטין. אני רק אומר שקיים, כתבתי לבצע, (לא ברור).

שלומי בני:

אז רק הערה, אני חושב שסקר כזה, בוודאי, בסיס או מנהל אבטחת המידע וסייבר צריך להיות מעודכן, לראות אותו וכולה, ובטח ובטח גם מנהל האגף המחשוב, זאת אומרת שתי הכובעים האלה שהיינו מולם, אין להם מושג, אז זה כאילו ממצא אחר, זאת אומרת אם הייתי צריך לעשות את אומרת המוצע קיים, אבל זה לא הגיע לידיעת העם,

ציון סמולר:

קיים.

שלומי בני:

קיים.

ציון סמולר:

שתיים, אחרי סקר כזה צריכים להבין כל דבר יש לו משמעות בסוף,

שלומי בני:

אגב, למה הוא בוצע ב – 23? כי אנחנו התחלנו את העבודה ב – 23, יכול להיות, אתה יודע שאנחנו התחלנו באמת לא היה,

ציון סמולר:

בסביבות אוגוסט,

שלומי בני:

צריך לראות, יכול להיות שאני חושב שבאזור הזה התחלנו, אני לא יודע בדיוק את התאריך, אבל, כן, נכון?

דוברת לא מזוהה:

כן,

שלומי בני:

אז יכול להיות כשאנחנו עשינו,

דוברת לא מזוהה:

במאי.

שלומי בני:

מאי התחלנו?

ציון סמולר:

הם סיימו את זה לקראת סוף שנה.

שלומי בני:

אז יכול להיות שלא,

ציון סמולר:

הבנתי,

שלומי בני:

אז יכול להיות שלא היה,

ציון סמולר:

אז כאילו, שאיתמר ידע מזה בוודאות,

שלומי בני:

אוקי,

ציון סמולר:

והם תחקרו גם את מיכה, הם כאילו,

שלומי בני:

אוקי, אז במאי – יוני לא היה,

ציון סמולר:

זה היה בתפר ה - ,

שלומי בני:

כנראה שזה היה בתפר,

עפרה ברכה:

(לא ברור).

שלומי בני:

מצוין.

ציון סמולר:

להיות בקשר,

שלומי בני:

אוקי, יופי. בסדר, אז קודם כל בוצע, זה מה שחשוב.

ציון סמולר:

כן, בוצע, אבל כמובן שאחד ל – 18.50 זה המלצה, אני חושב של החוק,

שלומי בני:

נכון, נכון,

ציון סמולר:

אני חושב שפה החוק מדבר. הנה כתוב, תראה בתגובת המבקר של מנהל מחשוב - בימים אלה מתבצע סקר של חברת BDO,

שלומי בני:

נכון,

ציון סמולר:

באמת רק התחיל, אבל לא הסתיים.

שלומי בני:

ולא, לא הסתיים,

ציון סמולר:

אז בסדר, אז מופיע פה ב - ,

שלומי בני:

אז פה יש בעצם שני ממצאים, מאוד, מאוד חשובים, אחד, מערכת הגבייה, אני לא צריך לספר פה על הנוכחים, מערכת ליבה משמעותית שמנהלת הליכי גבייה של מיליארדי שקלים, אחת המערכות החשובות של העירייה, היא בעצם עלתה, עלתה לאוויר, אוקי, עושים בדרך כלל בדיקות מסוימות, ואז מחליטים אם לעלות לאוויר או לא, מה שפה קרה, העלו את ה - , לאוויר, למרות שנמצאו לא מעט ממצאים בדגה גבוה, זה אפילו סיכון קריטי, ממש סיכון מאוד מאוד גבוה, העלו אותם בכל זאת לסיכון אבטחת מידע, מאוד מאוד, מאוד מאוד חשוב, שזה ממצא שצריך לקחת אותו לתשומת לב במערכות הבאות, כמובן, והדבר הנוסף זה שאנחנו בדרך כלל רגילים לראות איזה שהוא סייקלים של מבחני חדירה למערכות, אז אם נניח יש 200 מערכות ניקח את החלק הנמוך, אז אני אגיד אני עושה כל שנה, 50 מבחני חדירה, אז כולם ראשנים, אני עובר, אני עובר את אותה מערכת, שזה סביר. אז אנחנו מהבדיקה שלנו בוצעו פה, לא נעים לי להגיד, על כף יד אחת, במהלך, במהלך שנתיים, אולי איזה 4, או 5, מבחני חדירה, כאילו זה היה,

ציון סמולר:

נכון, לגמרי, אז אני רק אעדכן מה נעשה לפחות בנקודות האלה.

שלומי בני:

מצוין.

ציון סמולר:

אחד, עשיתי ישיבה עם מנהלת הפיתוח כרגע שנמצאת, כפופה, תמר מי שמכיר, תמר שמעון, כפופה למנמ"רית החדשה, שהיא תגיע, העברתי לה במייל גם סוג של הנחייה, כל מערכת שעולה, כל מערכת חדשה, שעולה לאוויר, היא תהיה מחויב בלית און, היא לא תעלה לפני מבדק חדירה, שיהיה גם בתיאום ציפיות, לפני שמעלים סוג של מערכת לגבי הלו"ז, והדברים, דבר ראשון, מבדק חדירה. יש לנו גם אופציה של מערכת ברייד, שהיא בעצם עושה את הבדיקה הזאת היא מעודכנת, אבל יש גם, אמרתי לה שיהיה גם מבדק חדירה לכל מערכת, שהיא מפתחת. במקביל לזה, אני אשמח שחברת משכ"ל - משק וכלכלה, לקחו ועיבדו תחתם סוג של חוזה והסכם, שהוא מסייע לרשויות מקומיות, אני לוקח את כל הנקודה הזאת, ובעצם שמה יש לנו אופציה לבוא ולהתקשר ולבצע מבדקי חדירה, ולעשות הרבה דברים עם מימון של, החלקה של השלטון המקומי, זה ככה זה נקרא זה,

עפרה ברכה:

מרכז לשלטון המקומי.

ציון סמולר:

המרכז לשלטון המקומי, מממנים עלות מאוד מאוד גבוה, בתחום הזה, גם לכתיבה של נהלים חדשים, זה לגבש לרשויות שהן חלשות,

שלומי בני:

כן,

ציון סמולר:

ואין להם בדרך כלל את התקציבים (לא ברור), התלבשנו על הנקודה הזאת, אני אגיד לך אנחנו גם התחברנו לסוף שלהם, חלקם מקבלים את זה במימון מאוד מאוד משמעותי. ומבדקי חדירה גם לקחנו עכשיו, זה נמצא בתהליך, לעבוד איתם לקבל את הסבסוד הזה ליהנות, אבל מה, צריכים עזרה בתקציב, הכנסנו את זה לתקציב התב"ר מה שככה לא הסתדר. אז גם לזה יש לנו כבר מענה, אני פשוט כל כך,

אלדד רבינוביץ:

תחזור אליהם דודו.

ציון סמולר:

אני כבר, אני פשוט נמצא פה, אני בוא נקדם על המוקדים, והסטודנטים, אני התחלתי פה בתור סטודנט בעירייה, הייתי פה סטודנט. ואני מכיר פשוט את כל ה - , איך זה, אבל,

עפרה ברכה:

טוב.

שלומי בני:

אוקי, טוב, נושא של, אנחנו, אני אקריא את זה, ואחרי זה אולי אני אסביר, קיים ניגוד עניינים מובהק,

עפרה ברכה:

אני רק אומר כאן משהו, אני לא זוכרת אם זה בהמשך, אבל היו כמה מבדקי חדירה שעשינו,

שלומי בני:

נכון,

עפרה ברכה:

יש בהמשך,

שלומי בני:

בהמשך. קיים ניגוד עניינים מובהק של חברת נס ספק המחשוב העיקרי של העירייה, שירותים אשר נועדו לבחון, את רמת אבטחת המידע של מערכות שפותחו ע"י חברת נס, לדוגמא מבדקי חדירה למערכת, אוקי, שירות ש - , חלק מתן שירותי אבטחת מידע של חברת נס לעירייה באופן כללי נעשים ע"י ספק שהומלץ ע"י חברת נס, ובכלל התשלום אליו מתבצע דרך חברת נס, חברת נס בעצם מספקת את 90, לא יודע, 8% מכוח האדם,

ציון סמולר:

הם מערך IT,

שלומי בני:

הם מערך ה - IT, כן,

עפרה ברכה:

כן,

שלומי בני:

אבל זכו במכרז כשר והדין, וזה מצוין. הם מפתחים גם כן מערכות לעירייה, כי זה בעצם אגף, אגף המחשוב, ולמעשה כשצריך לבדוק את אחת המערכות שהם פיתחו או שלא פיתחו, זה לא משנה, הם צריכים לבדוק כל מיני מערכות שהם מתחזקים,

אלדד רבינוביץ:

אז הם יושבים (לא ברור).

שלומי בני:

הם מביאים, ממליצים, בסדר? זה אמרו לי - לא, הם לא מביאים, הם ממליצים, בסדר,

אלדד רבינוביץ:

משולם להם, והם משלמים, לא, זה,

שלומי בני:

הם גם משלמים לו את הכסף, כן, זאת אומרת זה, זה עוד יותר חמור. זאת אומרת אם הם רק היו ממליצים טוב, זה ממצא חשוב. אבל אם הם ממליצים, וגם משלמים לו, אז בוודאי שאני אהיה תלוי במי ש - , המליץ עלי, וגם שילם לי, אז זה אני חושב נושא מאוד מאוד חשוב. צריך לקחת ספקים אובייקטיביים,

ציון סמולר:

בוא קיבל כבר מענה בתשובה הקודמת שאמרתי, אם זה דרך המשכ"ל,

שלומי בני:

נכון,

ציון סמולר:

ביצוע של חדירה, אנחנו נוכל, ממילא להתנתק בערכות האלה, אבל צריך להבין אנחנו גם רוכשים ציוד מחשובי דרך חברת נס, זאת אומרת גם שהם מפעילים עבורנו, כמובן שאני אומר הם לא צריכים להמליך לנו לספקים כאלה ואחרים, אבל אם הם, אסור שהתשלום יתבצע ע"י אגף המחשוב, דרך אגב שהוא מוציא הזמנה, על כל מבדק או דבר כזה, הוא יכול לבחור חברה ולבצע אותה, באמצעות, הוא זה שמפקח, הוא זה שעושה, זה רק הצינור כביכול התשלום שמופיע דרך

במסמכי המכרז של חברת נס. כדי לייצר פה תהליכים הרבה יותר מהירים, כי אם, אם נצטרך לעשות התקשרות לכל אחד כזה, זה מציעים, אתה לא תגמור.

שלומי בני:

אז תיקח ספק אחר, שהוא לא נס. יש לך עוד ספקים, קח, קח אחד אחר שהוא לא,

אלדד רבינוביץ:

למה לא לעבוד,

ציון סמולר:

זהו, אני שאלתי גם את השאלה, כי אני רציתי להבין הבהרות, כל החברות שמבצעות את המבדקי חדירה, זה לא חברת נס עצמה,

שלומי בני:

כן, כן, אני יודע,

ציון סמולר:

כן? בסדר?

עפרה ברכה:

מישהו שידוע,

אלדד רבינוביץ:

בוועדת מכרזים מקבלים המלצה מיועץ, על כמה אנשים, כמה חברות שהן רלוונטיות, ואפשר לעבוד איתם, זאת אומרת,

שלומי בני:

אאבל השאלה, בגלל שנס עובדים בכל העולם, גם החברה הזאת לא במקרה נס המליצה לעבוד באופן נקודתי,

ציון סמולר:

אני עובד איתם.

שלומי בני:

יש 300 ספקים כאלה,

ציון סמולר:

באופן (לא ברור).

שלומי בני:

אז אני אפתור לך גם את הבעיה הזאת, אז אל תחתים אותו על ניגוד עניינים, שאין לו ניגוד עניינים, הוא חברת נס,

ציון סמולר:

בסדר,

שלומי בני:

ואם יש לו ניגוד עניינים, שלא, לי יש לפעמים ניגודי עניינים, אני אומר חבר'ה,

אלדד רבינוביץ:

מצוין.

ציון סמולר:

בדיוק,

שלומי בני:

לא יכולה לעבוד איתה, ניגוד עניינים, זה חלק מתנאי ההעסקה,

ציון סמולר:

לכתוב את זה, את המסמך הזה, של ניגוד עניינים,

שלומי בני:

כן,

ציון סמולר:

מקובל לחלוטין.

שלומי בני:

שיכתבו. אני גם חתמתי על ניגוד עניינים,

ציון סמולר:

חד-משמעית,

שלומי בני :

שאני לא עובד עם עיריית ירושלים, בנושאים האחרים, רק בביקורת, אתה תרצה להעסיק אותי, אני אגיד לך - לא.

ציון סמולר :

תהיה הנחה בכמה שקלים?

שלומי בני :

אני אעשה לך.

ציון סמולר :

כן.

שלומי בני :

בעצם פה אנחנו, יש הנחייה של חמשת חברות כרטיסי האשראי, שבאות, התקינו תקנות שנקראות PCI DSS, שבעצם הם, המטרה שלהם בעצם ש - , מה שנקרא לכסות את עצמן, הם אומרים - רגע, אם אתה משתמש בכרטיס שלנו, ואנחנו נותנים גם ביטוח על זה, שאם גנבו אותו, וכולם רוצים שתהיה, שיהיה לך איזה שהוא הגנות מסוימות. אז זה לא משנה אגב, אם אתה סולק בעצמך, או לא סולק בעצמך, גם נתנו קישור כדי שתוכלו לראות, שמספיק שאתה מכבד את הכרטיסי אשראי, אתה אמור להיות בתוך, בתוך התקנות. עכשיו נכון, אם יש לך גוף אחר שסולק לך, אז אין בעיה, אז רוב הבקורות צריכות להיות אצלו, אבל אתה צריך לפקח עליו. לא יכול להיות שאתה אומר - לא, לא, אני לא סולק, ההוא סולק, לך אל ההוא, זה ברור שזה לא הגיוני,

ציון סמולר :

אז אני רק אגיד את התשובה שקיבלנו פה ממיכה, שהם כן עומדים בכל התקנים האלה, החברה מעבירה לו מידי שנה, את התקנים, מבדקי חדירה וכל דבר שהם עושים, נבדק ע"י יועץ, שלכם, חברת ייעוץ לבדוק את הנושא הזה. יש להם את כל התקנים עומדים בכל הדרישות, חברה ש - , אז זאת הסליקה שלה,

אלדד רבינוביץ :

גם לנו?

ציון סמולר :

כן, אנחנו כאילו הכול, לא משלמים פה בעירייה, אין לנו, אתה לא משלם פה.

אלדד רבינוביץ :

בעצם ההפניה מתוך האתר שלנו לחברה ההיא,

ציון סמולר:

בדיוק.

שלומי בני:

אז הם עשו את זה כנראה בעקבות הדו"ח שלנו, כן בתחילת הדרך אמרו לי - תשמע, אנחנו לא, אנחנו לא צריכים את זה, ואז אמרו לי, אתה יודע, ואז אמרו טוב, יכול להיות א', תקבלו ייעוץ משפטי, כן, כי בכל זאת זה עדיין, אם אתם, אם החוק חלופות עליכם או לא, אז יש ייעוץ משפטי, שהוא ייתן לכם את החוות דעת,

ציון סמולר:

תודה, תודה לך.

שלומי בני:

ושתים, אין בעיה, גם אם כן, זה לא, אם אתם לא סולקים, לפחות תעשו פיקוח. טוב, אז יש משתמשים רגילים במערכות המחשוב, שלומי בני, אוקי, יעקב כהן, ויש משתמשים שמשתמשים בין ה - , בין המחשבים עצמם, שמחשב רוצה לדבר עם מחשב אחר, אז יש לו משתמש, איך הוא מדבר? משתמש מסוים, זה נקרא משתמש אפליקטיבי כן, אז מה שאנחנו בדקנו בעצם שהסיסמאות האלה הם לא, הם לא, בעצם המשתמשים האלה לא החליפו סיסמאות הרבה מאוד שנים, מעל 3 שנים, זה אפילו הרבה יותר, יש כאלה 6 ו 7, אבל אנחנו אוהבים להיות שמרנים, יש לנו למעלה מ - 3 שנים, בעצם צריכים להחליף סיסמה, גם משתמשים אפליקטיביים. ייאמר, נקודה עכשיו צריך לזכור, זה לא פשוט, כי הרבה פעמים,

ציון סמולר:

גורם לשיבושים,

שלומי בני:

זה גורם לשיבושים, אוקי, אז אנחנו יודעים שהתחילו פרויקט כזה בעירייה, ושינו לא מעט משתמשים, זאת אומרת ייאמר לזכותם שהם יודעים את זה, ידעו את זה, עלו לזה, אבל עדיין לא סיימנו.

ציון סמולר:

אני רק אסביר זה סוג של סרוויסים שאתה מקבל מכל מיני מערכות, וכשהיא ניגשת למערכת, המערכת מבקשת סיסמה, את הדברים האלה צריכים להחליף, בוצע לופ אחד, וזה חלק מתוכנית העבודה של חבר נס, לבצע שחלוף כל הזמן צריכים להחליף את הסיסמאות האלה, אני מציע, ויש

פה עוד אופציה שאנחנו עכשיו מנסים לחבר, זה SDO, מי שמכיר את זה פה, אנחנו התחלנו להפיץ פה למעלה מ- 1000 משתמשים. נקודה של פתיחת, באמצעות הטלפון, מי שמכיר את זה, מי שיש לו פה?

שלומי בני:

כן,

אלדד רבינוביץ:

של BRT,

ציון סמולר:

אוטובוס יופי מצוין.

שלומי בני:

כן,

ציון סמולר:

אני כבר שמח, זה צריך להיות לכל ארגון, זה דברים משמעותיים,

אלדד רבינוביץ:

זה יותר טוב סיסמה?

ציון סמולר:

אני מסביר לכם זה דברים שהם כל כך תופסים אותנו בימים, ביום הראשון שלי בתפקיד. מה שאחרי המכרז, הכניס אותי לפורום של מנהלי אגפים, פתאום היה שם בלגאן בוואטסאפים של כולם, כי השתלטו על,

עפרה ברכה:

נכון, הייתה השתלטות,

ציון סמולר:

לכל מנהלי האגפים, ראשי מנהלים, מרימים אלי טלפון, מוקד שירות, שלום מה אפשר לעזור? אתה עכשיו בסייבר, תעזור לנו בוואטסאפ איך זה קורה? איך זה קורה, הדבר הזה? אז אחד, הקטע של הסיסמאות, זה גם באירועים קודמים פה בארגון שלנו זה, 43 משמעותי, כמו שאמרתי בתחילת דרכי, הקטע של התוקף הוא מודיע לך, החוליה הכי חלשה שיש, וכנראה שזה המשתמשים בעצם זה החוליה הכי חלשה, שקיימת פה, מול רובוט מאוד קשה להתמודד, יש לנו הרבה הצפנות, יש לנו

הרבה מערכות שתוקצבנו בעבר בתחום הזה של הסייבר. אבל המשתמש עצמו, אם הסיסמה שלו זה A ו- 123 123 a הוא לא יכול היום, נגיד בכובע הקודם שלי, שהייתי מסתובב בכל מיני חדרי ישיבות, הייתי רואה מדבקות, זה הסיסמה של הכניסה לזה, זה תמיד אני תוהה גם ממשלה לא ראיתי, הבנתי את המשמעות של הדבר הזה. אז אנחנו עוברים לטכנולוגיה הרבה הרבה יותר מתקדמת, אז אני שמח להגיד, שגם אגף התקציבים תקצב אותנו, אנחנו מתקצבים כ- 3000 יוזרים, אנחנו נצטרך לכולם,

שלומי בני:

תוסיפו קצת,

ציון סמולר:

מה?

עפרה ברכה:

זה ממש משדרג,

ציון סמולר:

הסנסורים,

אלדד רבינוביץ:

כל פרגון זה עוד צ'ק ליסט,

ציון סמולר:

או אפס,

דודו אמזלג:

כמעט זה ייגמר.

ציון סמולר:

עוד אפס, אני מאוד אהבתי, כן, אני מאוד אהבתי את ה- , את ה- 0.8, אני דרך אגב גם בקורס שאני נמצא עם עוד משרדי ממשלה, זה בעצם התקצוב שמקבלים, זה משהו שהוא באמת קורה.

שלומי בני:

רק צריך, הערה קטנה, לפעמים מערבבים בין ה- , בין התשתיות, זה אולי אני אגיד לדודו, גם כן וגם לך, לפעמים מערבבים האם זה, האם מערכת אבטחת מידע היא נכנסת בתוך התקציב הזה, או לא? אז אצלכם זה נכנס בתוך אגף, בתוך אגף המחשוב,

ציון סמולר:

כן, אבל לא מספיקה.

שלומי בני:

נכון, נכון, בסדר, הרי יש, חשוב שגם דודו ידע, אז שלא תצפה עכשיו, אתה לא צריך לתת לו 0.8 מעבר למה שיש לו בכל האגף, בסדר? הוא צריך לעשות את זה.

ציון סמולר:

אני קונה את זה,

שלומי בני:

בסדר?

ציון סמולר:

כן, איפה חתמו.

שלומי בני:

תרצה סיוע,

ציון סמולר:

אז אני חייב להגיד יכול להיות שזה גם מדבר על זה עבדתי, תלחץ על השקף, זה גם היה עניין של משתמשים, לא יודע, אני פשוט קפצתי פה לממצא,

שלומי בני:

אצלי זה לא מבוצעים שחזורים יזומים.

ציון סמולר:

אז אני רק רוצה להשלים, להשלים פה את הנקודה, שאנחנו באמת עברנו ל – SDO, ואנחנו גם הקשחנו את הסיסמאות, זאת אומרת אנשים ירצו לעבור לאוקטופוס, כי יהיה להם הרבה יותר קל, אני מאוד נהנה מזה, מאוד מאוד נהנה ברמה אישית, וכשהקשחנו את הסיסמאות, לפחות ל – 8 תווים, לשאלות ומספרים (לא ברור) קטנה.

עפרה ברכה:

סיסמא בעירייה זה, פה זה חתיכת,

ציון סמולר:

עכשיו מה קורה,

אלדד רבינוביץ:

חוויית לקוח.

ציון סמולר:

יש משהו מאחורי הקלעים שקורה,

עפרה ברכה:

הם גם (לא ברור) את כל מה שהיה,

ציון סמולר:

אני לא יודע כמה אתם מכירים, תמיד כשחוזרים מחופשה, במיוחד גם באוגוסט, כולם שוכחים את הסיסמאות שלהם, ואז המוקד פה מוצף עד לב השמיים, וכל הזמן זה חוזר הפיקים האלה. אז זה גם לתת את המענה לזה, בעצם.

עפרה ברכה:

טוב.

שלומי בני:

טוב, נושא הגיבוים הוא נושא מאוד חשוב, כי בסופו של דבר כשיש לנו חלילה תקיפה של כופר, וכולה, אבל לא רק בתחום אבטחת מידע, גם בתחום של הפעילות השוטפת, יימחק לנו משהו, מערכת שלא עובדת וכולה. כמובן שיש פה גיבוים, ויש פה מערך גיבוים מאוד מאוד משמעותי ואיכותי, אין דיון על זה, מה שכן אנחנו מצאנו שלא מבוצעים שחזורים יזומים, אין, אין איזה שהוא תוכנית, שאומרים - יופי, בחודש הבא, משחזרים את מערכת הגבייה, מאפס, מעלים אותה,

אלדד רבינוביץ:

מה זה שחזור? סליחה,

שלומי בני:

שחזור לקחת את הגיבוים, ולראות שהם עובדים. כן, כמו שאתה יודע, הוואטסאפ שלנו נמחק, רוצים לשחזר אותו.

ציון סמולר:

אתה יכול רק למקד אותי סליחה ב - ,

שלומי בני:

איפה זה נמצא אצלך? אני עם המצגת,

ציון סמולר:

סוג נמצא?

שלומי בני:

גיבויים ושחזורים, גיבויים ושחזורים, אני מניח שזה, שזה איפה שהוא באמצע הדו"ח.

ציון סמולר:

אני יודע לענות, הנה.

עפרה ברכה:

מצאת?

ציון סמולר:

כן, מצאתי, 18. טוב.

שלומי בני:

(לא ברור).

ציון סמולר:

כן, אני אענה, ברמת העיקרון זה הדבר הראשון שנגעתי בו, כשאני נכנסתי לתפקיד, כבר משבוע שעבר, עשינו נוהל, כתבנו נוהל שחזורים חדש, השחזורים מבוצעים, אני חייב להגיד לכם יש לנו מערכת מאוד מאוד טובה מהטובות בעולם, מערכת קונוולט שהיא באמת מובילה. יש לנו, יש לנו כמעט כל 4 שעות, פועל,

שלומי בני:

שחזור,

עפרה ברכה:

אמרתי את זה לנושא השחזור.

ציון סמולר:

מה זה?

עפרה ברכה:

זה נעשה באופן,

ציון סמולר:

אוטומט, באופן אוטומטי יומי, שבועי, שנתי. רק מה שאני בדקתי היום, אני שם את זה בסוגריים, כי מה שבדקתי, עדיין אין עד הסוף, שזה משוחזר ל – 3 שנים, אני ביקשתי להעלות את זה ל – 7 שנים,

עפרה ברכה:

אחורה כאילו?

ציון סמולר:

אחורה 7 שנים שיהיה, ובנוסף לזה, בכובע הקודם שלי בתפקיד, לקחנו 100 אנשים פה בארגון, ואת התיבות שלנו, הרי כולנו נמצאים פה בסביבת 365, עובדים שהם בענן, ובשביל לעשות גיבוי לאותו, אותו טכנולוגיה, יש טכנולוגיה אחרת שנקראת מטאלית, היא עולה הרבה מאוד כסף, אני אומר את זה אנחנו עשינו סוג של תעדוף לקחנו את ה – 100, את הראש העיר, חברי המועצה, מנהלי אגפים,

עפרה ברכה:

משהו שתוקצב במיוחד בעקבות דו"ח אחר שעשינו, אני חושבת,

ציון סמולר:

זה לא, הקטע הזה של העל, לא,

עפרה ברכה:

שאומר,

ציון סמולר:

אני אשמח לראות את זה,

עפרה ברכה:

כן.

ציון סמולר:

מתוקצב שם ל – 100 משתמשים, שיש לנו גיבוי בעצם ל – , לתיבות מיילים שלהם, חוץ מה – 100 אנחנו לא מגובים, בתיבות המייל, זה צריך לשים את הדגש. לגבי מה שקיים פה בארגון, יש לנו

מערכת טובה, שצריך עכשיו לבצע איתה גם סוג של התקשרות חדשה, מחודשת, כאילו להאריך איתם את התוקף, אבל השחזורים קורים, אז אני חייב להגיד,

אלדד רבינוביץ:

יש חדר שרת?

ציון סמולר:

אפשר להציג אותו,

אלדד רבינוביץ:

ראיתי שיש חדר שרתים לגיבוי.

ציון סמולר:

זה לא הולך ככה.

שלומי בני:

DR.

ציון סמולר:

DR אבל זה לא בדיוק הגיבוי, אם אתם רוצים אני אסביר קצת על ה - ,

עפרה ברכה:

כן, תסביר.

ציון סמולר:

בשמחה. אני אספר את הסיפור.

עפרה ברכה:

דודו,

ציון סמולר:

אני אספר את הסיפור, וטוב שאני מכיר כאילו קצת את ההיסטוריה בנקודות, היה פה חדר,

דודו אמזלג:

עולה כסף בסוף?

עפרה ברכה:

חכה, חכה לסוף.

ציון סמולר:

זה סכומים אחרים מה שאנחנו מכירים, זה סכומים אחרים מה שאנחנו מכירים, אבל. חדר מחשב בעיריית ירושלים, לפני בערך 7, 8 שנים, ניסה לעשות לעצמו ביטוח, אמר, בוא נעשה ביטוח, חשוב מאוד חדר מחשב, יושב פה לבד, דרך אגב מי שרוצה, אני יכול לעשות לו סיבוב, סיור שמה. באה חברת ביטוח, אמרו לה, היא לא מוכנה לעשות כזה דבר, לא עושה ביטוח, היא לא מסוגלת, כי היא לוקחת את הסיכון בכלל הנקודה הזאת, גם (לא ברור) עד דעתנו, לבוא ולקחת את המחשב שלנו ולהעביר אותו, העברנו אותו להר חוצבים, עם חדר שהוא טיר 3, הוא ניזון משני מקורות חשמל, נגד רעידת אדמה, התקפת טילים וכולה, וכולה, מקבלים הוסטינג מחברת בינת. באותה תקופה עשינו שיפוץ שמסתיים בימים אלה, שיפוץ שמתחת לפני השטח, ואף אחד לא מכיר את הפרויקט הזה, פרויקט ענק,

שלומי בני:

איפה? פה?

ציון סמולר:

פה ממש, בקומה ממש נמצאת בזה של נס, גם לא נשרף בשריפה שהייתה פה, היה הרבה ניסים שקרו, הקדוש ברוך הוא שומר עלינו מאוד חזק. ואנחנו כבר בשלבים האחרונים של השיפוץ שלו. שתדעו שפה המרכז תקשורת העירוני נמצא בחדר הזה, עם גיבוי של Commvault מכונה אחת נמצאת פה, מכונה אחת נמצאת בהר חוצבים. במקביל זה, לפני כ – 3 שנים לתקצוב של אגף התקציבים, הקמנו ובעזרה מאוד מאוד, אני חייב לציין את זה, משמעותית מאוד של, כפרה איך שהיא נכנסה, זה פשוט היה אחד מהמשימות, היא ראתה את זה. הקמנו אתר DR בהרצליה, שהוא עבר, שנה אחרונה לנתניה, השנה עבר לנתניה. אבל יש לנו אתר DR שבעצם שמה, יש לנו גיבוי ש – זה לא גיבוי של הדאטה וכל הדברים, בכל המערכות מידע שלנו מגובות שם, ובמידת הצורך, חס וחלילה אם יהיה פה איזה סוג של אסון, נוכל להפעיל 100 משתמשים שיוכלו לעבור עם לפטופים, להשתלט על המערכות ולתפעל את הארגון מרחוק, איפה שזה לא יהיה, וזה אירוע קיצוני.

עפרה ברכה:

אז זה הבנתי מצוות המשנה, שאולי הגדירו מי ה – 100 משתתפים או משהו בדומה, אבל זה לא הסתיים, לא עשו באמת את הניסוי הזה, שבאמת יעבדו 100 משתתפים באותה עת או משהו דומה לזה,

ציון סמולר:

נכון,

עפרה ברכה:

עוד לא סיימנו את הסיפור הזה,

ציון סמולר:

לא סיימנו, וחלק מהדברים שאני ביקשתי גם בתקציב, אני אומר לך דודו, זה כבר זה, זה לעשות סימולציה, סימולציה להנהלת העירייה.

עפרה ברכה:

בדיוק.

ציון סמולר:

כי מה קורה, אני באימונים שעשיתי בשנה האחרונה,

עפרה ברכה:

מה שיש בנתניה זהה למה שיש, פה בהר חוצבים?

ציון סמולר:

מה שיש בנתניה זה זהה למה שבגדול, בקטן.

עפרה ברכה:

אוקי,

ציון סמולר:

המשאבים שם,

עפרה ברכה:

אני מבינה,

ציון סמולר:

בקטן, בקטנה כדי שלא נשלם הרבה כסף, אלא שיהיו לנו את הדברים מינימאלי, בשביל לטייב.

עפרה ברכה:

אוקי,

ציון סמולר:

ואם נצטרך להגדיל את זה בבוא העת, זה (לא ברור), חס וחלילה היה קורה פה משהו אז, הכול היה הולך פשוט,

שלומי בני:

ולהגדיל את זה מ – 100 ל – 1000, תוך כמה זמן אתה מודד את זה?

ציון סמולר:

מ – 100 ל – 1000? אני לא יודע להגיד לך,

עפרה ברכה:

משתמשים,

ציון סמולר:

זה לקנות ציוד, זה לקנות ציוד, זה קונפיגורציות, זה סיפור,

שלומי בני:

אוקי,

ציון סמולר:

אבל במידה של אסון, תהליכים הרבה הרבה יותר זריזים, המשאבים גם במקום, אני מניח וכולה. אני חייב לציין גם שאנחנו לאט לאט בפיתוח, עוברים לאולמות הרבה יותר טובים, לאולמות ענן, אני תמיד דוגל בשיטה של שירותים, ולא שרתים. האולמות האלה של ברזלים כבר פסו מהעולם. אנחנו משתדלים להעביר את הכול לשם, ושמה הכול נמצא בגיבוי, יש מכרז ענק של המדינה שנכנס אליו, מכרז נימבוס, מי ששמע את השם, מכרז עצום, שבעצם לוקח את הצבא, ואת כל הזה, הצלחנו להיכנס, דרך אגב בנקודה הזאת בתפקיד הקודם שלה, אנחנו כבר נמצאים עם אמזון שם בנקודה, אנחנו נמצאים באז'ור שזה של מייקרוסופט, שהם לא זוכים בנימבוס, אבל כרגע אנחנו נמצאים שם, אבל המחירים שם של העלויות, הם מאוד מאוד,

דודו אמזלג:

אטרקטיביים.

ציון סמולר:

ממש 37% הנחה ו - , בסיס, ולהם, הם הקימו את כל ה - ריג'ן, ריג'ן זה אזור שהוא מגובה, בשלושה אתרים בארגון, בארץ שלנו, נמצא פה בגלל המידע החסוי וכולה. אז זה נמצא פה, שתדעו שזה כאן בכיוון של אגף המחשוב, המנמ"רית החדשה, אני גם אמליץ בפניה להמשיך את התנופה, הנקודה

לשם, שם מחייבים אתכם, מחייב אותנו בנקודה שימור, עדכונים, הזמן, עדכוני אבטחת מידע כך
מה שנדרש, סטנדרט הכי גבוה שקיים.

עפרה ברכה:

אז איך אתם מסיימים רק את הסיפור הזה של המאה, מאה יוזרים?

ציון סמולר:

מה שנצטרך לעשות בעצם, לעשות, רגע ויינתן תקציב בעזרת השם אנחנו נעשה פה סימולציה, זה
נמצא במשכ"ל נמצא עלות של את זה במשכ"ל. אני רציתי להגיד את זה, שעשו לי את הסימולציה
הזאת בלימודים, שלמדתי בבר אילן, וזה הרגשה הכי טובה, כי אתה פתאום אתה קולט ש - , מה
אתה עושה, מה אתה עושה שאין לך את זה, וזה סימולציה, זה משהו שמאוד מאוד מעניין, וכל אחד
יצטרך,

עפרה ברכה:

אנחנו צריכים לעשות סימולציה,

ציון סמולר:

משאבי אנוש,

עפרה ברכה:

יוזרים באותה עת? זה לא,

ציון סמולר:

לא, אז אמרתי שתרחיש, של תרחיש, ואז צריך לראות מה קורה. לעשות את הזה בו – זמני אנחנו
יכולים לראות, הרי יוזר את מגדירה 100 יוזרים, ופשוט נכנסים למחשב ובודקים, אנחנו יכולים
לעשות גם בבדיקה אצלנו, (לא ברור) גם חלק מזה, אין ברירה.

עפרה ברכה:

זה חלק מהדו"ח שלנו, שעשינו בנושא המשכיות תפקודית ב - , בהתאוששות מאסון משהו כזה, זה
היה תחת.

ציון סמולר:

כן.

עפרה ברכה:

טוב.

שלומי בני :

אוקי,

עפרה ברכה :

מעניין.

שלומי בני :

זה דווקא ממצא שדודו יאהב, כי זה ממצא בעצם ש - ,

עפרה ברכה :

מכניס כסף.

שלומי בני :

לפחות לא מוציא כסף.

דודו אמזלג :

היא חשדה.

שלומי בני :

זה בעצם יש כל מיני הקשחות, במערכות האלה, במערכות אבטחת המידע שצריך להקשיח אותם, לסגור כל מיני פורטים, לסגור כל מיני דברים, זה לא עולה כסף, זה לפעמים ביום יומיים, שלושה עבודה, אתה סוגר הרבה מאוד פרצות, זה בעצם הממצא. הוא מדבר פה על, על אקטיב דירקטורי, בעצם מערכת מרכזית שמנהלת את המשתמשים של העירייה, הוא בעצם מדבר על מערכת חומת האש. האנטי וירוס היה טוב אגב, זה, הוא היה, מוגדר נכון, הקשחות שבו היו טובות, אז זה בעצם ממצא ש - , שמדבר על חומת האש, ועל האקטיב דירקטורי, מניח שטיפלתם, כי זה משהו ש - , קל מאוד לטפל.

אלדד רבינוביץ :

כן, כן, זה בוצע.

שלומי בני :

טוב, פה בעצם אנחנו, אנחנו עוברים, בעצם לחלק השני של הביקורת, שעשינו פה מבדק חדירה, שני מערכות, בעצם בחרנו מערכות שהם מערכות רגישות, אם זה מערכת נכסים שיש בה, לא מעט מידע שהוא חשוב, שהוא עולה כסף וכולה, וגם מערכת של מצבת תלמידים שיש בה מידע רגיש, אולי פחות כספי, אבל מאוד מאוד רגיש, ילדים, מה, וכולה. אז בעצם מצאנו שישה ליקויים, ליקוי

אבטחת מידע במערכת בצוות נכסים, חמישה בעלי חשיבות גבוהה, שזה הרבה יחסית, ולמצבת התלמידים ארבעה ליקויים, שניים מתוכם בעלי חשיבות גבוהה.

אלדד רבינוביץ:

כשאתה אומר ליקויים, אתה מתכוון ליכולת להיכנס ולצפות בנתונים הפנימיים שלנו, ע"י אדם לא מורשה?

שלומי בני:

אז אני אחדד, אני אחדד, כדי להגיע לשמה, אתה קודם כל צריך לחדור לרשת הארגונית של העירייה, בסדר? שיש לה לא מעט,

ציון סמולר:

הגנות.

שלומי בני:

הגנות, בסדר? אתה ה – FIRE WALL שמקודם ראינו חומת אש, אנטי וירוס וזה, אבל גם הם לא הוגדרו כל כך טוב, אז אני, אתה יודע אז אני נזהר עם המילים, זאת אומרת אני לא יכול להגיד לך ש - , הרשת פה סגורה ויש פה, אתה, אתה סגור ב – 99.999%, לא, כי גם ראינו שגם הרשת, האקטיב דירקטורי, ה – FIRE WALL, הם פחות, אז כל הזמן אתה צריך לעבוד על הרשת הארגונית, אחרי שעברת את הרשת הארגונית, אז יש סיכוי, שאתה יכול להיכנס, סיכוי סביר, או סיכוי לא קטן שאתה יכול לחדור למערכות האלה, מה אתה יכול לעשות? או לצפות נתונים, לשלוח נתונים, לשנות נתונים וכולה. זה לא שעכשיו נשים ילד בן 16, הוא ייכנס ככה חופשי למערכות. אז צריך לשים את זה גם בפרופורציה. אבל בגלל שאנחנו רואים שם האקטיב דירקטורים, וגם ה – FIRE WALL לא מוגדרים כמו שצריך, כל מערך אבטחת המידע והסייבר הוא לא ברמה גבוהה,

אלדד רבינוביץ:

אחרי זה צריך לצאת מנקודת הנחה, שאנחנו יעד לתוקפים.

שלומי בני:

בהחלט, חד-משמעית.

ציון סמולר:

רק חודש שעבר, נראה לי לסבר את האוזן, אני מקבל סוג של דוחות, 1200 ניסיונות, זה כל פעם, וזה מתגבר והולך, אנחנו סמל שלטון, אל תשכח את זה.

עפרה ברכה:

בדיוק.

שלומי בני:

נכון, נכון, עכשיו עוד דבר, זה גם התכתב מאוד, מאוד נכון עם הממצא הקודם שלנו, שלא עושים מבחני חדירה, אז ברור שיהיה פה חמישה ממצאים בעלי חשיבות גבוהה.

אלדד רבינוביץ:

זה קריטי?

שלומי בני:

כן, זה קריטי מאוד, אם היה הכול, כל, אמרנו כל 4 שנים, או כל 3 שנים, אתה מגלגל את המערכת, אני מניח שהייתי מוצא פה אחד אולי, אולי שניים, אולי, בסך הכול. אז בגלל שלא עושים, אז אתה יודע מפתחים את המערכות האלה, וכשמפתחים אותם אז, אז יש, יש יוצרים פרצות חדשות שלא היו קודם.

ציון סמולר:

אז שוב, אני אתייחס לנקודות האלה, מה שמדובר פה,

דוברת לא מזוהה:

מתי אתם מסיימים?

אלדד רבינוביץ:

עוד מעט.

ציון סמולר:

יש פה נושא של פיתוח שנכנס לתוכנית העבודה, חלק מהמערכות פה, מערכות מאוד מאוד ישנות, יכול להיות שבן אדם אחד משתמש, וצריך לבצע סוג של הסבה של נתונים למערכות חדשות שפותחו במקביל. הנקודה, זה נמצא בחלק מתוכנית העבודה, זה מה שקיבלתי לפחות,

אלדד רבינוביץ:

המערכת החשבונאית יש מערכות מאוד מאוד ישנות, ששומרים, כי לא יודעים ל – ,

ציון סמולר:

נכון,

אלדד רבינוביץ:

הם לא יודעים להעביר את הנתונים, עשו מערכת חדשה לגזברות, וגם,

דודו אמזלג:

אני אומר לך למה,

ציון סמולר:

מספיק?

אלדד רבינוביץ:

כן.

דודו אמזלג:

מאוד מורכב להעביר את המערכת הכספית, למערכת חדשה. עכשיו מה שעבר מערכת הגבייה, זה משהו, היה איתה המון המון בעיות.

ציון סמולר:

עד היום מנסים. זה פשוט לא פשוט.

דודו אמזלג:

זה אירוע אירוע, אפשר להפסיד הרבה כספים.

אלדד רבינוביץ:

(לא ברור) שנה כזאתי מן הסתם חדירה יותר, והיא יותר קשה להגן עליה.

דודו אמזלג:

אני לא יודע, אני יודע שיש בעיות אחרות, אבל הגנה,

ציון סמולר:

אבל אני יכול להגיד לך, שככל המערכת יותר ישנה ולא מעודכנת, בעדכוני האבטחה הכי מעודכנים, אתה נמצא שם בחשיפה. בסופו של יום יש גם סוג של פועל שנקרא סגמנטציה של, אנחנו הולכים ללכת עליו מאוד מאוד חזק, שגם אם נכנס משהו לרשת של העירייה, ממקום למקום, יהיה לו מאוד קשה לזוז, אז צריך ש - , כל מה שדיברנו עם הסיסמאות, וכל מה שקיים, הוא צריך, אתה צריך לעצור אותו בכל חדר, בכל שלב, אם הוא תפס נכס מסוים, לא להמשיך להתקדם. ברגע שהרשת שלך שטוחה, וכל אחד יכול להיכנס בכל דבר, זה בעיה קשה. אלה דברים שאנחנו מטפלים בהם, חלק, יש כמה דברים פה בנקודה הזאתי זה חלק מתוכנית העבודה של המנמ"רית החדשה, זה כבר נמצא שמה, ויש את זה גם מתוקצב. הייתי חלק מהפיתוח, ויבוצע בהתאם לתוכנית העבודה,

אלדד רבינוביץ:

זה ייתן לי פתרון למערכת הכספית?

ציון סמולר:

המערכת הכספית זה סוגיה בפני עצמה, שהמנמ"רית החדשה שתיכנס, צריכה לבוא ולשבת עם הצרכים, של המינהל הכספים, זה מערכת חוצה ארגון, זה ERP, מערכת מאוד מאוד משמעותית, צריך לקבל החלטות לאיזה כיוונים הולכים, אנחנו להבטיח כמה ש - ,

עפרה ברכה:

צריך לעשות גם מבדקים,

ציון סמולר:

חייבים, חייבים, תבינו הנקודה הזאת פה,

עפרה ברכה:

בגלל זה הוצאתי את הביקורת הזאת. במיוחד בגלל (לא ברור) זה חובה,

ציון סמולר:

כי בקטע של הסייבר, נראה לי שהמבקרת, זה לא הנקודה, אם זה יקרה. השאלה זה מתי זה יקרה, ואיך אתה ערוך לזה, בסדר? השאלה אם המדינה מחליטה לבוא ולהפעיל פתאום עיריית ירושלים איזה משהו, אין לנו את הכלים, אין לנו את הכלים בכלל למנוע דבר כזה, גוגל מיליארד דולר כל שנה, התקציב שלהם של אבטחת מידע וסייבר, זה התקציב שלהם, מייקרוסופט האדירה גם מאות מיליוני דולרים, זה הסכומים, וגם מהם נופלים פה, ואנחנו רואים את זה, שהשירותים נופלים. זה הכול תלוי באיזה נקודה מסוימת אתה נמצא, אתה עושה את כל המקסימום, אתה מה שאתה יכול. כן.

שלומי בני:

גם נמצאו ליקויים באתר באינטרנט של העירייה, אמנם זה אתר אינטרנט שהוא, שהוא אינפורמטיבי, אבל עדיין זה סמל שלטון,

ציון סמולר:

גם האתר שלנו כל הזמן מנסים להפיל לו, ה - DDOS, תקיפת DDOS וכולה.

אלדד רבינוביץ:

מה? מה אחוזי הצלחה בתקיפות כאלה? אתה יודע להגיד? צריך להגדיר מה זה הצלחה, אבל זאת אומרת,

ציון סמולר:

כמה מילים זה הצלחה, לא טובה. משתלטים לך בקיצור, שמישהו משתלט, אתה מרגיש את זה, היה פה אירועים בעבר, בעבר היו פה כמה אירועים, בארגון שלנו.

אלדד רבינוביץ:

אפילו כריזות,

עפרה ברכה:

וגם את זה חשבתי ישר.

ציון סמולר:

כן, כן, אבל צריך להבין עוד משהו, ולעשות את האבחנה, כי זה תקציב בפני עצמו. מה שאנחנו מדברים כרגע,

דודו אמזלג:

תוכנית הבאה.

עפרה ברכה:

בבוקר הצבע (לא ברור) יותר טוב.

ציון סמולר:

כי מה שאנחנו מדברים עכשיו כרגע, אני חייב לסדר את זה, אנחנו מדברים פה על עולמות המחשוב ה – IT העירוניות של אגף המחשוב.

עפרה ברכה:

אתה רוצה לומר שאגף חירום וביטחון זה מערכת נפרדת?

ציון סמולר:

לגמרי.

עפרה ברכה:

זה אתה רוצה להגיד,

ציון סמולר:

הם משאבים אדירים אחרים, שנמצאים שם, יש לנו את מנת"י.

שלומי בני:

מנת"י.

עפרה ברכה:

נכון,

ציון סמולר:

יש לנו גופים,

עפרה ברכה:

גם חינוך לבד, לא?

ציון סמולר:

החינוך עצמו, הוא ברעיון שלה, יש לו את האופציות שלו, יש לנו חברות בת, השאלה לאן את הולכת, לאיזה כיוון,

אלדד רבינוביץ:

מה שאתה מייצר זה לא רחב, זה לא בעצם,

ציון סמולר:

כרגע הסקופ עצמו, לא מדבר על הנקודות האלה.

אלדד רבינוביץ:

אני לא יודע מה זה סקופ.

ציון סמולר:

סקופ זה הפעילות,

אלדד רבינוביץ:

כן,

שלומי בני:

תיחום העבודה, היקף העבודה.

ציון סמולר:

תודה. זה לא מדבר, הסכומים שאני מדבר כרגע זה הנקודה של אגף המחשוב, המחשוב העירוני הלאנס, (לא ברור) שלנו, בשביל, אני יודע פשוט מהכובע הקודם שלי גם שוב, הקטע של המצלמות, ותשתיות שקיימות שמה, אני מכיר שם את הפערים, באופן מקצועי, לא בקטע זה. נדרש משאבים רבים בשביל לגרום ליישר, קו ברמה אבטחתית, צריך לעשות שם לעבודה, פעולות חריש.

אלדד רבינוביץ:

הוא לא יכול להכיל את ה - , חלק, לפחות חלק מהדברים שאתה מספר,

ציון סמולר:

אל תשכח זה שאני אחד כרגע באגף, בוא נתחיל מזה, אחד. מקים עכשיו את כל המערך הזה, זה משהו שהוא,

עפרה ברכה:

זה גם כיף, להתחיל משהו מאפס.

ציון סמולר:

דבר ראשון אני נהנה, אני פשוט כיף לי אחד.

עפרה ברכה:

דברים כאלה,

ציון סמולר:

שתיים, אני אומר את כל הדברים האלה, ובאמת אכפת לי מהארגון הזה, אני פה שנים, אני ממש כאילו אכפת לי מכל דבר שלכם. צריך אבל לעשות סדר עדיפות, כי אני גם מכיר את התקציב, מכיר את כל מה שקורה. ולראות איך אנחנו מנסים את השמיכה לפעמים למשוך לשם, לפעמים לצד שני, אבל לפחות לנסות לעשות משהו כדי שלא יהיה פה, דברים הרבה יותר משמעותיים. חלק מדו"ח הביקורת, שלא ציינת פה בנקודה הזאת, ואני מוסיף אותה,

עפרה ברכה:

אבל הסיפור הזה של המצלמות, הוא לא חונה אצלך העניין הזה של אבטחה, הגנת סייבר וכולה.

ציון סמולר:

אני נותן שמה את האינפוט, אבל אני יכול לעשות לזה נוהל, מה אני צריך לפעול, אבל באופן הכללי, בשביל ליישם את זה, נדרש משאבים שלהם, שנמצאים חברת מוטורולה, לדוגמא אנחנו פה עם נס,

עפרה ברכה:

מבחינה מקצועית, אתה זה שצריך לתת להם מה, מה לעשות, מה,

ציון סמולר:

אני יכול לסייע להם.

עפרה ברכה:

מה הכלים שהם, לסייע זה בטח, אבל איפה זה חונה?

אלדד רבינוביץ:

אתה הרגולאטור שלהם?

עפרה ברכה:

אתה, בדיוק.

אלדד רבינוביץ:

בסייבר?

ציון סמולר:

של החבר'ה שמה?

שלומי בני:

אני חושב שצריך להגדיר את זה, זה אולי, זה אולי התפקיד של הנהלת העירייה, או מה תפקידו, מה תחומי האחריות, של המנהל הגנת הסייבר. האם הוא גם,

עפרה ברכה:

האם הוא כולל גם את ה - ,

אלדד רבינוביץ:

אני אמליץ שהוא יהיה הרגולאטור.

עפרה ברכה:

בדיוק,

אלדד רבינוביץ:

של כל המערכות.

שלומי בני :

אם אתה שואל אותי, צריך להיות אחד, אחד.

אלדד רבינוביץ :

כבר לא צריך הרבה עבודה,

שלומי בני :

עכשיו הוא רוצה עוד תקציב,

ציון סמולר :

בלי תקציב, אבל בלי אנשים. לבד עם עצמו.

עו"ד דני ליבמן :

יש מגמה חדשה בעירייה, שמנהלי האגף שהם האגף.

שלומי בני :

לשאלתך סליחה, הוא לא יכול להכיל את אותן ההגנות, בפלטפורמות שונות,

ציון סמולר :

תודה רבה.

שלומי בני :

ההגנות למצלמות, זה הגנות למצלמות. ההגנות למערכות כריזה, זה מערכות,

עפרה ברכה :

נכון, אבל,

שלומי בני :

למערכות כריזה, לא, כי הוא שאל, האם אתה לא יכול לעשות משהו,

אלדד רבינוביץ :

כן, זה הכוונה.

שלומי בני :

לסגור את כל הארגון וזהו, מה? אתה אומר, סגור לי את אבטחת המידע והסייבר,

אלדד רבינוביץ:

לא רק באבטחה,

שלומי בני:

אז זה שונה.

אלדד רבינוביץ:

הזכרתם הרבה מאוד מוצרים שונים, הרבה פעילויות.

שלומי בני:

פלטפורמות שונות, רשת מחשוב של קבצים,

ציון סמולר:

זה אחר לגמרי.

שלומי בני:

טלפונים סלולאריים שונים, מצלמות שונה, מערכות כריזה שונה. יש את כל העולם ה-OT, בסדר?
ה-OT זה בעצם כל הבקרים, כל המצלמות, כל ה- , כל משהו שהוא לא,

ציון סמולר:

שנמצאת במרחב הציבורי, יש מרחב פנימי שלנו, שזה של הקבלן, תודה רבה לך, ויש את הסביבה
החיצונית לארגון, כביכול, זה מתנהל ברשת אחרת, נפרדת. וטוב שכך,

שלומי בני:

כן,

ציון סמולר:

טוב שכך.

עפרה ברכה:

אז היום מי שדואג להגנה מפני מתקפות סייבר,

ציון סמולר:

זה שקד.

עפרה ברכה:

זה שקד?

ציון סמולר:

היום שקד שביט אמון על כל ה - , אופרציה, יש לו חברת מוטורולה, הוא מתקצב שם במיליונים, על ההגנות של הנקודות האלה. אני יודע שהיה גם בבוקר שיחה על זה עם מיכה, תמיד עטף אותו ועזר לו במה שאפשר, מיכה מזרחי זה הממונה על אבטחת מידע בארגון.

עפרה ברכה:

גורם אחד שיעשה.

אלדד רבינוביץ:

לא, אם יש אגף סייבר,

עפרה ברכה:

לא, כאילו,

אלדד רבינוביץ:

זה הגיוני שהוא, אתה מתכלל את הדבר הזה שתהיה רגולאטור ארגוני, לא? אני טועה בניתוח הארגוני?

ציון סמולר:

יכול להיות שצריך לעשות את זה בצורה,

אלדד רבינוביץ:

כן, זה על דודו, מה?

דודו אמזלג:

זה יקשרו לך את הזה, ואז אתה תראה.

עפרה ברכה:

אתה חושב שלומי, אתה בעצם לא מכיר פשוט את דו"ח המצלמות, אבל לאור המקצועיות שלך, שיכול להיות גורם אחד, שבעצם רגולאטור לכל ההיבטים, זה לא משנה שזה מצלמות, אני לא יודעת לדבר בשפה המקצועית, אבל הלוגיקה של, מצלמות זה באמצעות תוכנה כזו או אחרת, אמצעי כזה,

שלומי בני :

אני אגיד לך מה אני חושב, אני חושב שצריך להיות,

עפרה ברכה :

אולי צריך להיות אחד שמכיר את הנושא,

שלומי בני :

אני חושב שכן, אני חושב שכן, צריך להיות אדם אחד, בסופו של דבר שמדווח להנהלת הארגון.

עפרה ברכה :

שמדווח,

שלומי בני :

הנהלת עירייה, הנהלת ארגון, אחד.

עפרה ברכה :

והוא יודע לתת גם,

שלומי בני :

ראש העיר לא משנה מה,

ציון סמולר :

לשבת איתו קצת, הוא מאוד, לא יצאנו להכיר,

שלומי בני :

שב בשמחה בוודאי,

ציון סמולר :

בכיף, אפשר לשבת,

שלומי בני :

אחד, אתם לא יכולים לקבל מידע, לשלושה אנשים, אבטחת מידע.

ציון סמולר :

אני חייב,

דודו אמזלג:

זה עדיין (לא ברור).

שלומי בני:

עכשיו זה לא צריך להיות ענייני אגו, בסדר? זה לא, זה צריך להיות מישהו אחד, שבסוף מדווח להנהלת הארגון, כדי שהיא תוכל לתקצב, כדי שיהיה מודעות, כדי שיהיה,

אלדד רבינוביץ:

אני לא מדבר על הדיווח, אני מדבר על ה - , על כתיבת הנהלים, ועל הרגולציה ועל ה - , ועל הבקרה,

שלומי בני:

מבחינתי, אני לקחתי את הדיווח,

אלדד רבינוביץ:

אתה הולך למעלה, אני הולך ללמטה.

שלומי בני:

בכוונה לקחתי את הדיווח, כי משמה אתה מתחיל להוריד, את המדיניות, את הנהלים, את הכול, בהחלט.

עפרה ברכה:

תוכנית עבודה מסודרת, מבדקי חדירה, בדיקתם, צריכה להיות פה עבודה מסודרת, בואו, אנחנו לא רוצים להגיע לרגע הזה.

שלומי בני:

צריך להיות רגולאטור אחד,

עפרה ברכה:

אני גם סבורה.

אלדד רבינוביץ:

בסוף זה, טוב, זה,

עפרה ברכה:

מה?

אלדד רבינוביץ:

סיימנו, נכון?

שלומי בני:

בגדול כן.

אלדד רבינוביץ:

עוד משהו?

שלומי בני:

כן, אני חושב שכן,

ציון סמולר:

תודה רבה.

אלדד רבינוביץ:

אז בסוף אנחנו מדברים על אירוע שלא אולי יהיה, שקורה, קורה כל היום, וכנראה גם יהיה בצורה יותר גדולה.

שלומי בני:

שאותה יהיה, והוא יהיה,

אלדד רבינוביץ:

נכון,

ציון סמולר:

תמיד הוא מקדים אותנו, צריכים להבין שתמיד תמיד מקדימים אותנו בצורה מאוד מאוד קיצונית, כי רוצים להיות יותר חכמים ממה שאתה כבר היית חכם אתמול.

אלדד רבינוביץ:

מה שאתה גם רמזת, יש כאן מעורבות מדינתית, מעורבות של, של ביג, של חברות גדולות, ושל יכולות מאוד גבוהות.

ציון סמולר:

אתם דיברתם על רגולציה, ממה שאני מכיר לפחות, רגולציה לרשויות מקומיות, לא קיים. אבל אני מנסה לעשות שיתופי פעולה, כי אני מכיר גם חברים שלי שנמצאים ב - , במערך הסייבר הלאומי,

שהם בעצם יש להם איזה סוג של רגולאציה, וזה גם הם מסייעים לנו, בעת הצורך, צריך לסייע, ואני מנסה מאוד מאוד לחבר אותנו אליהם. כדי שהם ינחו אותנו, יגידו מה צריך ברף של המחשוב, אנחנו מחוברים לדוגמא עם מסוק שלהם, נותנים לנו דיווחים, מחזירים לי איזונים, קבלת תשובות, זה מה שהם נותנים לנו, והם סוג של עיניים, גם לוקחים חלק מכל האחריות של האירוע הזה. אז אני קבעתי פגישה, עם בן אדם שאחראי גם על עיריית ירושלים, וכל הזה, הכניס אותם, קבעתי שבוע הבא, אני אמור להיפגש איתו, אני מאוד אשמח אם אפשר, כאילו באמת להשתמש בשירות,

שלומי בני:

אני רק, אני רק אחדד אני בכובע של ביקורת.

עפרה ברכה:

צריך לשים לב ששלומי לא יועץ,

שלומי בני:

כן, אני בכובע של ביקורת,

עפרה ברכה:

כי אם הוא ייתן לך, להסביר לך את זה,

שלומי בני:

כן,

עפרה ברכה:

אם שלומי היום מייצץ לך משהו, ומחר הוא צריך לבקר, הוא לא יוכל לבקר אחר כך את הפעילות,

ציון סמולר:

רק הסוגיה הזאתי של הרגולציה.

עפרה ברכה:

אבל אם אתה רוצה קצת הסברים, קצת יותר על הדו"ח, וזה.

שלומי בני:

בנקודה של רגולציה אין, אין בעיה.

אלדד רבינוביץ:

עכשיו חלק נגזור את זה, גם זה יהיה שיפור, (לא ברור) של דיירים,

עפרה ברכה:

עזוב מה שאפשר, בוודאי.

ציון סמולר:

ברגולציה אני מאוד אשמח לשבת איתו, הנקודה הזאת,

עפרה ברכה:

בסדר.

ציון סמולר:

כי זה קווים שצריך, שלא לא אפורים,

עפרה ברכה:

בסדר, שלומי מכיר את זה, את המגבלות שיש לו.

אלדד רבינוביץ:

טוב, בסוף זה מטרת הביקורת לייעל,

ציון סמולר:

כן, לשפר, נכון.

אלדד רבינוביץ:

לייעל, ליישם את הביקורת.

שלומי בני:

הפתיחה שלי לא היה לפי, לפי כמות הממצאים, אני חייב לציין.

עפרה ברכה:

טוב, אני לא מסכמת את זה, אבל באמת אחרי, כמה דיונים? ארבעה? ארבעה דיונים.

דודו אמזלג:

אנחנו יומיים כבר.

עפרה ברכה:

אני יכולה לומר, מה?

דוברת לא מזוהה:

מיום שני.

עפרה ברכה:

יומיים, שאני באמת בוא נאמר שזה עושה לי קצת נחת שהדברים קורים, ואנשים באמת לוקחים, וחלק לא רק (לא ברור), לא הכול נעשה מנחת, לא היום ולא אתמול, זה לא זה. אבל באמת יש פה איזה שהיא, לוקחים את הדברים ומאמצים, חלק מההמלצות, אפילו חלק מהמקרים את רובן, והדוחות מהווים חלק מתוכניות העבודה, ומבחינתי זה הישג של הביקורת. ואנחנו משקיעים בזה באמת לא מעט זמן. כדי שהדוחות יהיו ברמה מקצועית טובה, שישתדלו לגעת, בכל הנקודות, בכל ההיבטים בכל נושא, אנחנו עושים באמת השתדלות, כמובן שאני לא לבד, יש את העובדים, והיועצים, וכשאנחנו מגיעים, ואנחנו רואים באמת רצון לתקן, לשפר, ולוקחים את זה באמת כחלק מתוכנית העבודה, מבחינתי זו המטרה שלי בסוף. וככל שדוח נכתב, ובסוף לא מאמצים אותו, או לא קורים דברים, בעקבותיו, אז הוא יכול להיות מעולה, אבל אם הוא רק מונח במגירה זה, אני גם ברמה האישית, ארגיש רע מאוד עם זה.

אלדד רבינוביץ:

מתחבר לדברים, ואנחנו בעצם התחלנו את כל, את כל היומיים האלה בדו"ח על, על מיגון, על מיגון של תושבי העיר, של דו"ח שבעצם יצא ב – 21, ולא מומש, ועכשיו ב – 23 פתאום התרסקנו ל – , מיגון, על מיגון פיזי, מיגון של תושבי העיר, זה דו"ח שיצא ב – 21, היו ממצאים מאוד חמורים. בעצם הגענו למלחמה בלי יישום של כמעט אף ממצא, ושם אנחנו הערנו את זה שבאמת הדוחות חייבים להיות מיושמים, וזה השאיפה בסוף, בסוף השאיפה של הוועדת ביקורת היא לא לעשות פול גז וניוטל, אלא לרבות שבאמת הדברים נכנסים לתוך תהליכי עבודה, וככל שרואים ראשי אגפים וראשי מינהלים ראשי מחלקות שבאים כצמאים לתיקון, מסתכלים מתייחסים לביקורת, כמשהו שהוא כלי עזר עבורם, אז באמת הדבר הזה יכול להיות להתממש, אני חושב שזה מה שראינו בדו"ח הזה, זה גם מה שראינו בעוד כמה דוחות היום, באמת נושא מאוד משמעותי, אני מקווה ש – , שהתקדמנו.

עפרה ברכה:

בעזרת השם.

ציון סמולר:

תודה רבה לכם.

עפרה ברכה:

תודה רבה, בהצלחה.

אלדד רבינוביץ:

תודה רבה.

עפרה ברכה:

תודה רבה שלומי.

סיום הדיון