כ״ט בחשון תשפ״ו
20 בנובמבר 2025
סימוכין: 2025-103-959

<u>דו״ח מישיבה מס׳ 23 של ועדת ביקורת</u>
<u>שהתקיימה ביום שני, י״ח בתמוז תשפ״ה (14.7.2025)</u>

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

נכחו: גב׳ עופרה ברכה, מבקרת העירייה
מר ינון נוימן, מנהל אגף לביקורת ובקרת יועצים
עו״ד דני ליבמן, משנה ליועמ״ש לנושאים מיוחדים
גב׳ אורטל אריה, מנהלת מחלקה בכירה לפיתוח תכנון ובקרה
עו״ד רונן יאס, עוזר ראשי ליועמ״ש
מר אהרן כהן, כלכלן תקציבים בכיר
מר ברק לוי, מנכ״ל עמותת לביא
מר צחי קינן, מנהל אגף לוגסטיקה ומערכות מידע בעמותת לביא
מר שלומי בני, יועץ הביקורת
מר צבי עבו, מזכיר ועדת ביקורת

<u>על סדר היום:</u>

דוח מבקרת העירייה בנושא: אבטחת מידע וסייבר בעמותת לביא

<u>פתיחת הדיון:</u>

<u>מר אלדד רבינוביץ, יו״ר הוועדה</u>: ממשיכים בביקורת על תחומי הסייבר הגנת המידע והפרטיות בחברות העירוניות. עד כה הביקורת הייתה משמעותית וחשובה. נמצאו נקודות משמעותיות לשימור ולשיפור.

תחום הסייבר והגנת הפרטיות משמעותי ומדובר בשנים האחרונות. בחודשים האחרונים הוא עלה מדרגה בגלל שיש הרבה שחקנים עולמיים ואזוריים בעלי יכולות משמעותיות בתחום, אנחנו חייבים להיות ערוכים ומוכנים כנגדם. אני מברך שוב על עריכת הביקורת ומברך את המבוקרים על המענה.

<u>גב׳ עופרה ברכה, מבקרת העירייה</u>: מינהל הביקורת בחר השנה להתמקד גם באבטחת מידע וסייבר בכל התאגידים העירוניים. יש המון סיבות למה נדרש מערך סייבר טוב אצלכם, ושמחה שביצענו ביקורת גם אצלכם.

<u>דיון הוועדה:</u>

פרק 1:

<u>המלצת המבקרת:</u>

- למפות ולרשום את מאגרי המידע הנדרשים לרישום בהתאם לחוק ותקנותיו וכן לקבוע את רמת אבטחת המידע הנדרשת בכל אחד ממאגרי המידע בהתאם לתקנות.
- לגבש מדיניות ונוהלי אבטחת מידע ובהם פירוט של ההנחיות ואמצעי אבטחת המידע בעמותה ובמאגרי המידע בפרט. אלה יכללו לכל הפחות את דרישות התקנות וכן נושאים נוספים כגון: ניהול אירוע אבטחת מידע, ניהול נכסי מערכות מידע ועוד.
- להכין מסמכים של מבנה מאגרי המידע וכן רשימת מצאי של מערכות המאגרים, בהתאם לדרישות בתקנות כגון: תיאור ופירוט התשתיות ומערכות החומרה, סוגי רכיבי התקשורת, מערכות התוכנה המשמשות להפעלת מאגרי המידע, רמת האבטחה של כל מאגר, תרשים הרשת הארגונית וכדומה.
- לקיים הדרכות לעובדי ולמשתמשי המערכות בעמותה באופן שוטף (ולא רק בקליטת עובד חדש) על חובותיהם לפי החוק, לקיים הונאות דיוג (פישינג) מדומות באופן תדיר כדי לתרגל את העובדים בזיהוי הודעות דוא"ל חשודות.
- ליישם מדיניות סיסמאות במערכת InfoCASH.
- לחייב משתמשים חדשים לשנות לאלתר את הסיסמה הראשונית שקיבלו בכניסתם הראשונה לרשת העמותה.
- להסיר משתמשי-על שאינם נדרשים לכך מתוקף תפקידם.
- לבצע תהליך של סקירת משתמשים והרשאותיהם ברשת העמותה ובמערכות העמותה אחת לתקופה כפי שתקבע העמותה. בתהליך הסקירה יש לאשרר מחדש את קיום המשתמש ואת הצורך בהרשאות שניתנו לו.
- לגבש נוהל בדיקה שגרתי של נתוני התיעוד של מנגנון הבקרה.
- לגבש נוהל התאוששות מאסון ונוהל התמודדות עם אירועי סייבר, הכולל הנחיות לעובדי העמותה ולעמותה איך להתנהל בקרות אירוע סייבר.
- לפתח תהליך לקיום המשכיות עסקית, אשר יכלול בין השאר מיפוי הסיכונים שלהם חשופה העמותה, ניסוח אסטרטגיית המשכיות עסקית (BCP), הגדרת התהליכים והמערכות החיוניות לעמותה בעת חירום, הדרכות ותרגול התוכנית ועוד.
- להגדיר שמירת לוג פעולות במערכות אבטחת המידע ובמערכות המידע למשך 24 חודשים.
- לבצע סריקה של הלוגים ממערכות אבטחת המידע וממערכות המידע. מומלץ לבחון מערכת SIEM (Security Information and Event Management) לניטור אירועי אבטחת מידע, או לחלופין לבחון לקבל את השירות בתצורת שירות מנוהל.
- לבצע אחת לרבעון סריקת גישה בעזרת כלי אוטומטי כדי לאמוד את רמת החריגות הקיימות בשרתי הספריות ולבצע טיפול מונע.
- לבצע אחת לרבעון Vulnerability scanning (סריקת פגיעויות) בעזרת כלי אוטומטי (כגון Nessus ודומיה) כדי לאמוד את רמת המפגעים הקיימים ברשת ולבצע טיפול מונע.
- ליידע את בעלי ההרשאות במאגר בדבר קיום מנגנון הבקרה.
- לקיים דיון אחת לשנה לפחות באירועי אבטחה, ולתעד את הדיון באמצעות פרוטוקול.
- להתקין דרך קבע את עדכוני האבטחה המופצים על ידי חברת מיקרוסופט, וכן לשדרג מערכות הפעלה שאינן נתמכות על ידה.
- לגבש נוהל ספקי מיקור חוץ.

- למפות את כל המערכות אשר הספקים ניגשים אליהן ולבנות תהליך עבודה סדור הכולל:
  - קביעת רמת הסיווג של כל ספק (באיזו מידה הוא ניגש למידע רגיש, אם הוא שומר אצלו חומר של העמותה וכו').
  - חיבור מאובטח של ספקים לרשת העמותה.
  - בקרה על חיבור הספקים, ובכלל זה אישור חיבור מראש וכו'.
  - בחינת הטמעת מערכת הקלטות למערכות שאליהן מתחבר הספק.
- לתאם סקר ספק אצל ספק שזוהה שהחיבור שלו גורם לעמותה סיכון ברמה בינונית ומעלה.
- לבצע ביקורת תקופתית אחת ל-24 חודשים לפחות ובהתאם לדרישות התקנות.
- לבצע מבחני חדירה אחת לתקופה כפי שתקבע העמותה.
- למפות את גורמי הסיכון הארגוניים לדלף מידע.
- למפות את מקומות אחסון החומר הרגיש ואת מסדי הנתונים שבהם מוחזק המידע.
- לכתוב נוהל להוצאת מידע ממערכות העמותה.
- להפעיל בקרות להתמודדות עם דלף מידע, כגון: הדרכות להגברת מודעות עובדים, הפעלת מנגנון לחסימת אמצעים נתיקים, התקנת מערכת שימוש בדואר אלקטרוני מאובטח להעברת מידע רגיש, ניטור ספריות רגישות המחזיקות בחומרים רגישים לעמותה, וכיוצא באלו.
- לבחון שימוש במנגנוןDLP - Data Loss Prevention Software (מערכות למניעה של דלף מידע) במערכות הדואר האלקטרוני והאינטרנט.

<u>תגובת המבוקר:</u>
רוב ההמלצות מומשו או בתהליך מימוש יחד עם יועץ. השאיפה היא לבצע את כל ההמלצות עד אחד בנובמבר 2025.

<u>המלצת ועדת ביקורת:</u>
לקבל את המלצות המבקרת.
בנוסף, עד יום 1.11.2025 עמותת לביא תישלח עדכון למבקרת וליו"ר ועדת הביקורת בנוגע להשלמת יישום ההמלצות.

פרק 2:
<u>המלצת המבקרת:</u>

- **בדוח הביקורת הושמט הפרק השני על המלצותיו מטעמים של אבטחת מידע, כך גם בפרוטוקול זה.**

<u>תגובת המבוקר:</u>
חלק בוצע במיידי וקיימת תוכנית עבודה ליתרה.

<u>המלצת ועדת ביקורת:</u>
לקבל את המלצות המבקרת.
בנוסף, עד לסוף השנה הקלנדרית עמותת לביא תשלח עדכון למבקרת וליו"ר ועדת הביקורת בנוגע להשלמת יישום ההמלצות.

פרק 3:

<u>המלצת המבקרת:</u>

- **בדוח הביקורת הושמט הפרק השלישי על המלצותיו מטעמים של אבטחת מידע, כך גם בפרוטוקול זה.**

<u>תגובת המבוקר:</u>

רוב ההמלצות מומשו או בתהליך מימוש.

<u>המלצת ועדת ביקורת:</u>

לקבל את המלצות המבקרת.

בנוסף, עד לסוף השנה הקלנדרית עמותת לביא תשלח עדכון למבקרת וליו"ר ועדת הביקורת בנוגע להשלמת יישום ההמלצות.

פרק 4:

<u>המלצת המבקרת:</u>

- **בדוח הביקורת הושמט הפרק הרביעי על המלצותיו מטעמים של אבטחת מידע, כך גם בפרוטוקול זה.**

<u>תגובת המבוקר:</u>

טופל במיידי.

<u>המלצת ועדת ביקורת:</u>

לקבל את המלצות המבקרת.

<u>סיכום:</u>

<u>מר אלדד רבינוביץ, יו"ר הוועדה:</u> ראינו דוח ביקורת משמעותי וראינו גם קבלה שלו בשתי ידיים תוך רצון לתיקון והתפתחות. מטרת הביקורת שתצמח לתוכניות עבודה, נראה שזה הכיוון. תודה לכולם על העבודה המקצועית.

אני מקבל את המלצות הדוח בהתאם למפורט לעיל, ממליץ למועצה לאמץ את מסקנות הוועדה. טבלת הממצאים וההמלצות המצורפת, מהווה חלק בלתי נפרד מפרוטוקול הדיון.

הישיבה נעולה.

בברכה,

אלדד רבינוביץ
חבר מועצת העיר ירושלים
יו"ר ועדת ביקורת