



ועדה לענייני ביקורת

כ"ט בחשוון תשפ"ו
20 בנובמבר 2025
סימוכין: 2025-103-959

דו"ח משיבה מס' 23 של ועדת ביקורת שהתקיימה ביום שני, י"ח בתמוז תשפ"ה (14.7.2025)

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

נכחו: גבי עופרה ברכה, מבקרת העירייה
מר ינון נוימן, מנהל אגף לביקורת ובקרת יועצים
עו"ד דני ליבמן, משנה ליועמ"ש לנושאים מיוחדים
גבי 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

על סדר היום:

דוח מבקרת העירייה בנושא: אבטחת מידע וסייבר בעמותת לביא

פתיחת הדיון:

מר אלדד רבינוביץ, יו"ר הוועדה: ממשיכים בביקורת על תחומי הסייבר הגנת המידע והפרטיות בחברות העירוניות. עד כה הביקורת הייתה משמעותית וחשובה. נמצאו נקודות משמעותיות לשיפור 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.

גבי עופרה ברכה, מבקרת העירייה: 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.



ועדה לענייני ביקורת

דיון הוועדה:

פרק 1:

המלצת המבקרת:

- 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 (פשינג) 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 החרیגות 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.
- ליידיע 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 ידיה.
- לגבש נוהל ספקי מיקור חוץ.



ועדה לענייני ביקורת

- 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 בקורות 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 רגשים לעמותה, וכיוצא באלו.
- לבחון שימוש במנגנון DLP - Data Loss Prevention Software (מערכות למניעה של דלף מידע) במערכות הדואר האלקטרוני והאינטרנט.

תגובת המבוקר:

רוב ההמלצות מומשו או בתהליך מימוש יחד עם יועץ. השאיפה היא לבצע את כל ההמלצות עד אחד בנובמבר 2025.

המלצת ועדת ביקורת:

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:

המלצת המבקרת:

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

תגובת המבוקר:

חלק בוצע במייד וקיימת תוכנית עבודה ליתרה.

המלצת ועדת ביקורת:

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



ועדה לענייני ביקורת

פרק 3:

המלצת המבקרת:

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

תגובת המבוקר:

רוב ההמלצות מומשו או בתהליך מימוש.

המלצת ועדת ביקורת:

לקבל את המלצות המבקרת.

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

פרק 4:

המלצת המבקרת:

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

תגובת המבוקר:

טופל במייד.

המלצת ועדת ביקורת:

לקבל את המלצות המבקרת.

סיכום:

מר אלדד רבינוביץ, יו"ר הוועדה: 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

פרק רביעי

הגנת הפרטיות, אבטחת מידע וסייבר בעמותת לביא

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 // 85

מבוא // 89

פירוט הממצאים

פרק ראשון:

בדיקת רגולציה, מדיניות, נהלים ותהליכים בתחום אבטחת מאגרי מידע // 95

פרק שני:

מבדק מערכות אבטחת מידע // הושמט

פרק שלישי:

מבדק חדירה פנימי // הושמט

פרק רביעי:

מבדק חדירה חיצוני // הושמט

סיכום // 110

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.

שלושת היעדים העיקריים של אבטחת מידע והגנת סייבר הם אלה:

שלמות – הגנה מפני שינוי זדוני של המידע או השמדתו, לרבות הבטחת אימות זהויות בעלי המידע.

זמינות – שמירה על זמינות ויעילות הגישה אל המידע בכל זמן נתון.

סודיות – הגבלת גישה או חשיפה, ובכלל זה הגנה על פרטיות וזכויות קנייניות.

זכות האדם לפרטיות היא אחת הזכויות החשובות בישראל והיא מעוגנת בחוק הגנת הפרטיות החל משנת 1981 (להלן: החוק) לרבות תקנותיו משנת 2017 (להלן: התקנות).

איסוף מידע פרטי הפך להיות קל יותר מבעבר עקב התקשרות של פרטים/ארגונים עם גופים רבים וקבלת שירותים מספקים שונים. סעיף 7 לחוק מגדיר "מאגר מידע" כאוסף נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב, למעט אוסף לשימוש אישי ולא עסקי או אוסף הכולל רק שם, מען ודרכי התקשרות (מידע שכשלעצמו אינו יוצר פגיעה בפרטיות).

חובת רישום מאגר מידע מעוגנת בסעיף 8 לחוק. מטרת הרישום היא להבטיח את ההגנה על הפרטיות במאגר, ולתת כלים, הן בידי רשם מאגרי המידע והן בידי הציבור שמידע על אודותיו מנוהל במאגרי המידע, לאכוף את הזכויות והחובות המוטלות בחוק הגנת הפרטיות על בעלי מאגרים.

הביקורת בחנה את מידת עמידתה של העמותה בהוראות חוק הגנת הפרטיות, התשמ"א-1981, ותקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, ואת המדיניות והנהלים בנושא אבטחת המידע, וערכה כמה בדיקות: מבדק טכנולוגי לבחינת רמת האבטחה הקיימת בעמותה, בדיקה פיזית לאבטחת המידע ומבדקי חדירה לרשת העמותה.

הביקורת העלתה ליקויים מהותיים ביישום הוראות חוק הגנת הפרטיות ותקנותיו בנושאים אלה: מדיניות ונוהלי אבטחת המידע, הקשחות עמדות קצה ושרתים, ניהול מערכת האנטי-וירוס, ניהול מערכת חומת האש, ניהול מערכת ה-AD (Active Directory – מערכת לניהול משתמשים), וכן העלתה ליקויים בעלי חשיבות גבוהה במבדקי החדירה שביצעה הביקורת.

עיקרי הממצאים

1. לעמותה אין כלל מסמכים של הגדרות מאגרי מידע ושל מבנה מאגרי המידע בהתאם לדרישות בתקנות. לא קיימת רשימת מצאי של מערכות המאגרים, והעמותה אף לא רשמה מאגר מידע של עובדיה.
2. לעמותה אין מדיניות אבטחת מידע מפורטת הכוללת את כל היבטי אבטחת המידע בארגון, בדגש על אבטחת מאגרי המידע.
3. העמותה אינה מקיימת הדרכות בנושא אבטחת מידע באופן סדיר לעובדיה ואינה מקיימת תרגולי הונאת דיוג (פשינג) באופן תדיר.
4. קיימים ליקויים משמעותיים במדיניות הסיסמאות של מערכות העמותה.
5. קיים מספר גבוה של משתמשי-על במערכות וברשת הארגון. ונוסף על כך, לא מבוצעת סקירה תקופתית לבדיקת הרשאות העובדים ברשת ובמערכות שמנהלות את מאגרי המידע.
6. בעלי מאגרי המידע לא קבעו נוהל בדיקה שגרתי של נתוני התיעוד של מנגנון הבקרה; לוגים וניטורי אירועי אבטחת מידע נאספים רק במערכת האנטי-וירוס ולא ביתר מערכות אבטחת המידע; לוג הפעולות במערכות אבטחת המידע ובמערכות המידע אינו נשמר למשך 24 חודשים.
7. לעמותה אין נוהל התאוששות מאסון ואין תוכנית להמשכיות עסקית.
8. ישנן מערכות שאינן מעודכנות בעדכוני אבטחת מידע קריטיים.
9. העמותה לא ביצעה ביקורת תקופתית כדי לוודא שהיא עומדת בהוראות החוק והתקנות.
10. העמותה לא ביצעה מבדקי חדירה משנת 2022.
11. עמדות הקצה, השרתים וה-GPO (Group Policy) אינם מוקשחים מספיק; שיטות העבודה הנהוגות אינן מקובלות בתחום אבטחת המידע והסייבר. נמצא מספר רב של הגדרות שאינן תקינות.
12. נמצאו ליקויים רבים בעלי חשיבות גבוהה בניהול ובתחזוקת מערכת האנטי-וירוס ובמערכת עדכוני אבטחת המידע. המערכות אינן מנוהלות ומתוחזקות בהתאם לסטנדרטים המקובלים.
13. נמצאו ליקויים רבים בעלי חשיבות גבוהה בניהול ובתחזוקת מערכת ה-AD (Active Directory - מערכת לניהול משתמשים), המערכת אינה מנוהלת ואינה מתוחזקת בהתאם לסטנדרטים המקובלים.
14. נמצאו ליקויים רבים בעלי חשיבות גבוהה במבדקי החדירה הפנימיים והחיצוניים שביצעה הביקורת.

המלצות מרכזיות

1. למפות את דרישות הוראות החוק והתקנות וליישמן במלואן, בין השאר - למפות את מאגרי המידע המחויבים ברישום בהתאם לחוק, וליצור מסמכי הגדרות מאגרי מידע.
 2. 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.
 3. להכין מסמכים של מבנה מאגרי המידע וכן רשימת מצאי של מערכות המאגרים, בהתאם לדרישות בתקנות.
 4. לקיים הדרכות לעובדי ולמשתמשי המערכות בעמותה באופן שוטף (ולא רק בקליטת עובד חדש) על חובותיהם לפי החוק, לקיים הונאות דיוג (פשינג) מדומות באופן תדיר כדי לתרגל את העובדים בזיהוי הודעות דוא"ל חשודות.
 5. להגדיר מדיניות סיסמאות נאותה במערכות העמותה.
 6. לבצע תהליך של סקירת משתמשים והרשאותיהם ברשת העמותה ובמערכות העמותה אחת לתקופה כפי שתקבע העמותה, וכן להסיר משתמשי-על שאינם נדרשים לכך מתוקף תפקידם.
 7. לקבוע נוהל בדיקה שגרתי של נתוני התיעוד של מנגנון הבקרה, להגדיר איסוף לוגים וניטורי אירועי אבטחת מידע מכל מערכות אבטחת המידע בעמותה, ולשמור לוג פעולות במערכות המידע ובמערכות אבטחת המידע למשך 24 חודשים לפחות.
 8. לגבש נוהל התאוששות מאסון ולבנות תוכנית להמשכיות עסקית.
 9. להתקין בדרך קבע את עדכוני האבטחה המופצים על ידי יצרני המערכות.
 10. לבצע ביקורת תקופתית כדי לוודא שהעמותה עומדת בהוראות החוק והתקנות.
 11. לבצע בהקדם סקר סיכוני אבטחת מידע ומבדקי חדירה.
 12. לטפל בדחיפות בהקשחת עמדות הקצה, השרתים וה-GPO (Group Policy), וכן בממצאים שעלו במערכות האנטי-וירוס, בעדכוני אבטחת מידע, בחומת האש ובמערכת ה-AD.
 13. לטפל בדחיפות בממצאים שעלו במבדקי החדירה הפנימיים שביצעה הביקורת.
 14. לטפל בממצאים שעלו בבדיקת תשתית למערכת הדואר האלקטרוני והאנטי-ספאם לדואר האלקטרוני.
 15. לטפל בממצאים שעלו בבדיקת אתר האינטרנט של העמותה.
- תמצית זו אינה כוללת את כל הממצאים שעלו וגם אינה מציגה את כל ההמלצות והפרטים המופיעים בגוף הדוח. לקבלת מידע זה יש לקרוא את הדוח המפורט.

סיכום

זכות האדם לפרטיות היא אחת הזכויות החשובות בישראל והיא מעוגנת בחוק הגנת הפרטיות החל משנת 1981 (להלן: החוק) לרבות תקנותיו. החוק מגדיר מהי פגיעה בפרטיות, ובין השאר הוא מסדיר גם את פעילותם של מאגרי מידע הכוללים מידע פרטי ורגיש.

במאי 2017 פורסמו תקנות הגנת הפרטיות ואבטחת מידע, התשע"ז-2017. התקנות מגדירות בפירוט את החובות של בעל מאגר מידע ליישום בקורות תהליכיות וטכנולוגיות לצורך אבטחת המאגר. הוראות אלו נכתבו, בין היתר, בשל העלייה המתמדת בהיקף ובעוצמת תקיפות הסייבר בארץ ובעולם. בין המותקפים ניתן למנות בתי חולים, אוניברסיטאות, עיריות, חברות ביטוח, תשתיות, אתרי אינטרנט ועוד. מתקפות שמשיגות את יעדיהן עלולות לערער את היציבות הארגונית, לפגוע בנכסי הארגון, במוניטין שלו ובלקוחותיו, ולעיתים אף לסכן חיי אדם.

עמותת לביא היא יעד פוטנציאלי לניסיון תקיפות סייבר, בין היתר בשל היותה עמותה עירונית של עיריית ירושלים, עיר הבירה של מדינת ישראל ואחד מסמליה החשובים. ניסיונות חדירה ודלף של מידע, תקיפה והשחתה של אתר האינטרנט ומניעת שימוש במערכות, הם רק חלק מהסיכונים הקיימים במרחב הסייבר של העמותה.

עם התרחבות השימוש בטכנולוגיות הדיגיטליות והגברת השימוש במערכות מידע ובמאגרי מידע גובר הסיכון כי מידע ארגוני או אישי ייחשף ברבים, בזדון או בתום לב, דבר העלול לפגוע בארגון או בפרטיותם של גורמים שפרטיהם כלולים במאגרי המידע של הארגון.

כשאבטחת המידע אינה מנוהלת כראוי נוצרות במאגרי המידע פרוצדורות רבות.

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

הביקורת בחנה את מידת עמידתה של העמותה בהוראות החוק והתקנות, ואת המדיניות והנהלים בנושא אבטחת המידע, וכן ערכה כמה בדיקות: מבדק טכנולוגי לבחינת רמת האבטחה הקיימת בעמותה, בדיקה פיזית לאבטחת המידע, ומבדקי חדירה לרשת העמותה.

הביקורת העלתה ליקויים מהותיים ביישום הוראות חוק הגנת הפרטיות ותקנותיו בנושאים האלה: מדיניות ונוהלי אבטחת המידע, הקשחות עמדות הקצה והשרתים, ניהול מערכת האנטי-וירוס, ניהול מערכת חומת האש, ניהול מערכת ה-AD, וכן העלתה ליקויים בעלי חשיבות גבוהה במבדקי החדירה שביצעה.

על העמותה לטפל בהקדם בממצאים שהועלו, בדגש על עמידה בהוראות החוק ותקנותיו וטיפול בפערים הטכנולוגיים שנמצאו, לרבות במבדקי החדירה.

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 לעמותה לעמוד בחובותיה הרגולטוריות, וכפועל יוצא להפחית את הסיכונים למיניהם מעצם התרחשות האירוע.

מבוא

עמותת לביא, העמותה העירונית לפיתוח החינוך בירושלים, מפתחת ומוציאה לפועל חינוך איכותי וחדשני בהתאמה לכלל הקהילות והמגזרים בירושלים. להלן תחומי פעילותה:

- **חינוך משלים** – העמותה מספקת מסגרות חינוכיות בשלושת המגזרים בעיר: כללי, חרדי וערבי, בימים ובשעות שבהן המסגרות הפורמליות אינן פעילות. מסגרות אלו למעשה מאפשרות לקיים רצף חינוכי לילדי העיר.
- **ליווי היסעים** – הפעלת מערך היסעים בשיתוף עם עיריית ירושלים עבור יותר מ-13,000 תלמידי החינוך המיוחד במוסדות הלימודים השונים.
- **ליווי בתי ספר בניהול עצמי** – סיוע למנהלי מוסדות החינוך בהפעלת הניהול העצמי במוסדות החינוך היסודי והעל-יסודי ברחבי העיר.
- **פרויקטים בתחום החינוך** – ניהול של יותר מ-150 תוכניות ופרויקטים חינוכיים מגוונים, ובכלל זה ניהול פדגוגי, כספי ולוגיסטי, בשיתוף עם העירייה.

בעמותה יש כמה מערכות מידע עיקריות להנהלת חשבונות, שכר ותשלומים.

מנהל אגף לוגיסטיקה ומערכות מידע בעמותה מוגדר כמנהל מערכות המידע וממונה אבטחת המידע של העמותה. העמותה מקבלת שירותי ניהול ותמיכה מקצועיים גם מחברת מטריקס.

בשנים האחרונות יש עלייה מתמדת בהיקף ובעוצמת האיומים במרחב הסייבר בעולם כולו ובישראל בפרט, המתבצעים באמצעות תוכנות זדוניות (נוזקות וכופרות) המתפשטות דרך רשת האינטרנט, דרך 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 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.

הזכות לפרטיות וחובת השמירה על צנעת הפרט עוגנו בחקיקה. חוק הגנת הפרטיות, התשמ"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.

יש לציין כי ב-14.8.2024 פורסם ברשומות תיקון מקיף בחוק הגנת הפרטיות (תיקון מס' 13). התיקון מעדכן ומבהיר את החקיקה בתחום, קובע הסדרים חדשים ומתקדמים, ומקנה כלי אכיפה יעילים,

באופן שיתאים לאתגרי העידן הדיגיטלי, יגביר את ההגנה על זכות היסוד לפרטיות של הציבור בישראל, ויחזק את ההתמודדות כנגד איומי הסייבר הגוברים.

הרשות להגנת הפרטיות היא יחידה במשרד המשפטים האמונה על הסדרה, פיקוח ואכיפת החוק להגנת הפרטיות.

הרשות מפקדת על הגנת המידע האישי במאגרי מידע דיגיטליים ועל מימוש הזכות לפרטיות. לתכלית זו מפעילה הרשות רגולציה, לרבות אכיפה מינהלית ופלילית, על כלל הגופים בישראל - פרטיים, עסקיים וציבוריים - המחזיקים או המעבדים מידע אישי "דיגיטלי".

כאמור, לשם שמירה על צנעת הפרט ועל הוראות החוק נדרשת נקיטת אמצעים לאבטחת המידע ומערכי המידע ולהגנה עליהם מפני פגיעה, חשיפה ושינוי - במזיד או בשוגג. יש לעשות זאת באופן שיישמרו הזמינות, השלמות והסודיות של המידע ומערכות המידע.

בהתאם לאמור לעיל, העמותה מחויבת לעמוד בהוראות החוק להגנת הפרטיות, התשמ"א-1981, ותקנותיו.

הביקורת בדקה את מידת עמידתה של העמותה בהוראות חוק הגנת הפרטיות, התשמ"א-1981, ותקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, את המדיניות והנהלים בנושא אבטחת המידע - אם העמותה ביצעה מבדק טכנולוגי לבחינת רמת האבטחה הקיימת בעמותה, בדיקה פיזית לאבטחת המידע, מבדקי חדירה לרשת העמותה וכן נושאים 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).

מטרת הבדיקה

לבחון את נאותות התנהלות העמותה בהיבטי אבטחת המידע וצמצום הסיכון לתקיפות סייבר כנגד רשת העמותה ומערכות המידע שלה, על ידי בחינת מימוש אבטחת המידע של העמותה בהתאם למדיניות, לנהלים ולנהוג בחברות אחרות דומות.

לבחון את מידת הציות לחוק הגנת הפרטיות ולתקנותיו, החל מתהליך רישום מאגרי המידע הקיימים בעמותה ואבטחת המידע הקיימת על אותם מאגרים ועד לניהול ותחזוקה שוטפת של המאגרים בהתאם לחוק ולתקנותיו.

הערכת רמת אבטחת המידע באמצעות מבדק טכנולוגי ומבחני חדירה.

היקף הבדיקה

עמידת העמותה בהוראות חוק הגנת הפרטיות, התשמ"א-1981, ותקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (בהנחה שלפחות לאחד ממאגרי המידע נדרשת רמת אבטחה בינונית), בדיקת המדיניות והנהלים בנושא אבטחת המידע, מבדק טכנולוגי לבחינת רמת האבטחה הקיימת בעמותה, בדיקה פיזית לאבטחת המידע, ומבדקי חדירה לרשת העמותה.

תקופת הביקורת

הביקורת נערכה בחודשים נובמבר 2024 – ינואר 2025.

פירוט הממצאים

פרק ראשון

בדיקת ציות להוראות חוק הגנת הפרטיות ותקנות הגנת הפרטיות

רישום מאגרי מידע

חוק הגנת הפרטיות, תשמ"א-1981 מגדיר "מאגר מידע" כאוסף נתונים באופן ממוחשב. מידע אישי כגון שמות, מספרי טלפון, כתובות וכו', שאינם גורמים לפגיעה כלשהי בפרטיות של בעלי המידע, אינם מוגדרים כ"אוסף נתונים למאגר מידע" ולא יהיה צורך ברישום.

סעיף 8(ג) לחוק הגנת הפרטיות מציין כי "בעל מאגר מידע חייב ברישום בפנקס ועל בעל המאגר לרשמו אם נתקיים בו אחד מאלה:

- (1) מספר האנשים שמידע עליהם נמצא במאגר עולה על 10,000;
 - (2) יש במאגר מידע רגיש;
 - (3) המאגר כולל מידע על אנשים והמידע לא נמסר על ידיהם, מטעמם או בהסכמתם למאגר זה;
 - (4) המאגר הוא של גוף ציבורי כהגדרתו בסעיף 23;
 - (5) המאגר משמש לשירותי דיוור ישיר כאמור בסעיף 17ג.
- בבדיקת הביקורת עלה כי בעמותה קיימים שלושה מאגרי מידע העונים על הגדרה בסעיף 8(ג) לחוק, כדלהלן:
- **עובדים** – מאגר הקיים במערכת השכר הכולל מידע רגיש לגבי העובדים, כגון חשבונות בנק. המאגר כולל כ-7,500 רשומות (סעיף 8(ג)(2) לחוק).
 - **ילדים** – מאגר מידע הכולל מידע על התלמידים ותעודות הזהות שלהם. המאגר כולל כ-25,000 רשומות (סעיף 8(ג)(1) לחוק).
 - **הורים, תלמידים ומוסדות** – מאגר הכולל מידע על ההורים, התלמידים ועל המוסדות שאליהם הם משתייכים. מאגר זה כולל כ-25,000 רשומות (סעיף 8(ג)(1) לחוק).
- העמותה היא גוף ציבורי, ולכן סעיף 8(ג)(5) לחוק חל עליה. המשמעות היא כי שלושת מאגרי המידע של העמותה חייבים ברישום ברשות להגנת הפרטיות.
- נמצא כי אף לא אחד מהמאגרים רשום ברשות.

מסקנות

1. אי רישום מאגר מידע ברשות להגנת הפרטיות מעמיד את העמותה במצב שבו אין היא עומדת בהוראות החוק ותקנותיו.

המלצות

1. למפות ולרשום את מאגרי המידע הנדרשים לרישום בהתאם לחוק ותקנותיו וכן לקבוע את רמת אבטחת המידע הנדרשת בכל אחד ממאגרי המידע בהתאם לתקנות.

מדיניות ונוהל אבטחת מידע

הבסיס לפעילות אבטחת המידע הארגוני צריך להיות מסמך מדיניות אבטחת המידע או לכל הפחות, ניהול אבטחת מידע. מסמך זה אמור לשקף את תפיסת מדיניות האבטחה הארגונית, לתאר את התקן לפעילות, את שיטות העבודה ואת העקרונות המנחים.

סעיף 4 בתקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017 דן בנושא ניהול אבטחת מידע לבעל מאגר שמסתמך על מסמך הגדרות המאגר. בסעיף זה מצוין שהנוהל יישמר והגישה אליו תהיה רק לאנשים מורשים. בהתאם לסעיף ג לתקנה, הנוהל אמור לכלול, בין השאר, את הנושאים האלה:

- (1) הוראות בעניין האבטחה הפיזית והסביבתית של אתרי המאגר, כאמור בתקנה 6;
 - (2) הרשאות גישה למאגר המידע ולמערכות המאגר, בהתאם לתקנה 8;
 - (3) תיאור של אמצעים שמטרתם להגן על מערכות המאגר, ואופן הפעלתם לצורך כך;
 - (4) הוראות למורשי הגישה למאגר המידע ולמערכות המאגר לצורך הגנה על המידע במאגר;
 - (5) פירוט של הסיכונים שהמידע במאגר חשוף להם במסגרת הפעילות השוטפת של בעל מאגר המידע, לרבות אלה הנובעים ממבנה מערכות המאגר כמפורט בתקנה 5(א), אופן קביעת סיכונים אלו ואופן הטיפול בהם, לרבות על ידי מנגנוני הצפנה מקובלים להגנה על המידע השמור במאגר או במערכות המאגר;
 - (6) אופן ההתמודדות עם אירועי אבטחת מידע כאמור בתקנה 11, לפי חומרת האירוע ומידת רגישות המידע;
 - (7) הוראות לעניין ניהול של התקנים ניידים ושימוש בהם, כאמור בתקנה 12.
- בהתאם לסעיף (ד) לתקנה, לגבי מאגרי מידע שחלה עליהם רמת אבטחה בינונית או גבוהה, יש להתייחס גם לנושאים האלה:
- (1) אמצעי הזיהוי והאימות לגישה למאגר ולמערכות המאגר, בהתאם לתקנה 9;

(2) אופן הבקרה על השימוש במאגר המידע, ובכלל זה תיעוד הגישה למערכות המאגר כאמור בתקנה 10;

(3) הוראות לעניין עריכת ביקורות תקופתיות לוודא קיומם ותקינותם של אמצעי האבטחה לפי נוהל האבטחה ולפי תקנות אלה כאמור בתקנה 16;

(4) הוראות לעניין גיבוי הנתונים האמורים בתקנה 18(א);(1)

(5) הוראות לעניין אופן ביצוע פעולות פיתוח במאגר ותיעודן, ובכלל זה אופן הגישה של אנשי הפיתוח לנתונים במאגר.

נוסף על אלה, תקנה 4(ה) לתקנות 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".

בעמותה קיים נוהל אבטחת מידע המעודכן לינואר 2024, הכולל התייחסות למגוון היבטים באבטחת המידע. עם זאת, לא נמצאה מדיניות אבטחת מידע שאושרה על ידי הנהלת העמותה, וכן נהלים אחרים בנושאים נוספים, כגון: נוהל ניהול אירוע אבטחת מידע, ניהול נכסי מערכות מידע ועוד.

מסקנות

2. בשל חוסר במדיניות ובנוהלי אבטחת מידע בנושאים בעלי חשיבות, קיים קושי ביישום אבטחת מידע נאותה ובפיקוח עליה בעמותה.

המלצות

2. לגבש מדיניות ונהלי 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.

מיפוי מערכות מאגר המידע וביצוע סקר סיכונים

סעיף 5 לתקנות דן במיפוי מערכות מאגר המידע וביצוע סקר סיכונים. להלן עיקרי הסעיף:

"א. בעל מאגר מידע יחזיק מסמך מעודכן של מבנה מאגר המידע וכן רשימת מצאי מעודכנת של מערכות המאגר, ובכלל זה:

(1) תשתיות ומערכות חומרה, סוגי רכיבי תקשורת ואבטחת מידע;

(2) מערכות התוכנה המשמשות להפעלת מאגר המידע, לניהול המאגר ולתחזוקתו, לתמיכה בפעילותו, לניטור שלו ולאבטחתו;

(3) תוכנות וממשקים המשמשים לתקשורת אל מערכות המאגר ומהן;

(4) תרשים הרשת שפועל בה המאגר, הכולל תיאור הקשרים בין רכיבי המערכת השונים ומיקומם הפיזי של רכיבים אלה;

(5) תאריך העדכון האחרון של המסמך ושל רשימת המצאי.

ב. המסמך המעודכן של מבנה מאגר המידע ורשימת המצאי יישמרו כך שפרטים מהם יימסרו לבעלי הרשאה רק בהיקף הנדרש לצורך ביצוע תפקידיהם.

בעמותה לא קיימים מסמכים מפורטים של מבנה מאגרי המידע, הכוללים בין היתר התייחסות לתשתיות, לרכיבי תקשורת, וכן תרשים לרשת בהתאם להוראות התקנות.

העמותה ביצעה סקר סיכונים במהלך נובמבר 2024 ובמסגרתו עלו 40 ליקויים. 6 ליקויים ברמת סיכון קריטית ו-15 ברמת סיכון גבוהה.

מסקנות

3. חוסר במסמכים של מבנה מאגרי המידע ורשימת מצאי של מערכות המאגרים מקשה על יישום מנגנוני אבטחת מידע נאותים על מאגרי המידע ועל פיקוח העמותה עליהם. כמו כן העמותה אינה עומדת בעטיו בהוראות החוק ותקנותיו.

המלצות

3. 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.

אבטחה פיזית ואבטחת מידע בניהול כוח אדם

אבטחה פיזית היא חלק ממערך ההגנה מפני פריצות אבטחה ושמירה על המידע בארגון. סעיף 6 לתקנות דן בנושא האבטחה הפיזית, כדלהלן:

"א. בעל מאגר מידע יבטיח כי המערכות המפורטות בתקנה 5(א)(1) יישמרו במקום מוגן, המונע חדירה וכניסה אליו בלא הרשאה, והתואם את אופי פעילות המאגר ורגישות המידע בו.

ב. בעל מאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, ינקוט אמצעים לבקרה ולתיעוד של הכניסה והיציאה מאתרים שבהם מצויות המערכות המפורטות בתקנה 5(א)(1) ושל הכנסה והוצאה של ציוד אל מערכות המאגר ומהן".

ארגונים מתמודדים עם הצורך ההולך וגדל של עובדים, לקוחות ושותפים עסקיים, בגישה אל מקורות המידע הארגוניים. עם זאת, נדרש למלא צורך זה מבלי להתפשר על רמת אבטחת המידע. על העמותה לוודא כי ההרשאות ניתנות לעובדים בהתאם לעקרון הצורך לדעת.

סעיף 7 לתקנות דן במתן הרשאות לעובדים, כדלהלן:

"א. לא ייתן בעל מאגר מידע גישה למידע המצוי במאגר ולא ישנה היקף הרשאה שניתנה, אלא אם כן נקט אמצעים סבירים, המקובלים בהליכי מיון עובדים ושיבוצם, כדי לברר שאין חשש כי בעל ההרשאה אינו מתאים לקבלת גישה למידע המצוי במאגר....

ב. בטרם יקבלו גישה למידע ממאגר המידע או לפני שינוי היקף הרשאותיהם, יקיים בעל מאגר מידע הדרכות לבעלי הרשאות בנושא החובות לפי החוק ותקנות אלה, וימסור להם מידע על אודות חובותיהם לפי החוק ונוהל האבטחה.

ג. במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, יקיים בעל המאגר פעילות הדרכה תקופתית לבעלי הרשאות שלו, בדבר מסמך הגדרות המאגר, נוהל האבטחה והוראות אבטחת המידע לפי החוק ולפי תקנות אלה, בהיקף הנדרש לצורך ביצוע תפקידיהם, ובדבר חובות בעלי ההרשאות לפיהם; הדרכה כאמור תיערך אחת לשנתיים לפחות, ולגבי הסמכה של בעל הרשאה לתפקיד חדש – סמוך ככל האפשר למועד תחילת הסמכתו".

בעמותה קיימת אבטחה פיזית מלאה, הכוללת בין היתר:

- מצלמות אבטחה ברחבי אתר העמותה;
- מאבטח בכניסה המתעד כניסות ויציאות;
- מבקרים לא מורשים להיכנס ללא ליווי של גורם מורשה;
- הכניסה מחייבת אמצעי זיהוי ייעודי לכל עובד.

עם זאת, לא קיים תיעוד של כניסת אנשים לחדר השרתים והתקשורת.

בקשר לניהול כוח האדם, קיבלה הביקורת כתייעוד:

- רשימת המורשים לכל מאגר מידע:

- מערכת א' – רשימת המשתמשים הקיימת במערכת כוללת 75 משתמשים פעילים.
- מערכת ב' – רשימת המשתמשים הקיימת במערכת כוללת 28 משתמשים פעילים
- מאגר מידע נוסף – מאגר המידע הנמצא בשרתים, הוא "אחסון מידע" בכוננים שונים. מכיוון שזה לא רק בכונן אחד מתייחסים לכלל הכוננים בעמותה כאל מאגר מידע אחד.

- כל עובד חדש שמתקבל לעמותה עובר הדרכת אבטחת מידע. הביקורת קיבלה לסקירה את ההדרכה המעודכנת לינואר 2025, ונמצא כי היא כוללת התייחסות למגוון היבטי אבטחת המידע ואמצעי התגוננות.
 - קיום תרגול הונאת דיוג (פשינג) האחרון בוצע במהלך ספטמבר 2022 על ידי חברה המתמחה בכך.
- להלן תוצאות התרגול: 35 מתוך 117 לחצו על הקישור והזינו פרטים ו-20 לחצו על הקישור ללא הזנת פרטים. לאחר קיום תרגיל הדיוג, העבירה הדרכה פרונטלית ב-13.12.2022 בנושא אבטחת מידע. ממועד אותה ההדרכה ועד למועד הביקורת לא בוצעו הדרכות בנושא זה לעובדים, ולמנהלי מאגרי המידע בפרט.

מסקנות

4. העמותה אינה עומדת בהוראות החוק ותקנותיו בכך שאינה מקיימת הדרכות לבעלי הרשאות בנושא חובותיהם לפי החוק ונוהל אבטחת המידע ברמה שנתית, ובכך מגבירה את הסיכון מצד המשתמשים לטעויות ולעבירה על החוק שכלל לא היו מודעים לו. כמו כן, בשל אי קיום הדרכות מודעות לעובדים בנושא אבטחת מידע וסייבר מתגבר הסיכון לשימוש לא נכון במערכות המידע, בדואר האלקטרוני הארגוני ובמרחב האינטרנט, וכן הסיכון לטעויות אנוש אשר יובילו לחדירה לרשת העמותה.

המלצות

4. לקיים הדרכות לעובדי ולמשתמשי המערכות בעמותה באופן שוטף (ולא רק בקליטת עובד חדש) על חובותיהם לפי החוק, לקיים הונאות דיוג (פשינג) מדומות באופן תדיר כדי לתרגל את העובדים בזהוי הודעות דוא"ל חשודות.

ניהול הרשאות גישה

גישה למאגרי מידע בארגון צריכה להינתן בהתאם לעקרון הצורך לדעת, כלומר, רק גורמים מורשים מתוקף תפקידם יקבלו הרשאות לעדכון או לצפייה במאגרי המידע. נוסף על כך, הגישה למאגרים תהיה מאובטחת בהתאם לרמת האבטחה שהוגדרה לאותו מאגר מידע.

סעיף 8 לתקנות מציין כי:

א. בעל מאגר מידע יקבע הרשאות גישה של בעלי הרשאות למאגר המידע ולמערכות המאגר, בהתאם להגדרות תפקיד; הרשאות הגישה לכל תפקיד תהיה במידה הנדרשת לביצוע התפקיד בלבד.

ב. בעל מאגר מידע ינהל רישום מעודכן של תפקידים, הרשאות הגישה שניתנו להם, ושל בעלי ההרשאות הממלאים תפקידים אלה (להלן: רשימת ההרשאות התקפות).

סעיף 9 לתקנות מציין כי:

"א. בעל מאגר מידע ינקוט אמצעים מקובלים בנסיבות העניין ובהתאם לאופי המאגר וטיבו, כדי לוודא כי הגישה למאגר ולמערכות המאגר נעשית בידי בעל הרשאה המורשה לכך בלבד לפי רשימת ההרשאות התקפות.

ב. במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה –

(1) אופן הזיהוי יעשה ככל האפשר על בסיס אמצעי פיזי הנתון לשליטתו הבלעדית של המורשה;

(2) ייקבעו בנוהל האבטחה גם הוראות לעניין תקנת משנה (א), ובכללן בנושאים אלה:

(א) אופן הזיהוי; היה אופן הזיהוי מבוסס על סיסמאות, יתייחס הנוהל גם לחזקת הסיסמה, מספר הניסיונות השגויים, ותדירות החלפת הסיסמאות שתיעשה בהתאם לתפקיד מורשה הגישה, ובכל מקרה לתקופה שלא תעלה על שישה חודשים;

(ב) ניתוק אוטומטי לאחר פרק זמן של אי-פעילות;

(ג) אופן הטיפול בתקלות הקשורות באימות זהות.

ג. בעל מאגר מידע ידאג לביטול ההרשאות של בעל הרשאה שסיים את תפקידו ובמידת האפשר לשינוי סיסמאות למאגר ולמערכות המאגר, שבעל הרשאה עשוי היה לדעת, מיד עם סיום תפקידו של בעל הרשאה.

בעמותה לא קיים נוהל לקליטה, לעזיבה ולשינוי תפקיד של עובדים, המפרט את הפעולות הנדרשות בהקשר של הגישה למאגרי המידע. לביקורת נמסר נוהל לעזיבת עובדים בלבד, ברמת טיוטה.

להלן תהליך ניהול הרשאות לעובדים בעמותה:

- **עובד חדש** – בעת קליטת עובד חדש לעמותה, מחלקת משאבי אנוש מחתימה את העובד על חוזה עבודה, על טופס אבטחת מידע ועל הסכם סודיות. נציג מחלקת משאבי אנוש שולח הודעת דוא"ל למנהל מערכות המידע כדי לפתוח משתמש חדש ברשת העמותה ותיבת דואר אלקטרוני בהתאם לתפקיד שהוגדר לו.

- **עובד עוזב** – בעת עזיבת עובד את העמותה, מחלקת משאבי אנוש שולחת בקשה בדואר האלקטרוני למנהל מערכות המידע להסרת הרשאות המשתמש שלו מהרשת (הפיכת המשתמש ל"לא פעיל") וממערכות המידע.

הביקורת בדקה את מדיניות הסיסמאות ואת משתמשי העל ברשת ובמערכות העמותה.

מסקנות

5. אי קיום מדיניות סיסמאות ותהליך סקירת משתמשים והרשאותיהם ברשת ובמערכות העמותה, חושף את העמותה למצב שבו יהיה אפשר לגלות את סיסמאות המשתמשים באופן קל יחסית, וכן ייתכן במצב הדברים הזה כי ישנם שמות משתמשים של עובדים שעזבו אך עדיין פעילים ברשת ובמערכות העמותה. קיום משתמשי-על שאינם נדרשים לכך מתוקף תפקידם, גם ברשת וגם במערכות של העמותה, חושף את העמותה לסיכון פריצות אבטחה ואי יכולת מעקב אחר פעולות כל משתמשי-העל.

המלצות

5. ליישם מדיניות סיסמאות במערכות.
6. לחייב משתמשים חדשים לשנות לאלתר את הסיסמה הראשונית שקיבלו בכניסתם הראשונה לרשת העמותה.
7. להסיר משתמשי-על שאינם נדרשים לכך מתוקף תפקידם.
8. 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.

שמירת לוג פעולות ותיעוד אירועי אבטחת מידע

סעיפים 10 ו-11 לתקנות, מחייבים שמירה של לוג פעולות ותיעוד של אירועי אבטחת מידע.

להלן דרישות סעיף 10 לתקנות:

- א. במערכות של מאגר מידע אשר חלה עליו רמת האבטחה הבינונית או הגבוהה, ינוהל מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למערכות המאגר (בתקנה זו – מנגנון הבקרה), ובכלל זה נתונים אלה: זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה.
- ב. מנגנון הבקרה לא יאפשר, ככל יכולתו, ביטול או שינוי של הפעלתו; מנגנון הבקרה יאתר שינויים או ביטולים בהפעלתו ויפיץ התראות לאחראים.
- ג. בעל מאגר מידע יקבע נוהל בדיקה שגרתי של נתוני התיעוד של מנגנון הבקרה, ויערוך דוח של הבעיות שהתגלו וצעדים שננקטו בעקבותיהן.
- ד. נתוני התיעוד של מנגנון הבקרה יישמרו למשך 24 חודשים לפחות.
- ה. בעל מאגר מידע יידע את בעלי ההרשאות במאגר בדבר קיום מנגנון הבקרה למערכות המאגר.

להלן דרישות סעיף 11 לתקנות:

א. בעל מאגר מידע אחראי לתיעוד כל מקרה שבו התגלה אירוע המעלה חשש לפגיעה בשלמות המידע, לשימוש בו בלא הרשאה או לחריגה מהרשאה (להלן – אירועי אבטחה); ככל האפשר יבוסס התיעוד האמור על רישום אוטומטי.

ב. בנוהל האבטחה יקבע בעל מאגר מידע גם הוראות לעניין התמודדות עם אירועי אבטחת מידע, לפי חומרת האירוע ומידת רגישות המידע, לרבות לעניין ביטול הרשאות וצעדים מידיים אחרים הנדרשים וכן לעניין דיווח לבעל המאגר על אירועי אבטחה ועל פעולות שננקטו בעקבותיהם.

ג. במאגר מידע שחלה עליו רמת האבטחה הבינונית, יקיים בעל המאגר דיון אחת לשנה לפחות באירועי האבטחה ויבחן את הצורך בעדכון של נוהל האבטחה; במאגר מידע שחלה עליו רמת האבטחה הגבוהה, ייערך דיון כאמור אחת לרבעון לפחות.

קיימת חשיבות מכרעת למוכנות הארגון בעת קרות אירוע אבטחת מידע וסייבר, החל משמירת לוגי פעולות של מערכות אבטחת המידע ומערכות המידע ועד לתוכנית להתאוששות מאסון והמשכיות עסקית.

אחת השיטות המוכחות לטיפול ולשיפור בנושא אירוע אבטחת מידע וסייבר היא שמירת לוגי פעולות לצורך תחקור, וכן ביצוע תרגילי סייבר אשר כוללים את הגורמים הרלוונטיים הנדרשים בעת קרות האירוע. ביצוע תרגול אירוע סייבר אחת לשנה, תוך שימוש במערכות ובתשתיות, מחזק את החוסן של הארגון בעת קרות אירוע סייבר אמיתי.

הביקורת בדקה את הבקורות שמפעילה העמותה באיתור כשלים, פגיעויות ואירועי אבטחת מידע. להלן תוצאות הבדיקה:

- בעלי מאגרי המידע לא קבעו נוהל בדיקה שגרתי של נתוני התיעוד של מנגנון הבקרה.
- לא קיימת מערכת לסריקת פגיעות על עמדות הקצה ותשתית הרשת הארגונית.
- לוג הפעולות במערכות אבטחת המידע ובמערכות המידע אינו נשמר למשך 24 חודשים.
- אין תהליך סקירת גישה ושינויים בתוך שרתי הקבצים בספריות הרגישות לאיתור חריגות.
- בעלי מאגרי המידע לא יידעו את בעלי ההרשאות במאגר בדבר קיום מנגנון הבקרה.
- לעמותה אין נוהל התאוששות מאסון.
- בעמותה לא קיימת תוכנית להמשכיות עסקית, אשר כוללת בין השאר מיפוי של הסיכונים שלהם חשופה העמותה, ניסוח אסטרטגיית המשכיות עסקית (BCP), הגדרת התהליכים והמערכות החיוניות לעמותה בעת חירום, הדרכות ותרגול התוכנית ועוד.
- לעמותה אין נוהל התמודדות עם אירועי סייבר (שיכול להיות חלק מנוהל התאוששות מאסון ותוכנית להמשכיות עסקית), הכולל הנחיות לעובדי העמותה לצורת ההתנהלות בקרות אירוע סייבר בעמותה, לטיפול באירוע הצפנה וכו'. נוסף על כך, לא בוצעו תרגילי סייבר מתודיים לדמות התמודדות עם אירועי סייבר פוטנציאליים.
- בעלי מאגרי המידע אינם מקיימים דיון אחת לשנה לפחות באירועי אבטחה.

מסקנות

6. אי קיום מספר רב של בקורות תיעוד, ניטור וההתמודדות עם אירועי סייבר מקטין את הסיכוי של העמותה להתמודד עם אירוע סייבר, החל משלב הבנת האירוע, דרך עצירתו ועד צמצום הנזקים בעקבותיו.

המלצות

9. לגבש נוהל בדיקה שגרתי של נתוני התיעוד של מנגנון הבקרה.
10. לגבש נוהל התאוששות מאסון ונוהל התמודדות עם אירועי סייבר, הכולל הנחיות לעובדי העמותה ולעמותה איך להתנהל בקורות אירוע סייבר.
11. 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.
12. להגדיר שמירת לוג פעולות במערכות אבטחת המידע ובמערכות המידע למשך 24 חודשים.
13. 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".
14. לבצע אחת לרבעון סריקת גישה בעזרת כלי אוטומטי כדי לאמוד את רמת החרیגות הקיימות בשרתי הספריות ולבצע טיפול מונע.
15. לבצע אחת לרבעון Vulnerability scanning (סריקת פגיעויות) בעזרת כלי אוטומטי (כגון Nessus ודומיה) כדי לאמוד את רמת המפגעים הקיימים ברשת ולבצע טיפול מונע.
16. ליידע את בעלי ההרשאות במאגר בדבר קיום מנגנון הבקרה.
17. לקיים דיון אחת לשנה לפחות באירועי אבטחה, ולתעד את הדיון באמצעות פרוטוקול.

אבטחת מערכות ותקשורת

- א. נושא אבטחת מערכות המפעילות את מאגרי המידע מעוגן בכל התקנות. בהתאם לסעיף 13 לתקנות, יש להקפיד על ניהול ותפעול תקין למערכות אלו. הסעיף מציין כי:

"א. בעל מאגר מידע יקפיד על ניהול ותפעול תקין של מערכות המאגר, לפי המקובל בהפעלת מערכות כאלה.
- ב. בעל מאגר מידע יפריד, בהיקף ובמידה הסבירים האפשריים, בין מערכות המאגר אשר ניתן לגשת מהן למידע, לבין מערכות מחשוב אחרות המשמשות את בעל המאגר.

ג. בעל מאגר מידע ידאג לכך שייערכו עדכונים שוטפים של מערכות המאגר, לרבות חומר המחשב הנדרש לפעולתן; לא ייעשה שימוש במערכות שהיצרן לא תומך בהיבטי אבטחה שלהן אלא אם כן ניתן מענה אבטחתי מתאים".

סעיף 14 לתקנות מתמקד בנושא אבטחת תקשורת במצבים שבהם אותן מערכות מחוברות לרשת חיצונית. בסעיף מצוין:

"א. בעל מאגר מידע לא יחבר את מערכות המאגר לרשת האינטרנט או לרשת ציבורית אחרת, בלא התקנת אמצעי הגנה מתאימים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק או שיבוש למחשב או לחומר מחשב.

ב. העברת מידע ממאגר המידע, ברשת ציבורית או באינטרנט, תיעשה תוך שימוש בשיטות הצפנה מקובלות.

ג. במאגר מידע שניתן לגשת אליו מרחוק, באמצעות רשת האינטרנט או רשת ציבורית אחרת, ייעשה שימוש נוסף על אמצעי אבטחה כאמור בתקנות משנה (א) ו-(ב), באמצעים שמטרתם לזהות את המתקשר והמאמתים את הרשאתו לביצוע הפעילות מרחוק ואת היקפה; לעניין גישה של בעל הרשאה למאגר מידע ברמת האבטחה הבינונית והגבוהה ייעשה שימוש באמצעי פיזי הנתון לשליטתו הבלעדית של בעל ההרשאה".

הביקורת מציינת כי קיימת חשיבות רבה ליישום עדכוני אבטחת המידע, שכן גורמים עוינים רבים מכירים את הפרצות למיניהן ואת דרכי ניצולן. קיימת חשיבות מרובה למעקב ועדכון המערכות השונות.

מסקנות

7. אי עדכון מערכות שונות מגביר את הסיכון לניצול חולשות אבטחת מידע מוכרות על ידי תוקף, ובכך העמותה אינה עומדת בהוראות החוק והתקנות.

המלצות

18. להתקין דרך קבע עדכוני אבטחה שונים.

גישת מיקור חוץ למאגרי המידע

ארגונים רבים מסתמכים על מיקור חוץ לקבלת שירותים כגון תמיכה במערכות מידע, חישובי שכר ועוד. הדבר חושף את הארגון לסיכון שאותו גורם חיצוני יגיע למידע רגיש בארגון. לנוכח זאת, אבטחה שוטפת במהלך גישת מיקור חוץ לרשת הפנימית של הארגון הפכה לאחד ממנגנוני האבטחה החשובים.

סעיף 15(א) לתקנות, מחייב את בעל המאגר כדלהלן:

"(1) יבחן, לפני ביצוע ההתקשרות עם הגורם החיצוני המסוים כאמור, את סיכוני אבטחת המידע הכרוכים בהתקשרות.

(2) יקבע במפורש בהסכם עם הגורם החיצוני (בתקנה זו – ההסכם) את כל אלה, בשים לב לסיכונים לפי פסקה (1)".

במסגרת הבדיקה נמצא כי לא קיים נוהל ספקי מיקור חוץ, אולם קיים מיפוי של ספקי העמותה אשר יש להם אפשרות גישה מרחוק למאגרי המידע. חלק מהספקים מתחברים לעמותה בעזרת אפליקציות P2P (Pear to Pear).

לא נעשית בעמותה סקירה תקופתית על ידי מנהל מערכות המידע לבדיקת התחברויות הספקים באותה התקופה.

בעמותה לא בוצע סקר סיכוני אבטחת מידע בהיבטי הספקים, אשר מטרתו להעניק תמונה מלאה על התחברות הספקים לרשת ולמערכות העמותה, על הציוד שאליו הם ניגשים, על החומרים של העמותה, על אמצעי ההגנה שהספק מפעיל ועוד.

מסקנות

8. במצב שבו לא קיים תהליך סדור לעבודה עם ספקים המתחברים לרשת העמותה, וכן לא נבחנים סיכוני אבטחת המידע בהתקשרות עם אותם ספקים, לעמותה אין "תמונה מלאה" של הסיכונים הטמונים בהתחברות מרחוק של ספקים.

המלצות

19. לגבש נוהל ספקי מיקור חוץ.
20. 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.
21. לתאם סקר ספק אצל ספק שזוהה שהחיבור שלו גורם לעמותה סיכון ברמה בינונית ומעלה.

ביצוע ביקורת תקופתית

ביצוע ביקורת תקופתית נועד לשמור על רמת אבטחה גבוהה בארגון ובמאגרי המידע. סעיף 16 לתקנות מחייב ביצוע ביקורת תקופתית אחת לתקופה כדלהלן:

"א. במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, בעל המאגר אחראי לכך שתיערך, אחת ל-24 חודשים לפחות, ביקורת פנימית או חיצונית, על ידי גורם בעל הכשרה מתאימה לביקורת בנושא אבטחת מידע שאינו ממונה האבטחה של המאגר, כדי לוודא את עמידתו בהוראות תקנות אלה.

ב. בדוח הביקורת ידווח המבקר על התאמת אמצעי האבטחה לנוהל האבטחה ולתקנות אלה, וזהה ליקויים ויציע אמצעים הדרושים לתיקון המצב.

ג. בעל מאגר המידע ידון בדוחות הביקורת שיועברו לו, ויבחן את הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבותיהם.

ד. ...

ה. ארגון שהוא בעל כמה מאגרי מידע, רשאי לקיים את החובה הקבועה בתקנה זו במסגרת ביקורת אחת לעניין כל מאגרי המידע שברשותו, המצויים באותה רמת אבטחה".

ביקורת תקופתית כוללת באופן תדיר סקר סיכוני אבטחת מידע ומבחני חדירה.

סקר סיכוני אבטחת מידע הוא תהליך המאפשר הגעה לרמת הגנה סבירה על מערכות המחשוב של הארגון תוך שמירה על איזון ההוצאות התפעוליות הנובעות מיישום אמצעי הגנה על מערכות אלה. התהליך כולל: זיהוי והערכת נכסי המידע הארגוניים, זיהוי סיכוני אבטחת המידע בהם, ניתוח הסיכונים, דירוג הסיכונים ועוד, כל זאת כדי לגלות חשיפות פוטנציאליות לפגיעה של נכסי המידע הקריטיים בארגון.

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

העמותה לא ביצעה מעולם ביקורת תקופתית וכן לא ביצעה מבדקי חדירה משנת 2022.

מסקנות

9. אי ביצוע ביקורת תקופתית מקטין את יכולת העמותה לשמור על רמת אבטחה, לרבות אבטחת המידע במאגרי המידע שלה. כמו כן, העמותה מעולם לא ביצעה מבחני חדירה הכוללים תוכנית טיפול בממצאים שעולים, דבר אשר מגביר את הסיכוי לכך שהעמותה אינה יודעת מהם סיכוני הסייבר והפגיעויות הקיימות במערך אבטחת המידע והסייבר שלה, ובעטיו אין היא עומדת בהוראות החוק ותקנותיו.

המלצות

22. לבצע ביקורת תקופתית אחת ל-24 חודשים לפחות ובהתאם לדרישות התקנות.
23. לבצע מבחני חדירה אחת לתקופה כפי שתקבע העמותה.

התייחסות לנושא של "דלף מידע" ארגוני

דלף מידע הוא מצב שבו מידע מהארגון עובר לגורמים שאינם מורשים. דלף מידע יכול לקרות כתוצאה מגניבת מידע מכוונת ממניעים של ריגול עסקי, מכשל טכני, מטעויות אנוש וכדומה.

הערוצים המרכזיים שדרכם יכול לדלוף מידע ארגוני הם הדואר האלקטרוני הארגוני, הדואר האלקטרוני הפרטי, רשתות חברתיות, מדיה נתיקה, מדפסות/פקסים, מכשירים סלולריים, גלישה לאתרים המכילים קוד עיון, מנגנוני AI ועוד.

אחת המטרות העיקריות של חוק הגנת הפרטיות ותקנותיו היא למנוע דלף מידע.

בבדיקה נמצא כי לא קיימת הנחיה על אופן הוצאת מידע אל מחוץ לעמותה ולא קיימת בקרה טכנולוגית על הוצאת מידע דרך מערכות הדואר האלקטרוני והאינטרנט.

מסקנות

10. חוסר בהנחיות או בנהלים להוצאת מידע אל מחוץ לעמותה ולקיום בקורות טכנולוגיות על הוצאת המידע, חושף את העמותה לדלף מידע ארגוני ולאי עמידה בהוראות החוק ותקנותיו.

המלצות

24. למפות את גורמי הסיכון הארגוניים לדלף מידע.
25. למפות את מקומות אחסון החומר הרגיש ואת מסדי הנתונים שבהם מוחזק המידע.
26. לכתוב נוהל להוצאת מידע ממערכות העמותה.
27. להפעיל בקורות 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.
28. לבחון שימוש במנגנון Data Loss Prevention Software - DLP (מערכות למניעה של דלף מידע) במערכות הדואר האלקטרוני והאינטרנט.

תגובת המבוקרים

עמותת לביא

המלצות הביקורת מקובלות.

העמותה תבחן את הצורך ברישום מאגרי המידע בהתאם לתיקון 13 לחוק הגנת הפרטיות ותגבש מסמך מדיניות אבטחת מידע ואת נוהלי אבטחת המידע הנדרשים. כמו כן, העמותה תבצע ביקורת תקופתית כדי לוודא עמידה בהוראות החוק והתקנות.

העמותה תגדיר מדיניות סיסמאות נאותה במערכות שנבדקו בהתאם להמלצות הביקורת ותבצע סקירת משתמשים והרשאות.

העמותה תגבש מסמך המשכיות עסקית.

סיכום

זכות האדם לפרטיות היא אחת הזכויות החשובות בישראל והיא מעוגנת בחוק הגנת הפרטיות החל משנת 1981 (להלן: החוק) לרבות תקנותיו. החוק מגדיר מהי פגיעה בפרטיות, ובין השאר הוא מסדיר גם את פעילותם של מאגרי מידע הכוללים מידע פרטי ורגיש.

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. הוראות אלו נכתבו, בין היתר, בשל העלייה המתמדת בהיקף ובעוצמת תקיפות הסייבר בארץ ובעולם. בין המותקפים ניתן למנות בתי חולים, אוניברסיטאות, עיריות, חברות ביטוח, תשתיות, אתרי אינטרנט ועוד. מתקפות שמשיגות את יעדיהן עלולות לערער את היציבות הארגונית, לפגוע בנכסי הארגון, במוניטין שלו ובלקוחותיו, ולעיתים אף לסכן חיי אדם.

עמותת לביא היא יעד פוטנציאלי לניסיון תקיפות סייבר, בין היתר בשל היותה עמותה עירונית של עיריית ירושלים, עיר הבירה של מדינת ישראל ואחד מסמליה החשובים. ניסיונות חדירה ודלף של מידע, תקיפה והשחתה של אתר האינטרנט ומניעת שימוש במערכות, הם רק חלק מהסיכונים הקיימים במרחב הסייבר של העמותה.

עם התרחבות השימוש בטכנולוגיות הדיגיטליות והגברת השימוש במערכות מידע ובמאגרי מידע גובר הסיכון כי מידע ארגוני או אישי ייחשף ברבים, בזדון או בתום לב, דבר העלול לפגוע בארגון או בפרטיותם של גורמים שפרטיהם כלולים במאגרי המידע של הארגון.

כשאבטחת המידע אינה מנוהלת כראוי נוצרות במאגרי המידע פרצות רבות.

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 מידת עמידתה של העמותה בהוראות החוק והתקנות, את המדיניות והנהלים בנושא אבטחת המידע, וכן ערכה כמה בדיקות: מבדק טכנולוגי לבחינת רמת האבטחה הקיימת בעמותה, בדיקה פיזית לאבטחת המידע, ומבדקי חדירה לרשת העמותה.

הביקורת העלתה ליקויים מהותיים ביישום הוראות חוק הגנת הפרטיות ותקנותיו בנושאים האלה: מדיניות ונוהלי אבטחת המידע, הקשחות עמדות קצה ושרתים, ניהול מערכת האנטי-וירוס, ניהול מערכת חומת האש, ניהול מערכת ה-AD, וכן העלתה ליקויים בעלי חשיבות גבוהה במבדקי החדירה שביצעה.

על העמותה לטפל בהקדם בממצאים שהועלו, בדגש על עמידה בהוראות החוק ותקנותיו וטיפול בפערים הטכנולוגיים שנמצאו, לרבות במבדקי החדירה.

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 לעמותה לעמוד בחובותיה הרגולטוריות, וכפועל יוצא להפחית את הסיכונים למיניהם מעצם התרחשות האירוע.

דוח שנתי 2024

הגנת הפרטיות, אבטחת מידע וסייבר בעמותת לביא

אני מבקש להודות למבקר העירייה על עריכת דוח מפורט בנושא זה, אשר פרט לפירוט הממצאים בו, כולל סקירה מעמיקה לגבי נושא הגנת הפרטיות, אבטחת מידע וסייבר שהוא נושא חשוב ומהותי בעל השלכות על העירייה, תאגידיה ותושביה.

החשיבות הרבה של הדוח טמונה בכך שאבטחת מידע הפכה לצורך בסיסי לאור העלייה המתמדת בהיקף ובעוצמת האיומים במרחב הסייבר בעולם כולו ובישראל בפרט. תאגידים עירוניים מהווים לצערי כר פורה למתקפות סייבר, בשל היקף השימוש שלהם במערכות מידע, בשל השימוש הרב שלהם באמצעים טכנולוגיים, בשל המידע הרגיש והרב שאותו הם מחזיקים ובשל רמת המוכנות וההגנה הנמוכות יחסית בחלק מהתאגידים.

בהתאם, במהלך השנים האחרונות היינו עדים למספר מתקפות סייבר על גופים ציבוריים. העירייה בראשותי מתייחסת לאיום הסייבר ברצינות מלאה וביצעה פעולות רבות בהשקעת משאבים לא מבוטלת, בכדי לוודא כי היא תהיה במוכנות מספקת למתקפה. כמובן שגם התאגידים העירוניים, המהווים את הזרוע הארוכה של עיריית ירושלים ופועלים בשם העירייה, נדרשים לפעול בסטנדרטים דומים ולא פחותים מאלה של העירייה. הדברים חשובים ביתר שאת בגוף דוגמת עמותת לביא, שכן עמותת לביא הוא התאגיד העירוני הגדול בישראל מבחינת מספר העובדים והיא מחזיקה במידע רגיש ביותר מתוקף עיסוקה בתחום החינוך.

הביקורת מצאה מספר ליקויים בהתנהלות עמותת לביא בעניין זה. בין היתר, נמצא כי לעמותה אין כלל מסמכים של הגדרות מאגרי מידע ושל מבנה מאגרי המידע בהתאם לדרישות בתקנות. כמו כן, נמצא כי לעמותה אין מדיניות אבטחת מידע מפורטת וכי היא אינה מקיימת הדרכות בנושא אבטחת מידע באופן סדיר לעובדיה. בנוסף, נמצא כי קיימים ליקויים משמעותיים במדיניות הסיסמאות של מערכות העמותה וכי בעלי מאגרי המידע לא קבעו נוהל בדיקה שגרתי של נתוני התיעוד של מנגנון הבקרה. עוד עולה כי לעמותה אין נוהל התאוששות מאסון ואין תוכנית להמשכיות עסקית, היא לא ביצעה ביקורת תקופתית כדי לוודא שהיא עומדת בהוראות החוק והתקנות ולא ביצעה מבדקי חדירה משנת 2022. כמו כן, נמצאו ליקויים בעלי חשיבות בניהול ותחזוקת מערכת האנטי וירוס, מערכת עדכוני אבטחת המידע ומערכת ה-AD (מערכת לניהול משתמשים) של העמותה.

מעיון בדוח מבקר העירייה בנושא זה, עולה כי הגורמים המקצועיים בעמותת לביא הסכימו עם כלל המלצות הביקורת ומסרו, בין היתר, כי העמותה תפעל לרישום מאגרי המידע ותגבש מסמכי מדיניות ונוהלי אבטחת מידע כנדרש. כמו כן, העמותה התחייבה לבצע ביקורת תקופתית כדי לוודא עמידה בהוראות החוק והתקנות. תגובת עמותת לביא מעידה על רצון אמיתי לשיפור וטיוב התנהלות העמותה בנושא זה לטובת הציבור.

עיריית ירושלים בראשותי תמשיך להשקיע ולקדם את נושא אבטחת המידע, בוודאי לאור המצב הבטחוני ולאור הגידול במספר אירועי הסייבר והתגברות הסיכון הנשקף לתאגידים העירוניים והכול, בכדי להיות מוכנים למתקפה הבאה ולהגן על העמותה ועל תושבי העיר באופן מיטבי.

אני מנחה את מנכ"ל העירייה ומנכ"ל העמותה לבצע מעקב על יישום המלצות הביקורת על ידי הגורמים המקצועיים הרלוונטיים.



הוועדה לביקורת – תמליל

מספר הוועדה : 23

מקום ההתכנסות : אולם חדר ישיבות קומה 0

תאריך הוועדה : ו' בתמוז תשפ"ה (2.7.2025)

מזכיר הוועדה בדיון : צבי אבו

שעת תחילת הוועדה : 15:40

שעות סיום הוועדה : 16:18

התמליל נכתב ע"י חברת גולד וורק ולא עבר בדיקה או הגהה ע"י גורם כל שהוא בעיריית ירושלים
עיריית ירושלים וחברת גולד וורק 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 ת M ג R ים גולד וורק תמלול והקלטה

יו"ר אלדד רבינוביץ:

אני מתכבד לפתוח את הדיון בוועדת ביקורת מספר 23, הגנת הפרטיות, אבטחת מידע וסייבר בחברת לביא,

עו"ד דני ליבמן:

עמותת לביא.

אלדד רבינוביץ:

עמותת לביא. נכון. אנחנו היום בסשן שלם של ביקורת על תחומי הסייבר, הגנת הפרטיות בחברות העירוניות, ביקורת שעד עכשיו מצאנו אותה כמאוד משמעותית, מאוד חשובה. עלינו על הרבה מאוד נקודות משמעותיות לשימור ולשיפור. תחום הסייבר, תחום הגנת הפרטיות הוא תחום מאוד משמעותי ומדובר בכל השנים האחרונות, בשנתיים האחרונות, במיוחד בחודשים האחרונים, הוא עלה עוד מדרגה, בגלל שיש הרבה שחקנים עולמיים ואזוריים בעלי יכולות משמעותיות בתחום, ואנחנו חייבים להיות ערוכים ומוכנים כנגדם. אז מי שיציג את הדברים זה שלומי. אני בסוף לא, לא בקיא בתחום ובפרטים, אבל אנחנו כבר קצת למדנו וקצת קצת שומעים. אז אני מברך על עריכת הביקורת ומברך אתכם על המענה ונשמע את הדברים.

עפרה ברכה:

למעשה, היום אתם החברה הרביעית, זה הדיון הרביעי. היום אנחנו פשוט במנהל הביקורת. חשבנו שנכון לבדוק את זה בכל התאגידים העיקריים. אתם עמותה, ואצלכם באמת נושא של אבטחת מידע וכל הסיפור גם של המאגרים, כל הצהרונים וכולה, וכולה, וכל מיני הסיבות שנוספו לכם גם בשנים האחרונות, אני חושבת שיש לזה חשיבות מאוד גדולה. שלומי נשמע ממנו באמת את הממצאים וההמלצות העיקריות וזה ההתייחסות.

אלדד רבינוביץ:

טוב, אני שמח שההתייחסות תהיה בעצם ממצא התייחסות, ממצא התייחסות, נוכל ככה לראות,

דובר לא מזוהה:

בבקשה.

שלומי בני:

אז נעים מאוד, שלומי בני, אנחנו מכירים מהביקורת.

עפרה ברכה:

כן, אנחנו, סליחה, אני רק לא אמרתי שאנחנו התחלנו את הביקורת הזו. כמובן שהיה מנכ"ל הקודם ארנון,

שלומי בני:

כן,

ברק לוי:

כן,

עפרה ברכה:

וברק ככה נכנס לזה וגם דיבר איתנו בימים האחרונים כדי לשמוע איך לדעת איך לבוא ואיך להיערך לנושא, ואנחנו כאן לכל דבר נסייע.

שלומי בני:

אז אני נעים מאוד. שלומי בני, שותף במשרד RSM שיף, אני בעצם ערכתי את הביקורת יחד עם הצוות מטעמי מול, תזכיר לי את השם,

צחי קינן:

צחי,

שלומי בני:

צחי, צחי והצוות. אז נעבור על עיקרי, עיקרי הממצאים. יש פה 10, 12 ממצאים עיקריים. יש לכם את הדוח המלא בפניכם. בקצרה עמותת לביא, עמותה עירונית לפיתוח החינוך בעיריית ירושלים. חינוך משלים, ליווי של הסעים, ליווי בתי ספר בניהול עצמי. וכמו שעפרה ציינה, יש פה נתונים שהם נתונים מן הסתם רגישים נתונים של ילדים, נתונים של הורים, ולכן הנושא של שמירת המידע, אבטחת המידע.

אלדד רבינוביץ:

ותעסוקה.

שלומי בני:

כן גם, צרכים מיוחדים יש פה. יש פה רגישות מידע. המידע פה רגיש, זה לא מידע רגיל ולכן יש פה עוד יותר, צריך לשים דגש בנושא של אבטחת מידע ושימור על, על המידע. אז מטרת הבדיקה הייתה בעצם שני דברים עיקריים, אחד, לבדוק את ה – עמידה את העמותה בהוראות החוק, ברישום מאגרי מידע ותקנות הגנת הפרטיות. זה החלק הראשון. והחלק השני, זה בעצם בדיקה טכנולוגית, כולל מבדקי חדירה, על מנת לבדוק את החוסן ואת רמת האבטחה של העמותה במקרה שמישהו ירצה לפרוץ אליה. אז הממצא הראשון זה נמצא של רישום מאגרי מידע. אז בעצם לא היו בכלל מסמכים, אין רישום של מאגרי מידע ופה זה קצת מקבל אפילו טיפה משנה תוקף, כי באמת כמו

שאמרתי יש פה מידע רגיש ו - , זה עוד יותר, עוד יותר חשוב מאשר לרשום ספק. אוקי, זה קצת יותר, זה יותר חשוב. ובאמת זה משהו שהערנו עליו וחושבים שזה מעבר לזה שזו עבירה על החוק. זה גם למעשה. בעייתי, כי אתה לא יודע איך לנהל את המאגר שלך, מה ההגדרות, מה המבנה שלו, איך אתה מתקף אותו וכולה. אז כאילו אנחנו ממצא,

ברק לוי:

ממצא התייחסות, אז רגע, אולי רק אני אגיד כמה מילים כלליות, ואז צחי יתייחס פרטנית להמלצות. רוצה לומר, קודם כל אני מאוד שמח על הדו"ח הזה, כי אני חושב שהוא הציף פערים, התחיל עוד כמובן בתחילת המנכ"ל הקודם, אני חודשיים בתפקיד שלי הנוכחי, אבל אני חושב שהוא עדיין בלי קשר למי המנכ"ל, זה דו"ח חשוב כי הוא הציף פערים, זה נושא שבעיניי הוא באמת אחד הדברים החשובים שמירה על אבטחת מידע וסייבר. עשינו ויש תוכנית מסודרת, איך צריך להתייחס לכל נושא, יש תוכנית לתיקון של כל הליקויים בדו"ח, אתה אומר 10, 12, אצלנו יש את הדו"ח המפורט, יש בו הרבה יותר אבל יש לנו על כל נושא ונושא שם התייחסות. חלק מהדברים, הדברים הדחופים כבר טופלו. צחי כבר טיפל והסדיר, חלקם עוד בשלבים, יש לנו ממש תוכנית מסודרת. מה עושים, מתי. בחודש אוגוסט אנחנו אמורים לעבור ממש חודש, אבל כבר ל - 3.6.5 זה גם אמור לתקן חלק משמעותי מתוך הליקויים ב - ,

אלדד רבינוביץ:

סליחה, מה זה 365?

ברק לוי:

של האבטחת מידע, זה מ - Changed Exchange

צחי קינן:

במקום ה - Exchange במיילים,

שלומי בני:

מיילים מתקדמים יותר שיושבים אצל מייקרוסופט,

ברק לוי:

מייקרוסופט.

שלומי בני:

לא אצלו.

ברק לוי:

כמו שהמעבר שהעירייה עשתה אז אנחנו אמורים לעשות אותו חודש הבא וזה אמור חלק גדול מהדברים לתקן וגם את השאר. מה שעדיין נשאר אנחנו אמורים להסדיר בחודשים הקרובים. יש לנו להערכתי עד הראשון לנובמבר כבר כל הפערים אמורים להיות מושלמים, לפי התוכנית שלנו. היינו גומרים את זה עוד קודם, אבל פתאום המלחמה וכל זה, אז הדברים ככה קצת, עוד התעכבו. בכל מקרה, תכף צחי יתייחס פרטני. ככלל הדוח הזה חשוב לנו מאוד, ההמלצות בו הם כולם ייושמו, חלקם כבר יושמו ומה שלא יטופל בתקופה הקרובה.

צחי קינן:

אני אתחיל ב - , קודם כל באמת תודה רבה על הביקורת, עשו את הביקורת תוך כדי שאני במילואים, אני סיימתי בראשון למאי 540 יום במילואים, אז רצתי עם שלומי ו - , אז אני ובימים אלו אני עדיין, חזרנו אחרי זה לעוד סבב עכשיו, אבל הכול בסדר.

ברק לוי:

צחי קצין בחיל האוויר, ויש לו הרבה, הרבה עבודה מאז ה 7 באוקטובר.

צחי קינן:

אז היינו, אז הייתי בתקופה הזאת גם תוך כדי וניסיתי לתת מענה מצוין. כמה ש - , כמה שאפשר. ביקורת מבורכת,

ברק לוי:

נתת מענה.

צחי קינן:

והביקורת מבורכת. היא מאוד מאוד מאוד. אצלנו, מאגרי מידע יושבים אצל, יושבים חיצוניים כאילו לעמותה על התאגיד, אם זה מלמ, אם זה מגער, כאילו לנו ישירות הם יושבים אצלם. עשו לי ביקור, אני ארבע שנים בתאגיד, לא היה לנו ביקורת אף פעם של אבטחת מידע, שנדרש על פי חוק כל שנתיים לעשות ביקורת זה, אז עשו לנו רק מבקר פעם אחת פנימי שלנו, ללא איזה ממצאים חריגים. ואני בנובמבר, לפני הביקורת, בפברואר, הייתה ביקורת. בנובמבר הבאנו סקר חיצוני של חברת Matrix, מטריקס נכנסה אלינו לפני שנה לתאגיד, אחרי שסיימנו את ההתקשרות עם עובד שלנו שהיה אחראי על המערכות מידע ונכנסה, ואחרי שנה הזמנתי חברה שתעשה בדיוק סקר סיכונים, ותהליך לזיהוי הפערים וזה. ואז, אחרי שלושה חודשים בדיוק קיבלנו את הדו"ח, הצגתי אותו גם להם עם הפערים ולהתחיל טיפול. אז שאנחנו ראינו שאנחנו צריכים שמאגרים שלא יושבים אצלי זה גם באחריות שלי שהיא חיצונית, ואנחנו נדרשים לבצע את זה. ישר התחלתי למלא את הטפסים ולשלוח לבקשות, ויש את התוספת 13 שנכנסת עכשיו ב - 15 לאוגוסט, שזה חלק נוסף ש - , כנראה ישנו את המדיניות, אבל אנחנו ממשיכים להפעיל את זה במטרה לטפל בזה במקביל, וזה חלק מאוד עיקרי מהממצאים, שזה חשוב לנו מאוד גם לעמוד בחוקים וגם לטפל בזה. כבר סיימתי, קיבלתי

מהחברות החיצוניות את הטפסים הנדרשים, אנשי קשר, אנחנו הולכים לרשום זה. בנוסף, אנחנו מתקשרים יועץ סייבר חיצוני, כדי שיעזור לנו בתהליך הזה, כדי לסגור את כל הפערים. בסוף אני הממונה, אבל אני לא איש מקצוע, בסוף צריך שנייה איזה מישהו שייתן פה את ה - Benefit שלנו. מתקשרים עם בן אדם חיצוני שיעזור לנו ובנינו תוכנית עבודה מפורטת, ואם נמשיך אני אגיד לכם, דברים שטיפלנו במידי, כאילו זה.

אלדד רבינוביץ:

עשיתם מיפוי של כל המאגרים שאצלכם?

צחי קינן:

כמובן, כמובן, בטח, בטח.

אלדד רבינוביץ:

יש לכם באיזה תוכנית עבודה אתה אומר לרישום של,

צחי קינן:

מסודרת, גם את הטפסים, אפילו שתוך כדי ביקורת ישר זיהינו, התחלנו לטפל ואת המאגרים מידע ולרשום מסודר,

אלדד רבינוביץ:

סליחה,

צחי קינן:

ועלינו תוכנית.

אלדד רבינוביץ:

(לא ברור) זמן של לוח זמנים. מתי בעצם זה יהיה רשום?

צחי קינן:

להערכת אנחנו מתכוונים עד, אחרי החגים לסיים את כל האירוע הזה.

אלדד רבינוביץ:

אתה יכול לשלוח מייל למבקרת עם העתק אלי, שרשמתם ואתם סגורים?

צחי קינן:

כמובן, אני גם, רוצה את כל הדו"ח, אנחנו נסדיר את כל השורות, טיפול, אתם תקבלו בסוף ממצא מדויק עם ממש חוברת מה בוצע הכול.

אלדד רבינוביץ:

מצוין.

שלומי בני:

אוקי. מדיניות אבטחת מידע, אני מניח שאם אתם מטפלים ברישום המאגרים. צחי, אז אתם גם כן תכתבו מדיניות אבטחת מידע,

צחי קינן:

לחלוטין.

שלומי בני:

אוקי. הדרכות מודעות לעובדים, כולל תרגילי פישנוג.

צחי קינן:

יש לי על זה מה להגיד שנייה.

שלומי בני:

אז תגיד,

צחי קינן:

אנחנו מקפידים, הצגתי את זה גם לביקורת. כל שנה לעשות הדרכה לכלל העובדים, הדרכה פרונטאלית ולעשות פישנוג חיצוני. אני לוקח חברה, השנה עשו לנו את זה מטריקס ולפני שנתיים עשו לנו את זה, חברה אחרי זה אחרת, סופטיקס. אנחנו שולחים מייל פישנוג לכל העובדים, בסוף אני מקבל דו"ח. בדו"ח רשום ברמה זה רמת רמזור, מי פתח, מי הכניס נתונים, מי זה, מי זה, וזה ממש דו"ח מפורט, ואחרי זה אנחנו עושים הדרכה פרונטאלית, בארבעה שבבים, כי אנחנו, מספיק אנשים שהם צריכים להיכנס, בארבעה שבבים באותו יום עם מדריך חיצוני. גם הצגתי את זה, אנחנו בזה אנחנו מאוד מקפידים.

שלומי בני:

אז רגע, אז זה ממצא שהוא לא נכון?

צחי קינן:

לא, זה לא שלא נכון, פשוט הראיתי לו ולא יודע למה, כאילו הראיתי, הצגתי את זה, גם תאריך. היה חסר השלמה וביצענו אותו לפני איזה חודשיים.

שלומי בני:

אוקי,

ברק לוי:

אז זה טופל בעצם,

צחי קינן:

זה לחלוטין, אני גם,

שלומי בני:

טוב, כי פה רשמנו שזה רק בקליטת העובד, אני רואה,

צחי קינן:

לא, אז יש, אז גם הוא, הצגתי לו יש לנו מצגת לקליטת העובד, הצגתי את זה, כל עובד שנכנס הוא חותם גם על טפסים, גם עובר מצגת, ויש פישניג הדרכה לכל התאגיד.

ברק לוי:

יש גם כל שנה גם לעובדים קיימים,

צחי קינן:

כל שנה,

ברק לוי:

לא רק החדשים,

צחי קינן:

לכל, לכולם.

שלומי בני:

אוקי, בסדר.

עו"ד דני ליבמן:

התרגולים האלה, באיזה תדירות?

צחי קינן:

אחת לשנה אני עושה.

שלומי בני:

תרגול אחת לשנה?

צחי קינן:

לא, לפישינג,

עו"ד דני ליבמן:

לעובדים פישינג,

צחי קינן:

כן, כן,

עו"ד דני ליבמן:

אני כל חמישה, שישה ימים, מקבל תרגול פישינג כמו מהעירייה, ואני מאוד שמח, כי אני בדרך כלל מצליח ואני מקבל מה זה, (לא ברור) זה עושה לי את היום, נהדר ענית.

אלדד רבינוביץ:

כשאתה לא פותח, הוא לא עונה לך כלום.

עו"ד דני ליבמן:

מה?

אלדד רבינוביץ:

אם אתה לא פותח, אז הוא לא אומר לך כלום.

שלומי בני:

איזה ציונים?

עו"ד דני ליבמן:

לא, אני לא, אני מקבל (לא ברור), אני שולח חזרה. זה הודעת פישינג. אומר לי - נכון, זיהית.

צחי קינן:

השתתפת בסקר.

ברק לוי:

אבל נראה לי שזה אצלך, כי הם לא מקבלים.

עו"ד דני ליבמן:

או שהם לא מגיבים לזה.

צחי קינן:

אני רק אוסיף שה - , איתך כמי עם הפישינג, כי אני אגיד לכם פה למשל ב – 3.5 רשום לכם, "הגיע מייל מחוץ לארגון", ב – Exchange אין לנו את ההערה הזאת, זה משהו שגם שיוסיף לתהליך,

עפרה ברכה:

כן.

צחי קינן:

אבל אנחנו פה בפישינג, מה אני עושה? אני עושה טמפלט של מנהלת אגף משאבי אנוש ששולחת לכולם למלות סקר למתנה לראש השנה, ואני עושה את זה לפני ראש השנה כאילו אנחנו ממש, עכשיו, אנחנו רוצים,

צבי אבו:

מנסים לדוג.

צחי קינן:

אנחנו מנסים לדוג אותם ברמה של, אחרי זה בהדרכה הם מבינים איפה הייתם צריכים לעלות על זה, כאילו תסתכלו על הכותבת, בסוף רשום להביא אבל נקודה פי.אם, כאילו משהו לא,

צבי אבו:

אתה יודע איפה אני נפלתי? שלחו לו, בתור חבר מועצה, פתיחה לחשבון זום שיהיה איזה תשמע סך הכול הגיוני, בקיצור 40 דקות, כל הזמן 40 דקות אתה מרענן,

צחי קינן:

כן, כן,

צבי אבו:

תשמע, נשמע הגיוני, סך הכול עיריית ירושלים, ונגיד לזה.

צחי קינן:

זה פשינג מתחכם, אנחנו משתדלים לעשות,

עפרה ברכה:

אני בהתחלה כשהתחלתי לעבוד בעירייה, הייתי פותחת את זה, לא היה לי סבלנות, רוצה לראות מה רוצים ממני, אבל זהו, למדתי.

שלומי בני:

האמת היא שיש, יש הרבה, הרבה רעיונות, אני גם עושה תלוש שכר. תלוש השכר של החבר שלו.

צחי קינן:

כן,

שלומי בני:

אז כולם רוצים לראות מה, אז עשיתי שבוע שעבר,

עפרה ברכה:

יש לך (לא ברור).

שלומי בני:

הם עוד לא יודעים שזה פשינג, הם עוד לא יודעים,

צחי קינן:

השנה,

עפרה ברכה:

זה רעיון יפה.

צחי קינן:

הדרכה אחרונה שעשינו,

שלומי בני:

אני אתן לך את זה.

צחי קינן:

הדרכה האחרונה שעשינו היה לנו אירוע במג"ק – וואן, מג"ק וואן זה נקרא שם,

שלומי בני:

(לא ברור).

צחי קינן:

במג"ק משהו היה שם.

ברק לוי:

מג"ק – קאס.

צחי קינן:

מג"ק – קאס של העמותה, היה לנו אירוע,

ברק לוי:

במישור אדומים,

צחי קינן:

במישור אדומים, מג"ק – קאס.

שלומי בני:

זה הלונה – פארק.

עפרה ברכה:

הלונה – פארק.

צחי קינן:

הלונה – פארק.

שלומי בני:

כן,

עפרה ברכה:

כן,

צחי קינן:

ואז שלחתי להם הודעה - שלום, אני הצלם שצילם את האירוע בתאריך הזה להיכנס לתמונה שלך, לבחור אנא כנס,

שלומי בני:

כן, כן, גם אני.

צחי קינן:

ואז אין נתונים, נכנסנו לראות את התמונה.

אלדד רבינוביץ:

אני רוצה רגע להתחבר לדיון שהיה כאן בשנה שעברה לגבי הסעות, הסעות ילדים בחינוך המיוחד, ששם בעצם יש היבט מאוד מיוחד של הגנת פרטיות ואבטחת מידע. בסוף אותו, אותו אדם שהוא מלווה הסעה חשוף להרבה פעמים להרבה מידע רפואי של ילדים, מי הילדים ומה המצב שלהם וכולה וכולה. ושמה אני חושב שצריך קצת לתגבר את המודעות. אני מבין שעושים להם הדרכות, אבל לפעמים זה כאילו אני סתם דיברתי אצלנו עם אנשים, לפעמים יש איזושהי תחושה של שמים לב כזה, .

ברק לוי:

שמה? שמה? מה אתה חושב שצריך לעשות יותר?

אלדד רבינוביץ:

שכאילו נותנים להם איזה שהוא הצהרה והם - כן, כן, כן. זאת אומרת לא יודע, אולי לעשות להם את המבחן,

צחי קינן:

לחדד?

אלדד רבינוביץ:

אולי לעשות להם איזשהו שאלון, אולי לעשות להם איזשהו מבחן, הם צריכים להבין בסופו של דבר שאותו ילד שהם מלווים אותו יש לו אירוע פרטיות משמעותי.

ברק לוי:

שמירה סודיות למלווים, אתה מדבר?

אלדד רבינוביץ:

כן, כן.

צחי קינן:

כן,

ברק לוי:

טוב, מאה אחוז, נרשום את זה.

צחי קינן:

למרות שאת הנתונים הוא מקבל פרונטאלית, הוא לא מקבל את זה בדף או במשהו.

אלדד רבינוביץ:

לכן, כל המבדקים שלך הם לא חלים עליו, הוא לא, הוא לא מתקשר איתך במייל, לא עובר,

צחי קינן:

בדיוק, לא עוזר להם.

ברק לוי:

בסדר גמור.

אלדד רבינוביץ:

זה אוכלוסייה גדולה, לפעמים זה גם לא אוכלוסייה, לא אנשים משכילים וכולה, וכולה.

עפרה ברכה:

אבל אין להם מכשירים,

אלדד רבינוביץ:

צריך להתאים אליהם.

ברק לוי:

כן,

אלדד רבינוביץ:

צריך להתאים להם את התובנה הזאת.

ברק לוי:

אנחנו נחدد להם את זה בהדרכות, אנחנו עושים איתם לפני כל תחילת שנה סטים כאלה של הדרכות. על מה, כאילו ל - ,

אלדד רבינוביץ:

אז הדרכות אני חושב שכן לומדים את זה,

ברק לוי:

אז נדבר גם למה לעשות,

אלדד רבינוביץ:

אולי משהו יותר,

עפרה ברכה:

צריך לרענן מידי פעם.

אלדד רבינוביץ:

כן, רענונים, או איזשהו מבחנים כאלה צריכים לעשות וכולה.

שלומי בני:

כן.

עפרה ברכה:

בדיקות פתע.

ברק לוי:

אוקי.

שלומי בני:

יופי. מדיניות סיסמאות במערכות של העמותה, מראה שזה היה תקין.

צחי קינן:

טופל במידי.

שלומי בני:

אוקי, סקירת משתמשים, קיים מספר גבוה של משתמשי על במערכות. אני רק אסביר למי שפחות מכיר, בעצם לכל מערכת יש משתמש על, משתמש חזק, אני מצפה שיהיה אחד, שניים שלושה לכל היותר, אצלכם מצאנו יותר,

צחי קינן:

נכון, גם הגבתי ב - , במבדק שאנחנו שייכים למטריקס. מטריקס יש לי עוד, יש לי אנשים חיצוניים ששולטים לי על המערכת מבחוץ והיה לנו באמת מספר גבוה, הורדתי את המספר קיבלתי את ההערה, עדיין זה כנראה יהיה חריג למישהו שרגיל, נגיד אחד, שתיים סיסו וזה,

שלומי בני:

אז זה יהיה ארבע,

צחי קינן:

אז אנחנו עומדים על 6, כרגע,

שלומי בני:

אוקי,

צחי קינן:

שזה נראה לי שעדיין זה צודק.

שלומי בני:

אוקי, בסדר. מנגנוני בקרה ולוגים, בעצם ההמלצה, קודם כל זה גם המלצה טכנולוגית, אבל זה גם הוראות החוק. צריכים לשמור על לוגים במערכות אבטחת המידע ל - 24 חודשים אחורה.

צחי קינן:

נכון,

שלומי בני:

יש? בוצע?

צחי קינן:

עוד לא, אנחנו כרגע בתהליך הזה לכתוב מערכת חדשה, לטפל בה, זה חלק מהעבודה של היועץ שמגיע איתנו.

אלדד רבינוביץ:

באיזה שלב אתם במערכת הזאת?

צחי קינן:

כרגע יש לנו את המערכת, הבאנו הצעות מחיר לקבל.

אלדד רבינוביץ:

אפיינתם צורך?

צחי קינן:

כן, כן, זה גם,

אלדד רבינוביץ:

הצעות מחיר?

צחי קינן:

עוד לא קיבל, עכשיו אנחנו אספנו הצעות מחיר, נחליט על איזה מערכת ללכת ואנחנו נתחבר אליה.

ברק לוי:

אנחנו השאיפה שלנו, עד חודש נובמבר לסיים עם כל התיקון, של כל הליקויים שבדו"ח הזה, כולם. לא, לא, לאו דווקא ספציפית פרטנית, יש תוכנית עבודה טיפול בכל הליקויים של הדו"ח אחד אחד ואת כולם אנחנו לפי התוכנית עד נובמבר נסיים.

אלדד רבינוביץ:

זה ריאלי עד נובמבר?

שלומי בני:

זה שאפתי, אבל אם לא יהיו מלחמות.

אלדד רבינוביץ:

אצל הקודמים, שדווקא זה להטמיע מערכת חדשה, זה אירוע מורכב קצת יותר.

שלומי בני:

אני חושב שעד נובמבר זה אפשרי, אני חושב שכן.

ברק לוי:

חלק כבר עשינו.

צחי קינן:

בסוף ההטמעה של המערכת זה בסוף, זה חלק מתוכנות, חלק ממערכות בסיסיות שאנחנו מנהלים אותם זה לא להטמיע לאנשים.

שלומי בני:

זה גם לא החלפה של, נגיד של דאטה בייס כמו שדיברנו.

צחי קינן:

כן,

שלומי בני:

שאפתני, אבל זה אפשרי.

אלדד רבינוביץ:

אז יהיה חלק מהדוח שתשלח,

צחי קינן:

מצד שני, אני גם, סליחה שאני מתפרץ כל פעם. סליחה, אבל,

אלדד רבינוביץ:

זה הדיון.

צחי קינן:

יש לנו אנחנו, אנחנו בעמותה, אנחנו השרתים שלי יושבים אצלי, אנחנו די שמרנים באירוע הזה. השרתים אצלי יושבים ב - , פיזית, כאילו אני לא משתמש בענן, אני לא משתמש ב - ואנחנו די בערוך, מאגר סגור אני אקרא לזה, אבל עדיין חשוב כמובן לעמוד בהגדרות.

אלדד רבינוביץ:

אז אתה בעצם תשלח כחלק מהדיווח גם שזה סודר,

צחי קינן:

כמובן.

אלדד רבינוביץ:

מצוין.

ברק לוי:

אנחנו נוציא לכם בעזרת השם, אני מקווה שזה נובמבר, נגלוש, אם נגלוש דצמבר, בכל מקרה, לפני סוף שנה נסגור את כל הליקויים ונעביר התייחסות לזה שכל ה - ,

צחי קינן:

יש לי 88.

ברק לוי:

הדו"ח תוקנו, 88 סעיפים,

צחי קינן:

,88

ברק לוי:

שלכל אחד, יש,

צחי קינן:

ממש תוכנית טיפול.

ברק לוי:

תראה איזה אקסל כזה, מיפוי של כל הסעיפים, כל אחד, מה סטאטוס באחריות, מי, מה, לו"ז, מה זה,

צחי קינן:

אני לא (לא ברור) להגיד,

ברק לוי:

יש פה תוכנית ל - ,

אלדד רבינוביץ:

לא, הוא,

ברק לוי:

הוא הכין את זה, לא אני, הוא הכין.

אלדד רבינוביץ:

יפה מאוד.

צחי קינן:

הוא הכין.

שלומי בני:

למעשה מה שאנחנו מציגים פה זה דברים, ליקטנו.

עפרה ברכה:

ברור

אלדד רבינוביץ:

זה היילייטס,

צחי קינן:

כן, כן,

שלומי בני:

טוב, תוכנית המשכיות עסקית והתאוששות מאסון, אני חושב שצריך לתת לזה קצת יותר, יותר בעל משמעות. עם כל ההיסעים וכל הזה. זה לא, איך אומרים? זה לא. אהלן. אהלן. נכון?

צחי קינן:

כן, אני אכווין, שנייה.

שלומי בני:

כן.

צחי קינן:

האירוע הזה הוא מאוד מאוד צודק ל - , אני אקרא לזה חברויות עסקיות, חברות, לא יודע שהדאטה – בייס שלהם הוא מאוד מאוד חשוב. אני יודע לשרוד מחר, לצאת לעבודה. ממקום הזה שאנחנו גם מחולקים. למשל היום ליווי הסעים, הכול יושב במגער.

שלומי בני :

לא, אני לא מדבר על מערכות המידע,

צחי קינן :

אתה,

שלומי בני :

אני מדבר בכלל על תוכנית להמשכיות עסקית.

צחי קינן :

של התאוששות אחרי אירוע.

שלומי בני :

לא, לא, לא. עזוב את ההתאוששות באסון

צחי קינן :

אוקי,

שלומי בני :

אני מדבר על המשכיות עסקית.

ברק לוי :

מה? מה אתה מתכוון? תסביר.

שלומי בני :

יש עכשיו, יש שביתה, או שיש מלחמה ועדיין החליטו את הילדים בעלי צרכים מיוחדים עדיין להסיע אותם. זאת אומרת אני מדבר ברמה העסקית, אני לא מדבר על מערכות המידע.

עפרה ברכה :

אז מה? איך להיערך כאילו?

צחי קינן :

תסביר לי, מה זה אומר.

שלומי בני :

איך להיערך, איך להיערך לתרחישים,

צחי קינן:

אז זה לא התאוששות,

שלומי בני:

זה התאוששות עסקית,

ברק לוי:

מה זה אומר?

שלומי בני:

אני רוצה,

צחי קינן:

המשכיות עסקית,

שלומי בני:

כן, במקרה שלכם זה יותר, יותר,

עו"ד דני ליבמן:

בוא נגיד בעירייה קוראים לזה רציפות תפקודית,

עפרה ברכה:

רציפות.

שלומי בני:

רציפות תפקודית.

עו"ד דני ליבמן:

הביקורת, נכון,

צחי קינן:

נכון, נכון,

עו"ד דני ליבמן:

ויש נוהל, נוהל ISO, שביקשנו שנפסיק אותו.

שלומי בני:

נכון, אולי המילה עסקית היא פחות, היא פחות טובה.

עפרה ברכה:

זה גם מתחבר אולי להתאוששויות.

צחי קינן:

רציפות תפקודית אני מאוד מתחבר.

שלומי בני:

רציפות תפקודית (לא ברור), פעילות העסקית.

עפרה ברכה:

זה כן, הוא כן צודק, אני חושבת, אם אתה זוכר גם את הדו"ח שזה, איך אתה מתפקד? איך אתה ממשיך את הרציפות של התפקוד, כשאתה מתאושש מאסון? ממשבר? מה שזה לא יהיה

שלומי בני:

כן.

ברק לוי:

למה זה? אבל מה הרלוונטיות פה? אבל למחשוב וסייבר דווקא?

שלומי בני:

אז אני אגיד, קודם כל הכי רלוונטי זה ההתאוששות מאסון, בצד של מערכות מידע.

ברק לוי:

אוקי.

שלומי בני:

כשאנחנו בודקים התאוששות מאסון אנחנו גם בודקים המשכיות תפקודית, נקרא לזה.

ברק לוי:

אוקי,

שלומי בני :

נעזוב את המילה העסקית, היא לא רלוונטית,

עפרה ברכה :

נכון, תפקודית.

ברק לוי :

כן,

שלומי בני :

משכיות תפקודית, אז אנחנו לא בודקים .. 19:50 אנחנו בודקים את שניהם. מסכים איתך שאפשר לעשות דוח שלם על המשכיות תפקודית בעמותת לביא,

צחי קינן :

נכון.

שלומי בני :

אבל סימנו וי, האם יש או אין, אין לכן

צחי קינן :

אין, צודק.

שלומי בני :

זהו, אירוע ענק,

ברק לוי :

לא, למה זה מעניין אותי? כי אני עכשיו ביקשתי לא עכשיו, לפני כמה ימים, אחרי,

עפרה ברכה :

מלחמה,

ברק לוי :

אחרי המלחמה שהייתה עם איראן, ביקשתי מסמכ"לית משאבי אנוש שלי שתתחיל לקדם לי, נוהל, כי תוך כדי המלחמה היינו צריכים לתפקד,

צחי קינן :

זה בעולם הרציפות התפקודית.

שלומי בני :

רציפות תפקודית.

עפרה ברכה :

גישה למערכות החינוך המיוחדות לא פעלו, נכון?

ברק לוי :

לא, מערכת החינוך לא פעלה, אבל,

עפרה ברכה :

כן, למה אני אומרת לו,

עפרה ברכה :

היו דברים, לדוגמה להעביר את מי שצריך לעבוד לעבודה מהבית, להעביר אותו לעבודה מהבית, דברים שכן התחלנו להעביר כל מיני תכנים, בגלל שכל מערכת החינוך לא פעלה היינו צריכים להעביר תכנים, מה זה היינו צריכים? יזמנו, יזמתי להעביר תכנים דרך הזום. אז ממש יום אחרי שהתחיל, התחילה המלחמה, אנחנו כבר התחלנו להעביר תכנים לכל הילדים של הצהרונים שלנו דרך הזום כל מיני הפעלות, מדריכות ובמקום הצהרונים שיהיה להם תכנים דרך הזום. אז ביקשתי מהסמנכ"לית משאבי אנוש שלי לבנות לי נוהל עבודה בחירום, כזה שזה מעולה.

שלומי בני :

מעולה, נכון,

צחי קינן :

נתנו מענה גם,

שלומי בני :

נכון,

צחי קינן :

לעובדים, לעובדים במשק שהם חיוניים לבתי חולים, אז עשינו, עשינו,

ברק לוי :

שמרטיפיות,

צחי קינן:

שמרטפים,

עפרה ברכה:

אז גם החינוך בעצם,

צחי קינן:

זה אנחנו,

עפרה ברכה:

לא?

ברק לוי:

כן, אנחנו הפעלנו,

צחי קינן:

אנחנו הפעלנו,

עפרה ברכה:

בתי חולים למשל שמרטפיות,

ברק לוי:

בבתי חולים, גם פה בספרא,

עפרה ברכה:

גם בעירייה היו, נכון,

צחי קינן:

כן, גם בספרא הפעלנו,

ברק לוי:

הפעלנו 11 שמרטפית עם עובדים שלנו שנתנו מענה לעובדי, העובדים שלה בתי חולים, עובדי רפואה
שישימו שם את הילדים כדי שיוכלו לעבוד.

עפרה ברכה:

אז אתם עושים מ – א' עד ת' בנושא שמרטפיות?

ברק לוי:

כן, השמרטפיות, תראי, זה מחולק, עד שנה שעברה, אנחנו הפעלנו לגמרי, לא, זה שאלה טובה מה שאת שואלת. השנה מה שקרה משרד הבריאות כתוצאה מהלקחים שלו של שנה שעברה, הוא עשה מכרז ויש לו חברה שזכתה, נקראת איך היא נקראת? לא זוכר, יש לו איזה חברה.

עפרה ברכה:

לא משנה.

ברק לוי:

אבל מנח"י פה לא מספיק סומכים על החברה של משרד הבריאות,

עפרה ברכה:

אוקי,

ברק לוי:

כי היא לא מספיק טובה. לא מספיק ערוכה, התכנים שם לא מספיק טובים, אז הם מבקשים מאיתנו לתגבר ולקחת אחריות על השמרטפיות האלה. אז אנחנו את ה - 11 האלה הם היו תחת אחריותנו.

עפרה ברכה:

שזה בבתי חולים וכאלה, ובספרא.

ברק לוי:

בבתי חולים ובספרא.

עפרה ברכה:

אז אתם גם לוגיסטי וגם תכנים והכול?

צחי קינן:

כן,

ברק לוי:

תכנים, ציוד הבאנו לוגיסטיקה רק להביא את הטושים,

עפרה ברכה:

זה לא מינהל חינוך בתוך העיר,

ברק לוי:

מה פתאום, הם מה, הם אין להם יכולת ביצוע,

צחי קינן:

אין להם את הכלים,

ברק לוי:

מפעילים אותנו, אנחנו הזרוע הביצוע שלהם.

שלומי בני:

אין, אין להם יכולות לוגיסטיות .

צחי קינן:

ערכות הפעלה, הכול,

ברק לוי:

סיסי היא הרימה אלי טלפון ביום שהתחיל ה-, זה מול איראן,

עפרה ברכה:

זהו, כי אני במוקד כל הזמן, ושמענו במינהל חינוך כל מה שהם מכירים,

ברק לוי:

סיסי דיברה איתי ביום, תקשיבי, זה התחיל ביום שישי בבוקר, סיסי היא דיברה איתי, אמרה לי,

עפרה ברכה:

ראש העיר ביקש,

ברק לוי:

סיסי ביום ראשון, ביום שישי שהיה זה, טלפנה אלי, אמרה לי, אני צריכה ביום ראשון תפעילו שבע, זה התחיל ב – 7,

עפרה ברכה:

נכון,

ברק לוי:

לך תפעיל בבתי חולים, אמרתי לה אין בעיה - אפעל. לא ידעתי איך, לא ידעתי עוד מה,

שלומי בני:

יפה,

ברק לוי:

לדבר עם האנשים.

שלומי בני:

לא ידעת איך.

עפרה ברכה:

(לא ברור),

שלומי בני:

אז אני שואל אם יש לך תוכנית,

ברק לוי:

אז עכשיו,

עפרה ברכה:

זה נערים ש - ,

ברק לוי:

בגלל זה עכשיו הסמנכ"לית,

שלומי בני:

אהבתי.

ברק לוי:

נכון, ובגלל זה עכשיו הסמנכ"לית,

שלומי בני:

אז מה שאני יכול להמליץ,

ברק לוי:

(לא ברור) בונה.

שלומי בני:

שאתם צריכים לעשות תרחישי ייחוס. זאת אומרת מצב של מלחמה, מצב של מגפה, המצב של,

עפרה ברכה:

מגישים למשל מוריה וזה, אתכם לא שונה.

ברק לוי:

כי מנח"י שם, הם ה - אנחנו בסוף,

עפרה ברכה:

הם הזרוע המבצעת,

ברק לוי:

הזרוע המבצעת, מבינה?

עפרה ברכה:

כן,

ברק לוי:

ולכן אתה צודק, ולכן אנחנו גם ביקשתי ממנה שתבנה וזה מה שאמרתי שזה ממש מתחבר, רציפות תפקודית או תוכנית נוהל עבודה בחירום זה ככה, אני הגדרתי לזה,

עפרה ברכה:

לא, סתם (לא ברור),

ברק לוי:

זה בדיוק,

שלומי בני:

זה הרעיון כן, זה פחות סייברי. כן, התאוששות מאסון זה הסייבר, אבל,

עפרה ברכה:

התאוששות מאסון, זה כן, אבל זה גם במערכות המחשוביות, שלזה זה כנראה אתה התכוונת.

שלומי בני:

כן, ההתאוששות מערכות זה מערכות מידע,

עפרה ברכה:

נכון,

שלומי בני:

והמשכיות התפקודית זה בגדול זה לא קשור.

עפרה ברכה:

איך הרציפות ממשיכה,

שלומי בני:

איך הרציפות ממשיכה,

עפרה ברכה:

רציפות ממשיכה,

שלומי בני:

נכון.

עפרה ברכה:

אבל שייתנו כל השירותים.

עו"ד דני ליבמן:

יש למכון התקנים, תקנים בנושא הזה, לפחות שניים שאני ראיתי עכשיו פה, פה יש ביטחון וחוסן תפקודי, מערכות עם רציפות עסקית, זה עולה 455 שקל, ויש עוד אחד שמסביר איך לייצר. בקיצור, בכמה מאות שקלים אתם קונים תקן ממכון התקנים שהוא אמור לעזור לכם.

אלדד רבינוביץ:

אין צורך את התקן, צריך לקנות את האדם שידוע ליישם אותו.

שלומי בני:

כו,

עו"ד דני ליבמן:

אנחנו,

אלדד רבינוביץ:

זה חומר (לא ברור).

עו"ד דני ליבמן:

מבקרת העירייה, לא,

עפרה ברכה:

אני לא מבינה למה,

עו"ד דני ליבמן:

איזה,

עפרה ברכה:

גם היה טעון שיפור,

עו"ד דני ליבמן:

מבקרת העירייה ביקשה שנשיג את זה, אמרנו לה, את זה צריך לקנות.

עפרה ברכה:

זה לא אני, בטוח.

עו"ד דני ליבמן:

לא, אמרנו תקנו, וקנו. והעירייה קנתה את זה.

ברק לוי:

זה גם יהיה בלוחות זמנים שאמרתי.

עפרה ברכה:

הלאה,

שלומי בני:

כן, טוב, עדכוני אבטחת מידע, מערכות הפעלה, מערכות הפעלה בעמדות הקצה ובחלק מהשרתים, מצאנו שלא היו עדכוני,

צחי קינן:
טופל במידי,

שלומי בני:
טופל במידי,

צחי קינן:
גם הוחלפו מערכת ה – FIREWALL, היה לנו צ'ק – פוינט, והיום אנחנו, עדכנו את פורטינט, מערכת גם מתקדמת, לתת לנו מענה הרבה יותר טוב, אנחנו אחרי זה.

שלומי בני:
ביקורת תקופתית, אחת ל – 24 חודשים צריכים לעשות בתקנות הגנת הפרטיות.

צחי קינן:
מכיר, אנחנו על זה,

שלומי בני:
יופי. מבדקי חדירה, לא ביצעתם, יחסית זה בסדר, 2022, אנחנו הגענו ל – 2025, לדעתי,

צחי קינן:
נכון,

שלומי בני:
נכון? זה יחסית זה לא כזה נורא,

צחי קינן:
זה אני אסביר,

עפרה ברכה:
מ – 2022?

שלומי בני:
לא, אני אומר יחסית, אחת ל – 3 שנים,

צחי קינן:

שנה שלמה לא התעסקנו בכלום,

שלומי בני:

שנתיים.

צחי קינן:

2023, 2024 הם הגיעו בדצמבר, לעשות סקר סיכונים.

שלומי בני:

כן, רק צריך בתדירות יותר,

צחי קינן:

(לא ברור),

שלומי בני:

יותר טובה,

צחי קינן:

לחלוטין אחת לשנה, אנחנו מתעסקים בזה ביחד עם הפישינג.

שלומי בני:

הקשחות של אקטיב – דירקטור, אנטי – וירוסים, או שרתים.

צחי קינן:

בוצע במידי,

שלומי בני:

בוצע כל מה שהקשחות שלא עולה כסף, אני מניח,

צחי קינן:

נכון, נכון, ויש לנו עוד תוכנית עבודה פה, של חלק שאנחנו רוצים. עוד הפעם, מערכות נוספות, שיהיה לנו יותר לעזרה, זה חלק בתהליך של ההצעות מחיר, ותוכנית, נסיים אותה.

שלומי בני:

טוב, עשינו מבדקי חדירה, גם פנימיים חיצוניים וגם לאתר אינטרנט,

צחי קינן:

נכון,

שלומי בני:

וגם שם מצאנו כל מיני ממצאים.

צחי קינן:

שטופלו במידי כל הממצאים של אתר אינטרנט.

שלומי בני:

אוקי,

צחי קינן:

זו חברה שמתחזקת לנו גם חיצונית, חברת אחזקה. טופלו כל ההערות שקיבלנו על האתר אינטרנט,

עפרה ברכה:

אוקי,

שלומי בני:

יופי

אלדד רבינוביץ:

יש לי עוד שאלה, אתה אמרת שאתם שמרנים ובעצם השרתים אצלכם מצד אחד, מצד שני אמרת שמאגרי מידע הם חברות חיצוניות,

צחי קינן:

נכון,

אלדד רבינוביץ:

אז על שניהם אני שואל, זה נכון לשמור את השרתים אצלך בענן, מבחינת אבטחת מידע והכול?

שלומי בני:

נראה, אין פה נכון, נכון או לא נכון, בסדר? זה לא, זה לא אפס או אחד, ההיבטים האם לשמור את זה אצלך או לשמור את זה בענן, זה לא בהיבטי אבטחת מידע, אלא זה בעיקר היבטים שהם

כלכליים, בעיקר. זאת אומרת אתה רוצה עכשיו לקנות שרתים ולתחזק אותם ולעשות להם גיבויים ולאבטח אותם, או שאתה קונה את השירות הזה אצל מישהו אחר, עולה לך קצת יותר. זאת אומרת, אבטחת המידע, אתה יכול לעשות אבטחת מידע מצוינת בענן, ואתה יכול לעשות אבטחת מידע מצוינת אצלך, השיקול הוא תמיד שיקולי שהוא כלכלי. זה כמו האם תקנה רכב או אם תעשה ליסינג,

אלדד רבינוביץ:

הבנתי.

שלומי בני:

נכון? ליסינג עולה קצת יותר, אז אתה בדרך כלל כנראה כאדם פרטי ואתה תקנה רכב. נכון? בדרך כלל אנחנו קונים רכבים.

אלדד רבינוביץ:

אז אתם בעצם אצלכם ואתם עושים את כל מה,

צחי קינן:

נכון, גם, גם השרתים שלי הם נקראים מאגרי מידע.

אלדד רבינוביץ:

מצוין.

שלומי בני:

נכון, אחד מחזיק, אחד בעלים.

אלדד רבינוביץ:

לגבי הנקודה השנייה של המאגרים שאתם אומרים שהם אצל כל מיני חברות חיצוניות.

צחי קינן:

כן,

אלדד רבינוביץ:

זה נכון שתחזיקו גם גיבוי, כי בסוף מדובר במאגרים שהם סופר קריטיים, כל הילדים שצריכים בכל המסלולים שלהם וכל. סתם אני, אני מאוד עסוק בהסעות ילדים כי זה היה דו"ח של כל, וגם אני שומע בסביבתי שזה נושא משמעותי, אבל ועוד כל מיני דברים אחרים, זאת אומרת אולי נכון להשאיר איזה שהיא איזה שהוא גיבוי.?

שלומי בני:

יש להם גיבויים.

צחי קינן:

אצלי הכול מגובה.

שלומי בני:

בוא תגיד אתה צחי.

צחי קינן:

יש לנו גיבויים מלא, אני יכול, נניח אתה יכול להפיל לי מערכת שלמה, אני מחולק קאר - נטר המלווים והעמותה שלי זה שתי, החדרי תקשורת מגבים מלא, מאה אחוז על אחד. זאת אומרת אחד נפל, יש לי מאה אחוז גיבוי מלא בשני ויש לי קלטות כמובן יש לנו נוהל גיבוי כל יום ראשון, עושה הקלטות של כל הגיבויים, שומר אותם בכספת.

שלומי בני:

זה חלק מהבדיקות שביצענו במהלך הביקורת, פשוט זה יצא תקין אז לא עלינו.

אלדד רבינוביץ:

מצוין.

שלומי בני:

זה חשוב, גיבויים זה אחד הנושאים החשובים.

אלדד רבינוביץ:

מעולה.

שלומי בני:

במשפט אחד, בסך הכול המצב היה טעון שיפור, בעיקר ב - . הוראות חוק, זאת אומרת, אם אתה לא עומד בחוק, אתה עמותה עירונית ואתה לא עומד בהוראות חוק, אז אי אפשר לתת לך ציון טוב. נכון? אי אפשר. אז גם פה היה טעון שיפור. מצד שני, בדברים מסיימים הם כן היו הדרכות הם עשו, היו יש, יש כאילו ניצנים של דברים קצת יותר טובים. אבל בסך הכול אם אני מסכם, לסכם את הכול טעון שיפור. לא עומדים בהוראות חוק. היו כל מיני דברים שמצאנו, אבל עושה רושם שהחבריה פה, יש תוכנית עבודה לפי, לפי זה, וגם אני יודע שגם חלק טופלו תוך כדי הביקורת.

ברק לוי:

נכון.

שלומי בני:

צחי היה איתנו בקשר ולא. אפילו שהוא היה בתוך מילואים, הוא גייגל בין הדברים ונפרדו.

ינון נוימן:

מפורדו הוא התקשר.

שלומי בני:

למה אתה מספר? ינון, זה לא. אבל הוא היה לדעתי בשני, לא?

ינון נוימן:

בנתנו.

אלדד רבינוביץ:

יש עוד מי שרוצה?

ברק לוי:

אני כמו שאמרתי אנחנו פה, על זה חלק מהדברים כבר טופלו, החשיבות מובנת ומה שטרם טופל יטופל בהקדם בחודשים הקרובים, בעזרת השם, עוד לפני סוף שנה נסיים את הכול, וגם נשלח לכם,

צחי קינן:

דו"ח מפורט.

ברק לוי:

עדכון שהכול טופל, כן.

עפרה ברכה:

טוב. אני מברכת על ההתייחסות ש - , על הרצינות שחברת לביא מגלה לדו"ח, ועוד הפעם כמו באחרים. אני שמחה שעסקנו בנושא ואנחנו מביאים תועלת וזה הופך לתכנית עבודה, אז אני מברכת על זה ואני גם בהזדמנות זו, מאחלת לך הצלחה.

צחי קינן:

תודה רבה.

עפרה ברכה:

ותודה רבה גם לשלומי ולינון ולאורטל, צחי לוועדת הביקורת.

צחי קינן:

שלומי הוא ביקורת מקצועית לחלוטין.

שלומי בני:

תודה.

צחי קינן:

מקצה לקצה.

עפרה ברכה:

אנחנו בוחרים את הכי טובים,

צחי קינן:

באמת.

עו"ד דני ליבמן:

אנחנו עושים ביקורות ברמה של חיל האוויר פה,

שלומי בני:

הישראלי.

אלדד רבינוביץ:

אני גם מתחבר לכל הדוחות, באמת דו"ח ביקורת משמעותי, תודה על הקיום שלו. בסופו של דבר זה מה שנותן ומאפשר לעמותה את ההתפתחות שלה, ואת הקיום. גם לעמוד בהוראות החוק וגם באמת ליישם את מה שהיא צריכה. מטרת הביקורת באמת לצמוח לתוכניות עבודה, נראה שזה הכיוון. אז תודה לכם על קבלת הביקורת בשתי ידיים. תודה לכולם על העבודה המקצועית. אני מקבל את המלצות הדוח בכפוף להערות או הוספות לעיל, אני ממליץ למועצה לאמץ את מסקנות הוועדה. עבודה מעולה.

שלומי בני:

תודה רבה.

צחי קינן:

תודה רבה.

אלדד רבינוביץ:

ביי, תודה רבה.

עפרה ברכה:

תודה לכולם.

סיום הדיון