



ועדה לענייני ביקורת

כ"ט בחשוון תשפ"ו
20 בנובמבר 2025
סימוכין: 2025-103-958

דו"ח משיבה מס' 22 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
גבי ליאת שמחה יופי, סמנכלי"ת כספים בחברת עדן
גבי הודיה בן גיגי, אחראית אבטחת מידע בחברת עדן
רו"ח שלומי בני, יועץ הביקורת
מר צבי עבו, מזכיר ועדת ביקורת

על סדר היום:

דוח מבקרת העירייה בנושא: אבטחת מידע וסייבר בחברת עדן

פתיחת הדיון:

מר אלדד רבינוביץ, יו"ר הוועדה: אנו בעיצומם סדרת דוחות ביקורת שבוחנים היבטים דומים של סייבר ואבטחת מידע בתאגידים עירוניים. דוחות הביקורת חשובים מאוד ואני מברך על הביקורת.

גבי עופרה ברכה, מבקרת העירייה: כולם כיום מבינים את המשמעות של נושא הגנת פרטיות, אבטחת מידע וסייבר. מה הנזק שיכול להיגרם מתקפת סייבר כזו או אחרת, וכמה חשוב הגנות והתנהלות בהתאם להוראות החוק. בחברת עדן נראה שטוב שבוצעה ביקורת, היה הרבה מה לתקן, גם פה חשוב לבחור באמת יועץ חיצוני ונשמח שתראו לנו את התקדמותכם בעניין.

דיון הוועדה:

פרק 1:

המלצת המבקרת:

- למפות ולרשום את מאגרי המידע הנדרשים לרישום בהתאם לחוק ותקנותיו וכן לקבוע את רמת אבטחת המידע הנדרשת מכל אחד ממאגרי המידע בהתאם לתקנות.
- להכין מסמך הגדרות מאגרי מידע שבו יפורטו כל הנושאים הנדרשים בתקנות, כגון: תיאור כללי של פעולות האיסוף והשימוש במידע, מטרות השימוש במאגר, רמת הסיכון של כל מאגר ועוד.



ועדה לענייני ביקורת

- על החברה למנות באופן רשמי (באמצעות כתב מינוי) ממונה אבטחת מידע אשר יפעל לפחות ליישום המשימות הבאות בהתאם להוראות התקנות:
- כתיבת נוהלי אבטחת מידע ואישורם על ידי מנהלי המאגרים והנהלת החברה.
- הכנת תוכנית לבקרה שוטפת על עמידה בדרישות התקנות, ביצוע התוכנית ועדכון בעלי המאגרים לגבי הממצאים שנמצאו.
- לגבש מדיניות ונוהלי אבטחת מידע המפרטים את הנחיות ואמצעי אבטחת המידע בחברה ובמאגרי המידע בפרט, אשר יכללו לכל הפחות את הדרישות בתקנות וכן נושאים נוספים כגון: הוראות בעניין האבטחת הפיזית והסביבתית, הרשאות גישה למאגרי המידע ומערכות המאגרים, מיפוי וסיווג נכסי המידע של החברה ועוד.
- להכין מסמכים של מבנה מאגרי המידע וכן רשימת מצאי של מערכות המאגרים בהתאם לדרישות בתקנות כגון: תיאור ופירוט התשתיות ומערכות החומרה, סוגי רכיבי תקשורת, מערכות התוכנה המשמשות להפעלת מאגרי המידע, תרשים הרשת הארגונית וכו'.
- לנהל תיעוד גישה (כניסה ויציאה) לחדר השרתים והתקשורת.
- לקיים הדרכות לעובדי ומשתמשי המערכות בחברה בדבר חובותיהם לפי החוק ונוהל אבטחת המידע (שיגובש), לקיים הדרכות מודעות לעובדים קיימים וחדשים בנושא אבטחת מידע וסייבר לפחות אחת לשנה.
- להקשיח את מדיניות הסיסמאות ברשת החברה ובמערכות החברה.
- לבצע תהליך של סקירת משתמשים והרשאותיהם ברשת החברה ובמערכות החברה אחת לתקופה כפי שתקבע החברה. 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 החברה ולחברה איך להתנהל בקרות אירוע סייבר.
- לפתח תהליך לקיום המשכיות עסקית אשר יכלול בין השאר מיפוי הסיכונים שלהם חשופה החברה, ניסוח אסטרטגיית המשכיות עסקית (BCP), הגדרת התהליכים והמערכות החיוניות לחברה 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.
- ליידע את בעלי ההרשאות במאגר בדבר קיום מנגנון הבקרה.
- לקיים דיון אחת לשנה לפחות באירועי אבטחה ולתעד את הדיון באמצעות פרוטוקול.
- ליישם מנגנון למניעת חיבור התקנים ניידים לתחנות הקצה של החברה, או לחלופין להפעלת מערכת הלבנה מרכזית אשר תבדוק התקנים ניידים לפני שהם מוכנסים לרשת הארגונית, ובכך לצמצם את הסיכון להוצאת מידע רגיש או פרטי מהחברה.
- 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 נגישים אליהן ולבנות תהליך עבודה סדור הכולל:
- קביעת רמת הסיווג של כל ספק (עד כמה הוא נגיש למידע רגיש, האם הוא שומר אצלו חומר של החברה וכו').
- חיבור מאובטח של ספקים לרשת החברה.
- בקרה על חיבור הספקים, ובכלל זה אישור חיבור מראש וכו'.
- לבחון הטמעת מערכת הקלטות למערכות שאליהן מתחבר הספק.
- לתאם סקר ספק אצל ספק שזוהה שהחיבור שלו גורם לחברה סיכון ברמה בינונית ומעלה.
- לבצע ביקורת תקופתית אחת ל-24 חודשים לפחות ובהתאם לדרישות התקנות.
- לבצע סקר סיכונים סייבר ומבחני חדירה אחת לתקופה כפי שתקבע החברה.
- למפות את גורמי הסיכון הארגוניים לדלף מידע.
- למפות את מקומות אחסון החומר הרגיש ואת מסדי הנתונים שבהם מוחזק המידע.
- לכתוב נוהל להוצאת מידע ממערכות החברה.
- 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 לחברה וכיוצא באלו.
- לבחון שימוש במנגנון DLP - Data Loss Prevention Software (מערכות למניעה של דלף מידע) במערכות הדואר האלקטרוני והאינטרנט.

תגובת המבוקר:

מודים על דוח הביקורת, מאגרי המידע מופו וכעת בהליך רישום. אנו עובדים עם יועץ אבטחת מידע על כל ההמלצות, רובם כבר בוצעו.

המלצת ועדת ביקורת:

לקבל את המלצות המבקר.
בנוסף, בתוך 30 ימים חברת עדן תשלח עדכון למבקר וליו"ר ועדת הביקורת בנוגע לרישום מאגרי המידע והשלמת יישום ההמלצות.

פרק 2:

המלצת המבקר:

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

תגובת המבוקר:

בוצע או בתהליך טיפול.

המלצת ועדת ביקורת:

לקבל את המלצות המבקר.
בנוסף, בתוך 30 ימים חברת עדן תשלח עדכון למבקר וליו"ר ועדת הביקורת בנוגע השלמת יישום ההמלצות.



ועדה לענייני ביקורת

פרק 3:

המלצת המבקר:

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

תגובת המבוקר:

רוב ההמלצות מומשו או בתהליך.

המלצת ועדת ביקורת:

לקבל את המלצות המבקר.

בנוסף, בתוך 30 ימים חברת עדן תשלח למבקר וליו"ר ועדת הביקורת בנוגע לרישום מאגרי המידע והשלמת יישום ההמלצות.

פרק 4:

המלצת המבקר:

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

תגובת המבוקר:

בבחינה או בטיפול.

המלצת ועדת ביקורת:

לקבל את המלצות המבקר.

בנוסף, בתוך 30 ימים חברת עדן תשלח למבקר וליו"ר ועדת הביקורת בנוגע לרישום מאגרי המידע והשלמת יישום ההמלצות.

סיכום:

מר אלדד רבינוביץ, יו"ר הוועדה: מטרת הביקורת זה להאיר פינות אפלות ולייצר תהליכי עבודה. כפי שאמרו בחברת עדן, הביקורת הגיעה במועד מתאים שבו הם התחילו גם כך לעשות סדר והביקורת סייעה מאוד להתקדמות החברה.

מודה למבקר ולמבקר, ותודה לחברת עדן שלקחה את הביקורת ברצינות. הושקע עמל גדול בתהליכי ביקורת, היא התקבלה באהבה ובשמחה והפכה לתהליך עבודה. יחס כזה נותן ערך משמעותי ותועלת לנושא המבוקר.

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 שלישי

**הגנת הפרטיות, אבטחת מידע
וסייבר בחברת עדן**

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 // 53

מבוא // 57

פירוט הממצאים

פרק ראשון:

בדיקת רגולציה, מדיניות, נהלים ותהליכים בתחום אבטחת מאגרי מידע // 63

פרק שני:

בדיקות טכנולוגיות של אבטחת מידע וסייבר ומבדקי חדירה // **הושמט**

סיכום // 80

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 בדקה את עמידת החברה בהוראות חוק הגנת הפרטיות, התשמ"א-1981, ותקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, את המדיניות והנהלים בנושא אבטחת המידע, וערכה כמה בדיקות: מבדק טכנולוגי לבחינת רמת האבטחה הקיימת בחברה, בדיקה פיזית לאבטחת המידע ומבדקי חדירה לרשת החברה.

הביקורת העלתה ליקויים מהותיים לגבי יישום 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) וליקויים בעלי חשיבות גבוהה במבדקי החדירה שביצעה הביקורת.

עיקרי הממצאים

1. לחברה אין כלל מסמכים של הגדרות מאגרי מידע ושל מבנה מאגרי המידע. לא קיימת רשימת מצאי של מערכות המאגרים, והחברה אף לא רשמה מאגר מידע של עובדיה.
2. החברה לא מינתה באופן רשמי ממונה אבטחת מידע, לא קיימים מדיניות אבטחת מידע ונוהלי אבטחת מידע כתובים.
3. קיימים ליקויים משמעותיים במדיניות הסיסמאות של הרשת ומערכות המידע של החברה.
4. 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.
5. לחברה אין נוהל התאוששות מאסון ואין תוכנית להמשכיות עסקית.
6. בחברה לא קיים מנגנון למניעת חיבור התקנים ניידים, או להפעלת מערכת הלבנה אשר תבדוק התקנים ניידים לפני שהם מוכנסים לרשת הארגונית.
7. ישנן מערכות שאינן מעודכנות בעדכוני אבטחת מידע קריטיים.
8. החברה לא ביצעה ביקורת תקופתית כדי לוודא שהיא עומדת בהוראות החוק והתקנות.
9. החברה מעולם לא ביצעה סקר סיכוני אבטחת מידע וסייבר ומבדקי חדירה.
10. עמדות הקצה, השרתים וה-GPO (Group Policy) אינם מוקשחים מספיק; שיטות העבודה הנהוגות אינן מקובלות בתחום אבטחת מידע וסייבר. נמצא מספר רב של הגדרות שאינן תקינות.
11. נמצא מספר רב של ליקויים בעלי חשיבות גבוהה בניהול ובתחזוקת מערכת האנטי-וירוס ובמערכת עדכוני אבטחת המידע. המערכות אינן מנוהלות ומתוחזקות בהתאם לסטנדרטים מקובלים.
12. נמצאו ליקויים רבים בעלי חשיבות גבוהה בניהול ובתחזוקת מערכת ה-AD (Active Directory - מערכת לניהול משתמשים), המערכת אינה מנוהלת ומתוחזקת בהתאם לסטנדרטים מקובלים.
13. נמצאו ליקויים רבים בעלי חשיבות גבוהה במבדקי החדירה הפנימיים והחיצוניים שבוצעה הביקורת.

המלצות מרכזיות

1. למפות את דרישות הוראות החוק והתקנות וליישמן במלואן. בין השאר - מיפוי מאגרי המידע המחויבים ברישום בהתאם לחוק, ויצירת מסמכי הגדרות מאגרי מידע.
2. למנות באופן רשמי ממונה אבטחת מידע ולגבש לאלתר מדיניות ונוהלי אבטחת מידע.

3. להגדיר מדיניות סיסמאות נאותה במערכות וברשת החברה.
 4. לקבוע נוהל בדיקה שגרתי של נתוני התיעוד של מנגנון הבקרה, להגדיר איסוף לוגים וניטורי אירועי אבטחת מידע מכל מערכות אבטחת המידע בחברה, ולשמור לוג פעולות במערכות המידע ובמערכות אבטחת המידע למשך 24 חודשים לפחות.
 5. לגבש נוהל התאוששות מאסון ולבנות תוכנית להמשכיות עסקית.
 6. ליישם מנגנון למניעת חיבור התקנים ניידים לתחנות הקצה של החברה, או לחלופין להפעלת מערכת הלבנה מרכזית.
 7. להתקין בדרך קבע את עדכוני האבטחה המופצים ע"י יצרני המערכות.
 8. לבצע ביקורת תקופתית כדי לוודא שהחברה עומדת בהוראות החוק והתקנות.
 9. לבצע בהקדם סקר סיכוני אבטחת מידע ומבדקי חדירה.
 10. לטפל בדחיפות בהקשחת עמדות הקצה, השרתים וה-GPO (Group Policy), ובמצאים שעלו במערכות האנטי-וירוס, בעדכוני אבטחת מידע, בחומת האש ובמערכת ה-AD.
 11. לטפל בדחיפות בממצאים שעלו במבדקי החדירה הפנימיים שביצעה הביקורת.
 12. לטפל בממצאים שעלו בבדיקת תשתית למערכת הדואר האלקטרוני והאנטי-ספאם לדואר האלקטרוני.
 13. לטפל בממצאים שעלו בבדיקת אתר האינטרנט של החברה.
- 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

חברת עדן

- בימים אלה חברת עדן שוכרת את שירותיה של חברת סייבר לצורך טיפול בפערים שהובאו לידיעתנו במסגרת הדוח.
- בכוונת הנהלת החברה לבחון את הפערים שהוצגו ולטפל באופן מעמיק ויסודי בפערים ככל שהם קיימים.
- בסיום ההליך נעביר לעיון הביקורת דוח פירוט תיקון הליקויים.

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.

חברת עדן היא יעד פוטנציאלי לניסיון תקיפות סייבר, בין היתר בשל היותה חברה 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 החברה.

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 שונים 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 בדקה את עמידת החברה בהוראות החוק והתקנות, את המדיניות והנהלים בנושא אבטחת המידע, וכן ערכה מבדק טכנולוגי לבחינת רמת האבטחה הקיימת בחברה, בדיקה פיזית לאבטחת המידע, ומבדקי חדירה לרשת החברה.

הביקורת העלתה ליקויים מהותיים לגבי יישום 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 וליקויים בעלי חשיבות גבוהה במבדקי החדירה שביצעה.

על החברה 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 לחברה לעמוד בחובותיה הרגולטוריות, וכפועל יוצא להפחית את הסיכונים למיניהם מעצם התרחשות האירוע.

מבוא

חברת עדן – החברה לפיתוח כלכלי בירושלים, היא הזרוע העירונית המטפלת בפיתוח כלכלי ותרבותי ובפיתוח המרחב הציבורי באזורי מסחר ותעסוקה אסטרטגיים בעיר ירושלים. החברה הוקמה על ידי עיריית ירושלים והרשות לפיתוח ירושלים בשנת 2001, לקידום תוכנית התחדשות והחייאה של מרכז העיר באמצעים יצירתיים ומגוונים. עם השנים התמחתה החברה במגוון תחומים:

- שיפור המרחב הציבורי, תכנון ובנייה של שטחי ציבור איכותיים, לרבות שדרוג תשתיות ושיקום חזות הרחוב
- יצירת עוגנים שלטוניים ומתן תמריצים להשקעות כלכליות של המגזר הפרטי
- קידום העשייה התרבותית
- שדרוג הפעילות העסקית
- קידום מיזמים עירוניים במתווה PPP (Public-Private Partnership), שותפות ציבורית-פרטית).

בשנת 2015 הפכה עדן לחברה עירונית עצמאית בבעלות עיריית ירושלים.

בשנים האחרונות יש עלייה מתמדת בהיקף ובעוצמת האיומים במרחב הסייבר בעולם כולו ובישראל בפרט, איומים המתממשים באמצעות תוכנות זדוניות (נזקות 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.

התקפות סייבר עלולות לגרום נזקים כגון פגיעה בתשתיות טכנולוגיה (חומרה, תוכנה ויישומים), פגיעה בשלמותו ובמהימנותו של המידע השמור במערכות המידע שבשימוש הארגונים השונים, דליפה של נתונים ומידע ממאגרי המידע וחשיפתם לגורמים שאינם מורשים לכך. במקרים חמורים הנזקים עלולים לגרום אף לפגיעה ברציפות התפקודית של הארגון.

כדי לצמצם את פוטנציאל הפגיעה בפרטיות הגלום במאגרי מידע, נחקק חוק הגנת הפרטיות הכולל הסדר ספציפי העוסק במאגרי מידע ממוחשבים.

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 (אבטחת מידע), התשע"ז-2017, המפרטות את אופן יישומה של חובת אבטחת המידע המוטלת בחוק הגנת

הפרטיות על כל בעל מאגר של מידע אישי, על מנהל המאגר ועל המחזיק בו. התקנות כוללות מיון של מאגרי מידע לפי מגוון מאפיינים (סוגי המידע הכלולים במאגר, מספר האנשים שמידע עליהם כלול במאגר ומספר בעלי ההרשאה) וקובעות לפי המאפיינים את רמת האבטחה שחלה על מאגר המידע. התקנות מגדירות בפירוט את החובות של בעל מאגר מידע ליישום בקורות תהליכיות וטכנולוגיות לצורך אבטחת המאגר.

יש לציין כי מליאת הכנסת אישרה ב-5.8.2024 בקריאה שנייה ושלישית תיקון מקיף בחוק הגנת הפרטיות. 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, על פיקוח ועל אכיפת 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 יש לנקוט אמצעים לאבטחת המידע ומערכי המידע ולהגן עליהם מפני פגיעה, חשיפה ושינוי - במזיד או בשוגג. יש לעשות זאת באופן שיישמרו הזמניות, השלמות והסודיות של המידע ומערכות המידע.

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

הביקורת בדקה את עמידת החברה בהוראות חוק הגנת הפרטיות, התשמ"א-1981, ותקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, את המדיניות והנהלים בנושא אבטחת המידע - אם החברה ביצעה מבדק טכנולוגי לבחינת רמת האבטחה הקיימת בארגון, בדיקה פיזית לאבטחת המידע, מבדקי חדירה לרשת הארגון, 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).

יחידת מערכות המידע בחברת עדן מנוהלת על ידי חברה חיצונית בשם "Global Network". החברה החיצונית אחראית גם לנושא אבטחת המידע בחברה.

בחברה יש כמה מערכות מידע עיקריות להנה"ח, ניהול פרויקטים, ניהול חניונים ושכר.

מטרת הבדיקה

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

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

הערכת רמת אבטחת המידע, באמצעות מבדק טכנולוגי ומבחני חדירה.

היקף הבדיקה

עמידת החברה 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 בחברה, בדיקה פיזית לאבטחת המידע, ומבדקי חדירה לרשת החברה.

תקופת הביקורת

הביקורת נערכה בחודשים אוגוסט – אוקטובר 2024.

פירוט הממצאים

פרק ראשון

בדיקת ציות להוראות חוק הגנת הפרטיות ותקנות הגנת הפרטיות

רישום מאגרי מידע

החוק להגנת הפרטיות 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 כאוסף נתונים למאגר מידע ולא יהיה צורך ברישומם.

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.
- מבדיקת הביקורת עולה כי בחברה קיימים שני מאגרי מידע העונים על ההגדרה בסעיף 8(ג) לחוק, כדלהלן:

- לקוחות – מאגר המידע הקיים במערכת SBO, הכולל מידע רגיש, כגון פרטי ספקים וחשבונות הבנק שלהם (סעיף 8(ג)(2) לחוק).
 - מתכננים ויועצים – מאגר המידע הקיים במערכת מניפה כולל מידע רגיש, כגון מספרי תעודות זהות של העובדים וחשבונות הבנק שלהם (סעיף 8(ג)(2) לחוק).
- שני המאגרים לעיל רשומים ברשות להגנת הפרטיות. התיעוד שנתקבל בביקורת הוא צילום בלבד מתוך האתר של הרשות להגנת הפרטיות. לא נתקבלו מסמכים חתומים של רישום המאגרים. נוסף על כך, החברה לא רשמה מאגר מידע של עובדיה, התואם גם הוא להגדרה בסעיף 8(ג) לעיל.

מסקנות

1. אי רישום מאגר מידע ברשות להגנת הפרטיות או רישום באופן חלקי מעמידים את החברה במצב שבו אינה עומדת בהוראות החוק ותקנותיו.

המלצות

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

מסמך הגדרות מאגרי מידע

בהתאם לתקנות הגנת הפרטיות, על בעל מאגר מידע לנהל "מסמך הגדרות מאגר". במסמך נדרש לפרט את הנושאים המנויים בתקנה ויש לעדכן אחת לשנה לפחות. אם נעשים עדכונים מהותיים במהלך השנה, נדרש לעדכן את המסמך עם קרות השינויים.

סעיף 2 לתקנות מציין כי:

"א. בעל מאגר מידע יגדיר במסמך הגדרות מאגר (להלן: מסמך הגדרות המאגר), את כל העניינים האלה לפחות:

- (1) תיאור כללי של פעולות האיסוף והשימוש במידע;
 - (2) תיאור מטרות השימוש במידע;
 - (3) סוגי המידע השונים הכלולים במאגר המידע, בשים לב לרשימת סוגי המידע שבפרט 1(3) בתוספת הראשונה;
 - (4) פרטים על העברת מאגר המידע, או חלק מהותי ממנו אל מחוץ לגבולות המדינה או שימוש במידע מחוץ לגבולות המדינה, מטרת ההעברה, ארץ היעד, אופן ההעברה וזהות הנעבר;
 - (5) פעולות עיבוד מידע באמצעות מחזיק;
 - (6) הסיכונים העיקריים של פגיעה באבטחת המידע, ואופן ההתמודדות עמם;
 - (7) שמו של מנהל מאגר המידע, של מחזיק המאגר ושל הממונה על אבטחת מידע בו, אם מונה כזה.
- ב. בעל מאגר מידע יעדכן את מסמך הגדרות המאגר בכל עת שנעשה שינוי משמעותי בנושאים המפורטים בתקנת משנה (א), ויבחן את הצורך בעדכון כאמור, בשל שינויים טכנולוגיים ארגוניים או אירועי אבטחה כאמור בתקנה 11, בכל שנה עד 31 בדצמבר.
- ג. בעל מאגר מידע יבחן, אחת לשנה, אם אין המידע שהוא שומר במאגר רב מן הנדרש למטרות המאגר".

על אף האמור בתקנות, בחברה לא קיימים כלל מסמכי הגדרות מאגרי מידע.

מסקנות

2. אי קיום מסמכי הגדרות מאגרי מידע מעמיד את החברה במצב שבו אינה עומדת בהוראות החוק ותקנותיו.

המלצות

2. להכין מסמך הגדרות מאגרי מידע שבו יפורטו כל הנושאים הנדרשים בתקנות, כגון: תיאור כללי של פעולות האיסוף והשימוש במידע, מטרות השימוש במאגר, רמת הסיכון של כל מאגר ועוד.

ממונה על אבטחת מידע

סעיף 17 ב(א) לחוק הגנת הפרטיות מטיל חובת מינוי ממונה אבטחת מידע בעל הכשרה מתאימה עבור גופים העומדים באחד מהתנאים האלה:

- הגוף מחזיק בחמישה מאגרי מידע.
 - גוף ציבורי.
 - גוף פיננסי; בנק, חברת ביטוח, חברה העוסקת בדירוג או הערכת אשראי.
- סעיף 3 לתקנות הגנת הפרטיות מפרט את ההוראות שיחולו על ממונה אבטחת המידע, כדלהלן:
- (1) ממונה אבטחה יהיה כפוף ישירות למנהל מאגר המידע או למנהל פעיל של בעל המאגר או המחזיק בו, לפי העניין, או לנושא משרה בכירה אחר הכפוף ישירות למנהל המאגר;
 - (2) הממונה על אבטחה יכין נוהל אבטחת מידע ויביאו לאישור בעל המאגר;
 - (3) הממונה יכין תוכנית לבקרה שוטפת על העמידה בדרישות תקנות אלה, יבצע אותה ויודיע לבעל מאגר המידע ולמנהל המאגר על ממצאיו;
 - (4) הממונה על אבטחה לא ימלא תפקיד נוסף שעלול להעמידו בחשש לניגוד עניינים במילוי תפקידו לפי תקנות אלה;
 - (5) הטיל בעל מאגר המידע על ממונה על אבטחה משימות נוספות על החובות המנויות בפסקאות (2) ו-(3), לשם ביצוע תקנות אלה, יגדיר בצורה ברורה;
 - (6) בעל מאגר המידע יקצה לממונה את המשאבים הדרושים לו לשם מילוי תפקידו.

יחידת מערכות המידע בחברת עדן מנוהלת על ידי חברה חיצונית בשם "Global Network". החברה החיצונית אחראית גם לנושא אבטחת המידע בחברה. עם זאת, לא קיים כתב מינוי לממונה אבטחת מידע, לא קיים נוהל אבטחת מידע ולא קיימת תוכנית לבקרה שוטפת לעמידה בדרישות התקנות.

מסקנות

3. אי מינוי ממונה אבטחת מידע, חוסר בנוהל אבטחת מידע ותוכנית בקרה שוטפת לעמידה בדרישות התקנות, משמעותם כאי עמידת החברה בהוראות החוק ותקנותיו.

המלצות

3. על החברה למנות באופן רשמי (באמצעות כתב מינוי) ממונה אבטחת מידע אשר יפעל לפחות ליישום המשימות הבאות בהתאם להוראות התקנות:
- כתיבת נוהלי אבטחת מידע ואישורם על ידי מנהלי המאגרים והנהלת החברה.
 - הכנת תוכנית לבקרה שוטפת על עמידה בדרישות התקנות, ביצוע התוכנית ועדכון בעלי המאגרים לגבי הממצאים שנמצאו.

מדיניות ונוהל אבטחת מידע

הבסיס לפעילות אבטחת המידע הארגוני הוא מסמך מדיניות אבטחת המידע או לכל הפחות, נוהל אבטחת מידע. מסמך זה אמור לשקף את תפיסת מדיניות האבטחה הארגונית, לתאר את התקן לפעילות, את שיטות העבודה והעקרונות המנחים.

סעיף 4 לתקנות דן בנושא נוהל אבטחת מידע לבעל מאגר שמסתמך על מסמך הגדרות המאגר. הנוהל 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) הסיכונים שחשוף להם המידע שבמאגר במסגרת הפעילות השוטפת של בעל מאגר המידע, לרבות אלה הנובעים ממבנה מערכות המאגר כמפורט בתקנה 5(א), אופן קביעת סיכונים אלה, 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, מאגר מידע שחלה עליו 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 בעדכונן של הנוהל במקרים אלה:
- (1) נעשים שינויים מהותיים במערכות המאגר או בתהליכי עיבוד מידע.
- (2) נודע על סיכונים טכנולוגיים חדשים הנוגעים למערכות המאגר".
- בחברה לא קיימים מדיניות ונוהלי אבטחת מידע המפרטים את אמצעי אבטחת המידע בה ובמאגרי המידע בפרט.

מסקנות

4. בשל חוסר במדיניות ובנוהלי אבטחת מידע מפורטים קיים קושי בחברה ביישום אבטחת מידע נאותה ובפיקוח עליה, וכן החברה אינה עומדת בהוראות החוק ותקנותיו.

המלצות

4. לגבש מדיניות ונוהלי אבטחת מידע המפרטים את הנחיות ואמצעי אבטחת המידע בחברה ובמאגרי המידע בפרט, אשר יכללו לכל הפחות את הדרישות בתקנות וכן נושאים נוספים כגון: הוראות בעניין האבטחה הפיזית והסביבתית, הרשאות גישה למאגרי המידע ומערכות המאגרים, מיפוי וסיווג נכסי המידע של החברה 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.
- בחברה לא קיימים מסמכים של מבנה מאגרי המידע וכן רשימת מצאי של מערכות המאגרים.

מסקנות

5. חוסר במסמכים של מבנה מאגרי המידע ורשימת מצאי של מערכות המאגרים מקשה על יישום מנגנוני אבטחת מידע נאותים על מאגרי המידע ופיקוח החברה עליהם. כמו כן החברה אינה עומדת בהוראות החוק ותקנותיו.

המלצות

5. להכין מסמכים של מבנה מאגרי המידע וכן רשימת מצאי של מערכות המאגרים בהתאם לדרישות בתקנות כגון: תיאור ופירוט התשתיות ומערכות החומרה, סוגי רכיבי תקשורת, מערכות התוכנה המשמשות להפעלת מאגרי המידע, תרשים הרשת הארגונית וכו'.

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 אבטחה פיזית, כדלהלן:

"א. בעל מאגר מידע יבטיח כי המערכות המפורטות בתקנה 5(א) 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".

במשרדי החברה בירושלים קיימים אמצעי אבטחה פיזית כלהלן:

- מצלמות אבטחה ברחבי אתר החברה.
 - מאבטח בשער הכניסה לחברה.
 - בכל קומה או משרד קיימת דלת אשר הכניסה דרכה מותרת אך ורק למורשים, באמצעות מפתח ייחודי לכל אחד מהם.
 - ארונות התקשורת וחדרי השרתים נעולים ומאובטחים
- עם זאת, לא קיים תיעוד של גישות שנעשו לחדר השרתים והתקשורת.

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 החברה לוודא כי ההרשאות הניתנות לעובדים הן 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".

בחברה לא מתקיימות הדרכות לבעלי הרשאות בנושא החובות לפי החוק והתקנות, לא נמסר לעובדי החברה ולמשתמשיה נוהל אבטחת המידע, וכלל לא מתקיימות הדרכות מודעות לעובדים קיימים או חדשים בנושא אבטחת מידע וסייבר.

מסקנות

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

המלצות

6. לנהל תיעוד גישה (כניסה ויציאה) לחדר השרתים והתקשורת.
7. לקיים הדרכות לעובדי ומשתמשי המערכות בחברה בדבר חובותיהם לפי החוק ונוהל אבטחת המידע (שיגובש), לקיים הדרכות מודעות לעובדים קיימים וחדשים בנושא אבטחת מידע וסייבר לפחות אחת לשנה.

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; הרשאת 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 ייעשה 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 לחוזק 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 ההרשאה עשוי היה לדעת, מיד עם סיום תפקידו של בעל ההרשאה.

בחברה 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 טיטה.

להלן תהליך ניהול הרשאות לעובדים בחברה:

- עובד חדש – בעת קליטת עובד חדש לחברה, מחלקת משאבי אנוש מחתימה את העובד על חוזה עבודה והסכם סודיות. נציג מחלקת משאבי אנוש שולח מייל למנהל המחשוב כדי לפתוח משתמש חדש ברשת החברה, שלו תיבת דואר אלקטרוני בהתאם לתפקיד שהוגדר לו. מתן הרשאות למערכות המידע בחברה נעשה על ידי כל משתמש (הסבר בהמשך).
- עובד עוזב – בעת עזיבת עובד את החברה מחלקת משאבי אנוש שולחת בקשה במייל למנהל המחשוב להסרת הרשאות המשתמש מהרשת (הפיכת המשתמש ל"לא פעיל"). הרשאות במערכות המידע מטופלות על ידי משתמשי-העל, אשר קובעים את סטוס המשתמש של העובד כ"לא פעיל", או שמוחקים אותו, בהתאם למערכת הרלוונטית.

הביקורת בדקה את מדיניות הסיסמאות ברשת ובמערכות החברה השונות.

מסקנות

7. מדיניות סיסמאות לא מוקשחת ואי קיום תהליך סקירת משתמשים והרשאותיהם ברשת ובמערכות החברה, חושפים את החברה למצב שבו יהיה ניתן לגלות את סיסמאות המשתמשים באופן קל יחסית, וכן ייתכן כי ישנם משתמשי עובדים שעזבו ועדיין פעילים ברשת ובמערכות החברה.

המלצות

8. להקשיח את מדיניות הסיסמאות ברשת החברה ובמערכות החברה.

9. לבצע תהליך של סקירת משתמשים והרשאותיהם ברשת החברה ובמערכות החברה אחת לתקופה כפי שתקבע החברה. 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 מיידיים 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, יערך 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 החברה באיתור כשלים, פגיעויות ואירועי אבטחת מידע. להלן תוצאות הבדיקה:

- 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.
- 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.
- לחברה אין נוהל התאוששות מאסון.
- בחברה לא קיימת תוכנית להמשכיות עסקית, אשר כוללת בין השאר מיפוי של הסיכונים שלהם חשופה החברה, ניסוח אסטרטגיית המשכיות עסקית (BCP), הגדרת התהליכים והמערכות החיוניות לארגון בעת חירום, הדרכות ותרגול התוכנית ועוד.
- לחברה אין נוהל התמודדות עם אירועי סייבר (שיכול להיות חלק מנוהל התאוששות מאסון ותוכנית להמשכיות עסקית), הכולל הנחיות לעובדי החברה לצורת ההתנהלות בקרות אירוע סייבר בחברה, לטיפול באירוע הצפנה וכו'. נוסף על כך, לא בוצעו תרגילי סייבר מתודיים לדמות התמודדות עם אירועי סייבר פוטנציאליים.
- בעל מאגר המידע אינו מקיים דיון אחת לשנה לפחות באירועי אבטחה.

מסקנות

8. אי קיום מספר רב של בקורות תיעוד, ניטור והתמודדות עם אירועי סייבר, מקטין את הסיכוי של החברה להתמודד עם אירוע סייבר, החל משלב הבנת האירוע, דרך עצירתו ועד צמצום הנזקים בעקבותיו. כמו כן, החברה אינה עומדת בהוראות החוק והתקנות.

המלצות

10. לגבש נוהל בדיקה שגרתי של נתוני התיעוד של מנגנון הבקרה.
11. לגבש נוהל התאוששות מאסון ונוהל התמודדות עם אירועי סייבר, הכולל הנחיות לעובדי החברה ולחברה איך להתנהל בקרות אירוע סייבר.
12. לפתח תהליך לקיום המשכיות עסקית אשר יכלול בין השאר מיפוי הסיכונים שלהם חשופה החברה, ניסוח אסטרטגיית המשכיות עסקית (BCP), הגדרת התהליכים והמערכות החיוניות לחברה בעת חירום, הדרכות ותרגול התוכנית ועוד.

13. להגדיר שמירת לוג פעולות במערכות אבטחת המידע ובמערכות המידע למשך 24 חודשים.
14. 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".
15. לבצע אחת לרבעון סריקת גישה בעזרת כלי אוטומטי כדי לאמוד את רמת החריות הקיימות בשרתי הספריות ולבצע טיפול מונע.
16. לבצע אחת לרבעון Vulnerability scanning (סריקת פגיעויות) בעזרת כלי אוטומטי (כגון Nessus ודומיה) כדי לאמוד את רמת המפגעים הקיימים ברשת ולבצע טיפול מונע.
17. ליידע את בעלי ההרשאות במאגר בדבר קיום מנגנון הבקרה.
18. לקיים דיון אחת לשנה לפחות באירועי אבטחה, ולתעד את הדיון באמצעות פרוטוקול.

התקנים ניידים

סעיף 12 לתקנות מחייב כי "בעל המאגר יגביל או ימנע אפשרות לחיבור התקנים ניידים למערכות המאגר במתכונת ההולמת את רמת אבטחת המידע שחלה על המאגר, את רגישות המידע, את הסיכונים המיוחדים למערכות המאגר או למידע הנובעים מחיבור ההתקן הנייד ואת קיומם של אמצעי הגנה מתאימים מפני סיכונים אלה; בעל מאגר מידע המאפשר שימוש במידע מהמאגר בהתקן נייד או העתקה שלו להתקן נייד ינקוט אמצעי הגנה בשים לב לסיכונים המיוחדים הקשורים לשימוש בהתקן נייד באותו מאגר מידע; לעניין זה יראו שימוש בשיטות הצפנה מקובלות כנקיטת אמצעים סבירים להגנה על מידע שהועתק להתקן הנייד".

בחברה לא קיים אמצעי למניעת חיבור התקנים ניידים. כך לדוגמה ניתן לחבר זיכרון נייד (Disk On Key) למחשבי החברה ולהוציא מהם מידע.

מסקנות

9. אי קיום מנגנון למניעת חיבור התקנים ניידים או להפעלת מערכת הלבנה חושף את החברה לסיכון להוצאת מידע רגיש או פרטי, ונוגד את החוק ותקנותיו.

המלצות

19. ליישם מנגנון למניעת חיבור התקנים ניידים לתחנות הקצה של החברה, או לחלופין להפעלת מערכת הלבנה מרכזית אשר תבדוק התקנים ניידים לפני שהם מוכנסים לרשת הארגונית, ובכך לצמצם את הסיכון להוצאת מידע רגיש או פרטי מהחברה.

אבטחת מערכות ותקשורת

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 שאותן מערכות מחוברות לרשת חיצונית. הסעיף מציין:

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

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

10. אי עדכון מערכות שונות מגביר את הסיכון לניצול חולשות אבטחת מידע. יתר על כן הדבר משקף אי עמידה של החברה בהוראות החוק והתקנות.

המלצות

20. להתקין כדרך קבע עדכוני אבטחה שונים.

גישת מיקור חוץ למאגרי המידע

ארגונים רבים מסתמכים על מיקור חוץ לקבלת שירותים כגון תמיכה במערכות מידע, חישובי שכר ועוד. נושא זה חושף את הארגון לסיכון שבו לאותו גורם חיצוני יש אפשרות לגשת למידע רגיש בארגון. לאור זאת, אבטחה שוטפת במהלך גישת מיקור חוץ לרשת הפנימית של הארגון הפכה להיות אחד ממנגנוני האבטחה החשובים.

סעיף 15 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 או מיפוי של ספקי החברה אשר יש להם אפשרות גישה מרחוק למאגרי המידע. חלק מהספקים מתחברים לחברה דרך VPN עם MFA למערכת מניפה, וחלק מתחבר דרך תוכנות כמו Anydesk.

לא נעשית בחברה סקירה תקופתית על ידי מנהל מערכות המידע לבדיקת חיבור הספקים באותה תקופה.

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

מסקנות

11. במצב שבו לא קיים תהליך סדור לעבודה עם ספקים המתחברים לרשת החברה, וכן לא נבחנים סיכוני אבטחת המידע בהתקשרות עם הספקים הנ"ל, לחברה אין "תמונה מלאה" של הסיכונים הטמונים בהתחברות מרחוק של ספקים.

המלצות

21. לגבש נוהל ספקי מיקור חוץ.

22. למפות את כל המערכות אשר הספקים ניגשים אליהן ולבנות תהליך עבודה סדור הכולל:

- קביעת רמת הסיווג של כל ספק (עד כמה הוא ניגש למידע רגיש, האם הוא שומר אצלו חומר של החברה וכו').
 - חיבור מאובטח של ספקים לרשת החברה.
 - בקרה על חיבור הספקים, ובכלל זה אישור חיבור מראש וכו'.
 - לבחון הטמעת מערכת הקלטות למערכות שאליהן מתחבר הספק.
23. לתאם סקר אצל ספק שזוהה שהחיבור שלו גורם לחברה 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, זיהה 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.

מבדיקת הביקורת עלה כי לא מבוצעת בחברה ביקורת תקופתית.

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 מידע ארגוניים, זיהוי סיכוני אבטחת מידע, ניתוח הסיכונים, דירוג הסיכונים ועוד, כל זאת כדי לגלות חשיפות פוטנציאליות של נכסי המידע הקריטיים בארגון לפגיעה.

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.

החברה ביצעה סקר סיכונים כללי, אשר בחלקו קיימת התייחסות לנושא אבטחת מידע וסייבר באופן מצומצם מאוד. כמו כן, לא קיימת תוכנית לטיפול בממצאים שעלו בסקר.

החברה מעולם לא ביצעה מבחני חדירה לרשת הארגונית.

מסקנות

12. אי ביצוע ביקורת תקופתית מקטין את יכולת החברה לשמור על רמת אבטחה, לרבות אבטחת המידע במאגרי המידע שלה. כמו כן, החברה מעולם לא ביצעה סקר סיכוני סייבר מפורט ומבחני חדירה הכוללים תוכנית טיפול בממצאים שעולים, דבר אשר מגביר את הסיכוי לכך שהחברה אינה יודעת את סיכוני הסייבר והפגיעויות הקיימות במערך אבטחת המידע והסייבר שלה, וגורם לה לא לעמוד בהוראות החוק ותקנותיו.

המלצות

24. לבצע ביקורת תקופתית אחת ל-24 חודשים לפחות ובהתאם לדרישות התקנות.

25. לבצע סקר סיכוני סייבר ומבחני חדירה אחת לתקופה כפי שתקבע החברה.

התייחסות החברה לנושא של "דלף מידע" ארגוני

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

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 עוין, מנגנוני AI ועוד.

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

לא קיימת הנחיה על אופן הוצאת מידע אל מחוץ לחברה ולא קיימת בקרה טכנולוגית על הוצאת מידע דרך מערכות הדואר האלקטרוני והאינטרנט.

מסקנות

13. חוסר בהנחיות או בנהלים להוצאת מידע אל מחוץ לחברה ולבקורות טכנולוגיות על הוצאת המידע, חושף את החברה לדלף מידע ארגוני ולאי עמידה בהוראות החוק ותקנותיו.

המלצות

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

תגובת המבוקרים

חברת עדן

בימים אלה חברת עדן שוכרת את שירותיה של חברת סייבר לצורך טיפול בפערים שהובאו לידיעתנו במסגרת הדוח.

בכוונת הנהלת החברה לבחון את הפערים שהוצגו ולטפל באופן מעמיק ויסודי בפערים ככל שהם קיימים.

בסיום ההליך נעביר לעיון הביקורת דוח פירוט תיקון הליקויים.

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.

חברת עדן היא יעד פוטנציאלי לניסיון תקיפות סייבר, בין היתר בשל היותה חברה 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 החברה.

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 שונים 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 עמידת החברה בהוראות החוק והתקנות, את המדיניות והנהלים בנושא אבטחת המידע, וכן ערכה מבדק טכנולוגי לבחינת רמת האבטחה הקיימת בחברה, בדיקה פיזית לאבטחת המידע ומבדקי חדירה לרשת החברה.

הביקורת העלתה ליקויים מהותיים לגבי יישום 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 (מערכת לניהול משתמשים) וליקויים בעלי חשיבות גבוהה במבדקי החדירה שביצעה.

על החברה 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 לחברה לעמוד בחובותיה הרגולטוריות, וכפועל יוצא להפחית את הסיכונים למיניהם מעצם התרחשות האירוע.

דוח שנתי 2024

הגנת הפרטיות, אבטחת מידע וסייבר בחברת עדן

אני מבקש להודות למבקרת 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 כר פורה למתקפות סייבר, בשל היקף השימוש שלהם במערכות מידע, בשל השימוש הרב שלהם באמצעים טכנולוגיים, בשל המידע הרגיש והרבה 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 העירייה 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.

הביקורת מצאה מספר ליקויים בהתנהלות חברת עדן בעניין זה ובכלל זה בנושא רגולציה, מדיניות, נהלים ותהליכים בתחום אבטחת מידע וסייבר. כך לדוגמה, נמצא כי החברה לא רשמה או רשמה באופן חלקי את מאגרי המידע שלה בהתאם לחוק הגנת הפרטיות, כמו כן נמצא כי בידי החברה לא קיימים מסמכים של הגדרות מאגרי מידע ושל מבנה מאגרי המידע וכי החברה לא מינתה באופן רשמי ממונה אבטחת מידע. כמו כן, נראה כי לחברה אין מדיניות ונוהלי אבטחת מידע וכי בחברה לא בוצע סקר סיכוני אבטחת מידע וסייבר ומבדקי חדירה. בנוסף לכך, הצביעה הביקורת על ליקויים בנושא בדיקות טכנולוגיות של אבטחת מידע וסייבר והתייחסה, בין היתר למערכת חומת האש ומערכת AD (מערכת לניהול משתמשים). כן, הביקורת הצביעה על כך שנמצאו ליקויים במבדקי החדירה הפנימיים והחיצוניים שבוצעו על ידה.

מעיון בדוח מבקרת העירייה בנושא זה, עולה כי חברת עדן קיבלה על עצמה להטמיע את המלצות הביקורת באופן מהיר. חברת עדן הודיעה כי שכרה את שירותיה של חברה המתמחה בתחום אבטחת מידע וסייבר לצורך טיפול בליקויים שעלו במסגרת הדוח. החברה העריכה את משך ביצוע התיקונים והרישום למאגרי המידע במספר חודשים, כך שהליקויים אמורים להיות מוסדרים במהירות. כמו כן, גורמי המקצוע מטעם חברת עדן התחייבו להעביר לעיון הביקורת דוח פירוט תיקון הליקויים. תגובה זו מעידה על רצון אמיתי לשיפור וטיוב התנהלות החברה בנושא זה לטובת הציבור.

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

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



הוועדה לביקורת – תמליל

מספר הוועדה : 22

מקום ההתכנסות : אולם חדר ישיבות קומה 0

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

מזכיר הוועדה בדיון : צבי אבו

שעת תחילת הוועדה : 12: 15

שעות סיום הוועדה : 15: 36

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:

שלום, שלום לכל החברים, אני מתכבד לפתוח את, דיון בוועדת הביקורת מספר 22, הגנת פרטיות, אבטחת מידע וסייבר בחברת עדן. אנחנו בעיצומו של, עיצומם של כמה דוחות ביקורת שבעצם בוחנות היבטים דומים בעניינים של סייבר ואבטחת מידע. בחנו שתי חברות, אנחנו בוחנים עכשיו את חברת עדן. מי שינהל את הדיון בעיקר זה שלומי, אני פחות מבין בתחום. אז אני מברך על הביקורת.

עפרה ברכה:

אז זהו, אני גם כן מברכת על זה שעשינו את הביקורת. נושא מאוד מאוד חשוב. כולנו כבר יודעים מה המשמעות של הנושא של הגנת הפרטיות, אבטחת מידע וסייבר. מה, מה הנזק שיכול להיגרם מתקפת סייבר כזו או אחרת, וכמה חשוב כל ההגנות וכל ההתנהלות בהתאם להוראות החוק. כמובן, כל מה שקשור להגנת הפרטיות ואבטחת מידע. אני אומר שבעדן באמת אחד המקומות שהרגשנו שטוב שעשינו את הביקורת, נכנסנו כאילו פרצנו לדלת פתוחה. היה הרבה מה לתקן, גם פה לבחור באמת יועץ חיצוני ותיכף תציגי כל מה שעשיתם, שלומי בבקשה.

אלדד רבינוביץ:

רק בעצם זה היה הדיון אם אפשר, יהיה שהוא יציג איזשהו נמצא. אתם תענו, כדי שנראה שאנחנו לא מפספסים דברים.

ליאת שמחיוף:

בסדר גמור.

עפרה ברכה:

לגבי הממצאים, לא,

אלדד רבינוביץ:

לא, יהיה על 100,

עפרה ברכה:

אנחנו הולכים רק על העיקריים.

אלדד רבינוביץ:

נדברים על המרכזיים,

שלומי בני:

12 ה מרכזיים,

עפרה ברכה:

כן, משהו ממש מרכזי. ומי הגברת?

הודיה בן גיגי:

אני אחראית אבטחת מידע, ואני ריכזתי את הנושא הזה בעיקר.

עפרה ברכה:

כן נכון, ראיתי אותך אז נראה לי שהיית בפגישות, (לא ברור).

הודיה בן גיגי:

כן,

שלומי בני:

את שוחחת איתי שלשום?

הודיה בן גיגי:

כן, אתמול,

שלומי בני:

אוקי,

הודיה בן גיגי:

איתך, דיברתי אחר כך עם כל הבוריס, עם כולם.

שלומי בני:

אוקי,

הודיה בן גיגי:

כי הם היו מעולים.

שלומי בני:

עם מי דיבר גם? עם בוריס?

הודיה בן גיגי:

בוריס, ו - ,

שלומי בני:

כבר הגעת לכולם, ואדם,

הודיה בן גיגי:

ואדם כן,

שלומי בני:

אוקי,

ליאת שמחיוף:

אני גם בשיעורי בית. אני אגיד גם בהמשך למה שעפרה אמרה, שהנושא הזה זוהה אצלנו בסקר סיכונים שנערך ממש ממש בסמוך לפתיחת הביקורת הזאת. אז זה ככה, ממש התחבר לנו. סקר סיכונים שעשינו אותו במהלך 22 גלש ל - 23 וזה אחד הדברים שזיהינו גם שם. היו לנו הרבה מאוד ממצאים ותוך כדי שהתחלנו לטפל בממצאים של הסקר אז גם הצטרפה הביקורת הזאת. אז שני הדברים ככה התאחדו לנו. נושא סופר קריטי, סופר משמעותי ובאמת לא כקלישאה. תמיד אומרים אנחנו מודים על דוחות הביקורת, אבל פה אנחנו באמת מודים על דו"ח הביקורת. זה היה מאוד מאוד חשוב עבורנו. וגם בסוף לקבל גם כלים ותעודות בתוך כל ההתנהלות של החברה יש דו"ח ביקורת, חייבים להתייחס לזה זה חייב לקרות עכשיו, ובאמת גם היינו בקשר עם אורטל, עם עפרה, ממש כאילו ממש עם כולם, כדי, שלומי וכל הטילים בחיפה. ככה להסתנכרן לאיזשהו מצב של מינימום ליקויים וכל דבר שעלה אנחנו נתנו לו מענה. יש כאן, אמרתי כ - 100 ממצאים, אתם רוצים לעבור על 12, אז מבחינתנו יש לנו תשובה להכל ובאמת סופר חשוב.

שלומי בני:

טוב, אז כולם מכירים, נראה לי. אבל משפט, שלומי בני מ - RSM שימוש חורג. אני ערכתי את הביקורת יחד עם הצוות שלי. בעצם הביקורת פה בוצעה בשני מישורים, תקנות הגנת הפרטיות כמו שאנחנו מכירים עם החוק וכולי. והחלק השני בדיקות, בדיקות טכנולוגיות כולל מבחני חדירה לרשת הארגונית. חברת עדן היא בעצם חברה לפיתוח כלכלי בירושלים, היא זרוע נוספת נקרא לזה של, של פיתוח, פיתוח ותרבות. למעשה, בעצם, כמו שציינתי קודם, בעצם המטרה פה הייתה שתי מטרות עיקריות אחת זה תקנות הגנת הפרטיות והחוק, והחלק השני זה בדיקה טכנולוגית ומבחני חדירה. אז בעצם לחברה בעצם לא היה מסמכים בכלל. כל עולם מאגרי המידע לא, לא נוהל, לא טופל בעצם. לא הגדרות מאגרים, לא מבנה מאגרים. זאת אומרת, זה בעצם כמו שלמדנו קודם, זה סוג של עבירה, סוג זה בעצם עבירה על החוק. בעצם כל חברה שיש לה מאגרי מידע מכמות מסוימת של רשומות. אנחנו לא ניכנס כרגע לכללים, אבל בגדול צריכה לרשום את מאגרי המידע שלה. ליאת, אתרוצה להגיד? כן.

ליאת שמחיוף:

אז אנחנו בעצם התחלנו בהכנה של, של הרישומים של, של מאגרי מידע. זאת אומרת, זה משהו שאמורים לרשום אותו במשרד המשפטים וכולי. אז אנחנו מיפינו את ה-, את מאגרי המידע שקיימים בחברה, ספקים, עובדים, מנויים שלנו בחניונים, יש לנו באמת כמה וכמה מאגרי מידע ואנחנו בתהליך של רישום, של המאגרים, והגופים.

אלדד רבינוביץ:

יש לך צפי? תוכנית עבודה מתי זה אמור (לא ברור)?

הודיה בן גיגי:

כן, אנחנו ממש בסוף, ראיתי שהיה המלצה בעצם עשו על, עם שני מערכות שבעצם שם יש לנו את מאגר מידע מניפה ו – SAP. אנחנו ממש בסיום על זה עם היועץ אבטחת מידע שלנו ואנחנו נשלח את זה,

ליאת שמחיוף:

זה יקרה כנראה, אנחנו ממש בסוף.

שלומי בני:

אני רק אגיד הערה, תראו, אנחנו כשאנחנו עושים ביקורת אנחנו מה שנקרא אומרים לפחות שני מאגרים או מציינים שני מאגרים שלא נרשמו. יכול להיות שיש שלושה. זאת אומרת, יכול להיות שיש לכם למשל מצלמות. אני לא בדקתי למשל את תחום המצלמות,

הודיה בן גיגי:

יש לנו, ואנחנו,

שלומי בני:

אז אתם צריכים. אתם צריכים למפות וגם פה יש שם למפות את דרישות הוראות החוק, כן? למשל מצלמות אז עד 29 ימים, כולל 29 היום לא חייב לרשום ומעל 30 יום כן צריך לרשום. אבל שוב אז לכן אנחנו לא נכנסים. אני גם לא בדקתי את מערכות ה – ORT, או מצלמות או בכלל זה. בדקנו את הרשת הארגונית. ולכן לתת לך לעשות מיפוי ולבוא להחליט אם יש לכם יועץ אבטחת מידע.

הודיה בן גיגי:

כן,

שלומי בני:

הוא אמור, הוא אמור לדעת את הדברים האלה, ואם לא.

הודיה בן גיגי:

יש לנו, ואנחנו על זה מאוד בחניונים, בעיקר כי יש לנו שם מלא.

שלומי בני:

מנויים?

הודיה בן גיגי:

פחות כן,

שלומי בני:

מנויים שזה אנשים.

ליאת שמחיוף:

המנויים הם בסוף רישומים, אז זה,

הודיה בן גיגי: כן,

ליאת שמחיוף:

כתבתם את זה כבר,

שלומי בני:

אוקי,

ליאת שמחיוף:

בהמלצה שלכם.

שלומי בני:

בסדר,

אלדד רבינוביץ:

אין בעיה, בעצם אתם תעשו עכשיו מיפוי, מיפוי,

ליאת שמחיוף:

אנחנו כבר,

אלדד רבינוביץ:

(לא ברור) ביצוע, אתם תוכלו בבקשה להודיע, אבל כשזה נרשם? עם העתק אלי? תודה רבה.

שלומי בני:

אוקי, הממצא השני זה בעצם ממונה אבטחת מידע, אבטחת מידע, אבטחת מידע וסייבר וכולה. גם בעצם לא היה ממונה וגם לא היה מדיניות, לא נהלים כתובים. צריכים שיהיה נהלים, גם אם אין ממונה אז לפחות שיהיו נהלים שיהיו כתובים ו - ,

הודיה בן גיגי:

כן, בזה אנחנו מאה אחוז, כבר בנינו,

ליאת שמחיוף:

זה כבר יושם,

הודיה בן גיגי:

יש כבר מעל חצי שנה, יש לנו כבר תוכנית עבודה, אנחנו שמה.

שלומי בני:

אחלה.

ליאת שמחיוף:

אוקי,

שלומי בני:

יש מינוי רשמי? מכתב?

הודיה בן גיגי:

יש מינוי רשמי.

אלדד רבינוביץ:

הוא מכין מסמכי מדיניות?

הודיה בן גיגי:

כן,

ליאת שמחיוף:

הוא הכין.

אלדד רבינוביץ:

תקפתם אותם?

ליאת שמחיוף:

כן, זה כן, זה אצלנו. הכול, אנחנו עובדים ממש, יש לנו שיחת סטאטוס, אנחנו עברנו על כל ההמלצות עם ה - ,

שלומי בני:

אוקי, מצוין.

הודיה בן גיגי:

לדעתי אבטחת מידע.

שלומי בני:

טוב, מדיניות סיסמאות ברשת ובמערכות האחרות. מדיניות סיסמאות ברשת,

הודיה בן גיגי:

כן,

שלומי בני:

שיניתם אותה?

הודיה בן גיגי:

כן, כן, בטח. זה ה - IT שלנו. צוות IT, חברת גלובאל בטח עשיתם את זה, שינינו את זה. אני אומרת לך אני ישבתי עם ה IT שלנו. ואנחנו כן, כתוב שזה שונה.

ליאת שמחיוף:

כן, הקשחנו את המדיניות, סיסמאות וגם את התחלופה של הסיסמאות. לא יודעת אם זה זה או שורה אחרת, אבל,

שלומי בני:

כן, יש לנו מדיניות סיסמאות זה אורך, מורכבות.

ליאת שמחיוף:

כן, זה גם האורך,

הודיה בן גיגי:

כן, כן,

ליאת שמחיוף:

וגם התחלופה,

שלומי בני:

גם במערכות וגם ברשת.

ליאת שמחיוף:

כן.

שלומי בני:

אוקי, ניטור לוגים, בעצם גם התקנות וגם הרבה בסט - פרקטיס דורשים שיהיה לנו לוגים לפחות 24 חודשים, על מנת שנוכל לתחקר אירועים, במידה והיו,

הודיה בן גיגי:

כן,

שלומי בני:

אז,

הודיה בן גיגי:

לא היו לנו 24 חודשים.

שלומי בני:

נכון,

הודיה בן גיגי:

היה לנו 12 והעלינו את זה. ויש לנו גם, בטח זה יהיה גם בהמשך, יש לנו סימסוג שהבאנו מערכת ניטור, אז במיוחד הם שומרים את הלוגים שלנו.

שלומי בני:

מצוין,

הודיה בן גיגי:

כן,

אלדד רבינוביץ:

הוספתם המערכת שלא הייתה לכם.

הודיה בן גיגי:

כן,

ליאת שמחיוף:

כן,

שלומי בני:

זה בעצם מערכת שאוספת לוגים מכל מיני מערכות ושומרת אצלה,

הודיה בן גיגי:

כן,

שלומי בני:

וגם היא עושה כל מיני בדיקות. המערכת הזאת זה הסימסוג שהיא תיארה פה. תוכנית להמשכיות עסקית והתאוששות מאסון, התוכנית להמשכיות עסקית זה לא גרידא מערכות מידע, זה יותר גם ביזנס זה, והתאוששות מאסון בהיבט של מערכות מידע.

הודיה בן גיגי:

אני אבדוק שנייה אחת,

ליאת שמחיוף:

זה הנוהל IRP הזה ש - , שכתבנו.

שלומי בני:

יש, DRP,

הודיה בן גיגי:

כן,

שלומי בני :

ויש BCP.

ליאת שמחיוף :

לא, IRP. קיים נוהל,

הודיה בן גיגי :

גם BCP קיים,

ליאת שמחיוף :

אסון, נוהל להתמודדות עם אירועים, עם אירועי סייבר, ה – BCP וההמשכיות עסקית.

שלומי בני :

כן,

ליאת שמחיוף :

יש לי שני הנהלים האלה ביחד.

שלומי בני :

עשיתם אותם?

הודיה בן גיגי :

כן, כן,

אלדד רבינוביץ :

מי כתב לכם אותם בעצם?

ליאת שמחיוף :

החברת סייבר,

שלומי בני :

החברת סייבר?

ליאת שמחיוף :

את הסעיפים שהם כאילו,

הודיה בן גיגי:

איתם, יועץ עסקי.

אלדד רבינוביץ:

הבנתי, יועץ חיצוני.

ליאת שמחיוף:

כן, יועץ חיצוני,

עפרה ברכה:

זה חברה שהתקשרתם איתה בעקבות הדו"ח?

ליאת שמחיוף:

כן,

עפרה ברכה:

כי כל זה, גם היו,

שלומי בני:

כן,

ליאת שמחיוף:

כן, כן,

עידו הרשקוביץ:

אני לא יודע אם נאמר או לא נאמר, אבל אתם נכנסתם לבקרה של הדבר הזה. בדיוק התחלנו כבר להתחיל לחשוב איך עושים את זה, ואני רוצה להגיד פה תודה גם לכם, כי האצתם לנו את כל ה - ,

עפרה ברכה:

כן, זה היה מאוד,

עידו הרשקוביץ:

מה שנקרא את כל הזה נתתם לנו באמת,

ינון נוימן:

רעיונות גם,

עידו הרשקוביץ:

כי זה עולם ועוד, ואני אגיד את האמת, אני לא מבין את זה, אמיתי.

אלדד רבינוביץ:

אתה יושב בצד הנכון.

עידו הרשקוביץ:

מדברים פה סינית, אני אפילו לא יודע איפה אני יכול להיכנס בכלל, אני אומר בקצה.

עפרה ברכה:

יש (לא ברור).

עידו הרשקוביץ:

אני יודע שזה אירוע סופר חשוב, סופר,

עפרה ברכה:

נכון,

עידו הרשקוביץ:

סופר סופר חשוב, וזה שבאתם ונכנסתם עם הבקרה זו אחת הבקורות הטובות שנעשו לנו לחברה,

ינון נוימן:

ביקורת,

עפרה ברכה:

ביקורת.

עידו הרשקוביץ:

וביקורת, ואנחנו מיישמים את זה באהבה, ובמה שנקרא ברצון. צריך להגיד פה תודה גם להודיה ולליאת הודיה שהובילה ככה את כל הדבר הזה.

ליאת שמחיוף:

תהליך מאוד

עידו הרשקוביץ:

כן, תהליך ארוך, סייזיפי וטוב וחשוב. זהו, זה מה שיש לי להגיד ב - ,

ליאת שמחיוף:

תודה.

עידו הרשקוביץ:

ומבחינתי כאילו אני כמנכ"ל נותן יד חופשית לכל מה שקשור להיבט הזה. אני רואה את זה כמו ביטחון שאני נותן יד חופשית לכל מה שקשור לביטחון, בפרויקטים ובדברים שאנחנו עושים. אותו דבר אני רואה פה. זה מה שאמרתי גם להם. כל מה שקשור לביטחון מידע כל זה מבחינתי מה שצריך להשקיע, תשקיעו. אני לא חוסך בזה. אני לא,

ליאת שמחיוף:

כן, מעבר גם לאור כל מתקפות הסייבר בשנה האחרונה ש –

עידו הרשקוביץ:

כן,

ליאת שמחיוף:

אינסופי. אנחנו מקבלים פקסים, אני לא יודעת גם אתם, אבל מכל מיני ארגונים לשחרור, לא? אתם לא מקבלים? פעם בשבוע אנחנו מקבלים,

עפרה ברכה:

שולחים, נגיד שאנחנו הלכנו לעזור.

ליאת שמחיוף:

פקסים יפה.

שלומי בני:

טוב. התקנים ניידים דיסק און קידוחים, בעצם לא היה מנגנון למניעה של חיבור,

הודיה בן גיגי:

נכון. כרגע יש לנו עדיין אפשרות של חיבור. לא מנענו, אבל אנחנו באמצע תהליך עם הסימסוק. הם גם העלו לנו את זה ואנחנו בתהליך כזה. אני לא אגיד לך שאין לנו עדיין כי אנחנו רוצים, כי יש לנו כמה מחשבים שכן יצטרכו, אז הם מורשים, הם יעשו אותם בנפרד כמו שרת בנפרד, ואז הם יוכלו, ומי שירצה ילך מקסימום למחשב הנוכחי. אז כרגע, אבל זה (לא ברור).

שלומי בני :

נכון, נהוג לעשות.

אלדד רבינוביץ :

זה נקרא הלבנה מה ש - ,

שלומי בני :

סוג של.

אלדד רבינוביץ :

כן, זה.

שלומי בני :

סוג של הפרדה יפרידו 3, 4 מחשבים מתוך כל העשרות מחשבים האחרים של הארגון, שאם אתה רוצה דיסק און קי אתה ניגש לשמה, ואז שם עושים כל מיני פעולות כדי לבדוק שסוג של הלבנה.

ליאת שמחיוף :

אצלנו לפעמים, נניח, מגישים במכרזים את כל החומר על דיסק און קי. זאת אומרת, זה עיקר השימוש, ואז זה באמת משהו שמגיע ממקור חיצוני ואתה כן רוצה לוודא שלא הכנסת איתו,

אלדד רבינוביץ :

וסריקה לא מספיקה, סריקה של הדיסק און קי, כתנאי להפעלה שלו.

שלומי בני :

לא, לא, זה לא מספיק,

ליאת שמחיוף :

זה לא מספיק.

שלומי בני :

זה לא מספיק טוב. זה בקרה אחת מתוך שלושה ארבעה בקרות שהייתי מצפה. אגב, למה אתם לא משתמשים בהעלאה של קבצים דרך פורטל או משהו? למה?

הודיה בן גיגי :

אנחנו אגב, אנחנו זה גם תהליך שאנחנו נעשה. אנחנו עדיין.

שלומי בני :

זה לא קשור לאבטחת מידע, זה סתם שאלה.

ליאת שמחיוף :

זה מורכב, אתה מדבר על הגשה מקוונת של (לא ברור)?

עפרה ברכה :

כן, כן,

ליאת שמחיוף :

זה מורכב. ובוא נגיד שאנחנו בניגוד לחברה הקודמת שישבתם איתם קודם, חברת מוריה עובדת עם קבלני ענק. אנחנו לפעמים עובדים קבלנים.

שלומי בני :

קטנים יותר,

ליאת שמחיוף :

יותר קטנים,

שלומי בני :

ואז יותר קשה להם לעלות?

ליאת שמחיוף :

מה זה קשה להם? לא יודעים איך להתעסק עם הדברים האלה.

שלומי בני :

ובין דיסק און קי הם יודעים להתעסק?

ליאת שמחיוף :

זה, זה יותר קל כי אתה נותן להם,

עפרה ברכה :

הוא שומר את החומר,

ליאת שמחיוף :

איזה שהיא התוכנה לא יודעת. תוכנה של מחירון דקל והם, כאילו, הם יודעים לתמחר את זה על התוכנה הספציפית, אבל עכשיו, זה מאוד מאוד מורכב לצד המגיש לעשות הגשה מקוונת וזה גם ברישיונות וכולה. אז בחנו את זה, ולאור סביבת העבודה שלנו,

אלדד רבינוביץ:

הפתרון שמוצע הוא טוב בעיניך? להקצות מחשבים ספציפיים לזה.

שלומי בני:

כן, זה פתרון טוב.

אלדד רבינוביץ:

והמחשבים האלו צריכים להיות מנוטרים בצורה יותר משמעותית מאחרים,

שלומי בני:

יותר משמעותית מאשרים אחרים,

אלדד רבינוביץ:

לעשות איזה שהוא מגבלת גישה ביניהם לבין הרשת.

שלומי בני:

נכון, בגלל זה הם עושים את ההפרדה.

אלדד רבינוביץ:

מצוין. מערכות הפעלה בתחנות הקצה בכלל, דיברנו על סליחה. גם מערכות הפעלה, גם עמדות הקצה וגם וגם השרתים. דיברנו רק במשפט שאנחנו מצפים שיהיו לנו עדכוני אבטחת מידע שוטפים, על כל המערכות הפעלה שלנו. בגלל שמידי פעם מוצאים חולשות במערכות ה - במערכות ההפעלה, ומצאנו שהיו פה לא מעט מקרים שלא בוצעו עדכוני אבטחת קריטיים, זאת אומרת, זה ממש פרצות שהתגלו על ידי מיקרוסופט. הם הוציאו שחרור של גרסה מעודכנת ואתם לא התקנתם אותם.

הודיה בן גיגי:

נכון, אני יכולה להגיד לך שיש על זה יותר. זאת אומרת יש לנו IT שמגיע פעמיים בשבוע, לפחות פעם בשבוע הוא עובר על כל המחשבים. מי שלא מעדכן, דבר ראשון בהדרכה, כן הוא מדריך כל פעם שכל פעם שיש עדכוני אבטחת מידע לעדכן, שזה לא יהיה הכתום הזה למטה ואף אחד לא מתייחס אליו. אז כן, יש עדכונים והוא מעדכן הוא עובר ממש על כל העמדות, בודק שיש עדכונים והבנתי ממנו שגם יש לנו מערכות הפעלה כמו אלה שאינם נתמכות. אז גם יש להם, הוא התקין דרך (לא ברור), הוא נתן את זה,

אלדד רבינוביץ:

זה לא אמורה להיות אוטומטי, אי אפשר לתת הגדרה שזה אוטומטי?

שלומי בני:

בגדול לא, בגדול לא. בגדול לא, אתה יכול לעשות שזה יחסום אותך מלהיכנס אם אין לך מערכת הפעלה עדכנית, אבל לפעמים יש כל מיני עדכוני, עדכונים שהם קטנים, פיצורים כן, קטנים. אז אתה לא רוצה לחסום עכשיו את כל המשתמשים, בגלל שיש איזשהו פיצור שהוא, שהוא קטן, אז אתה צריך להיות בתור מנהל IT לעקוב ולראות מתי יש עדכונים קריטיים ואז לאכוף אותם ולא.

אלדד רבינוביץ:

מנהל IT שיש לנו הוא חיצוני.

ליאת שמחיוף:

כן, זה חברה האחות של החברה של הסייבר. זאת אומרת זה חברות קשורות, אבל הם גם מסונכרנות,

הודיה בן גיגי:

עובדות בשיתוף פעולה הוא מגיע פעם,

ליאת שמחיוף:

פעמיים.

הודיה בן גיגי:

יש לנו גם ישיבת גם צוות כל ה It סייבר פעם בשבוע,

שלומי בני:

אוקי,

הודיה בן גיגי:

אז יש פה, אנחנו מוציאים על זה.

שלומי בני:

זה נושא שהוא מאוד חשוב, כי זה בעצם זה לא עולה כסף וזה מצמצם לי משמעותית את הסיכון.

הודיה בן גיגי:

כן.

שלומי בני :

זה מסוג ההמלצות שאנחנו אוהבים. זה המלצות של הגדרות ופעולות של כמה, של כמה דקות. רגע,

הודיה בן גיגי :

אני יודעת שזה,

שלומי בני :

רגע, סליחה. זהו, ביצוע ביקורת תקופתית. אז דיברנו קודם על רישום, מאגרים וכולה. אז לא בוצע ביקורת תקופתית של תקנות הגנת הפרטיות. צריך לעשות את זה אחת ל 24 חודשים.

אלדד רבינוביץ :

השארתם בסקר, אבל עדיין.

ליאת שמחיוף :

לא עשינו סקר סיכונים לפני ה - ,

הודיה בן גיגי :

לפני הביקורת.

ליאת שמחיוף :

לפני הביקורת הזאת, אז ממש זה גם,

הודיה בן גיגי :

כן חלק מהייעוץ. אבטחת מידע שלקחנו אז זה בתוכנית העבודה, אחת לשנה או אחת ל 24 חודשים, אנחנו נעשה ניהול סיכונים, ומשהו של,

שלומי בני :

וביקורת תקופתית ספציפית על התקנות צריך. אוקי,

הודיה בן גיגי :

כן,

שלומי בני :

זה לא, זה לא כללי של נושא של סייבר, ספציפית היא יישום, שניתן לראות שם מאגרי מידע מעודכנים, לראות שהנהלים.

הודיה בן גיגי:

כן,

דני:

אגב גם התקנות יכולות, גם התקנות יכולות להשתנות מדי שנה.

שלומי בני:

נכון,

דני:

אתם צריכים לראות אולי השינוי ולעמוד בו,

שלומי בני:

ויש שינוי, ראשון לאוגוסט תיקון 13, תדברו עם היועץ אבטחת מידע שלכם,

ליאת שמחיוף:

כן,

שלומי בני:

הוא בטח מכיר, יופי.

ליאת שמחיוף:

בהגנת הפרטיות?

שלומי בני:

כן. בגדול זה לא שינה הרבה, אלא יותר את יכולות האכיפה של הרשות. בסדר?

הודיה בן גיגי:

כן,

שלומי בני:

זאת אומרת מה שהם יכולים להשיט, בגדול, השינויים הם פחות נוגעים אליכם, אבל תתייעצו איתו זה הכי טוב,

הודיה בן גיגי:

כן,

שלומי בני:

בסדר. סקרי סיכונים, מבדקי חדירה, אלו שני כלים שבעצם אנחנו מאוד אוהבים, כי בעצם הם אומרים לנו מה, מה רמת האבטחה. אז בעצם החברה לא ביצעה מעולם סקר סיכוני אבטחת מידע וסייבר או מבדקי חדירה.

הודיה בן גיגי:

אז דבר ראשון מבדק חדירה, סקר סיכונים כבר בוצע עכשיו, מבדק חדירה גם, אחרי שלקחנו את היועץ אבטחת מידע והכול, אז,

ליאת שמחיוף:

גם אתם עשיתם את זה, סקר חדירה,

שלומי בני:

נכון,

ליאת שמחיוף:

ביחד, עם נכון?

שלומי בני:

נכון, אנחנו עשינו, אבל זאת אומרת,

עפרה ברכה:

כן, בטח.

שלומי בני:

עד שאנחנו עשינו אף אחד לא עשה, אז בגלל זה הממצא,

ליאת שמחיוף:

לא, אז עשו אחר כך עוד פעם,

הודיה בן גיגי:

זה חלק מהזה, אז זה,

אלדד רבינוביץ:

עשו והממצאים הם ש - ?

הודיה בן גיגי:

האמת שאני הייתי בחופשת לידה. אני לא יודעת להגיד לך בדיוק,

עפרה ברכה:

מזל טוב.

הודיה בן גיגי:

תודה אז, אבל הוא שלח לי את זה. אני יכולה ל –

ליאת שמחיוף:

לא, אני חושבת שזה היה, אני חושבת שזה היה,

הודיה בן גיגי:

אבל אני מאמינה שאם היה משהו,

ליאת שמחיוף:

היה תקין בזה, תכף אני אראה. פשוט יש לי פה כל כך הרבה שורות.

שלומי בני:

כן, זה גם לא באותו סדר כמו אצלך.

הודיה בן גיגי:

בסדר.

ליאת שמחיוף:

אני מנסה להבין באיזה אחד מהם זה ה - .

שלומי בני:

מה שחשוב זה את הממצאים ברמה גבוהה. פשוט לתקן אותם תוך שלושה חודשי בדרך כלל.

ליאת שמחיוף:

אני יכולה לרשום את זה בדרך כלל.

שלומי בני :

אז פה אנחנו לקחנו סל של כל מיני. הרי בסוף אמרנו יש לנו פה איזה 100, 100 ממצאים,

ליאת שמחיוף :

98,

שלומי בני :

98 ליתר דיוק. אז לקחנו פה ממצא אחד משמעותי שהוא כל מיני הגדרות והקשחות שהיינו מצפים שיהיו, רובם, רובם לא עולים כסף. אוקי, אז ששוב פעם אנחנו מאוד אוהבים את הממצאים האלה שלא אוהבים,

אלדד רבינוביץ :

פשוט שלא

שלומי בני :

כן, בדיוק כשיש שלושה ימי עבודה של האיש IT והוא פותר 450 ממצאים. אז זה בעצם הרשימה שיש אצלך, הוא בחלקה, אז תגידו באופן כללי.

אלדד רבינוביץ :

הגדרות בעצם עשיתם.

הודיה בן גיגי :

כן. כשעברנו עם ה It והיועץ אבטחת מידע על כל ההמלצות. זאת אומרת באמת עברנו אחד אחד, זה כל התקופה הזאתי לא נחנו. באמת עברנו איתם את הכל כמעט עשינו, אני יכולה להגיד לך, אולי שזה שני דברים שזה בתהליך או משהו כזה. כאילו אנחנו, בוא נגיד אנחנו יודעים הכול, אנחנו מבינים הכל ושינינו את הדברים שצריך.

ליאת שמחיוף :

אני אגיד שאפילו ההדרכה של, בנושא של אבטחת מידע היא תואמה ל - 22 ביוני, שיא המתקפה. אנשים במקלטים ולא ביטלנו, זאת אומרת, כולם עלו, כל אחד עם ה - ,

שלומי בני :

זה הזמן הכי טוב. כולם יהיו,

אלדד רבינוביץ :

יש מה לעשות.

שלומי בני :

יש מה לעשות.

ליאת שמחיוף :

הם אמרו לא דוחים את זה, זאת אומרת, זה משהו שנקבע ביומנים. כל העובדים עלו כולל אנשים ממילואים. זאת אומרת, זה היה ממש חובה לכולם. בגלל באמת לאור החשיבות שראינו כמו ש - , עידו גם נכנס ואמר ומה שנקרא לא, לא היינו מסונכרנים בפתיח הזה, אבל.

הודיה בן גיגי :

אני רק רוצה סתם להבין בכללי, יש רמה מסוימת של דחיפות של, כאילו זאת אומרת יש המלצה בינונית, המלצה פחות?

שלומי בני :

אז אני אגיד מה שאתם ראיתם בדו"ח בממצאים מרכזיים והמלצות מרכזיות יש שם באיזה 12, 13,

הודיה בן גיגי :

כן,

שלומי בני :

זה, זה הרמה דחיפות הגבוהה ביותר. צריך לקחת בחשבון שכל מה שהוראות חוק זה צריך לעשות מידי כי שם אני לא יכול להיות 9, אני צריך להיות 10.

ליאת שמחיוף :

בהוראות חוק אנחנו השלמנו הכול,

הודיה בן גיגי :

כן,

ליאת שמחיוף :

גם חתמנו. דרך אגב היינו צריכים את זה בשביל מאגרי מידע לחניונים, הרי אנחנו מעניקים הנחות לתושבי, לאני ירושלמי, כדי לקבל את מאגר המידע ולתת אותו למערכות שלנו. היינו צריכים לחתום על הצהרה של אבטחת מידע וכל ה - , שאנחנו באמת עומדים בכל התקנות והוראות החוק. בוא נגיד כשקיבלנו את ההצהרה הזו לא יכולנו לא יכולנו לחתום עליה. זה פשוט הכול הסתנכרן לאותו, לאותו מסלול וחתמנו עליה לפני, לא יודעת חודש, חודש ומשהו אז,

שלומי בני:

לא דיברתי איתי על ההצהרה הזאת לפני.

ליאת שמחיוף:

נכון, כי זה, זה פשוט הכול, הכול הסתנכרן לאותו לאותם, לאותו מסלול שפשוט חייבים לטפל בנושא הזה. אני אגיד גם כאילו אמרת איזשהו פתיח על עדן, אז עדן זה חברה שסך הכול 28 עובדים אז, אז יש דברים שהם לא, לא בליבת העשייה הזאת, לפעמים כאילו לא כל כך נותן להם דגש. וזה, זה היה סופר באמת סופר חשוב, הדוח הזה ובכלל הטיפול בנושא הזה.

שלומי בני:

טוב, היו ממצאים במבדק הפנימי והחיצוני, זה גם חלק מהקחשות, אני מניח שגם בזה עם תיארותם שאתם,

ליאת שמחיוף:

כן,

שלומי בני:

נכון שגם כן.

הודיה בן גיגי:

כן, הוא כתב,

ליאת שמחיוף:

כן בהקשחות טיפלנו כן,

שלומי בני:

אם אני אסכם בגדול מהצד שלי, אז השתמש אדוני במונח טעון שיפור, זה היה טעון שיפור. זאת אומרת, היו הרבה מאוד ממצאים, ואם אני שם את זה בנושא של הוראות חוק שזה גם משמעותי, ועושה רושם שנעשתה פה עבודה, אני יודע גם שהם יצרו איתי קשר, אמרתי שלשום אפילו גם דיברנו, ולפני זה עוד דיברנו. אז כנראה שאנשים פה עובדים, אז כנראה שעובדים.

הודיה בן גיגי:

האמת שבעקבות זה אפילו הלכתי ללמוד DPO ואבטחת מידע, שזה מאוד מעניין, אז שזה גם מאוד מעניין וגם מאוד מאוד מבחינתי,

ליאת שמחיוף:

רלוונטי.

הודיה בן גיגי:

רלוונטי, אז כן,

ינון נוימן:

את המבחנים את עשית?

שלומי בני:

גם החברה הרוויחה.

ליאת שמחיוף:

ביחד עושים.

הודיה בן גיגי:

אני אעשה,

שלומי בני:

את הרווחת והחברה הרוויחה.

עידו הרשקוביץ:

כן, כן, כן.

שלומי בני:

נכון?

עידו הרשקוביץ:

חד משמעית.

עפרה ברכה:

טוב אז פעם נוספת היום שאנחנו רואים שקלענו בול בנושא, ממש התפרצנו לדלת פתוחה, ומנגד החברה לוקחת את זה בשתי ידיים וזה הופך להיות תוכנית עבודה. ליאת ממש התקשרה אליי בסמוך לבדיקה או לדו"ח כבר וסיפרה לי מה הם מתכוונים לעשות. שאלה מה התהליך, אז באמת אני אברך את הרצינות הזאת. זה מבחינתי הישג לביקורת שאנחנו גם בוחרים נושא טוב, וזה גם מתיישב לכם טוב עם תוכנית העבודה ועם הצרכים, וגם בסוף לוקחים ונושא חשוב מאוד שלוקחים

את זה בשתי ידיים ועושים ומתקנים ויש פה איזשהו תהליך אז באמת מברכת עליו ולהמשיך עם זה.
אתם יודעים, הנושא זה רק הולך ומתפתח,

ליאת שמחיוף:

כן,

עפרה ברכה:

אז אנחנו צריכים להיות על זה מה שנקרא. ותודה רבה לכם. תודה רבה לשלומי.

שלומי בני:

תודה רבה.

אלדד רבינוביץ:

לאנשי הביקורת.

אלדד רבינוביץ:

יש עוד מישהו שרוצה לסכם? טוב, אז באמת מטרת הביקורת זה להאיר פינות אפלות וזה לייצר תהליכי עבודה, והביקורת הזאתי נראה שבאמת כמו שאמרתם, הסתדרו הכוכבים. באה במקום, שאתם התחלתם להסתכל עליה וקיבלתם שירות מאוד מקצועי. אני חושב ששלומי, שבאמת יודע להסתכל טוב ויודע לבחון ויודע לעזור לכם להכווין אתכם למקום הנכון. אז באמת הביקורת כאן עשתה את עבודתה בצורה מצוינת. אז תודה למבקרת ותודה לשלומי, ותודה לכם שלקחתם את זה ברצינות. בסופו של דבר הושקע כאן עמל מאוד גדול ופה בתהליכי ביקורת, וכשזה מתקבל באהבה ובשמחה ונהפך לתהליך עבודה, זה באמת נותן, נותן, נותן ערך והכל מתקבל בהתנגדות. אז זה באמת נהיה, נהיה לא נעים ומיותר ואתם קיבלתם את זה בצורה הטובה. והשתמשתם בזה, אז באמת אני מברך, מברך אתכם, אני רק אסיים בנוסח הנדרש. אני מקבל את המלצות דוח בכפוף להערות הנוספות לעיל, ממליץ למועצה לאמץ את מסקנות הוועדה. הישיבה נעולה.

שלומי בני:

תודה רבה.

אלדד רבינוביץ:

תודה רבה רבה.

עפרה ברכה:

בהצלחה.

סיום הדיון