כ״ט בחשון תשפ״ו
20 בנובמבר 2025
סימוכין: 2025-103-958

<u>דו״ח מישיבה מס׳ 22 של ועדת ביקורת</u>
<u>שהתקיימה ביום שני, י״ח בתמוז תשפ״ה (14.7.2025)</u>

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

נכחו: גב׳ עופרה ברכה, מבקרת העירייה
מר ינון נוימן, מנהל אגף לביקורת ובקרת יועצים
עו״ד דני ליבמן, משנה ליועמ״ש לנושאים מיוחדים
גב׳ אורטל אריה, מנהלת מחלקה בכירה לפיתוח תכנון ובקרה
עו״ד רונן יאס, עוזר ראשי ליועמ״ש
מר אהרן כהן, כלכלן תקציבים בכיר
גב׳ ליאת שמחה יופי, סמנכלי״ת כספים בחברת עדן
גב׳ הודיה בן גיגי, אחראית אבטחת מידע בחברת עדן
רו״ח שלומי בני, יועץ הביקורת
מר צבי עבו, מזכיר ועדת ביקורת

<u>על סדר היום:</u>

דוח מבקרת העירייה בנושא: אבטחת מידע וסייבר בחברת עדן

<u>פתיחת הדיון:</u>

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

<u>גב׳ עופרה ברכה, מבקרת העירייה</u>: 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.

<u>דיון הוועדה:</u>

פרק 1:
<u>המלצת המבקרת</u>:

- למפות ולרשום את מאגרי המידע הנדרשים לרישום בהתאם לחוק ותקנותיו וכן לקבוע את רמת אבטחת המידע הנדרשת 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.

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

- 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 החריגות הקיימות בשרתי הספריות ולבצע טיפול מונע.
- לבצע אחת לרבעון Vulnerability scanning (סריקת פגיעויות) בעזרת כלי אוטומטי (כגון Nessus ודומיה) כדי לאמוד את רמת המפגעים הקיימים ברשת ולבצע טיפול מונע.
- ליידע את בעלי ההרשאות במאגר בדבר קיום מנגנון הבקרה.
- לקיים דיון אחת לשנה לפחות באירועי אבטחה ולתעד את הדיון באמצעות פרוטוקול.
- 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 ידה.
- לגבש נוהל ספקי מיקור חוץ.

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

- 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.
- 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 סיכוני 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 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.
- לבחון שימוש במנגנון DLP - Data Loss Prevention Software (מערכות למניעה של דלף מידע) במערכות הדואר האלקטרוני והאינטרנט.

<u>תגובת המבוקר:</u>
מודים על דוח הביקורת, מאגרי המידע מופו וכעת בהליך רישום. אנו עובדים עם יועץ אבטחת מידע על כל ההמלצות, רובם כבר בוצעו.

<u>המלצת ועדת ביקורת:</u>
לקבל את המלצות המבקרת.
בנוסף, בתוך 30 ימים חברת עדן תשלח עדכון למבקרת וליו"ר ועדת הביקורת בנוגע לרישום מאגרי המידע והשלמת יישום ההמלצות.

פרק 2:
<u>המלצת המבקרת:</u>

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

<u>תגובת המבוקר:</u>
בוצע או בתהליך טיפול.

<u>המלצת ועדת ביקורת:</u>
לקבל את המלצות המבקרת.
בנוסף, בתוך 30 ימים חברת עדן תשלח עדכון למבקרת וליו"ר ועדת הביקורת בנוגע השלמת יישום ההמלצות.

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

פרק 3:
<u>המלצת המבקרת:</u>

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

<u>תגובת המבוקר:</u>
רוב ההמלצות מומשו או בתהליך.

<u>המלצת ועדת ביקורת:</u>
לקבל את המלצות המבקרת.
בנוסף, בתוך 30 ימים חברת עדן תשלח עדכון למבקרת וליו"ר ועדת הביקורת בנוגע לרישום מאגרי המידע והשלמת יישום ההמלצות.

פרק 4:
<u>המלצת המבקרת:</u>

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

<u>תגובת המבוקר:</u>
בבחינה או בטיפול.

<u>המלצת ועדת ביקורת:</u>
לקבל את המלצות המבקרת.
בנוסף, בתוך 30 ימים חברת עדן תשלח עדכון למבקרת וליו"ר ועדת הביקורת בנוגע לרישום מאגרי המידע והשלמת יישום ההמלצות.

<u>סיכום:</u>
<u>מר אלדד רבינוביץ, יו"ר הוועדה</u>: 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 למבקרת 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

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