כ״ט בחשון תשפ״ו
20 בנובמבר 2025
סימוכין: 2025-103-956

<u>דו״ח מישיבה מס׳ 20 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 אורי מנחם, מנכ״ל חברת אריאל
מר אילן גפני, יועץ מערכות מידע של חברת אריאל
מר מודי בן אבו, מנהל מחשוב בחברת אריאל
גב׳ דבורה מלמד, תקציבנית בחברת אריאל
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 אריאל

<u>פתיחת הדיון:</u>

<u>מר אלדד רבינוביץ, יו״ר הוועדה</u>: הסייבר והגנת המידע אלו תחומים מתפתחים ומשמעותיים. בשנים האחרונות קיימת הכרה כי זהו אחד האיומים המשמעותיים ברמה הלאומית, ובתקופה של המלחמות עולמיות כנגד מדינות וקבוצות רבות עוצמה יש לו חשיבות גוברת. אני מברך על הדוח הזה ומקווה שהתוצר שלו יהיה מוגנות גוברת של כולנו.

<u>הגב׳ עופרה ברכה, מבקרת העירייה</u>: אנו בביקורת זהינו שהזירה הבאה שגוף כמו עיריית ירושלים צריך להתמודד איתה זה תחום הסייבר. בשנת 2024 ערכנו בכל התאגידים עירוניים ביקורת בנושא אבטחת מידע, הגנת הפרטיות וסייבר, לפי הצורך במתכונת שונה. בחברת באריאל, נראה שזה דבר טוב שנעשה. המצב לפני הדוח היה חשוף אך חברת אריאל במהלך הדיונים לקחה את הדוח בשתי ידיים. החברה עשתה תהליך תיקון ליקויים רציני.

<u>דיון הוועדה:</u>

פרק 1:

<u>המלצת המבקרת:</u>

- למפות ולרשום את מאגרי המידע הנדרשים רישום בהתאם לחוק ותקנותיו, וכן לקבוע את רמת אבטחת המידע הנדרשת מכל מאגר מידע 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.
- על החברה למנות באופן רשמי (באמצעות כתב מינוי) ממונה אבטחת מידע אחד (במידת הצורך, הממונה יקבל ייעוץ והכוונה מחברה אשר מתמחה בתחום אבטחת מידע והוראות החוק) אשר יפעל לכל הפחות ליישום משימות אלה בהתאם להוראות התקנות:
  - יהיה אחראי לכתיבת נוהלי אבטחת מידע ויביאם לאישור מנהלי המאגרים.
  - יכין תוכנית לבקרה שוטפת על עמידה בדרישות התקנות, יבצע את התוכנית ויעדכן את בעל המאגר ומנהלו לגבי הממצאים שנמצאו.
- לבחון ולבדוק את תוכנית העבודה של היועץ החיצוני בתחום אבטחת המידע, את המשימות שניתנו לו ואת רמתו המקצועית בתחום אבטחת מידע וסייבר, ובהתאם לכך לשקול את המשך העסקתו.
- לגבש מדיניות או נוהל 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 הארגון 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'.
- לקיים הדרכות לעובדי ומשתמשי המערכות בחברה על אודות חובותיהם לפי החוק ונוהל אבטחת מידע (שיגובש), לקיים הדרכות מודעות לעובדים מועסקים וחדשים בנושא אבטחת מידע וסייבר לפחות אחת לשנה.
- להגדיר משתמשי-על במערכות בהתאם לעקרון "הצורך לדעת" ועקרון "הפרדת התפקידים". כך לדוגמה, ניתן להגדיר את מנהל המחשוב כמשתמש-על במערכות, ובתנאי שאינו לוקח חלק בתהליך עסקי בחברה.
- להסיר הרשאות משתמש של עובד שעזב סמוך ככל הניתן למועד עזיבתו.
- להגדיר מדיניות סיסמאות מוקשחת ברשת, ובמערכות Infoacash וחשבשבת.
- לקיים תהליך סקירה של משתמשים והרשאותיהם ברשת הארגון 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 - Business Continuity Plan), הגדרת התהליכים והמערכות החיוניות לארגון בעת חירום, הדרכות ותרגול התוכנית ועוד.
- להגדיר שמירת לוג פעולות במערכות אבטחת המידע ובמערכות המידע למשך 24 חודשים.

- לסקור את הלוגים ממערכות אבטחת המידע וממערכות המידע. מומלץ לבחון מערכת SIEM לניטור אירועי אבטחת מידע או לחלופין לבחון קבלת השירות בתצורת "שירות מנוהל".
- לבצע אחת לרבעון סריקת גישה בעזרת כלי אוטומטי כדי לאמוד את רמת החריגות הקיימות בשרתי הספריות ולבצע טיפול מונע.
- ליידע את בעלי ההרשאות במאגר בדבר קיום מנגנון הבקרה.
- לקיים אחת לשנה לפחות דיון באירועי אבטחה ולתעד את הדיון בפרוטוקול.
- ליישם מנגנון מניעת 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 כדרך קבע את עדכוני האבטחה המופצים על ידי חברת מיקרוסופט. לשדרג מערכות הפעלה שאינן נתמכות על ידה.
- לחתום על חוזה עם חברת חשבשבת, שבו יעוגנו הנושאים המחייבים בהתאם לדרישות החוק והתקנות.
- לבצע ביקורת תקופתית, אחת ל-24 חודשים לפחות ובהתאם לדרישות התקנות.
- לגבש נוהל גיבויים ושחזורים עבור תהליך הגיבויים והשחזורים בחברה בהתאם להוראות החוק, לתקנות ולצרכים התפעוליים של החברה.
- לשמור תיעוד מתאים של שחזורים שמבצעת החברה.
- 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, 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>
נעשו תיקונים של 99 אחוז מההמלצות שניתנו. בכל הנוגע למאגרי מידע עשינו כל הנדרש בחוק ואף מעבר.

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

פרק 2:

<u>המלצת המבקרת:</u>

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

<u>תגובת המבוקר:</u>

אנחנו כעת בישורת האחרונה לקראת הוצאת הזמנת עבודה לאנשי מקצוע שיטפלו בנושא ויתנו ליווי שוטף.

<u>המלצת ועדת ביקורת:</u>

לקבל את המלצות המבקרת.

בנוסף, בתוך 30 ימים חברת אריאל תשלח עדכון למבקרת וליו"ר ועדת הביקורת בנוגע לתחילת העבודה עם אנשי המקצוע.

<u>סיכום:</u>

<u>מר אלדד רבינוביץ, יו"ר הוועדה</u>: מברך שוב את המבקרת על הדוח החשוב ומודה לחברת אריאל על העבודה המקצועית ועל השיתוף הפעולה, ובעיקר שאימצו את הדוח בשתי ידיים ומתקנים את הנדרש. התיקון משמעותי גם לחברה, גם לירושלים וגם לציבור שמכניס פרטים אישיים באתר החברה.

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