



ועדה לענייני ביקורת

כ"ט בחשוון תשפ"ו
20 בנובמבר 2025
סימוכין : 2025-103-956

דו"ח משיבה מס' 20 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 : 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

על סדר היום :
דוח מבקרת העירייה בנושא : אבטחת מידע וסייבר בחברת אריאל

פתיחת הדיון :

מר אלדד רבינוביץ, יו"ר הוועדה : 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.

הגב' עופרה ברכה, מבקרת העירייה : 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.



ועדה לענייני ביקורת

דיון הוועדה:

פרק 1:

המלצת המבקרת:

- 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.



ועדה לענייני ביקורת

- 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 בקורות 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.

תגובת המבוקר:

נעשו תיקונים של 99 אחוז מההמלצות שניתנו. בכל הנוגע למאגרי מידע עשינו כל הנדרש בחוק ואף מעבר.

המלצת ועדת ביקורת:

לקבל את כל המלצות המבוקרת.
בנוסף, עד לסוף השנה הקלנדרית חברת אריאל תשלח עדכון למבוקרת וליו"ר ועדת הביקורת בנוגע להשלמת יישום ההמלצות.



ועדה לענייני ביקורת

פרק 2:

המלצת המבקר:

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

תגובת המבוקר:

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

המלצת ועדת ביקורת:

לקבל את המלצות המבקר.

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

סיכום:

מר אלדד רבינוביץ, יו"ר הוועדה: מברך שוב את המבקר 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

פרק שני

הגנת הפרטיות, אבטחת מידע וסייבר בחברת אריאל

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 // 17

מבוא // 21

פירוט הממצאים

פרק ראשון:

בדיקת ציות לחוק הגנת הפרטיות, ותקנותיו // 27

פרק שני:

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

סיכום // 48

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 ומעוגנת 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, 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; 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. בחברה קיימים לפחות שלושה מאגרי מידע החייבים רישום לפי חוק הגנת הפרטיות, ברשות להגנת הפרטיות, אולם אף לא אחד מהמאגרים רשום ברשות.
2. לחברה אין כלל מסמכים של הגדרות מאגרי מידע ושל מבנה מאגרי המידע, החברה לא מינתה באופן רשמי ממונה אבטחת מידע, לא קיימת מדיניות אבטחת מידע ונוהלי אבטחת מידע כתובים, וכן לא קיימת רשימת מצאי של מערכות המאגרים.
3. היועץ החיצוני של החברה אינו ממלא את תפקידו באופן מקצועי בתחום אבטחת המידע.
4. משתמשי המערכות אשר משמשים חלק מהתהליך העסקי, מוגדרים כמשתמשי-על במערכות. הגדרה זו מגבירה את הסיכון לכך שמשתמש ינצל את ההרשאה הגבוהה (הרשאת-על) לביצוע פעולות לא מורשות על ידו, ולחברה יהיה קושי רב, עד כדי חוסר אפשרות, לפקח ולגלות פעולות אלו.
5. קיימים ליקויים במדיניות הסיסמאות של הרשת וכלל לא קיימת מדיניות סיסמאות במערכת א'.
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. לחברה אין נוהל התאוששות מאסון ואין תוכנית להמשכיות עסקית.
8. בחברה לא קיים מנגנון למניעת חיבור התקנים ניידים, או מערכת הלבנה אשר תבדוק התקנים ניידים לפני שהם מוכנסים לרשת הארגונית.
9. ישנן מערכות שאינן מעודכנות בעדכוני אבטחת מידע קריטיים.
10. החברה לא ביצעה ביקורת תקופתית לוודא שהיא עומדת בהוראות החוק והתקנות.
11. החברה מעולם לא ביצעה סקר סיכוני אבטחת מידע ומבדקי חדירה.
12. 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 וחלק אף בבירור מחדל.
13. נמצא מספר רב של ליקויים בעלי חשיבות גבוהה בניהול ובתחזוקת מערכת חומת האש. המערכת אינה מנוהלת ומתוחזקת בהתאם לסטנדרטים מקובלים.
14. נמצאו ליקויים רבים בעלי חשיבות גבוהה בניהול ובתחזוקת מערכת AD (מערכת לניהול משתמשים), המערכת אינה מנוהלת ומתוחזקת בהתאם לסטנדרטים מקובלים.
15. 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 - מיפוי מאגרי המידע המחויבים ברישום בהתאם לחוק, בניית מסמכי הגדרות מאגרי מידע, מינוי רשמי של ממונה אבטחת מידע, גיבוש מדיניות ונוהלי אבטחת מידע וכו'.
2. לבחון ולבדוק את תוכנית העבודה של היועץ החיצוני בתחום אבטחת המידע והסייבר, את המשימות שניתנו לו בתחום זה ואת רמתו המקצועית, ובהתאם לכך לשקול את המשך העסקתו.
3. להגדיר משתמשי-על במערכות המידע בהתאם לעקרון "הצורך לדעת" ועקרון "הפרדת התפקידים".
4. להגדיר מדיניות סיסמאות נאותה ברשת החברה ובמערכת א'.
5. 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.
6. לגבש נוהל התאוששות מאסון ולבנות תוכנית להמשכיות עסקית.
7. ליישם מנגנון למניעת חיבור התקנים ניידים לתחנות הקצה של החברה, או לחלופין להפעלת מערכת הלבנה מרכזית.
8. להתקין בדרך קבע את עדכוני האבטחה ולשדרג מערכות שנדרש לשדרגן.
9. לבצע ביקורת תקופתית כדי לוודא שהחברה עומדת בהוראות החוק והתקנות.
10. לבצע בהקדם סקר סיכוני אבטחת מידע ומבדקי חדירה.
11. לטפל בדחיפות בהקשחת עמדות הקצה, השרתים וה-GPO (Group Policy); בממצאים שעלו במערכת חומת האש ובמערכת ה-AD, וכן לטפל בדחיפות בממצאים שעלו במבדקי החדירה הפנימיים והחיצוניים שביצעה הביקורת.

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

תגובת המבוקרים שולבה במקומות הרלוונטיים בגוף הדוח.

סיכום

זכות האדם לפרטיות היא אחת הזכויות החשובות בישראל ומעוגנת בחוק הגנת הפרטיות החל משנת 1981 (להלן: החוק) לרבות תקנותיו. החוק מגדיר מהי פגיעה בפרטיות ומסדיר 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. המתקפות עלולות לערער את היציבות הארגונית, לפגוע בנכסי הארגון, במוניטין שלו ובלקוחותיו, ולעיתים אף לסכן חיי אדם.

חברת אריאל היא יעד פוטנציאלי לניסיון תקיפות סייבר, וזאת 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.

יחידת מערכות המידע בחברת אריאל מורכבת ממנהל מחשוב, אשר מופקד על מערכות המידע ואבטחת המידע בחברה, יחד עם חברת ייעוץ חיצונית שנשכרה לשם כך.

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

הביקורת בדקה את עמידת החברה בהוראות החוק והתקנות, המדיניות והנהלים בנושא אבטחת המידע, וכן ערכה 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; 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 בממצאים שהועלו בהקדם, 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 אריאל היא החברה העירונית לתרבות, לחברה, לחינוך, לרווחה, לספורט ולאומנויות. החברה בבעלותה המלאה של עיריית ירושלים, פועלת למען פיתוח העיר ירושלים ומפיקה עשרות אירועים רבי משתתפים בשנה. אירועי חוצות הפונים לקהלים ישראלים ובין-לאומיים, כדוגמת: יריד חוצות היוצר, פסטיבל האור, צלילים בעתיקה, מתחם החלקה על הקרח, עיר הקרח ועוד.

החברה מונה כ-60 עובדי מטה ומורכבת משני תאגידים (ישויות נפרדות גם לצורך דיווח לרשויות):

- אריאל א' – תאגיד המנהל מגוון רחב של פרויקטים ואירועי תרבות (כגון: יריד חוצות היוצר, פסטיבל האור, צלילים בעתיקה) עבור העירייה, בהתאם לתוכנית העבודה ודרישות העירייה מעת לעת.
- אריאל ב' – תאגיד המנהל את אצטדיון טדי, בריכת הסולטן והיכל הפיס ארנה (שלושת מתקני התרבות והספורט הגדולים בעיר) וחלק האספלט של מתחם התחנה.

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.

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 יש לנקוט אמצעים לאבטחת המידע ומערכי המידע ולהגן עליהם מפני פגיעה, חשיפה ושינוי – במזיד או בשוגג. יש לעשות זאת באופן שיישמרו הזמירות, 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 אריאל מורכבת ממנהל מחשוב, אשר מופקד על מערכות המידע ואבטחת המידע בחברה, יחד עם חברה חיצונית ששכרה החברה. נוסף על כך, תקציבנית החברה הכפופה לסמנכ"ל הכספים מופקדת מצד המשתמשים על המערכות הכספיות של החברה.

בחברה יש כמה מערכות מידע עיקריות להנה"ח, לתקציב, למשאבי אנוש, לניהול תשלומים ואתר אינטרנט.

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 וכלה בניהול ותחזוקה שוטפת של המאגרים בהתאם לחוק ותקנותיו.

הערכת רמת אבטחת המידע, באמצעות מבדק טכנולוגי ומבדקי 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.

הביקורת לא בדקה מערכות שאינן מערכות מידע (כגון: מערכת מצלמות, מיזוג אוויר וכדומה).

תקופת הביקורת

הביקורת נערכה בחודשים פברואר - מאי 2024.

פירוט הממצאים

פרק ראשון

בדיקת ציות לחוק הגנת הפרטיות ותקנותיו

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 לפחות שלושה מאגרי מידע העונים על ההגדרה בסעיף 8(ג) לחוק, כדלהלן:
- ספקים – מאגר המידע הקיים במערכת ב', הכולל מידע רגיש, כגון פרטי ספקים וחשבונות הבנק שלהם (סעיף 8(ג)(2) לחוק).
 - עובדים – מאגר המידע הקיים במערכת ג' כולל מידע רגיש, כגון מספרי תעודת זהות של העובדים וחשבונות הבנק שלהם (סעיף 8(ג)(2) לחוק).
 - רשומות נתוני הורים וילדים – מאגר מידע במערכת א' הכולל מעל 10,000 רשומות עם פרטי הורים וילדים בגנים (סעיף 8(ג)(1) לחוק).
- יצוין כי אף לא אחד מהמאגרים הנ"ל רשום ברשות להגנת הפרטיות במשרד המשפטים.

מסקנות

1. אי רישום מאגרי המידע ברשות להגנת הפרטיות, היעדר מסמכי הגדרות מאגרי מידע ואי קביעת רמת אבטחת המידע הנדרשת מכל מאגר, משקפים אי עמידה של החברה בהוראות החוק ותקנותיו.

המלצות

1. למפות ולרשום את מאגרי המידע הנדרשים לרישום בהתאם לחוק ותקנותיו, וכן לקבוע את רמת אבטחת המידע הנדרשת מכל מאגר מידע בהתאם לתקנות.

מסמך הגדרות מאגרי מידע

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

תקנה 2 מציינת 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 משקף אי עמידה של החברה 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.

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, חברה ביטוח, חברה העוסקת בדירוג או בהערכת אשראי.

בתקנה 3 לתקנות הגנת הפרטיות מפורטות ההוראות שיחולו על הממונה על 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 האבטחה 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 האבטחה לא ימלא תפקיד נוסף שעלול להעמידו בחשש לניגוד עניינים במילוי תפקידו לפי תקנות אלה;

(5) הטיל בעל מאגר המידע על הממונה על האבטחה 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. עולה כי יחידת מערכות המידע בחברת אריאל מורכבת ממנהל מחשוב, אשר מופקד על מערכות המידע ואבטחת המידע בחברה, יחד עם חברה חיצונית ששכרה החברה. לא קיים כתב מינוי לממונה אבטחת מידע, לא קיים נוהל אבטחת מידע ולא קיימת תוכנית לבקרה שוטפת על העמידה בדרישות התקנות.

מסקנות

3. שיטת עבודה של "אחריות משותפת" בתחום אבטחת המידע פוגעת ביכולת של החברה לקבל החלטות בדבר פעולות הנדרשות בתחום אבטחת המידע.
4. בהתאם לממצאי דוח זה (אשר פורטו עד כה ויפורטו בהמשך), עולה לכאורה כי היועץ החיצוני של החברה אינו ממלא את תפקידו באופן מקצועי בתחום אבטחת המידע, החל מייעוץ לחברה לגבי עמידה בהוראות החוק ועד לפרקטיקה מקובלת בתחום אבטחת המידע (הקשחת עמדות קצה ושרתים, ניהול מערכת אנטי-וירוס, ניהול מערכת "חומת אש" ועוד).
5. אי מינוי ממונה אבטחת מידע, חוסר בנוהל אבטחת מידע ותוכנית בקרה שוטפת לעמידה בדרישות התקנות, משמעותם אי עמידת החברה בהוראות החוק ותקנותיו.

המלצות

3. 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.
4. 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.

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 ואת העקרונות המנחים.

תקנה 4 לתקנות דנה בנושא נוהל אבטחת מידע לבעל מאגר שמסתמך על מסמך הגדרות המאגר. הנוהל יישמר והגישה אליו תתאפשר 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 הגנה 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, במאגר 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 כך, תקנה 4 (ה) לתקנות הגנת הפרטיות, 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."
- נמצא כי לחברה לא קיים נוהל אבטחת מידע המפרט את אמצעי אבטחת המידע בחברה ובמאגרי המידע בפרט.

מסקנות

6. בשל חוסר במדיניות או בנוהל אבטחת מידע מפורט קיים קושי ביישום אבטחת מידע נאותה ובפיקוח עליה בחברה, וכן הדבר משקף אי עמידה של החברה בהוראות החוק ותקנותיו.

המלצות

5. 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.

מיפוי מערכות מאגר המידע וביצוע סקר סיכונים

תקנה 5 דנה במיפוי מערכות מאגר המידע וביצוע סקר סיכונים. להלן עיקרי התקנה:

"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

7. היעדר מסמכים של מבנה מאגרי המידע ורשימת מצאי של מערכות המאגרים מקשה על יישום מנגנוני אבטחת מידע נאותה על מאגרי המידע ופיקוח החברה עליהם; כמו כן הדבר משקף אי עמידה של החברה בהוראות החוק ותקנותיו.

המלצות

6. 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'.

תגובת המבוקרים

הנהלת החברה לא קיבלה עד קבלת הדוח כל אינדיקציה מיועציה השונים לחובת רישום מאגרי המידע וניהולם על פי התקנות, ולכן נותנת לנושא זה דחיפות מיוחדת שכן אין בכוונתה להיחשב ולו לכאורה כמפירת חוק. לכן בוצעה פנייה דחופה לחברות המתמחות ברישום מאגרי מידע כחוק, בניית נהלים וטיפול שוטף באבטחת המידע כפי שמופיע במספר סעיפים, כולל מבדק חדירה וסקר סיכונים בסוף התהליך. משך ביצוע התיקונים והרישום מוערך בכשלושה חודשים, שבסיומם נוכל לפרט אילו פעולות לא בוצעו ומאיזו סיבה. נודה לביקורת חוזרת עם סיום התיקונים לשם קבלת דוח מעודכן.

אבטחת פיזית ואבטחת מידע בניהול כוח אדם

אבטחה פיזית היא חלק ממערך ההגנה מפני פריצות אבטחה ושמירה על המידע בארגון. תקנה 6 דנה בנושא אבטחה פיזית, 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".

במשרדי החברה הממוקמים במתחם ארנה בירושלים, קיימים אמצעי אבטחה פיזית כלהלן:

- מצלמות אבטחה ברחבי אתר החברה.
- מאבטח בשער הכניסה לחברה.
- בכל קומה או משרד יש דלת אשר הכניסה דרכה היא אך ורק למורשים באמצעות מפתח ייחודי לכל עובד.
- ארונות התקשורת וחדרי השרתים נעולים ומאובטחים.
- החל מהקורונה, אין קבלת קהל באתר החברה.

ארגונים מתמודדים עם הצורך ההולך וגדל של עובדים, לקוחות ושותפים עסקיים בגישה אל מקורות המידע הארגוניים. נוסף על כך ישנו צורך לאפשר גישה למשתמשים נוספים, מבלי להתפשר על

רמת אבטחת המידע. על החברה לוודא כי הרשאות העובדים ניתנות בהתאם לעקרון "הצורך לדעת". תקנה 7 דנה 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".

הביקורת העלתה כי בחברה לא מתקיימות הדרכות לבעלי הרשאות בנושא חובות בעלי ההרשאות לפי החוק והתקנות, לא נמסר לעובדי החברה ולמשתמשיה נוהל אבטחת המידע, וכלל לא מתקיימות הדרכות מודעות לעובדים מועסקים או חדשים בנושא אבטחת מידע וסייבר.

מסקנות

8. אי קיום הדרכות לבעלי הרשאות בנושא חובות בעלי ההרשאות לפי החוק והתקנות מגביר את הסיכון מצד המשתמשים לעשיית טעויות ועבירה על החוק שכלל לא היו מודעים אליו, 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 הארגון. יתר על כן, הדבר משקף אי עמידה של החברה בהוראות החוק ותקנותיו.

המלצות

7. 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.

תגובת המבוקרים

1. ביחס לאבטחת המידע, כל עובד חותם בחוזה העסקה על הסכם סודיות.

2. בהתאם להמלצת הביקורת יבוצעו הדרכות אחת לתקופה בהתאם לנוהל שייכתב על ידי יועץ אבטחת המידע שהחברה תשכור, כאמור בסעיף קודם.

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.

תקנה 8 מציינת 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)".

תקנה 9 מציינת 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 פזי 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 הרשאה עשוי היה לדעת, מיד עם סיום תפקידו של בעל הרשאה.

בבדיקת המורשים למערכות החברה נמצא כי משתמשי-העל במערכות (מנהלי המערכות) אינם נדרשים לכך מתוקף תפקידם, ואף קיים חשש לפגיעה בעקרון הפרדת התפקידים.

הביקורת בדקה את משתמשי העל במערכות: הנהלת חשבונות, משאבי אנוש וניהול תקציבים.

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 ממחלקת משאבי אנוש שולח מייל למנהל המחשוב כדי לפתוח משתמש חדש ברשת החברה עם תיבת דואר אלקטרוני בהתאם לתפקיד שהוגדר לעובד. הרשאות למערכות המידע בחברה ניתנות על ידי כל משתמש-על (שונה לכל מערכת כפי שצוין מעלה).
 - **עובד עוזב** – בעת עזיבת עובד את החברה, מחלקת משאבי אנוש שולחת בקשה במייל למנהל המחשוב להסרת יכולת השימוש של המשתמש מהרשת (הפיכת המשתמש ל"לא פעיל"). הרשאות במערכות המידע מטופלות על ידי משתמשי-העל, אשר הופכים את המשתמש של העובד ל"לא פעיל", או שמוחקים אותו בהתאם למערכת הרלוונטית.
- הביקורת בדקה את מדיניות הסיסמאות ברשת ובמערכות החברה השונות.

מסקנות

9. משתמשי-העל במערכות המידע בחברה הם משתמשי המערכת אשר משמשים חלק מהתהליך העסקי. הגדרה זו מגבירה את הסיכון לכך שמשתמש ינצל את ההרשאה הגבוהה (הרשאת-על) לביצוע פעולות לא מורשות על ידו, ולחברה יהיה קושי רב, עד כדי חוסר אפשרות, לפקח ולגלות פעולות אלו.
10. בתהליך הסרת הרשאות (או הפיכה ל"לא פעיל") של עובדים עוזבים, נמצא כי קיים הפרש זמן של מעל חודש בין תאריך עזיבת העובד לבין המועד שבו מסירים את הרשאותיו כמשתמש, מצב המגביר את הסיכון לשימוש לא נאות במשתמש של העובד.
11. במדיניות הסיסמאות של הרשת לא קיימת חובת החלפת סיסמה אחת לתקופה, אין הגבלה של מספר ניסיונות כושלים לגישה ואין נעילת מסך לאחר פרק זמן מסוים. מדיניות הסיסמאות בחשבשבת אינה כוללת דרישה למורכבות סיסמה ואילו במערכת א' כלל לא הוגדרה מדיניות סיסמאות. מצב זה מגביר את הסיכון לתקיפה ולגניבה של סיסמאות על ידי עובדים אחרים או על ידי גורמים עוינים, וחדירה למערכות המידע של החברה.
12. אי קיום תהליך סקירת משתמשים והרשאותיהם ברשת ובמערכות החברה חושף את החברה למצב שבו שמות המשתמש של עובדים שעזבו וכן הרשאות של עובדים שהחליפו תפקיד בחברה עדיין פעילים ברשת ובמערכות החברה, וכתוצאה מכך חלה פגיעה עקרון "הצורך לדעת".
13. גם בעניינים האמורים החברה אינה עומדת בהוראות החוק ותקנותיו.

המלצות

8. 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 מתהליך עסקי בחברה.
9. להסיר הרשאות משתמש של עובד שעזב סמוך ככל הניתן למועד עזיבתו.
10. להגדיר מדיניות סיסמאות מוקשחת.
11. 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.

תגובת המבוקרים

המלצה 1: בבדיקה מול מערכת ב' מסתבר כי לא ניתן להפריד את ההרשאות המלאות של המערכת. בהמשך להמלצת הביקורת אנו נעביר את ההרשאות המלאות למנהל המחשוב כאשר מנהל החשבונות הראשי יישאר עם הסמכויות המלאות, ללא פתיחת משתמשים. נבהיר כי בהמשך לדוח ביקורת שבוצע בעבר קיימות בקורות בהנהלת חשבונות, לפיהן מורשי החתימה הם אלו שחותמים על הכספים שיוצאים מהחברה (צ'קים וכו'). ביחס למערכות א' ו-ג', הממצא אינו מדויק, משתמשי-העל במערכות אלו הם בבחינת אנשי קשר מול הספק החיצוני, כל פעולה כמו הגדרת משתמשים מבוצעות על ידי הספק החיצוני. מכאן שמתקיים עקרון הפרדת התפקידים כנדרש בדוח.

המלצה 2: במהלך ביצוע טיפול ויישום באבטחת מידע כאמור, ייכתב נוהל מסודר בנושא זה. כעת נדגיש כי קיים נוהג לפיו מנהלת משאבי אנוש מעדכנת את מנהל מערכות המידע בחברה בדבר שינויים במשרות ועזיבת עובדים. מנהל מערכות מידע משנה/מבטל את הרשאות העובדים בהתאם. על פי החלטת ההנהלה העדכון יבוצע בתוך 24 שעות (הביקורת הציעה חודש).

המלצה 3: החברה מקבלת את המלצת הביקורת. החלפת הסיסמאות נקבעה לפי AD, והחלפת AD- תבוצע אחת ל-180 יום.

המלצה 4: יבוצע בהתאם להחלטת החברה לאחר המלצות חברת הייעוץ כאמור.

התייחסות הביקורת

הפרקטיקה המקובלת לשמירת עקרון הפרדת התפקידים היא מתן הרשאות-על לגורם שאינו חלק מתהליך העבודה, ומכאן באה המלצת הביקורת בעניין.

שמירת לוג פעולות ותיעוד אירועי אבטחת מידע

תקנות 10 ו-11 מחייבות שמירה של לוג פעולות ותיעוד של אירועי אבטחת מידע.

להלן דרישות תקנה 10:

- 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 תקנה 11:

- 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 וכלה בתוכנית 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. תרגול אירוע סייבר אחת לשנה, תוך כדי שימוש במערכות ותשתיות, מחזק את החוסן של הארגון בעת קרות אירוע סייבר אמיתי.
- הביקורת בדקה בקרות 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.
- לחברה לא קיימת תוכנית להמשכיות עסקית אשר כוללת, בין השאר, מיפוי הסיכונים שלהם חשופה החברה, ניסוח אסטרטגיית המשכיות עסקית (Business Continuity Plan - 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 לעובדיה לצורת ההתנהלות בקרות אירוע כזה, טיפול 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

14. אי קיום מספר רב של בקורות תיעוד, ניטור וההתמודדות עם אירועי סייבר מקטין את הסיכוי של החברה להתמודד עם אירוע כזה, החל משלב הבנת האירוע, דרך עצירתו וכלה בצמצום הנזקים בעקבותיו. כמו כן, הדבר משקף אי עמידה של החברה בהוראות החוק והתקנות.

המלצות

12. לגבש נוהל בדיקה שגרתי של נתוני התיעוד של מנגנון הבקרה.
13. לגבש נוהל התאוששות מאסון ונוהל התמודדות עם אירועי סייבר, הכולל הנחיות לעובדי החברה ולחברה איך להתנהל בקרות אירוע סייבר.
14. לפתח תהליך לקיום המשכיות עסקית, אשר יכלול בין השאר מיפוי הסיכונים שלהם חשופה החברה, ניסוח אסטרטגיית המשכיות עסקית (Business Continuity Plan- BCP), הגדרת התהליכים והמערכות החיוניות לארגון בעת חירום, הדרכות ותרגול התוכנית ועוד.
15. להגדיר שמירת לוג פעולות במערכות אבטחת המידע ובמערכות המידע למשך 24 חודשים.
16. לסקור את הלוגים ממערכות אבטחת המידע וממערכות המידע. מומלץ לבחון מערכת SIEM לניטור אירועי אבטחת מידע או לחלופין לבחון קבלת השירות בתצורת "שירות מנוהל".
17. לבצע אחת לרבעון סריקת גישה בעזרת כלי אוטומטי כדי לאמוד את רמת החריגות הקיימות בשרתי הספריות ולבצע טיפול מונע.

18. ליידע את בעלי ההרשאות במאגר בדבר קיום מנגנון הבקרה.
19. לקיים אחת לשנה לפחות דיון באירועי אבטחה ולתעד את הדיון בפרוטוקול.

תגובת המבוקרים

- המלצה 1:** בדיקה שגרתית קיימת. נשלחו לצוות הביקורת דוחות המעידים על הבדיקות המתבצעות באופן שוטף. יגובש נוהל כתוב בהתאם.
- המלצה 2:** ייכתב נוהל על פי המלצות הביקורת.
- המלצה 3:** קיים מערך התאוששות מאסון עם אפיון רמות ההמשכיות העסקית. יגובש נוהל כתוב בהתאם.
- המלצה 4:** קיים לוג ל-60 יום, נבצע הארכה בהתאם להמלצה.
- המלצה 5:** מבוצעת כיום בדיקה שוטפת. תירכש תוכנה מתאימה עבור מנהל המחשוב לשם ביצוע הבדיקה על ידו.
- המלצה 6:** תירכש תוכנה מתאימה כאמור לעיל.
- המלצה 7:** ימומש כחלק ממסקנות ייעוץ אבטחת המידע והסייבר.
- המלצה 8:** ימומש כחלק ממסקנות ייעוץ אבטחת המידע והסייבר.

התקנים ניידים

תקנה 12 מחייבת 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".

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

מסקנות

15. היעדר מנגנון למניעת חיבור התקנים ניידים או מערכת הלבנה אשר תבדוק התקנים ניידים לפני שהם מוכנסים לרשת הארגונית, חושף את החברה לסיכון של הוצאת מידע רגיש או פרטי, וכן משקף אי עמידה של החברה בחוק ותקנותיו.

המלצות

20. 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.

תגובת המבוקרים

אופי פעילות החברה מחייב שימוש בהתקנים ניידים, כחלק מהעבודה השוטפת. המנגנון לניטור התקנים ניידים קיים, מתבצעת בדיקה על פעולות שהוגדרו כגון וירוס. כיוון שקיימות דרכים רבות לשליפת מידע, העובדים חתומים על הסכם סודיות. עם זאת, החברה תשקול צמצום האפשרות למשתמשים ספציפיים, בהתאם לנוהל שייכתב.

אבטחת מערכות ותקשורת

נושא אבטחת מערכות המפעילות את מאגרי המידע מעוגן בכל התקנות. בהתאם לתקנה 13 יש להקפיד על ניהול ותפעול תקין למערכות אלו. בתקנה מצוין 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".

תקנה 14 מתמקדת בנושא אבטחת תקשורת למקרים שאותן מערכות מחוברות לרשת חיצונית. כדלקמן:

"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

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

המלצות

להתקין כדרך קבע עדכוני אבטחה שונים.

תגובת המבוקרים

- 1. באחריות הספק החיצוני לבצע את העדכונים באופן שוטף. קיים שרת אחד שאין לו גישה למאגרי מידע והוא קיים רק לצורך שליפת מידע היסטורי המבוצע באופן חיצוני.
- 2. מדובר במערכת אחת בלבד בארגון.

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 שלאותו גורם חיצוני יש גישה למידע רגיש בארגון. לנוכח זאת, אבטחה שוטפת של תהליך גישת מיקור החוץ לרשת הפנימית של הארגון הפכה להיות אחד ממנגנוני האבטחה החשובים.

תקנה 15 מחייבת את בעל המאגר כדלהלן:

- 1. לבחון לפני ביצוע ההתקשרות את סיכוני אבטחת המידע הכרוכים בהתקשרות.
- 2. לקבוע במפורש בהסכם עם הגורם החיצוני את כל הפרטים, בשים לב לסיכוני אבטחת המידע הכרוכים בהתקשרות.

בידי החברה הסכמי התקשרות מפורטים הכוללים בין היתר התייחסות לשמירה על סודיות, שירותי תמיכה בחירום וכו' עם ספק התוכנה של מערכת ג' ועם ספק התוכנה של מערכת א', אולם אין בידה הסכם עם ספק מערכת ב' אשר כולל התייחסות לדרישות התקנות.

התחברות מרחוק של ספקי מיקור חוץ מותנית באישור מנהל המחשוב. החיבור מבוצע באמצעות מערכת שונות, ולטענת מנהל המחשוב, במהלך החיבור מרחוק הוא מנטר את פעולות הספק עד לסיום ההתחברות. חיבור הספקים נעשה לצורכי תמיכה או עדכונים בהתאם לדרישת החברה או מנהל המחשוב.

בחברה לא נערך סקר סיכוני אבטחת מידע בהיבטי ספקים אשר מטרתו לספק תמונה מלאה על התחברות הספקים לרשת ולמערכות החברה, לציווד שאליו הם ניגשים ולחומרים של החברה, וכן על אמצעי ההגנה שהספק מפעיל ועוד.

מסקנות

17. בידי החברה אין הסכם התקשרות עם ספק מערכת ב' הכולל התייחסות לשמירה על סודיות, למתן שירותים ותמיכה בעת חירום וכן לדרישות המחייבות בחוק ובתקנות. מצב זה מגביר את הסיכון הקיים לחברה לזליגת מידע מצד הספק, וכן משקף אי עמידה שלה בהוראות החוק והתקנות.

המלצות

22. לחתום על חוזה עם ספק מערכת ב', שבו יעוגנו הנושאים המחייבים בהתאם לדרישות החוק והתקנות.

תגובת המבוקרים

החברה מחדשת את ההסכם עם חשבשבת מדי שנה בהזמנת עבודה כנדרש שמשמרת תנאי הסכם היסטורי. לאור בקשת המבקר החברה ביקשה וקיבלה מחשבשבת מסמך שמירת סודיות חתום על ידי חשבשבת.

ביצוע ביקורת תקופתית

ביצוע ביקורת תקופתית נועד לשמור על רמת אבטחה גבוהה בארגון ובמאגרי המידע. תקנה 16 מחייבת 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".

עולה כי לא מבוצעת בחברה ביקורת תקופתית.

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

סקר סיכוני אבטחת מידע הוא תהליך המאפשר הגעה לרמת הגנה סבירה על מערכות המחשוב של הארגון תוך כדי 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, במטרה לגלות חשיפות פוטנציאליות 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.

הביקורת העלתה כי החברה לא ביצעה מעולם סקר סיכוני אבטחת מידע ומבדקי חדירה.

מסקנות

18. אי ביצוע ביקורת תקופתית ואי עריכת סקר סיכוני אבטחת מידע ומבדקי חדירה, בניגוד להוראות החוק והתקנות, מקטינים את יכולת החברה לשמור על רמת אבטחה, לרבות אבטחת המידע במאגרי המידע שלה.

המלצות

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

תגובת המבוקרים

ההמלצה תיושם בהתאם לנוהל שייכתב על ידי החברה לאבטחת מידע.

גיבויים ושחזורים

קיימים גורמי סיכון רבים על מערכות המידע, כגון: הגורם האנושי (אם בשוגג ואם בזדון), תקלות, וירוסים, מזקי טבע, וכו'. גורמים אלו עלולים לגרום לפגיעה בנתונים המנוהלים במערכות המידע ואף להפסקת פעילות מערכות אלו. כדי להבטיח את המשך פעילות מערכות המידע על הארגון לנקוט פעולות למיניהן - בין השאר עריכת גיבויים וביצוע שחזורים יזומים לבדיקתם.

תקנה 18(א) מציינת כי:

"במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, יקבע בעל המאגר במסמך:

- (1) נהלים לביצוע גיבוי כאמור בתקנה 17(ב), באופן תקופתי שגרתי;
 - (2) נהלים להבטחת שחזור הנתונים כאמור בתקנה 17(ב), ובלבד שביצוע השחזור יהיה באישור מנהל המאגר;
 - (3) כי במסגרת תיעוד אירועי אבטחה כאמור בתקנה 11, יתועדו גם הליכי שחזור המידע, ובכלל זה – זהותו של מי שביצע את הליכי השחזור ופרטי המידע ששוחזר."
- בחברה קיימת מערכת גיבוי VEEAM, אשר מנהלת את תהליכי הגיבוי וכן גיבוי לקלטות של השרתים האלה:

- שרת Ariel-DC-New
- שרת Ariel-Terminal
- EST
- SQL

לחברה אין נוהל גיבויים ולא קיים תיעוד של שחזורים יזומים שבוצעו.

מסקנות

19. היעדר נוהל גיבויים ושחזורים חושף את החברה למצב שבו לא יבוצעו כנדרש תהליכי הגיבוי והשחזור של המידע, מה שעלול לפגוע בנתוני מערכות המידע ואף להפסקת פעילות מערכות אלו.

המלצות

24. לגבש נוהל גיבויים ושחזורים עבור תהליך הגיבויים והשחזורים בחברה בהתאם להוראות החוק, לתקנות ולצרכים התפעוליים של החברה.
25. לשמור תיעוד מתאים של שחזורים שמבצעת החברה.

תגובת המבוקרים

המלצה 1: קיימים גיבויים, ייכתב נוהל לגבי גיבויים.

המלצה 2: מבוצע באופן שוטף. יש תיעוד שחזורים, נרשם במערכת השחזורים עם שמירה של 3 שנים לאחור.

התייחסות הארגון לנושא של דלף מידע ארגוני

דלף מידע פירושו שמידע מהארגון עובר לגורמים שאינם מורשים. דלף מידע יכול להיות תוצאה של גניבת מידע מכוונת ממניעים של ריגול עסקי, של כשל טכני, של טעויות אנוש וכו'.

הערוצים המרכזיים שדרכם יכול לדלוף מידע ארגוני הם הדואר האלקטרוני הארגוני, הדואר האלקטרוני הפרטי, הרשתות החברתיות, מדיה נתיקה (DOK - Disk On Key), 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 מחוץ לחברה ולא קיימת בקרה טכנולוגית על הוצאת מידע דרך מערכות הדואר האלקטרוני והאינטרנט.

מסקנות

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

תגובת המבוקרים

המלצה 1 ו-2: קיים בחברה מיפוי ספריות של המידע והגישה אליו לפי מחלקות. הגישה אל המידע של מחלקות בעלות מידע רגיש יותר מוגבלת למשתמשים מסוימים.

המלצה 3: ייכתב נוהל.

המלצה 4 ו-5: החברה קיבלה לאחרונה הצעת מחיר למערכת CyFox XDR שתיתן מענה הולם. במהלך השנה הקרובה החברה תבחן, עם יועצי האבטחה שלה, רכישה של מערכת לפי שיקולי עלות תועלת.

סיכום

הזכות של האדם לפרטיות היא אחת הזכויות החשובות בישראל ומעוגנת בחוק הגנת הפרטיות החל משנת 1981 (להלן: החוק) לרבות תקנותיו. החוק מגדיר מהי פגיעה בפרטיות ומסדיר 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 אריאל 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.

יחידת מערכות המידע בחברת אריאל מורכבת ממנהל מחשוב, אשר מופקד על מערכות המידע ואבטחת המידע בחברה, יחד עם חברת ייעוץ חיצונית שנשכרה לשם כך.

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, המדיניות והנהלים בנושא אבטחת המידע, וכן ערכה 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; 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 בממצאים שהועלו בהקדם, 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 אריאל

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, תאגידה 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 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 להיות 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 מצביעה על מספר ליקויים בהתנהלות חברת אריאל בעניין זה. מספר רב של ליקויים נגעו לנושא רגולציה, מדיניות, נהלים ותהליכים בתחום אבטחת מידע וסייבר. כך לדוגמה, נמצא כי החברה לא רשמה 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 היא לא מינתה באופן רשמי ממונה אבטחת מידע. כמו כן, נראה כי לחברה אין נוהל התאוששות מאסון ואין תוכנית להמשכיות עסקית וכי היא מעולם לא ביצעה סקר סיכוני אבטחת מידע ומבדקי חדירה. בנוסף לכך, הצביעה הביקורת על ליקויים בנושא ניהול ותחזוקת מערכת חומת האש ומערכת AD (מערכת לניהול משתמשים). כן, הביקורת הצביעה על כך שנמצאו ליקויים במבדקי החדירה הפנימיים והחיצוניים שביצעה הביקורת.

מעיון בדוח מבקרת העירייה בנושא זה, נראה כי אין ספק שקיים בראש ובראשונה צורך במיפוי החקיקה והתקנות מכוחה וביבוס נוהלי אבטחת מידע ונהלים נוספים בהתאם להמלצת הביקורת. כן, יש לרשום את מאגרי המידע ולמנות ממונה אבטחת מידע כנדרש על פי דין.

עיינתי בתגובת גורמי המקצוע השונים של החברה ואני מברך על תגובתם כי הם מקבלים את רובן של ההמלצות לרבות ההמלצות בדבר גיבוש נהלים שונים ועדכון מערכות והליכים שונים, ואף החלו ליישמן. גורמי המקצוע ציינו כי החברה מתכוונת לבצע טיפול שוטף באבטחת המידע ואף לבצע מבדק חדירה וסקר סיכונים בהקדם.

עיריית ירושלים בראשותי תמשיך להשקיע ולקדם את נושא אבטחת המידע, בוודאי לאור המצב הבטחוני ולאור הגידול במספר אירועי הסייבר והתגברות הסיכון הנשקף לעירייה ולתאגידים העירוניים והכול, בכדי להיות מוכנים למתקפה הבאה ולהגן על המידע המצוי בידי 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 : 20

מקום ההתכנסות : אולם חדר ישיבות קומה 0

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

מזכיר הוועדה בדיון : צבי אבו

שעת תחילת הוועדה : 14: 17

שעות סיום הוועדה : 14: 46

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 ג ו R M ים גולד וורק תמלול והקלטה

יו"ר אלדד רבינוביץ:

אני מתכבד לפתוח את הדיון, אני מתכבד לפתוח אתה דיון, וועדת ביקורת מספר 20, הגנת פרטיות אבטחת מידע לסייבר בחברת אריאל. האמת שהפעם אני הבאתי חבילה של פופקורן, בשביל לצפות בהצגה. הנושא הזה הוא באמת מאוד חשוב, אבל אני לא כל כך מבין בו. אז אני אשמח על ההזדמנות ללמוד,

אורי מנחם:

אתה לא לבד.

אלדד רבינוביץ:

מה?

אלדד רבינוביץ:

תחום הסייבר והגנת המידע זה תחום מתפתח, משמעותי, כבר כמה שנים שמדברים עליו, כעל אחד האיומים המשמעותיים ואפילו ברמה הלאומית, אני חושב שבחודשים האחרונים, בשנה האחרונה, שנתיים האחרונות, זה נהפך להיות הרבה יותר דרמטי, כשנהיו כאן כל מיני מלחמות עולמיות, מול קבוצות ומדינות בעלות יכולות גבוהות, גם יכולות מדינתיות, וגם יכולות שכליות מאוד מאוד גבוהות, ולכן אני מאוד מברך על הדו"ח הזה, מאוד מברך על הדיון הזה, ואני מקווה שהתוצר שלו יהיה, שנהיה כולנו מוגנים יותר, בכבוד.

עפרה ברכה:

אז אני אגיד רק משפט אחד, שאנחנו, הכול בסדר. שאנחנו בביקורת גם לא מבינים גדולים בעולם הזה, אבל בהחלט זיהינו את ה - , את הזירה הבאה, שגוף צריך להתמודד איתה. ועיריית ירושלים, עם כל הגודל שלה, והמעמד שלה, והמיקום שלה, היא מהווה יעד, ולכן בחרנו לעשות ביקורת בנושא הזה, בתאגידים העירוניים, זאת אומרת ב - 2024 ערכנו בכל בתאגידים עירוניים ביקורת בנושא אבטחת מידע, הגנת הפרטיות וסייבר. לעיתים לפי הצורך במתכונת טיפונת שונה. אני אגיד שבאריאל בדיעבד, אני חושבת שזה אחד הדברים הטובים שעשינו לחברת אריאל, בהחלט מצאנו שהנושא הוא חשוב, ולא סגור עד הסוף הטיפול. עם זאת אני אומרת שבמהלך הדיונים שקיימנו איתם, אז באמת ראינו ש - , שחברת אריאל לקחה את הדו"ח בשתי ידיים, מה שנקרא, ועשתה תהליך תיקון הליקויים תהליך מאוד רציני, ושלומי יציג את הממצאים בצורה מפורטת, ואחרי זה נשמע התייחסות.

שלומי בני:

אז צהריים טובים לכולם. אני אציג את עצמי בשורה, למי שלא מכיר, שלומי בני, שותף במשרד RSM שיף הזנפרץ ושות', עורכת הביקורת, ערכתי את הביקורת הזאת, ואת הביקורת בשאר התאגידים העירוניים. משפט אחד לפני שאני מתחיל, אמנם אתם לא, אולי לא מספיק יודעים,

ומכירים את תחום אבטחת המידע לסייבר, אבל אתם מכירים את עולם ניהול הסיכונים, וזה מה שרשום. כשאנחנו מדברים על סיכונים, אנחנו מדברים באותה שפה, והמטרה של הדו"ח, היא באמת להעביר לכם את הסיכונים, אנחנו לא נדבר פה על הגדרת FIREWALL, כי זה באמת, זה לא יהיה זה. אבל אנחנו כן נדבר על סיכונים, וזה בעצם היה הרעיון, אז גם אם מישו לא מכיר, עדיין נוכל להתחבר, אני מקווה שהוא יהיה (לא ברור). רקע כללי, צריך להציג את הרקע הזה או ש - ?

עפרה ברכה:

מילים ספורות.

שלומי בני:

כמה מילים חברת אריאל היא בעצם חברה עירונית שאחראית לתרבות, לחינוך של עיריית ירושלים, היא בעצם מונה כ - 60 עובדי מטה, שיש להם בעצם יוזרים בתוך, בתוך המערכות, מחולקת לשתיים כמו שצוין פה בחצי בדיחה, אריאל א', אריאל ב', אז אריאל א' הוא בעצם מנהל את הפרויקטים ואת אירועי התרבות הגדולים, של פסטיבל האור, חוצות היוצר, וכולה. ואריאל ב' בעצם מנהל את האצטדיון טדי, בריכת הסולטאן, היכל הפיס וכולה, זו ההפרדה. בכל מקרה במערכות המידע אנחנו מדברים על אותם מערכות מידע, זה רק איזה שהוא הסבר כללי למי שפחות מכיר. מטרת הבדיקה, יש פה בעצם בגדול, שתי מטרות עיקריות, אחד זה באמת לבדוק את רמת אבטחת המידע והסייבר של הארגון עד כמה הוא חשוף לתקיפות סייבר חיצוניות או פנימיות, מתוך ארגון, מתוך הארגון, והחלק השני בדקנו גם את הציות להוראות החוק של תקנות הגנת הפרטיות, ורישום מאגרי המידע. בסך הכול זה שתי נושאים שהם די מתחברים אחד לשני, כי גם חוק הגנת הפרטיות תקנות אבטחת המידע של החוק בעצם מגדירות ומנחות מה צריך לבצע בתחום של אבטחת המידע. כך שהם לא רחוקים מאוד אחד משני, ולכן הם מתחברים ודרך כלל אנחנו אוהבים לעשות את הדו"ח בזה ביחד, ואז בעצם החברה מרוויחה, מצד אחד את הממצאים, המלצות, איך להגן על עצמה, מצד שני איך זה תואם את הוראות החוק/תקנות. אז אנחנו פותחים עם,

אלדד רבינוביץ:

אני רק (לא ברור), אתה מציג בעצם איזה שהם ממצאים, אני אשמח שבעצם תהיה תגובה אחד לאחד, כדי שלא נשכח דברים ובסוף.

שלומי בני:

מצוין. אז הדבר הראשון שאנחנו נפתח איתו, זה באמת רישום מאגרי מידע, אנחנו הגדרנו פה שלפחות קיימים שלושה מאגרי מידע, יכול להיות שיותר, אני לא רוצה להתחייב, אבל בגדול לפחות שלושה, כי יש מצלמות.

אלדד רבינוביץ:

מאגר מידע זה נגיד רשימת מינויים, או רשימת לקוחות בכל מיני,

שלומי בני :

מדויק, מדויק, בעצם רשם המאגרים, משרד המשפטים החליטו שיש חוק, שבא ואומר, ברגע שאתה מנהל, יש לך כמות מסוימת של רשומות, נתונים מסוימים, עם מאפיינים מסוימים, אתה חייב לרשום אותם, למה? כי אתה לא יכול להתחיל לאסוף על אנשים את המידע רפואי, כלכלי, לא משנה, דעות פוליטיות וכולה, ולעשות עם זה מה שאתה רוצה, אז יצא חוק שבא ואומר, יש כללים מסוימים, שאתה צריך לרשום את ה - , את המאגר הזה. אחרי שאתה צריך לרשום אותו, אתה צריך לשמור עליו, אוקי, שלא כל אחד יכול לבוא ולשלף מידע, ולעשות מה שהוא רוצה. אז הממצא הזה בא ואומר, לפחות יש שלושה מאגרי מידע, שזה מאגרי מידע שהיה צריך לרשום אותם שלא נרשמו, אז קודם כל זו עבירה על החוק, בסדר? אגב מה - 1 לאוגוסט, עד ה - 1 לאוגוסט, עד תיקון 13, בא ואומר - אנחנו, זה למעשה עבירה פלילית, בסדר? אבל הם כמעט ולא היו אוכפים את זה. מה - 1 לאוגוסט מעבר לזה שזה עבירה פלילית, זה גם עבירה שאפשר לקנוס את החברה, ואת בעלי התפקיד, זאת אומרת זה כבר קיבל משנה תוקף. והם גם אמרו - אנחנו נקנוס, אנחנו נהיה. כאילו רצו לפתוח תיקים פליליים, אם לא רשמת מאגר כזה או אחר, היו יותר סלחנים, 1 לאוגוסט זה קצת יותר מחמיר, ויש לנו, יש להם כבר יותר שיניים. אז שלושה מאגרי מידע שלא נרשמו, ובעצם ההמלצה הייתה קודם כל למפות את דרישות הוראות החוק, להחליט על מה צריך, מה צריך לרשום את זה, כי אמרתי יכול להיות שיש ארבעה, וחמישה ושישה אנחנו התמקדנו וציינו שלפחות שלושה בוודאות, וגורם החברה.

אורי מנחם :

אני אגיד רק שוב, אני מתחבר באמת למשפט פתיח, כי לא ידעתי שאתה רוצה לנהל את זה בצורה הזאת, שמעלים סוגיה, ואז אנחנו מתייחסים, אז את הפתיח שלי אני אעשה כרגע, כי אני מאוד מתחבר למה שהמבקרת אמרה, אני חושב ש - , בסופו של יום הביקורת שנעשתה בחברה, עשתה אותו בחברה,

אלדד רבינוביץ :

זה מה שאמורה לעשות ביקורת.

אורי מנחם :

היה פה שיתוף, כאילו אתה חשוף לדברים, ואז אתה רואה הרבה דברים שקורים, וגם חלקם הלא קטן אפילו נקרא לזה ככה, לא פעלו ולא עבדו כמו שצריך, זה הייתה לנו באמת הזדמנות מאוד טובה לרדת לשורש העניין, ולעשות באמת את ה - , מחקר הפנימי שלנו, ואת העבודה שלנו על מנת לשפר את הדברים. אני חושב שבמהלך התקופה, אחורה אני מדבר על מספר חודשים, אתם תראו גם את הממצאים, אפשר להגיד שהיו פה לא מעט ממצאים, סדר גודל של איזה 70, 80 ממצאים שהביקורת הצביעה עליה, אבל בסופו של יום אם אנחנו נסתכל היום בנקודת הזמן הזאת, אנחנו על

99%, ו – 98% משהו כזה מסמנים כבר וי, כאילו שביצענו עבודה והדברים בוצעו ותוקנו ושופרו, מתוך תקווה כמובן ש - , שוב הדבר הזה גם נורא נורא מפתח, נורא נורא משתנים. אז גם לנו צריך לשים אותנו עם יד על הדופק, וגם יש לנו חברה שמלווה אותנו, ולקחנו את זה מאוד מאוד ברצינות, ולא נמצא פה עופר שהוא סמנכ"ל החברה שהוא למעשה היה בן אדם שריכוז, לפחות מטעמי את הסוגיה, אבל מודי שהוא מנהל המחלקה ודבורה שהיא תקציבנית שהיא מעורבת בכל ה - , בכל המהלך הזה של העבודה אל מול הביקורת, וכמובן אילן שהוא יועץ, גפני תקשורת, אז הוא הגוף שמלווה אותנו, אז אנחנו באמת לקחנו את זה בשיא הרצינות, וכמובן תשמעו את ההתייחסות שלנו.

אלדד רבינוביץ:

זה הנחת של עבודת הביקורת, אני חדש בעבודות הביקורת, המבקרת כן וותיקה ממני. בסופו של דבר מטרת הביקורת היא לא להצליף, ולא להרביץ, ולא לעשות רע, וגם לא לחשוף את האנשים, והמטרה,

אורי מנחם:

אנחנו מתעסקים בספורט, לקחנו את זה בצורה ספורטיבית.

אלדד רבינוביץ:

המטרה היא בסופו של דבר לייצר תיקון, ולהיות שותפים לתיקון, וכשיש מבוקר, שהוא באמת מתייחס לזה ככה, ולוקח את זה בשתי ידיים, אז באמת התחושה היא שלא סתם משקיעים את כל האנרגיות,

עפרה ברכה:

הצלחנו.

אלדד רבינוביץ:

ויש הצלחה משמעותית.

עפרה ברכה:

נכון,

אלדד רבינוביץ:

אז תודה.

מודי בן אבו:

אפשר להציג את ה - ,

שלומי בני :

כן,

אילן גפני :

אני אתן רק איזה שהיא, איזה שהיא הקדמה, ומה עשינו, ואז באמת נוכל להציג, אז נוכל להציג, אבל מה נעשה? סעיף סעיף?

אורי מנחם :

כל פעם יציגו, ותיכנסו?

אילן גפני :

לא, אני אציג את הסך הכול, ואחר כך אני מניח שיאמינו לי לנתונים שלי.

אורי מנחם :

אז יכול להיות ש - , סליחה שאני מתערב, אבל יכול להיות שכדאי שבאמת הוא יציג את הכול, ואז התייחסות לכל.

אלדד רבינוביץ :

ככה זה נוח?

אילן גפני :

כן, כן, זה נראה לי עדיף,

אלדד רבינוביץ :

אין בעיה,

עפרה ברכה :

כן,

אלדד רבינוביץ :

אין בעיה,

אורי מנחם :

בבקשה.

שלומי בני :

אז אני חוזר חזרה.

אורי מנחם:

אנחנו לא נדלג על שום סעיף, אל תדאג.

עפרה ברכה:

אנחנו מתמקדים בהמלצות העיקריות,

שלומי בני:

נכון,

אורי מנחם:

בסדר גמור.

שלומי בני:

כמו ש - ,

אורי מנחם:

ראשי פרקים,

שלומי בני:

יש בערך 70, אנחנו התמקדנו באמת בדברים היותר משמעותיים,

אילן גפני:

יש 87,

עפרה ברכה:

אתה צריך עותק מהמצגת?

שלומי בני:

87,

עפרה ברכה:

אני רואה שאין לך.

שלומי בני:

שאתם תראו,

עפרה ברכה:

טוב, אנחנו עוקבים על המסך, זה בסדר.

שלומי בני:

בסדר.

אורי מנחם:

צריך להחזיר, סליחה,

עפרה ברכה:

תראה את המצגת.

שלומי בני:

טוב, אז הנושא השני, זה אחראי אבטחת מידע, בעצם אנחנו מצפים שבארגון, כמו ארגון כזה יהיה איזה שהוא ממונה אבטחת מידע, אבטחת מידע וסייבר, גם דרישות התקנות דורשות את זה, גם הבסט – פרקטיס דורש את זה, ובאמת כשאנחנו הגענו, אז אמרו לנו - תראו, היועץ החיצוני שהוא גם היועץ מערכות מידע, הוא גם היועץ אבטחת מידע. אז אנחנו הגדרנו את הממצא הזה, ב - , היועץ החיצוני של החברה אינו ממלא את תפקידו באופן מקצועי, בתחום אבטחת מידע,

אלדד רבינוביץ:

זה לא התחום שלו.

שלומי בני:

כן, בסופו של דבר ראינו את הפערים, אז מיותר לציין ש - , זה לא היה על הצד הטוב ביותר. נושא נוסף זה משתמשי על, אנחנו מצפים בעצם, שבמערכות המידע מי שמשמש על, מי שיגדיר את כל המשתמשים, מי שיהיה הבעל הבית של המערכת, זה לא יהיה המשתמש העסקי, זה לא יהיה סמנכ"ל כספים, או חשבשבת, יש סיבה, כי בסופו של דבר הוא זה שאחרי על כל מערך הכספים, אני לא רוצה שהוא יהיה גם אחראי על המערכת, כי אז הוא יוכל לעשות מה שהוא רוצה,

אלדד רבינוביץ:

עניין של הרשאות.

שלומי בני:

כן, אז הוא יוכל לעשות מה שהוא רוצה, אף אחד לא ידע את זה. נכון? הוא, אז אנחנו רוצים הפרדה, אנחנו רוצים שמנהל מערכות המידע, איש הוא חיצוני שלא מכיר את התהליכים, שלא מעורב בתהליכים, הוא זה שיהיה אחראי על מערכת המידע. אז פה מצאנו משתמשי על, בעצם שהם חלק מהתהליך העסקי, למשל סמנכ"ל הכספים או דבורה ב - , במערכת שהיא מנהלת. נושא נוסף מדיניות סיסמאות, אז אנחנו מצאנו, בעצם בדקנו את מדיניות הסיסמאות גם ברשת, וגם במערכת. מערכת אינפוקס זה מערכת שדרכה משלמים עבור גני הילדים העירוניים,

דבורה מלמד :

גובים,

שלומי בני :

גובים את ה - , משלמים מצד ה - , מצד התושבים, גובים מצד החברה, את ה - , את התשלום עבור גני הילדים העירוניים, ולמעשה מדיניות הסיסמאות גם ברשת הארגונית, וגם במערכת לא היו מספיק נאותים. אורך סיסמא, אתם מכירים מהבנק, נכון?

אלדד רבינוביץ :

8 אותיות גדולות, (לא ברור).

שלומי בני :

אז אתה מבין בסייבר, הוא אמר שלא,

עו"ד דני ליבמן :

הוא מבין בבניין קיים.

אלדד רבינוביץ :

יש לי סיסמאות לקוח בסייבר,

שלומי בני :

זה חשוב. מגנוני בקרה, בעצם גם ה - , גם התקנות דורשות, וגם הבסט – פרקטיס דורש, בסדר? זה שתי דברים שונים, אבל שוב הם מתחברים אחד לשני, שבעצם סט של לוגים, מה זה לוגים? כשאני בא למערכת מידע, מערכת מידע או מערכת אבטחת מידע, אני רוצה לראות מה היה, בחודש האחרון, חודשיים האחרונים, שנה אחרונה, שואלים אותנו למה, למה צריך כל כך הרבה זמן, סיבה מאוד פשוטה, לפעמים תוקף, הוא לא תוקף אותך עכשיו, אלא הוא תקף אותך לפני שמונה חודשים,

אלדד רבינוביץ :

הוא רדום,

שלומי בני :

הוא ממתין כן,

אלדד רבינוביץ :

הוא רדום,

שלומי בני :

יש לו זמן, הוא תקף 20, במקביל הוא רואה מתי נוח לו, ולכן אנחנו רוצים לוגים ארוכים יותר, אוקי, עמוקים יותר, כדי שנוכל לבוא ולתחקר מאיפה הוא נכנס, ולחסום אותו, אז גם,

אלדד רבינוביץ :

זה עוזר גם לשחזור של המערכת?

שלומי בני :

כן, לא לנתונים, למערכת עצמה, שהיא תוכל להמשיך לעבוד, בתשתיות של המערכת עצמה. אז יש לנו בעצם, אז גם, וגם הוראות החוק דורשות את זה, לא סתם, כנראה שיש סיבה. אז גם פה למשל לא ראינו שיש לוגים שנאספים בצורה, ל – 24 חודשים, אגב זה הוראות החוק 24 חודשים, נקוב המספר. תוכנית להמשכיות עסקית, אז תוכנית המשכיות עסקית, זה משהו שהוא לא ספציפי רק ל – IT, אוקי, תוכנית המשכיות עסקית זה בכלל על הארגון עצמו, אוקי, זה הרבה יותר רחב, מאשר רק מערכות המידע, התאוששות אסון, בדרך כלל מדברת על מערכות המידע. אז פה הסתכלנו ראינו שאין לא את זה, ולא את זה, בסדר? מה קורה אם חלילה נופל טיל, או מה קורה אם יש מגפה, או מה קורה יש איזה שהוא שריפה, איך ממשיכים להתחיל, איך ממשיכים לתפעל את ה – , את הארגון. אז נהוג שיהיה איזה שהוא המשכיות עסקית. וחברות יצרניות זה הרבה יותר משמעותי, כי אם זה קו ייצור וכולה. אבל גם פה צריך לעשות איזה שהוא משהו, איך בסופו של דבר אנחנו גורמים לכולם להמשיך לעבוד, גם בזמן שיש מלחמה, והם בתוך הבתים למשל, בתוך מקלטים. התקנים ניידים, התקנים ניידים זה מה שנקרא, אחד המקומות היותר, היותר חלשים, כי בעצם התקן נייד, אני לא, דיסק – קון – קי, מישהו פה אמר מקודם שאי-אפשר להכניס דיסק – קון – קי, זה מצוין שאי-אפשר להכניס דיסק – קון – קי, כי בעצם אנחנו לא יודעים מה הוא עבר לפני כן, נכון? אז בחברה לא היה מנגנון שיועד למנוע, שהגדירו אותו למנוע התקנים ניידים. עדכוני אבטחת מידע, לכולנו יש פלאפונים, לרובנו יש פלאפונים,

ינון נוימן :

למה אתה מסתכל עלי?

שלומי בני :

לא, סתם, לרובנו יש פלאפונים, והם תשימו לב אחת לתקופה הוא צריך עדכון גרסה, נכון? עדכון גרסה כזה מעצבן, תמיד הוא 10.1, או 10.2, ואז אם אתם תסתכלו למה הוא דורש את העדכון גרסה, אז הוא גם ירשום לכם, אז הוא ירשום לכם פיצ'רים חדשים, ירשום לכם, ואחד הדברים שירשום לכם זה הוא ירשום לכם זה עדכוני אבטחת מידע. כי בעצם כל הזמן, בעצם מאתגרים את מערכות ההפעלה, מנסים לתקוף אותם, ואז פתאום מצאו שיש איזה שהיא חולשה מסוימת. ואז החברה שייצרה את מערכת ההפעלה, באה ומעדכנת את הגרסה, כדי שהגרסה הזאת תהיה סגורה, לפרצה שהם מצאו, לכן עדכוני אבטחת מידע הם מאוד מאוד חשובים. עכשיו גם פה יש קריטיים, יש חשובים, ויש נמוכים, בסדר? אז מצאנו פה, ש - , הקריטיים אפילו לא עודכנו. בסדר אם זה היה החלשים, אז אולי לא הייתי מעלה את זה מבין ה - 12 הממצאים החשובים, אבל בגלל שזה קריטי, אז זה מקבל משנה תוקף. ביקורת תקופתית, התקנות דורשות אחת ל - 24 חודשים לעשות ביקורת, לראות ש - , ביקורת פנימית שלך, אוקי, לא המבקרת הפנימית, או המבקר הפנימי, אלא החברה עצמה צריכה לעשות את זה, אחת ל - 24 חודשים, צריכים לעבור, ולראות אם הם עומדים בתקנות עצמם, ואם לא, אז לתקן, אז גם זה לא נעשה, שוב, אמרנו לא היה רישום של מאגרים, אז בוודאי שלא תהיה בביקורת תקופתית. סקר, סקר סיכונים בתחום של סייבר, וגם מבדקי חדירה, זה בעצם שני כלים מאוד חזקים שלנו, כדי להעריך עד כמה החברה יודעת להתמודד עם תקיפה, עד כמה היא חשופה לתקיפות, בסדר? אז נהוג לעשות סקר סיכונים אחת ל - 18 חודשים, או 24 חודשים, זה גם בסדר, ומבדקי חדירה, גם לרשות הארגונים, וגם למערכות, אז פה מעולם החברה לא, לא ביצעה, אני רק אגיד את זה במשפט, שהחברה נפרדה מעיריית ירושלים במערכות, במערכות התשתית שלהם, בשנת 2021, זאת אומרת זה לא שהחברה היה לה תשתיות משנת 98, ואני בא ואני אומר - תשמעו, כמעט 20 שנה לא עשו, אלא יש פה איזה שהוא כוכבית ש - , אנחנו הגענו ל - 24, 3 שנים, נכון, זה הרבה זמן, אבל עדיין זה לא 30 שנה,

אלדד רבינוביץ:

ראיתי שעשית.

שלומי בני:

נכון, נכון, אנחנו עשינו מבדקי חדירה, לתשתיות, לראות אם אפשר להיכנס אם אפשר לחדור אל התשתיות, וחלק מהממצאים, תיכף נראה אותם גם כן בהמשך, הם כתוצאה מהמבדק חדירה. אז זו ההערה, אז הנה הגיעו הממצאים הבאים, שזה, כמו שאמרתי אנחנו לא נרד עכשיו לאיך (לא ברור) את ה - FIREWALL וכולה, או את האקטיב - דירקטורי, אבל בגדול בחלק מהבדיקות שעשינו, כולל מבדקי החדירה, למעשה מצאנו שיש פערים בהקשחות, בעצם בהגדרות, של מערכת אקטיב - דירקטורי, שזה מערכת שמנהלת את כל המשתמשים בארגון, כל ה - 60 משתמשים, אוקי, אולי גם יותר, כי זה לא רק משתמשים שהם בני אדם, גם כל מיני משתמשי באפליקציות. וגם עמדות הקצה, זאת אומרת המכשירים עצמם, צריך להקשיח אותם, אוקי, שלא כל אחד, שלא, אי-אפשר להיות אדמיניסטרטור, משמש על על המחשב, שלא יהיה אפשר להתקין דיסק - קון - קי וכולה. ו - FIREWALL שזה חומת אש, שבעצם חומת אש זה בעצם החומה שלנו, מערכת ההגנה שלנו, בין

העולם החיצון, לרשת הארגונית, אז יש פה איזה חבילה של איזה 20, 25 ליקויים, תלוי איך סופרים את זה, ושמנו את זה בשקף אחד, כי באמת זה לא ייתן לכם יותר מידי מידע, אם אני אגיד לכם את ההגדרה, אבל זה ממצא שהוא משמעותי, שהוא בעל ערך משמעותי, אני חושב שחלק מהדברים כבר טופלו, גם חלק מהשיחות שהיו לנו. טוב, אז אם אני, אם אני אסכם, בסדר? את כל מה שאמרתי, ואתם מוזמנים לשאול שאלות, כן, אני, אני מקווה ש - , הייתי ברור, אבל אם לא תשאלו שאלות, אם אני מסכם, בגדול, המצב בחברת אריאל היה, לא מספיק טוב, בסדר? נקרא לזה ככה, לא, לא מספיק טוב, דורש הרבה מאוד שיפור.

עו"ד דני ליבמן:

טעון שיפור, בדיוק.

שלומי בני:

טעון שיפור, המונח היותר נכון,

עו"ד דני ליבמן:

טעון שיפור.

שלומי בני:

טעון שיפור, כן, כן, טעון שיפור, והרעיון הוא, הרעיון הוא להביא אותו לטוב מאוד, בסדר? גם אם לא מצוין, אנחנו לא בנק, זה לא בנק, וזה לא תעשייה אווירית, זה בכל זאת זה חברה עירונית, וחשוב והכול, אבל צריך להביא אותו לכיוון 9, בסדר? אז הוא היה ב - 5, גם בנושא של הוראות החוק, חייבים לעמוד, שם אנחנו צריכים להיות 10, כן, אתה לא יכול להגיד אני 9 בהוראות החוק. הוראות החוק אתה צריך להיות 10, שמה בדברים של הבסט - פרקטיס, אתה יכול להיות 9, זה בסדר, יש מקומות 9.2, יש יכול להיות 8.8, זה בסדר. ובאמת זה אני חושב המטרה שהייתה לעפרה וינון, ולי, באמת לתת את הממצאים שבסופו של דבר יטופלו, ובאמת תעלה רמת אבטחת, אבטחת המידע והסייבר של הארגון.

אלדד רבינוביץ:

תודה רבה.

אילן גפני:

אז מה שאנחנו עשינו אני אשמח עכשיו לקבל, זה או זה.

מודי בן אבו:

המחשב מחובר.

אורי מנחם:

תקלה באבטחת מידע, הצלחת להתחבר.

ינון נוימן:

דיסק – קון – קי וכל מיני.

אילן גפני:

הוא רצה לבדוק שאי-אפשר,

שלומי בני:

הוא רצה לבדוק ערנות.

אילן גפני:

הטבלה הזאת שהצגת, זה גם אפשר. אוקי, יופי, תודה. כמו שאורי אמר, דרך אגב השקף הסופי, ואני תיכף אפרט ואני אסביר מה עשינו. אנחנו נמצאים בהשלמה של 62 מתוך 71% של הסעיפים שעלו בדו"ח. 21% נמצאים,

אורי מנחם:

זה לא אחוזים, אתה מדבר על אחוזים,

אילן גפני:

לא, 71%, 62 סעיפים מתוך 87, הלכתי ופרטתי את הדו"ח רב העמודים לנושאים, לשורות, שורות, שורות, מה שאתם יכולים לראות פה, לאיפה זה הגיע, ואיזה עמוד השורה, איפה נמצא אפילו הצילומים שעשית, בעצם פרטנו את זה שיהיה נוח לעבוד, והתחלנו לעבוד. אלה התוצאות, ותיכף אני אסביר מה עשינו. כמו שאמרתי 71% כבר בוצעו, 21% ממש נמצאים בתהליך, תיכף אני אסביר למה. יש אחוז, יש אחד שנמצא בבדיקה, מכיוון שזה איזה שהוא שינוי שנדרש שעלול להשפיע בצורה מאוד מאוד רחבה, על המערכות, בעיקר על המערכות הקריטיות שלנו, שהם בקרת הכניסה.

מודי בן אבו:

כרטוס.

אילן גפני:

כרטוס ובקרת הכניסה, המצב שבו מגיעים אלפי צופים, ונכנסים דרך השערים, גם המערכות האלו עובדות על שרתים, ופה צריך להיזהר מאוד מאוד מאוד, כי יקרו דברים גרועים אם לא נעשה את זה. מתוך 6 ההמלצות, דחינו, מתוך סליחה, 87 ההמלצות, דחינו 6 המלצות, 5 המלצות קיימות, היו קיימות, הראינו,

אורי מנחם:

הראנו שהם קיימים.

אילן גפני:

מסמכים, הראנו מסמכים, קצר בתקשורת. אני מודה הבחור שעבד מולם לא תמיד היה משתף פעולה,

אורי מנחם:

שירותי.

אילן גפני:

שירותי ומשתף פעולה, הוא כבר לא נמצא איתנו יותר. ולכן זה כנראה לא עבר, והמלצה אחת, שהיא בעצם המלצה של, הנושא של חיבורים פיזיים,

שלומי בני:

(לא ברור).

אילן גפני:

כן, בדיוק. המלצה אחת שאומרת, לא יכול להיות חיבור כמו פה פתוח, בגדול, כדי שמישהו יוכל לבוא ולהיכנס, ההחלטה של הנהלת החברה הייתה, המקום מוגן, סגור, הרבה יותר מהעירייה, אי-אפשר להיכנס ככה סתם, ואנחנו לא רואים מצב שמישהו יבוא, וממש ידחף,

שלומי בני:

החלטה סבירה נקרא,

אילן גפני:

נדחף, כן,

שלומי בני:

החלטה סבירה.

עפרה ברכה:

טוב.

אילן גפני:

אז זה מה שעשינו. בעצם כשהלכנו וחילקנו את כל ההמלצות, פירקנו את זה, אני שוב, אני לא אעבור אתכם, אבל אתם יכולים לראות, ולא רק שככה,

אלדד רבינוביץ:

יש לי שאלה,

אילן גפני:

היו תהליכים,

אלדד רבינוביץ:

תעבור, אבל באמת יש איזה שהוא מדרוג של ההמלצות?

אילן גפני:

כן,

אלדד רבינוביץ:

זאת אומרת הקריטיות טופלו, הקריטיות בבדיקה?

אילן גפני:

זה לא בדיוק הקריטיות, אנחנו טיפלנו בכל ההמלצות, חוץ מאחת, כמו שאמרנו. והמדרוג, וכמו שאתם רואים היו מספר דיונים כולל עם שלומי, אנחנו חילקנו את זה ככה, המלצות בדבר, רשת התקשורת, בוצעו מידית, כל נושא של סיסמאות של החלפות, של עניינים כאלה, אלה ההמלצות שבוצעו. כל ההמלצות בנושא של הגנת הפרטיות, תחום שלא היה בכלל בחברה, ועשינו בעצם איזה שהוא תהליך מול חברות שמתמחות ביעוץ הגנת הפרטיות, הבאנו חברה חיצונית, שנבחרה, החברה הזאת עשתה דו"ח מקיף מאוד מאוד הרבה יותר מהדוח בעצם, מהנתונים שאתם נתתם, ונתנה לנו דו"ח משלה עם המלצות רבות, כמו שאני אומר שוב, מעבר לדו"ח הביקורת, יישמנו את כל ההמלצות האלה, זה לקח הרבה מאוד זמן, כולל רישום על מאגרי המידע, כולל אבטחה, כולל רישום, כל הנכסים.

אלדד רבינוביץ:

זאת אומרת יש עמידה בכללי החוק,

אילן גפני:

לגמרי.

מודי בן אבו:

הוספנו עוד מאגרים, סליחה, שאני קוטע אותך,

אילן גפני :

כן,

מודי בן אבו :

חוץ מהמאגרים ששלומי ציין.

אילן גפני :

למשל, למשל מצלמות,

מודי בן אבו :

נכון,

אילן גפני :

מצלמות, אם אתה שומר עד 30 יום, אתה לא חייב לרשום, אז אנחנו לא נכנסנו לכל הזה, אבל,

מודי בן אבו :

אבל היה (לא ברור), ועשינו וכן,

אורי מנחם :

אמרנו לפחות שלושה, היה לפחות שלושה.

אילן גפני :

יפה, אז בהחלט עשינו כמו שאורי אמר, לקחנו את זה ברצינות, הכי גדולה, ביצענו את כל הדברים האלה. כשאתם רואים פה, כשרשמתי, שבחלקם עדיין בתהליך זה פשוט,

אורי מנחם :

כל מה שאתם רואים, בטבלה שהוא רץ.

אלדד רבינוביץ :

כן, כן,

אורי מנחם :

אתם רואים את העמודה בוצע, בוצע, בוצע, בוצע,

אלדד רבינוביץ :

כן,

אורי מנחם :

אז עכשיו הוא יורד למה שנקרא בביצוע,

עפרה ברכה :

התכלת,

אילן גפני :

אז עכשיו הביצוע זה ככה, מעבר, חוץ מהדו"ח הראשוני, ובעצם היישור קו לעמידה בתקנות בסעיף 13, של הגנת הפרטיות, אנחנו מביאים שני אנשי מקצוע חיצוניים, בדיוק כמו שאמרת, מומחה הגנת פרטיות, זה אותו, זה די.פי.או מה שרשום פה, ומומחה אבטחת מידע. עשינו גם בנושא הזה תהליך מול מספר חברות, פנינו למספר חברות, קיבלנו הצעות, ובעצם אנחנו רק מחכים שמנהל הכספים יגיע,

דבורה מלמד :

מסכימה.

אילן גפני :

כן, כדי להוציא את הזמנת העבודה, ויהיה לנו ליווי שוטף,

אורי מנחם :

יש כבר החלטה,

אילן גפני :

יש החלטה, יש החלטה,

אורי מנחם :

זה רק התקשרות.

אילן גפני :

רק צריך להוציא את הזמנת העבודה. ויהיה לנו ליווי שוטף של ממונה הגנת הפרטיות, מהחברה ושל אבטחת המידע.

אלדד רבינוביץ :

אשמח אם אפשר לעדכן את וועדת הביקורת, כשזה קרה, תשלחו לנו מייל.

מודי בן אבו :

מעולה.

אילן גפני :

אז יש לנו את הליווי, את הליווי הזה, והדבר האחרון, זה כל נושא של אמרת, של שמירת הלוגים, של בדיקה, של אירועי עבר וכן הלאה. גם בזה עשינו, יצאנו בעצם מכרז, בדקנו הרבה מאוד אפשרויות של מערכות, אלא מערכות לא זולות. ובסוף התקבלה החלטה גם בזה, כבר התקבלה החלטה, ללכת עם מערכת של משכ"ל של מרכז השלטון המקומי, יש להם איזה שהוא מערכת שהם מציעים של חברת נס, שמפעילה צ'ק - פוינט, וכן הלאה, שוב מעבר אפילו לדרישות דו"ח הביקורת, אנחנו ניישם את המערכת שלהם, ואז בעצם כל נושא, לוגים, שמירות, גיבויים, המשכיות עסקיות, וכל הדברים האלה מנוהלים על ידם בתשלום חודשי.

אלדד רבינוביץ :

מתי היא הייתה אמורה להיות מיושמת? או אמורה להיות מיושמת?

אילן גפני :

שוב, המערכת נבחרה, ופשוט אנחנו מחכים להזמנת העבודה.

אורי מנחם :

אנחנו נעדכן, אני מקבל את מה שאתה מבקש, דבורה, ברגע שאנחנו מסיימים את ההתקשרות, הודיעו פה,

דבורה מלמד :

נוציא את ה - ,

אורי מנחם :

בכתב, בצורה מסודרת שהשלמנו את המהלך של, מה שנקרא של הליך ההתקשרות, ובזה,

אילן גפני :

אני מקווה ששבוע הבא כבר.

אלדד רבינוביץ :

אז כן, למבקר עם העתק אלי.

אילן גפני:

כמו שאמרתי בדיקה של נושא אחד, שאנחנו פשוט חייבים לראות שהוא באמת לא משפיע על, על כל מערכות הכניסה שלנו, ומספר נושאים, כמו שאמרנו שנשלחו,

אורי מנחם:

כי הם היו, זה לא שהם לא היו,

אילן גפני:

כן, הם היו,

אורי מנחם:

זה כן,

אילן גפני:

נושאים שהיו, והנה אותו אחד שלא נדחה, ולא היה, זה אותה הגנה שטענו ש - , השמירה הפיזית במקום היא מספיק טובה, זאת אומרת בעצם אנחנו נמצאים כמו שנאמר ב - 99% השלמה, או הצגה בעצם של דברים שהיו, ואחרון, אולי נשאר אותו ככה בשביל שיהיה,

שלומי בני:

שיהיה משהו,

אילן גפני:

כן,

אורי מנחם:

שניפגש עוד פעם,

שלומי בני:

שלא (לא ברור).

אילן גפני:

זהו, יפה.

עפרה ברכה:

תודה רבה, איך אמרת בהתחלה? זה סוג של דוחות שעושה לי נחת, לא החלק הראשון של הדו"ח עצמו שפחות הייתה לי נחת. אבל אחרי זה, איך שאריאל לקחה וכל התהליך שהיא עשתה המקצועי,

עם שינוי ביועץ, וכל הפעילות שראינו כרגע, אז מבחינתי המטרה הושגה ו - , זה בדיוק התפקיד שלנו, ו - , מבחינתי כשדו"ח ביקורת הופך להיות תוכנית עבודה זה בסדר.

אלדד רבינוביץ :

עוד משהו רוצה להתייחס? אז גם אני אסכם, אז באמת אני מברך את המבקר, בכלל על הדו"ח, דו"ח משמעותי וחשוב, אני מברך ומודה לאורי, שלקחתם ואימצתם את הדו"ח בשתי ידיים, תיקנתם עשיתם, אני חושב שהדבר הזה הוא משמעותי, גם לכם, כחברה, גם לנו כירושלים, וגם לציבור, בסוף ש - , הרבה אנשים מכניסים את הפרטים שלהם אצלכם, והרבה נכנסים ל - , לכל מיני דברים שאתם עושים, אז תודה לכולם על העבודה המקצועית ועל השיתוף הפעולה, מקבלת את המלצת הדו"ח בכפוף להערות והוספות לעיל, וממליץ לוועדה המקומית לאמץ את מסקנות הוועדה, הישיבה נעולה.

עפרה ברכה :

תודה רבה.

אורי מנחם :

תודה רבה.

עו"ד דני ליבמן :

להמליץ למועצה.

אלדד רבינוביץ :

מה?

עו"ד דני ליבמן :

להמליץ למועצה.

עפרה ברכה :

כן, כן, הוא אמר לוועדה,

אלדד רבינוביץ :

למועצה, אתה צודק, אני,

עפרה ברכה :

למועצה, טעון שיפור.

שלומי בני:

אז צריך להתחיל את הישיבה מהתחלה?

עפרה ברכה:

אתה תהרוג אותנו וזה, להיות פה בחדר הזה כל כך הרבה שעות זה.

שלומי בני:

אורי, תודה.

סיום הדיון