כ״ט בחשון תשפ״ו
20 בנובמבר 2025
סימוכין: 2025-103-957

<u>דו״ח מישיבה מס׳ 21 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
מר יובל אגמון, סמנכ״ל חטיבת משאבים והתקשרויות בחברת מוריה
מר עומר סטביסקי, ראש אגף ביקורת במוריה
גב׳ לימור גמיש, אגף בקרה וביקורת במוריה
מר שי פרידמן, יועץ מטעם חברת מוריה
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 מוריה (חברה לפיתוח ירושלים בע״מ)

<u>פתיחת הדיון:</u>

<u>מר אלדד רבינוביץ, יו״ר הוועדה</u>: אנחנו בסדרה של דוחות העוסקים בסייבר והגנת הפרטיות. את הדוח ערך מבקר מאוד מקצועי. מברך את המבקרת ואת המבקר, על הדוח.

כפי שאמרנו, דוח הביקורת חשוב מאד. הרבה מהתקיפות כיום נמצאים דווקא באזורים של סייבר וכך גם הרבה מהפגיעה בפרטיות נמצאת במרחב האינטרנטי.

<u>גב׳ עופרה ברכה, מבקרת העיריה</u>: תחום הסייבר חשוב מאוד ובא להגן על החברה. בדוח זה מדובר בחברת מוריה שיש בה פעילות ענפה בירושלים.

<u>דיון הוועדה:</u>

פרק 1:

<u>המלצת המבקרת:</u>

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

<u>תגובת המבוקר:</u>

רוב הליקויים טופלו. אנו בוחנים עם יועץ האבטחה שלנו כיצד לתקן ולא לפגוע בנתונים במסד הנתונים. צופים שיטופל עד תחילת השנה החדשה.

<u>המלצת ועדת ביקורת:</u>

לקבל את המלצות המבקרת.

בנוסף, עד סוף השנה הקלנדרית תשלח חברת מוריה עדכון למבקרת וליו"ר ועדת הביקורת בנוגע למסד הנתונים.

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>

טופל

<u>המלצת ועדת ביקורת:</u>

לקבל את המלצות המבקרת.

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>

טופל

<u>המלצת ועדת ביקורת:</u>

לקבל את המלצות המבקרת.

פרק 4:

<u>המלצת המבקרת:</u>

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

<u>תגובת המבוקר:</u>

מרבית הנקודות טופלו למעט שתי הערות שדורשות החלפת מערכת, הן בטיפול כעת. אנו מקדישים את כל המאמצים הנדרשים על מנת לבצע את כל ההמלצות.

<u>המלצת ועדת ביקורת:</u>

לקבל את המלצות המבקרת.

בנוסף, בתוך 30 ימים חברת מוריה תשלח עדכון למבקרת וליו"ר ועדת הביקורת בנוגע להחלפת המערכות.

<u>סיכום:</u>

<u>מר אלדד רבינוביץ, יו"ר הוועדה</u>: שוב אודה ואברך את המבקרת והמבקר על הדוח החשוב.

אני שמח ש'בזבזנו' את הזמן על דוח שהממצאים בו לא משמעותיים ושתוקנו ברובם.

בעיני, חלק משמעותי מעבודת הביקורת זה לפעול באופן רוחבי, לעיתים גם מבלי לדעת מראש את תוצאות הבדיקה. כך יוצא שלעיתים יש ממצאים משמעותיים ולעיתים לא. מאוד משמח כשלא.

מודה גם לחברת מוריה על העבודה המקצועית והרמה גבוהה של ההתייחסות לתחום אבטחת המידע והסייבר.

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 חמישי

אבטחת מידע וסייבר בחברת מוריה

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 // 115

מבוא // 118

פירוט הממצאים

פרק ראשון:
בדיקת רגולציה, מדיניות, נהלים ותהליכים בתחום אבטחת מאגרי מידע // **הושמט**

פרק שני:
מבדק מערכות אבטחת מידע // **הושמט**

פרק שלישי:
מבדק חדירה פנימי // **הושמט**

פרק רביעי:
מבדק חדירה חיצוני // **הושמט**

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.

אחת הדרכים הנפוצות לבחון את מערכות האבטחה של ארגון היא באמצעות מבחני חדירה. מבחני החדירה נועדו לבדוק את הפרצות הקיימות ברשת הארגון או במערכת הנבדקת. הבדיקות מבוצעות בדרך כלל באמצעות כלים אוטומטיים לצורכי מיפוי, סריקה ואיסוף מידע, וכן באמצעות בדיקות ידניות.

הביקורת בדקה את מידת עמידת החברה בנושא אבטחת המידע, וכן ערכה מבדק טכנולוגי לבחינת רמת האבטחה הקיימת בה, בדיקה פיזית לאבטחת המידע ומבדקי חדירה לרשת החברה ולמערכות נוספות.

הביקורת העלתה ליקויים בנושאים האלה: יישום הקשחות עמדות קצה ושרתים, ניהול מערכת האנטי-וירוס, ניהול מערכת חומת האש, ניהול מערכת ה-AD (Active Directory - מערכת לניהול משתמשים), וכן ליקויים בעלי חשיבות גבוהה במבדקי החדירה שהיא ביצעה.

עיקרי הממצאים

1. לא קיים רכיב אשר נדרש לצורך הגנה על המידע.
2. נמצאו כמה ליקויים בתחזוקת מערכת חומת האש.
3. נמצאו כמה ליקויים בערכת ה-AD שאינה מוקשחת מספיק.
4. במבדק החדירה הפנימי והחיצוני לרשת החברה נמצאו מספר הקשחות שלא הוגדרו.
5. מערכת הדואר האלקטרוני אינה מפעילה תוסף נדרש בהתאם לפרקטיקה המקובלת.
6. באתר האינטרנט של החברה נמצאו כמה ליקויים בהקשחות.
7. במבדק חדירה שבוצע לשתי מערכות של החברה, נמצאו כמה ליקויים, מקצתם בעלי סיכון גבוה.

המלצות מרכזיות

1. להתקין רכיב אשר נדרש לצורך הגנה על המידע.
2. להקשיח את מערכת חומת האש.
3. להקשיח את מערכת ה-AD.
4. להגדיר את ההקשחות בהתאם לממצאים במבדקים הפנימיים והחיצוניים שבוצעו.
5. להתקין תוסף הנדרש בהתאם לפרקטיקות המקובלות במערכת הדואר האלקטרוני.
6. להגדיר את ההקשחות הנדרשות באתר האינטרנט של החברה.
7. לטפל בליקויים שנמצאו במערכות החברה, בהתאם לרמת הסיכון שהוגדרה על ידי 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.

סיכום

חברת מוריה 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.

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

בחברת מוריה יש כחמישים משתמשים המוגדרים במערכות המידע שלה. יש לה כמה מערכות מידע לניהול תהליכי העבודה וכן כמה פורטלים בעלי חשיבות גבוהה.

הביקורת בדקה את מידת עמידת החברה בנושא אבטחת המידע, וכן ערכה מבדק טכנולוגי לבחינת רמת האבטחה הקיימת בה, בדיקה פיזית לאבטחת המידע ומבדקי חדירה לרשת החברה ולשתי מערכות שלה.

הביקורת העלתה ליקויים בנושאים האלה: יישום הקשחות עמדות קצה ושרתים, ניהול מערכת האנטי-וירוס, ניהול מערכת חומת האש, ניהול מערכת ה-AD (Active Directory – מערכת לניהול משתמשים), וכן ליקויים בעלי חשיבות גבוהה במבדקי החדירה שהיא ביצעה.

על החברה לטפל בממצאים שהועלו בהקדם, בדגש על הפערים הטכנולוגיים שנמצאו, לרבות במבדקי החדירה של המערכות.

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 מוריה לפיתוח ירושלים בע"מ היא החברה העירונית הגדולה ביותר ונמנית עם חברות התשתית הבינוי והפיתוח הגדולות בישראל. החברה משמשת כזרוע הביצוע המרכזית של עיריית ירושלים ומשרד התחבורה, ומופקדת על הפרויקטים המרכזיים והחשובים בעיר ירושלים ובמטרופולין.

בין הפרויקטים המובילים שמקדמת מוריה בירושלים: הקמת קווי הרכבת הקלה (אינפרא 1), כבישים ועורקי תחבורה ראשיים, מנהרות וגשרים, נתיבי תחבורה ציבורית, חניונים תת-קרקעיים, פיתוח שכונות חדשות, פארקים וגינות ציבוריות, בניית מבני חינוך ומוסדות ציבור, מבני דת ועוד.

במהלך שנת 2023 ביצעה החברה כ-300 פרויקטים, בהיקף ביצוע שיא של כ-3.1 מיליארד ש"ח.

בשנים האחרונות ישנה עלייה מתמדת בהיקף ובעוצמת האיומים במרחב הסייבר בעולם כולו ובישראל בפרט, איומים היוצאים אל הפועל באמצעות תוכנות זדוניות (נוזקות וכופרות) המתפשטות דרך רשת האינטרנט, דרך הדואר האלקטרוני, או באמצעות חיבור פיזי של התקני זיכרון למיניהם למחשבים ברשת הארגונית. התקיפות נעשות מתוחכמות יותר ויותר על ידי אוטומציה והפצה המונית שלהן. 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.

בחברת מוריה יש כחמישים משתמשים המוגדרים במערכות המידע שלה. יש לה כמה מערכות מידע לניהול תהליכי העבודה וכן כמה פורטלים בעלי חשיבות גבוהה.

לחברה כמה אתרים (אתרי Web) כלהלן:

- אתר ראשי – פותח על ידי הספק "דובל פתרונות דיגיטליים". האתר כולל בתוכו מידע על החברה, על מבנה ההנהלה, על פניות לציבור, על אודות הפרויקטים ועוד.
- אזור אישי מנהל פרויקטים – האתר יושב על שרתי החברה ונבנה לצורך ניהול הפרויקטים שלה. הכניסה לאתר מוגבלת למנהלי הפרויקטים באמצעות שם משתמש וסיסמה.
- פורטל ספקים – האתר מתממשק למערכת "פריורטי" (Priority Software) ומקנה לספקים את האפשרות לניהול חשבוניות והתחשבנות מול החברה. הפורטל בבעלות חברת FBC (חברת יישום והטמעה של מערכת הפריוריטי ואתרי Web המתממשקים לפריוריטי) הכניסה לאתר היא באמצעות שם משתמש וסיסמה (כולל Multi Factor Authentication - MFA).
- פורטל פניות הציבור – פורטל שבאמצעותו ניתן להגיש טפסים בעניין נזקי גוף ורכוש. בפורטל הפונים נדרשים להזין פרטים אישיים (שם פרטי, שם משפחה, ת"ז, טלפון וכו'), לתאר את האירוע ולהעלות מסמכים רלוונטיים.
- פורטל מתכננים – פורטל המאפשר רישום למאגר המתכננים של מוריה, הגשת טפסים למכרזים, מתן הצעות מחיר וכדומה.

צוות אבטחת המידע של החברה הוא ספק חיצוני (Primesec) המעמיד גורם מטעמו לשמש כממונה אבטחת המידע של החברה (chief information security officer – CISO). נוסף על כך, קיים ספק חיצוני (בינת סמך) אשר מספק שירותי תמיכה עבור התשתיות ומערכות המידע באופן כללי.

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.

היקף הבדיקה

נערכו בדיקות כלליות של אבטחת מידע במאגרי המידע וברשת, ושל מערכות אבטחת המידע, וכן נערכו מבחני חדירה.

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

תקופת הביקורת

הביקורת נערכה בחודשים אוגוסט – אוקטובר 2024.

דוח שנתי 2024

הגנת הפרטיות, אבטחת מידע וסייבר בחברת מוריה

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

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

בהתאם, במהלך השנים האחרונות היינו עדים למספר מתקפות סייבר על גופים ציבוריים. העירייה בראשותי מתייחסת לאיום הסייבר ברצינות מלאה וביצעה פעולות רבות בהשקעת משאבים לא מבוטלת, בכדי לוודא כי היא תהיה במוכנות מספקת למתקפה. כמובן שגם התאגידים העירוניים, המהווים את הזרוע הארוכה של עיריית ירושלים ופועלים בשם העירייה, נדרשים לפעול בסטנדרטים דומים ולא פחותים מאלה של העירייה. הדברים נכונים ביתר שאת, לתאגיד עירוני כגון מוריה, שהוא התאגיד העירוני הגדול בישראל מבחינת היקף הפעילות שלו והוא מבצע פרויקטים בהיקפים עצומים, חלקם בעלי חשיבות לאומית.

אני רואה חשיבות גדולה בטיפול מהיר בליקויים שהתגלו. אבטחת מידע וסייבר נועדו להגן על התאגידים העירוניים וכפועל יוצא מכך על הציבור. ניתן רק לתאר את הכאוס האפשרי שעלול להיגרם כתוצאה מהשבתת תשתיות או השמדה של מאגרי מידע על ידי גורמים עוינים או בשוגג. על חברת מוריה להתייחס לאיומי הסייבר כאיום על פעילותה הרציפה והסדירה לכל דבר ועניין.

הביקורת מצאה ליקויים בהתנהלות חברת מוריה בעניין זה. בין היתר, נמצא כי לא קיימת הצפנה למסד הנתונים של החברה, וכי מערכת חומת האש המותקנת בחברה עושה שימוש בפרוטוקול לא מאובטח. כמו כן, מערכת ה-AD (מערכת לניהול משתמשים) אינה מוקשחת מספיק, ובמבדקי החדירה הפנימיים והחיצוניים נמצאו ליקויים שונים. בנוסף, נמצא כי כתובות הדוא"ל האישיות של הנהלת החברה חשופות לתקיפת דיוג (Fishing), וכי מערכת הדוא"ל אינה מפעילה תוסף למניעה של דלף מידע (DLP). כמו כן, נמצאו ליקויים בהקשחות אתר האינטרנט של החברה.

אני מברך על תגובת גורמי המקצוע מטעם מוריה ממנה עולה כי הם מקבלים את רובן של ההמלצות לרבות ההמלצות הנוגעות לפורטלים ואף העבירו את הטיפול בעניין לספק האתר. עוד עולה כי חלק מהמלצות הביקורת כבר יושמו על ידי החברה כגון עדכונים במערכת חומת האש ומערכת ה-AD. כמו כן, גורמי המקצוע התחייבו לפעול בכובד ראש על מנת לאמץ את שאר המלצות הביקורת ואף לאמץ את חלקן עוד במהלך שנת 2025. תגובתם מעידה על רצון אמיתי לשיפור וטיוב התנהלות החברה בנושא זה לטובת הציבור.

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

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

הוועדה לביקורת – תמליל

מספר הוועדה: 21
מקום ההתכנסות: אולם חדר ישיבות קומה 0
תאריך הוועדה: ו׳ בתמוז תשפ״ה (2.7.2025)
מזכיר הוועדה בדיון: צבי אבו
שעת תחילת הוועדה: 14:50
שעות סיום הוועדה: 15:06

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.

יו״ר אלדד רבינוביץ:
שלום לכולם, אני מתכבד לפתוח את הדיון, וועדת הביקורת מספר 21, אבטחת מידע וסייבר, לחברת מוריה, חברה לפיתוח ירושלים בע״מ בסוגריים. כמו שאמרתי בוועדה הקודמת, זה לא התחום שלי, עם זאת זה תחום,

ינון מלמד:
זה הולך ומשתפר אבל עד ה - ,

אלדד רבינוביץ:
כן, זה אני לומד,

ינון מלמד:
דיון הבא,

אלדד רבינוביץ:
לומד מאחד לאחד. דיון מאוד מאוד חשוב, דו״ח ביקורת מאוד מאוד חשוב, בסוף, בסוף כולנו היום הולכים לאזורים של סייבר, היום הרבה מהתקיפות הם באזורים של סייבר, הרבה פגיעה בפרטיות נמצאת במרחב האינטרנטי, במרחב ה - , מרחבי המחשוב, יש לנו מבקר מאוד מקצועי, מברך את המבקרת, ואת המבקר, על הדו״ח הזה. יש לך מה לומר?

עפרה ברכה:
הרחבנו כבר בישיבה הקודמת על החשיבות של הנושא הזה, בסוף אנחנו באים ואנחנו במידה מסוימת מגנים על החברה פה, אנחנו מדברים על חברת מוריה עם פעילות מאוד אנפה. וכמובן לטובת הציבור, אנחנו נבקש משלומי שעשה את הביקורת, להציג את עיקרי הדברים.

אלדד רבינוביץ:
ככל הניתן אני אשמח כשעולה ממצא, תגיעו אליו אחד אחד, שאנחנו לא מפספסים.

שלומי בני:
אז נעים מאוד, למי שאני לא מכיר, או שלא מכיר אותי, שלומי בני, שותף ב – RSM, ואני בעצם ערכתי את הביקורת יחד עם הצוות מטעמי, בנושא של אבטחת מידע וסייבר, בחברת מוריה. אז כמה מילים, מוריה היא חברה מאוד גדולה של, חברה עירונית מאוד גדולה, שבעצם אחראית על תשתיות משמעותיות, ברחבי עיריית ירושלים, אם זה הקמת קווי הרכבת הקלה, כבישים, צמתים, וכולה. חברה מאוד גדולה, חברת תשתיות, אני חושב אחת היותר גדולות בישראל אפילו. ולמעשה אנחנו פה עשינו טיפה ביצענו ביקורת אבטחת מידע וסייבר, לא נגענו בתקנות הגנת הפרטיות, אני לא אתייחס לדו״ח הקודם, כמובן רק אציין פה, שפה התמקדנו יותר בנושא של אבטחת מידע

וסייבר, כי מסקר ראשוני שראינו, על פניו היו נראים, נראים שהדברים מטופלים בנושא של תקנות הגנת הפרטיות. ולכן לא רצינו להעמיק במשהו שהיה נראה לנו על פניו תקין, והעדפנו לקחת את התשומות, לנתב אותם למקומות קצת שונים, אז אתם תראו פה קצת טוויסטים בבדיקות שלנו. אז הדבר הראשון, לא הייתה, אני חייב להגיד, שרמת האבטחה בסך הכול הייתה יחסית טובה, בסדר, יחסית טובה, הייתה ברמה טובה.

<u>אלדד רבינוביץ:</u>
פתיחה טובה.

<u>שלומי בני:</u>
טובה, טובה פלוס, אפילו אני אגיד, טובה פלוס.

<u>עומר סטיביסקי:</u>
אתה יכול להגיד טובה מאוד,

<u>שלומי בני:</u>
לא, לא, לא, הייתה טובה פלוס. ולכן אנחנו השתדלנו ללכת לכיוון של מבדקי החדירה, לפורטלים של ה - , של החברה, יש להם כמה פורטלים, בדקנו כמה, אתם תראו גם כן את מה שמצאנו, אבל בסך הכול באמת המצב היה טוב, יחסית. התקשינו למצוא, אבל מצאנו בסוף. הצפנת מסדי נתונים. מסדי נתונים שמכילים מידע רגיש, אם זה לקוחות, ספקים וכולה, נתונים פיננסיים, מצפים ש – , יצפינו את ה - , את הנתונים. אתם רוצים להגיב?

<u>יובל אגמון:</u>
זה, זה נתון, אנחנו בדיוק בבחינה, יש מכל ההמלצות אני גם, בכל ההמלצות, לדעתי זה, יש עוד משהו שנוגע לספק חיצוני שאולי ניתקל בו בהמשך, שאנחנו בתהליך חלופה שלו, וזה הנושא בעצם שעדיין לא, לא טיפלנו. אנחנו בוחנים את זה, גם בוחנים עלויות, חשוב להבין המסד נתונים הזה, זה אנחנו עוברים מערכת, זה מסד נתונים של המערכת הקודמת שלנו, ויש שם נתונים של תושבים, או משהו כזה, אז אנחנו בוחנים, גם עלויות, עלויות בדיוק קיבלנו הצעות מחיר, ואת החשיבות, המשמעות, מבחינת כאילו הפגיעה ו - , בוחנים, מול היועץ אבטחת מידע שלנו, אנחנו בעצם נעשה את ההצפנה הזאת, או שכבר, נכיל אותה כבר על ה - , על המערכת החדשה, שאנחנו עובדים עליה, שכבר,

<u>שלומי בני:</u>
תוך כמה זמן אתם עוברים?

<u>יובל אגמון:</u>

אנחנו בתחילת,

שי פרידמן:
עד סוף שנה,

שלומי בני:
עד סוף שנה?

יובל אגמון:
כל המערכת הכספית, בעצם כבר עברה למערכת, מערכת פריוריטי, אנחנו בתחילת שני נתיבים,

שלומי בני:
זאת אומרת פחות, פחות מחצי שנה,

יובל אגמון:
פחות מחצי שנה, אנחנו כבר מעבירים,

שלומי בני:
כן, זה באמת,

שי פרידמן:
מערכת שהיא SAAS,

יובל אגמון:
עושים איזה שהוא,

שלומי בני:
כן.

שי פרידמן:
שכבר סס ו - ,

יובל אגמון:
באמצע נתונים, לא של תושבים, ולא נתונים אישיים, ולכן,

שלומי בני:אוקי,

יובל אגמון:
בסוף,

שי פרידמן:
אנחנו בוחנים את הדבר הזה.

שלומי בני:
בסדר. פרוטוקול לא מאובטח, במערכת ה – FIREWALL, כמו שתיארתי מקודם, ה – FIREWALL זה בעצם מערכת שמפרידה בינינו, לבין הרשת הארגונית לעולם החיצוני, יש חוקים במערכת שהם לא בשימוש, חוקים, זה בעצם הגדרות שהם לא מספיק טובות, שאנחנו מצאנו. לא מצאנו פה הרבה, אבל המעט שמצאנו העלינו את זה.

שי פרידמן:
עברנו על כל ההגדרות,

שלומי בני:
כן,

שי פרידמן:
על החוקים ו - , ויישמנו.

שלומי בני:
הערה רק, יש, יש נושאים, יש ממצאים שמטפלים בהם בקליק? שני קליקים? שלושה קליקים, בסדר 10 דקות עבודה, ויש ממצאים שעולים כסף.

שי פרידמן:
זה להחליף מערכת.

שלומי בני:
להחליף מערכת, הצפנת מסד נתונים, זה אירוע, בסדר? זה כדי שנבין שאנחנו. גם פה, במערכת ה - , ברשת, במערכת האקטיב – דירקטורי, שזה בעצם מערכת שמנהלת את כל המשתמשים של החברה, בעצם מצאנו מספר, מספר הקשחות שלא בוצעו, גם פה יחסית לא הרבה, מצאנו בצורה יחסית מעטה, נניח שגם זה,

שי פרידמן:

זה טופל,

שלומי בני:
טופל,

שי פרידמן:
זה טופל,

שלומי בני:
כי גם זה משהו שהוא,

יובל אגמון:
יש גם פרוטוקול של פעם ב - ,

שי פרידמן:
כן,

יובל אגמון:
מספר חודשים, נעשה אוטומטית, צמצמנו את הלוחות זמנים ו - ,

שי פרידמן:
כן.

שלומי בני:
אוקי, גם פה איזה שהוא פרוטוקול SMB, בתחנות הקצה,

שי פרידמן:
גם,

שלומי בני:
גם פה הקשחה של, של התחנות קצה, שהוא, שחשוב, כי תחנות קצה זה אחד מהנקודות, תחנות קצה, זה בעצם המחשבים שעליהם עובדים העובדים, בסדר? זה נקרא תחנת קצה. אז זה בדרך כלל מקום מיועד לפורענות, כי משם אנחנו גולשים מהר מאוד לשרתים. עשינו גם פה מבדק פנימי, ומבדק חיצוני לשרת של הארגון, אז במבדק החיצוני, מצאנו שתי הגדרות שלא הוקשחו, ואני מניח שגם בזה,

שי פרידמן:
הוקשחו זה גם מהיר.

שלומי בני:
כי גם זה מהיר. מערכת הדואל, בעצם יש שתי דברים שעלו פה במערכת הדואל, אחד, אנחנו לא אוהבים שיש לנו כתובות מיילים של, גורמי הנהלה באתר אינטרנט, או בכל מיני מקומות של החברה, למה? כי אם ה - , הכתובת עם השם של הבן אדם נמצאת באתר אינטרנט של מוריה, נגיד סמנכ״לית הכספים, או סמנכ״ל הכספים, אז מי שרוצה לתקוף, יודע בעצם להתחקות אחר המייל שלו, ויודע לשלוח כאילו זה מהמייל שלו, למייל שלו, או הפוך, לשלוח אליו, ויגיד לו - חיים, שים לב, אני מנהלת החשבונות, כך וכך, צריך להעביר כך וכך כסף, בסדר? זאת אומרת ברגע שיש לי את השם של הבן אדם, שם פרטי, שם משפחה, ואת הכתובת שלו, זה כבר נתונים שהם יותר קלים לעשות פישינג, בסדר? להתחקות.

אלדד רבינוביץ:
רגע, אני אייצג הציבור, דווקא לציבור זה מאוד טוב ונוח, שהוא יודע להגיע לפונקציונרים הרלוונטיים בחברה, יש איזה שהוא מתח מסוים.

שלומי בני:
נכון, אז יש לי, יש לי פתרון לזה, אז אנחנו נשים כתובת מייל, שהיא לא של הבן אדם, למשל אם זה סמנכ״ל הכספים, בוא נשים לו פיננס שטרודל מוריה CO.IL, ואז הוא יודע שהוא קיבל את זה מהמחלקה, כן, של המחלקה,

יובל אגמון:
זה יכול להגיע ישירות אליו,

שלומי בני:
כן, אבל הציבור לא יראה את זה,

שי פרידמן:
בדיוק.

שלומי בני:
כן, ואז זה יפתור, זה יפתור את הבעיה. כי גם אני באתר האינטרנט של המשרד, רוצה שיהיה לנו את הכתובת, כמו שאתה אומר שיפנו אלי, אז אנחנו עושים את זה בשיטה הזאת. הדבר השני, זה במערכת של הדואל, אנחנו היינו ממליצים, נקרא לזה, לא תמיד, אבל ממליצים שיהיה איזה שהוא תוסף של מניעה של דלף מידע, אוקי. למשל אם מישהו שולח, רשימה אנפה של, של תושבים, אני

מוציא את זה מהמייל, אני רוצה שהמערכת תגיד - רגע, רגע, יש פה תעודות זהות, אנחנו רוצים שמישהו נוסף יסתכל, אנחנו עוצרים אותך, בסדר? אז זה נקרא DLP,

שי פרידמן:
אז הנושא הזה של כל הקונטקט, אנחנו שינינו את הכתובת, כבר אין שמות פרטניים, זה לפי מחלקה. דלף מידע זה תהליך, ואנחנו כבר באמצע, אנחנו, גם נסיים איתו ב - , בחודשים, שבועות, חודשים הקרובים.

יובל אגמון:
אני אומר, זה למשל תהליך, שמצריך להגדיר, זאת אומרת מתי המערכת תתריע, זאת אומרת שעל כל דבר, כל הכובד שיש עכשיו מהנדס שמעביר תוכניות, ששוקלות הרבה, אני לא רוצה שהיא תתריע, זה גם משקל, זה גם תכנים. אז אנחנו בעיצומה של הגדרות, של המערכת,

שי פרידמן:
כי בסוף לא על כל מייל רוצים שיתריע, כי אז יעשו את הכול approve, approve, ויאשרו את זה, אז זה צריך להיות משהו באמת שהוא אמת,

עפרה ברכה:
שהוא צריך,

שי פרידמן:
בדיוק.

עפרה ברכה:
שלא תהיה איזה דו״ח כזה.

שי פרידמן:
נכון.

שלומי בני:
ביצענו בדיקה, בעצם יש, יש את האתר אינטרנט של מוריה, ובפנים יש כל מיני פורטלים, אז כרגע אני מדבר על האתרים אינטרנט האינפורמטיבי, אוקי, אז גם פה מצאנו כל מיני חוסר בהקשחות, ליקויים, אני מניח שטיפלתם,

שי פרידמן:
כן, זה היה מהיר,

שלומי בני:
כי זה משהו שהוא יחסית מהיר.

שי פרידמן:
קל, נכון.

שלומי בני:
טוב, אז פה כבר נכנסנו לפורטלים, עשינו ממש מבדקי חדירות, לפורטלים, ניסינו לראות את הפורטלים עד כמה הם עמידים בפני תקיפות, אם אפשר לשנות אותם, אם אפשר להפיל אותם, כל מיני שיטות, להשחית אותם. אז יש פורטל של טופס, זה בעצם טופס של נזקי גוף ורכוש, שבעצם אני, אם אני נפצעתי כתוצאה מאיזה פרויקט או משהו, אני מגיש את הטופס הזה,

עפרה ברכה:
טופס מקוון לציבור?

שלומי בני:
כן,

דוברת:
כן,

שלומי בני:
בדיוק, זה טופס מקוון, מקוון לציבור.

יובל אגמון:
בעצם 106, שהוא על,

לימור גמיש:
כן, כן,

יובל אגמון:
כשלים, אז זה ה - , זה הנושא של נזקים, מי שניזוק, יכול לפתוח טופס, ונכנס ישירות למערכות.

שלומי בני:

עכשיו, זה חשוב, למה זה חשוב? כי בעצם זה משהו שהוא אישי שלי, זאת אומרת אם אני נפצעתי וזה, אני לא, לא רוצה שהמידע הזה ידלוף ל - , אז פה מצאנו כמה, כמה ממצאים, שאחד מהם הגדרנו אותו בעל סיכון גבוה. שבעצם בא ואומר בגדול, כן? שקל מאוד להפיל את הפורטל הזה, אם אני רוצה להפיל, אם אני איראני, קל מאוד להפיל אותו.

<u>אלדד רבינוביץ:</u>
להפעיל או לקחת נתונים?

<u>שלומי בני:</u>
להפיל אותו, גם המידע.

<u>יובל אגמון:</u>
אין שם מידע,

<u>שי פרידמן:</u>
הוא לא אוגר מידע,

<u>שלומי בני:</u>
הוא לא אוגר מידע, אבל קל מאוד להפיל אותו, גם להפיל אותו, אנחנו לא רוצים ש - , אתה יודע בסוף יתהדרו, הנה הפלנו אתר, פורטל של עיריית ירושלים, זה מה ש - , זה בסופו של דבר מה שיצטייר, אני מניח שגם בזה טופל, נכון? כי זה מאוד פשוט,

<u>שי פרידמן:</u>
כן, זה אחד.

<u>שלומי בני:</u>
זה הרייטינג, נכון, אז זה טופל.

<u>שי פרידמן:</u>
כן, כן.

<u>שלומי בני:</u>
נמצאו שמה עוד ממצאים, אבל נתנו את זה, כי הוא הסיכון הגבוה. טוב, פה בדקנו את פורטל מתכננים, זה גם פורטל ש - , בעצם מתכננים מעלים את השרטוטים, ואת כל מה ש - ,

<u>יובל אגמון:</u>

זה פורטל של מתכננים, כמו המאגרים של העירייה, מאגרי היועצים של העירייה, שהם נרשמים בעצם,

לימור גמיש:
מאגר,

יובל אגמון:
מאגרי החברה, שניתן לבחור אותם.

שלומי בני:
עכשיו לשאלה הקודמת שלך, אז פה, כשיש לך הרבה מאוד ליקויים, כשיש הרבה מאוד ליקויים, אז מן הסתם קל יותר לגנוב מידע. אני לא יכול להגיד - טוב, מחר בבוקר נבוא ב – 3 דקות אני מוציא מידע, אבל אנחנו מדברים על עולם הסיכונים, שיש לך פה שורה ארוכה של דברים, אז הרבה יותר קל לגנוב מידע, כן, אז פה נתנו הרבה מאוד המלצות, וזה כבר יותר משמעותי.

שי פרידמן:
נכון, אז זה לא בכמה דקות. את רוב הליקויים פה טיפלנו, כי שמנו את הכול תחת מאחורי Cloudflare, ונשארו שני ליקויים שאנחנו צריכים יותר את התמיכה ואנחנו כבר מחליפים את המערכת הזאתי, לאותו מערכת SAAS,

שלומי בני:
את הפורטל,

שי פרידמן:
את הפורטל בדיוק,

יובל אגמון:
מכניסים אותו לתוך הפריוריטי,

שי פרידמן:
לתוך הפריוריטי שהיא גם, זה גם רצינו לעשות, אבל פשוט הממצאים הקדימו לנו את זה. אז כל הנושא של העדכון גרסאות אנחנו עוד לא ביצענו. כל הרשימה מוסתרת מאחורי ה – Cloudflare, והנושא של התיקיות, כי זה JAVA SCRIPT, אז זה, זה מערכות שהם קצת,

שלומי בני:

אז זה, זה יישאר,

<u>שי פרידמן:</u>
זה שני אלה,

<u>יובל אגמון:</u>
זה מעבר, מעבר כבר למערכת החדשה.

<u>שלומי בני:</u>
מתי אתם מתכוונים רק לעבור?

<u>שי פרידמן:</u>
אותו רעיון, פחות או יותר להגיע לאותו סוף שנה,

<u>יובל אגמון:</u>
סוף שנה,

<u>שי פרידמן:</u>
תחילת שנה, כן, נסיים את האירוע הזה. אוקי, אז רוב הזה, מתוך הרשימה הזאתי נשארו שני משימות שלא ניתן לסגור אותם ב – Cloudflare.

<u>שלומי בני:</u>
אוקי, בסדר, אני יכול להמשיך?

<u>עפרה ברכה:</u>
כן, בטח.

<u>שלומי בני:</u>
טוב, הסיכון, בגדול, אז אם אני אסכם את ה - , את הדברים בגדול בנושא של, של אבטחת מידע סייבר, שוב אנחנו לא נגענו בתקנות הגנת הפרטיות, אבל ברמה הטכנולוגית, החברה במצב טוב, יחסית, ולכן אנחנו העמקנו יותר במבחני, במבחני החדירה של הפורטלים, ובאמת ראינו, שמה מצאנו דברים שהם קצת, קצת יש להם בשר, ובאמת יכולנו לתת ערך, ולא הסטנו את המשאבים שלנו למיין – סטרים. זהו, זה מהצד שלי.

<u>אלדד רבינוביץ:</u>
רגע, יש לכם עוד מקום שאתם רוצים להגיד?

יובל אגמון:
אני חושב בעיקר ש - , אנחנו, באמת מודים על הביקורת, כי זה בעצם הנושא הזה, כמו שאמרת אנחנו בדקנו ומצאנו, אני חושב שבתחום אבטחת מידע, עברנו מספר ביקורות, גם פנים, גם משרד התחבורה בעצם, אי-אפשר כמעט שלא למצוא כשאתה מחפש בתחום הזה, וזה תמיד טוב לבוא ולמצוא, אנחנו חושבים איפה להשתפר, באמת עשינו פוקוס מאוד גדול, בשנתיים שלוש האחרונות על התחום הזה. כמו שאתם רואים תיקנו את מה שאפשר, ו - , זהו, זה באמת,

עומר סטיביסקי:
ובאמת,

שלומי בני:
ובסוף שנה אתם מסיימים,

יובל אגמון:
גם עכשיו בשעת המלחמה עם איראן, וגם, בתחום הזה הקשחות איפה שצריך,

שי פרידמן:
סגרנו את הגישה מהעולם,

יובל אגמון:
סגרנו גישה מהעולם, זאת אומרת יש ממש פוקוס על התחום הזה, ו - , בסוף מוריה, יש לה מידע, בעיקר מידע עסקי, פחות מידע של תושבים, גם מוריה מנותבת ע״י משרד התחבורה, אבל אנחנו לא מפעילים מערכות של רמזורים, סליחה, או מנהרות או משהו כזה, זאת אומרת אין, גם אם מישהו נכנס לתוך מוריה, הוא לא יכול להשבית פה, להשבית פה צומת או משהו כזה. אנחנו מביאים הכול, אנחנו בעצם מנותבים ברמת, רמה הכי גבוהה, גם משרד התחבורה, ו - ,

שי פרידמן:
אנחנו יושבים עם שני מערכי SOC, שכל פעולה שאנחנו עושים, היא ברמה מאוד מאוד גבוה, עם דומיין אדמינו, באינטרה או בגלובל,

שלומי בני:
אתה מדבר בסינית כן, אוקי.

שי פרידמן:
בקיצור, כל פעולה שאנחנו עושים שהיא קריטית,

שלומי בני:
זו בקרה, חדר בקרה, בקרה עם מסכים,

שי פרידמן:
כל אירוע שקורה, אנחנו מקבלים לפי התראות, מי מקבל,

יובל אגמון:
קבוצת וואטסאפ שאנחנו מקבלים,

שי פרידמן:
קבוצות וואטסאפ שכל אחד איזה שהוא אירוע מסוים,

שלומי בני:
כן,

שי פרידמן:
שהוא אירוע קריטי, כן? מקבל אפטד און – ליין, אז עם מערכות, מערכי SOC האלה,

שלומי בני:
אחד של משרד התחבורה,

שי פרידמן:
ועוד אחד שלנו חיצוני, אחד אקסטר, אחד משרד התחבורה. זה בגדול.

עפרה ברכה:
אז שוב אני חושבת שבחרנו טוב מבחינת הנושא, מוריה באמת אמנם לא זו שמתפעלת את הרמזורים וכולה, אבל בכל אופן אני חושבת שזה התאגיד הכי גדול בארץ,

שלומי בני:
הכי גדול, התאגיד עירוני,

עפרה ברכה:
כן, תאגיד עירוני,

שלומי בני:

כן,

עפרה ברכה:
אני מתהדרת בזה,

שלומי בני:
כן, בוודאי.

עפרה ברכה:
ירושלים. היקפים מאוד מאוד גדולים, ועשייה מאוד מאוד גדולה, ואני חושבת שזה טוב, הדו״ח הזה שעשינו אותו, זה טוב שלקחתם אותו ברצינות, טיפלתם ו - , אנחנו תמיד בסוף ברמה הפרקטית, באנו ראינו שהנושא של הגנת הפרטיות הוא בסך הכול תקין וסביר, אז החלטנו להפנות באמת את המשאבים ל - , לחלק השני שלה ביקורת. אני חושבת שטוב שעשינו כך. ומה שנותר לתקן, אני אשמח שזה ייעשה.

שי פרידמן:
אנחנו על זה,

עפרה ברכה:
בהצלחה רבה.

יובל אגמון:
תודה רבה.

אלדד רבינוביץ:
אני רגע אסכם, אז דבר ראשון, שוב להודות למבקרת, וגם לך על ה - , על הדו״ח החשוב, אני שמח שבאנו ובזבזנו את הזמן שלנו על דו״ח שבאמת האמצעים בו הם לא משמעותיים, ומה שהיה כבר תוקן. זה חלק משמעותי בעיני מעבודת הביקורת, לעשות, כשעושים ביקורת רוחב. ובאמת לא באים מוכוונים מראש, אלא באמת בודקים, אז לפעמים מוצאים, לפעמים לא מוצאים, ותודה לכם על העבודה המקצועית וכל הכבוד על הרמה גבוהה. אני רק אקריא את מה שאני צריך להקריא,

עומר סטיביסקי:
הסטנדרט, חשוב לציין הסטנדרט לא רק בנושא הזה,

אלדד רבינוביץ:
כן,

עומר סטיביסקי:
וועדות ישום וכל דו״ח של המבקרת, וגם המבקר הפנימי,

אלדד רבינוביץ:
חברה שעובדת טוב, מצליחה. מקבלת את המלצות הדו״ח בכפוף להערות, והוספות לעיל, ממליץ למועצה לאמץ את מסקנות הוועדה. הישיבה נעולה.

יובל אגמון:
תודה רבה.

עפרה ברכה:
כל טוב.

סיום הדיון