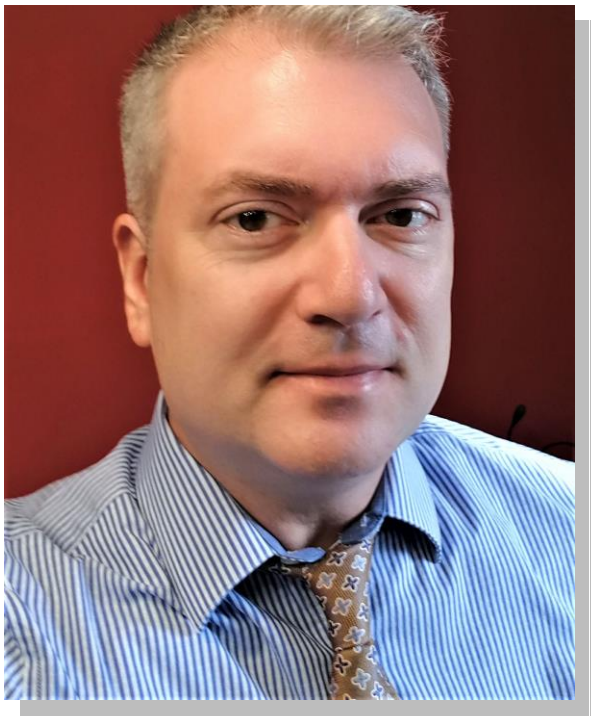

# איך לצמצם כשלי אבטחת מידע וסייבר בארגון

*רמי איצלב, MBA, CISA*

*שותף מנהל, ERA*

*פורסם: 15.05.2022*

אבטחת המידע בכלל ותחום הסייבר בפרט מהווים, ללא ספק, מוקדי סיכון מהותיים הן בקרב חברות מסחריות והן בקרב גופים ממשלתיים שונים (כגון: עיריות, משרדי ממשלה, מועצות מקומיות, חברות ממשלתיות).

לאחר שחברות ותחומי פעילות שלמים ניזוקו קשות, עד לקריסה טוטאלית, בארץ ובעולם בגלל תקיפות האקרים (לדוגמה: חברת ביטוח **שירביט** בישראל [1] בחודש דצמבר 2020), נראה כי נקלט המסר אצל בעלי העניין והופנו לתחום אבטחת מידע השקעות רציפות ומשמעותיות.

עם זאת, לא בכל ארגון הופנם כי השקעה לבדה אינה מבטיחה שמערך אבטחת מידע וסייבר יהיה אפקטיבי. למזער את הסיכונים, חייבים לבקר את אבטחת המידע וסייבר, על-ידי בקרה וביקורת אבטחת מידע, בתדירות גבוהה ובצורה אפקטיבית.
אחרת כל ההשקעה עלולה לרדת לטמיון!

מטרת המאמר היא לתת כיוון, "על רגל אחת" לפעולה מקצועית, לצורך הסדרת נושא בדיקות אבטחת מידע בארגונים. התחום נרחב ביותר ודורש התעמקות רבה. כמובן שאין תחליף לייעוץ מלא והכוונה מקצועית בנושא.

## פעילויות הבקרה

בקרה אפקטיבית על אבטחת מידע וסייבר ניתן להשיג על-ידי הצעדים הבאים:

1. **מינוי גורם פנים ארגוני לתפקיד בקר אבטחת מידע / מנהל אבטחת מידע.**
   גורם זה אמור להיות מומחה טכנולוגי עם ידע ארגוני מספק, על-מנת להבין תהליכים ולקיים בקרות שוטפות.
   נציין כי למנהל אבטחת מידע יש תחום אחריות רחב יותר מזה של בקר אבטחת מידע, אך במאמר זה לא נרחיב בנושא ספציפי זה.
   להלן מספר דגשים בנוגע לפעילותו:

- ✓ בקר אבטחת מידע צריך לקבל סמכויות מההנהלה הבכירה. ללא סמכויות פורמליות עלולות להיווצר בעיות בקבלת נתונים, מענה מהעובדים השונים, היעדר דיווחים ועיכובים.
- ✓ על הבקר לגבש ולאשר בהנהלה תכנית עבודה מסודרת, עם יעדים ברורים ותקצוב לפעילות.
- ✓ הבקר יעסוק במגוון נושאים, כולל בין היתר: בחינת הרשאות גישה למערכות, ביצוע סריקות ברשת לגילוי חשיפות אבטחה, העברת הדרכות לעובדים, בחינת מודעות לסייבר ואבטחת מידע, הערכת סיכונים והעברת תרגילי הנדסה חברתית [2].
- ✓ בחינת סביבה רגולטורית ופעולה אקטיבית לצורך וידוא עמידה של הארגון בחוקים ותקנות בנושא אבטחת מידע, סייבר ופרטיות שחלים על החברה.
- ✓ באופן טבעי, בקר / מנהל אבטחת מידע ייעזר בעבודתו ביועצים חיצוניים בהתאם לתחום מומחיותם (כגון: בדיקות חדירה, סקרי סיכונים, תרגילי הנדסה חברתית ועוד).

***2.* הסדרת דיווחים ועדכונים בנושא אבטחת מידע וסייבר כחלק מעבודת הוועדות השונות של הנהלת הארגון, עד לרמת הדירקטוריון.**

<u>להלן מספר דגשים בנוגע לזה:</u>

- ✓ הדיווחים צריכים להיות מוצגים ועל הדיונים להתקיים בתדירות רבעונית לפחות.
- ✓ יש לבצע מעקב אחר יישום החלטות הוועדות.
- ✓ בקר / מנהל אבטחת מידע ייקח חלק פעיל בדיווחים ודיונים בפורומים אלה (אך הוא לא הגורם היחיד שיהיה מעורב – תידרש בין היתר מעורבות של מנהל מערכות מידע, מנהל תפעול, קצין ביטחון ועוד).
- ✓ במקרים חריגים (כגון: אירועי תקיפה על-ידי האקרים, זליגת נתונים רגישים מחוץ לחברה ועוד) יש לכנס דיונים מיוחדים, מעבר לישיבות תקופתיות. לעיתים יידרש דיווח לרשויות החוק / משרד המשפטים ועוד.

***3.* אימוץ תקני אבטחת מידע מקובלים.**

קיימים בעולם מספר תקנים בנושא אבטחת מידע, שהם וולונטריים, לצד רגולציות מחייבות. אחד התקנים המקובלים ביותר הוא ISO 27001 – תקן לניהול אבטחת מידע בארגונים [3].

ארגון שלוקח על עצמי לעמוד בתקן מגבש סדרה של בקרות ומטמיע שיפורים שונים במערך אבטחת המידע שלו. עמידה בתקן מחייבת ביקורת חיצונית תקופתית על-ידי גוף בינלאומי מסמיך.

בפועל, תהליך ההכנה להסמכה הוא זה שנותן את ה- impact המשמעותי, כולל שינוי תהליכי עבודה, הטמעת כלים טכנולוגיים מתקדמים, גיבוש נהלים ועוד.

## פעילויות הביקורת

**ג**ם במקרה שהארגון מיישם בקרה בדומה למתואר לעיל, קיים סיכון בלתי מבוטל להיכשל אם לא מפעילים ביקורת פנימית ויעוץ חיצוני בלתי תלויים בתחום אבטחת המידע והסייבר.

חשוב לזכור שבקרה וביקורת הם שני חלקים של המנגנון השלם והם לא יכולים לבוא אחד על חשבון השני!

הביקורת מבוצעת על-ידי יועצים מקצועיים ומוסמכים, בעלי ניסיון רב שנים באבטחת מידע וסייבר.

להלן רשימת תחומים עיקריים שנבדקים המתאימה לרוב הארגונים:

- ✓ מדיניות אבטחת מידע ונוהלי עבודה

- ✓ ניהול אבטחת מידע בארגון
- ✓ אבטחת מידע בתחום משאבי אנוש
- ✓ אבטחה פיזית וסביבתית (הגנה מפני אסונות, אבטחת גישה לאזורים רגישים)
- ✓ אבטחת מידע בתהליכי רכש, פיתוח ותחזוקה של מערכות מידע
- ✓ אבטחה לוגית (שימוש באמצעי אבטחה ייעודיים כגון חומת אש, אנטיוירוס, DLP)
- ✓ בדיקות חדירה (מרשת האינטרנט, בתוך הרשת הפנימית, תשתיתיות ואפליקטיביות)
- ✓ הערכת סיכוני אבטחת מידע וסייבר
- ✓ בדיקת ערנות עובדים והנדסה חברתית
- ✓ בקרות גישה ומידור מידע
- ✓ טיפול באירועי אבטחת מידע חריגים
- ✓ ניהול משתמשים והרשאות במערכות המחשב
- ✓ גיבוי ושחזור נתונים
- ✓ תוכנית המשכיות עסקית
- ✓ עמידה בדרישות רגולציה (כגון: תקנות הגנת הפרטיות, הוראות ניהול בנקאי תקין, הוראות המפקח על שוק ההון וביטוח, חוק GDPR של האיחוד האירופי ועוד)
- ✓ אבטחת מידע שאינו ממוכן
- ✓ הפצה והשמדה של מסמכים רגישים

## לסיכום

רוב איומי אבטחת מידע המתממשים בארגונים יכולים להימנע אם מפעילים מערך בקרה וביקורת יעילים.

על אף ההשקעה הנדרשת (משאב אנושי וכספי), בטווח הארוך היא תשתלם ובמקרים מסוימים אף תציל את הארגון מפגיעה קשה או קריסה מוחלטת.

## הערות

**שירביט חברה לביטוח** [1] – היסטוריה של החברה כולל אירוע הסייבר המדובר

https://he.wikipedia.org/wiki/%D7%A9%D7%99%D7%A8%D7%91%D7%99%D7%98_%D7%97%D7%91%D7%A8%D7%94_%D7%9C%D7%91%D7%99%D7%98%D7%95%D7%97

**הנדסה חברתית (אבטחת מידע)** [2] – הגדרה מלאה

https://he.wikipedia.org/wiki/%D7%94%D7%A0%D7%93%D7%A1%D7%94_%D7%97%D7%91%D7%A8%D7%AA%D7%99%D7%AA_(%D7%90%D7%91%D7%98%D7%97%D7%AA_%D7%9E%D7%99%D7%93%D7%A2)

**ISO 27001 – תקן לניהול אבטחת מידע בארגונים** [3] תקן אבטחת מידע המקובל בעולם, פורסם על-ידי ISO www.iso.org ו- IEC www.iec.ch. https://en.wikipedia.org/wiki/ISO/IEC_27001