PEARL COHEN

היערכות משפטית לאירוע אבטחה

קבוצת האינטרנט, הסייבר וזכויות היוצרים

ינואר 2022

כיצד להיערך משפטית לאירוע אבטחה

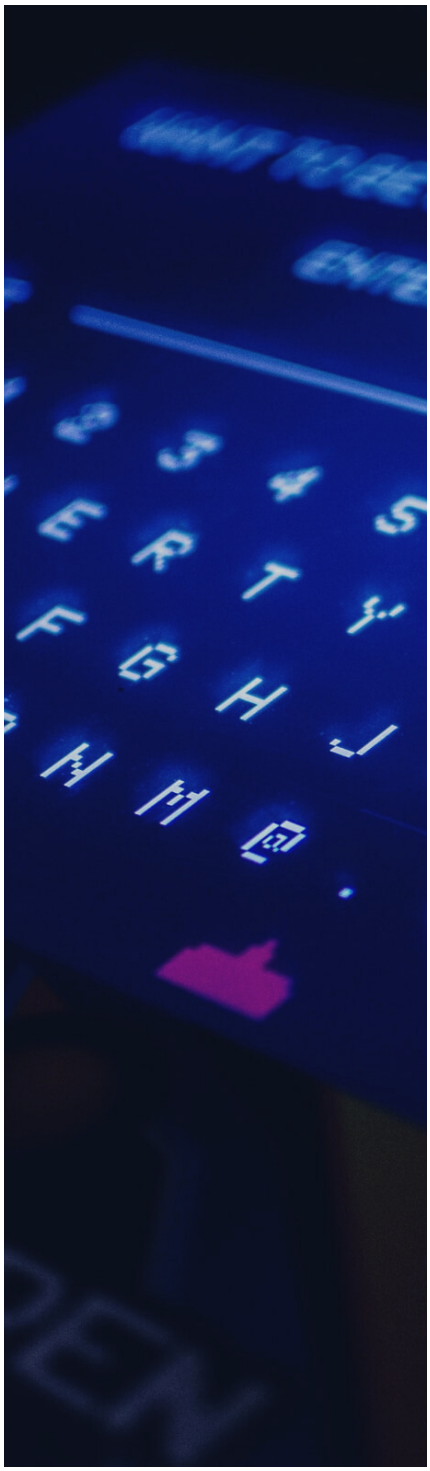
התקפות הסייבר נגד חברות וארגונים בישראל וברחבי עולם גוברות. ההתקפות מגוונות – גניבת קבצים רגישים (מידע אישי, סודות טכניים ומסחריים) ונעילתם בכופרה (RANSOMWARE), שיבוש פעילות שרתים (DDOS), ניצול פרצות אבטחה בתוכנה כדי להגיע ליעדים אחרים (כפי שנעשה בהתקפה על חברת עמיטל בישראל או על SOLAR WIND בארצות-הברית) ועד לחדירה שקטה לצרכי איסוף מודיעיני. במקביל, הסביבה הרגולטורית מקשיחה את דרישותיה, לקוחות וספקים מציבים דרישות, התקשורת תאבה לדווח על תקיפות ועלויות הביטוח מתייקרות בזמן שתנאיו הולכים וקשים.

היערכות מלאה לאירוע אבטחה דורשת **תהליך ארגוני עמוק.** היא נוגעת בהבנת הסיכון הנשקף לארגון; בקביעת סדרי עדיפויות ומיפוי פערים; ברכש טכנולוגי של אמצעי אבטחה; קביעת נהלים ותהליכים ארגוניים; בחירת ספקים – מי יבצע חקירה של נתיב החדירה לארגון, יוודא אם התוקף עוד מצוי במערכותיו, מי ינהל אתו משא ומתן ומי יעסוק ביחסי-הציבור של האירוע ובקשרי הלקוחות; הדרכת עובדים; תרגול ההנהלה, צוותי ה-IT והארגון; תיעוד וגיבוי מידע – ולא פחות חשוב מכך, היערכות משפטית מוקדמת.

בזמן האירוע, אין זמן לכל אלה. האירוע דורש תפעול ותשומת לב מלאה, לצד הניסיון להמשיך במידת האפשר בעבודה השוטפת של הארגון. יש להכין מבעוד מועד את כל הדרוש כדי שאפשר יהיה להתמקד בו. ויש להבין אל נכון כי **לתהליך ההכנה אין סוף**. הוא מחייב עדכון מתמיד בהתאם להתפתחויות הטכנולוגיות, העסקיות והמשפטיות. מה שהיה נכון בתחילת 2021 אינו מספק עוד לסופה.

איך להתכונן משפטית לאירוע אבטחה?

זוהי רשימה לא ממצה. לארגונים שונים צרכים שונים. אבל זו נקודת התחלה טובה לגיבוש הדרוש לארגון שלך.



זהה את הסיכונים האפשריים, לדוגמה –

- דלף מידע אקראי (משלוח קובץ עם מידע רגיש לגורם – בתוך הארגון או מחוצה לו – שלא אמור לקבל אותו, חשיפתו של מידע כזה באתר האינטרנט הארגוני ועוד...);
- גניבה מכוונת של מידע רגיש (הצעתו למכירה ב-DARK NET או איסופו על ידי ארגון מודיעיני עוין);
- נעילת קבצי המחשב בכופרה אגב דרישת תשלום במטבע קריפטוגרפי;
- למד והפק לקחים מאירועי עבר בחברות דומות בעולם או בישראל, בהסתמך על מידע גלוי ברשת

חנך בקביעות את הארגון ל"עיצוב לפרטיות", מזעור מידע אישי ומחיקת מידע לא נחוץ.

דאג שספקי הארגון יתקשרו עמכם בהסכם המחייב אותם ליישם אמצעי אבטחה כדי להגן על נתיב החדירה באמצעותם ומוודא שבעת אירוע אבטחה אצלם, הם ידווחו מידית אליכם. קבע איתם נהלי שיתוף פעולה.

החלט אם להמליץ להנהלה לרכוש פוליסה לביטוח סיכוני סייבר. עלויות אירוע אבטחה הן אסטרונומיות. חברות IR (INCIDENT RESPONSE), מומחי משא ומתן וספקים נוספים דורשים שכר טרחה בסכומים גבוהים. עלויות שיקום הרשת, שיחזור המידע ורכש טכנולוגי הן עצומות, ולביטוח יש ערך גם כי הוא מחייב את הארגון להיערך מבעוד מועד לאירוע.

מפה את הסביבה הרגולטורית ודרישותיה

- באילו טריטוריות פועל הארגון – האם רק בישראל או גם במדינות אחרות;
- בכל טריטוריה רלבנטית, זהה את הרגולטור הנוגע למידע אישי (לדוגמה, הרשות להגנת הפרטיות) והרגולטור הענפי הטעון דיווח (לדוגמה, רשות ני"ע, הבורסה, המפקח על הבנקים או משרד הבריאות);
- דע מראש לאיזה מהגורמים הללו עליך לדווח ובאיזה סוג של אירוע: הכן רשימה של דרכי הדיווח (לדוגמה, טפסים מובנים שקבע הרגולטור), אמצעי הדיווח (לאיזה כתובת דואל או באיזה אתר עליך להזין את הדיווח) – וקבע מי יכין את הדיווח, מי יאשר אותו ומי יבצע אותו בפועל.

קבע נוהל לפיקוח הדירקטוריון על תחום הסייבר וסיכוניו, וודא שהנהלת הארגון מעורבת בהכנתו.

דע והיערך מבעוד מועד לאילו לקוחות עליך לדווח וכיצד –

- האם ובאילו נסיבות עליך להודיע ללקוחות הקצה, ומתי תבחר להודיע הגם שאינך חייב בכך לפי חוק? לדוגמה, בכל מדינה בארצות-הברית יש חובה שונה למסור הודעה כזו. בישראל אין חובה גורפת לידוע לקוחות קצה. עם זה, הרשות להגנת הפרטיות יכולה לחייב בכך את הארגון.
- איזה מהחוזים עם לקוחותיך וספקיך מחייבים אותך לתת הודעה על אירוע אבטחה: בארגון יכול שיהיו גם מאות ואלפי חוזים כעת. הכן רשימה הקובעת כיצד, למי לדווח ובאיזה פרק זמן אתה מחויב לדווח.

הבן את ההגבלות המשפטיות – לדוגמה, האם הארגון רשאי לשלם במטבע קריפטו לתוקף או שהוא מסתכן בעבירות (סיוע לטרור, הלבנת הון ועוד)? האם החוזים שלך עם לקוחותיך מגבילים את חופש הפעולה שלך בטיפול באירוע אבטחת מידע? דאג לעדכון הידע.

הכן נוסחי תבנית של הודעות ללקוחות, לעובדים, לספקים ולתקשורת, המתחשבים בדרישות הרגולטוריות והחוזיות החלות עליך. באירוע תשתמש בהם כבסיס להודעות הממשיות.

וודא שהספקים הדרושים לך מצויים ברשימה המאושרת על-ידי הביטוח – חברת ה-IR, ספק שירותי המו"מ, חברת יחסי הציבור והתקשורת – וחשוב ביותר שגם עורכי הדין המלווים את האירוע. לעורכי הדין המשמשים יועצים משפטיים לארגון ביום-יום יש יתרון מכריע ובלבד שהם בעלי המומחיות והידע הדרושים.

וודא שהיועצים המשפטיים יהיו חלק מצוות ניהול האירוע בארגון ויתורגלו אתו. לכל פעולה יש השלכות שיכולות להימשך שנים ארוכות לאחר תום האירוע בדמות דרישות רגולטוריות או תובענות ייצוגיות ואחרות.

היערכות משפטית נכונה לאירוע אבטחה תאפשר לנהל אותו נכון ולמזער את הסיכונים לארגון.
כתמיד, אנו עומדים לרשותכם לכל צורך בעניין.

חיים רביה, עו"ד
ראש מחלקת האינטרנט,
סייבר וזכויות היוצרים
HRavia@PealCohen.com

דותן המר, עו"ד
מחלקת האינטרנט,
סייבר וזכויות היוצרים
DHammer@PearlCohen.com

האמור במזכר זה אינו מתיימר למצות את כל ההיבטים בנושאים שהוא סוקר. מטרתו היא עדכון כללי בלבד. אין להסתמך על האמור במזכר כעצה משפטית.