נעמי אסיא ושות' משרד עורכי דין,
עורכי פטנטים ונוטריון
Naomi Assia & Co. Law Offices
Patent Attorneys and Notary
רחוב הברזל 32, רמת החייל, תל-אביב 69710
32 Habarzel St., Ramat-Hachayal, Tel-Aviv 69710, Israel
טל: 972-3-6444808 פקס: 972-3-6444818 :Fax
Email: assia@computer-law.co.il • www.computer-law.co.il

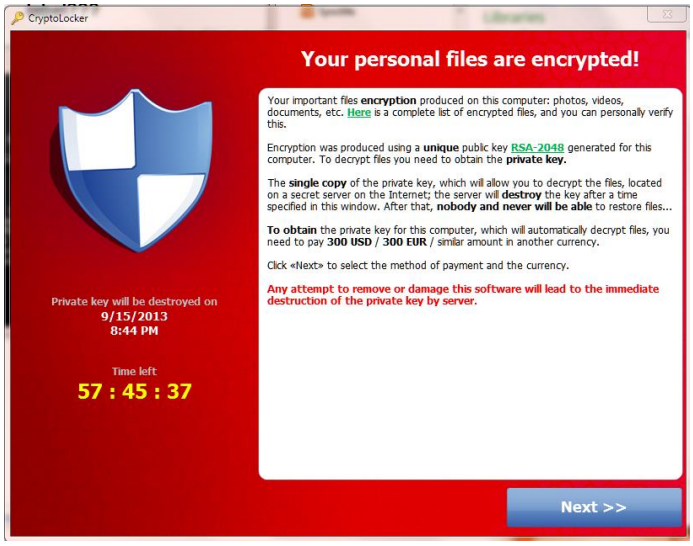
אחריות אישית של נושאי משרה להגנת הארגון מפני מתקפת סייבר

מהי מתקפת סייבר?

מתקפת סייבר הינה חדירה לארגון על ידי תקיפת מערכות המחשב ו/או תשתיות מבוססות מחשב, בדרך כלל, על ידי גורמים חיצוניים לארגון או גורמים המבקשים להזיק לארגון, באופן שמידע רגיש האגור באותן מערכות מחשב, יזלוג החוצה וייעשה בו שימוש העלול להזיק לנושאי המידע, הם האנשים אשר לגביהם מתייחס המידע המופיע במאגר המידע, לחברות המסחריות, לרשויות אשר אגרו את המידע או למדינה בה פועלת החברה.

הקישוריות ההולכת וגוברת בין מערכות המידע בתוך הארגון והתלות המתעצמת בשירותי מחשוב ותקשורת המסופקים על ידי צדדים שלישיים, כדוגמת טכנולוגית מחשוב ענן, יוצרות חולשות במערכות ההגנה של אותן מערכות מחשב, העשויות לחשוף אותן לסיכונים משמעותיים. במקביל, מספר האיומים ועוצמתם גדלו באופן משמעותי, כמו גם זמינות כלי ההתקפה וקלות ביצוע התקיפה.

דוגמא לאחת ממתקפות הסייבר הנפוצות בעולם היא "מתקפת כופר" בה פתיחה של קובץ המצורף לדואר אלקטרוני שנשלח לארגון, גורם להצפנה של הקבצים הנמצאים במחשבי הארגון. בשלב הבא, מוצגת הודעה למשתמש ולפיה הוא יוכל לקבל את המפתח שמאפשר לפתוח את ההצפנה, רק אם ישלם לתוקף סכום כופר מסוים, עד לתאריך מסוים. בדרך כלל, שיטת התשלום המבוקשת על ידי התוקפים היא באמצעות ביטקוין, דבר המקשה לעקוב אחר מקבלי הכופר. את הוירוס עצמו ניתן לרוב להסיר בקלות יחסית, אבל, את הקבצים שנחסמו באמצעות הצפנה, אי אפשר לקרוא יותר.



איור 1 – דוגמא למסך המתקבל בניסיון לפתוח קובץ לאחר "מתקפת כופר"

-

<u>הגברת אחריות נושאי משרה להגנה מפני מתקפת סייבר בארה"ב</u>
שינויים שאירעו לאחרונה במדיניות של מספר גופי רגולציה בארה"ב מתווים את הכיוון של הגברת אחריות נושאי משרה להגנה על ארגונם מפני מתקפות סייבר.
ועדת הסחר הפדרלית (FTC), החלה לפעול לתבוע חברות שלא פעלו באופן נאות להגן על חברתם ממתקפות סייבר. דוגמא לכך היא התביעה במקרה של FTC V. Wyndham. במקרה זה תבעה ועדת הסחר הפדרלי את רשת המלונות המפורסמת לאחר שזו נפרצה במתקפת סייבר בפעם השלישית ברציפות, תוך חשיפת פרטי לקוחותיה, ולאחר שלא נקטה פעולות מתאימות לאחר שתי הפריצות הקודמות.
הוועדה לניירות ערך ולבורסות (SEC) פרסמה אף היא לאחרונה רשימת הנחיות להגנה מפני סייבר עבור חברות העוסקות בתחום ההשקעות. מומחי הועדה יבדקו את החברות האלה בעזרת Auditors חיצוניים שיפעלו מטעמם. הוועדה לניירות ערך ולבורסות אף תבעו חברות בתחום ההשקעות בארה"ב על אי-עמידה ברמת הגנת סייבר על חברתם.
בתחום אחר, **משרד ההגנה האמריקאי** (DoD) פרסם לאחרונה מדיניות חדשה בנושא הקובעת כי כל ספק או ספק משנה של משרד ההגנה האמריקאי מחויב לדווח על כל אירוע סייבר המתרחש אצלו ומחויב לאפשר למומחי המחשוב של משרד ההגנה האמריקאי גישה לרשת בה אירע האירוע.
בשורה התחתונה: בארה"ב גוברת המגמה להטיל אחריות מוגברת על המנהלים למוכנות נאותה של חברותיהם בפני מתקפות סייבר.

<u>המצב בישראל</u>
חוק החברות מטיל אחריות אישית על מנהלים בחברה במידה ולא נקטו בצעדים בכדי למנוע נזק, אשר ניתן היה לצפות שיקרה. כך למשל בהקשר של פרטיות, כאשר מנהל בחברה ידע, כי מאגרי המידע של החברה, המכילים מידע על לקוחות החברה חשופים לגורמים עוינים, אך לא ננקטו על ידי אותו מנהל כל הפעולות הסבירות שעשויות היו למנוע את חשיפת המידע ואת הפגיעה בנושאי המידע, עלול אותו מנהל לשאת באחריות אישית על כך, חרף היותו רק "עובד" של החברה.
בישראל הנושא טרם נבחן בבתי המשפט ולכן מומלץ למנהלים לנקוט ב"חבילת צעדים" מקדימים על מנת לעמוד בחובות הזהירות והאמונים בהם הם חבים כלפי חברה.
פעולות ארגוניות מומלצות שכאלה הם בראש ובראשונה קביעת מדיניות ברורה של הארגון בנושא הגנת הסייבר. הקצאת משאבים ארגוניים ליישום המדיניות. מעקב על יישום המדיניות בארגון, לרבות בחינת האפקטיביות של המדיניות אשר נקבעה, ועדכונה בהתאם להתפתחויות. חינוך והדרכה של העובדים בחברה לנושא הסייבר, קבלת דיווחים שוטפים לגבי אירועי סייבר, הן בתוך הארגון והן בארגונים אחרים ומינוי עובד בארגון בעל ידע וניסיון מתאימים לתפקיד העוסק בהגנת הסייבר של הארגון, אשר ינהל תחתיו את יישום מדיניות הארגון בנושא.

<u>ביטוח סייבר</u>
כלי נוסף העומד לרשות מנהלי הארגונים הוא ביטוח סייבר.
חברות הביטוח זיהו את הסיכונים הכרוכים בהחזקה של מידע אישי או מידע יקר ערך אחר, ופיתחו מוצרים הבאים להגן על חברות וארגונים מפני סיכונים אפשריים של גניבת המידע וזליגתו לידיים בלתי רצויות. גניבת המידע עלולה לפגוע הן בלקוחות הקצה של אותן חברות והן בצדדים שלישיים. משנה לשנה, עולה הממוצע של עלות הנזקים לחברות כתוצאה מדליפה או גניבה של מידע.
הנזקים לחברות יכולים להתבטא במספר פרמטרים: עלויות חקירה ובדיקה של מקור הדליפה, עלויות ההודעה ללקוחות וצדדים שלישיים, עלויות משפטיות, איבוד מוניטין, התרסקות מניות החברה ועוד כהנא וכהנא נזקים ישירים ועקיפים.
מוצרי הביטוח יכללו בדרך כלל כיסוי במקרים של מניעת שירות באמצעות התקפה על שרתי החברה, שימוש לא מורשה במידע, שינוי המידע, הפצת המידע וחשיפתו על ידי גורמים עוינים, אובדן של

-

נכסים דיגיטאליים, הטמעה של תוכנה זדונית הפוגעת במידע או המייצאת אותו מחוץ לארגון, סחיטה או מעשה טרור הקשור למידע שנגנב/הודלף, נזק לא ממוני ללקוחות הקצה (הוצאת דיבה), הוצאות עלות ההודעה ללקוחות וצדדים שלישיים, עלויות משפטיות ועלויות יועצים לניהול המשבר.

בברכת שנה אזרחית שמחה,