



חשד למתקפת סייבר על שירביט

רשות שוק ההון ומערך הסייבר הלאומי הודיעו כי דלף מידע על פרטי ביטוח של לקוחות | קבוצת האקרים שלקחה אחריות על האירוע פרסמה תעודות זהות ורישיונות של לקוחות

תגיות: חברות ביטוח, שירביט, רשות שוק ההון ביטוח וחסכון, עינת מירון, מערך הסייבר הלאומי

חברות קשורות

שירביט חברה לביטוח בע"מ



מאת: מערכת עדיף

09:32 01/12/2020

רשות שוק ההון, ביטוח וחסכון ומערך הסייבר הלאומי עדכנו על אירוע דלף מידע מחברת הביטוח **שירביט**. אמש (ב') החלו החברה בסיוע המערך לבדוק חשד לאירוע סייבר על אתר ושרתי החברה שבוצע על ידי האקרים.

בהודעה משותפת של הרשות והמערך נמסר כי "מבדיקה ראשונית עולה כי מדובר במידע על פרטי ביטוח של לקוחות. במאמץ משותף לרשות ולמערך, הבדיקה ממשיכה. בעקבות כך שב וחייד המערך יחד עם הרשות את ההנחיות לגופים המוסדיים במשק".

בשלב זה אתר האינטרנט של שירביט מושבת.

קבוצת האקרים שקיבלה אחריות למתקפה לא הסתפקה בכך וגם פרסמה תעודות זהות ורישיונות של לקוחות. כן פורסמה הקלטה של שיחה בין לקוחה לחברה.

נורה אדומה לרגולטור

לדברי עו"ד **גיא שמואלי**, שותף במשרד עורכי הדין שמואלי שמשון RGS העוסק בהגנת הפרטיות, סייבר ודיני ביטוח, הדיווח של רשות שוק ההון, ביטוח וחסכון ומערך הסייבר הלאומי על חשש מדליפת מידע משרתי חברת ביטוח חייב להדליק נורה אדומה ברשות שוק ההון ובמערך הסייבר הלאומי.

"חברות הביטוח כפופות לחוזר ניהול סיכוני סייבר בגופים מוסדיים אשר מפרט בהרחבה את דרישות אבטחת המידע המחמירות הנדרשות מגופים מוסדיים. החברות מונחות לפעול בצורה אקטיבית בתחום אבטחת המידע ונערכות בהן בחינות תקופתיות מחמירות, על מנת לבחון את מערכות המידע ולוודא את העמידה בהוראות. גורמי הביטוח חייבים לבצע בדיקות מקיפות על מנת לבחון כיצד הצליחו האקרים לעקוף את מנגנוני האבטחה המחמירים והאם מדובר בפרצה שעלולה לסכן גופים מוסדיים אחרים", אומר עו"ד שמואלי.

במקביל, מסביר עו"ד שמואלי, כי מידע אישי ורגיש של מיליוני ישראלים נמצא במאגרי מידע של גורמים שכלל אינם כפופים להוראות החוזר. "זו סוגיה מטרידה מאוד בעיני. גופים רבים, שאינם גופים מוסדיים, מחזיקים מידע רגיש מאוד בתחומים שונים במערכות המידע שלהם. מדובר על מידע אישי, מידע רפואי, מידע ביומטרי, מידע כלכלי ועוד. על גופים אלה הוראות חוזרי הרגולציה לעניין סיכוני סייבר כלל לא חלות. הגופים מחויבים לעמוד בתקנות הגנת הפרטיות (אבטחת מידע) והנחיות רשות הגנת הפרטיות להגנה על מידע ושמירה על פרטיות הלקוחות. התקנות האלה חלות על כל המשק הישראלי ומטרתן להגן על האנשים שמידע אודותיהם קיים במאגר המידע. גופים רבים אינם מקיימים את הוראות התקנות, וכלל אינם מודעים לחובה שלהם לעמוד בהן או לעצם קיומן. התוצאה היא כי מידע של מיליוני ישראלים עלול להיות חשוף וגלוי להאקרים".

ביצוע תהליכים ארגוניים המותאמים לסיכון העסקי

עינת מירון, מומחית Cyber Resilience להערכות והתמודדות עם אירועי סייבר בהיבטים העסקיים התייחסה לאירוע וציינה: "הדיווחים על מתקפת הסייבר בחברת שירביט גובו עם לקיחת אחריות של קבוצת BlackShadow ועם מסמכים המעידים על גודל האירוע ועומק החדירה. כידוע, שירביט זכתה שנים רבות במכר ביטוחי הרכב של עובדי המדינה ולכן עצם האירוע מטריד רבים.

"רק בהיבט המסמכים שדלפו - מידע שכזה אמור להיות מנוהל, לכל הפחות, כמאגר מידע בסיווג רגיש, גבוה, בהתאם לתקנות הגנת הפרטיות. העובדה שהגיעו אל מידע נרחב כל כך מעידה על רצף של כשלים, העדר בקורות וניהול לקוי. בנוסף, אם נכון הדיווח על מחיקת השרתים עצמם והעדר גיבויים, הרי ששירביט נמצאת כרגע בבעיה כפולה ומכופלת.

"אקסיומה ידועה היא שכל ארגון ייפרץ במוקדם או במאוחר. אין באמת דרך למנוע זאת. אבל, חשוב להבהיר ולהדגיש, כי ניתן בהחלט לצמצם את החשיפה לסיכוני הסייבר, אם מבצעים תהליכים ארגוניים

המותאמים לסיכון העסקי. אנחנו רגילים לסמוך כמעט בצורה עיוורת על מערכות טכנולוגיות במעגלים האבטחה אבל השנה היא כמעט 2021. להמשיך לעשות את אותו הדבר ולצפות לתוצאות אחרות, לא באמת מוכיח את עצמו.

"בתפיסת Cyber Resilience שפיתחתי אנחנו משתלבים בשגרת העבודה הקיימת ומייצרים מעורבות ישירה וברורה של מנכ"ל החברה בהתייחסות לנושאים אלה, מקימים ועדת היגוי שמנטרת סיכונים עסקיים ומציבה יעדים ברורים למעקב וטיפול ומשלבים מגוון דיסציפלינות מקצועיות כדי להגדיר, אולי לשנות ובטח לטייב, תהליכים פנים ארגוניים ייעודיים.

"בנוסף, חשוב לציין דבר נוסף ולא פחות מהותי: הרגולטור הגדיר רשימת משימות והחלטות שאמורות להיות מיושמות בכל ארגון מפוקח במטרה למנוע התמודדות עם אירוע סייבר. העובדה שלמרות קיומן של הנחיות אלה, אנחנו נחשפים לעוד ועוד אירועים שבהכרח היה ניתן למנוע באמצעות בקורות יעילות יותר, היא נורה אדומה דווקא לרגולטור עצמו".

[סגור חלון..](#)