מעריב השבוע - עסקים
עמוד 8 , 29/01/2021 , 24.44 x 33.3
כתבים: טליה לוין
76033513

טליה לוין

רשת ביטחון

שוק ביטוחי הסייבר תופס תאוצה ברחבי העולם, אולם בישראל הוא עדיין מדשדש מאחור ■ מתברר שאומת הסטארט־אפ מסתמכת רק על מערך האבטחה של הרשת ואומרת "לי זה לא יקרה" ■ מומחית בתחום: "לצערי, רבים לא נחשפו למוצר הזה"

ליפת האבטחה החמורה שהתרחשה לאחרונה בחברת שירביט אולי זכתה לכותרות רבות, אבל היא לא לבד שם. פריצות הסייבר, כבר כתבנו על כך לא אחת, הן תופעה שהולכת ומתרחבת, בייחוד בשנים האחרונות.

הרגולציה הישראלית עדיין לא מחייבת ביטוחי סייבר, בדומה לביטוחי רכב פרטי, אך אין ספק שההתרחשויות האחרונות גרמו לכך ששוק ביטוחי הסייבר הבינלאומי צומח והופך מבוקש בקרב חברות גדולות.

מנגד, דווקא ישראל, מעצמת ההייטק והסטארט־אפ, עדיין נשרכת מאחור, וסביר להניח שהאזרח הפשוט בעל העסק הקטן אפילו לא שמע על "ביטוח סייבר". כיצד זה ייתכן?

"לא מפתיע שרבים לא נחשפו לכך, ולצערי חלק גדול מהקהל לא מכיר את המוצר הזה כלל", אומרת מיכל שלמה, סמנכ"לית ביטוח מסחרי ומומחית לביטוחי סייבר בחברת AIG ישראל. "בישראל אנחנו עדיין נמצאים קצת מאחור. סקר שערך מערך הסייבר מצא שרק 13% מהחברות בישראל רוכשות ביטוח סייבר. בעולם האחוז גבוה יותר".

שלמה מסבירה ששוק ביטוחי הסייבר הבינלאומי הוא שוק הביטוחים הצומח ביותר, והוא מגיע לסדר גודל של כ־20 מיליארד דולר. "כמו במקרים רבים, הוא מונע מרגולציה", היא מוסיפה. "אנחנו רואים שבמדינות שבהן יש רגולציה מחמירה על הגנת הפרטיות, יש גם רכישה ניכרת של ביטוחי סייבר. בארה"ב, לצורך העניין, קיימת חובת הודאה של ביטוחי סייבר".

מה הכוונה?

"אם אני מחזיק מידע של צדדים שלישיים והמידע דלף ממני, אני צריך ליצור קשר עם כל אחד ואחד מהצדדים השלישיים ולהודיע להם שהמידע דלף. האירוע הופך לפומבי ויש הרבה תביעות בעקבות כך".

דוגמה טובה מלפני שש שנים היא הפריצה הגדולה לרשת הקמעונאות טארגט, שנאלצה ליצור קשר עם 80 מיליון לקוחות ולהודיע להם שפרטיהם דלפו. "באירופה נכנסו לתוקף בשנת 2018 תקנות שמחייבות כל מיני אמות מידה של ניהול מערכות מידע, ומי שלא עמד ברגולציה מקבל קנס של 20 מיליון יורו. לאחרונה אף פורסם כי גופים רבים קיבלו קנסות כבדים", אומרת שלמה. "קיבלנו לא מעט פניות מלקוחות ישראלים בנושא. אומנם בישראל קיימות תקנות להגנת הפרטיות, אבל לרגולציה בארץ אין שיניים. אז אנחנו רואים יותר חקירות בגופים והרשות להגנת הפרטיות קצת יותר אקטיבית, אבל עדיין לא ראינו מקרים של רגולציה נחרצת מאוד".

ואז מגיעה פריצת אבטחה חמורה כמו במקרה של שירביט וכולם מתעוררים.

"בדיוק. כשמידע דולף יש גל של פניות, בייחוד כשמדובר בחברות מסחריות. אבל זו בדיוק אחת הסיבות שהביטוח הזה לא נפוץ. אנחנו מדברים על עולמות הביטוח, ובסופו של דבר אנשים לא רוצים לרכוש ביטוחים. גם כשאנחנו רוכשים, אנחנו מתפללים שלא ניאלץ להשתמש בהם. כדאי לציין סיבה נוספת: חוסר מודעות. נפגשתי עם מנכ"לים רבים שאמרו לי 'אני לא צריך ביטוח, אני מוגן. יש לי אנשי אבטחה מהשורה הראשונה'. היום אנחנו יודעים שאין מאה אחוז הגנה".

יש חברות שטוענות שהן לא מעניינות מספיק לתקיפה. מה את אומרת להן?

"חשוב לדעת שהתקיפה על טארגט למשל, מקורה באחד הספקים שלה. לאחרונה פורסם שחברת טכנולוגיה בשם עמיטל עברה אירוע סייבר, ובעקבותיה 20 חברות פעילות בתעשייה עברו אירוע דומה. שרשרת אספקה שהובילה למתקפות מראה שאף אחד לא חסין".

מה המשמעות של ביטוח סייבר?

"בביטוח סייבר יש שלושה מרכיבים עיקריים: הנזק שיכול להיגרם כתוצאה מאירוע סייבר, כופר, השבתת מערכות, השבתת אתר המכירה. בביטוח סייבר אנחנו מכסים אובדן הכנסות, הביטוח יכסה את כל תיקון המערכות. נזק של צדדים שלישיים - אם אני מחזיק מידע של לקוחות שדלף לרשת ונגרם להם נזק והם תובעים אותי או וירוס שדלף מהמערכות שלי והדביק וגרם נזק. הדבר השלישי שנותן ביטוח סייבר הוא הוצאות ניהול האירוע. כאשר המכונית נהרסת, אקנה מכונית חדשה. כאשר עוברים אירוע סייבר, בעלי עסקים הם חסרי אונים ולא יודעים מה לעשות. חברת ביטוח שמנהלת אירועי סייבר עומדת לצדו של המבוטח בניהול האירוע. כולל ספקים שראו ויודעים להעריך מאיפה חדר התוקף ומה הנזק שנגרם ואיך מחזירים את המערכות לפעולה וכולל התנהלות משפטית אם צריך וגם התנהלות עם התקשורת".

"תמיד יהיו חורים"

"כל חברה שרוצה שהביזנס שלה יתקיים לא נשארה אדישה למה שקרה עם שירביט. ולא רק שירביט, אלא גם כל המתקפות הרוסיות והאיראניות שקורות כרגע", אומרת דקלה ורד, מנהלת חטיבת solutions בחברת Experis, שאחראית על תחום הסייבר ואבטחת המידע בחברה. "אתה בודק אם מה שאתה עושה אתה עושה בצורה הטובה ביותר או שיש לך חורים. בעולם של אבטחת מידע תמיד יהיו חורים, וזה עולם של ניהול סיכונים".

כולנו מטורגטים בעצם?

"כל מי שמחזיק מידע רגיש כנראה מטורגט. ברור שיש גופים שמטורגטים יותר מאחרים כמו בנקים וגופים ממשלתיים. ישראל מטורגטת מאוד וגם ארה"ב ואיראן ורוסיה. ברוב המקרים אלו תוכנות אוטומטיות שרצות ומנסות לתפוס קודים, לתפוס איזושהי פרצה. וברגע שמצאת את הפרצה, לא משנה לך איפה מצאת אותה כי הרבה פעמים אפשר להתגלגל מאתר אחד לשני. לאחרונה מדברים הרבה בתקשורת על אבטחת מידע בשרשרת אספקה. ואכן, יכול להיות שהפגיעות שלך באה מצד ג' שאתה מתקשר איתו".

"אפשר להשוות תקיפות סייבר למוטציות הקורונה", היא מוסיפה. "אנחנו רואים עוד ועוד מוטציות שמשתכללות כמו חיידקים עם עמידות לאנטיביוטיקה. ככה זה מתקפות סייבר. גם ההאקרים לא פראיירים ומשתכללים כל הזמן. כל מיגון יוצר אתגר בצד השני".

ורד: "אנחנו רואים עוד ועוד מוטציות שמשתכללות כמו חיידקים עם עמידות לאנטיביוטיקה. ככה זה מתקפות סייבר. גם ההאקרים לא פראיירים ומשתכללים כל הזמן. וכל מיגון יוצר גם אתגר בצד השני"

ורד טוענת שלא די בהגנות ושמערך אבטחה מתחיל קודם כל בהתנהלות של החברה. "הגורם האנושי הוא הגורם החשוב ביותר", היא אומרת. "זה מתחיל במודעות של ההנהלה ויורד למודעות של עובדים. אם אני משאירה מחשב פתוח ולא נעלתי כשיצאתי לשירותים, מישהו יכול להוציא דברים. ובעקבות הקורונה צריך לשים דגש על נוהלי עבודה מהבית. אני לא מפחדת מטכנולוגיה. אני לא חושבת שאנחנו צריכים להיות מונעים מהפחד,

זליכה: "כשאני עושה ביטוח, אני מבקשת לדעת במה הגוף מבין את הסיכון ומטפל בו. צריך לבחון את זה מהעובד הקטן ועד לרמת הדירקטוריון, מודעות בכל הרמות. בכל השרשרת יכולה להיות חוליה חלשה. זו לא רק דאגה של מנהל אבטחת מידע, אלא של כל החברה"

מעריב השבוע - עסקים
עמוד 9 , 29/01/2021 , 17.88 x 33.33
כתבים: טליה לוין
76033514

משרדי שירביט. ורד: "בעולם של אבטחת מידע תמיד יהיו חורים"

צילום: פלאש 90

אלא להיות מודעים להשלכות. כל הגופים שעברו לעבוד מרחוק נדרשו להשקיע הרבה יותר".

ניהול סיכונים

"מה שזכה לחשיפה תקשורתית העלה את המודעות הציבורית", אומרת ורד זליכה, שותפה וראש תחום סייבר ואינטליגנציה מלאכותית (AI) במשרד ליפא־מאיר ושות', לשעבר ראש תחום מדיניות ויוזמות בינלאומיות במערך הסייבר הלאומי. "מה שמעניין להביט עליו במבחן הזמן היא הדרך שבה החברות מתמודדות אחרי האירוע עצמו. ניקח למשל אירוע שהיה בארה"ב לפני חמש שנים, שבו הייתה חדירה למידע של חברת ביטוח בריאות. לפי הפרסומים, חדרו למידע שכלל פרטים של 80 מיליון תיקים של מבוטחים. מה שמעניין באירוע הזה הוא שעכשיו, חמש שנים אחרי, אפשר לראות איך ארגון נדרש להתנהל ולהתמודד אחרי האירוע עצמו".

אנחנו מדברים הרבה על היערכות לאירוע ועל ההתמודדות איתו, אבל פחות על מה שקורה בהתנהלות לאחריו.

"היה אפשר לראות שאחריו נדרשה החברה לנהל מערכה רגולטורית ומשפטית רב־ממדית בכמה מישורים בעת ובעונה אחת. התנהלו גם מהלכים אזרחיים, בדיקה של הרגולטור הפדרלי. היו הליכי בדיקה מצד הרגולטורים ותובעי מדינה בארה"ב. מרבית ההליכים הסתיימו בהסדרים של החברה. לפי מה שפורסם בתקשורת, כשמסתכלים על המכלול אפשר לראות שהחברה התחייבה לנקוט מגוון צעדים שישפרו את הגנת הסייבר, לא רק ברמה הטכנולוגית אלא גם ברמה העסקית".

מה למשל?

"צורך בעריכת ניהול סיכונים מקיף, דיווח לדירקטוריון על ענייני הגנת הסייבר, קביעה באילו מקרים של אירועי אבטחה צריך ליידע את המנכ"ל, קיום ביקורות על ידי צד ג'. יש מגוון צעדים שאותם התחייבה החברה לנקוט מלבד שיפור אמצעי ההגנה הטכנולוגיים".

מה אפשר ללמוד מהאירועים האלו בראייה לעתיד?

שלמה: "נפגשתי עם מנכ"לים רבים שאמרו לי: 'אני לא צריך ביטוח, אני מוגן. יש לי אנשי אבטחה מהשורה הראשונה'. היום אנחנו יודעים שאין מאה אחוז הגנה"

"אני חושבת שהמודעות הולכת וגדלה, והגנת הסייבר נחשבת לחלק בלתי נפרד מניהול הסיכונים הארגוניים ומההתנהלות העסקית. ארגון יכול לשפר את הגנת הסייבר וגם את המוכנות שלו לאירועים בכמה מישורים: לגבש נהלים מתאימים לרגולציה, לבחון את ההסכמים עם הספקים של הארגון ולוודא שיש להם הגנה שעומדת בקריטריונים, תוכנית מגירה לאירוע סייבר. צריך להיערך כמו שנערכים לאירוע חירום".

האם יבוא יום ונראה פה בישראל חובת ביטוח סייבר, לפחות בחברות בתחומים מסוימים?

"לאחרונה פורסמה בישראל טיוטת הנחיה של הממונה על רשות שוק ההון, שמנחה את חברות הביטוח לעבודה מקיפה בנושא הסייבר. יש סעיפים שחברות הביטוח נדרשות להתייחס אליהם. עדיין לא פורסמה הנחיה סופית, אבל הצפי הוא ששוק הביטוח בישראל יידרש לכך".

בניגוד לזליכה, שלמה לא צופה שיהיה ביטוח סייבר מחייב בישראל. "אף שממליצים לגופים לרכוש", היא אומרת. "רוצים להעלות את המודעות. כשאני מזמינה ספק, אני רוצה לדעת שיש לו מערך ביטוחים למקרה שייגרם לו נזק. חשוב לי לומר שביטוח לא מחליף הגנה. הוא מוצר משלים. וכשאני עושה ביטוח, אני מבקשת לדעת כמה הגוף מבין את הסיכון ומטפל בו. צריך לבחון את זה מהעובד הפשוט ועד לרמת הדירקטוריון – מודעות בכל הרמות. בכל השרשרת יכולה להיות חוליה חלשה. זו לא דאגה רק של מנהל אבטחת המידע, אלא של כל החברה".■■■