יותר תקיפות בארגונים עם רצפת ייצור", כך אמר **עמית מלצר**, יועץ בכיר להגנת סייבר.

הוא סקר בדבריו את המגמות האחרונות בשוק אבטחת המידע. "האקלים עדיין ידידותי לתקיפות סייבר: החקיקה הבינלאומית נגד פשעי סייבר אמנם התקדמה אבל עדיין לא מושלמת ויש מדינות שהן יכולים לפעול מהן בלי הרבה הפרעות", אמר מלצר. "המדינות האלה עוצמות עין אם הן יכולות להשתמש בפושעים הללו לריגול".

לדבריו, "התפתחות הכלכלה השחורה של הפשיעה והמוביל מרחיבים את הפשיעה נגד ארגונים. הכלכלה השחורה מציעה לקנות קיטים ולפתח שיטות תקיפה מתקדמות יחסית מהר. התקיפות האלה עוברות מתחת לרדאר של תוכנות ההגנה".

הוא הסביר ש"המתקפות יתעצמו ככל שהאינטרנט של הדברים יעלה ויהפוך את הסביבה לרוויה באיומים. האיומים הם לא רק מה-IT ומצריכים חשיבה רחבה יותר. תקיפות מגיעות גם מתוכנות קבלניות או מעובדים של קבלנים".

מלצר אמר כי "יש חלחול של מוצרים שמשמשים לתקיפות סייבר מהשוק הגבוה לכלים עממיים שנסחרים באתרים לא חוקיים במחירים של בין 100 ל-1,500 דולר".

הוא התייחס בדבריו גם לשוק הישראלי וציין, כי הוא "פחות ערך עבור פושעי הסייבר הכבדים מכמה סיבות: ראשית, הגודל שלו. המוטיבציה לתקוף בישראל היא יותר לאומית-לאומנית ולא פשיעה. שנית, ישראל היא החצר האחורית של חלק לא מבוטל מהארגונים שמבצעים תקיפות, בייחוד באוקראינה וברוסיה, ואתה לא עושה את צרכיך במקום שאתה צריך אותו". בתשובה לשאלה האם סיבה נוספת לכך היא השפה העברית הוא השיב: "כן, אבל לא חסרים פושעים שגמרו אוניברסיטה ויודעים לנסח מכתב איום בעברית צחה".

בהתייחס לרגולציה אמר מלצר כי "רואים תזוזה אצל הרגולטור לגבי אבטחת המידע של התשתיות הקריטיות. פעם הרגולטור לא אישר לאף גוף פיננסי לשתף פעולה בכל מה שקשור בהגנה, אבל יש שינוי מתוך הבנה שאיומי סייבר הם איומים לאומיים ולא פקטור של תחרות עסקית".

הוא סיים את דבריו בהמלצות: "צריך שינויים ארגוניים ושינויים בתהליכי ההגנה, יותר מטכנולוגיה נוספת, כדי להתמודד מול תקיפות סייבר. הדרך היחידה להימנע מפגיעויות של מתקפות סייבר היא לאחד מרכזים ארגוניים למרכז אחד, עם תהליך עבודה מאוחד. ארגונים צריכים לעשות את זה ולשם זה הולך".

"בלי לקרב את אנשי האבטחה לאנשי התהליכים הקריטיים בארגון יהיה קשה להגן על התהליכים הקריטיים", הוסיף. "המתודולוגיה היא להגן על נכסי הליבה במקום לנסות לזהות את התוקף. צריך להציל חיים, לבטוח את השרידות של העסק ולא לרדוף אחרי הפושעים".

"בנוסף", אמר מלצר, "יש לנסות לייצר מודיעין על ידי שיתופי פעולה. חברות מסחריות יכולות להתארגן ביחד לצורך כך. לפחות 50% ממודיעין הסייבר מעניין את כל החברות המסחריות ולא צריכים לחלוק את הסודות הפנימיים של כל חברה. זה חוסך בעלויות".

## איך תוקף לומד על המטרה שלו?

**ג'קי אלטל**, מומחה לאבטחת מידע ב-Altal security ומנהל בתחום התקיפה בשיא סקיוריטי, הסביר באילו דרכים יכול תוקף לנקוט כדי ללמוד כמה שיותר פרטים על המטרה שלו.

"ראשית, יש כיום מידע רב באמצעי תקשורת המונים ומדיה חברתית שונים", אמר. "צריך לאסוף את המידע מכל מיני מקומות. למשל, יש מידע חשוף ברשת - באתרים, בפורומים ובצ'אטים - ומידע בדארקנט, כולל פורומים שכל התפקיד שלהם הוא למכור מידע עבור כמה שיותר כסף. אפשר גם לבנות מנוע חיפוש אישי באמצעות גוגל (Google) שיוקדש לנושאים מסוימים שקובעים".

הוא הסביר שתוקף צריך למצוא את נקודות החולשה של הקורבן שלו ולתקוף, ושקל לעשות את זה במכשירים סלולריים. "אפשר לקנות רישיון של ארגון, לדאוג לכלי זדוני, לקחת את המכשיר ממישהו לשנייה, להיכנס לאתר, ללחוץ OK ולקבל שליטה על הטלפון. יש פה בעיה קשה מאוד", אמר.