חצי ממתקפות הסייבר - מצליחות ומתגלות רק לאחר כמה חודשים

"מחקר העלה שב-84% מהמתקפות הצליחו התוקפים לחדור למערכות הארגון תוך שעה בממוצע וש-66% מהחדירות מתגלות רק לאחר חודשים - משך זמן בו ההאקרים עושים שמות במידע הארגוני", אמר יהונתן גד, יושב ראש ומנכ"ל משותף, אינוקום מקבוצת אמן * הוא ציין ש-"זהות ההאקרים השתנתה ויש שינוי בסוג המתקפות - הן מורכבות יותר ומצליחות לחדור את קו ההגנה הקיים של ארגונים"

יוסי הטוני > צילום: קובי קנטור

לצד העובדות שכמות מתקפות הסייבר גדלה ורמת המורכבות שלהן הולכת ומשתכללת יש נתון לא פחות חשוב: מחקרים מצביעים שמחצית מהמתקפות מצליחות ושבשני שליש מהמקרים הן מתגלות רק לאחר כמה חודשים", כך אמר **יהונתן גד**, יושב ראש ומנכ"ל משותף של אינוקום מקבוצת אמן. לדבריו, "אחת הבעיות בעולם האבטחה היא הפער בין מועד המתקפה למועד הגילוי שלה. אחד המחקרים העלה שב-84% מהמתקפות הצליחו התוקפים לחדור למערכות הארגון תוך שעה בממוצע וש-66% מהחדירות מתגלות רק לאחר חודשים - משך זמן בו ההאקרים עושים שמות במידע הארגוני".

יהונתן גד

גד דיבר בפתח כנס לקוחות שערכה החברה תחת השם Cyber Defense 360 באולמי סטוקו, ליד מגרשי הטניס בתל אביב, בהשתתפות יותר מ-150 מקצועני אבטחת מידע.

הוא ציין ש"זהות ההאקרים השתנתה. לא מדובר עוד בצעירים לא מנוסים ורודפי תהילה אלא בהאקרים מקצועיים, שפועלים בשליחות מדינות או ארגוני פשע מקוון".

"המטרה היא לחסום את המתקפה עוד לפני שהיא מגיעה ללב ה-IT הארגוני ואם לא מצליחים בכך, נדרש לתת מענה מיידי לאירוע האבטחה", אמר גד. "צריך לספק לארגונים קו הגנה חזק ומודרני".

לדבריו, "אם עובדים מביאים רכיבי מחשוב אישיים מהבית לארגון, לא ייתכן מצב בו מנהל האבטחה יאשר להם להשתמש רק ב-2-3 יישומים. יש לספק לו מעטפת אבטחת מידע כוללת, גם עבור המיחשוב האישי שלו. צריך לאפשר לו לעבוד בצורה מאובטחת בכל מקום ועם כל רכיב".

"אנחנו בפירוש מבחינים בשינוי בסוג המתקפות. הן מורכבות יותר ומצליחות לחדור את קו ההגנה הקיים של ארגונים", הוסיף. "המתקפות המסוכנות ביותר הן מסוג APT, מתקפות מתמשכות וממוקדות, כי הן מיועדות לאנשים ספציפיים שההאקרים רוצים באמצעותם לגרום נזק לארגון או לגנוב מידע ארגוני יקר ערך עסקי". לגבי השוק הישראלי, בהקשר הזה, אמר גד ש"בארץ נפוצה התפיסה של 'לי זה לא יקרה', אבל זה קורה".

הוא סיכם באמרו ש"כל הארגונים, גם הקטנים והבינוניים נמצאים על הכוונת של ההאקרים".

מה עם ניהול הסיכונים?

פול דיוויס, סגן נשיא פייראיי לאזור אירופה, אמר ש-"האיומים הולכים ונהיים מתוחכמים יותר, ויותר מבעבר הם מצליחים לעקוף את מערכי ההגנה המסורתיים בארגונים. לצד אבטחת מידע נדרש לערוך ניהול סיכונים, כי ברור שאין 100% הגנה. יותר ויותר מנהלי אבטחת מידע מבינים שהגישה המסורתית לאבטחת מידע אינה יעילה".

הוא ציטט מחקר שערכה החברה ממנו עולה, כי 89% מהמתקפות שנחקרו היו מסוג APT, שקשורות לכלים שפותחו והופצו על ידי קבוצות האקרים סיניות. לדבריו, החוקרים מצאו 184 מדינות ששימשו בסיס לפעילות תקיפה או שהיו בהן שרתי פיקוד ובקרה (CnC). מדובר בגידול של 41% לעומת 2010, אז נמצאו שרתים ב-130 מדינות. רוב המדינות מהן התבצעה הפעילות הן מאסיה וממזרח אירופה.

פול דיוויס

לדברי דיוויס, הפלטפורמה של פייראיי "היא הדור הבא להגנה מפני איומים. יש בה מנוע ניתוח של האיומים, אנחנו עובדים בשילוב מוצרי אבטחה אחרים ומספקים מענה להגנה נגד מתקפות מסוג Zero Day, תוך שימוש בשיטת 'ארגז חול', בו מתבצעת 'הפצצה' של הנוזקה. 'הפצצה' זו מאפשרת לזהות את הנוזקה ולמנוע את חדירתה למערכות הארגון".

הוא סיכם בציינו, כי "מנעד איומי הסייבר התרחב והם משתנים ומשתכללים. מצב זה מאפשר לפושעי הסייבר להתחמק בקלות מאיתור ולהיכנס ליותר ארגונים - ויותר גדולים. מדובר במגיפה עולמית של הזן החדש של מתקפות סייבר מתקדמות".

"לצמצם חלון החשיפה של התוקף"

"כיוון שמוסכם על כולם שאין מצב של הגנה מוחלטת ומוכללת, המטרה היא לצמצם את חלון החשיפה של התוקף, לזהות את המתקפה עוד בתחילתה ולמזער את נזקה", כך אמר **ג'יימס פטינסון**, סגן נשיא לאזור EMEA בסולרה, המיוצגת בישראל על ידי אינוקום.

הוא פתח את דבריו בציטוט מבודח של יוגי ברה, שאמר: "קשה מאד לחזות, ובעיקר קשה לעשות זאת לגבי העתיד". המטרה של פטינסון בציטוט הייתה להמחיש את הקושי בזיהוי מתקפות עתידיות. "מטרתנו היא לחקור את כל שכבות ה-IT אשר נפגעו ממתקפה", אמר פטינסון.

לדבריו, "מדי יממה נוצרות 100 אלף נוזקות. כמו כן, יש יותר מתקפות והן יותר מתוחכמות. במצב דברים זה, מערך ההגנה ההיקפי המסורתי אינו מספק את רמת אבטחת המידע הנדרשת עבור ארגונים".