טילים קיברנטיים עלייך, ישראל

"ישראל לא חסינה - היא המדינה המותקפת ביותר במזה"ת אחרי לבנון", אמר מרקו ריבולי, סגן נשיא אזורי בסימנטק, בכנס הלקוחות שערך הסניף הישראלי של ענקית האבטחה ◆ "אנו בעיצומו של עידן חדש, של מתקפות שהמניע שלהן הוא לא רק כספי, אלא גם פוליטי - והמשמעות היא שעל ארגונים להיערך מראש עם מערך שלם של שכבות הגנה" ◆ שמוליק אנג'ל, סימנטק ישראל: "למרות שתקציבי האבטחה נותרו שטוחים, היקף הפעילות שלנו גדל"

יוסי הטוני > צילום: קובי קנטור

במיפוי כמות האיומים בהיבט הגיאוגרפי, המזרח התיכון הוא האזור המותקף ביותר. בתוכו, ישראל היא המדינה השנייה בהיבט כמות המתקפות, לאחר לבנון. על ארגונים בישראל להבין, כי הם אינם חסינים - ולהיערך בהתאם", כך אמר **מרקו ריבולי**, סגן נשיא אזורי בסימנטק. ריבולי היה דובר המפתח בכנס הלקוחות שקיים הסניף הישראלי של ענקית אבטחת המידע. הכנס, שהופק על ידי אנשים ומחשבים, נערך במרכז הכנסים אבניו שבקריית שדה התעופה, בהשתתפות יותר מ-800 לקוחות ושותפים עסקיים.

מרקו ריבולי, סגן נשיא אזורי בסימנטק

לדברי ריבולי, ארגונים נדרשים לחשוב מחדש כיצד עליהם להיערך לצורה חדשה של הגנה על המידע ועל מערך המיחשוב והתקשורת הארגוניים, תוך הטמעת ניהול הסיכונים כחלק משולב בתהליך. הוא תיאר את התפתחות האיומים ברשת, וציין כי בין השנים 1986 ל-1991 החלו להופיע הווירוסים הראשונים. לדבריו, במהלך העשור האחרון של המאה הקודמת ועד 2005, עילת הווירוסים הייתה הרצון בתהילה של כותביהם. ב-2005, אמר, חל שינוי מהותי בנוזקות, שכבר הפכו משוכללות יותר, והמניע ליצירתן השתנה והפך להיות פלילי-כלכלי. כך, הסביר, הן החלו לגרום לאובדן מידע וגניבתו.

כיום, אמר ריבולי, המתקפות ממוקדות יותר, מורכבות יותר ומשוכללות יותר - והסיבה היחידה לקיומן היא גניבת מידע. "לצד העלייה בכמות המתקפות ובמורכבותן, ניכר גידול גם בהיקף הנזק הכספי מכל תקיפה, בשל ההטרוגניות של תשתיות ה-IT וריבוי מערכות ה-IT והמורכבות שלהן".

הוא תיאר בפני משתתפי הכנס את המתקפה הקיברנטית שהובילה הנוזקה שאמון כלפי חברת הנפט הגדולה, סעודי ארמקו. הנוזקה, אמר ריבולי, הייתה מסוג "מתקפת יום אפס" והיא תקפה ב-16 באוגוסט השנה - היום האחרון של חג הרמאדאן. לדבריו, הנוזקה הייתה נטולת חתימה, עירבה פישינג עם מתקפה ממוקדת והייתה בעלת יכולות להשמדת מידע והצפנה עצמית. הנוזקה, הסביר, פגעה במגוון הגרסאות של מערכת ההפעלה חלונות של מיקרוסופט, כולל חלונות סרבר במהדורות 2003 ו-2008. בשל המתקפה, אמר ריבולי, שותקו יותר מ-35 אלף מחשבי תאגיד הנפט הענק.

> מרקו ריבולי: "יש להכניס 'שכל' להיבט האבטחה. רק מוצרים זה כבר לא מספיק. ה-'רעים' מגבירים את פעילותם ושוכרים אנשי אבטחה המתמחים בשלל מקצועות בתוך עולם הפריצה - מיפוי, איתור מטרות, פריצה בפועל, השתלטות על מערך ה-IT הארגוני"

"בעיצומו של עידן חדש"

"אנו בעיצומו של עידן חדש, של מתקפות שהמניע שלהן הוא לא רק כספי, אלא גם פוליטי", אמר ריבולי, "והמשמעות היא שעל ארגונים להיערך מראש עם מערך שלם של שכבות הגנה. תגובה לאחר המתקפה כבר לא תועיל כבעבר. יש להכין תוכנית מסודרת, הכוללת הנחת מוצא שיש סיכוי שהארגון יותקף, וייתכן אף שהוא כבר הותקף ואיננו יודעים זאת. יש להכין תוכניות גיבוי והתאוששות מאסון".

הוא תיאר את ציר הזמן של הכנה למתקפה, ואמר כי השלב הראשון הוא ההיערכות; לאחריו, המועד בו ניתנת - אם ניתנת - התראה; לאחר המתקפה יש את משך הזמן שייקח לגלות ולנטר אותה; ולבסוף - ההתאוששות מאסון. "ככל שארגונים ישקיעו מראש, בזמן שטרם המתקפה, ככה הם יחסכו עלויות לאחר שזו תקרה וכך הנזק הכספי שייגרם להם יהיה קטן יותר", אמר ריבולי.

לדבריו, "יש להכניס 'שכל' להיבט האבטחה. רק מוצרים זה כבר לא מספיק. ה-'רעים' מגבירים את פעילותם ושוכרים אנשי אבטחה המתמחים בשלל מקצועות בתוך עולם הפריצה - מיפוי, איתור מטרות, פריצה בפועל, השתלטות על מערך ה-IT הארגוני, גניבת מידע, השמדתו והפצתו. העולם של הרעים התמקצע מאוד בשנים האחרונות וארגונים טרם הפנימו את זה. ארגוני האקרים פועלים כמו ישויות מדינתיות מבחינת העוצמות שלהם".

דרגת המוכנות של ארגונים

ריבולי חילק את הארגונים לארבעה סוגים מבחינת המוכנות שלהם: כאלה המגיבים באופן ידני ולא ממוכן לאחר המתקפה, כאלה שיש להם כלי הגנה אך באופן חלקי, כאלה שכבר הצליחו לשלב את מערך כלי ההגנה וליצור תמונה משולבת של ה-IT שלהם, ולבסוף - אלה המסוגלים לספק הגנה דינמית והם בעלי יכולת עמידות גבוהה של מערכות ה-IT. רוב הארגונים, ציין ריבולי, נמצאים באמצע - בין הקבוצה השניה והשלישית