

איומים עלייך, ישראל

פטריס פרש, פורטינט: "ארגונים שלא יערכו ל-APT יקרו ב-2012" ❖ "כדי לשרוד, על הארגונים לשנות את האופן שבו הם פועלים בעולם ההגנה והאבטחה", אמר פרש, סגן נשיא גלובלי למכירות ותמיכה בפורטינט העולמית

יוסי הטוני < צילום: קובי קנטור



פטריס פרש, סגן נשיא גלובלי למכירות ותמיכה בפורטינט העולמית

לגדול השנה, לאור העובדה ששלושת הרבעונים מאז תחילת 2011 הניבו לחברה מכירות בסך של 335 מיליון דולרים. הוא ציין, כי יש בקופה של פורטינט חצי מיליארד דולרים במזומן וכי החברה שמה דגש משמעותי על מו"פ. כך, אמר, מאז הקמתה החברה השקיעה במו"פ יותר מרבע מיליארד דולרים, כאשר בשנה החולפת עמד היקף ההשקעה שלה בתחום זה על יותר מ-10% והגיע ל-44.2 מיליון דולרים. לחברה, ציין פרש, יש יותר מ-100 אלף לקוחות ארגוניים ויותר מ-800 אלף מוצרים שלה הוטמעו בעולם. בשנה הבאה, פורטינט צופה לחצות את רף מיליון המוצרים כבר ברבעון הראשון של 2012, אמר.

"לצערנו", הוסיף פרש, "מנמ"רים רבים מכחישים ומדחיקים את העובדה שפתרונות הפיירוול והאנטי-וירוס, ומערכות מניעת החדירה מבוססות החתימות המותקנים ב-IT שלהם מספקים הגנה מוחלטת, אף שהדבר נכון רק בחלקו. כך, מחקר של גרטנר שפורסם באחרונה העלה, כי 4%-8% מהמחשבים בבתי העסק משמשים כזומבים, ובכתיים הפרטיים הנתון גבוה יותר ועומד על 20%, למרות עדכוני האבטחה".

הוא סיכם באמרו, כי עולם האבטחה עבר שינוי. "בעיות האבטחה הפכו להיות ממוקדות יותר במצב הרשתות הפנימיות בארגון ולא בניסיונות חדירה חיצוניים", אמר פרש. לדבריו, "הדגשים החשובים ביותר הם מימוש אבטחת המידע וניטור הרשת, תוך אי פגיעה ברציפות המידע וגרימה של עיכוב ברשת, כי היישומים ככדים יש בהם מימדים של חו"ז וקול. אנחנו היחידים בשוק שמספקים פתרון אחד ומוכלל".

"הסניף הישראלי צמח בכל מגזרי השוק"

"מנהלי אבטחת מידע מכינים שעליהם לשנות את האופן שבו הם מגנים על מערך ה-IT הארגוני שלהם. אחת ההוכחות לכך היא הצמיחה שלנו בכל מגזרי השוק - בתעשייה, בטלקום ובמגזר הפיננסי, כמו גם בקרב ארגוני SMB. השנה חוונו גידול משמעותי בפעילות שלנו, בשיעור דו-ספרתי, וכך

חלק ממנהלי אבטחת מידע בארגונים, לצערי, שרויים בנמום ואינם מכינים את השינוי הדרמטי שעוברים האקרים, יחד עם האיומים הנלווים אליהם. ארגונים שלא יערכו בצורה מיטבית לקראת מתקפות ממוקדות ומתמשכות (APT) ולא ישנו את האופן שבו הם פועלים בעולם ההגנה והאבטחה - לא יצליחו את 2012?, כך אמר פטריס פרש, סגן נשיא גלובלי למכירות ותמיכה בפורטינט העולמית.

פרש היה דובר המפתח בכנס שערך הסניף הישראלי של החברה. לכנס, בהפקת אנשים ומחשבים, הגיעו יותר מ-400 מנהלי אבטחת מידע ומקצוענים בתחום. הוא נערך במלון דיוויד אינטרקונטיננטל בתל אביב.

בדבריו ציין פרש שלוש מגמות-על בעולם האבטחה: הראשונה היא השינוי מהרס אתרים לשם ונדליזם ופרסום לגניבת מידע שיטתית ומתמשכת לטובת מניעים כלכליים, או לצורך פעילות ריגול בין מדינות או ארגונים שלוחי מדינות. השנייה היא ריבוי רכיבי אבטחת מידע בארגונים, שלא תמיד פועלים בסנכרון ביניהם, ובכל מקרה - יש קושי לתזמר, לנהל ולבקר אותם. המגמה השלישית היא מעבר של מערכי IT ארגוניים לעבודה בתצורת מיחשוב ענן, מה שמקשה על השליטה במידע והשליטה בגישת המשתמשים אליו.

לדברי פרש, אחד האתגרים שמולם נדרשים מנהלי אבטחת המידע בארגונים להתמודד הוא הצורך בטיפול ובאבטחת נכחי המידע הגדולים. "לצד אלה קיימים אתגרי העבר: מניעת דליפת מידע ארגוני (DLP) ועבודה של עובדים מחוץ לארגון", אמר. "אתגר נוסף שקיים בשנתיים האחרונות הוא אבטחת סביבת ה-IT הווירטואלית, תוך ניטור תעבורת הרשת בסביבה ובמערכות אלה. זאת, לצד הצורך שלא לפגוע בחוויית המשתמש הארגוני בעת עבודתו בסביבה מאובטחת. פורטינט שמה דגש על מימוש האתגרים הללו".

"ה-APT הופך פתרונות אבטחה ללא רלוונטיים"

הבעיה החריפה ביותר, ציין פרש, היא ה-APT (Advanced Persistent Attacks). לדבריו, "מדובר במושג ששואל מעולם הביון והמודיעין, ומשמעו מתקפות מתקדמות ומתמשכות. סוג איום שכזה הופך הרבה מאוד מפתרונות אבטחת המידע ללא רלוונטיים, לכאלה שעונים על איומי האתמול, מאחר שכל פתרונות האבטחה מבוססי חתימות לא מסוגלים להתמודד עם האיומים הללו. מה שנדרש הוא פתרון פרו-אקטיבי, שיועד לזהות באופן מקדמי את ניסיונות ההידבקות של המחשבים הללו על ידי רשתות בוטנט ולחסום את דרכי התקשורת עם המפעילים המרוחקים של הבוטנט".

פרש ציין שפורטינט נוסדה ב-2000 והונפקה בבורסה ב-2009. מטה החברה ממוקם בסאנווייל שבקליפורניה, והיא מונה יותר מ-1,500 עובדים. מחזור המכירות שלה בשנה החולפת עמד על 325 מיליון דולרים, וצפוי

פטריס פרש: "אחד האתגרים שמולם נדרשים מנהלי אבטחת המידע בארגונים להתמודד הוא הצורך בטיפול ובאבטחת נכחי המידע הגדולים. לצד אלה קיימים אתגרי העבר: מניעת דליפת מידע ארגוני (DLP) ועבודה של עובדים מחוץ לארגון"