

להרוג את המפתחים?

ד"ר גארי מק'גרו, גורו אבטחת מידע: "איש לא מלמד את המפתחים אבטחה - אז אולי 'נהרוג' אותם" ♦ "צריך לצמצם את הפער בין המפתחים לאנשי האבטחה, כי לכולם יש אינטרס מובהק לדבוק ולאמץ מדיניות אבטחת מידע ופיתוח יישומים באופן מאובטח", אמר מק'גרו ♦ לדבריו, "הסיבה לכך היא ש-80% מהמתקפות מגיעות ליישומים"

יוסי הטוני

אפליקטיביות, כפי שנהוג לחשוב. בראש סדר העדיפויות נמצא תהליך בחינת הקוד, לאחריו ביצוע מבדקי אבטחה מבוססי סיכונים ורק אחרי כן יש לערוך מבדקי חדירה".
הוא סיים באומרו, כי "כל הבדיקות והניתוחים מאוד חשובים אבל, בסופו של דבר, הכי חשוב לתקן את הפרצות. טיפשי ככל שזה יישמע, אם לא יתוקנו הבאגים - אין ערך לכלל כלי אבטחת המידע המוטמעים בארגון".

מוצר אבטחה שפותח בישראל

במהלך הכנס הושקו מוצרים ושירותים חדשים שמאפשרים לארגונים להגן על עצמם מפני תקיפות, לנהל את הסיכונים הכרוכים בשמירה על המידע ולהרחיב את יכולות האבטחה הארגונית. המטרה היא לאפשר להם להתמודד טוב יותר עם האיומים ההולכים וגוברים בעולם העסקי המודרני.

על פי HP, המוצרים והשירותים החדשים מאפשרים לארגונים להתמודד טוב יותר עם אתגרי האבטחה שלהם באמצעות מערכת ניהול אירועי אבטחת מידע רוחבית, אחודה ומקיפה, שמאפשרת לנהל את הסיכונים והתאימות לרגולציה. ענקית ה-IT ציינה, כי ארגונים לא עומדים כיום בפני איום או תוקף יחיד. הם נלחמים באיומים מאורגנים וממומנים היטב. גישת HP לתחום אבטחת מידע, מסרה החברה, נשענת על שיבוש מחזורי ההתקפה לצד מניעה וגילוי איומים בזמן אמת, בשכבת היישום לחומרה או בממשקי התוכנה.

עוד הושקו באירוע פתרונות שמסייעים לארגונים להתגבר על אירועי סייבר ולשפר את תפקודם של צוותי אבטחת המידע באמצעות שימוש בניטור נתונים ממערכות Big Data בזמן אמת וזיהוי איומים ברמת היישום.

כך, הוצג המוצר HP ArcSight Risk Insight, שפותח במלואו בישראל. המוצר מסייע לצוותי אבטחת מידע לזהות מתקפות מתקדמות, לנתח אירועים ולקבוע האם האיום קריטי והאם יש לו השפעה על מערכות הארגון.

כמו כן, הושקה בכנס משפחה חדשה של פיירוולים מהדור ה-NGFW (HP TippingPoint Next Generation Firewall), שמסוגלים להגן על לקוחות מאיומים בסביבות המכשירים הניידים והענן. מדובר בחמישה מוצרים חדשים שמרחיבים את קו מוצרי הגנת הרשת שלה ומסייעים לארגונים לשבש את פעילות פושעי הסייבר לפני פגיעתם ברשת.



ד"ר גארי מק'גרו

איש לא מלמד את מפתחי התוכנה אבטחת מידע במהלך תהליך הפיתוח. ייתכן שאחת הדרכים לטפל בבעיה היא 'להרוג' את המפתחים", כך אמר ד"ר גארי מק'גרו, גורו ומומחה בעל שם עולמי לאבטחת מידע.

ד"ר מק'גרו, סמנכ"ל טכנולוגיות ב-Cigital, היה דובר המפתח בכנס HP Protect, שנערך לפני ימים אחדים בווישינגטון. לדבריו, "קיים מרחק בין אנשי הפיתוח לאנשי אבטחת המידע. כל קבוצה מרוכזת בתחומה ודואגת לטריטוריה שהיא חולשת עליה. צריך לצמצם את הפער ביניהן, כי לכולם יש אינטרס מובהק לדבוק ולאמץ מדיניות אבטחת מידע ופיתוח יישומים באופן מאובטח. הסיבה לכך היא ש-80% מהמתקפות מגיעות ליישומים".

הוא ציין, כי בכל ארגון יש כמה וכמה מחזורי פיתוח של אבטחה, (SDLC (Security Development Life Cycle). "כמעט לכל פרויקט פיתוח יש תהליך משלו, מה שעוד יותר מקשה על הארגון לאמץ ולהטמיע תהליך מאובטח. המשוואה פשוטה: אם יש יותר שורות קוד שפותחו - יש יותר באגים", אמר.

בדיקות חדירה אינן הפתרון לבעיות אבטחה אפליקטיביות

על פי ד"ר מק'גרו, "בדיקות חדירה הן לא הפתרון לבעיות אבטחה

