

מוטי שגיא: "מה שנדרש ממנהלי אבטחת המידע הארגוניים הוא לעבור מגישה של אבטחה תגובתית לאבטחה צופה פני עתיד, פרו-אקטיבית. ארגונים מצאו את עצמם מלאים בטכנולוגיות אבטחה שונות"

סלולרי חכם המכיל יישומי רשת".

ניתוחים של אירועי אבטחת מידע

מוטי שגיא, יועץ אבטחת מידע בכיר בפורטינט ישראל, הציג ניתוחים של כמה אירועי אבטחת מידע, על מנת להמחיש את השינוי שחל בסוג התקיפה ובתחכום של התוקפים.

הוא מנה שני עקרונות שלדבריו מנחים את עולם אבטחת המידע: "העיקרון הראשון הוא יפחות הוא יותר". זה מושג שנכון גם בארכיטקטורה וגם באבטחת מידע, כי נדרש לשמור על פשטות. התקנה של ריבוי מוצרים ותצורה מקשה על ניהולם, בבחינת יתפסת מרובה לא תפסת. העיקרון השני הוא 'האמת', אלוהים נמצא בפרטים הקטנים. לעתים, ההבדל בין התקפה מוצלחת ללא מוצלחת הוא בפרטים הקטנים שהמגן התכונן אליהם. הסיבה לאיומי אבטחת המידע, אמר שגיא, היא הפסוק מספר בראשית: 'כי יצר לב האדם רע מנעוריו'".

שגיא ניתח בפני המאזינים את הפריצה שאירעה במרץ השנה למערך ה-IT של RSA, חטיבת האבטחה של EMC. לדבריו, ייחודה של המתקפה הוא כפול - הן בגלל רמת התחכום שלה והן בשל העובדה שה-IT של RSA לא היה היעד של הפורצים, כי אם זה של לקוח שלה - לוקהיד-מרטין. "מה שקרה זה שההאקרים לקחו קובץ אקסל, תקעו בו תוכן של פלאש ושולחו לשני עובדים בפשיעו ממוקד, המכונה 'חנית'", אמר שגיא. "לאחר החדירה הראשונית, ההאקרים הצליחו לשוטט ברשת התקשורת של RSA. כך ולהוציא את המידע שהיה דרוש להם לטובת הפריצה ללקוח של RSA. הם הצליחו לעבור מבעד ה-SSLVPN של ענקית התעופה".

כן הציג שגיא את סיפורו של "אגוז צרפתי" - בלוגר שחשף בבלוג שלו באתר תפוז את הספילרים של "האח הגדול", "הישרדות" ו"כוכב נולד". הוא ביצע זאת על ידי משלוח של הודעות מזויפות בפייסבוק למפיקי התוכניות, ובאמצעותן פיתה אותם להיכנס לדף מזויף. כך הוא הצליח לחזור לתיבות הדואר הפרטיות של אותם מפיקים, ומתן השיג את המידע החסוי.

שגיא סיכם בציינו, כי "מה שנדרש ממנהלי אבטחת המידע הארגוניים הוא לעבור מגישה של אבטחה תגובתית לאבטחה צופה פני עתיד, פרו-אקטיבית. ארגונים מצאו את עצמם מלאים בטכנולוגיות אבטחה שונות. איחוד של כל פונקציות האבטחה השונות למערכת אחת מאפשר לצמצם משמעותית את העלות שלהן ומפשט את הצורך בניהולן המורכב. אנחנו מספקים מענה לאיומי האבטחה העכשוויים והעתידיים".



אלי פרנס, מנהל אזורי ישראל, קפריסין ויוון בפורטינט

יהיה גם בשנה הבאה. בגלל העלייה הזאת, נגדיל את כמות אנשי המכירות בחברה", כך אמר **אלי פרנס**, מנהל אזורי ישראל, קפריסין ויוון בפורטינט, שהנחה את האירוע.

פורטינט, אמר פרנס, נמנית על חמש חברות אבטחת המידע הגדולות בעולם וקצב הצמיחה הרבעוני שלה עומד על 35%. הוא ציין, כי החברה ביצעה יותר מ-10,000 הטמעות של מוצריה בישראל. "אנחנו פעילים בעולם ה-UTM, ר"ת של ניהול איומים אחוד. חברות המחקר תמימות דעים בהערכתיהן שתחום ה-UTM הוא החשוב ביותר בעולם האבטחה. כבר כיום אנחנו מובילים את התחום הזה, עם נתח השוק הכי גבוה. זאת, כיוון שהיינו הראשונים להכין את חשיבותו והיינו חלוצים לספק מערכת אחודה לניהול איומים. יש לנו יסוד סביר להניח שנמשיך להוביל את השוק הזה".

יתרונה של גישת ניהול האיומים האחוד, סיכם פרנס, "הוא בכך שהיא מספקת מענה למגוון איומים, למורכבות שלהם, כמו גם לשימוש ברכיבי מיחשוב שונים מצד המשתמשים הארגוניים, דוגמת מחשב נייד וטלפון



מוטי שגיא, יועץ אבטחת מידע בכיר בפורטינט ישראל

