

הגרסה הבאה של צ'ק פוינט, הם יידרשו לתוספות. לפיכך, הם ערכו הליך בדיקה למכונות של פאלו אלטו והתרשמו מאוד. "בפרק זמן קצר, שבועות בודדים, הוטמעו ארבע מערכות פאלו אלטו בארבעת סניפי החברה, ועוד מערכת הזמנה, לטובת יתירות ושירות, לשם גיבוי", סיכם רשף. "אנשי אטיוניטי קיבלו פתרון אחד שפותח על ידי חברה אחת ומספק מענה כולל ויכולות ניהול ושליטה מלאות".

מחקר: המתקפות הקיברנטיות גדלות בכמות ובתחכום - מתמקדות בחברות IT

חוקרים מפייראיי בדקו 12 מיליון מתקפות שבוצעו על מחשבים שמותקנת בהם הפלטפורמה של החברה וגילו ש-89% מהן היו מתקפות מתמשכות וממוקדות ♦ הן בוצעו מ-184 מדינות - 41% יותר מאשר הנתון שנאסף ב-2010, שעמד על 130 מדינות ♦ לדברי החוקרים, "מדובר במגיפה עולמית של הזן החדש של מתקפות סייבר מתקדמות"

חברות IT והיי-טק הן בין המותקפות בתדירות הגבוהה ביותר על ידי האקרים - כך עולה ממחקר חדש. ככלל, הנתונים מעלים שמספר המתקפות הקיברנטיות והאיכות שלהן נמצאים בעלייה.

המחקר בוצע על ידי פייראיי, שמוצגת בישראל על ידי אינוקום מקבוצת אמן. החוקרים בדקו 12 מיליון מתקפות שהנתונים אודותיהן נאספו מאלפי מחשבי משתמשים בהם הוטמעה הפלטפורמה של החברה. 89% מהמתקפות שנחקרו היו מסוג APT (מתקפות מתמשכות וממוקדות) שקשורות לכלים שפותחו והופצו על ידי קבוצות האקרים סיניות.

הדו"ח מצא 184 מדינות ששימשו בסיס לפעילות התקיפה 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. המתקפות שנחקרו משתמשות בשרתי פיקוד ובקרה כדי לשמור על תקשורת עם המחשבים הנגועים, כך שהתוקפים יכולים להוריד או לשנות את הנוזקות כדי למנוע זיהוי שלהן, לחלק נתונים או להרחיב את המתקפות בתוך הארגונים.

לדברי דייוויד דה-וולט, מנכ"ל פייראיי, "מנעד האיומים התרחב ואימי הסייבר 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".

יוסי הטוני

בהמשך הציג פטינסון את הפתרונות של סולרה ואמר שהם "מאפשרים לארגונים לקבל מבט מלא על הרשת שלהם ומספקים תוכן והקשר לכל אירוע אבטחה. אנחנו נותנים מענה לעולם האיומים המשתנה ומסייעים לארגונים לצמצם את הפער, עם ניטור של כל פעילות הארגון ברשת והצפת המידע הרלוונטי לצוות אבטחת המידע - מה ואיפה לחפש. אנחנו מספקים תגובת נגד לאירועי אבטחת מידע ולניתוח שלהם".

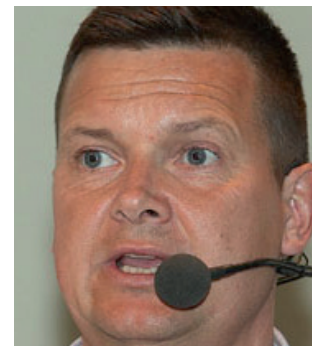


גיימס פטינסון

מדס רונברג, מנהל מכירות אסיה ב-Precise Biometrics, אמר שהחברה מספקת כלי לזיהוי המשתמש באמצעות כרטיס חכם, טביעות אצבע או שתי הטכנולוגיות יחדיו, לטובת כניסה לרשת הארגונית גם עם טלפון חכם או טאבלט. "כל ארגון יהיה בסופו של דבר בעולם הנייד", ציין.

"השאלה שנוותרת פתוחה היא איך לאבטח עולם זה באופן שיאפשר שימושים אישי ועסקי במובייל, מבלי לפגוע בחוויית המשתמש ותוך אבטחה מרבית של המכשיר. הפתרון שלנו מביא את תשתית תחנת העבודה הנייחת אל העולם הנייד".

הוא הציג סיפור לקוח שעסק בהטמעת הפלטפורמה של החברה בקרב אלפי עובדי משרד החוץ האמריקני, לאחר שהוחלט לאשר להם לעבוד עם מכשירי iPhone.



מדס רונברג

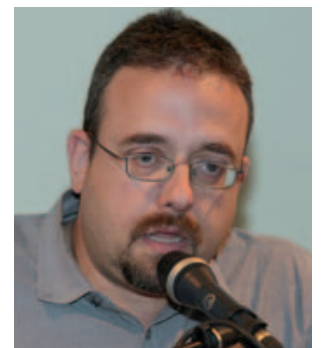
"מרדף בלתי פוסק אחרי פתרונות אבטחה"

"ארגונים נמצאים במרדף בלתי פוסק אחרי פתרונות אבטחת מידע, מה שמביא אותם לעשות שימוש במספר רב של טכנולוגיות נישא. זה גורר עמו עלויות גבוהות, עומס רב וקשיים תפעוליים, מבלי שמערך ההגנה יתפקד כראוי", כך אמר אסף רשף, מהנדס מערכות בכיר לאבטחת מידע בנטקום מקבוצת מלם-תים.

הוא הציג, כסיפור לקוח, פרויקט שביצעה נטקום לפני כמה חודשים להסבת מערך אבטחת המידע של אטיוניטי, ספקית מוצרי תוכנה ארגונית - מזה של צ'ק פוינט לזה של פאלו אלטו, המיוצגת בארץ על ידי אינוקום.

אטיוניטי היא חברה גלובלית, עם שני סניפים בארץ ושניים בחו"ל, וסביבות הפיתוח שלה הן "רגישות", ציין רשף. הוא הוסיף, כי מערך ההגנה של אטיוניטי התבסס על גרסה R65 והם שקלו מעבר לגרסה R7 של צ'ק פוינט.

"הדרישות של אנשי האבטחה בחברה היו: פיירוול, IPS, איכות שירות, זיהוי מודעות יישומים וזיהוי משתמשים. הם רצו שיפור ברמת הביצועים של כל אלה", אמר. "אנשי האבטחה של אטיוניטי הבינו שאם יטמיעו את



אסף רשף