

כלי חדש למניעת פריצה לבסיסי נתונים פיננסיים

בכנס הציגה RSA לראשונה את כלי חדש למניעת פריצה לבסיסי נתונים פיננסיים - RSA Distributed Credential Protection, המערבב ומסדר את הנתונים באופן אקראי. כך, המידע מחולק לשני שרתים שונים, והתוקפים אינם יכולים לפענחו גם אם חדרו לאחד מהם ואפילו לשני הכלי יהיה זמין ללקוחות בסוף השנה.

הטכנולוגיה המדוברת מיועדת להגן על סיסמאות כניסה ופרטי זיהוי סודיים אחרים השמורים בבסיסי נתונים מפני התקפות מקוונות. הכלי החדש, שמתוכנן לעבוד עם כלי הגנת סיסמאות קיימים, מסוגל לצמצם באורח דרמטי את הסבירות להתקפות בזק (Smash-and-Grab) על שרתי סיסמאות באמצעות סידור הנתונים באופן אקראי. מומחי RSA הבחינו שלאחרונה מתרבות יותר דווקא ההתקפות על שרתי הסיסמאות האחוריים (Back-End) שבמרכז הנתונים, במקום התקפה ישירה על השרתים הקדמיים (Front-End) המנהלים את הזהויות של הלקוחות. התקיפות הללו גורמות נזק רב ללקוחות, קמעונאים ופורטלים פיננסיים,

אורגנית והן על ידי רכישות. ישראל היא תמיד מקום מעניין לאתר בו את הדבר הבא בטכנולוגיה בכלל ובאבטחת מידע בפרט.

דרכי התגוננות לאיומי אבטחה במובייל

RSA, חטיבת אבטחת המידע של EMC, פרסמה דו"ח חדש של מועצת החדשנות באבטחת עסקים (SBIC Security for Business Innovation Council) - גוף המורכב מ-19 מנהלי אבטחת מידע בארגונים בינלאומיים. זאת, במסגרת הכנס השנתי 2012 של RSA, שנערך באחרונה בלונדון.

הדו"ח מתייחס לגידול המתמשך במספר המכשירים הניידים בארגונים, ומשתף את הקוראים בתובנות המומחים כיצד יש להתייחס לאיומי האבטחה במכשירים אלה, תוך כדי מיקסום ההזדמנויות העסקיות. על פי הדו"ח, השינויים המתמשכים שאנו חווים בטכנולוגיה ניידת מותירה אחריה חללי אבטחה נרחבים. מספר גדל של מכשירים ניידים פרטיים מקבלים גישה לרשתות ארגוניות ולמידע מאוחסן של חברות עסקיות - תופעה שעלולה לגרום לתוצאות הרסניות, החל מאובדן או דליפה של

קניין רוחני יקר ערך ועד לנזקי מוניטין. בקרב חברי המועצה קיימת הסכמה שהגעה העת שארגונים עסקיים ישלבו את ניהול הסיכונים שלהם בחזון המכשירים הניידים. לטענת המומחים, ניצול ההזדמנויות העסקיות שיוצרים המחשבים הניידים יכול לבוא לידי ביטוי רק אם הארגונים יידעו מהם הסיכונים וכיצד לטפל בהם.

הדו"ח של SBIC מציג חמש אסטרטגיות לבניית תוכניות אבטחה יעילות למכשירים ניידים, בהן הקמת צוותים ייעודיים לניהול האבטחה שיקבעו כללים התנהלות ברורים ויצירת תוכנית פעולה לטווח הקצר. הטכנולוגיות לאבטחת מכשירים ניידים משתנות בקצב מהיר, ולכן במקרים רבים אין אפשרות לבצע השקעות בתוכניות לטווחים ארוכים.

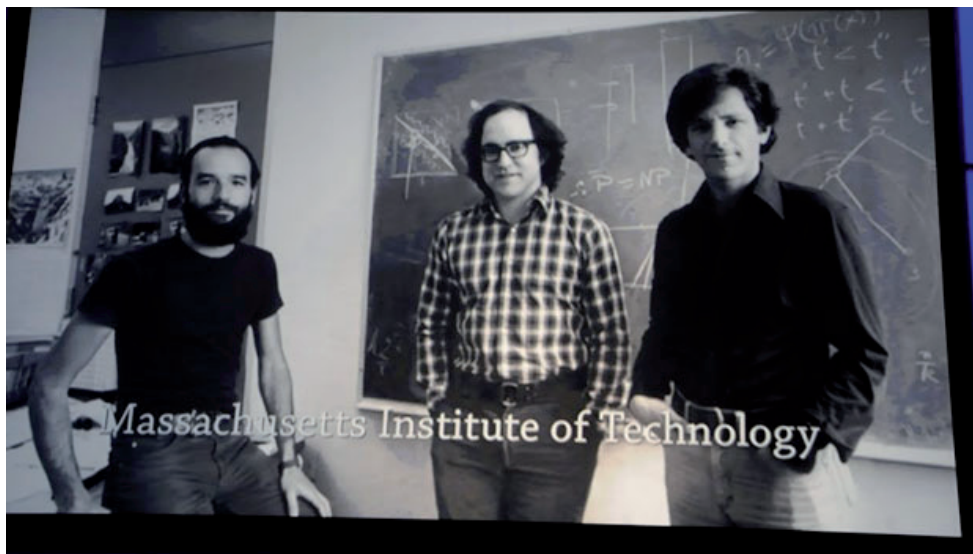
אסטרטגיה נוספת היא בניית

יכולות אבטחה. הידיעה כיצד יש לתכנן אפליקציות למכשירים ניידים שיגנו על המידע בארגונים היא עניין גורלי, אך צוותי אבטחת מידע רבים אינם אחוזים במידת המומחיות הנדרשת.

עוד הוצע בדו"ח שילוב השימוש במכשירים ניידים בחזון ארוך הטווח של הארגון. זאת, מאחר שגופים עסקיים צריכים לעדכן את גישתם אבטחת המידע שלהם, ולכלול בה תהליכי אימות נתונים, חלוקת הרשת למקטעים, בקרים לאבטחת מידע וחיבור מבוסס ענן בין רשתות. אסטרטגיה נוספת שהועלתה בדו"ח היא הרחבת המודעות - על צוותי האבטחה בארגונים להעמיק ולרענן את הבנתם בסביבת הפעולה של המכשירים הניידים.

ארט קובילין, סגן נשיא EMC ויו"ר RSA: "שכיחותם של מכשירים ניידים ואפליקציות המותאמות אליהם מעניקה ערך עסקי משמעותי לארגונים, אבל הסיכונים הם עצומים באותה מידה. הדו"ח החדש של מועצת החדשנות באבטחת עסקים מספק הדרכה אסטרטגית שתעזור לארגונים לא רק לצמצם את הסיכונים מפריצות אבטחה, אלא גם לממש את מלוא היתרונות שמציעים להם המכשירים הניידים".

יצוין, כי הדו"ח התבסס על חוות דעתם של מנהלי אבטחה ראשיים בארגוני ענק בינלאומיים, בהם EMC, נוקיה, פדקס, נורת'רופ גרומן, HSBC, סאפ, אי-ביי, ועוד.



שלושת מייסדי RSA נפגשו בסטודנטים ב-MIT בארה"ב בשנות השבעים. ב-1977 הם פיתחו את אלגוריתם ההצפנה במפתח ציבורי החזק ביותר עד היום, הנושא את ראשי תיבות שמם והמשמש את עולם האבטחה גם בימינו. ב-1982 הקימו את RSA ופרשו ממנה ב-2007. מימין: לאונרד אדלמן, רונלד ריבסט ועדי שמיר

וחשפות מיליוני סיסמאות ופרטי זיהוי לסכנת גניבה. האתרים Zappos eHarmony, ולינקדאין אף חוו זאת על בשרם באחרונה.

באמצעות הטכנולוגיה החדשה, אפילו במקרה שהתוקף מצליח לחדור לאחד משני השרתים המאחסנים את המידע המעורבב והמחולק, הנתונים שיצליח להשיג יהיו כאמור חסרי תועלת. המידע יוכל להתערבל שוב בלחיצת כפתור, כך שגם פריצה נוספת לאחד משני השרתים לא תסייע לתוקף להשיג את מבוקשו. התוקפים יאלצו למעשה לחדור כמעט בו זמנית לשני השרתים או מרכזי המידע, מבלי שייחשפו, על מנת להשיג מידע בעל ערך. כל אחד משני השרתים יכול להימצא במרכז הנתונים או במרכז נתונים אחר, בענן - או צירוף כלשהו שלהם, לפי בחירת הלקוח.

לפי המחקר האחרון של חברת התקשורת האמריקנית ורייזון בנושא פריצות מידע בארגונים, בשנת 2011 היוו השרתים יעד מרכזי לפריצות ב-64% מהמקרים שנחקרו וב-94% מהפגיעות שנרשמו. מדובר בתקריות שעלולות לגרום בעקבותיהן תביעות משפטיות ותיקונים יקרים, נזקים למוניטין, הפרעה לפעולה העסקית השוטפת ושחיקה בבסיס הלקוחות. באמצעות ערבוב וחיתוך נתונים רגישים לשני שרתים שונים, מסייעת הטכנולוגיה החדשה של RSA לנטרל את נקודת החולשה העיקרית של פורטלים רבים.

* **הכותב היה אורח חברת EMC**