

"יש כמה דרכים
 לשמור על הזהות
 של המשתמש, אבל
 צריך לדעת שהזהות
 של המשתמש היא
 השער לכל העולם
 שנמצא מחוץ לרכיב
 שלו. המשתמש נכנס
 לפייסבוק - והזהות שלו
 חשופה לגניבה, הוא
 נכנס לג'י-מייל - ושוב
 הזהות שלו חשופה"

קצת פחות - אבל עדיין, בכל אחת משלוש הדרכים שתיארתי - הזהות שלך פתוחה וחשופה לגניבה. למזלנו, "הבחורים הרעים" עדיין לא הצליחו להתגבר על נושא הזהות ולגנוב אותה בקלות, אבל הם עובדים על זה במרץ, ואני די בטוח שזה יעד די מרכזי אצלם, כי ברגע שהצלחת להתגבר על הגנת הזהות - זהו, הבן אדם וכל מה שיש לו נמצא בידים זדוניות, ומכאן, המרחק עד לגרימת נזק ממשי למשתמש קצר מאוד."

מה לגבי הגנות מתקדמות יותר לעסקים קטנים ובינוניים? האם יש לך המלצות?

"אנחנו מספקים כיום הגנות לארגונים גדולים וגם למשתמשי קצה. ואני יודע שהלקוחות שלנו מאוד מרוצים. אני מסכים איתך שבאמת יש שוק שעדיין לא כיסינו במלואו וזה שוק העסקים הקטנים. אם פירמה של עורכי דין או משרד רואי חשבון מחזיק

רשת אלחוטית, אז הוא למעשה חושף את העסק שלו וכל המידע שיש שם לפני לא מעט האקרים מזדמנים. זה נכון שבכל הראוטרם יש אמצעי הגנה שונים שרובם מצוינים, אבל אני חושב שלא רחוק היום וחברות כמו שלנו יתחילו לספק פתרונות גם לשכבה הזאת. תאר לעצמך שפירמה של עורכי דין, שיש להם 50 מחשבים, ובמקום להתעסק עם תוכנות הגנה לכל עמדה בנפרד - הם יחזיקו תוכנה אחת שתשב ב"שער", כלומר בראוטר - הפתרון הזה יאפשר לכל עובדי ומשתמשי הרשת של הפירמה להיות בטוחים שהם מוגנים - כי ההגנה תתחיל כבר בשער הכניסה והיציאה. זה לא ימנע מהם את הצורך בתוכנות הגנה מקומיות, שישמשו אותם בכל פעם שהם מתחברים לרשתות אחרות, אבל בתוך המשרד עצמו? אין ספק שהם יהיו מוגנים בצורה טובה מאוד. זה עדיין רחוק ולא בר ביצוע כיום, אבל לפי דעתי זה כיוון שלא רחוק היום וחברות אבטחת המידע ייכנסו אליו."

את העבודה שלי ונמאס לי לחכות שעות עד שהמחשב מתחיל לעבוד אחרי שתוכנות ההגנה מסיימות את הבדיקות שלהן - האם אני נוהג בטיפשות?

"בטיפשות אתה לא נוהג, אבל גם לא בחוכמה... אני בהחלט מבין את המגמה החדשה של משתמשי קצה, שאומרים - 'אני לא צריך יותר תוכנת הגנה במחשב שלי'. המגמה הזאת נובעת מהעובדה שיותר ויותר אנשים משתמשים בענן, וכתוצאה משימוש בענן אין להם יותר מידע אישי במחשב שלהם. האנשים שומרים את כל המידע שלהם בפייסבוק, בגוגל אפס או בשירותי ענן אחרים - ואז הם אומרים לעצמם, 'לשם מה אני צריך אנטי וירוס? הרי אין לי כלום על המחשב'. הרי אם תוכנה זדונית נכנסת למחשב של משתמש הקצה - הוא מבצע פורמט ומתחיל להתחלה - מאחר שאת כל המידע האישי שלו הוא שומר בענן - אז אין לו כל בעיה לפרמט את המחשב אפילו כל יום. זו פעולה די פשוטה וכל משתמש יכול ללמוד לבצע אותה בכמה דקות. עד לפני כמה שנים, כל המידע שלנו ישב אצלנו ולכן היה חשש מוצדק לבצע פרמוט, כי היה צריך לגבות את התמונות שלנו, המסמכים וכד' - וכל גיבוי גרר אחריו לפעמים גם שכפול של וידוסים לגיבוי, ולמעשה לא נפטרנו מהצרות... אבל היום? כל זה מאחורינו. משתמש הקצה הרגיל חושב לעצמו שהוא לא צריך יותר להגן על המחשב שלו - אנחנו בטוחים ויודעים שזו בעיה, אנחנו מבינים שמשמשי הקצה לא ערים לכלל המשמעותיות הנגזרות מחשיפת הרכיבים כולם - כי לא מדובר רק על מחשב, אלא גם על טלפון וכד' - לכל מיני תוכנות זדוניות שעוללות לגרום לצרות גם למידע שנמצא בענן. זה אולי נשמע דמיוני, שלב הבא יהיה, שאיזו תוכנה זדונית תשתמש ב"שער" הזה ותיכנס גם לענן משום שאנו חושפים את אמצעי הקצה שלנו לתוכנות זדוניות ללא כל הגנה - ומה יקרה אז?

מה אתה חושב על נושא גניבת זהויות?

"גניבת זהות היא אחד הנושאים החמים שיעסיקו עוד ועוד חברות כמו שלנו. אנחנו מדברים על בעיה מהותית מאוד, כי לכל משתמש יש זהות. הזהות שלו אינה בהכרח נעולה ושמורה על גבי מחשב אישי או טאבלט בלבד - הזהות הזאת נמצאת בכל הרכיבים של המשתמש, כולל טלפון חכם. ברגע שאתה נכנס לחנות אפליקציות דרך הטלפון החכם שלך - זהו, הזהות שלך פתוחה ונתונה לאימים. אנחנו חושבים על כל מיני פתרונות להגנת הזהות, מטבע הדברים אין לי אפשרות להרחיב על זה כרגע, אבל אני יכול לומר שהנושא מאוד מאוד מעסיק אותנו. יש כמה דרכים לשמור על הזהות של המשתמש, אבל צריך לדעת שהזהות של המשתמש היא השער לכל העולם שנמצא מחוץ לרכיב שלו. המשתמש נכנס לפייסבוק - והזהות שלו חשופה לגניבה, הוא נכנס לג'י-מייל - ושוב הזהות שלו חשופה. ברור שכשואו נכנס לבנק שלו - הזהות חשופה

אוניברסיטת בן-גוריון בנגב

ESRL Symposium 2012

8 במאי 2012 | אוניברסיטת בן-גוריון
 אולם הסנאט על שם מינקוף | 16:00-09:30

הכנס אינו בתשלום אך מותנה בהרשמה מראש

לרישום מחר' אירועים טל' 03-7330777 או באתר <http://esrl.events.co.il>

סמנו את התאריך ביומנכם!
ההרשמה החלה

ORACLE