Cyber Security, מציאות ואשליית הביטחון

אבנר מימון, מנהל פיתוח עסקי ומכירות, אורקל ישראל

מחקר חדש של חברת הייעוץ PwC מצא, כי הונאות סייבר מדורגות במקום השני ברשימת הפשעים הפיננסיים. גם בבנק ישראל פרסמו לאחרונה שהם שוקלים להקים מרכז סייבר בנקאי וזו רק ההתחלה. סייבר סקיוריטי זו תופעה ששיגעה את העולם בשנים האחרונות וערערה במעט את תחושת הביטחון הסובייקטיבית של כל אחד מאיתנו. כן, אמרתי ערערה במעט, כי למרות שלל האיומים החדשים והתגברות הפשיעה הקיברנטית רובנו עדיין רגועים, או לפחות מתנהלים ככאלה.

אבנר מימון

בכנס סייבר שנערך לאחרונה, גם אני ניסיתי לזעזע את הקהל. כמו כולם, גם אני ניסיתי לעורר רגשות פחד ואימה, וזאת מכיוון שתחום אבטחת המידע מסתמך לא רק על ידע, אלא גם על תחושות בטן. בעולם הסייבר והביטחון מתקיים tradeoff בלתי פוסק בין תחושת הביטחון האישית שלנו לבין המציאות בשטח. מכיוון שכך, ההחלטות שלנו בענייני ביטחון מתקבלות בד"כ על בסיס תמהיל של תחושות בטן, הבנת המציאות הסובייקטיבית שלנו והערכת סיכונים שמשתנה באופן תמידי ולא על בסיס מידע עובדתי כפי שהיינו מצפים.

חשוב שנבין שבזמן שאנחנו מרגישים בטוחים במשרד, יש מישהו שמתכנן לגנוב הרשאות גישה מהעובדים שלנו ומאיתנו בכדי לחדור למאגרי המידע הרגישים ביותר. ההתקפות האחרונות מלמדות שהתוקפים לא עושים שימוש בטכנולוגיות מיוחדות ומפנים את רוב המשאבים שלהם לכיוון העובדים וגניבת הרשאות הגישה שלהם. למעשה, מחקרים מלמדים כי 76% מפרצות אבטחת המידע נגרמות ברשת כתוצאה מגניבת הרשאות גישה מעובדים. מסיפור גניבת המידע בחברות Target , EBay ורבים אחרים מסתבר שבניגוד לתחזיות האימה של עידן הסייבר, הטכנולוגיה היא לא הבעיה וכך גם לא התחכום של ההתקפות. מחקרים מראים כי רוב המקרים יכלו להמנע או להצטמצם באופן ניכר ע"י הטמעת נהלים ופתרונות: להזדהות חזקה, להצפנה, לניהול משתמשים פריבילגיים, מערכות IDM , ועוד.

בעידן הסייבר, המציאות שבה כל יום מתווספת התקפת סייבר חדשה משתנה בקצב מהיר ומובילה חלק מאתנו למסקנה שפתרונות אבטחת המידע הקיימים לא מספיק טובים ושצריך פתרון אחר, לא סטנדרטי ומיוחד. האמנם? בדו"ח האחרון של Verizon נמצא כי בשנת 2013 הנזק שנגרם לכלכלה העולמית כתוצאה מהונאות של אשראי הגיע ל-11 מיליארד דולר, ועדיין 89% מהחברות הנסקרות לא עברו את הביקורת של PCI!! התקן שפורסם לראשונה ב-2009, במטרה להגן על פרטי כרטיסי האשראי, לא מבוצע כהלכה למרות שניתן ליישמו עם מספר לא רב של פתרונות סטנדרטיים. המלצות הוועדות והרגולציות נועדו למנוע או לפחות למזער את הסיכונים, אך מה קורה בפועל? כולנו הופכים לעורכי דין שמנסים למצוא פרצות בנוסח הרגולציה ובמקום למנף את הרגולציה לחיזוק מערך אבטחת המידע לתועלתנו, אנחנו חושבים איך אפשר לעומד ברגולציה במינימום השקעה!! איננו מעוניינים בהצפנה או במגוון רחב של פתרונות אחרים. אנחנו רוצים להמשיך להרגיש בטוחים ואנחנו רוצים סייבר... אנחנו רוצים משהו חדש ומרגש כי שאר הפתרונות הסטנדרטיים זה כל כך 2008... ובנתיים, בזמן שאנחנו בודקים את הטרנד החדש והמסעיר שנקרא סייבר סקיוריטי, קצב ההונאות והסיפורים על גניבות אשראי רק הולך וגדל כפי שניתן לראות מדוגמאות נוספות מהדו"ח:

> מסתבר שבניגוד לתחזיות האימה של עידן הסייבר הטכנולוגיה היא לא הבעיה , כך גם לא התחכום של ההתקפות . מחקרים מראים כי רוב המקרים יכלו להמנע או להצטמצם באופן ניכר ע"י הטמעת נהלים ופתרונות סטנדרטיים.

- Phishing ו-Pharming זו תופעה שמתגברת ולמרות ש-780,000 מיילים של Phishing מצליחים להונות מישהו כל יום (מתוך 156 מליון מיילים שנשלחים כל יום) לקוחות לא טורחים ליישם פתרון.
- 37% מהונאות האשראי פגעו במוסדות פיננסיים - עובד בלשכת האשראי בקוריאה גנב 40% מרשימת כרטיסי האשראי שהיו שייכים ל 20 מליון קוריאנים - אילו הוטמעה פתרון למניעת גישה ומעקב אחר משתמשים חזקים מקרה זה היה נמנע (נכון גם למקרה Edward Snowden ורבים אחרים...)
- 113 טלפונים נגנבים כל דקה בארה"ב - כמה ארגונים מיישמים פתרון לניהול הרשאות גישה ו-MDM לטלפונים החכמים שלנו?

עד לסיפור הבא.

ORACLE