שוב פעם גנבו את הסיסמאות? אולי הגיע הזמן לגישה אחרת?

ישי ורטהיימר, דירקטור, ייעוץ באבטחת מידע, KPMG סומך חייקין

70 מיליון פרטי משתמשים. כמות הנתונים שנגנבה מבסיס הנתונים של רשת הקמעונאות Target גדולה ביותר מפי עשרה מכמות הרשומות במאגר משרד הפנים שדלף לפני כמה שנים. בכנס אינפוסק האחרון דיברתי על פרשה זו, אולם בעוד אני יושב לספר על האירוע ולנסות ללמוד ממה שקרה שם, מתפרסם שבסיס הנתונים של משתמשי eBay גם הוא דלף, ושם מספר המשתמשים הוא 145 מיליון...

ראשית, שווה להתעכב רגע על המשמעות של דליפת כמות כזו של נתונים. כאשר דלפו כמה אלפים של כרטיסי אשראי במדינת ישראל, והנתונים שלהם פורסמו, געשה הארץ. אולם בסופו של דבר, הונאות אמיתיות כמעט ולא קרו, וגם מידע פרטי של לקוחות (בהקשר של כרטיסי האשראי) לא דלף, כך שהנזק לאותם אזרחים שמספר כרטיס האשראי שלהם דלף היה אי נעימות זמנית וקצרה.

כאשר נגנב מאגר של נתונים בהיקף הדומה למחצית אזרחי ארצות הברית, הגודל עושה הבדל גדול. גם אם חלק קטן מהנתונים מאפשר פגיעה בפרטיות או שיבוש חייהם של אזרחים, עדיין זו יכולה להיות פגיעה עצומה. אם יוודע אילו משתמשים נפגעו, למשל אילו כתובות אימייל מעורבות, יתכן וארגונים נוספים יאלצו להחליף סיסמאות של לקוחותיהם בהתאם, והפרשה תמשיך להתגלגל.

אל תנהלו את סיסמאות הלקוחות - אתם ממש גרועים בזה!

אבל איך זה יתכן? הרי כבר שנים אומרים לנו שהשיטה של זיהוי באמצעות סיסמה אינה יעילה מספיק? וגם אם לא מדובר בגניבת בסיס נתונים ענק, הרי ברור לכולם שהתקפות פישינג וטרויאניים יכולים לגנוב בקלות את סיסמת המשתמש?

אני רוצה לטעון שארגונים לא מסוגלים לנהל באופן אפקטיבי מידע רגיש במיוחד. אפשר לנסח את הטענה באופן בוטה יותר: "לא כדאי לכם להיות אחראיים על זיהוי הלקוחות שלכם - אתם לא טובים בזה!".

אי אפשר לגנוב ממך מידע שאתה לא שומר

כדי להסביר את הטענה, אתחיל בדוגמה פשוטה ונפוצה. כידוע, כבר מזה כמה שנים דורשות חברות כרטיסי האשראי מבתי העסק לפעול על פי תקן אבטחת המידע PCI-DSS. מדובר בתקן בינלאומי שיישומו מורכב ויקר, וכל בתי העסק המבצעים מסחר אלקטרוני מחויבים לעמוד בו באופן מלא.

באופן מעשי, מרבית בתי העסק בישראל בחרו באפשרות הפשוטה והזולה ביותר, והיא - לא לשמור פרטי כרטיסי אשראי בכלל. אתרי מסחר אלקטרוני אלו ביצעו מיקור חוץ (Outsourcing) לנושא שמירת פרטי כרטיסי האשראי באופן מאובטח, ופעולה זו מבוצעת על ידי חברות המתמחות בביצוע עסקאות אשראי מאובטחות. החלופה של יישום התקן בעצמם מורכבת ויקרה הרבה יותר.

מעבר לכדאיות של חלופת מיקור החוץ, נראה שחברות המסחר האלקטרוני מבינות שאין להן עניין להתעסק באבטחת כרטיסי האשראי. חברות אלו מעדיפות להתמקד בליבה העסקית שלהן בנושא שיווק, מכירה, שירות וניהול שרשרת האספקה ולא לבזבז פוקוס על נושאים שאינם הכרחיים.

אם נחזור לסוגיית ניהול סיסמת הלקוח, או במילים אחרות סוגיית האותנטיקציה, גם כאן מדובר בנושא מורכב, שדורש מיקוד משמעותי על מנת לבצעו כהלכה.

עבור ארגונים רבים, ניהול הזהות של הלקוח הינה סוגיה משמעותית. בנקים, למשל, משקיעים מאמץ רב בזיהוי של הלקוחות כחלק מדרישות מניעת הלבנת הון. אולם, כאשר מדובר בתהליכי הזדהות בערוצים שונים, כגון זיהוי הלקוח

ישי ורטהיימר

בעת ביצוע פעולות באינטרנט, באמצעות הטלפון הנייד, בדואר אלקטרוני וכדומה, נדרשים פתרונות חזקים וגמישים, ונראה ששיקולי עלות-תועלת של הבנקים לא מצדיקים תמיד פתרונות מסוג זה.

זיהוי לקוחות באמצעות סיסמה? כבר שנים מספידים את השיטה הזו, וכבר מזמן קיימות חלופות טובות יותר, אולם הבנקים בישראל עדיין ממשיכים להשתמש בסיסמאות לזיהוי לקוחותיהם. אפשר להבין מדוע - גם הבנקים לא מעוניינים להשקיע יותר מידי תשומת לב, זמן וכסף, בפתרונות הזדהות חכמים יותר. הסתמכות על צד שלישי שמספק שירותים ליותר מארגון אחד, עשויה להיות חלופה יעילה יותר ועדיפה כלכלית. הטלפונים החכמים שינו את העולם - אחוז גבוה מאזרחי המדינה מחזיק בידיו מחשב עם מסך, מקלדת וחיבור לרשת. מדובר באמצעי זיהוי חכמים וגמישים. אמצעים אלה מהווים תשתית מצוינת למודלים יעילים של הזדהות, אימות, הצפנה וניהול מידע רגיש. כתוצאה מכך, עלות היישום של מערך מסוג זה הולכת ופוחתת והכדאיות הולכת ועולה.

באינטרנט זה עובד, בדנמרק זה עובד

החל משנת 2010, יכול כל אזרח דני לקבל אמצעי זיהוי המכונה NemID, מדובר באמצעי זיהוי פיסי, המחולל סיסמאות מתחלפות. כל הבנקים בדנמרק, כמו גם ארגונים ממשלתיים וכמה ארגונים פרטיים מסתמכים על אמצעי זה לזיהוי לקוחותיהם.

ניתן לטעון שבאופן זה אנו "שמים הרבה ביצים בסל אחד", אך למעשה ניתן לצמצם סיכון זה באמצעות מודלים שמאפשרים להסתמך על המערכת רק באופן חלקי. אך העניין העיקרי הוא שכאשר ישנה חברה שכל מהותה היא שמירה על אמצעי הזיהוי של לקוחותיה - היא יכולה למלא משימה זו טוב יותר מאחרים.

חברות אינטרנט רבות היום מסתמכות על גוגל ופייסבוק לשם זיהוי המשתמשים שלהם. כנראה שלא נראה בעתיד הקרוב בנק שיאפשר ללקוחותיו להזדהות באמצעות חשבון הפייסבוק שלהם, אולם אולי הגיע הזמן שגם ארגונים רציניים כמו בנקים, חברות ביטוח ותקשורת, יבחנו ברצינות את האפשרות להסתמך על שירותי אותנטיקציה של גורם המתמחה בכך.

המבחן האמיתי, שבא בעקבות אירועי כשל, הנו האם אנחנו לומדים ומשתפרים כתוצאה מכך. אירועי כשל כה משמעותיים, כמו אלו שהעולם חווה בתקופה האחרונה, צריכים ללמדנו שיעורים משמעותיים, לגרום לנו לבחון מחדש את הפרדיגמות שאנחנו מורגלים אליהן, ולפתח גישות טובות יותר להתמודדות עם אתגרים אלו.

שירותי אבטחת המידע של KPMG סומך חייקין מהווים חלק מרשת KPMG העולמית, אשר הינה אחת מפירמות השירותים המקצועיים הגדולות בעולם. שירותי הייעוץ בישראל מקיפים את מכלול נושאי אבטחת המידע, החל מהנושאים האסטרטגיים והארגוניים ועד למגוון הנושאים הטכנולוגיים המעמיקים.

לפרטים נוספים:
ישי ורטהיימר, טל: 03-6848504 , דוא"ל: iwertheimer@kpmg.com

KPMG
cutting through complexity