

לקבל תמונה אמינה של סיכויי אבטחת המידע ושכדאי להתייחס לנושא ברצינות. בנוסף, לפעמים עדיף פשוט לא להחזיק מידע מסוכן, כגון מספרים של כרטיסי אשראי."

"לשנות את הקונספציה על אבטחת מידע"

"יש סיבה טובה לחשוש מאיומי סייבר. הם הולכים ומשתנים, האיומים של היום הם לא האיומים של לפני שנתיים, ועל ארגונים לשנות את הקונספציה בבואם להתמודד איתם", כך אמר **בן כפולר**, מנהל מכירות אזורי לישראל, יוון וקפריסין בפאלו אלטו.

לדבריו, "ההאקרים הרבה יותר מתקדמים ממה שנוטים לחשוב. אלה כבר לא האקרים 'קטנים' אלא ארגונים שמושקעים בהם הרבה מאוד משאבים ומוטיבציה. על ארגונים להפוך את הדף בחשיבה על ההגנה



ישי ורטהיימר

בנקז אלא חברת האשראי, ולכן אין שום סיבה שהם יציאו כסף. כאן צריך להיכנס הרגולטור ולחייב אותם לעשות זאת". לסיכום, אמר ורטהיימר, "המקרה של Target מוכיח כי ההנהלה חייבת

הונאות בחנו את הנתונים ולאחר שאחד מהם הדליף זאת לבלוגר, החברה החלה להגיב, אך זה היה כבר מאוחר מדי".

"האם הפריצה הייתה מתוככמת?", שאל והשיב: "תלוי את מי שואלים. אנשי אבטחת מידע יאמרו שזו פריצה בנאלית, אבל היא הוכיחה שוב שמתקפה ממוקדת מצליחה".

לדבריו, "המסקנה מהמקרה הזה היא שכמו שהבנקים מגנים על הכספומטים שלהם, סוחרים חייבים לאבטח את נקודות הקצה שלהם. אם זה היה קורה, לא הייתה בעיה. זה לא קורה מאחר שמדובר בהוצאה גדולה לאותם סוחרים ומאחר שאם מישהו משלם להם בכרטיס אשראי גנוב - לא הם נושאים

אל תסמכו על הטכנולוגיה

חשוב שתוודאו שהשמירה על האתרים שלכם, הגישה אליהם והשימוש באפליקציות יפוקחו על ידי מוח אנושי שיוודע לנתח מצבים וגם להזהיר מפניהם

מהדוברים טען כי הכלים הקיימים כיום פותחו ותוכננו כדי להלחם את המלחמה של אתמול. מפת האיומים משתנה מדי כמה חודשים ואולי אפילו מהר יותר. שום חברה לא יכולה לעמוד בקצב של הפורצים, שלומדים את הכלים, מהר מאוד מזהים את החולשות שלהם ומפתחים שיטות איך לעקוף אותם.

המסקנה מתובנה זו היא שהגנה על אתרים של ארגונים צריכה להיות שילוב של יישום הכלי הנכון עם המוח האנושי. צריך להשתמש בשיטות מתוככמות שכוללות מעקב, איסוף נתונים ועין פקוחה 24 שעות ביממה על הרעשים שמסביב לרשת. חלק מהחברות שמספקות את השירותים האלה הגדירו את פעילותן כ-"סיירת אבטחה", בדומה לסיירות הפיזיות, שמספקות שמירה היקפית על בתים ומגורים. היכולת לזהות דפוסי התנהגות של משתמשים, ובמיוחד חריגה מהם, שמורה בעיקר למומחים וכאלה שלא ישנים בלילות. הכלים יכולים להיות לעזר, אבל בשורה התחתונה, לא כדאי לסמוך עליהם. אל תתפתו להיענות לעצותיהם של אלה שמעוניינים שתיקנו את המוצרים שלהם. חשוב שתוודאו שהשימוש על האתרים שלכם, הגישה אליהם והשימוש באפליקציות יפוקחו על ידי מוח אנושי. שיוודע לנתח מצבים וגם להזהיר מפניהם. ויפה שעה אחת קודם.

יהודה קונפורט

"אם חשבתם שההאקרים עובדים קשה, אתם טועים", אמר אחד הדוברים. "הם לומדים את דפוסי ההתנהגות של הארגונים, כולל את הטעויות שהם עושים, למשל חוסר הזהירות בשחרור מידע, כגון סיסמאות והרשאות, ובתוך זמן קצר חייהם נעשים קלים והם אף אולי נעשים עשירים".

"לי זה לא יקרה" - הגרסה הארגונית

משתתפי הכנס שמעו ממומחי האבטחה, כי האקסיומה שלפיה "הארגון שלי מוגן" ("לי זה לא יקרה" - הגרסה הארגונית) חלפה מהעולם מזמן. חברות אבטחת המידע הגדולות ביותר מפתחות שיטות וכלים כדי להגן על האתר ועל הארגון רגע אחרי שהפורץ נכנס, כי אין דבר כזה הגנה הרמטית. ח"כ מאיר שטרית אמר, ובצדק, ש-"לא משנה כמה תשקיע באבטחה, מספיק שהפורץ יצליח פעם אחת להפיל לך את הרשת וכל המאמצים שלך ירדנו לטמיון". בהתאם לכך, מרבית הפתרונות שהוזכרו בכנס מאפשרים לזהות מראש משתמשים בעלי כוונות זדון ועוצרים אותם רגע לפני שהם מתחילים לבצע את זממם.

אולם התובנה המעניינת ביותר, שעברה לאורך כל הכנס, היא שאסור לסמוך על כלים וטכנולוגיה. עד כמה שהיא נשמעת מוזרה, אומרים אותה מומחים ולוחמי סייבר ותיקים, בעלי הרבה מאוד חוכמה וניסיון חיים. חלק

כנס InfoSec 2014 של אנשים ומחשבים העלה שתי תובנות מרכזיות: האחת היא שמרבית הארגונים עדיין תקועים בסוף שנות ה-90 ומשקיעים חלק גדול מהמשאבים בהגנה על רשת התקשורת הארגונית, באמצעות פיירוולים, תוכנות אנטי וירוס ועוד דברים שאנחנו מכירים מאז. התובנה השנייה היא שמי שנוהג כך טועה בגדול ומסכן את הנכס היקר הקיים בכל ארגון: המידע.

ההאקרים, הן אלה בעלי הכוונות הפליליות-כלכליות והן אלה בעלי הרקע הפוליטי-אידיאולוגי, מכוונים את מאמציהם לפגוע באתרי האינטרנט של הארגונים. והרי אין כיום ארגון רציני שלא מפעיל אתר. מנהלי האבטחה מודעים למציאות המשתנה אבל עדיין לא ניתן לומר שהם עשו את השינוי המחשבתי, את המהפך הארגוני. כך נוצרו יחסי כוחות לא שווים בין הפורצים, שרובם עובד באופן עצמאי וספק אם יש באמת תיאום ביניהם, למומחי האבטחה מכל הארגונים ומכל הסביבות העסקיות והציבוריות.

הדוברים השונים בכנס השתמשו בכל הטכניקות המוכרות כדי לשכנע את מאות המאזינים, שהגיע הזמן להתקדם, רגע לפני שיהיה מאוחר. קודם כל, צריך להכיר את הבעייתיות לעומק, כולל הקלות הבלתי נסבלת של משתמשים ובעלי תפקידים המתמסרים בקלות רבה לכל האקר מתחיל.