



להגן על מה שחשוב באמת

כאשר מתמודדים מול התקפות הסייבר, במקום להתמקד בתשתיות ובהגנה היקפית - ולהזניח את ההגנה על המידע עצמו - מומלץ להגן ישירות על המידע הארגוני

על המידע הארגוני היא כנראה ההשקעה הטובה ביותר בתחום. רשתות נופלות, שרתים קורסים, פריצות והתקפות סייבר מתרחשות באופן יומיומי - אך אם המידע הארגוני עצמו מאובטח, אין משמעות לכל אלה. על מנת לממש בצורה היעילה והטובה ביותר מדיניות של אבטחת המידע הארגוני, יש לבחון את תרחישי השימוש (Use Cases) הטיפוסיים בארגונים מודרניים, בהקשר של שיתופי מידע החשופים לסיכון של זליגת המידע.

הענן - שירותי האחסון בענן צמחו וצברו פופולריות עצומה בשנים האחרונות. סביר להניח שרוב העובדים בארגון משתמשים בצורה זו או אחרת בשירותים כאלה על מנת לסנכרן קבצים ומידע בין מכשירים שונים שברשותם. לרוב, המכשירים נמצאים במיקומים שונים.

אנשי הנהלה בכירה וחברי דירקטוריון - שכבת בעלי התפקידים הבכירים בארגון חשופה באופן מתמיד למידע הרגיש ביותר, ובאופן אירוני עליהם גם להפיץ ולחשוף מידע זה לגורמים שמחוץ לחברה.

ספקים חיצוניים, שותפים עסקיים ויצרנים אחרים - הארגון המודרני מקיים מערכת אקולוגית שלמה סביבו.

על ידי התבוננות בשלושת התרחישים הללו אפשר להתחיל לגבש אסטרטגיית אבטחה ארגונית.

גיבוש אסטרטגיית אבטחה

יש מגוון מוצרים המכוונים להגנה על המידע הארגוני ישירות תחום אחד הוא של כלי הצפנת קבצים בענן On-Premise. אלה מוצרים המצפינים את הקבצים הארגוניים באופן אוטומטי לפי הגדרות ידועות מראש, ומאפשרים עריכה, קריאה, הדפסה ושליחה של קובץ רק על פי סט הרשאות גרנוולרי המוגדר לפי משתמש. כלים בתחום זה יכולים להיות מוטמעים מרמת הענן ועד לרמת הארגון. תחום שני הוא פתרונות מניעה של זליגת מידע (DLP). כיוון שאי אפשר לקטלג כל קובץ ארגוני לפי הרשאות מסוימות, מומלץ להשתמש בפתרונות DLP על מנת לבדוק קבצים הנמצאים בתנועה ברשת הארגונית.

תחום שלישי הוא חסימת התקנים חיצוניים (USB), המביא לחסימה גורפת של הוצאת קבצים מהארגון באמצעות אמצעי אחסון חיצוניים כגון USB או מדפסות.

תחום רביעי הוא הצפנת תחנות קצה או מדיות נתיקות, הכולל הצפנה של כל תחנת קצה והמידע שעליה, על מנת למנוע נפילת התחנה לידי ידיים עוינות.

אבטחה עדכנית ואופטימלית

תחום ההגנה על המידע הוא תחום המתפתח ומשתפר במהירות דינמית זו היא נדבך מרכזי בשיקולי מנהל האבטחה הארגוני בבואו ליישם את מדיניות אבטחת המידע הארגונית שלו. כיום יש כמה מוצרים בשלים בתחום, המאפשרים לכל ארגון רמת הגנה מצוינת תוך שמירת האיזון העדין בין אבטחת המידע ובין חוויות המשתמש וההמשכיות העסקית. שילוב ואיזון בין הפתרונות השונים הן בהגנה על המידע והן בהגנה על התשתיות - הם שיביאו בשנים הקרובות לצמצום ממדי הנזק שנגרם לארגונים בעקבות ההתקפות הרבות שאיתן הם מתמודדים.

* אמיר שן, מהנדס פריסייל, חטיבת אבטחת מידע, בית תקשורת מחשבים

חד התחומים הטכנולוגיים המתפתחים בקצב ובעוצמה מהירים ביותר הוא תחום אבטחת המידע. חברות אבטחה צצות כפטריות אחרי הגשם, בעיקר בישראל, שגם ראש ממשלתה הכריז באחרונה כי עליה לחתור ולהיות מעצמת סייבר מובילה.

ואולם בחינה קרה ואובייקטיבית של המצב מעלה ספקות באשר לרמתה של אבטחת המידע בשנים האחרונות. בדיקה של מכון המחקר פונמון מעלה, כי 83% מהחברות הבינלאומיות מצהירות כי היו קורבן להתקפת סייבר בשנה האחרונה. ממצא נוסף הוא, כי חלה עלייה של 20.6% במספר התקפות הסייבר בשנת 2013 לעומת 2012. על פי מחקר נוסף של PwC, 92% מהחברות היו קורבן להתקפת סייבר מוצלחת.



למרות ההיצע הבלתי מוגבל של מוצרי אבטחת מידע וההתקדמות בתחום, כיצד ממשיכים ההאקרים להכות ולהצליח במתקפותיהם? התשובה מורכבת ומסובכת, וכאן ינותח היבט אחד מהתשובה, שבזכות התקפות עדיין מצליחות לחדור מבעד לכל שכבות ההגנה. היבט זה הינו ההתמקדות המופחתת של פתרונות ההגנה בשכבה הבסיסית ביותר, שכבת המידע.

הישות הראויה ביותר להגנה בארגון מודרני היא המידע של הארגון. אקסיומה זו חקוקה אפילו בשמו של התחום: "אבטחת מידע". אך המצב בעולם האמיתי שונה, ורוב מומחי האבטחה ומוצרי האבטחה מתמקדים יותר בהגנה על תשתיות הרשת ובהגנה ההיקפית, מאשר בהגנה על המידע עצמו. ייתכן שהסיבה לכך היא שאבטחת המידע עצמו היא תחום מאתגר ומסובך יותר מאשר הגנה על התשתיות, אולם אין ספק שאם אפשר היה לנעול ולאבטח את המידע עצמו, הצורך בהגנה על התשתיות ועל הרשת היקפית היה מצטמצם מאוד.

בפני מנהלי האבטחה יש לא מעט אתגרים בדרך להגן על המידע. משתמשי הרשת אינם מקבלים בקלות הפרעה לקצב ולצורת העבודה שלהם; אנשי-IT בארגון אינם ששים לקבל את תקורת העבודה הנוספת. חשוב להבין, כי למרות כל האתגרים והקשיים, ההשקעה בהגנה