



# העידן החדש של אבטחת המידע

אם בעבר עיקר החשש של ארגונים היה מפני פריצה לשרתים ולמערכות מידע, הרי שכיום יש מציאות חדשה, שלפיה יש צורך להגן של רכיבים, כלים וממשקים שכלל לא נמצאים פיזית בארגון



נרס לאבנ'י

היכולת לאכוף תרבות ארגונית היא קשה, אם כי לא בלתי אפשרית. אפשר להגיד שאנו חיים בוואקום, שבו ארגונים ממשיכים ליישם תפיסת אבטחה שנכונה למלחמה של אתמול, ללא היערכות מספקת למלחמה של היום או המחר. זו המציאות עבור הגנה פנימית למניעת הונאות וגניבות, וגם לגבי היערכות למתקפות סייבר. זהו השלב שבו הנהלות ארגונים, מועצות מנהלים ובעלי מניות חייבים להתעשת ולהטיל על המנהלים הבכירים את האחריות לגיבוש תפיסת ניהול מערך אבטחה חדש. אלו צריכים לעבוד בצמוד למנהל אבטחת המידע והמנמ"ר, ולנסח מחדש את התרבות הארגונית הקשורה במידע, בתקשורת בין עובדים ובכללי הזהירות.

זוהי האסטרטגיה החדשה של עולם אבטחת המידע, שלפיה יש לפעול על מנת שארגונים יהיו ערוכים לאיומים הקיימים, דוגמת מתקפות סייבר. זה לא ייקח יום ואפילו לא חודש, אבל חייבים להתחיל מיד. זאת, על מנת שנהיה מוכנים בזמן וכנדרש למלחמת הסייבר המתקרבת לאזורנו. בסופו של יום, ועדות החקירה או ביקורת הרגולטור לא יקבלו שום תירוץ מאלו שיצטרכו לתת את הדין, כי כפי שנהוג לומר: הכתובת כבר מזמן על הקיר.

הטענה שלפיה אבטחת מידע אינה רק עניין של טכנולוגיה מושמעת כבר מהיום הראשון שבו פרץ התחום לעולם. אולם ההתרחשויות שאירעו בשנים האחרונות בעולם אבטחת המידע יצרו מציאות חדשה בתחום עבור רשתות ארגוניות. איומים שבעבר נחשבו לשוליים תופסים היום מקום מרכזי בסדר היום של כל מנהל אבטחה בארגון. כיום, כאשר מדברים על אבטחת מידע הכוונה היא בעיקר לאיום אחד מרכזי: התקפות סייבר.

עם זאת, גם כאן לא מדובר בחידוש טכנולוגי, שכן ניסיונות תקיפה של רשתות ארגוניות וחדירה למאגרי מידע רגישים היו מאז ומעולם חלק ממפת האיומים שכל מנהל אבטחת מידע התמודד עמם. מה שהשתנה הם האובייקטים שעליהם יש להגן. אם בעבר עיקר החשש היה מפני פריצה לשרתים ולמערכות המידע הארגוניות, הרי שכיום מנהל האבטחה צריך להגן על שורה של רכיבים, כלים וממשקים שכלל לא נמצאים פיזית בארגון - אלא על גופם של העובדים והמנהלים.

בכנס Pulse 2012 שערכה יבמ בלאס וגאס, אמרה **נרס לאבנ'י** - סגנית נשיא ומנהלת תחום ניהול סיכונים, הלימה לרגולציות ואסטרטגיית אבטחה בחטיבת האבטחה של יבמ, כי ריבוי הרשתות ומכשירי הקצה יצרו מספר אסטרטגיות של נקודות תורפה, שמנהלי מערכות המידע צריכים להתמודד איתם. גם כאן לאבנ'י לא חידשה דבר, אבל היא כיוונה את הזרקור לתופעה שהולכת ומתרחבת במרבית הארגונים, ולא בטוח שכרגע יש לה מענה. עם כל כך הרבה רכיבי תקשורת, שרתים וכלים שעומדים לרשותו של כל עובד IT כיום, לא יהיה זה ריאלי לצפות שאכן אפשר יהיה להעמיד "שומר" על כל נקודה ונקודה. הרי גם לפני עידן המובייל לא העמידו חומות אש ליד כל עמדת PC של כל עובד. שיטת ההגנה הייתה מרחבית, בצורת שכבות, והיא נשענה על אלמנטים דומיננטיים של נהלים, כללים, הסברה ותהליכי עבודה. במילים אחרות: תרבות ארגונית.

במציאות ההיא, למנהל אבטחת המידע הייתה שליטה גדולה יותר על העובדים שלו. זאת, מאחר שהם עבדו במתחם אחד או כחלק מקמפוס מוגדר. מלאכת האכיפה הייתה ברורה יותר, ועבירות של אבטחת מידע נחשבו לקשות וחמורות. כעת, כאשר הגבולות הווירטואליים נפרצו והענן הוא תווך התקשורת וגם השרתים שלו,

## מגמות חדשות, שחקנים חדשים

הסקר השנתי של ד"ר ג'ימי שוורצקוף, מנכ"ל STKI, מצביע על מגמת ההצטרפות שמאפיינת את שוק ה-IT ומספק כמה תובנות באשר לשינויים הרבים שצפוי הענף לעבור בעתיד

דרישה. אל מגרש המשחקים הזה יעלו שחקנים חדשים, שייצגו אתגרים שה-IT לא התמודד איתם עד היום. למנמ"ר המסורתי שכולנו מכירים יש כעת קליינטים חדשים, שמכתיבים חוקים חדשים בעולם העסקי, הפועל בעיקר בווב.

מגמת ההצטרפות באה לידי ביטוי בכך שהלקוח מביא את המחשב שלו מהבית, כאשר במקרה הזה המחשב הוא הטלפון החכם או הטאבלט. ארגונים שנתח רציני מהמכירות שלהם מתבצע באמצעות האינטרנט יצטרכו להתיידד עם עולמות חדשים, כמו תשלומים באמצעות הסלולר,

אחת התובנות המרכזיות שעלו מהסקר השנתי של ד"ר **ג'ימי שוורצקוף**, מנכ"ל STKI, היא ש-2012 תהיה שנה שבה תבוא ליד ביטוי מגמה מעניינת: המיחשוב הקלאסי - עם תחומים כמו דואר אלקטרוני ארגוני, דאטה-סנטר, ביסיסי נתונים ועוד - יפנה לאט-לאט את מקומו לטובת טרנדים חדשים ומדוברים, כמו נייודות, CRM, חברתי, המעבר לענן Big Data-I.

כל אלו ישתלבו במגמה רחבה יותר, הקשורה רבות להתנהגות לקוחות ה-IT: מגמת ההצטרפות. זה לא אומר שהתחומים האלו ייעלמו, זה רק אומר שנקבל אותם באותו האופן שאנו מקבלים חשמל, מים ודלק - לפי