Governance. בתחילת שנות ה-2000, לאחר שמצב אבטחת המידע בתשתיות והן במישורים הארגוניים והתהליכיים השתפר והתייצב, החלה תקופת ההשקעה באפליקציות ובקוד. התפתחות זו הייתה אולי המשמעותית ביותר עד כה, מכיוון שרוב פרצות אבטחת המידע בעבר ובהווה קיימות ברובד זה של המחשוב. לאחרונה אנו חווים התקפות רבות שמביאות לנזקים כספיים ו/או הישגים מודיעיניים וצבאיים משמעותיים. מדינות, צבאות, פשע מאורגן והרבה ידע ציבורי לוקחים חלק בצד ההתקפי, בעוד שיש תחושה של סטגנציה מסוימת בתחום הפתרונות החדשים לאבטחת מידע. התפתחות זו מדאיגה מאוד, ולדעתי תלווה אותנו בשנים הקרובות".

כמי שסוקרים קודם כל את השוק המקומי, חשוב לנו לדעת היכן ניצבת ישראל בתחום האבטחה, יחסית למדינות אחרות. אבי וייסמן, מנכ"ל שיא-סקיוריטי, המכללה לאבטחת מידע ולוחמת מידע, סובר כי "בפן המינהלי, ישראל דומה

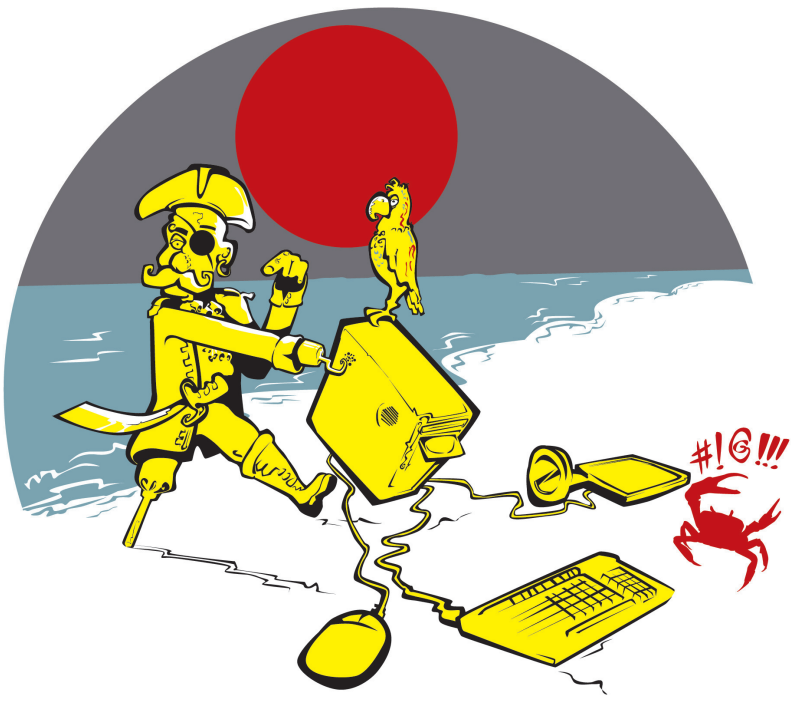
אבי וייסמן

בתרבות הארגונית של המשתמשים למקובל במערב, אך לוקה בהשכלה המקצועית של אנשי ה-IT (שאינם אנשי אבטחת מידע). היא לוקה עוד יותר בתרבות המינהלית והניהולית של אנשי אבטחת המידע עצמם. כל אלה יחדיו מחדדים את הסיכונים לארגונים כאן. בתחום ההתקפי, הרמה כאן כנראה גבוהה בזכות בוגרי היחידות הצה"ליות הייעודיות". גם זילביגר מעריך את מצבנו באופן דומה: "לדעתי, ישראל נמצאת במקום כלשהו באמצע. בשנים הראשונות היה לנו יתרון בכך שהיו פה חברות טכנולוגיה רבות, עם פתרונות אבטחת מידע מתקדמים. בשנים האחרונות כל אלה אינם מספיקים. המישור התהליכי/ארגוני חשוב מאוד בהתמודדות עם בעיות אבטחת מידע. במקומות רבים בעולם, התרבות הארגונית/עסקית מוכוונת לטיפוח נושאים אלה יותר מאשר בישראל. בנוסף, בישראל אין השקעות גדולות מאוד מצד המדינה ביצירת מתודולוגיות וסטנדרטים ואין דרישה פורמלית ממוסדות ממשלה כפי שמקובל במדינות אירופה וצפון אמריקה. כל אלה שמים את ישראל במקום כלשהו אחרי המדינות המתקדמות ביישום אבטחת מידע".

ניסיון לצפות לאן פני הדברים, עד לגיליון החגיגי הבא שכנראה יסכם את העשורים הבאים של עיתוננו וענפנו המקצועי, איננו דבר של מה בכך, בתחום הכל כך דינמי. וייסמן חוזה תמונה לא פשוטה: "במרוצת השנים נוצר פער מובהק, שלפיו לתוקף יתרון מקדמי מובהק, שעל מנת להתגבר עליו המגינים נאלצים להשקיע משאבים רבים בהשוואה לתוקף. הסיבה לכך נעוצה באופי פרוטוקולי התקשורת ומערכות ההפעלה. הן נבנו מלכתחילה לפתיחות ולשיתופיות. בעוד שיצרני מערכות ההפעלה השקיעו משאבים רבים בתיקון לקות זו, והצליחו בכך במידה רבה, הרי שבתחום התקשורת הלקות לא תיפתר בשני העשורים הקרובים, משום שפתרונה מחייב שיתוף פעולה כמעט בלתי אפשרי בין גופי ענק עסקיים, לצד מדינות".

המודעות תלך ותגבר

אדי סער, מי שביצע סקרי סיכונים של מערכות מידע עבור חברות הביטוח במאות ארגונים, צופה קדימה בשמץ של אופטימיות באשר למעגל האבטחה המשיק לביטוח. "אני מאמין כי בסופו של דבר המודעות תלך ותגבר והנהלות הארגונים יבינו שחשוב לבטח את המערכות הממוחשבות מצד הנתונים לא פחות ואף יותר מאשר את מערכות החומרה. אני מניח שיתפתחו פוליסות שיגנו על המבוטח מפני גניבת זהויות, שימוש לרעה בנתונים ונזקים תוצאתיים, שכיום לא תמיד מבוטחים. הבעיה העיקרית בדרך: חברות הביטוח עצמן, שלא בהכרח ערות לזה. הפוליסות מיושנות, לא אטרקטיביות, וחברות הביטוח אינן רואות בינתיים בביטוח הסיכונים החדשים פתח ליוזמה עסקית".

מאור סוגר את המעגל ושב ומחבר את נושא האבטחה לתחום טכנולוגיית המידע: "אבטחת מידע היא מרדף חתול-עכבר. בדרך כלל, הצד המגן נמצא צעד אחד אחורה. האבולוציה של אבטחת המידע תלויה בהתפתחות של עולם המיחשוב. אם עולם ה-IT הולך לכיוון של ענן וניידות, אבטחת המידע תלך גם היא לשם. מימד נוסף הוא הגידול העצום בתלות של האנושות במערכות מידע ומיחשוב. תלות זו מהווה כר פורה להתפתחות הזירה הקיברנטית כשדה קרב לכל דבר. השימוש ביכולות קיברנטיות צפוי לעלות מאוד בשנים הקרובות, המושג של הגנה על העורף צפוי לקבל טוויסט וירטואלי חריף מאוד בשנים הבאות"

שחר מאור: "אבטחת מידע היא מרדף חתול-עכבר. בדרך כלל, הצד המגן נמצא צעד אחד אחורה. האבולוציה של אבטחת המידע תלויה בהתפתחות של עולם המיחשוב. אם עולם ה-IT הולך לכיוון של ענן וניידות, אבטחת המידע תלך גם היא לשם"