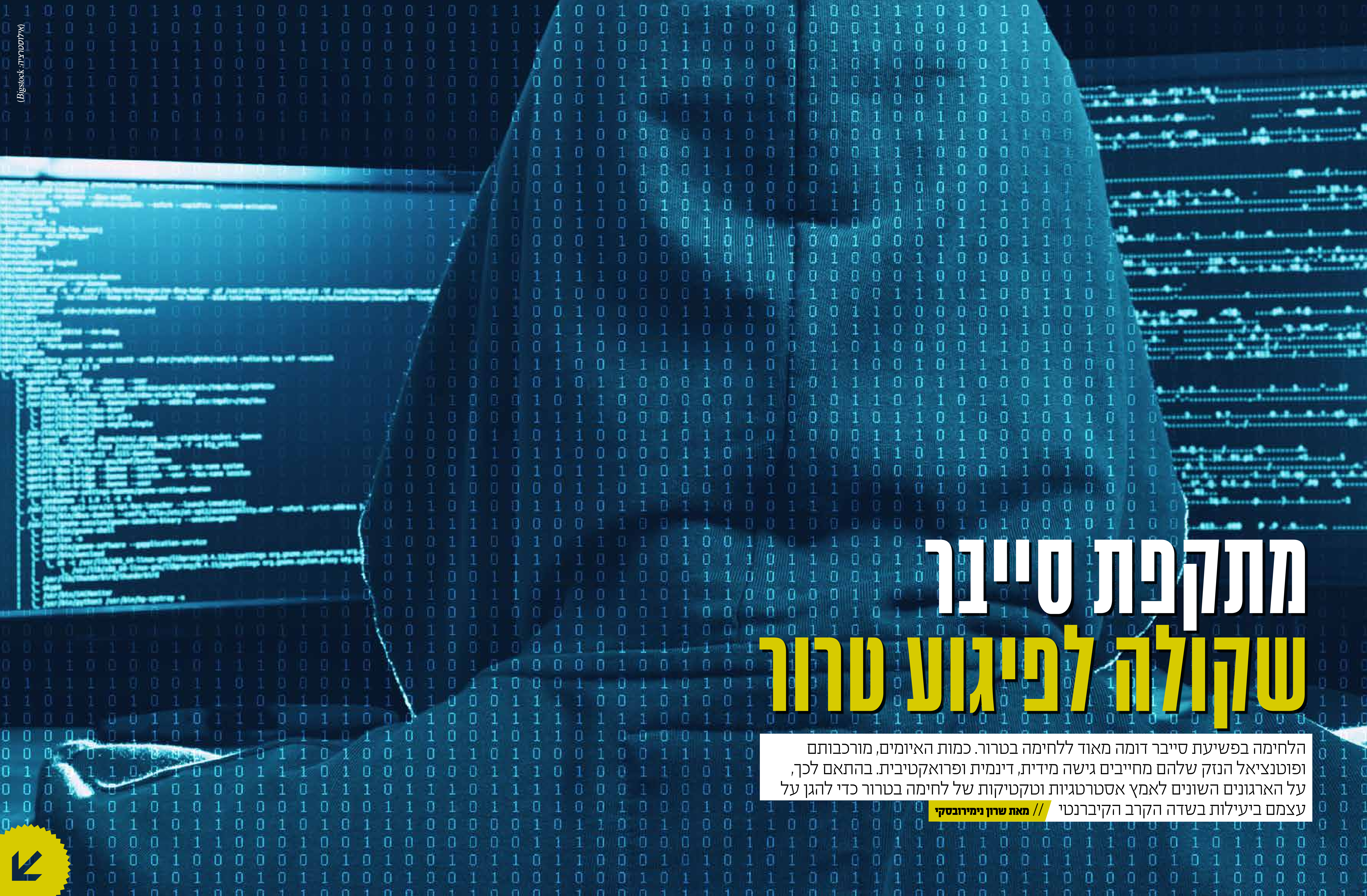

(אילוסטרציה: Bigstock)

מתקפת סייבר שקולה לפיגוע טרור

הלחימה בפשיעת סייבר דומה מאוד ללחימה בטרור. כמות האיומים, מורכבותם ופוטנציאל הנזק שלהם מחייבים גישה מידית, דינמית ופרואקטיבית. בהתאם לכך, על הארגונים השונים לאמץ אסטרטגיות וטקטיקות של לחימה בטרור כדי להגן על עצמם ביעילות בשדה הקרב הקיברנטי

// **מאת שרון נימירובסקי**

(אילוסטרציה: Bigstock)

בשנת 2016, שוויו של ענף פשיעת הסייבר העולמי היה כ-500 מיליארד דולר – מספר מדהים במונחי שווי של שווקים בינלאומיים. לצורך השוואה, שוויו של ענף הסחר בסמים באותה שנה היה סביב 350 מיליון דולר. עם זאת, בעוד שמעורבות בענף הסחר בסמים כרוכה בסיכון משמעותי, ההאקר הממוצע פועל מביתו הפרטי או מבית-קפה, באמצעות המחשב הנישא שלו – מסתור מושלם ברמת סיכון אפסית כמעט.

בימים אלה אנו עדים למספר גדל והולך של מתקפות סייבר המציבות לעצמן כמטרה ארגונים שונים ומתפתחות כל הזמן. כדי להפיק רווחים מפשיעת סייבר אדם אינו חייב להיות האקר. אחת ההגדרות האפשריות לעיסוק הזה, השנוי במחלוקת, היא "פשע כשירות" (Crime as a Service). באמצעות רשת האינטרנט יכול כל אדם לרכוש בקלות רבה "חבילת פשע" – אחדות מן החבילות האלה אפילו מוצעות בחינם לכל דורש – ובאמצעותה להתחיל לתקוף כל מטרה, בלא להבין כיצד החבילה פועלת, ובכך להתחיל להפיק רווחים מידית. לאור זמינותם של היישומים הללו, הקלים לשימוש, בשילוב ההזדמנות להפיק רווחים קלים, אין זה פלא שמדי יום מתרחשות אלפי מתקפות סייבר. ההאקרים יכולים לסחור במידע שהם שואבים מן המטרות שלהם – למעשה בלא להסתכן כלל.

> "הצבא הישראלי מלמד את אנשי אבטחת הסייבר שלו 'לישון עם האויב' – להכיר את האויב, לחשוב כמותו ולפעול כפי שהוא פועל. אסטרטגיה צבאית זו היא הגישה המתאימה ביותר לטיפול בפשיעת סייבר"

ענף האבטחה לטכנולוגיות מידע (IT) ועולם הסייבר בכלל משקיעים אלפי שעות עבודה ומאות אלפי דולרים, מדי שנה, בשדרוג הכלים והידע המשמשים להתגוננות מפני המתקפות הללו, בעיקר במגזר הציבורי ובמגזר העסקי. בישראל, הרשות הלאומית להגנת הסייבר מנטרת גם מתקפות של גורמים פרטיים. עם זאת, הניסיון מלמד שחברות אבטחת מידע מובילות כדוגמת צ'ק פוינט, פאלו אלטו, קספרסקי ואחרות יכולות להגיב לאיומים רק לאחר 48 עד 72 שעות. בעולם הסייבר, זהו פרק זמן ארוך מאוד. הסיבה לכך נובעת מן הקושי לזהות מתקפות סייבר כאשר המודלים של התקיפה משנים את מתכונתם מדי יום. בנוסף לכך, חברות האבטחה נוטות להגיב באופן כוללני ורחב ולא להתמקד בארגון המסוים שנגדו כוונה המתקפה.

לפיכך ברור שפרוטוקולי ההגנה בהם משתמשים רוב הארגונים אינם מספקים תגובה נאותה למתקפות סייבר, במיוחד בעידן של גמישות עסקית ונקודות-מבט רחבות. עקב כך, כמעט כל כלי כופרה (Ransomware) יכול לעקוף בקלות את כל שכבות ההגנה המוכרות. כמות האיומים, מורכבותם ופוטנציאל הנזק שלהם מחייבים את הארגונים המעוניינים להגן על עצמם לאמץ גישת אבטחה מידית, דינמית ופרואקטיבית. אם הארגונים לא יצליחו להגן על עצמם, כל ההשקעות שלהם במשאבים (ציוד וכוח-אדם) תרדנה לטמיון שוב ושוב.

יש לאתר כל איום סייבר בעוד הגורם המאתר נותר מוגן ככל האפשר. בישראל, גופי אבטחת הסייבר הצבאיים רכשו ניסיון רב במהלך השנים, ומתוך הניסיון הזה ניתן לגזור וליישם שיטות פעולה מתאימות. הצבא הישראלי מלמד את אנשי אבטחת הסייבר שלו "לישון עם האויב" – להכיר את האויב, לחשוב כמותו ולפעול כפי שהוא פועל. אסטרטגיה צבאית זו היא הגישה המתאימה ביותר לטיפול בפשיעת סייבר – עלינו להתעלם לחלוטין מן העובדה שאנחנו הצד המתגונן ולהגדיר לעצמנו מהי הנקודה שפגיעה בה תהיה המכאיבה ביותר מבחינתנו, מהן נקודות התורפה שלנו והיכן צפוי להיגרם לנו הנזק החמור ביותר – ולהתמקד בנקודות הללו. אנו חייבים גם לזכור שהשיטות של אתמול אינן רלוונטיות בהכרח גם כיום.

ההכרה ביעילותה של גישה זו חלחלה לעומק רב אף יותר במהלך השנה הנוכחית, יחד עם ההבנה שמלחמת סייבר היא מלחמה כוללת נגד טרור. מדינת ישראל נתפסת כמרכז כלל-עולמי לחדשנות בתחום זה וכיצואנית מובילה של תוכנות אבטחת סייבר להגנה, שנגזרו מיישומים צבאיים. עם זאת, בפועל, ממשלת ישראל אינה מקדמת אסדרה (רגולציה) מספיקה בתחום זה, וחברות מקומיות רבות, שאינן חייבות על פי חוק לעמוד אפילו בקריטריונים מינימליים של אבטחת מידע, מסכנות גורמים רבים בו-זמנית. לאחרונה למדנו שרשות שוק ההון, הביטוח והחסכונות של ישראל אתרה תקלות אבטחת סייבר אצל מספר ישויות מוסדיות – חברות ביטוח, קרנות פנסיה, קופות גמל וקרנות השתלמות – שבהן הציבור משקיע מיליארדי שקלים. הרשות מנהלת כרגע ביקורת מקיפה בענף זה כדי לקבוע כיצד לנהל את סיכוני הסייבר המאיימים עליו. לנו לא נותר אלא לקוות שבמסגרת המרוץ נגד הזמן בעולם הסייבר, התקלות הללו תטופלנה בהתאם לתפיסה הצבאית, וזאת כדי להשיג יתרון – ולו יתרון קטן – בשדה הקרב הקיברנטי. ⦿

שרון נימירובסקי הוא מנכ"ל חברת WhiteHat Security