

המתקפות שאיננו יודעים עליהן גדולה בהרבה מאלו שהתפרסמו, נתון המעיד על חולשת הארגונים וחוזקת התוקפים", כך אמר **אלכס לנשטיין**, מומחה סייבר בינלאומי ומהנדס בכיר בפייראיי (FireEye), המיוצגת בארץ על ידי אינוקום מקבוצת אמן.

בנוסף לעבודתו בפיתוח ומכירה של מוצרים עוסק לנשטיין בחקר תחום האבטחה, ומפרסם מאמרים ומחקרים בעיתונות בארה"ב. במהלך השנים, למרות גילו הצעיר, היה לנשטיין אחראי לגילוי ולעצירת כמה מתקפות קיברנטיות גדולות בארה"ב.

לדבריו, "עולם הסייבר משתנה באופן מהיר והאקרים מנסים השכם והערב למצוא דרכים חדשות לתקוף ארגונים ומדינות. התקפות כמו Rustock מוכיחות, כי גם חברות המיישמות את כל פתרונות האבטחה המסורתיים בקפידה, נפרצות על ידי האקרים שרמת התחכום שלהם עולה בהתמדה".

רוב המדינות, אמר לנשטיין, "מגדירות קבוצה של ארגונים ואתרים קריטיים עליהם משקיעים משאבים כדי שלא ייפוצו. כמו בכל מלחמה, גם במלחמת סייבר, מטרת האויב היא לשבש את תשתיות המדינה

הנתקפת. השאלה היא האם מדינת ישראל עשתה כל שביכולתה כדי להגן על אתרי תשתיות קריטיות כגון תשתיות מים, חשמל, תקשורת, בנקאות ועוד. ממה שידוע לי, הממשלה שלכם אכן עושה זאת, אך חשוב לקבוע תאריך יעד בו כלל התשתיות הקריטיות תהיינה מוגנות. מוטב שזה ייעשה מהר ככל היותר, עם הכלים הטובים ביותר הקיימים בשוק".

"כל ארגון במגזר העסקי-פרטי", אמר, "חייב לבדוק האם הוא מועד לתקיפה ואם כן, לנקוט בכל האמצעים להגן על עצמו. מתקיפים טיפוסיים עלולים להיות מתחרים אשר מחפשים מידע עסקי ותוכניות עבודה, או פורצים לאתרים על מנת לסחוט כסף מהבעלים". לארגונים ישראלים, ציין, "יש בעיה נוספת, כיוון שהם עלולים להיות מותקפים מסיבה פוליטית ולא עסקית, כפי שאנו רואים בשבועות האחרונים. כיום בארה"ב, החוק מחייב חברות אשר מידע נגנב מהן, ליידיע את הציבור בכך. זה כמוביל לבעיה תדמיתית קשה, בעיקר אם מדובר בחברות מהמגזר הפיננסי. לכן, על החברות לנקוט בכל דרך אפשרית כדי להימנע מפריצה ואם קרתה - לגלות אותה מהר ככל הניתן".

"במציאות", אמר לנשטיין, "אנו יודעים רק על התקפות שפורסמו

הסייבר כנייר לקמוס

הסייבר הפך לנייר הלקמוס של כל מה שאנו מכירים בתחום אבטחת המידע - הוא משקף את כל מה שעשינו, ובעיקר כל מה שעוד לא עשינו ♦ העובדה שהאקרים הצליחו לשתק אתרים, חשפה מציאות שהיתה ידועה אמנם לרבים, אבל איש לא טרח לשנות אותה; זו מציאות שבה אנו מבינים שאבטחה זה חשוב מאוד, אבל רק אם מדובר בממשלה, בצבא ובמוסדות הציבור ♦ אם לא נראה במטה הסייבר הלאומי כגוף שתפקידו לסייע לכל אחד מאיתנו במגזר הפרטי-עסקי, אלף מטות ומומחי צבא לא יוכלו לסייע לנו

התקנת מערכת הגנה אחת או חסמת פריצה אחרת - קח בחשבון שהידיב שלך ימצא בתוך זמן קצר פתרון חלופי. עליך להתקדם הלאה ולמצוא את המענה לאיום הבא.

הבעיה המרכזית בהיערכות לעידן הסייבר, היא העדר גוף ממשלתי-רגולטורי שייפקח ויתאם. המסר החשוב הזה בא לידי ביטוי

בדבריו של המרצה הראשי, ד"ר **אביתר מתניה** - ראש מטה הסייבר שהוקם לא מכבר במשרד ראש הממשלה. ד"ר מתניה, שטרם נחשף בציבור במסגרת תפקידו הנוכחי, מנה את תפקידי המטה אחד לאחד, כאשר החוט שמקשר בין כל התפקידים הוא תיאום, בקרה, שליטה ואיגום משאבים. הממשלה יכולה לחוקק חוקים, לפרסם תקנות ולקבוע עונשים או תמריצים שיובילו ארגונים להשקיע יותר באבטחה, אולם התיאום תלוי בנו - האזרחים.

אם אנחנו לא נראה במטה הסייבר כגוף שתפקידו לסייע לכל אחד מאיתנו, אלף מטות ומומחי צבא לא יוכלו לסייע. כמו שבהתקפות טרור פיסייות, על האזרחים לעשות הכל כדי להגן על עצמם - כך גם בעולם הסייבר. אתגר נוסף הוא כמובן התיאום בין כל הרשויות וגופי האבטחה שכבר קיימים היום. אם תשאלו את ד"ר מתניה, יהיה לו קשה לומר איזו משימה קשה יותר...

אולי הוא פלשתיני? האם מדובר בכלל בהאק אחד, או באוסף של אנשים שהקשר היחיד ביניהם הוא הסלוגן שאימצו? אלו הן מסוג השאלות שאיש לא יודע את התשובה עליהן. אם תשאלו את הדרגים המקצועיים, התשובה ממש לא מעניינת.

העובדה שהאקרים הצליחו לשתק אתרים, חשפה מציאות שהיתה ידועה אמנם לרבים, אבל איש לא טרח לשנות אותה. זו מציאות שבה אנו מבינים שאבטחה זה חשוב מאוד, אבל רק אם מדובר בממשלה, בצבא ובמוסדות הציבור. ישראל אמנם מובילה בעולם בתחום האבטחה והביטחון, אבל כשזה מגיע למישור האזרחי - הפרטי והעסקי, אנו שמים את האבטחה על אש קטנה. נכון, יש חומות אש וכלים למניעת חדירה, אבל לא הרבה מעבר לזה.

אבי וייסמן - מנכ"ל שיא סקויריטי, שהנחה את CyberSec 2012, אמר ובצדק כי לאזרח הקטן אין את היכולת לעשות הרבה במלחמת סייבר. זה תפקידה של הממשלה. ואכן, בשם הצורך הזה, קם מטה הסייבר במשרד ראש הממשלה. אבל זה לא מדויק, כי האזרח הקטן יכול לעשות. הוא יכול, למשל, להגן טוב יותר על המערכות שלו. רוב האזרחים לא יודעים בכלל עד כמה המערכות שלהם לא מוגנות, ובכך שוברים את אחד הכללים החשובים ביותר באבטחה: לא להירדם בשמירה. אם

מאות המשתתפים שנהרו למרכז הכנסים אווניו כדי לקחת חלק בכנס CyberSec 2012, באו כדי לשמוע על האיום האיראני, שתופס כותרות יומיות בשנתיים האחרונות. עם זאת, רוב ממשלתי הכנס ידעו היטב שאיראן היא רק התידוף ושהנושא האמיתי אבטחת הסייבר. כך, המסר המרכזי באירוע היה, שהסייבר הפך לנייר הלקמוס של כל מה שאנו מכירים בתחום אבטחת המידע - המציאות, האיומים ובעיקר אמצעי ההגנה. הוא משקף את כל מה שעשינו בתחום הסייבר, ובעיקר כל מה שעוד לא עשינו.

מאז שהחלו לדבר על האיום האיראני במובן של פעילות מנע יזומה, הוזכרה העובדה שהמחיר על תקיפה שכזו עלול להיות, בין היתר, מתקפה קיברנטית על אתרים רגישים, כדי לשבש את חיי העורף. את הקדימונים למה שעלול לקרות קיבלנו בחודשים האחרונים, בדמות פרסום נתוני האשראי והפריצות החוזרות ונשנות לאתרי אינטרנט ישראלים - חלקם מהבולטים ביותר בנוף המקוון.

בוקי כרמלי ממשרד הביטחון, שהשתתף בכנס היום, אמר כי מדינות לעולם לא מבצעות תקיפות סייבר נגד מדינות אחרות. הוא התכוון לכך שאף מדינה לא תרצה להיות מזוהה עם תקיפה שכזו, כי בכך היא תאבד את התכלית העיקרית של הפעולה: אנונימיות. האם ההאקר הסעודי הוא איראני בתחפושת?

בוקי כרמלי ממשרד הביטחון, שהשתתף בכנס היום, אמר כי מדינות לעולם לא מבצעות תקיפות סייבר נגד מדינות אחרות. הוא התכוון לכך שאף מדינה לא תרצה להיות מזוהה עם תקיפה שכזו, כי בכך היא תאבד את התכלית העיקרית של הפעולה: אנונימיות. האם ההאקר הסעודי הוא איראני בתחפושת?

יהודה קונפורטס