

בשנה זו, אחרי ההכרזות הגדולות של 1997 נראה היה שצריך קצת לנוח, אבל חברת קומפקט הדהימה את העולם כשהודיעה על רכישת הענקית דיגיטל בחודש ינואר 1998 ובכך נסתם הגולל על אחת ממערכות ההפעלה הטובות בעולם שנהגו על ידי קן אולסן, ה-VM. באביב 1998 הכריזו ביפן על נגן ה-MP הראשון בעולם, מה שסימן את סופו של



שמו של נגן ה-CD שכל אדם החזיק בידו בעת ריצה או הליכה בפארק. אבל היו עוד מהפכים וסיומים בשנת 1998, למשל זו השנה שבה ה-IE של מיקרוסופט עקף את נטסקייפ, ומאז, ה-IE "לא רואה אף אחד במראה", כמו שאומרים באיטליה. בשנה זו נוסד גם שירות קטן וחביב שאפשר רכישה בכסף קטן דרך האינטרנט ללא צורך בתשלום מזומן - הפיי-פאל היה רק בחיתוליו, ורוב האנשים לא הבינו מי בכלל ירצה אי פעם לרכוש משהו באינטרנט לבד מספרים באמזון...

והיה עוד שירות שאף אחד לא האמין שהוא יתפוס - בראשית 1998 הופיע הבלוג הראשון, האפשרות להתבטא ולכתוב מה שבא לכם - בהתחלה זה נראה שעשועו וסתם, ואף אחד לא האמין שזה יהפוך לסופה ענקית של מיליוני בלוגים שנכתבים כל יום, כל רגע.

אצלו הצליחו שני ישראלים לעשות את "זה", והם מכרו את החברות שהקימו לחברות אמריקניות. בועז איתן, שהקים את סייפן ב-1998 ומייסי ממק, ישראל מזין ואלי משיה, שמכרו את החברה לפלטינום, לימים חלק מ-CA, ביותר מ-400 מיליון דולרים.

כיצד להתמודד עם התקפות סייבר חדשות (ישנות - בתלבושת חדשה)

האם זה נכון? אז זהו, שלא. אין זה תחום חדש, וההתקפות לא מתחילות ולא נגמרות באינטרנט. לדוגמה, בשנת 1999 הסעירו שלושת האחים באדיר מכפר קאסם את המדינה. האחים, שלושתם עיוורים מלידה, פוצו על המום שלהם בשמיעה חדה במיוחד. הם פיתחו יכולת לזהות את צלילי החיוג הדיגיטליים (DTMF) של המרכזיות וכך למצוא סממאות שעזרו להם לפרוץ למרכזיות שונות ולמערכות של תאים קוליים. בין המרכזיות שנפרצו היו המרכזיות של חברות פלאפון, קומברס, גלי-צה"ל ועוד.

אז לא קראו לזה התקפת סייבר (השם המקובל לתקיפה מסוג זה הוא Freaking) אבל אם חושבים על כך, האם פגיעה בתשתית המיחשוב של מרכזיות טלפונים לא יכולה לגרום נזק משמעותי? למשל, פגיעה במוקד שירות של חברת טלפונים, בנק, משטרה, שירותי חילוץ וכדומה? לסיכום, דרכי ניתוח וחשיבה ישנים וטובים המקובלים על מומחי אבטחת מידע ומנהלי סיכונים, כמו גם חשיבה "מחוז לקופסה", הלוקחת בחשבון את מרחב האפשרויות, מהווים ערכת כלים חשובה וחיונית להתמודדות עם האיומים הישנים והחדשים העומדים בפנינו ומכונים "התקפות סייבר".

* גלעד ירון, שותף, סמנכ"ל שירותים מקצועיים, SECOZ

מוכרים? נכון, כבר שמעתם אותם פעם. הלא אלה שלושת האיומים המאפיינים את תחום אבטחת המידע הישן והטוב המכונים כשם סוכנות הביון האמריקאית CIA (Confidentiality, Integrity, Availability).

כדי להיערך כראוי להתקפת סייבר יש לנתח את הסיכונים הנובעים ממנה בשלושה צירים:

- מה עלול לקרות - מי עלול לתקוף אותנו? מאיפה? איזו חולשה הוא עשוי לנצל? מה יהיה הנזק שייגרם לטכנולוגיה כתוצאה מהתקפה זו?
- מה הסבירות שזה יקרה - ניתן לחלק את השאלה לשני חלקים: מה הסבירות שהתקפה מסוימת שניתחנו בשלב קודם תקרה, ללא התחשבות במערכות והבקורות שהארגון מיישם (זה נקרא סיכון מובנה), ומה הסבירות שהתקפה תצליח לאחר שתיחסם באמצעים שיישם הארגון (לכך קוראים סיכון שירוי).
- מה הנזק שעשוי להיגרם לארגון/למדינה/לפרט אם תצליח ההתקפה, או במילים אחרות, אז מה? האם שאלות אלה נשמעות לכם מוכרות? נכון, כבר שמעתם אותן פעם. הלא אלה שלוש השאלות ששואלים במסגרת ניהול סיכונים. התקפות סייבר הן נושא חדש, הממוקד בהתקפת שירותים המוצעים ללקוחות דרך תשתית האינטרנט.

ל עיתון מקומי המכבד את עצמו פרסם בשבועות האחרונים ים של מילים על חזית המלחמה החדשה שנפתחה לה פתאום. גם גברת לוי מחדרה יודעת היום לאיית סייבר בלי להתבלבל. האם לאור זאת ברור למה אנחנו מתכוונים כשאנו אומרים "התקפת סייבר", ומה עושים עם זה? האם נדרשת תורה חדשה להתמודדות עם התקפות אלה, או אולי מדובר על גברת ישנה באדרת חדשה?

נתחיל בהגדרה. התקפת סייבר היא פעולה זדונית, מבוססת מחשב, שמטרתה לחשוף, לשנות, להפריע או להשמיד מידע המאוחסן על מערכת מחשב. התקפת סייבר מכוונת אל מטרה ממוקדת, קיים גורם המכוון אותה ועוצמת הפגיעה שלה היא משמעותית. התקפות סייבר ממוקדות במידע. התקפות אלה עלולות לגרום למידע שלושה סוגים של פגיעות:

- פגיעה בזמינות המידע - הפרעה לתפקוד השוטף של תשתיות המיחשוב ברמה האישית, העסקית והציבורית. כך ניתן לפגוע בזמינות שירותים פרטיים, כמו חברות מסחריות, וכן בשירותים קריטיים, כגון המערכת הפיננסית, אספקת המים, החשמל, הטלפונים וכדומה.
 - פגיעה בסודיות המידע - ניצול מידע רגיש, פרטי או מסווג. לגניבת מידע עלולה להיות השפעה משמעותית ברמת הפרט (למשל גניבת כרטיסי אשראי ומידע פרטי), ברמת ארגונים עסקיים (למשל, גניבת סודות מסחריים) וברמה הלאומית (כמו גניבת מידע ביטחוני חסוי).
 - פגיעה בשלמות המידע - שינוי מכוון במידע הנובע ממטרות פוליטיות, כלכליות או סתם "בשביל הכיף". דוגמאות לכך - שינוי נתונים עסקיים כחלק מהונאה, שינוי מידע רפואי העלול לפגוע בחולה, פגיעה במידע ביטחוני או לאומי ועוד.
- האם מאפיינים אלה נשמעים לכם

SECOZ היא חברת ייעוץ, המתמחה בניהול סיכונים בשילוב עם טכנולוגיות מידע. בתשע שנות קיומה עוסקת החברה בשילוב נושאים אלה: אבטחת מידע, המשכיות עסקית, ניהול סיכוני IT, ניתוח דרישות רגולטוריות וניהול יעיל של מערכות מידע. החברה מובילה פרויקטים טכנולוגיים/תהליכיים מורכבים, שבמוקדם התווך בין העולם העסקי בארגון ובין השכבה הטכנולוגית. החברה יועצת לארגונים גדולים בארץ ובעולם בתחומי הבנקאות, הביטוח, התקשורת, גופים מוסדיים ועוד. החברה מנוהלת על ידי אופיר זילביגר וגלעד ירון, מעסיקה כ-20 עובדים ופועלת מהעיר מודיעין. שיתוף פעולה בין החברה ואנשים ומחשבים הוביל להקמתו של כנס אבטחת המידע המוביל בישראל - InfoSec. הכנס מתקיים מדי שנה כבר יותר מעשור.