ההאקר המקצוען

מאת רב פקד מאיר זוהר
ראש צוות חקירת עבירות מחשב ביחידה הארצית לחקירות הונאה

[הכתבה נלקחה מבטאון משטרת ישראל 6\98]

מבוא

בחוק המחשבים התשנ"ה, 1995, הגדיר המחוקק "מחשב" כמכשיר הפועל באמצעות תוכנה לביצוע עיבוד אריתמטי או לוגי של נתונים וציודו ההיקפי, לרבות מערכת מחשבים, אך למעט מחשב עזר. ניתן, לפיכך, להגדיר עבירת מחשב כאשר המחשב משמש כמטרת העבירה, וכאשר המחשב משמש לביצוע העבירה. בקטיגוריה של המחשב למטרת עבירה, הכוונה היא, לחדירות ולפריצות מבחוץ אל תוך חומר המחשב. הפריצה למחשב יכולה להתבצע מתוך רצון לעשות רווח וכחדירה סתמית.

עשיית רווח

גניבה של מידע עסקי ואינטלקטואלי (ריגול תעשייתי, רשימת לקוחות, מחקרים ופטנטים) - המשטרה חקרה חדירה למחשב וגניבה של רשימות לקוחות של" קאונטרי קלאב" באזור המרכז, ומכירתן למועדוני ספורט מתחרים. שינוי, תיקון והוספת מידע לצרכי רווח - המשטרה חקרה תלונה בחשד של פריצה למחשב משרד הרישוי, לצורך הוצאת רשיונות נהיגה במרמה - בעתונות פורסם בהרחבה, כי נערים חודרים לחומר המחשב במשרד הרישוי, ויוצרים לעצמם רשיונות פיקטיביים. גניבת כסף- באוגוסט 94 פרץ מומחה מחשבים מרוסיה למחשב ה CITIBANK -בניו יורק, וביחד עם כנופיה רוסית, העביר כעשרה מיליון דולר לחשבונות בנק בארצות שונות. לישראל הועברו כמיליון דולרים לחמישה בנקים שונים. המשטרה בשתוף ה FBI-תפסה אחד מחברי הכנופייה, כאשר ניסה למשוך את הכספים, והסגירה אותו לארה"ב.

חדירה סתם

חדירה למחשב לצורך לימוד המערכת, מתוך סקרנות, אתגר מקצועי וסיפוק האגו. לאחרונה, התפרסמה בכלי התקשורת החקירה המתנהלת כנגד הפורץ הישראלי המכונה ANALYZER- בחשד לפריצה למחשבי הפנטגון. בראיון באינטרנט טען, כי הוא פרץ למחשבי מוסדות שונים וביניהם למחשב הכנסת, כדי לחשוף את חולשות האבטחה באותם מחשבים, וכדי "לסתום פרצות" באבטחה.

שימוש פלילי אחר

גרימת נזק לקבצים -

המשטרה חקרה פרשה של מתכנת, שנאשם בחדירה אל מערכת המחשב של הטכניון ואל מוסדות אחרים, שגרמה נזק במחיקת קבצי מערכת, ושיתוק מערכת המחשב.

הפלת מערכות המחשב-

לפעמים, כשנעצר "האקר" מפורסם, מאיימים חבריו להפיל מערכות מחשב רגישות, עד אשר לא ישוחרר ממעצרו.

החדרת וירוסים-

המשטרה חקרה חשד כי אחת מחברות ANTIVIRUS ייצרה וירוסים והפיצה אותם, כדי לקדם מכירותיה.

שימוש במידע לצורך סחיטה-

המשטרה חקרה חדירה למחשב מעבדה, המכיל תוצאות בדיקות רפואיות וביניהן תוצאות בדיקת איידס.

מניעת גישה למידע -

המשטרה חקרה עובד בחברת היי-טק בחשד, כי בטרם פיטוריו על ידי החברה, הצפין את הקבצים החייוניים להמשך פיתוח מוצר היי-טק, עד אשר יתקבלו דרישותיו הכספיות.

דרך הפעולה

ברוב המקרים, החודר מגדיר עצמו כמנהל המערכת SUPERUSER) או (ROOT ומסוגל, למעשה, לחדור לכל קובץ במחשב, ולעשות במחשב כבתוך שלו. החודר המקצוען יכול להעלים את עקבות חדירתו, על ידי מחיקת קבצים מסויימים וכל סימן לפעילותו הבלתי חוקית, כך שפעילותו אינה ידועה למנהלי הרשת. החודר יכול, למשל, לגרום לקריסת המערכת ולמחיקת קבצי המחשב החיוניים ביחד עם קבצי היומן, שעלולים להסגירו. לעתים, גם לאחר שנודע על חדירה לא חוקית למערכת המחשב, מסרב הקורבן להתלונן במשטרה, אם משום חשש לפגיעה ביוקרה, ואם משום החשש, כי פנייתו לא תיענה ביעילות, בחשאיות ובמקצועיות הדרושה. לעתים, מגיע החודר ליעדו הסופי לאחר שעבר במספר מחשבים ברחבי תבל, כך שקיים הצורך להתחקות על עקבותיו במספר מחשבים. הדבר מצריך שיתוף פעולה של מספר מנהלי מערכות מחשב, משטרות וגופי חקירה בעולם (המשטרה קיבלה, למשל, בקשת סיוע מחיל האוויר האמריקאי לאיתור אלמוני, שחדר למחשביו בבסיס באחד האיים, דרך ספק שירות אינטרנט ישראלי, ואף העבירה שם של חשוד במעשה). "ההאקר המקצוען" יכול גם לזייף את מספר ה IP שלו, והוא יכול להתחזות כמשתמש חוקי, שאותו המערכת מכירה, ויכול גם להיכנס תחת מספר IP שאין אפשרות להתחקות אחריו IP SPOOFING -) שיטת תקיפה ופריצה למערכות שבה מזייף הפורץ את כתובת חבילות המידע הנשלחות ממחשב למחשב ברשת האינטרנט). "ההאקר המקצוען" לא ישתמש לעולם בחשבון אינטרנט חוקי, אלא בחשבונות פרוצים של משתמשים תמימים. אותו "האקר" יכול גם לחדור למרכזיות טלפונים (PBX) לזייף ו\או לשכפל מספרי טלפון סלולאריים, לגנוב ולזייף שירותי טלפוניה (PHREAKING) ובכך לקבל שירותי תקשורת חינם, ולמנוע את אפשרות זיהיו באמצעות הטלפוניה. קיים חשש ש"ההאקר המקצוען" יצפין את המידע שבמחשבו, כדי למנוע שיחזור פעולותיו. במידה שיגיע לחקירה משטרתית - ישמור על זכות השתיקה. קיימים באינטרנט מאות אתרים, שבהם ניתן לקבל הסבר מקצועי, תוכנות וכלי- פריצה, המאפשרים כמעט לכל אחד לפרוץ למחשבים. קיים חשש, כי לא רק "האקרים" מקצועיים יפרצו למחשבים, אלא גם נערים תמימים, שיעשו זאת מתוך סקרנות ואתגר אינטלקטואלי. עם זאת, קיים חשש, כי גורמים עבריינים (המתחילים להבין את הפוטנציאל הגלום ביכולת המיחשוב) ינצלו צעירים אלה וירתמו את יכולתם הטכנולוגית לביצוע מעשי פשע. ראוי להדגיש (ובמיוחד לאור האווירה הסלחנית המאפיינת את הטיפול בעבירות מחשב) כי הן המחוקק (כפי שהדבר בא לידי ביטוי בחוק המחשבים) והן המשטרה, רואים בחומרה את התופעה של עבירות המחשב בכלל ואת תופעת החדירות למחשבים בפרט. סעיף 4 לחוק המחשבים קובע עונש מירבי של שלוש שנות מאסר על חדירה לחומר מחשב שלא כדין. סעיף 5 לאותו חוק קובע עונש מירבי של חמש שנות מאסר לחדירה למחשב לצורך ביצוע עבירה אחרת. מבחינת המשטרה אין הבחנה אם הפריצה למחשב בוצעה ממניעים אידאליסטיים, ממניעי אגו או מתוך רצון לעשיית רווח אישי. החקירה תיערך באותה נחישות, שכן הנסיון מלמד, שפורץ החודר מביתו הבטוח (בדרך כלל בזהות שאולה) למחשב המרוחק מזירת העבירה, עושה בו כבתוך שלו ומפיץ את המידע על חולשת המערכת לאחרים, עלול בקלות להתפתות ולבצע עבירה אחרת.