גליון מס' 178

ההאקר

סגן-ניצב מאיר זוהר ר' מפלג עבירות מחשב, יאח"ה

כיום, ניתן למצוא תוכנות פריצה כמעט בכל אתרי ה"האקרים" ברשת האינטרנט רשת זו מספקת לפורצים גישה נוחה למערכות מחשב, ומאפשרת להם להחליף מידע על כלי-פריצה ועל חורי אבטחה ה"האקרים" המקצועיים מפתחים את כלי-הפריצה בעצמם ומשכללים אותם לפי כלים אלה יכול מפלג עבירות מחשב ביאח"ה להעריך את יכולתו המקצועית של העבריין, ולקבוע, האם מדובר ב"האקר" חובב או ב"האקר" מקצוען תהליך הפריצה למחשבים כולל שלושה שלבים - סריקה, פריצה ופעילות עוינת המחוקק רואה בחומרה את התופעה של עבירות מחשב בכלל, ואת תופעת החדירות למחשבים בפרט, וקבע (ס' 4 לחוק המחשבים) עונש מירבי של שלוש עד חמש שנות מאסר בגין חדירה למחשב

תהליך הפריצה למחשבים משתנה בהתאם ליכולתו המקצועית של הפורץ, לכלים שבהם הוא משתמש ולמערכת המחשבים והאבטחה נשוא הפריצה. תהליך הפריצה נערך בשלושה שלבים עיקריים - סריקה, פריצה ופעילות עוינת.

סריקה- הפורץ סורק את מערכת המחשבים, במטרה למצוא חור אבטחה, שדרכו הוא יכול לחדור למערכת המחשב. הפורץ מפעיל תוכנות סריקה כמו PORT SCANNER (תוכנה המחפשת יציאות (PORTS) פתוחות ברשת הארגונית, שדרכן ניתן לחדור למערכת) וכמו ה-WAR DIALER (תוכנה הסורקת מספרי טלפון בארגון, בחיפוש אחר שלוחות עם מודם, שניתן לגשת דרכן ברשת).

פריצה- החודר יפעיל תוכנות לחיפוש פרצות ידועות במערכת ההפעלה, חשבונות גישה בלתי מוגנים ודלתות אחוריות (BACK DOOR), על מנת להיכנס למערכת. לאחר החדירה למערכת, יתקין הפורץ תוכנות, שמטרתן הרחבת שליטתו במערכת, והפיכתו למנהל המערכת (SUPER USER) . תוכנה כמו PACKET SNIFFER , המושתלת ברשת, מנטרלת את

תעבורת הרשת, ומעבירה אותה אל הפורץ, השולף מידע על שמות משתמשים חוקיים, על סיסמאות גישה וכן נתוני מידע אחרים.

פעילות עוינת- לאחר שהשיג שליטה במערכת המחשב, יבצע הפורץ את המשימה שלשמה הוא פרץ - מחיקת קבצים או גניבתם, שינוי קבצים והפקת פלט כוזב, התקנת וירוסים ותולעים (WORMS) או שימוש במשאבי מערכת המחשב (BUFFER OVERFLOW), שאליה הוא פרץ. בשלב זה יתקין הפורץ במערכת "סוס טרויאני" כמו ה- ROOTKIT, לביסוס שליטתו במערכת ולכניסה עתידית. לאחר הפריצה ישתמש הפורץ בתוכנות השרת או בתוכנות אחרות המיועדות לכך, לשם מחיקת סימנים, העלולים להסגירו - קבצי LOG נתונים, קבצי מערכת (SYSTEM) והגדרות אבטחה.

כיום, ניתן למצוא תוכנות פריצה כמעט בכל אתרי ה"האקרים" ברשת האינטרנט. גם אדם ללא רקע מקצועי יכול להשתמש בתוכנות אלה, על מנת לחדור למערכות מחשב. רשת האינטרנט מספקת לפורצים גישה נוחה למערכות מחשב, מאפשרת להם להחליף מידע על כלי-פריצה ועל חורי אבטחה וללמוד מניסיונם הפלילי של אחרים. ה"האקרים" המקצוענים יותר יפתחו את כלי הפריצה בעצמם וישכללו אותם. "האקרים" אלה מכירים היטב את מערכות המחשב שאליהן הם פורצים, ומפתחים כלים טכנולוגיים משוכללים יותר לפריצת אותן מערכות. לפי כלי הפריצה שבהם נעשה שימוש, יכול מפלג עבירות מחשב ביאח"ה להעריך את יכולתו המקצועית של העבריין, ולקבוע אם מדובר ב"האקר" חובב או ב"האקר" מקצוען.

מאפייני הפורץ

הפורץ החובב - משתמש מחשב סקרן, לרוב קטין, המנסה את כוחו בפריצה למערכות מחשב, בעיקר לשם האתגר והסיכון בכך. הידע המקצועי שלו קטן, והנזק שהוא גורם מוגבל למדי. רוב פורצי המחשב שטופלו ע"י מפלג עבירות מחשב הם פורצים חובבים. ראוי להדגיש (ובמיוחד לאור האווירה הסלחנית, המאפיינת את הטיפול בעבירות מחשב ואת היחס האמביוולנטי כלפי "האקרים", שלכאורה אינם עושים דבר רע אלא חושפים חולשות אבטחה במערכות המחשב), כי הן המחוקק (כפי שהדבר בא לידי ביטוי בחוק המחשבים) והן מפלג עבירות מחשב 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.

הפורץ המקצועי - מומחה מחשב ומתכנת, הפורץ למערכות מחשב של ארגונים פינאנסיים ושל חברות מסחריות, בעיקר לצורך גניבת מידע, ריגול תעשייתי והפקת רווחים לא חוקיים. הפורץ המקצוען קשה לגילוי, ובדרך-כלל יכולתו המקצועית גבוהה מזאת של חוקרי המשטרה. קיימת ההערכה, כי הפורצים המקצועיים הם הגרעין הקשה שמפתח כלי פריצה, מרכז את הפעילות הקהילתית ומבצע הרבה מהפריצות הראוותניות למערכות מאובטחות היטב.

החודר המקצוען- יכול להעלים את עקבות חדירתו ע"י מחיקת קבצי ה- LOG וכל סימן אחר לפעילותו הבלתי חוקית. בצורה זו פעילותו אינה ידועה למנהלי הרשת. החודר יכול, למשל, לגרום לקריסת המערכת ולמחיקת קבצי המחשב החיוניים ביחד עם קבצי ה- LOG שעלולים להסגירו. לעתים, גם לאחר שנודע על חדירה לא חוקית למערכת המחשב, מסרב הקורבן להתלונן במשטרה, אם משום החשש לפגיעה ביוקרה ואם משום החשש, כי פנייתו לא תיענה ביעילות, בחשאיות ובמקצועיות הדרושה.

IP SPOOFING - שיטת תקיפה ופריצה למערכות, שבה מזייף הפורץ את כתובת חבילות המידע (DATA PACKETS) הנשלחות ממחשב למחשב ברשת האינטרנט. ה"האקר המקצוען" יכול גם לזייף את מספרי ה- IP שלו, בצורה שבה יוכל להתחזות למשתמש חוקי שהמערכת מכירה, ו/או להיכנס תחת מספר ה- IP שאין אפשרות להתחקות אחריו. ה"האקר

המקצוען" לא ישתמש לעולם בחשבון אינטרנט חוקי אלא בחשבונות פרוצים של משתמשים תמימים. כן יכול ה"האקר" לשנות את זהותו בדואר אלקטרוני (SPOOFING E-Mail) למטרות פליליות (כמו מרמה ואיום).
אותו "האקר" יכול גם לחדור למרכזיות טלפוניה (PBX) , לזייף ו/או לשכפל מספרי טלפון סלולאריים, לגנוב שירותי טלפוניה PHREAKING)) ולזייפם, ובכך לקבל שירותי תקשורת חינם, ומה שגרוע מכך, למנוע את אפשרות זיהויו באמצעות הטלפוניה.

קיים חשש שה"האקר המקצוען" יצפין את המידע שבמחשבו, על מנת למנוע את שיחזור פעולותיו, ובמידה שיגיע לחקירה משטרתית, ישמור על זכות השתיקה.

המניע

חדירה סתם - בדרך -כלל מבוצעת החדירה למחשב לצורך לימוד המערכת, מתוך סקרנות, אתגר מקצועי וסיפוק ה"אגו" (לפני שנתיים התפרסמה בכלי בתקשורת החקירה שניהל מפלג עבירות מחשב כנגד הפורץ הישראלי המכונה "ANLYZER" , בחשד לפריצה למחשבי הפנטגון, למחשבי הצבא ולמחשבי מוסדות חינוך. בריאיון באינטרנט טען, כי הוא פרץ למחשבי גופים ומוסדות שונים, וביניהם מחשב הכנסת, על מנת להראות את חולשות האבטחה באותם מחשבים, ועל מנת "לסתום את הפרצות" באבטחה).

מבחינת מפלג עבירות מחשב, אין הבחנה אם הפריצה למחשב בוצעה ממניעים אידיאליסטים, ממניעי "אגו" או מתוך רצון לעשיית רווח אישי. החקירה תיערך באותה נחישות, שכן הניסיון מלמד, שפורץ החודר מביתו הבטוח (בדרך-כלל בזהות שאולה) למחשב המרוחק מזירת העבירה, ועושה בו כבתוך שלו, מפיץ את המידע על חולשת המערכת לאחרים, ועלול בקלות להתפתות ולבצע עבירה אחרת.

החדירה אינה פעולה המתבצעת סתם כך בעולם וירטואלי. תוצאותיה יכולות להיות כואבות וממשיות כאחד, כמו גניבה, הרס ושינוי מידע ארגוני. בכל מקרה, החדירה מחייבת את מנהלי המערכת להשבית את המחשב לצורך התקנת מערכת ההפעלה מחדש, וחיסול ה"סוסים הטרוייאנים", שאותם עלול הפורץ להתקין במחשב, לצורך כניסה בעתיד. (בארה"ב, חייב מנהל מערכת מחשב ממשלתית להתקינו מחדש לאחר הפריצה).

עשיית רווח - גניבה של מידע עסקי ואינטלקטואלי (ריגול תעשייתי, רשימת לקוחות, מחקרים ופטנטים); שינוי, תיקון והוספת מידע לצורכי רווח (מפלג עבירות מחשב חקר תלונה בחשד של פריצה למחשב משרד הרישוי, לצורך הוצאת רישיונות נהיגה במרמה); גניבת כסף (באוגוסט 94' פרץ מומחה מחשבים מרוסיה למחשב ה- CT בנק בניו-יורק, וביחד עם כנופייה רוסית, העביר כ10- מיליון דולר לחשבונות בנק בארצות שונות. לישראל הועברו כמיליון דולר לחמישה בנקים שונים. המשטרה, בשיתוף ה- FBI תפסה חבר כנופייה, כאשר ניסה למשוך את הכספים, והסגירה אותו לארה"ב).

שימוש פלילי אחר - גרימת נזק לקבצים (מפלג עבירות מחשב חקר פרשה של מתכנת שנאשם בחדירה אל מחשב הטכניון ומחשבי מוסדות אחרים, וגרם למחיקת קבצי מערכת ולשיתוק מערכת המחשב); הפלת מערכות המחשב; החדרת וירוסים (המשטרה חקרה חשד, כי אחת מחברות ה- ANTI VIRUS ייצרה וירוסים והפיצה אותם על מנת לקדם את מכירת מוצריה); שימוש במידע רפואי ואישי לצורך סחיטה ואיומים (מפלג עבירות מחשב חקר חדירה למחשב מעבדה, המכיל תוצאות בדיקות רפואיות, וביניהן תוצאות בדיקות איידס שנעשו בקופ"ח); מניעת גישה למידע ע"י הצפנה ושינוי סיסמאות גישה (הצוות חקר עובד בחברת הייטק בחשד, כי טרם פיטוריו ע"י החברה הצפין את הקבצים החיוניים להמשך פיתוח מוצר הייטק, עד אשר יתקבלו דרישותיו הכספיות).

ההיבט החוקי - חוק המחשבים

המקום המרכזי שהמחשב תופס בעידן המודרני, התגברותה של עבריינות המחשבים והסכנות הנובעות לחברה טכנולוגית בפגיעה במחשבים, הניעו את המחוקק הישראלי לתת טיפול שלם, במסגרת אחת, בתחום המחשב. המחשב וחומר המחשב זכו להתייחסות מיוחדת בחוק.

החוק כולל ארבעה פרקים. הפרק הראשון עוסק בהגדרת האובייקטים המוגנים בחוק. בפרק ההגדרות - הגדיר המחוקק "מחשב" כמכשיר הפועל באמצעות תוכנה לביצוע עיבוד אריתמטי או לוגי של נתונים וציודו ההיקפי, לרבות מערכות מחשבים, אך למעט מחשב עזר. הגדרה מרחיבה זו מקשה על הגדרת המחשב - יומנים דיגיטאליים, טלפונים סלולאריים וכו', וכן גם על הגדרת "עבירות מחשב" - כאשר אסכולה אחת טוענת שכל עבירה ב"סביבה ממוחשבת" הינה

עבירת מחשב, והאחרת, המצמצמת יותר, רואה כעבירת מחשב רק את העבירות שהוגדרו בחוק המחשבים.

הפרק השני עניינו עבירות מחשב - סעיפים 2-6 לחוק:

סעיף 2 - שיבוש או הפרעה למחשב או לחומר מחשב: מפלג עבירות מחשב ביאח"ה חקר לאחרונה עובד בחברת הייטק, שלפני פיטוריו יצר "סיסמת על" במחשבי החברה ולקוחותיה, וסירב למסור את הסיסמא לבעליה. המפלג גם חקר עובד בחברת תוכנה, שהצפין את קבצי תוכנת הפיתוח, תוך איום שאם לא ייענו תביעותיו הכספיות, לא ישחרר את הקבצים מההצפנה. גם הצפת המחשב בדואלים (עופר שדות) או במנות מידע (PING) נחקרו עפ"י סעיף זה.

סעיף 3 - יצירת מידע או פלט כוזב: עבירות קלאסיות כגון זיוף, מרמה וגניבה המבוצעות באמצעות מחשב. אנשי המפלג חקרו מנהלת חשבונות, אשר באמצעות המחשב יצרה שיקים מזוייפים. מעבר לעבירת המרמה היא גם עברה עבירה עפ"י חוק המחשבים. כן נחקרה עובדת בכירה במשרד האוצר, שפיתחה באמצעות המחשב רשומות של ספקים פיקטיביים, והעבירה בצורה זו במרמה כספים לחשבונותיה השונים.

סעיפים 4-5 - חדירה למחשב

סעיף 6 - עריכה והפצה של תוכנה מרושעת: בהרשעה ראשונה בעבירה זו בישראל (מדינת-ישראל נ' גיל פז) כתב השופט בגזר-דין מיום 24.2.98: "יש, איפא, להבהיר לכל מי שמבקש לכתוב "תוכנה מרושעת" או המבקש להחדיר תוכנה שכזו למחשב או המבקש לעשות במחשבו שימוש מרושע אחר, כי בית-המשפט לא יקל עמו בדין כאשר יתפס בכף". לאחרונה הורשע כותב תוכנת וירוס בשם פז"ם, ששידל את חברתו החיילת להתקין את הווירוס במחשבי הצבא, ובכך גרם נזק כבד למחשבים ולמידע האגור בהם.

הפרק השלישי עוסק בדיני נזיקין.

הפרק הרביעי עוסק בתיקוני חקיקה עקיפים בתחום הראיות.