האתיקה של הפריצה הממוחשבת – מי יפרוץ לרשת שלי ?

מאת אופיר זילביגר, מנכ"ל SECOZ

בחינת פריצה (Penetration Testing) היא תהליך שבו נבדקת יעילותו של מערך האבטחה בארגון באמצעות פריצה יזומה אל רשתות ומשאבי המחשוב של הארגון. מנהלי אבטחת מידע או האחראים על הנושא בארגון מבקשים לאתר חולשות ופרצות המאפשרות חדירה אל המערכות הקריטיות בארגון לפני שגורם עוין אחר יעשה זאת וזאת תוך ניצול מכוון של נקודות תורפה ושימוש בטכניקות פריצה המבוססות על ידע טכני מובהק.

העלייה ברמת הפגיעות של מערכות מחשב ורשתות תקשורת, וריבוי אירועי הפריצה (כולל התקפות של האקרים מהאינטרנט ומתוך הרשת הפנימית) למערכות אלה, מחייבים את המומחים לאבטחת המידע להיות מעודכנים ברזי ההתקפות והטכנולוגיה ולהקדים תרופה למכה.

בדיקת העמידות בפני פריצות מחשב היא תהליך בקרה המאפשר להתבונן בארגון מעיניו של פורץ מחשבים ("האקר").

שימוש ב"האקרים" בדימוס (שחזרו בתשובה) לצורכי שירותי ייעוץ רגישים כגון פריצה אתית(Ethical Hacking) עלול לחשוף את הארגון לסיכונים רבים.

רבים מאותם האקרים - המוכרים גם בכינוי "מגבעות אפורות" נכנסו לעסקי הייעוץ בתחום אבטחת המידע. לעיתים הם אף מתפארים בהיותם האקרים לשעבר או אפילו לא לשעבר. מצב זה גורם למבוכה ומעורר חששות בקרב ארגונים, המתחבטים אל מי עליהם לפנות לקבלת שירותי ייעוץ בתחומים רגישים ורבי חשיבות אלה.

רמת הידע הכוללת של היועץ אינה השיקול הבלעדי והמכריע, מכיוון שייעוץ בתחום אבטחת המידע מחייב יותר מאשר כישורים טכניים גרידא. ייעוץ בתחום זה, הוא למעשה שילוב ואינטגרציה של תהליכים עסקיים, נהלים ומדיניות עסקית יחד עם ניסיון רב-תחומי מצטבר בתחום. לרבים מבין ההאקרים לשעבר אין כלל הבנה של הנושאים והשיקולים העסקיים המורכבים אשר נלווים לאינטגרציה של פתרונות אבטחת מידע במסגרת עסקים גלובליים ובזירת העסקים האלקטרוניים.

בביצוע פרוייקט של "Security Penetration Testing" יש לשים דגש על הסיכון בו הארגון נמצא במהלך הבדיקה כגון הסיכון לאובדן שירותים לא מכוון (Denial of Service) או להפלת מערכות שיגרמו נזק גדול מערך מניעת הפריצה שלה כיוונו.

האבטחה היא התגלמות התפיסה של 'האמן, אך בדוק ואמת' (trust but verify). המנהלים צריכים לשאול את עצמם: האם אני יכול להפקיד בידי אדם זה את הטיפול במשאבים הרגישים ביותר שלנו?

תרבות ה- 'סמוך' הנפוצה בישראל, אשר מתאפיינת בחוסר שימוש במתודולוגיות ובנהלים נאותים, מתירה שימוש בהאקרים לשעבר. מחסור בכוח אדם מקצועי בתחום אבטחת המידע מחד וזמינותם ועלותם הנמוכה של 'ילדים' (המתאפיינים לעיתים בכינוי Script Kiddies) מאידך מביאים ארגונים לשימוש בכוח אדם לא מומלץ זה ועשוי להוביל לתוצאות המפורטות לעיל.

SECOZ | Tel. +972.8.971.66.05 | Fax. +972.8.971.65.94 | Hashdera Hamercazit 15, Ligad Center, POB 23 Modi'in 71700, Israel

מומלץ ליישם ארבעה קריטריונים מנחים על מנת להבטיח את האמינות והמהימנות של צוות ייעוץ בתחום אבטחת מידע:

1. הצוות צריך להשתמש במתודולוגיה מובנית, המתוכננת למנוע הרס של נתונים, השבתת מערכות או כל פגיעה אחרת בתהליכי עיבוד המידע. הפרוטוקול המיושם (נוהל הפעולה המוגדר) צריך לכלול מנגנונים שיבטיחו דיווח מיידי ללקוח על אודות נקודות פגיעות מהותיות שנתגלו, וכן העברה משמעותית של ידע. בנוסף, הצוות חייב להגדיר וליישם מתודולוגיה שתבטיח את אמינות והמהימנות של כל כלי ההאקרים שייעשה בהם שימוש במהלך ההתקשרות.

2. רמת המקצוענות, הרקע והיושר של כל חברי הצוות חייבים להיות ללא רבב. חברי הצוות חייבים לעבור בהצלחה מערך מקיף ויסודי של בדיקות רקע לפני תחילת ההתקשרות.

3. הצוות חייב להיות בעל ידע וכישורים טכניים גבוהים ביותר. חברי הצוות חייבים להכיר היטב את שיטות התקיפה וכלי התקיפה החדישים ביותר, וכמו-כן עליהם להבין באופן מלא את כל ההשפעות והסיכונים הנלווים לשימוש בכלים או בהרצת התוכניות.

4. לצוות חייב להיות ניסיון רב בתחום התעשייה הרלוונטי. חברי הצוות חייבים להבין שבכל תחום תעשייה קיימות דרישות אבטחה שונות, ועליהם להיות מסוגלים להציע הצעות להתמודדות עם נקודות חולשה אשר יתאימו לרמת הסיכון הקבילות והמקובלות בארגון שלו הם מייעצים.

ניתן להניח במידה רבה של ודאות כי כל יועץ אשר עונה על ארבעת הקריטריונים הנ"ל הוא מקור אמין ומהימן של שירותי ייעוץ, והוא יצליח לעמוד במשימת הייעוץ באופן משביע רצון.

SECOZ | Tel. +972.8.971.66.05 | Fax. +972.8.971.65.94 | Hashdera Hamercazit 15, Ligad Center, POB 23 Modi'in 71700, Israel