



מבדקי חדירה מינימום השקעה מקסימום תועלת

בתקופה האחרונה אנו עדים למס' לא מבוטל של אירועי "תקיפה" רועשת על רשתות ארגוניות ישראליות ע"י האקרים במדינות השונות המעוניינים למחות כנגד מדינת ישראל. גם שמה של ישראל לא נפקד בפעולות מעין אלו כנגד מאמץ הגרעין האיראני. מאמר זה דן ביכולתנו כמעריך אבטחה לתת מענה כנגד חדירה לרשתות הארגון עליו אנו מופקדים וזאת ע"י מבדקי חדירה יזומים. מבדקים אלו נועדו לבדוק את רמת החשיפה של הארגון אל מול פריצה אפשרית לרשת הארגונית.

מאת: אורן שני*

מהם מבדקי חדירה?

מבדקי החדירה הינם בדיקות מעשיות לקביעת רמת החשיפה של הארגון אל מול פריצה אפשרית לרשת הארגונית. בניגוד לבדיקות אבטחה אחרות, מבדקי החדירה אמורים לקבוע באופן חד משמעי; האם ניתן לפרוץ לארגון אם לאו ומהן הדרכים המעשיות בהן יבחר ה"תוקף" לביצוע פעולה זו. באופן זה מסכמת בדיקת חדירה אחת, מגוון רחב של בדיקות תיאורטיות אחרות ואי לכך הינה עדיפה בשיקולי עלות מול תועלת לארגון.

קיימות שתי בדיקות חדירה אפשריות: האחת באמצעות רשת האינטרנט אל תוך הרשת הארגונית והשנייה פריצה מתוך הרשת הארגונית עצמה אל משאבים רגישים אליהם לא אמור הפרוץ להגיע. הבדיקה הראשונה תדמה תוקף חיצוני שמנסה לקבל מידע או להשתיל קובץ עיני ברשת הארגונית, למשל לקורא דואר ארגוני רגיש, להשתיל קובץ תקיפה שמטרתו פגיעה בעבודה השוטפת בארגון וכו'. הבדיקה השנייה מדמה עובד או ספק/קבלן שיושבים בתוך הרשת הארגונית המנסה להגיע למידע אליו אין לו הרשאות, למשל, רשימת הלקוחות, מחירונים, תוכניות שיווק, יישומי סליקה וכו'.

מהם סוגי מבדקי החדירה הקיימים?

מבדקי חדירה - רשת חיצונית (Penetration Testing - External Network)

בדיקה זו כוללת תקיפה של מערך התקשורת מכיוון רשת האינטרנט לעבר רשת החברה. מבדק זה מבוצע ברמת התקשורת אל מול ממשק התקשורת החיצוני של החברה (FW) האמור להגן על עמדות הקצה והשרת הפרוסים במשרדי החברה. מטרת המבדק - לחדור את מעטפת ההגנה החיצונית של הרשת ולהגיע לנכסי מידע מעניינים כגון תכתובת דואר ארגוני רגיש, הזמנות מלקוחות, ספקים וכו'.

מבדקי חדירה - רשת פנימית (Penetration Testing - Internal Network)

בדיקה זו כוללת תקיפה של מערך התקשורת הפנימי בארגון. בחינה זו מבוצעת ברמת התקשורת תוך התממשקות ל"נקודה חמה" ברשת הפנים ארגונית, במטרה לדמות גורם אשר קיבל קישור לרשת הפנימית ומנסה להגיע למקורות מידע אשר אין לו הרשאות עבורן (כגון קבלן אשר חורג מתחום פעולתו או לחילופין

עובד שמנסה לצפות במידע של הממונים עליו ללא הרשאה). מטרת הבחינה במקרה זה הינה לקבל הרשאות גישה בלתי מורשות על הרשת הפנימית המקומית וממנה להשתלט על נכסי מידע כגון רשימת לקוחות, מחירונים, תוכנית שיווק עתידית וכו'.

מבדקי חדירה לאפליקציה (Penetration Testing - Application Level)

מבדקי החדירה ברמת האפליקציה (יישום) יכללו סקירה היקפית, הלכה למעשה של אפליקציות מרכזיות בארגון, בין אם המשמשות את לקוחות החברה או את עובדיה לשימושים פנימיים או חיצוניים. הבחינה מבוצעת ברמות המשתמש השונות (משתמש פשוט, משתמש פריווילגי וכו') הקיימות באפליקציות, כאשר בחינה זו תנסה לאמוד את היכולת של תוקף פוטנציאלי להסב נזק תדמיתי או כלכלי לחברה או ללקוחותיה.

מבדקי חדירה ל מערכות הטלפוניה - VoIP

על ארגונים בכל הגדלים אשר אימצו טכנולוגיה של Telephony IP לשקול ברצינות את נושא אבטחת המידע גם באפיק

בבדיקה פשוטה יחסית שאינה יקרה הכוללת ניסיון חדירה פשוט שייעודו תקיפת הרשת והוצאת מידע מתוכה. באם בבדיקה פשוטה זו מצליחה להשיג את מטרתה, ניתן לקבוע כי מנגנוני סינון המידע הנכנס כשלו, רמת אבטחת המידע בעמדות הקצה הינה נמוכה ורמת סינון והגבלת מידע יוצא הינה נמוכה. מתוך מסקנות אלה ניתן לקבוע תוכנית פעולה לצמצום הסיכונים לשם הבטחה של שמירת יתרון עסקי, כמו גם שמירה על חוקים ותקנות. ■

*הכותב הינו מנכ"ל משותף בחברת "SecAudit" העוסקת בנייהול סיכונים, ביקורת מערכות מידע ואבטחת מידע. החברה מספקת קשת שירותים המאפשרים להעריך סיכונים, לשפר את הבקורות הקיימות ולהגביר את רמת הביטחון בתהליכים ובמערכות הארגון.

info@secaudit.co.il
www.secaudit.co.il

כמו כן משולבת תקיפה ידנית המבוססת על תוצרי הכלים הממוכנים, בה מבוצעת הדמיית תקיפה פרטנית על מנת לאתר חולשות ולממשן ברמת התקשורת והרשת בכדי להביא למצב בו המערכת מאפשרת גישה בלתי מורשית למשאביה בכל אחת מהרמות: מערכות ההפעלה, רכיבי התקשורת או האפליקציות.

התוצר המתבקש מבדיקות אלו חייב לתת תשובות לשאלות שנשאלו: האם הרשת חדירה ואם כן היכן וכמובן מהן הפעולות שיש לנקוט על מנת לסגור פרצות אפשריות אלו הן בפן החומרי, הן בפן התוכני והן בפן הניהולי.

בדיקות החדירה מוצעות בישראל ע"י מס' ארגונים המתמחים באבטחת מידע, בבדיקות אלו הינן יקרות יחסית, שכן הן מחייבות רמת מקצועיות גבוהה של הבודק וכמו כן מדובר בזמן בדיקה לא מבוטל. לאלו שאין בידם את המשאבים הדרושים לבדיקות מעין אלו אנו ממליצים על בדיקה המתמקדת ב"חוסן הרשת"

זה. אל מול מספרים גדלים והולכים של ארגונים המאמצים Telephony IP עולים האקרים ופושעים מסוגים שונים המנצלים חולשות הקיימות בטכנולוגיה זו למטרותיהם. האיזמים הנפוצים ב VoIP הינם: גניבת שיחות, ציטוט והאזנה, מניעת שירות - Denial of Service, פריצה ל VoIP ומשם פריצה לרשת הארגונית.

אופן ביצוע הבדיקות:

כבכל בדיקה בה נעזרים במומחה חיצוני (חוקר, בודק פוליגרף וכדומה) טרם תחילת הבדיקות מומלץ לקיים פגישה להבנת מערך המחשוב הקיים בארגון. אין ספק שפגישה זו תקל על ה"תוקף" אך מנגד תביא לצמצום היקף שעות הבדיקה ובכך לצמצום העלויות.

במסגרת הבדיקה מבוצע שימוש בכלים ממוכנים המסוגלים לדמות מצבי תקיפה שמטרתם לאתר חולשות ברמות השונות, חוסר בתיקוני אבטחה מותקנים, הרשאות גישה חלשות וכו'.

הבחירה המועדפת בפרויקטים:



מצלמות IP מקצועיות



- WDR איכותי
- Lux נמוך
- IR CUT Filter
- עדשות מגה-פיקסל ייעודיות
- זיודים מיוחדים - כימות אנטי-ונדל,
- זיוד לתנאים קשים Arctic
- תוכנת NVR מקצועית כלולה עם המצלמה



security & control systems
טכנולוגיה • שירות • פתרונות

להשיג באונו ביטחון- המפיץ הבלעדי בישראל

info@onosecurity.co.il | 03-6323231