# מתקפת אפס הימים

הכירו את האיום הגדול ביותר כיום בתחום הסייבר: "מתקפת אפס ימים", המנצלת פרצות לא ידועות. שמירה על נהלים וביצוע פעולות בצורה שיטתית יכולים להפחית בצורה משמעותית את הסיכון.
רו"ח מיכאל בוטניק מנכ"ל פירמת אינטגרטי הפירמה המובילה בישראל ובעולם בנושא סייבר והגנת הפרטיות.
פגיעה במערכי צנטריפוגות, תוכנות זדוניות המדביקות מיליוני מחשבים תוך מספר שניות, התקפה על מערכות תשלומים, גניבת מיליוני כרטיסי אשראי, הדלפת מידע מסווג ממערכות מידע. מה משותף לכל אלה? בחלק מהמקרים לא מדובר בהתקפות רגילות של האקרים בודדים, אלא בשימוש בנשק סייבר מתוחכם על ידי ארגוני ביון, צבאות, ארגוני פשע וארגוני טרור נגד תשתיות צבאיות ואזרחיות קריטיות של מדינות, מחוזות וארגונים בינלאומיים.
מתקפת אפס ימים (מאנגלית Zero day attack)- :הוא כינוי לשימוש בפרצת אבטחה בתוכנה, שלא היתה ידועה עד כה לציבור הרחב וספקי התוכנה, על ידי גורמים זדוניים, לצורך יצירת מתקפת סייבר יעילה ואפקטיבית שאמורה לעקוף כל מערכות ההגנה בארגון המותקף.לדוגמא:תולעת Stuxnet, לצורך חדירה והשתלטות על מערכות מפעל להעשרת אורניום, השתמשה בסדרה מכובדת של פרצות אבטחה לא ידועות, כולל במערכות הפעלה ייחודיות. לרוב, נוהגים חוקרים ומומחי אבטחה להתריע על פרצת אבטחה לפני פרסומה בקרב הציבור הרחב, ובכך לאפשר לחברה בעלת התוכנה זמן לחקור ולתקן אותה, ולהפיץ ללקוחותיה עדכון תוכנה לפני שתפורסם ותנוצל על ידי הגורמים הזדוניים.
ביצוע מחקר ואיתור פרצה חדשה לצורך שימוש זדוני יכול להיות תהליך מורכב. כיום, פרצות כאלה מתגלות לרוב על ידי ארגוני פשע, ארגוני טרור, שרותי ביון וצבאות, כמו גם בידי קבוצות האקינג מובילות אשר משקיעים משאבים כבירים בנושא. גם ספק תוכנה מסוגל לגלות פרצה כזו ולא לפרסם תיקון מסיבות שונות.
כאשר אין ניסיון מדוע מתקפות אלה כל כך מסוכנות ולא ניתנות לגילוי מוקדם על ידי מערכות האב– טחה? התשובה לכך היא, כי כמעט כל מערכות האבטחה הקיימות מבוססות על חוקים וחתימות כגון חומות אש, אנטי וירוס, מסנני תוכן וכדומה. תוכנות האבטחה מחזיקות מאגרים של חוקים וחתימות של קוד זדוני, ובצורה זו הן יכולות להגן מפני ההתקפות שאירעו בעבר ועבורן נוצרו חתימות המזהות אותן. מכיוון שבמתקפת אפס ימים מתגלה פרצה לא מוכרת לשימוש מיידי, בינתיים לא ניתן לתקן אותה, ומוצרי אבטחה לא מכירים.
ולא מזהים אותה. מדובר בהתקפת הסייבר היעילה והאפקטיבית ביותר שקיימת כיום. חשוב גם להבין את וקטורי התקיפה הנפוצים בסוגי מתקפות אלה. הווקטורים הנפוצים הם הדבקת תחנה קצה בארגון או התקן נייד, באמצעותו גולשים לאתר אינט– רנט לגיטימי שהושתל בו קוד זדוני, שליחת קובץ נגוע או לינק לדוא"ל של עובדי האר– גון תוך שידול המשתמשים לפתוח אותו, חיבור והפעלת התקן זיכרון נייד או תקליטור למחשב ועוד. בחלק מהמקרים התקיפה דורשת שיתוף פעולה מסוים של הגורם האנושי, או קיום שירות מסוים שפעיל ונגיש אשר כולל פרצת אבטחה שטרם תוקנה. מה בכל זאת ניתן לעשות על מנת למזער סיכונים או נזקים כתוצאה ממתקפת אפס ימים? הנה כמה צעדים מומלצים.
ביצוע סקר סיכוני סייבר ממוקד בארגון על ידי מומחים אובייקטיביים, על מנת להעריך את מוכנות הארגון למניעה, גילוי וצמצום נזקים ממתקפות אפס ימים בהתייחס לערך נכסי המידע עליהם יש להגן. הסקר יאפשר לאתר מוקדי סיכון בהם נדרש לטפל, להמליץ על פתרונות בהתייחס לעקרון עלות/תועלת ולבנות תוכנית עבודה מתאימה ליישום. בהמשך יש לקיים הערכות סיכונים תקופתיות לבחינה של מפת האיומים והצורך בביצוע שינויים נוספים.

יישום מדיניות, נהלים ותוכניות הדרכה אפקטיביים בהיבטי אבטחת מידע בארגון, לצורך הגברת מודעות המשתמשים למתק– פות סייבר, הטמעת כללים לשימוש מאובטח במחשב, דוא״ל ואינטרנט, כללים לשמירה על סודיות מידע, דיווח יזום על אירועים חריגים ועוד. עיקרון חשוב באבטחת מידע גורס, כי החוליה החלשה במערך אבטחת מידע הוא המשתמש הקצה. כפי שצוין, חלק מהמתקפות מבוצעות בשיתוף פעולה של משתמש הקצה בארגון, ועל כן משתמש בעל מודעות גבוהה לא ישתף פעולה עם התוק– פים והדבר יקשה על ביצוען.
ביצוע סגמנטציה פיזית או לוגית של רשתות בארגון מול שותפים עסקיים וספקים, ובכך להקשות על מתקפה להתפשט בו במהירות. במסגרת זו על הארגון לא לאפשר שירותי של אינטרנט ודוא״ל ברשתות רגי– שות מסוימות בתוכו. הגבלת הרשאות גישה ופעולה למש– תמשים בתוכנות הארגון בהתאם לעקרונות הבאסים: הצורך לדעת, הפרדת תפקידים וקיום פריבילגיות מינימאליות. כאשר מיושמים עקרונות אלה, הרי שגם אם משתמש או תוכנה מסוימים הודבקו, ההר– שאות המוגבלות של המשתמשים יקשו על התפשטות המתקפה במהירות בתוך הארגון.

<u>עירנות מתמדת</u>

שימוש ברשימה לבנה(whitelisting) של תוכנות. במקרה זה המשתמש מוגבל להת– קנה ולהרצה של תוכנות במחשב בהתאם לרשימה המאושרות ע״י הארגון. הדבר ימנע בחלק מהמקרים התקנה של תוכנות זדוניות ביוזמת המשתמש או שימוש זדוני בהרשאות המשתמש.
קיום תוכנית פעולה לתגובה לאירועי סייבר. לא ניתן לחזות ולמנוע כל מתקפות סייבר, בפרט שהן אינן ידועות. לאור זאת, קיום תוכנית פעולה מאורגנת ומתורגלת וצוות תגובה מיומן ומקצועי לגילוי וטיפול באירועי סייבר, אמורים לצמצם נזקים כתו– צאה מאירועים כאלה, לרבות נזקי מוניטין.
שימוש בכלים לאיסוף, ניתוח אירועים חריגים במערכות מידע ובמערכות אבטחה. התרעות על אירועים חריגים עשויות לסייע בחלק מהמקרים בגילוי מתקפות.
קיום שליטה ומיפוי מלא בכל סביבות מערכות המידע של הארגון. מיפוי מפורט של כל הרכיבים הלוגיים ופיזיים המרכיבים את רשת הארגון, קשרים בין רכיבים, לרבות מול העולם החיצון ורכיבי מערכות מידע של הארגון, מאפשר רמת שליטה ובקרה יעילה ואפקטיבית. שליטה ובקרה מאפשרות להגיב במהירות לאיתור רכיבים שהודבקו ולהפעיל תוכנית למזעור נזקים והפסקת מתקפה. שליטה ובקרה מאפשרות ליישם מנגנוני אבטחה באופן יעיל ואפקטיבי ולצמצם כמה שניתן אפשרויות מתקפה פוטנציאליות.
קיום תוכנית יעילה ואפקטיבית להת– קנה בזמן עדכוני תוכנה לפרצות אבטחה שפורסמו. הדבר לא ימנע הדבקה בפרצה שטרם פורסמה, אך ארגונים רבים נכשלים גם במשימה לעדכן בזמן את מערכותיהם על מנת להתמודד עם פרצות שכבר פור– סמו. מתקפת סייבר מתוחכמת כוללת לעיתים שילוב של שימוש בפרצות ידועות ולא ידועות, ועל כן מערכות מעודכנות יקשו על מתקפות להתפשט.
יישום תהליכי הקשחה בכל הרכי– בים תוך צמצום שטחים החשופים למתק– פות סייבר. לדוגמא: חסימת כל הפורטים, חשבונות, שיתופים ושירותים לא נחוצים בתוך הארגון וכלפי רשתות חיצוניות.
שימוש במערכות הפעלה חדישות יותר, בהן כבר מוטמעים מנגנוני אבטחה פנימיים המקשים על מתקפות אפס ימים וזאת תוך ביצוע שדרוגים מתוכננים ובזמן. כך למשל, מערכת ההפעלה Windows XP כבר לא נתמכת על ידי חברת מיקרוסופט, אך ארגו– נים רבים לא תכננו מעבר מסודר ממערכת הפעלה זו ומהווים טרף קל למתקפות.
בחינת שימוש בפתרונות מתקדמים שמציעים הגנה מפני מתקפות אפס ימים. לאור חריפות הבעיה קמו חברות הזנק רבות שמנסות לנצל את הגל, וגם ספקי מערכות אבטחה קיימים הוסיפו פונקציות שונות לפתרון הבעיה. חשוב לבצע בחינה יסודית של פתרונות קיימים וחדשים, לרבות התאמתם לסביבה הארגונית, רמת האקטיביות והיעילות שלהם, תוך קבלת ייעוץ אובייקטיבי ממומחים בתחום.

בחינת רכישת פוליסת ביטוח נגד סיכוני סייבר, תוך קבלת ייעוץ ממומחים בתחום.
לסיכום: אכן מדובר באיום הסייבר המסוכן ביותר הקיים כיום. יחד עם זאת, גישה מתודולוגית ופרואקטיבית של הארגון תאפשר להתמודד טוב יותר עם איומים אלה ולמזער נזקים. חשוב להדגיש, כי שימוש במוצר אבטחה כזה או אחר, אינו מחליף עקרונות אחרים שפורטו לעיל. על כן, גם אם הארגון בחר במסלול לפתרון הבעיה, עדיין עליו לשמור על כל העקרונות שהוצגו, לא להיכנס לאופוריה ולשמור את האצבע על הדופק.

כדי להיערך כנדרש לאור האיומים המתוארים יש לבצע הערכת סיכונים לפרטים אנא ליצור קשר עם jennifere@corporateintegrity.co.il