מתקפות סייבר

מתקפות סייבר הן איום משמעותי על ארגונים וגורמים פרטיים כאחד. הנה כמה מהסוגים הנפוצים ביותר של מתקפות סייבר והדרכים להימנע מהן.

נוזקות (Malware):

מונח כללי המתאר כל סוג של תוכנה זדונית שנועדה לחדור או להזיק למחשב, לאסוף מידע רגיש, להשיג גישה לרשתות מחשב פרטיות או להציג תוכן פרסומי בלתי-רצוי, וזאת ללא ידיעת המשתמש.

- **וירוסים:** תוכנות שמתחברות לתוכנות אחרות ומבצעות פעולות זדוניות כמו מחיקת קבצים או השחתת מידע.
- **תולעים (Worms):** נוזקות שמשכפלות את עצמן ומפיצות את עצמן דרך רשתות מחשב, ללא צורך בתוכנה מארחת.
- **סוסים טרויאניים (Trojans):** תוכנות שמתחזות לתוכנות לגיטימיות אך מבצעות פעולות זדוניות ברקע, כמו גניבת מידע או פתיחת דלת אחורית לתוקפים.
- **כופרה (Ransomware):** תוכנה זדונית שמצפינה את קבצי המשתמש ודורשת כופר כדי לשחררם. מתקפות אלה עלולות לשתק ארגונים שלמים, ולגרום להפסדים כספיים משמעותיים.
- **רוגלות (Spyware):** תוכנות שעוקבות אחרי פעילות המשתמש ומעבירות מידע רגיש לתוקפים.
- **תוכנות פרסום (Adware):** תוכנות שמציגות פרסומות בלתי-רצויות או מפנות את המשתמש לאתרים פרסומיים.

מניעת שירות מבוזרת (DDoS):

מתקפה שמטרתה לשבש את פעילות האתר או השירות על ידי הצפתו בתעבורה מזויפת, מה שגורם לקריסתו.

סוסים טרויאניים (Trojans):

תוכנות זדוניות שמתחזות לתוכנות לגיטימיות ומאפשרות לתוקפים גישה למערכות המחשב של הקורבן.

התקפות מתמשכות מתקדמות (APT):

מתקפות ממוקדות ומתוחכמות, שמטרתן לחדור לרשתות ארגוניות ולהישאר בהן לאורך זמן כדי לגנוב מידע רגיש.

פישינג (Phishing):

מתקפה שבה תוקפים שולחים הודעות דוא"ל מזויפות, שנראות כאילו נשלחו מגורם אמין, במטרה לגנוב מידע אישי כמו סיסמאות ופרטי כרטיסי אשראי או לתקוף את המחשב/טלפון של הקורבן.

אלביט מערכות
מטה החברה • ביטחון

Elbit Systems
ESOC