21 מאי 2020
כ"ז אייר תש"פ
סימוכין:ב-ס-1087

היערכות להשחתת אתרי אינטרנט

תקציר

לאחרונה דווחו אירועי השחתת אתרי אינטרנט בישראל.
על מנת להגיב באופן המיטבי לאירוע מסוג זה, על בעלי האתר להיערך מראש.
להלן העקרונות העיקריים להיערכות זו.

פרטים

1. הדרך העיקרית להימנע מאירועי השחתה ופגיעה באתרים הינה הקפדה על נהלי פיתוח מאובטח. עקרונות אלו פורטו על ידי מערך הסייבר הלאומי ב- https://www.gov.il/he/departments/general/securedevelopment.
2. מטרת מסמך זה, פירוט עיקרי ההכנות שיאפשרו לבעלי אתר שהושחת, חזרה מהירה ככל האפשר לשגרה.

דרכי התמודדות

1. מומלץ לוודא כי מבוצע גיבוי עיתי לאתר, והגיבוי נבדק מעת לעת על מנת לוודא את תקינותו.
2. מומלץ כי לפחות עותק אחד של הגיבוי יישמר באופן שאינו מקוון, למניעת פגיעה בו-זמנית באתר ובגיבוי.
3. מומלץ להכין מראש דף חלופי אליו ניתן להפנות את התעבורה לאתר במהלך הטיפול בפגיעה או בהשחתה.

4. מומלץ לסכם מראש עם הארגון המארח את האתר (אם האתר מתארח אצל גורם חיצוני) לגבי גבולות הגזרה בטיפול באירוע השחתה, ומי מהצדדים אחראי לביצוע אילו פעולות על מנת להשיב האתר לפעילות בהקדם האפשרי.
5. מומלץ שלא להחזיר האתר לפעילות בטרם ביצע גורם מקצועי זיהוי של וקטור התקיפה דרכו בוצעה הפגיעה, והפגיעות תוקנה למניעת הישנות האירוע.

לכל מידע נוסף ניתן לפנות אלינו. במידה שעלו ממצאים בבדיקתכם, נבקש לקבל היזון חוזר.

מקורות

שיתוף מידע עם ה-CERT הלאומי אינו מחליף חובת דיווח לגוף מנחה כלשהו, ככל שחלה על הגוף חובה כזו.
המידע נמסר כפי שהוא (as is), השימוש בו הוא באחריות המשתמש ומומלץ להיעזר באיש מקצוע בעל הכשרה מתאימה לצורך הטמעתו.

בברכה,
CERT-IL