בעקבות מתקפות סייבר חוזרות ונשנות אשר גורמות להשחתת אתרים רבים של חברות וארגונים קטנים ובינוניים, אנו מביאים לכם מספר המלצות בסיסיות ופרקטיות אשר הקפדה עליהן תסייע לכם להתמודד בעתיד עם מתקפות סייבר דומות המתרחשות במרחב האינטרנט מדי יום.

10 הדברות להגנה על אתרי אינטרנט

1. **חומת אש אפליקטיבית** - האם האתר מוגן ע"י חומת אש אפליקטיבית (WAF) והאם כל מנגנוני ההגנה של חומת האש מופעלים על האתר? מימוש הגנה זו באופן קפדני יצמצם את יכולת ההאקרים לפרוץ לאתר.
2. **הפרדת שכבות** - האם בסיס הנתונים של האתר מנוהל בשרת שונה משרת האפליקציה והאם יש בקרה תקשורתית של חומת אש (FireWall) על התקשורת בין שני שרתים אלו? זוהי התצורה הרצויה למזעור סכנת הגישה של האקרים למידע השמור באתר.
3. **הזדהות חזקה** - האם גישה לממשק ניהול האתר מותרת רק למורשיי בית העסק וההזדהות הינה חזקה (FA, MFA2) ? אם אין אפשרות למימוש הזדהות חזקה, יש להגדיר סיסמא בת 8 תווים אשר מורכבת מאותיות, ספרות ותווים מיוחדים ואשר מוחלפת בתדירות קבועה.
4. **חסימת מניעת שירות** - מומלץ להפעיל, במידה וניתן, מנגנוני הגנה נוספים כגון מנגנון לזיהוי ומניעה של מתקפות מניעת שירות (DDOS) ומערכת לזיהוי ומניעה של מתקפות רשת (IPS). האם מופעלים?
5. **עדכון טלאי אבטחת מידע** - האם המרכיבים של האתר (מערכת ההפעלה, בסיס הנתונים, ותשתיות האפליקציה) עוברים עידכוני אבטחה באופן תדיר לכל הפחות מדי 3 חודשים? לרוב ניתן להגדיר שהעדכון יהיה אוטומטי. פרצות ידועות במערכות מסייעות להאקרים לפרוץ למערכות המידע.
6. **חסימת חשבונות סטנדרטיים ומוכרים** - האם סיסמאות ברירות מחדל של משתמשים מובנים בחשבונות המערכת(אשר מוגדרות ע"י יצרני המערכות טרום התקנת המערכת) מוחלפות בסיסמאות ייחודיות? אי החלפת סיסמאות ברירת מחדל מסייעת להאקרים להשתלט על מערכות ולחדור למערכות המידע.
7. **הצפנת סיסמאות** - האם מתחזקי/מפתחי האתר השאירו קבצים עם סיסמאות גישה ב-CLEAR TEXT (לא מוצפנות) בתשתיות האתר? זוהי טעות נפוצה של גורמי תחזוקה ופיתוח וקבצים אלה משמשים האקרים למימוש ההתקפות שלהם ויש למחוק אותם מיידית.
8. **מחיקת חשבונות שלא בשימוש** - האם מתבצע מעבר יזום, אחת לתקופה, על מורשי הגישה לתחזוקת האתר בו מתבצע מחיקת משתמשים שאינם מורשים לגישה אליו? פעילות זו הינה באחריות בעל האתר ומונעת גישה לא מורשית תוך שימוש במשתמשים ישנים.
9. **פרו אקטיביות** - האם מתבצעת סריקה תקופתית על האתר למציאת חולשות/פגיעויות באתר או בתשתיות האתר? ניתן לבצע זאת ע"י כלים חינמיים מוכרים הקיימים באינטרנט או באמצעות רכישת שירות מגורם מקצועי.
10. **גיבוי** - האם האתר ובסיס הנתונים שלו מגובים (BACKUP) בתדירות יומית ומתבצעת בדיקה שאכן ניתן לשחזר את המידע מהגיבוי? זהו הליך חיוני למקרה שהאתר או הנתונים בו הושחתו או הוצפנו ע"י האקרים.