



# הגן על נכסי האינטרנט שלך, הגן על העסק שלך

בעולם המקוון, אבטחה ראויה של אתר החברה שלך היא יותר מעוד רעיון טוב, היא חיונית על מנת שתוכל להגן על עצמך, על הלקוחות שלך ועל המוניטין שלך

הנכסים המקוונים של העסק:  
 ● תכנות מאובטח וביקורת קוד - בצעו את ההנחיות המומלצות על ידי ה- Open Web Application Security Project (OWASP) וגופים אחרים. כך מתכנתים יוכלו לבנות אפליקציות מאובטחות ואמינות יותר ולהוריד את מספר המניפולציות לאורך מחזור החיים של האפליקציה. ברגע שפותח, הקוד חייב לעבור סקירה וביקורת על ידי גורם צד שלישי, עצמאי, שהוא בלתי תלוי בצוות הפיתוח.

**ה** מסחר האלקטרוני שינה את הדרך שבה העולם עושה עסקים. מלבד היותו "הפנים של העסק", אתר האינטרנט הוא צינור עסקי. לקוחות העסק ולקוחות פוטנציאליים מחפשים בו מידע מוצרים ופתרונות, שותפים עסקיים מחפשים מקור מידע, וכמובן, צרכנים רוכשים בו מוצרים. בחברות כגון אמזון, אי-ביי ואחרות, אתר האינטרנט של חברה הוא העסק עצמו. ברור אם כן, שאתר אינטרנט שלא עובד כראוי, משפיע באופן ישיר על שורת הרווח.



● בצעו הערכה לרמת הפגיעות של האפליקציה ומבחיני עמידות בפני פריצה - בצעו סקירה של אפליקציות, ידנית או על ידי כלים אוטומטיים, על מנת לגלות חולשות. מבחיני עמידות בפני פריצה יש לימו את התמונה עבור אפליקציות קריטיות בארגון.

● השתמשו בפירוול ספציפי ל- Web-Web Application Firewall (WAF), שלמעשה מאפשר לארגונים למצוא ולחסום התקפות בשכבת האפליקציה. פירוול בעל מומחיות כזאת נחוץ בנוסף לפתרונות אבטחת רשת קונבנציונאליים אשר מגנים מפני התקפות ברמת הרשת בלבד. התקפות מתוחכמות ניתנות לחסימה רק על ידי אבטחה רב שכבתית. ככל שה-IT והאוטומציה נכנסים לחיי היום יום שלנו, כך גם תגדל כמות ורגישות המידע האישי והעסקי, השוכנים זה לצד זה בבסיס הנתונים של ארגונים שונים. אם נצרך לכך גם את התקפות הסייבר שהולכות ועולות בתחכום שלהן ובמספרן סביב העולם, ברור שהגיע הזמן שארגונים ייקחו צעדים אקטיביים לאבטחת המידע של הלקוחות שלהם, שנמצא תחת השגחתם. בניית אפליקציות מאובטחות, ביצוע שגרתי של מבחני פגיעות ושימוש בפירוול אפליקטיבי מודרני, כולם תורמים להגנה עמוקה שיכולה לקרב אותנו יותר לעמידה באתגר.

\* אלון גולדפיז, מהנדס מכירות בכיר, פורטינו ישראל

ההפרעה להכנסות של העסק היא רק חלק מהבעיה. עוצמתו של אתר האינטרנט של החברה היא גם חולשתו - הוא פתוח ונגיש לכולם. הנגישות הזאת הופכת את אתר האינטרנט למטרה טבעית לפושעי סייבר, האקרים ואקטיביסטים. התוצאה השלילית של פריצה ברורה - פגיעה במוניטין של החברה וגניבה של מידע רגיש, כדוגמת מספרי כרטיסי אשראי ומידע אישי.

## אתגרים באבטחת אתרי אינטרנט

אתרי אינטרנט הם יותר מדרך נוחה וקלה להגיע למידע או לרכוש מוצרים. יותר ויותר אפליקציות ארגוניות מבוססות על הרשת, והגישה אליהן היא דרך אותה תוכנת גלישה בה משתמשים צרכנים על מנת לרכוש מוצרים שונים. כתוצאה מכך, הסיכון שבגניבת מידע ארגוני רגיש הולך ועולה באופן דרמטי. הקושי באבטחת אתרי האינטרנט והאפליקציות שלהם טמון בארכיטקטורה ובדינאמיקה שלהם. בעוד אבטחת הרשת

היא יחסית ברורה, אתרי אינטרנט מורכבים ממאות ואפילו אלפי אלמנטים שונים הכוללים בין היתר כתובות אינטרנט, פרמטרים, קוקיז ועוד. יצירת מדיניות עבור כל אחד מהפרטים הללו באופן ידני היא משימה כמעט בלתי אפשרית. בנוסף, אתרי אינטרנט משתנים לעיתים תכופות, דבר שמקשה אף יותר לעדכן את מדיניות האבטחה בכל פעם מחדש.

הקושי באבטחת אתרי אינטרנט הופך חמור אף יותר בשל חולשות רבות במערכת ההפעלה של אתרי האינטרנט עצמם והאפליקציות שרצות עליה, אתגרים בפיתוח ויישום עדכונים, תיקונים בקוד ועדכונים אחרים, לצד לחץ של Time-To-Market. בנוסף, מאחורי רוב אתרי האינטרנט נמצאת תשתית מבוזרת המשרתת את אתר האינטרנט עצמו, דבר שהופך את התמונה למורכבת אף יותר. התוצאה: לעולם לא ניתן יהיה להניח שאפליקציות מבוססות רשת הן מאובטחות - הן דורשות אמצעי אבטחה עצמאיים.

## להגן על הנכסים המקוונים שלך

על מנת להגן על אתרי אינטרנט יש לנקוט בגישה הוליסטית, הכוללת את מבנה האתר ואת האפליקציות שלו, כמו גם את הרשת העומדת בבסיסו. הנה שלוש גישות ממוקדות שיעזרו לכם להגן טוב יותר על