SecAudit

תקן PCI-DSS מבולבלים? ...אנחנו לא!

חברות רבות, גם כאלה הפועלות בשגרה להגברת רמת אבטחת המידע, מוצאות עצמן מבולבלות אל מול דרישות ה -PCI (Payment Card Industry).

רקע

יש להבין תחילה את הרקע לכתיבת התקן ע"י קונסורציום חברות האשראי העולמי. כלקח מאירועי גניבת נתוני כרטיסי אשראי בעולם הוחלט על ידי חברות האשראי הבינלאומיות להנהיג מדיניות לשמירת נתוני כרטיסי האשראי. מועצת ה (Payment Card Industry) - PCIפרסמה תקן לאבטחת נתוני כרטיסי אשראי אשר נודע בשם DSS - PCI (Payment Card Industry - Data Security Standard)התקן מחייב כל גוף המעביר, מעבד או שומר נתוני כרטיסי אשראי ובתוך כך חברות סולקות, בתי עסק, אתרי מסחר אלקטרוני וספקי שירות צד שלישי, לעמוד בדרישות שהוגדרו.

מועצת ה PCI - מורכבת מחמש חברות האשראי הגדולות בעולם והינה הגוף הבלעדי המסמיך מבקרים מטעמם לבצע הסמכה לאותן חברות העונות להגדרות שנקבעו על ידי המועצה. חברות שאינן עומדות בדרישות התקן מסתכנות בקבלת קנסות והגבלת ביצוע עיסקאות ופעולות אשראי. כל אותן החברות מחוייבות לטיפול מקיף במערכות המידע לשם עמידה מלאה בתקן ובנוסף נדרשות לביצוע ביקורת על פי התקן אחת לשנה. ההסמכה לעמידה בתקן ניתנת לאחר ביצוע בדיקה מקיפה ומילוי כל דרישות התקן, כאשר הפעילות חייבת להתבצע על ידי גוף המוסמך על ידי המועצה לביצוע הביקורת וההסמכה - QSA) Qualified Security Assessors).בנוסף, מסמיכה מועצת ה PCI - חברות לביצוע בחינת פגיעויות (Vulnerability Assessment) לרשתות הארגונים הנדרשים להסמכה - ASV) Approved Scanning Vendors).המועצה מגדירה תקנים ודרישות עבור פיתוח אפליקציות ומוצרים המעבדים משדרים או שומרים מידע ונתוני כרטיסי אשראי.

אם כל למה PCI?

יישום דרישות התקן מעלה בצורה משמעותית את רמת האבטחה בארגון ואת רמת אבטחת נתוני כרטיסי האשראי המאוחסנים, מועברים או מעובדים. תקן ה PCI - כולל 6 פרקים ראשיים ו- 12 תתי פרקים המתייחסים לכלל היבטי אבטחת מידע הנדרשים מהארגון. הפרקים המופיעים בתקן כוללים: בניית רשת מאובטחת, הגנה על נתוני כרטיסי האשראי, ניהול פגיעויות, הטמעת בקרת גישה, פיקוח ובקרה מתמדת על רשת הארגון ותחזוקת מדיניות אבטחת מידע.

התקן מחלק את בתי העסק ל- 4 רמות דירוג המבוססות על כמות הפעולות המבוצעות על ידי הארגון בשנה. על פי רמת הדירוג, נקבעות הדרישות לעמידה בתקן. ככל שכמות הפעולות המבוצעות בכרטיסי אשראי גדולה יותר, הדרישה האבטחתית מקיפה ועמוקה יותר. הארגון מחוייב בביקורת ע"י חברה חיצונית על בסיס שנתי, סקירת הרשת לאיתור חולשות וביצוע מבחני חדירה יזומים.

לגבי מועדים לעמידה בתקן: עד למועד זה היו אמורים כל הארגונים (בכל הרמות) לעמוד בתקן. מאחר והחיים לא פשוטים כל כך, העבירה מועצת ה - PCIאת ההחלטה על עמידה במועד לחברת האשראי מולה אתם עומדים, כך שמדובר בתא ריך בר משא ומתן (לפחות חלקית). אם מעניין אתכם לקרוא זאת באתר ארגון ה PCI - הכנסו לכתובת הבאה:

https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf

אחת הסיבות העיקריות להגדרת התקן הועלתה כאמור כלקח מאירועי אבטחת מידע שונים בעולם, אירועים בהם נחשפו נתוני כרטיסי אשראי כתוצאה מאבטחה לקויה של המידע וכמובן מהתקפות מרובות וניצול פרצות במנגנוני האבטחה של הארגון על ידי גורמים עבריינים. גניבות מידע אלו הסבו נזקים גבוהים (בכסף ובמוניטין) לבתי העסק ולתעשיית כרטיסי האשראי עצמה.

אורן שני: "ארגון המיועד לבצע הסמכה חייב להבין כי התהליך אינו פשוט ומטרתו אחת - מניעת גניבת נתוני כרטיסי אשראי. לשם כך חייבת הנהלת הארגון להירתם למשימה, בעיקר כצורך עיסקי. סעיפי התקן הקשורים בהצפנת המידע ואיסוף דיווחי בקרה ממערכות, מצריך מהארגון משאבים, ביצוע התאמות הן באפליקציות התומכות והן בתשתיות התקשורת ומערכות הארגון. אי יישום דרישות התקן יגרמו לנזקים עתידים גדולים יותר. ההוצאות עבור עמידה בתקן זולות לאין שעור מההוצאות בעקבות דליפת המידע, שלא לדבר על פגיעה במוניטין הארגון."

שני מוסיף כי: "חברות רבות, גם כאלה הפועלות בשגרה להגברת רמת אבטחת המידע, מוצאות עצמן מבולבלות אל מול דרישות ה .PCI - ביכולתנו לתרגם את דרישות התקן ל"גובה העיניים", בצורה פשוטה ברורה ומעשית. פעילות זו לוקחת בחשבון את דרישות התקן אל מול עלויות התאמה, ומציגה ללקוח את האפשרויות המיטביות לביצוע, כאשר בפועל קיימת כל העת התייחסות לנושא עלות-תועלת ללקוח. לאחר הבנת המצב הקיים בארגון באשר לטיפול בכרטיסי האשראי מבוצע ניתוח פערים מקיף אל מול דרישות התקן ברמת המדיניות והנהלים, תשתיות התקשורת, מערכות ההפעלה, בסיסי הנתונים והאפליקציה. בשלב הבא מבוצע ליווי לשם סגירת הפערים, קודם ע"י רכיבים קיימים בכל אחרת מהרמות, לאחר מכן ע"י השלמות תפורות ללקוח ובשלב אחרון ע"י כלים חיצוניים. עם סגירת הפערים ועמידה מלאה בדרישות התקן, מסופק חזרה מענה מאושר לסגירת המעגל ."