תקן PCI DSS

רקע

פירוט התקן

יתרונות התקן

4 רמות בית העסק

שאלונים

לוחות זמנים

רקע

אבטחת מידע ירודה וגידול בפעילות לא חוקית הסבו לבתי עסק ותעשיית כרטיסי אשראי נזקים גבוהים בכסף ובמוניטין. חברות כרטיסי האשראי פיתחו תקן המכיל את כלל הדרישות להיבטי אבטחת נתוני כרטיס אשראי. התקן מחייב כל גוף שמעביר, מעבד או שומר נתוני כרטיסי אשראי חברות סליקה, בתי עסק וספקי שירות צד שלישי כאחד.

בעבר חברות האשראי הנהיגו נהלי אבטחת מידע פרטיים. הצורך בתקן אחיד ומבוסס נבע מהתובנה שבנושא אבטחת מידע תעשיית האשראי מחויבת לפעול בהתאמה, בנחרצות, וללא פשרות.
חברות האשראי חברו יחדיו והקימו את מועצת תעשיית האשראי (PCI Council)
ה Council הינו פורום עולמי פתוח שהוקם ע"י חמש חברות אשראי בינלאומיות ב 2006.
מטרת הארגון לפתח, לנהל, להפיץ, ולעדכן את תקן ה PCI.
החברות הבינלאומיות מכירות במועצה כגורם הבלעדי המאשר בודקי אבטחה לתקן ה PCI
(QSA and ASV).
Qualified Security Assessor and Approved Security Vendor
מועצת ה PCI קבעה נהלים ברורים ו 12 דרישות בהן כל ארגון המעביר, מעבד או שומר נתוני כרטיסי אשראי חייב לעמוד. 12 דרישות אבטחת המידע כוללות הסבר טכני מפורט המסביר דרכי פעולה לבית עסק.

פירוט התקן

1. התקנת ותחזוקת Firewall על מנת להגן על נתוני כרטיסי האשראי
2. אל תשתמש בסיסמאות ברירת מחדל של ספקי התוכנה הגן על נתוני כרטיס
3. הגן על נתוני כרטיס השמורים בבסיס הנתונים
4. הצפן תשדורת נתוני כרטיס העוברים ברשת הפעל תכנית ניהול פגיעות
5. השתמש ועדכן תוכנות אנטי וירוס
6. פתח ושמר מערכות ואפליקציות מאובטחות ישם מדיניות בקרת גישה יעילה
7. הגבל גישה של עובדיך לנתוני כרטיסי אשראי על בסיס תפקידם בחברה
8. הענק שם משתמש ייחודי לכל בעל גישה למחשב
9. הגבל גישה פיסית לנתוני כרטיסי האשראי פקח ובדוק את מערכותיך באופן שוטף
10. עקוב ופקח על הגישה למערכותיך ונתוני כרטיסי האשראי
11. בדוק באופן שוטף את מערכות אבטחת המידע שלך והתהליכים הרלוונטיים הפעל מדיניות אבטחת מידע
12. הפעל מדיניות אבטחת מידע אפקטיבית העונה על איומים קיימים ועתידיים

יתרונות התקן

הגנה בפני קנסות ותביעות מצד חברות האשראי הבינלאומיות במקרה של חדירת גורם עוין למערכות החברה וזליגת מידע (נתוני כרטיסי אשראי).
יישום תקן PCI הינו חלק מהטיפול השוטף בפעילות אבטחת מידע ויטופל במסגרת המשאבים שקיימים.
הגברת תחושת הביטחון של הצרכן, תרומה לשמירת וחיזוק מוניטין החברה.
יישור קו מול חברות מתחרות בחו"ל שכבר עומדות בתקן.

4 רמות בית העסק

1 ב.ע שמעביר יותר מ-6,000,000 עסקות בשנה ללא קשר לאמצעי העברת העסקה.
כל ב.ע שהותקף ע"י האקר או שסבל מהתקפה שהובילה לזליגת נתוני כרטיס.
כל ב.ע שחברת האם רואה לנכון לכלול ברמה אחת כולל הדרישות של רמה זו וזאת על מנת לצמצם את הסיכון.
כל ב.ע שחברת אם אחרת החליטה לקבוע כשייך לרמה אחת.
ב.ע ברמה זו מחויב בסקר סיכונים שנתי –AUDIT וסריקות רשת רבעוניות המבוצעות ע"י חברה (QSA) וחברה (ASV) שמוסמכות לכך ע"י מועצת ה- PCI

2 ב.ע שמעביר בין 1,000,000 ל 6,000,000 עסקות בשנה ללא קשר לאמצעי העברת העסקה.
ב.ע ברמה זו מחויב במילוי שאלון הערכה עצמית שנתי (SAQ) וסריקות רשת רבעוניות המבוצעות ע"י חברה (ASV) שמוסמכת לכך ע"י מועצת ה- PCI.

3 ב.ע שמעביר בין 20,000 ל 1,000,000 עסקות במסחר אלקטרוני בשנה.
ב.ע ברמה זו מחויב במילוי שאלון הערכה עצמית שנתי (SAQ) וסריקות רשת רבעוניות המבוצעות ע"י חברה (ASV) שמוסמכת לכך ע"י מועצת ה- PCI.

4 ב.ע שמעביר פחות מ- 20,000 עסקות במסחר אלקטרוני או פחות ממיליון עסקות רגילות בשנה.
ב.ע ברמה זו מחויב מילוי שאלון הערכה עצמית שנתי (SAQ) וסריקות רשת רבעוניות המבוצעות ע"י חברה (ASV) שמוסמכת לכך ע"י מועצת ה- PCI.

שאלונים והתאמתם לבית העסק שלך

סוג שאלון	תיאור
A	בתי עסק הפועלים ללא נוכחות כרטיס בלבד (עסקות במסמך חסר) ופעילות כרטיסי האשראי נעשית במיקור חוץ
B	בתי עסק המחוברים ישירות לשב"א ואינם שומרים נתונים
C	בתי עסק עם מערכות תשלום שמחוברות לרשת האינטרנט ואינם שומרים נתוני כרטיס
D	שאר בתי העסק שלא עונים לקריטריונים מעלה וגם כל נותני שרות צד ג'-SP שמותר להם למלא שאלון.

את השאלונים המלאים ניתן להוריד באתר מועצת ה PCI
www.pcisecuritystandards.org

לוחות זמנים

על מנת לעמוד ביעדי החברות הבינלאומיות ולהדביק את קצב המקבילים בחו"ל, החברה מחויבת ללוח זמנים צפוף ודורש.
בתי עסק ברמה 1
מועד לדיווח על סיום הפעילות (סקר פערים) 31/3/2009
מועד לדיווח על סיום הפעילות (סריקות) 31/12/2008
מועד אחרון לקבלת הסמכה 30/9/2009
בתי עסק ברמות 2,3,4
מועד לדיווח על סיום הפעילות (שאלון) 31/1/2009
מועד לדיווח על סיום הפעילות (סריקות) 31/12/2008
מועד אחרון לקבלת הסמכה 30/6/2009