PCI Compliance

אשר אלעזר, CISSP, CSSI, מנהל תחום אבטחת מידע, BDO זיו האפט

אחד הנושאים המרכזיים המדירים שינה מעיניהם של מומחי ומנהלי אבטחת המידע העובדים בחברות אשראי שונות, הוא מידת החשיפה של פעילות כרטיסי האשראי העוברת דרכם. הקידמה הטכנולוגית הביאה עימה שינוי בהרגלי הצריכה של הציבור אשר מתבטא בשימוש גובר והולך בשירותים מקוונים לצרכים שונים כגון תשלומים, קניות, העברת כספים, שימוש בשירותי מידע של חברת האשראי ועוד. שימוש מוגבר בטכנולוגיות אלו המשלבות פעילות בכרטיסי אשראי מגדיל את קשת האיומים: מגניבה של כרטיס אשראי ו"גיהוצו" עד לחסימתו, אנו מתקדמים לזיוף כ. אשראי בעזרת ציוד מתקדם, שימוש במספר כ. אשראי בקניה טלפונית בה אנו זקוקים רק למידע ללא כרטיס פיזי, חדירה למאגרי מידע של חברות האשראי לצורך גניבת זהויות ומספרי כ. אשראי, ניצול פרצות במערכות המידע של חברות האשראי לביצוע חיובים \ תשלומים לא חוקיים, פגיעה בפעילות חברת האשראי ע"י שיתוק מערכות מידע אינטרנטיות ועוד.

כאמור, כרטיסי האשראי נהפכו כיום לאמצעי התשלום המקובל והנוח ביותר הן בתשלומים בבתי עסק שונים, והן בתשלומים המבוצעים דרך הטלפון או דרך אתרים מאובטחים. נוחות השימוש איננה מגיעה ללא בעיות: גורמי פשיעה שונים, שוקדים בחריצות על מציאת דרכים לניצול חולשות אנוש, או חולשות קיברנטיות, כדי לשפר את מאזנם השנתי.
פעילות זו איננה ללא תוצאות חיוביות מנקודת ראותם של "הרעים והחרוצים". חיפוש קצר במנוע הידוע אחר מילות מפתח כגון: **RBS Worldpay**, **Hannaford Brothers**, או**Heartland Payment Systems**, יניב שפע של מידע די מדהים לגבי היקף הנזק אשר נגרם בתחום זה, והנזק הפוטנציאלי במידה ומקרים אלו יישנו ביתר חריפות. (מידע מדויק לגבי הפסדי חברות האשראי כתוצאה מפעילות פשיעה הקשורה לכ. אשראי ניתן לקבל, תמורת תשלום, באתר www.nilsonreport.com .

לעזרתם של ידידנו חסרי השינה מחברות האשראי נחלץ ארגון בשם PCI-SSC (Payment Card Industry – Security Standards Council) המכונה "Council". ארגון זה עוסק באכיפת תקן משותף לכלל חברות האשראי בנושא אבטחת כרטיסי האשראי, אופן השימוש בהם, אופן ייצורם ואף התוכנה בעזרתה נעשה השימוש.
ארגון זה צמח מתוך הבנה של חברות האשראי שהתמודדות משותפת מול שפע האיומים המשתכללים הינה חסכונית ויעילה יותר, ותקן אחד משותף עדיף על פני פיתוחים נפרדים כיון שהוא מקל על הסוחרים ומיושם בצורה אפקטיבית יותר. עד 2004 לכל חברת אשראי היתה תכנית נפרדת להתמודדות מול האיומים הקשורים לשימוש בכרטיסי האשראי ולמערכות המידע המעורבות בתהליכי הסליקה. ב 2004 הוקם ה "Council" ע"י חברות האשראי

המרכזיות: American Express, Discover Financial Services, JCB International, MasterCard Worldwide, Visa, Inc. הארגון עוסק כיום בהסדרת התקנים השונים של PCI, הכשרה של כוח אדם מקצועי, הגברת מודעות ופעולות אחרות.

מהו אם כן התקן?

ראשית נציין כי התקן הינו מחייב את לקוחות חברות האשראי ואי עמידה בו עלולה לגרום לקנסות כבדים ואף להשעיית שירותי סליקה מטעם חברת האשראי.
בישראל, תאריך היעד לעמידה בתקן לכלל הגורמים אליהם הוא מתייחס הוא סוף שנת 2009.

תקן ה PCI מורכב משלושה "תתי תקנים" המתייחסים כל אחד אל פן אחר של תחום כרטיסי האשראי. גרסה ראשונה של תקן ה PCI פורסמה ב 2006, ואילו הגרסה העדכנית הינה 1.2 אשר יצאה לאור בסוף 2008. במקביל לתקן עצמו מפרסם הארגון הנחיות והמלצות בתחומים שונים המשיקים לנושא כ. האשראי. (אתר ה Council – https://www.pcisecuritystandards.org) .

מרכיבי ה PCI:

1. **PCI-DSS**: Payment Card Industry – Data Security Standard, דרישות התקן הן בתחום השימוש בכרטיסי האשראי. תקן זה מחייב סוחרים וחברות סליקה בכרטיסי אשראי. בתקן זה קיימות 4 רמות סיווג כאשר כל רמה מכתיבה את טיב הבקרות הנדרשות לעמידה בסטנדרט. הבקרות מחולקות ל 12 תחומים החל מאופן הגדרת החוקים ב Firewall דרך ההגנות על ה DB בו מוחזקות רשומות כרטיסי האשראי וכלה בנהלי אבטחת מידע ובדיקות חדירה למערכות אשר בשימוש. החלוקה לרמות הסיווג מבוססת על מספר הטרנזקציות בכרטיסי אשראי המבוצעות ע"י הארגון \ הסוחר ומפורטות בהמשך.

2. **PCI PA-DSS**: Payment Card Industry Payment Application – Data Security Standard, דרישות התקן הן בתחום פיתוח ויישום התוכנה. תקן המחייב יצרני תוכנה לשימוש כרטיסי אשראי לעמידה בתנאים מוגדרים. המטרה המרכזית היא לוודא תהליך פיתוח מאובטח בקרב בתי התוכנה, וכן למנוע מצב אפשרי בו תוכנה אשר פותחה עומדת בסתירה לדרישות ה PCI-DSS.

3. **PCI PED**: Payment Card Industry – Approved PIN Entry Devices, דרישות התקן הן בתחום פיתוח ויישום החומרה. בתקן זה ישנן דרישות חומרה

מסוימות מיצרני כרטיסי האשראי והמסופונים לסוגיהם לגבי אופן האחסון וההגנה על המידע. חלק מהבדיקות נעשות במסגרת מעבדה מורשית על מנת לוודא את התאימות הנדרשת.

חלק זה של המאמר יציג את תקן ה PCI-DSS ודרישותיו, במאמרים הבאים יובאו החלקים הנוספים המרכיבים את ה PCI.

PCI-DSS

כאמור תקן זה מתייחס לסוחרים ולחברות סליקה. קיימות ארבע רמות סיווג עבור הסוחר או חברת הסליקה, כאשר לכל רמת סיווג מוגדרות בהתאמה הבדיקות הנדרשות, והגורם המוסמך לבצען. הסיווגים וכן הדרישות והגורם המבצע מפורטים בטבלה הבאה:

רמה	קריטריון לסיווג	סוג הבדיקה הנדרשת	ביצוע הבדיקה
1	סוחר המבצע מעל 6 מליון טרנזקציות בשנה.	• שנתי: הסמכה לעמידה בתקן PCI-DSS. • רבעוני: ביצוע סריקה לאיתור בעיות אבטחת מידע.	הסמכה ע"י גורם מורשה (QSA) סריקה ע"י גורם מורשה (ASV).
2	סוחר המבצע בין 150,000 ל - 6 מליון טרנזקציות בשנה.	• שנתי: מילוי שאלון הערכה עצמית • רבעוני: ביצוע סריקה לאיתור בעיות אבטחת מידע.	מילוי שאלון עצמאית או ע"י גורם חיצוני. סריקה ע"י גורם מורשה (ASV).
3	סוחר המבצע בין 20,000 ל - 150,000 טרנזקציות בשנה.	• שנתי: מילוי שאלון הערכה עצמית • רבעוני: ביצוע סריקה לאיתור בעיות אבטחת מידע.	מילוי שאלון עצמאית או ע"י גורם חיצוני. סריקה ע"י גורם מורשה (ASV).
4	סוחר המבצע עד 20,000 טרנזקציות בשנה.	**המלצה** למילוי השאלון וביצוע הסריקה.	מילוי שאלון עצמאית או ע"י גורם חיצוני. סריקה ע"י גורם מורשה (ASV).

שלב ראשון בתהליך ה PCI-DSS הוא שיוך הסוחר או החברה לקטגוריה המתאימה. לאחר מציאת הקטגוריה המתאימה אנו יכולים להסיק אילו בדיקות יש לבצע על מנת לעמוד בתקן. כפי שניתן לראות בטבלה הקודמת, ישנן שלוש בדיקות שונות אפשריות, ננסה לעמוד על מאפייני בדיקות אלו.

1. **שאלון הערכה עצמית – (Self Assessment Questioner – SAQ)**

שאלון זה מחולק למספר קטגוריות המותאמות לאופי העסק. יש לבחור את השאלון המתאים ולמלאו בצורה מדויקת ולאחר מכן להעבירו ל Council לצורך הערכה ובדיקה בליווי מסמכים נדרשים. הטבלה הבאה מציגה באופן בסיסי את החלוקה לסוגי עסקים וסוג השאלון המתאים, הסברים וקריטריונים מפורטים לגבי כל סיווג נמצאים באתר עצמו ואמורים לסייע לממלא השאלון לבצע את הסיווג המתאים.

מומלץ לבעלי העסקים השונים לתת לאיש מקצוע לבצע את הסיווג ולמלא את השאלון על מנת לייעל את העבודה ולהימנע מטעויות.

סיווג הסוחר	תיאור הסיווג	סוג השאלון - (SAQ)
1	סוחרים ללא כ. אשראי נוכח: מסחר דרך אינטרנט, דוא"ל, טלפון. כל העיבוד של המידע נעשה ע"י גורם אחר ולא ע"י הסוחר.	A
2	סוחרים עם עמדות תשלום עצמאיות (מכשירי ה"גיהוץ" הידניים), ללא אחסון נתוני כרטיס האשראי בצורה אלקטרונית.	B
3	סוחרים עם עמדות תשלום עצמאיות (Dial-up Terminal), ללא אחסון נתוני כרטיס האשראי בצורה אלקטרונית.	B
4	סוחרים עם אפליקציות תשלום המחוברות לאינטרנט, ללא אחסון נתוני כרטיס האשראי בצורה אלקטרונית.	C
5	כל שאר הסוחרים שאינם נכללים בקטגוריות קודמות או אלו אשר הוגדרו ע"י חברת האשראי כשייכים לקטגוריה זו.	D

2. **סריקה (Authorized Scanning Vendor – ASV)**

ה Council מחזיק ברשימה של ספקים המאושרים על ידו לביצוע סריקות ברשת הסוחר לאיתור בעיות הקשורות לאבטחת מידע. ספקים אלו נדרשים לעמוד בתנאים שונים אשר העיקרי שבהם הוא ביצוע סריקה בתשתית המועמדת לרשותם ע"י ה Council. תשתית זו מוגדרת מראש עם בעיות אבטחת מידע שהספק הנבחן אמור לאתר ולהתריע עליהן. הספק נבחן על:

- ניהול הבקשות לביצוע עבודות סריקה (Administration)
- ביצועי תוכנת הסריקה (Performance)
- רמת הדוחות המוצגים ללקוח (Reports)

אישור ה ASV הינו שנתי והספקים נדרשים לבצע את תהליך ההסמכה כל שנה מחדש.

3. **הסמכה על ידי גורם מורשה (Qualified Security Assessor – QSA)**

גם בתחום זה מנהל ה Council את רשימת הספקים המורשים לבצע הסמכות PCI-DSS, וגם כאן ישנן דרישות שונות בהן הספק מוכיח את יכולותיו וכישוריו. הספקים נדרשים להעביר את הארגון עצמו דרך מסכת של מסמכים ותנאים, להעמיד כוח אדם בעל הכשרה מקצועית מתקדמת בתחום אבטחת המידע או הביקורת: הסמכת CISSP, CISA או CISM הינה תנאי לקבלת הכשרה על ידי ה Council לצורך ביצוע ההסמכה.

על מנת לעבור את ההסמכה הארגון ייבדק בששת התחומים הבאים:

1. בנה ותחזק רשת מאובטחת
   a. התקן ותחזקה Firewall לצורך הגנה על מידע
   b. אל תשתמש בהגדרות ברירת מחדל של יצרנים לסיסמאות מערכת או להגדרות אבטחה אחרות
2. הגן על מידע בעל הכרטיס
   a. הגן על מידע מאוחסן (השתמש בהצפנה)
   b. הצפן תעבורת המידע של בעל הכרטיס או מידע רגיש אחר על תשתית ציבורית
3. תחזק תכנית לניהול פגיעויות (Vulnerabilities)
   a. השתמש בתוכנת אנטי וירוס ועדכנה בקביעות
   b. פתח ותחזק מערכות ואפליקציות מאובטחות
4. יישם אמצעי בקרת גישה חזקים
   a. הגבל גישה למידע על בסיס הצורך לדעת העסקי
   b. הקצה קוד גישה אישי יחודי לכל עובד בעל גישה למחשב
   c. הגבל גישה פיזית לנתוני בעלי כרטיס האשראי
5. נטר ובחן את הרשתות באופן סדיר
   a. עקוב ונטר אחר הגישה אל משאבי הרשת ונתוני בעלי כרטיס האשראי
   b. בחן את מערכות ותהליכי אבטחת המידע באופן סדיר
6. תחזק מדיניות אבטחת מידע
   a. תחזק מדיניות אשר מתייחסת לנושא אבטחת המידע

סיכום

נושא ה PCI מצריך הן הבנה ונסיון טכנולוגיים והן ידע בתחום אבטחת מערכות מידע וביצוע ביקורות. למרות שה Council מנסה לתת כלים וכללים ברורים עדיין יש מרחב לשיקול דעת

ולפרשנות של הכללים עצמם. לפיכך מומלץ לגופים הזקוקים להסמכה זו לבצע הערכה מוקדמת מדויקת ככל האפשר ביחס לצרכיהם כי ייתכן וחלק מהדרישות על פי התקן מתמלאות ע"י ביקורות אחרות, עמידה בתקנים אחרים, או תצורת מערכת מתאימה.

לוח הזמנים לעמידה בתקן הוא קצר (עד סוף 2009) ולכן מומלץ להתחיל את התהליך כבר כעת, חשוב לציין שכלל הפעילות, גם פעילות שהיא לכאורה פשוטה כגון מילוי שאלון הערכה עצמית (SAQ), היא פעילות מחייבת שיש בה נשיאת אחראיות כלפי חברות האשראי והלקוחות, ולכן מצריכה עבודה יסודית וכובד ראש.