שאלות נפוצות- FAQ

1 למה דורשים ממני לעמוד בתקן PCI DSS?

אין עוררין שנתוני כרטיס אשראי הם אטרקטיביים מאד לפורצי מערכות מידע (האקרים) . אנו עדים יותר ויותר לניסיונות וגם הצלחות בתחום זה אשר זוכות להד תקשורתי רב.תקן PCI DSS נועד להגן על הלקוחות שלך והאמון שיש להם באתר שלך (מוניטין בית עסק). אמון זה חיוני לנכונות של הלקוחות שלך "להפקיד בידיך" נתונים אישיים וכספיים. לכן כמעט בכל אתר תמצא מסמך מדיניות אבטחה-SECURITY POLICY.

לפי ניסיונן של חברות ייעוץ גדולות ושל המותגים הבינלאומיים- ויזה אירופה ומסטרקארד העולמי- מגזר סחר האלקטרוני מאוים במיוחד ע"י קהילת ההאקרים.לנוכח איום ממשי זה ויזה אירופה הוציאה הנחייה שעל כל בית עסק אינטרנטי לעמוד בתקן PCI DSS באופן מלא או לחלופין לבצע REDIRECTING של דף התשלום שלו לגורם מוסמך-SP (SERVICE PROVIDER) אשר עומד בתקן בעצמו. לאומי קארד, כזכיין של ויזה אירופה לסליקת כרטיסי ויזה, חייבת למלא אחרי הנחייה זו, ומכאן פנייתנו אליך.

2 מה זה REDIRECTING?

REDIRECTING הוא קוד אשר גורם לכך שדף התשלום של אתר אינטרנט נפתח בפועל באתר של ספק שרות - נותן שרות צד ג' או באנגלית SP.שרות זה ידוע גם כ- HOSTED PAYMENT PAGE

.

3 מה היתרונות ב-REDIRECTING?

בית עסק אשר משתמש בשרות REDIRECTING נדרש למלא שאלון מקוצר (13 שאלות בלבד) – A (נמצא בחוצץ זה). בית העסק נדרש כמובן לעמוד בכל 13 סעיפי התקן הרלוונטיים במקרה זה. לעומת זאת בית עסק אשר לא משתמש בשרות REDIRECTING נדרש למלא שאלון מלא (למעלה מ- 200 שאלות)- D ו**לעמוד בכל תקן PCI DSS** על כל המשתמע מכך - שעות עבודה רבות והוצאות לא מבוטלות לסגירת פערים. בנוסף בית העסק גם נדרש לבצע סריקות רשת רבעוניות (בתשלום) באמצעות חברה אשר מוסמכת לכך- ASV.

4 מי מוסמך לבצע עבור בית העסק שרות REDIRECTING ?

רק ספק שרות ברמה הגבוהה ביותר- SERVICE PROVIDER LEVEL ONE מורשה ע"י לאומי קארד לספק שרות REDIRECTING לבית עסק אשר סולק איתנו. רק SP- LEVEL ONE עובר בדיקה והסמכה ע"י חברה יעודי- QSA אשר בסוף התהליך מנפיקה לו תעודת הסמכה. תעודות אילו מקלות על בית העסק לוודא שה-SP אכן עומד בתקן PCI DSS

5 מה הדרישות של חברות האשראי מבית עסק שבחר ב-REDIRECTING?

א. שאלון A- עליך למלא שאלון A (ניתן בעברית) כאשר יש להשיב בחיוב לכל השאלות בו או לחלופין ניתן לציין שהשאלה לא רלוונטית עבורך.הסבר על מילוי השאלון ניתן למצוא בתחילת מסמך השאלון בחוצץ זה.
ב. אישור REDIRECTING- צרף לשאלון אישור בכתב מחברת ה-SP שאכן נרשמת לשרות REDIRECTING.

את כל החומרים המוזכרים בסעיפים א+ב יש לשלוח (בעדיפות ראשונה) לפקס מספר: 03 -6178997. אם אין לך גישה לפקס ניתן לשלוח לכתובת המייל:

pci@leumi-card.co.il

6 מה הדין לגבי אתר שאין בו סליקה ישירה של כרטיסי אשראי

חובת עמידה בתקן PCI DSS חלה גם כאשר אין סליקה ישירה של כרטיסי אשראי באתר. אם אין סליקה בפועל באתר שלך דהינו אתה "אוסף" כל פעם את הנתונים שהושארו ע"י הלקוחות שלך ומחייב אותם במסוף בחנות/משרד ע"י הקלדת מספר הכרטיס+תוקפו עליך לבחור בין שרות TOKENISATION+REDIRECTING (ראה מטה-שאלה 7 להסבר אודות TOKENISATION) לבין הסרת האפשרות להשאיר נתוני כרטיסי אשראי באתר.במקרה השני ניתן לבקש מהלקוח להשאיר מספר טלפון בלבד (ליד) ולחזור אליו יותר מאוחר כאשר את נתוני כרטיסי האשראי תקבל במעמד השיחה.שים לב שלפי תקן PCI DSS חל איסור לשלוח נתוני כרטיסי אשראי במייל ללא הצפנה לכן **אין** לבקש מהלקוח לשלוח נתונים אילו במייל.

7 <u>מה הדין לגבי אתר עם עסקאות חוזרות/הוראות קבע שבו הלקוחות לא נכנסים כל פעם מחדש?</u>

במקרה כזה מעבר לשירות REDIRECTING תברר מול ה- SERVICE PROVIDER שלך האם הוא גם מוסמך לספק שירות TOKENISATION. מדובר בשרות שבו אתה מעביר לו (ל-SP) את מספר כרטיס האשראי ובחזרה אתה מקבל מספר אחר שהוא חסר משמעות- TOKEN.אתה שומר רק את ה- TOKEN הזה ובכל פעם שיש צורך לחייב /לזכות את הלקוח אתה שולח בחזרה ל-SP את ה- TOKEN עם הוראה מתאימה –חיוב/זיכוי והסכום הרלוונטי.

8 <u>מה עליי לעשות אם למרות הכל אני עדיין מעדיף לעמוד בתקן PCI DSS לבדי ללא שרות REDIRECTING</u>

אם למרות כל הקשיים והחסרונות שמפורטים בשאלה 3 מעלה אתה עדיין מעדיף לעמוד בכל תקן PCI DSS יש לשלוח בהקדם מייל עדכון על כך ללאומי קארד לכתובת המייל

pci@leumi-card.co.il

יש לפרט במייל את הסיבות לכך ונציג שלנו יהיה איתך בקשר על מנת לדון בנושא

9 <u>אם לאחר קריאת כל החומר הרלוונטי בחוצץ זה אני עדיין זקוק לעזרה / יש לי שאלה נוספת - למי אני יכול לפנות?</u>

למרות הניסיונות שלנו לספק את כל החומר הרלוונטי ולחשוב על כל השאלות/בעיות שעלולות לעלות תמיד יהיה פרט שלא חשבנו עליו או שלא הובהר כהלכה.במקרה כזה אתה מוזמן לפנות לכתובת המייל:

pci@leumi-card.co.il

ניתן גם להתקשר לטלפון 03-6178550 ולדבר עם נציג שלנו – בן

אגף משאבי אנוש, ניהול סיכונים ורגולציה
מחלקת ניהול סיכונים ורגולציה