דצמבר 2013

מידעון PCI קומסק – דצמבר 2013

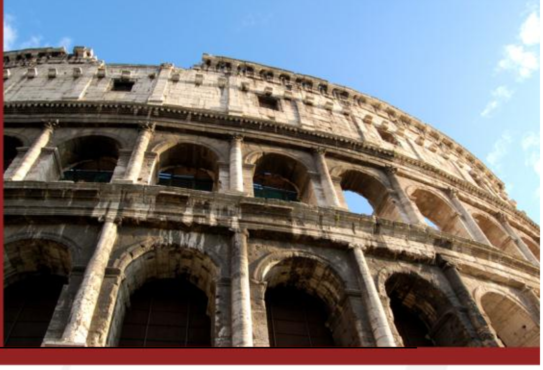
דבר העורך

שלומות,
החודשים האחרונים היו גדושים בחדשות, ארועים ושינויים, אך ללא ספק העיקרי שבהם הוא ההכנות וההערכות לפרסומה הקרוב של גרסה 3.0 של תקן PCI DSS.
בכנס מיוחד שערכה קומסק לציבור לקוחותיה בנושא הגרסה החדשה של התקן, הוצגו השינויים שבגרסה החדשה, ונדונו ההשלכות והמשמעויות שלהם על תהליך העמידה בתקן.
ציון דרך חשוב נוסף הינו הסמכתו של פתרון ראשון לתקן P2PE ואישורו על ידי מועצת PCI, דבר שללא ספק ייתן דחיפה משמעותית לנושא ה- P2PE בעולם אבטחת התשלומים ולעמידה בתקן מצד ארגונים שיעשו שימוש בפתרונות אלה באופן רחב.
אנחנו מאחלים לכם קריאה נעימה ומעודדים אתכם לפנות אלינו בכל הערה, הארה או שאלה, בכתובת הבאה : ComsecQSA@comsecglobal.com.

זרקור על.... גרסה 3.0 של תקן PCI DSS!

כפי שהבטחנו, אתם – לקוחותינו – הייתם הראשונים להיחשף לגרסת התקן החדשה, PCI DSS 3.0, בכנס יחיד מסוגו שערכנו ב- 24.10, ובו הצגנו את השינויים בגרסה החדשה ואת משמעויותיהם אליכם, הארגונים העומדים בתקן.
ב- 7 לנובמבר פורסמה רשמית גרסה 3.0 של התקן. השינויים, חלקם מהותיים, רובם ככולם בעלי מטרת-על להפוך את התקן לגמיש ומותאם ספציפית לכל ארגון וארגון, ולהתמקד בהנחלת והטמעת אבטחת מידע בארגון, כולל הבנה ומודעות לבקרות הנדרשות, ולא רק עמידה בתקן ובדרישותיו.
בכך נושאת גרסאת התקן החדשה את דגל המעבר מ"**עמידה בתקן" לאבטחת מידע**, באמצעות מספר דגשים עיקריים, השזורים בשינויים בה :

1. **גמישות ביישום דרישות התקן**
   a. במקרים מסוימים, מתן אפשרות ליישום בקרות חלופיות שוות ערך לדרישה ספציפית (WAF, סיסמאות, לוגים).
   b. מתן משקל גדול יותר לפרשנותו ושיקול הדעת של ה- QSA.
   c. גמישות מול חוזק- החמרה במתודולוגית הבדיקה והתיעוד המצופים מה- QSA כדי לוודא יישום.
2. **הסברה ומודעות לאבטחת מידע ודרישות תקן- PCI**
   a. דגש על תחזוקת העמידה בתקן כחלק מפעילות הארגון השוטפת (BAU) – בין הסמכות.
   b. דגש על הבנת הכוונה מאחורי הדרישה (לא "לעמוד בסעיף").
   c. הדרכות מודעות לנושאי אבטחה חדשים (סיסמאות, פיתוח).
   d. לכל דרישה תוצמד דרישה לתיעוד רלוונטי ומסמכים.
3. **אחריות משותפת וחלוקת סמכויות**
   a. מיפוי וחלוקת סמכויות כחלק מהעמידה בתקן.
   b. העברת אחריות לספקי השירות ולגורמי צד ג' וקבלת התחייבות לעמידה בדרישות התקן.
   c. יותר "שיניים" בהסכמים עם גורמי צד ג'.
   d. הרחבת הדרישה לעמידה בתקן מארגוני צד ג' (ספקי Hosting, אינטגרטורים, אחסון ועוד).



שאל את ה- QSA – האם נתוני כרטיסי אשראי מוצפנים באתר חיצוני נכללים בסביבת נתוני כרטיסי האשראי?

סעיף 3.4 של תקן PCI DSS מנחה להגן על נתוני כרטיסי האשראי (מס׳ הכרטיס- PAN), באשר הם נשמרים. בכלל זה מסדי נתונים, קבצים שטוחים, לוגים ואחרים, גם באותם המקרים כאשר הם נשמרים על מדיית גיבוי, כגון קלטת.

בהמשך לזה, דרישת התקן לפיה יש להגן על נתון ה- PAN באמצעות הצפנה, חיתוך (Truncation), טוקניזציה או גיבוב (Hash) , תקפה גם כאשר המידע נשמר במדיית גיבוי.

עם זאת, אחד השינויים המבורכים שהביא תקן P2PE לעולם אבטחת התשלומים בכללותו, הינו היכולת להתחשב בכך שהגישה למפתחות ההצפנה נפרדת מהגישה למידע המוצפן. ולכן, תקן PCI DSS מאפשר כיום להחשיב נתוני כרטיס אשראי מוצפנים כמחוץ ל- Scope כאשר, *ורק כאשר*, מובטח כי לישות המחזיקה במידע המוצפן אין גישה למידע האמיתי ולתהליך ההצפנה, ואין לה את היכולת לבצע פענוח של המידע- אין לה מפתחות הצפנה בסביבה ואין לה גישה לסביבה בה נשמרים מפתחות ההצפנה.
ולכן, במקרים בהם הנתונים המוצפנים נשמרים בתנאים מאובטחים במתקן חיצוני או נפרד, הם נחשבים מחוץ לסביבת נתוני האשראי של הארגון, ולא חלות עליהם שלל בקרות האבטחה הרגילות כגון לוגים, הקשחה, החלפת מפתחות ועוד. כמובן, עדין יש לשמור על אבטחה סביבתית ועל בקרות גישה ראויות מצד ספק האחסון או חוות השרתים, כפי הנדרש בתקן.

חדשות ועדכונים

P2PE – הוסמך ואושר הפתרון הראשון!

בסוף אוקטובר האחרון, כמעט שנה מאז פורסמה גרסתו האחרונה של תקן P2PE – Point to Point Encryption, אושר על ידי מועצת PCI פתרון P2PE ראשון מוסמך לתקן. הפתרון עצמו, מבית החברה האיטלקית לשרותי תשלום EPS (European Payment System), מסתמך על מסופוני Ingenico. במועצת PCI מאשרים כי בחודשים הקרובים נראה פתרונות נוספים שעברו הסמכה ורשומים ברשימת פתרונות- P2PE מוסמכים. במקביל, נראה ארגונים בתחום הקמעונאות, מלונאות, תיירות, וסקטורים נוספים, מטמיעים את הפתרונות כדי להגיע לעמידה יעילה וחסכונית בתקן PCI DSS.

הסמכות PA-DSS בגרסה 1.2 אינן בתוקף

החל מתאריך ה- 28 לאוקטובר, הסמכות מוצרים לתקן PA-DSS בגרסאות מוקדמות מגרסה 2.0 (1.2, 1.2.1 וכד׳) – כבר אינן תקפות ויש צורך להסמיכן מחדש לתקן PA-DSS בגרסה 2.0.

על בתי תוכנה וארגונים המפתחים מוצרים ואפליקציות שאושרו לתקן זה בגרסאות המוקדמות לבצע הערכה מחודשת של המוצר בהתאם לגרסה הנוכחית ולעבור הסמכה ואישור מחודשים של המוצר על ידי PA-QSA.

תקן PCI... גם ברוסית!

לאחרונה הקימה מועצת PCI אתר מיוחד וייעודי לתקן PCI בשפה הרוסית, הכולל תרגום מלא של מסמך התקן הרשמי והמלא ומסמכים תומכים רבים - כולם מתורגמים במלואם לשפה הרוסית. אנו מקדמים בברכה את עובדת זמינותם של חומרים אלה גם מכאן בישראל, בה קהל רב של דוברי רוסית שימצאו אותם לעזר רב. למתעניינים – אתר תקן PCI בשפה הרוסית : http://ru.pcisecuritystandards.org/minisite/en/.