دليلك إلى معايير أمن بيانات الدفع باستخدام البطاقات (PCI DSS)

بنك أبوظبي التجاري
ADCB
MERCHANT SERVICES

المحتويات

مقدمة

نحن ملتزمون في بنك أبوظبي التجاري بتزويد التجار الذين نتعامل معهم بكافة المساعدات لتمكينهم من حماية أعمالهم من التهديد المتنامي لإمكانية إنتهاك بيانات الحسابات، إذ يلجأ المجرمون الذين ينتهكون بيانات الحسابات إلى إستخدام أساليب ووسائل حديثة ومتطورة بإستمرار للحصول على معلومات حسابات العملاء. وبناء عليه، يكون من الأهمية بمكان أن يقوم التجار بتطبيق ضوابط قوية للتقليل من إمكانية الوقوع فريسة لهذا النوع من التحايل والإنتهاك إلى أدنى حد ممكن. معايير أمن بيانات الدفع بإستخدام البطاقات هي عبارة عن مجموعة من المتطلبات الشاملة لتحسين طرق حماية بيانات حسابات الدفع وتشكل أفضل الممارسات في مجال بطاقات الدفع بالنسبة لأي شركة تقوم بتخزين و/أو معالجة و/أو إرسال بيانات حملة البطاقات. وبما أنك أحد التجار، يكون من الضروي أن تفهم هذه المعايير وتقوم بتطبيق ضوابط في بيئة أعمالك لتفادي العقوبات المالية المحتملة علاوة على تكاليف التحقيقات والدعاية السلبية لأعمالك في وسائل الإعلام بسبب تعرضك لإنتهاك بيانات الحسابات. ويكون من المهم أيضاً أن تتأكد من أن أي كيان طرف ثالث يقوم بتخزين و/أو معالجة و/أو إرسال بيانات حسابات حملة البطاقات بالنيابة عنك يطبق معايير أمن بيانات الدفع بإستخدام البطاقات. لقد تم وضع وتطوير هذه المعايير بواسطة مجلس معايير أمن بيانات الدفع بإستخدام البطاقات(PCISSC) وقد تم تضمينها بشكل رسمي في برامج أمن البيانات على موقع ماستركارد (SDP) وبرامج أمن معلومات الحسابات لدى فيزا .(AIS)هذه المعايير تنطوي على العديد من الأوجه الأمنية التي تتضمن متطلبات لإدارة أمن المعلومات وسياسات وإجراءات وهيكلة للشبكة وتصميم للبرمجيات وإجراءات وقائية هامة أخرى. وتتكون معايير أمن بيانات الدفع بإستخدام البطاقات من ٦ مبادئ رئيسية مصحوبة بإثنى عشر مطلباً. وتنطبق هذه المعايير على كافة التجار، إلا أن نطاق التقييم يختلف على أساس حل أمن المعلومات الذي تستخدمه وكيفية إدارة وتشغيل أعمالك. ويمكن الإطلاع على هذه المتطلبات في الصفحة التالية.

ما هي المتطلبات الإثنتى عشرة الرئيسية لمعايير أمن بيانات الدفع بإستخدام البطاقات

يظهر الجدول التالي المعايير الرئيسية

معايير أمن بيانات الدفع بإستخدام البطاقات	
بناء والحفاظ على شبكة آمنة	١- تركيب وصيانة جدار ناري لحماية البيانات ٢- عدم إستخدام إعدادات ثابتة موردة من قبل بائعين بخصوص نظام كلمات المرور وإعدادات الحماية الأخرى.
حماية بيانات حملة البطاقات	٣- حماية البيانات المخزنة الخاصة بحملة البطاقات. ٤- تشفير عمليات إرسال بيانات حملة البطاقات والمعلومات الحساسة من خلال الشبكات العامة المفتوحة.
الإحتفاظ ببرنامج لإدارة إمكانية إنتهاك البيانات	٥- إستخدام برمجيات مكافحة الفيروسات وتحديث تلك البرمجيات بإنتظام. ٦- تطوير وإدامة أنظمة وتطبيقات آمنة.
تطبيق إجراءات قوية للتحكم بالدخول	٧- حظر الوصول إلى بيانات حملة البطاقات وإقتصاره على الأشخاص الذين يحتاجون إلى الإطلاع على تلك البيانات ٨- تحديد هوية فريدة لكل شخص لديه حق الدخول إلى نظام الحاسب الآلي. ٩- حظر الوصول الفعلي إلى بيانات حملة البطاقات
متابعة وإختبار الشبكات بإنتظام	١٠- تتبع ومراقبة كافة عمليات الوصول إلى مصادر الشبكة وبيانات حملة البطاقات. ١١- إختبار أنظمة وإجراءات وعمليات الحماية بإنتظام.
الإحتفاظ بسياسة لأمن المعلومات	١٢- الإحتفاظ بسياسة تتعامل مع موضوع أمن المعلومات.

وفر الحماية اللازمة لأعمالك

الإلتزام بمعايير أمن بيانات الدفع بإستخدام البطاقات يقلل بشكل كبير جداً من إمكانية التعرض لحالات إنتهاك بيانات الحسابات وبالتالي حماية سمعة أعمالك والحفاظ عليها.

ما هو إنتهاك بيانات الحساب؟

حالة إنتهاك بيانات الحساب هي تلك الحالة التي يحصل فيها شخص غير مفوض أو أشخاص غير مفوضين على إمكانية الوصول إلى بيانات حامل البطاقة المحتفظ بها في بيئة أعمالك سواء على وسائط إلكترونية أو بطريقة ورقية. ويمكن التعرف على هذه الحالات بالعديد من الطرق، بيدا أنه عادة ما يتم إكتشافها قبل إستخدام البطاقات بطريقة إحتيالية في مكان أخر. وفور الإبلاغ عن أي حالة إنتهاك محتملة لبيانات الحسابات، يجب حضور أحد محققي الأدلة الجنائية إلى الموقع لتحديد مصدر الإنتهاك والتعرف على كمية بيانات حامل البطاقة التي تم سرقتها (الصفحة ٣).

ما هي الأثار المحتملة لأي حالة من حالات إنتهاك بيانات الحسابات؟

إذا وقعت ضحية لعملية تلاعب بيانات الحسابات، فإنك تكون عرضة للعقوبات المالية وإيقاف أو أنهاء أعمال محلك التجاري بالإضافة إلى التعرض لمخاطر الإضرار بسمعتك التجارية وكذلك يصبح من المتعين عليك القيام بمهام تدقيق إضافية بصفة مستمرة. لقد كان هناك دائماً الكثير من الأمثلة على حالات إنتهاك بيانات الحسابات في جميع أنحاء العالم حيث تعرضت جميع الأعمال والشركات الصغيرة منها والكبيرة أيضاً لهذا النوع من التحايل. ومن المهم إدراك أن المجرمين لا يستهدفون أي نوع معين من الأعمال، بل يقومون بإستغلال أي مواطن ضعف في أنظمة الدفع فور التعرف عليها.

من أين أبدأ؟

يمكن الإطلاع على معايير أمن بيانات الدفع بإستخدام البطاقات على الموقع الإلكتروني
www.pcisecuritystandards.org

ونحن نوصي بقيامك بعمل تحليل الفجوة من خلال تعبئة إستبيان التقييم الذاتي المعني، وعندما يلزم، تعيين مقاول مسح معتمد لإجراء إختبار القابلية للإنتهاك. ويمكن الحصول على نسخة من إستبيان التقييم الذاتي وقائمة بمقاولي المسح المعتمدين من على الموقع الإلكتروني الخاص بمعايير أمن بيانات الدفع بإستخدام البطاقات. ويمكن الإطلاع على مزيد من المعلومات عن إستبيانات التقييم الذاتي في الصفحة (٧) من هذا الكتيب.

ما هي متطلبات الإمتثال الخاصة بي؟

يشكل الإمتثال لمعايير أمن بيانات الدفع بإستخدام البطاقات جزءاً من إتفاقية التاجر التي قمت بتوقيعها، بيدأن متطلبات التحقق من هذا الإمتثال تختلف على أساس عدد المعاملات التي تقوم بتنفيذها سنوياً والحل المالي الذي تستخدمه. وبالإضافة إلى ذلك، فإن إستخدام الأطراف الثالثة الملتزمة بمعايير أمن بيانات الدفع بإستخدام البطاقات يشكل أيضاً جزءاً من إتفاقية التاجر التي قمت بتوقيعها (الصفحة ٤).

كيف أحدد متطلبات التحقق من الإمتثال؟

تحتفظ كل من ماستركارد وفيزا بمستويات معاملات مختلفة فيما يتعلق بتنظيم المتطلبات. وتقوم متطلبات التحقق من الإمتثال الخاصة بنا على أساس تلك الصادرة عن ماستركارد أو فيزا وهي المتطلبات التي يمكنك الإطلاع عليها عبر الإنترنت أو من خلال مقالات أخرى منشورة في خطط البطاقات ومعايير الأسواق.

وسيقوم بنك أبوظبي التجاري بمراجعة عدد المعاملات التي تقوم بتنفيذها سنوياً وسوف نقوم بإبلاغك إذا إحتجنا إلى التحقق من إمتثالك للمعايير كتاجر من المستوى الأول أو الثاني أو الثالث. وفي جميع الأوقات، يكون لمستويات معايير أمن بيانات الدفع بإستخدام البطاقات الخاصة ببنك أبوظبي التجاري الأولوية على مستويات ماستركارد وفيزا. ونحن نحتفظ بحق إعادة تصنيف مستواك في أي وقت لأي سبب كان.

ما هو إستبيان التقييم الذاتي؟

إستبيان التقييم الذاتي هو عبارة عن أداة للتحقق من الالتزام بالمعايير مصممة لمساعدة التجار غير المطالبين بالخضوع إلى تقييم أمني بالموقع أثناء التقييم الذاتي للتأكد من مدى إلتزامهم بمعايير بيانات الدفع بإستخدام البطاقة. وهناك العديد من إستبيانات التقييم الذاتي التي تناسب بيئات عمل مختلف التجار، منها على سبيل المثال حلول النقاط الطرفية المستقلة وحلول التجارة الإلكترونية المعهود بها بالكامل إلى مقاول خارجي. ويتعين عليك تعبئة إستبيان التقييم الذاتي الذي يتناسب مع أعمالك، وإذا ساورك أي شك، يتعين عليك تعبئة إستبيان التقييم الذاتي (د). ويمكن الإطلاع على إستبيان التقييم الذاتي وتنزيله من الموقع الإلكتروني الخاص بمعايير أمن بيانات الدفع بإستخدام البطاقات.

يظهر الجدول التالي مختلف أنواع إستبيانات التقييم الذاتي:

نوع إستبيان التقييم الذاتي	البيان	إستبيان التقييم الذاتي
١	عدم وجود البطاقة (التجار الذين يستخدمون التجارة الإلكترونية أو الأوامر من خلال البريد / الهاتف، جميع وظائف بيانات حملة البطاقات).	(أ)
٢/٣	هذا لا ينطبق أبداً على تجار البيع المباشر للعملاء وهم التجار الذين لا يحتفظون بوسائل إلكترونية لتخزين بيانات حملة البطاقات أو التجار الذين يستخدمون النقاط الطرفية المستقلة دون التخزين الإلكتروني لبيانات حملة البطاقات.	(ب)
٤	التجار الذين يحتفظون بأنظمة نقاط البيع المرتبطة بالإنترنت دون تخزين إلكتروني لبيانات حملة البطاقات .	(ج)
٥	جميع التجار الآخرين (غير المتضمنين في الأنواع من ١ إلى ٤ أعلاه) وجميع مزودي الخدمات.	(د)

ما هو إختبار القابلية للإنتهاك؟

الغرض من إختبار القابلية للإنتهاك هو التأكد من أن أنظمتك محمية من التهديدات الخارجية مثل الدخول غير المصرح به أو هجمات القراصنة أو الفيروسات الضارة. وتقوم أداة المسح بإختبار كافة معدات شبكاتك وأنظمتك وتطبيقاتك للتعرف على أي مواطن ضعف يمكن من خلالها التلاعب بالمعلومات. وهذه الإختبارات والمسوحات مصممة بحيث لا تكون مخترقة للشبكات أو المعلومات ويجب تنفيذها بواسطة مقاول مسح معتمد. وعادة ما لا يكون إجراء إختبار القابلية للإنتهاك مطلوباً بالنسبة للتجار الذين يستخدمون الأجهزة الطرفية المستقلة. أما الإختبارات الدورية الربع سنوية فهي ضرورية للتأكد من إستمرار أنظمتك وتطبيقاتك في توفير مستويات مناسبة من الأمن والحماية للمعلومات. ويمكن الحصول على القائمة الحالية لمزودي خدمات المسح المعتمدين من على الموقع الإلكتروني الخاص بمعايير أمن بيانات الدفع بإستخدام البطاقات.

ما هو تقييم أمن المعلومات في الموقع؟

إذا كنت مطالباً بتعبئة إستبيان تقييم بالموقع، فإنك تحتاج إلى اللجوء إلى خدمات مُقيم أمن معلومات مؤهل ومعتمد من قبل مجلس معايير أمن بيانات الدفع بإستخدام البطاقات مرة كل سنة للتحقق من إمتثال أعمالك لمعايير أمن بيانات الدفع بإستخدام البطاقات. وإذا كانت أعمالك تطلب إجراء تقييم سنوي في الموقع، فإنك قد ترغب في تضمين متطلبات معايير أمن بيانات الدفع بإستخدام البطاقات ضمن إجراءات التدقيق السنوي المعتادة لأعمالك بغرض التقليل من التكلفة. وبما أنه من المرجح أن تصبح هذه التكلفة من بين التكاليف المتكررة، فإننا نوصي بتخصيص مبلغ في الموازنة للقيام بمراجعة هذه المعايير كجزء من مصاريفك السنوية. ويجب عليك إبلاغنا بمُقيم أمن المعلومات المعتمد الذي تقترحه ومواعيد إجراء التقييم بالموقع وخطة التحقق من الإمتثال لهذه المعايير.

ما الذي يتعين علي فعله إذا لم أكن ملتزماً بالمعايير ؟

بعد تعبئتك لإستبيان التقييم الذاتي، قد تكتشف أنه هناك بعض الإجراءات المتبعة في بيئة أعمالك غير المطابقة لمعايير أمن بيانات الدفع بإستخدام البطاقات. وفي هذه الحالة، يكون من الضروري أن تقوم بتطوير خطة تحدد الإجراءات التي يتعين إتخاذها بخصوص العناصر غير المطابقة للمعايير بالإضافة إلى الإطار الزمني التقديري لإتمام كل من هذه الإجراءات. وإذا كنت تاجر غير ملتزم من المستوى الأول أو الثاني أو الثالث، فإنك مطالب بتقديم خطة إصلاح من خلال أداة منهج تحديد الأولويات بنهاية كل ربع سنة.وبتحقيق التقدم اللازم نحو الإلتزام بهذه المعايير، فإنك تمنح نفسك وأعمالك أفضل فرصة ممكنة لتفادي العقوبات المترتبة على عدم الإمتثال.

أداة منهج تحديد الأولويات

تم تطوير أداة منهج تحديد الأولويات بواسطة مجلس معايير أمن بيانات الدفع بإستخدام البطاقات لمساعدة التجار غير الملتزمين بتحديد أولويات إجراءاتهم الإصلاحية. وتقوم أداة منهج الأولويات بتقسيم متطلبات إجراءات حماية بيانات الدفع بإستخدام البطاقات إلى ٦ أعمال رئيسية تحدد تلك المتطلبات التي تحتاج إلى العناية القصوى. ويمكن الإطلاع على أداة منهج تحديد الأولويات على الموقع الإلكتروني الخاص بمعايير أمن بيانات الدفع بإستخدام البطاقات.

ما هي متطلبات تطبيقات الدفع؟

إذا قمت بإستخدام أي من تطبيقات البرمجيات الجاهزة المتاحة بالأسواق يجب عليك التأكد من توافقها مع معايير أمن معلومات تطبيقات الدفع. وقد تم تطوير معايير أمن معلومات تطبيقات الدفع بواسطة مجلس معايير أمن بيانات الدفع بإستخدام البطاقات بغرض التأكد من إلتزام بائعي البرمجيات والجهات الأخرى التي تقوم بتطوير تطبيقات الدفع وتخزين و/أو معالجة و/أو إرسال بيانات حملة البطاقات بالعمل في بيئة متوافقة مع معايير أمن بيانات الدفع بإستخدام البطاقات. ويمكن الحصول على قائمة بتطبيقات الدفع المتوافقة مع هذه المعايير من على الموقع الإلكتروني الخاص بمعايير أمن بيانات الدفع بإستخدام البطاقات ويقتصر أي تطبيق دفع مطور داخلياً بالشركة أو تم تعديله بشكل كبير ليفي بمتطلبات الشركة على نطاق أعمال ومتطلبات التاجر أو مزود خدمة معايير أمن بيانات الدفع بإستخدام البطاقات وليس من المطلوب أن يكون متوافقاً مع معايير أمن بيانات تطبيقات الدفع.

ما الذي يتعين علي القيام به في حالة حدوث إنتهاك لبيانات حساب؟

لمنع خسارة المزيد من البيانات، يجب عليك إبلاغ بنك أبوظبي التجاري فوراً وفي غضون ٢٤ ساعة عن طريق مدير العلاقات المصرفية الذي تتعامل معه بأنك تشك في حدوث حالة إنتهاك لبيانات الحسابات وإجراء تحقيقات دقيقة في الحالة المشكوك فيها أو المؤكدة لخسارة أو سرقة بيانات حامل البطاقة ومعلومات المعاملة.

ولحماية الأدلة وتسهيل التحقيقات:

- لا تقم بالدخول إلى أو إدخال أي تغييرات على الأنظمة التي تم إختراقها (أي لا تقم بالدخول إلى إطلاقاً إلى الماكينة وقم بتغيير كلمات المرور ولا تقم بالدخول إلى جلسة بإستخدام ROOT.
- لا تقم بإقفال الأجهزة المرتبطة بالأنظمة التي تم إختراقها. وعوضاً عن ذلك قم بعزل الأنظمة التي تم إختراقها عن الشبكة (أي قم بفصل الكابل من المصدر).
- إحتفظ بالسجلات والأدلة الإلكترونية.
  أحتفظ بسجل لكافة الإجراءات
- إذا كنت تستخدم شبكة لاسلكية قم بتغيير معرف ضبط الخدمة SSID على نقطة الدخول AP والأجهزة الأخرى التي قد تستخدم هذه التوصيلة بإستثناء أي أنظمة يعتقد أنه قد تم إختراقها.
- ممارسة أقصى درجات الحيطة والحذر ومتابعة ومراقبة جميع الأنظمة التي تحتوي على بيانات حملة البطاقات ومعلومات المعاملات.

تطلب خطط البطاقة قيام محقق أدلة جنائية متخصص في مجال صناعة بطاقات الدفع بالتحقيق في أي مخالفات أو إنتهاكات تؤثر على التجار الذين نتعامل معهم. ونحن سوف نطلب منك ومن أي طرف ثالث يقوم بمساعدة أعمالك في مجال تنفيذ ومعالجة المعاملات، مساعدتنا وتمكيننا من حضور التحقيقات.

ما هي العقوبات التي قد تفرض على شركتي في حالة الإخفاق في الوفاء بمتطلبات معايير أمن بيانات الدفع بإستخدام البطاقات؟

- إذا أشارت نتيجة تقييم أعمالك من خلال خطط البطاقة إلى عدم إلتزام أعمالك بمعايير أمن بيانات الدفع بإستخدام البطاقات، فإنك تكون عرضة لعقوبات مالية. ويخضع التقييم إلى تقدير خطط البطاقة المعنية وتبدأ الغرامات بمبلغ ٢٥,٠٠٠ دولار أمريكي بالنسبة للتجار غير الملتزمين من المستويين الأول والثاني و ١٠,٠٠٠ دولار أمريكي بالنسبة للمستوى الثالث عن أول ربع سنة. ويكون هناك إحتمال لمضاعفة الغرامات كل ربع سنة تظل خلاله غير ملتزم بمعايير أمن بيانات الدفع بإستخدام البطاقات.

- وفي حالة تعرض أعمالك لحالة من حالات إنتهاك بيانات الحسابات، يحتمل أن تكون ملزماً بدفع غرامات مالية قد تصل إلى مئات الألوف من الدولارات. وهناك العديد من العناصر والعوامل التي يتم دراستها وأخذها في الإعتبار بواسطة خطط البطاقات عند تقدير الغرامات المالية منها على سبيل المثال لا الحصر عدد الحسابات التي تم إختراقها و وجود بيانات حساسة وعدد الحسابات التي يتعين مراقبتها بواسطة مصدر البطاقة ومستوى التاجر في الإلتزام بمعايير أمن بيانات الدفع بإستخدام البطاقات.