منشآت
monsha'at
الهيئة العامة للمنشآت الصغيرة والمتوسطة
Small & Medium Enterprises General Authority

مركز ذكاء

كتيب

الأمن السيبراني في التجارة الإلكترونية

المحتويات

منشآت
monsha'at
هيئة العامة للمنشآت الصغيرة والمتوسطة
Small & Medium Enterprises General Authority

مركز ذكاء

عن مركز ذكاء

جاء إنشاء مركز ذكاء كأول مركز متخصص في التقنيات المتقدمة لخدمة رواد الأعمال والمنشآت الصغيرة والمتوسطة في المملكة. يهدف المركز لتمكين قطاع المنشآت الصغيرة والمتوسطة من توظيف التقنيات المتقدمة لتطوير هذه المنشآت وزيادة تنافسيتها وأن يكون حلقة ربط ما بين رواد الأعمال وصناع القرار في مجالاته المتخصصة.

يتخذ مركز ذكاء لعلوم البيانات والذكاء الاصطناعي مدينة الخبر مقرًا له، ويقع مركز ذكاء لإنترنت الأشياء والأمن السيبراني في مدينة الرياض، ويخدم المركز بفرعَيه شتى أنحاء المملكة العربية السعودية.

بإمكانك النقر على الشعارات والروابط الموجودة في هذا الكتيب للذهاب إلى المواقع الإلكترونية الخاصة بها.

سياسة الاستخدام

إن المعلومات الواردة في هذا الكتيب تم تجميعها وتنسيقها بجهود موظفي مركز ذكاء التابع للهيئة العامة للمنشآت الصغيرة والمتوسطة "منشآت"، ولا ينبغي لقارئها أن يعمل بها دون مشورة مناسبة من المتخصصين.

للمزيد من المعلومات نرجو التواصل على البريد الإلكتروني support@thakaa.sa

مقدمة:

تشير التقديرات إلى أنّ عدد المتسوقين عبر الإنترنت في المملكة يشهد زيادة كبيرة خلال هذا العام 2022، حيث من المتوقّع أن يواصل الارتفاع في عدد المتسوقين ليصل إلى 19.3 مليون متسوق بنهاية عام 2022. هذا الإقبال الكبير يشجع رواد الأعمال على التوسّع في التجارة الإلكترونية، إلا أنّه يزيد من ضرورة الاهتمام بتأمين البيئة السيبرانية في جميع مراحل عمليات التجارة الإلكترونية، حيث تجدر الإشارة إلى أنّ عدداً من التقارير الصادرة بهذا الشأن تشير إلى زيادة كبيرة (تصل إلى 300% خلال الفترة منذ بداية 2020 وحتى منتصف 2022) في أعداد المتسوقين إلكترونيّاً الذين تعرضوا إلى مخاطر سيبرانية كالاحتيال المالي، وقد أحدثت هذه الزيادة مخاوفاً كبيرة في مجال الأمن السيبراني، وجعلته من أبرز التحدّيات التي تواجه عالم التجارة الإلكترونية منذ عام 2020 وحتى الآن.

ومن الجدير بالذكر أنّ اهتمام مواقع التجارة الإلكترونية بممارسات الأمان يمنحها ميزة تنافسية قويّة، فيجب أن تولي منشآت التجارة الإلكترونية اهتمامها الدائم بأمن البيانات، خصوصاً المنشآت التي تعتمد على المعاملات النقدية بشكلٍ يومي. ومن المهم الإشارة إلى أنّ السطح المعرّض للخطر السيبراني يكون واسعاً ليسع جميع الأطراف ذات العلاقة بالعمليات في التجارة الإلكترونية (البائع، منصة البيع، منصّة الدفع، العميل، إلخ)، وقد يشتمل السطح المعرضّ للخطر على مناطق ضعف تكون نتيجة لإهمال بشري كأن يتعرّض الضحية للتصيّد الاحتيالي نتيجة تفريطه في المحافظة على بياناته، أو نتيجة لثغرة في سياسات وإجراءات العمل، مثل: أن يكون وصول المهاجم للأجهزة في بيئة العمل للضحية سهلاً دون ضبط لعمليات الدخول والخروج، أو نتيجة لثغرات تقنية بحتة كأن يكون جهاز العميل مصاباً ببرمجيات خبيثة تتنصّت للبيانات التي تُرسل من قِبَل المتصفّح.

وفيما يلي توضيحٌ لأنواع البيانات التي قد تُستخدم في التجارة الإلكترونية، وأماكن تخزينها، و أبرز التهديدات التي تواجهها مواقع التجارة الإلكترونية، وكيفية التعامل معها، وأفضل الممارسات والأساليب المتّبعة لتجنّبها.

أهم البيانات في التجارة الإلكترونية :

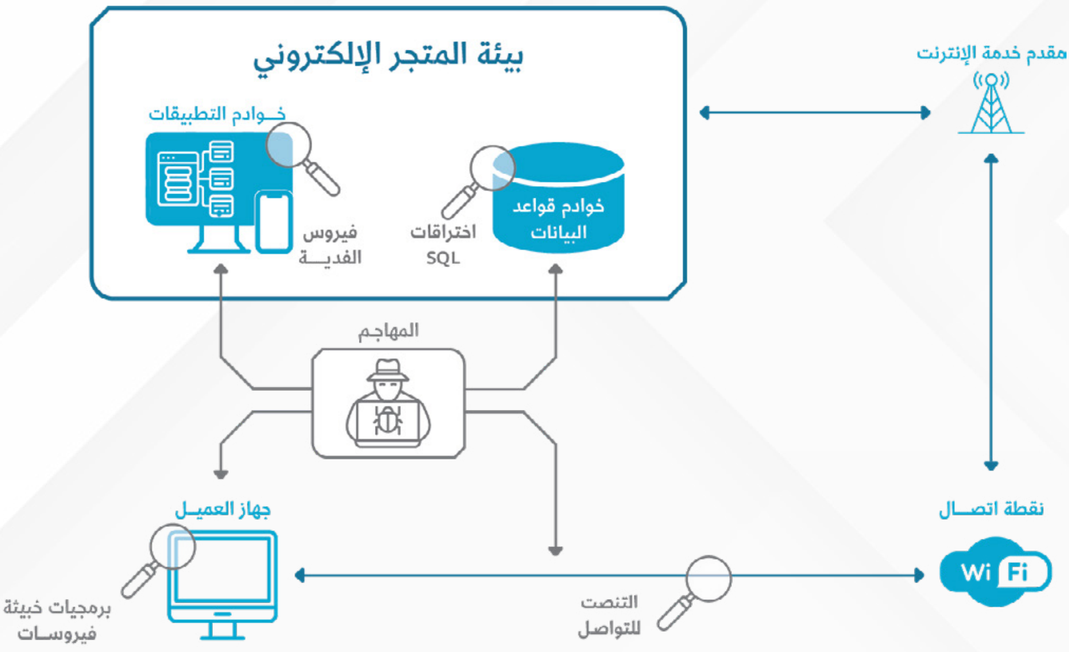
- بيانات العملاء الشخصية.
- بيانات العملاء المالية.
- بيانات التركيبة السكانية للعملاء.
- إحصائيّات المخزون.

وتخزّن في :

- السحابة.
- الخوادم المحلية لمتاجر الويب.
- نقاط البيع (POS).
- تطبيقات الهواتف الذكية.

التهديدات الشائعة التي تواجهها مواقع التجارة الإلكترونية:

عادةً ما تمرُّ عملية شراء المنتج أو الخدمة في التجارة الإلكترونية بخطوات متشابهة في جميع أنواع المتاجر الإلكترونية، مثل: متاجر التجزئة، ومنصّات تقديم الخدمات، ومنصّات المزايدة الإلكترونية. وتتنوّع التهديدات السيبرانية بتنوّع تلك الخطوات. الشكل التالي يوضّح بعض أنواع التهديدات في كل مرحلة من مراحل عمليات الشراء في التجارة الإلكترونية.



وفيما يلي شرح لأمثلة لتلك التهديدات:

1- اختراق كلمة المرور

يقوم المخترق في هذا النوع من التهديدات بإجراء محاولات للدخول على حساب العميل، إما بإجراء عدد كبير جدّاً من المحاولات باستخدام ما يسمّى "هجوم القاموس" وهو عبارة عن قاموس واسع لأشهر كلمات المرور المستخدمة، مثل: "Password" و"12345678"، أو بالحصول على كلمات المرور بطرق غير مشروعة كأن يقوم المهاجم باستغلال ثغرات في الجهاز الذي يستخدمه الضحية والتنصّت على كلمات المرور التي يستخدمها الضحية، ومن ثم استخدامها للوصول لحساب الضحية، أو أن يقوم المهاجم بالتنصّت على مراسلات الضحية (في حال كونها غير مشفّرة) ثم الحصول على كلمات المرور. كثيراً ما تؤدّي هجمات اختراق كلمات المرور لنتائج يكون تأثيرها أكثر ضرراً من مجرّد الوصول لحساب المستخدم، فبحسب تقرير شركة فرايزون لتسريب البيانات Verizon Data Breach Investigations Re- 2020 port، فإنّ ما يُقدّر بـ 37% من حالات تسريب البيانات التي كان سببها وصولاً غير مصرّح به لبيانات المنشآت الضحية كانت بسبب استخدام كلمات مرور ضعيفة أو مخترقة.

2- التصيّد الاحتيالي

تشير كثير من التقارير الحديثة إلى زيادة في حملات التصيّد الاحتيالي تجاوزت الـ 300% في فترة مابعد جائحة كورونا مقارنة بسنة 2019. ونلاحظ أنّ وسائل الإيقاع بالضحية قد تنوّعت بشكل كبير، حتى أصبح المهاجم يدرس الضحية من نواحٍ مختلفة ليبتكر الوسيلة المناسبة التي تزيد من احتمالية الإيقاع بالضحية، منتحلاً صفة لا تمتُّ له بصلة. إنّنا نلاحظ في أوقات متكررة هجمات تصيّد احتيالي تنتحل صفة شركات توصيل الشحنات من المتاجر الإلكترونية، وينجح كثير من تلك الهجمات في الإيقاع بالضحية. ونتيجة لهذا النوع من الهجمات، تسرّبت الكثير من البيانات المالية للعملاء في التجارة الإلكترونية.

3- البرمجيات الخبيثة

في السنوات الأخيرة تضاعف عدد الثغرات البرمجية التي يتم اكتشافها والإعلان عنها في قواعد بيانات الثغرات البرمجية، مثل: قاعدة البيانات الوطنية للثغرات National Vulnerability Database، وهي قاعدة بيانات حكومية أمريكية يتم تحديثها بشكل يومي بالثغرات التي تم اكتشافها. فمن المتوقّع أن يتجاوز عدد الثغرات التي تم الإعلان عنها في قاعدة البيانات هذه اثنين وعشرين ألف ثغرة في مئات المنتجات البرمجية، حيث تضاعفت بما يزيد عن ثلاث مرات خلال مدة ست سنوات، حيث لم تتجاوز 7000 ثغرة في سنة 2016. تقوم البرمجيات الخبيثة التي تستغل الثغرات في البرمجيات على جهاز الضحية بأداء مجموعة متنوعة من الوظائف الضارّة، كالتنصُّت على جهاز العميل للحصول على بيانات حسّاسة، مثل: بيانات البطاقات الائتمانية أو الحسابات البنكية. كما أنّ تلك البرمجيات قادرة على القيام بزيارات متعدّدة للمتاجر الإلكترونية في فترة زمنية قصيرة جدّاً، وبالتالي إجهاد خوادم الويب، ممّا يجعل موقع المتجر بطيئاً للمستخدمين الحقيقيّين.

4- هجمات رفض الخدمة الموزّعة DDoS

تهدف هجمات رفض الخدمة الموزّعة (DDoS) إلى تعطيل موقعك والتأثير على إجمالي مبيعاته. وفي مجال التجارة الإلكترونية، غالباً مايكون الدافع لمثل تلك الهجمات ماديّاً مباشراً أو غير مباشر، مثل: تعطيل الخدمة وقت المواسم أو تشويه سمعة متاجر منافسة.

أهم طرق مكافحة التهديدات السيبرانية لمنشآت التجارة الإلكترونية

هناك طرق عدة لمعالجة هذه التهديدات أهمّها ما يلي:

1. التشفير:

يُنصح رواد الأعمال بالاستفادة من التشفير للبيانات سواءً أثناء تخزينها في الخوادم، حيث يتم تحويل بيانات المستخدم من نص عادي إلى نص مشفّر لا يمكن قراءته إلا بعد فكّ تشفيره، أو أثناء تراسل البيانات بين الأطراف المختلفة في خطوات عملية الشراء من المتاجر الإلكترونية، وذلك باستخدام قنوات التواصل الآمن، مثل: بروتوكول HTTPS؛ لمنع المهاجم من التعرّف على محتوى الرسائل المرسَلة بين العميل والمتجر في حال قام بالتنصّت على الشبكة.

2. التعامل مع بطاقات الدفع الآمنة :

تصبح العديد من شركات التجارة الإلكترونية ضحية للاحتيال عبر بطاقات الائتمان وبطاقات الخصم؛ بسبب استخدام بوابات دفع غير موثوقة، ستسمح لك معظم منصّات المتاجر الإلكترونية بالتعامل مع العشرات من بوابات الدفع الشائعة والموثوقة، مثل: قائمة بوّابات الدفع في المنصة الوطنية الموحّدة وقائمة الشركات المرخّص لها من البنك المركزي.

3. استخدام برامج الحماية من البرمجيات الضارّة :

استخدم برامج الحماية وحدّثها باستمرار على كل جهاز مستخدم في بيئة الأعمال الخاصّة بتجارتك الإلكترونية (بما في ذلك أجهزة الحاسب الآلي والهواتف الذكية والأجهزة اللوحية)؛ لحماية أنظمة تجارتك الإلكترونية من البرمجيات الضارّة (كالفيروسات على سبيل المثال). حيث تتيح لك برامج مكافحة الفيروسات الجيّدة معرفة ما إذا كان أحد المتطفّلين يحاول تثبيت فيروس أو برنامج ضارٍّ على جهازك الكمبيوتر.

4. النسخ الاحتياطي لبياناتك :

فقدان البيانات بسبب عطل في الأجهزة أو الهجمات الإلكترونية شيء محتمل الحدوث، وإذا لم تنسخ بياناتك احتياطيّاً بانتظام، فأنت معرّض لخطر فقدانها نهائيّاً. لم يعد الاحتفاظ بالنسخ الاحتياطية أمراً مكلفاً من الناحية المالية كما كان سابقاً. أصبح الكثير من مقدّمي خدمات الحوسبة السحابية وخدمات استضافة المتاجر يوفّرون خدمة النسخ الاحتياطي بثمن رخيص.

5. تدريب الموظفين بشكل جيّد :

لا بدّ أن يكون طاقم العمل على دراية بالقوانين والسياسات المتعلّقة بحماية معلومات المستخدم، كما لا يجوز أن يقوم بمشاركة بيانات اعتماد تسجيل الدخول، ولا بدّ من مراجعة الموظفين الذين يمكنهم الوصول إلى معلومات العميل الحسّاسة، وبمجرّد أن يقدّم الموظف استقالته، فعليك أن تمسح تفاصيله وتلغي كل إمكانيات وصوله لبيانات العملاء والمنشأة.

6. توعية عملائك واستخدام سياسات أمنية جيّدة :

لا تحدث بعض الحوادث السيبرانية من جانب واحد (الشركة) بل قد تحدث من الجانب الآخر (العميل)، فقد يستخدم كلمات مرور ضعيفة أو قد يقدّم معلومات حسّاسة لمواقع التصيّد الاحتيالي لتقع في أيدي المتصيّدين. لذلك فإنّه من المهم تبنّي سياسات تضمن أمان بيانات العميل مع المحافظة على تجربة تصفّح متميّزة. من الطرق الدارجة في المتاجر الإلكترونية لحماية كلمات المرور "استخدام معايير التحقّق المتعدّد".

أفضل ممارسات الأمن السيبراني في التجارة الإلكترونية

- خذ بعين الاعتبار استخدام خيارات تحقّق إضافية :

فعّل خاصية التحقّق المتعدّد العناصر للهوية عند توفّر ذلك في الأنظمة أو التطبيقات ذات العلاقة بتسجيل دخول عملائك؛ وذلك لحماية المستهلكين الذين تتعامل معهم في التجارة الإلكترونية. مثل: تسجيل اشتراك في خيارات التحقّق الإضافية (مثل: رسائل البريد الإلكتروني) التي تقدّمها تطبيقات التجارة الإلكترونية ومواقعها (ويشمل هذا حسابات مواقع التواصل الاجتماعي).

- تحكّم بعدد حسابات مسؤولي الأنظمة :

امنح موظفي تجارتك الإلكترونية أقل مستوى من صلاحيات المستخدم المطلوبة للقيام بمهامهم الوظيفية وامنح صلاحيات مسؤول النظام بحذر شديد، حيث يتمتّع حساب مسؤول النظام بصلاحيات خاصة للقيام بتغييرات في النظام لا يمكن لحسابات المستخدمين الآخرين القيام بها.

- حدّث تطبيقاتك بانتظام على جميع الأجهزة :

أكثر الطرق كفاءة في الحماية ضد البرمجيّات الضارّة والفيروسات هي إبقاء جميع أجهزة وتطبيقات تجارتك الإلكترونية (خاصّةً أنظمة التشغيل) محدّثة بآخر التصحيحات الأمنية.

- استعن بمواقع موثوقة لعرض إعلاناتك :

اعمل على حماية إعلاناتك من النقرات الاحتيالية وذلك عن طريق عرض إعلاناتك على مواقع موثوقة والتي تعرف أنّها مصدر لعملاء حقيقيين.

- اطّلع على التهديدات السيبرانية أوّلاً بأول :

اشترك بالتنبيهات والإنذارات السيبرانية؛ لتبقَ على اطّلاع بمستجدّات الأمن السيبراني والتهديدات النشطة من خلال متابعة آخر التحديثات والمستجدّات من منظّمات موثوقة (مثل: المركز الوطني الإرشادي السعودي للأمن).

يوجد عدد من المنشآت السعودية التي تقدّم حلولاً مميّزة في مجالات مختلفة في الأمن السيبراني.
يمكن الاطّلاع على قائمة من المنشآت السعودية المتخصّصة في مجال الأمن السيبراني هنا.

تمت مراجعة هذا الكتيب من قبل :

د. منير عبدالله الشيخ.

أكاديمي ومستشار أمن سيبراني. حاصل على الدكتوراة في إدارة الأمن السيبراني من جامعة ملبورن. وماجستير أمن الحاسب والشبكات من جامعة موناش بالإضافة إلى شهادات مهنية في المجال. عمل كمدير أمن سيبراني بجامعة جدة وحاليّاً يعمل ككبير مستشاري حوكمة المخاطر والالتزام في إحدى الشركات الوطنية. نشر مجموعة من المقالات والمجلات الأكاديمية المتخصصة في الأمن السيبراني.

كذلك كتب مجموعة من المقالات في الصحف المحلية. مهتم بالتوعية السيبرانية وتغيير السلوك.

حدود المسؤولية

تقدم "منشآت" المصادر التعليمية وهي خدمة من خدمات مكتبة مركز ذكاء التي تقدمها منشآت والتي تساهم وتساعد في إثراء المحتوى العربي لمصادر التعلم عبر الإنترنت لتوفير المعرفة لفئات مختلفة في مجالات التقنية وريادة الأعمال، ولا تقدم "منشآت" أو من يمثلها أيّ قرارات أو ضمانات سواءً بشكل صريح أو ضمني حول اكتمال أو دقة أو موثوقية أو ملاءمة أو توافر هذه البيانات أو المعلومات أو المواد ذات الصلة الواردة في الكتيّب لأي غرض كان ولا يجوز استخدامها لغرض آخر غير الاستخدام العام ولا تتحمل "منشآت" أو من يمثلها – بأي حال من الأحوال- أي أضرار مادية أو معنوية، مباشرة أو غير مباشرة قد تحصل، وتؤكد "منشآت" أو من يمثلها أنها غير مسؤولة سواءً بشكل كامل أو جزئي عن أي ضرر مباشر أو غير مباشر، عرضي أو تبعي أو عقابي خاصًا كان أو عامًا، كما أنها غير مسؤولة عن أي فرصة ضائعة أو خسارة أو ضرر من أي نوع، ومنها على سبيل المثال لا الحصر، أي ضرر أو فيروس قد يتعرض له الحاسوب الشخصي نتيجة الدخول إلى هذه الصفحة، وأن "منشآت" أو من يمثلها تبذل الجهد للتأكد من أن المعلومات المتوفرة من خلال المصادر التعليمية شاملة ودقيقة قدر المستطاع. وكما تؤكد "منشآت" على الالتزام بحقوق النشر وحقوق الملكية الفكرية لمحتويات المصادر التعليمية بما في ذلك شعار "منشآت" ولا يحق نشر أي معلومات أو رأي يتم التعبير عنه هنا دون الحصول على إذن خطي مسبق للقيام بذلك من قبل "منشآت".

منشآت
monsha'at
هيئة العامة للمنشآت الصغيرة والمتوسطة
Small & Medium Enterprises General Authority

مركز ذكاء

Thakaa.sa