الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

مبادئ توجيهية
لتأمين أنظمة المعلومات بالفنادق

عـــام

إخلاء المسؤولية / الحقوق القانونية

قامت الوكالة الوطنية للأمن السيبراني (NCSA) بإعداد ووضع هذا المنشور بعنوان " مبادئ توجيهية لتأمين أنظمة المعلومات بالفنادق" - الإصدار 2.0 لمساعدة الفنادق (قطاع الضيافة) على فهم وتخفيف المخاطر السيبرانية على أنظمة المعلومات الخاصة بهم. وهي مسؤولة عن مراجعة هذه الوثيقة والمحافظة عليها.

وعلى الوكالة بصفتها مصدر ومالك، بغض النظر عن طريقة نسخ أي نسخة سواء أكانت كلية أو جزئية من هذه الوثيقة؛ بما يخص « مبادئ توجيهية لتأمين أنظمة المعلومات بالفنادق ».

في حالة طلب أي نسخ بخصوص هذه الوثيقة بقصد التسويق التجاري، يلزم الحصول على إذن كتابي من الوكالة الوطنية للأمن السيبراني. ولها أحقية في تقييم مدى فعالية وإمكانية تطبيق جميع النسخ المطورة فيما يخص الأغراض التجارية.

ولا يجوز تفسير الإذن الصادر عن الوكالة الوطنية للأمن السيبراني على أنه تأييد للنسخ المطورة ولا يجوز للمطور بأي حال من الأحوال الإعلان عن ذلك أو إساءة تفسيره بأي شكل من أشكال في وسائل الإعلام أو المناقشات الشخصية / الاجتماعية.

مراقبة الوثائق

تفاصيل الوثيقة	
رقم هوية الوثيقة	IAG-NGE-GHIS
الإصدار	إصدار 2.0
التصنيف والنوع	عام
الخلاصة	تم إعداد هذه الوثيقة كدليل لمساعدة لمساعدة مؤسسات قطاع الضيافة على فهم وتخفيف المخاطر السيبرانية على أنظمة المعلومات الخاصة بهم.

المراجعة / الموافقة

القسم / المهمة	تمت المراجعة / الموافقة	الإصدار	التاريخ
شؤون الحوكمة والضمان السيبرانى الوطني		2.0	

سجل النسخ المنقحة

الإصدار	المؤلف:	وصف المراجعة	التاريخ
1.0	شؤون الحوكمة والضمان السيبرانى الوطني	منشور	يوليو 2018
2.0	شؤون الحوكمة والضمان السيبرانى الوطني	منشور	يناير 2023
2.0	شؤون الحوكمة والضمان السيبرانى الوطني	منشور (تعديلات تصحيحية طفيفة)	ديسمبر 2023

التفويض القانونية

يحدد القرار الأميري رقم (1) لسنة 2021 فيما يخص إنشاء الوكالة الوطنية للأمن السيبراني، صلاحياتها (المشار إليها فيما يلي باسم "الوكالة الوطنية للأمن السيبراني"). وتتمتع الوكالة الوطنية للأمن السيبراني بسلطة الإشراف على أمن البنية التحتية الوطنية الحيوية وتنظيمها وحمايتها من خلال اقتراح وإصدار السياسات والمعايير وضمان الامتثال.

وقد تم إعداد هذه الوثيقة مع الأخذ في الاعتبار بالقوانين المعمول بها في دولة قطر. وفي حالة نشوء تعارض بين هذه الوثيقة (أحكام أو بنود محددة) وقوانين دولة قطر، تسود قوانين دولة قطر. وبذلك، يعتبر أي مصطلح من هذا القبيل (أحكام أو بنود محددة) محذوفًا من هذه الوثيقة، دون المساس بالأحكام المتبقية من هذه الوثيقة. ويلزم في هذه الحالة إجراء تعديلات لضمان الامتثال للقوانين السارية ذات الصلة بدولة قطر.

جدول المحتويات

1 المقدمة

1.1 السياق

ينزل الضيوف إلى الفندق حاملين شعور يشبه بيوتهم. إنهم يتوقعون أن تكون مريحة وتتمتع بالخصوصية والأمان. وعادة، ما تركز الفنادق على مثل هذه التوقعات. وعلاوة على ما سبق، فهناك نوع آخر من الاهتمام، إذ يوجد هناك اهتمام كبير بالأمن المادي داخل الفنادق، وتكون الأبواب مزودة بأقفال (أقفال تعتمد على البطاقة الذكية لمزيد من الراحة والأمان)، وتحتوي الغرف على خزائن إلكترونية برقم التّعريف الشخصي (PIN) يمكن للضيف ضبطها.

ويتوقع الضيوف أن نفس مستوى الحماية يمتد إلى أصولهم الرقمية عند اتصالهم بالبنية التحتية الرقمية للفندق، مثل الشبكة المحلية أو الشبكة المحلية اللاسلكية للوصول إلى الإنترنت.

وتحتاج الفنادق إلى طمأنة ضيوفها بأن الأمن الرقمي يمثل أولوية مهمة مثل الأمن المادي وأن المعلومات المقدمة من قبل الضيوف (سواء كانت مادية (تنسيق ورقي) أو رقمية) سيتم تأمينها ضد التهديدات المحتملة بما في ذلك التهديدات الإلكترونية.

2 الغرض والنطاق والاستخدام

2.1 الغرض

الهدف من هذا الدليل الإرشادي هو مساعدة الشركات في قطاع الضيافة على فهم مخاطر أمن المعلومات المحتملة التي يواجهونها وتحديد الضوابط المناسبة للتخفيف من هذه المخاطر أو تجنبها.

2.2 النطاق

الأعمال التجارية مثل الفنادق والشقق الفندقية والمطاعم داخل قطر.

2.3 الاستخدام

ستساعد الإرشادات الواردة في هذه الوثيقة المؤسسات في قطاع الضيافة على تأمين أنظمة المعلومات الخاصة بها ضد المخاطر السيبرانية. وتوفر الوثيقة فهماً لمختلف أنواع التهديدات التي قد تواجهها المؤسسات ونهجاً منظماً للتصدي لها.

3 التعريفات الرئيسية

المؤسسات/المؤسسة تشير إلى المؤسسات العاملة في قطاع الضيافة داخل دولة قطر.

4 الإرشادات

4.1 فهم المخاطر

تنبع أشد المخاطر التي يتعرض لها قطاع الفنادق والترفيه، مثل أي عمل تجاري، من التوقعات المبالغ فيها المرتبطة بالضيوف بخصوص الراحة والخصوصية والأمان. وعلى الرغم من أن هذه المؤسسات قد تعتبر بطبيعتها قليله الأهمية، إلا أن مثل هذه الشركات تعتبر كنزًا من المعلومات التي قد تكون جذابة للغاية لمجرمي الإنترنت ونشطاء القرصنة والجهات الحكومية. وتتضمن المعلومات التي تحتفظ بها هذه الشركات المعلومات الشخصية مثل التفاصيل المتعلقة بجواز السفر وأي بطاقات هوية أخرى وبطاقات الائتمان والعناوين الشخصية أو التجارية ومخططات السفر والإعجابات الشخصية والعادات وما إلى غير ذلك. ويمكن للمستخدم ضار استغلال هذه المعلومات لانتحال الهوية أو شن هجمات الهندسة الاجتماعية أو التصيد الاحتيالي أو ارتكاب عمليات احتيال مالية من بين أشياء أخرى. وعلى هذا النحو، فإن الشركة نفسها معرضة للخطر لأنها قد تصبح محور الهجوم لمثل هذه المعلومات.

وتشمل المخاطر الرئيسية التي تواجهها الشركات ما يلي:

1. فقدان البيانات الشخصية المتعلقة بالضيوف، مما يؤدي إلى انتهاك الالتزامات المترتبة عن قانون الخصوصية وربما المطالبات الفردية المتعلقة بالخسارة.
2. فقدان المعلومات السرية، والذي قد يصل إلى حد انتهاك العقد و / أو فقدان المزايا التجارية.
3. هجمات حجب الخدمة، ومنع استخدام أنظمة التشغيل، بما في ذلك أنظمة الحجز.
4. الاحتيال المالي بمعلومات بطاقة ائتمان العميل، بما في ذلك عمليات الحجز التي تتم باستخدام الهويات المسروقة.
5. الأضرار التي تلحق بالسمعة نتيجة لحدوث أي من هذه المخاطر

مخاطر الجهة الخارجية المتعلقة بفقدان المعلومات الشخصية أو السرية بسبب المجرمين الذين يستهدفون البيانات الحساسة عبر مزود الجهة الثالث - على سبيل المثال، مواقع حجز الغرف أو شركات تأجير السيارات، التي تحتفظ بمعلومات عن الضيوف.

4.2 التهديدات المتطورة

فيما يلي بعض التهديدات الرئيسية التي تواجه قطاعات الفنادق والترفيه.

هجمات التصيد الاحتيالي: تعتبر هجمات التصيد الاحتيالي في الأساس خطوة مسبقة لهجوم ضار شامل موجه نحو مؤسسة ما. والهدف الأساسي منه هو الحصول على أوراق اعتماد المستخدم من خلال تقنيات الهندسة الاجتماعية والتسلل إلى نظام الوكالة لزرع وإطلاق التهديدات المستمرة المتقدمة.

الهجمات المستندة إلى شبكة الواي-فاي: يمكن استخدام أنظمة الواي-فاي التقليدية، وهي جهات ضعيفة وضارة، ما لم يتم تأمينها بشكل كافٍ (قد يكون هؤلاء من جهات داخليه مثل الموظفين أو نزلاء الفندق أو الجهات الخارجية مثل المتسللين ومجرمي الإنترنت وما إلى غير ذلك) لاختراق أنظمة الشركات أو زملائهم المستخدمين.

دارك هوتيل: المتغير الجديد هو هجوم التصيّد بالحربة الموجهة والبرامج الضارة التي يطلق عليها اسم "دارك هوتيل". ودوره المهاجمة بشكل انتقائي لزوار الفنادق من رجال الأعمال من خلال شبكة الواي-فاي الداخلية بالفندق. وتستهدف الهجمات على وجه التحديد كبار المديرين التنفيذيين في الشركة، باستخدام شهادات رقمية مزورة، تم إنشاؤها عن طريق أخذ المفاتيح العامة الضعيفة الكامنة وراء الشهادات الحقيقية في الاعتبار، لإقناع الضحايا بأن تنزيلات البرامج التي تم تحميلها صالحة

هجمات حجب الخدمة الموزعة وهجمات شبكة البوت نت ازدادت شعبية هجمات حجب الخدمة الموزعة لتنفيذ مجموعة من أنشطة لإقحام البرامج الضارة. ضمن هذه الهجمات، يستخدم المهاجمون شبكات البوت نت الخاصة بالشبكات المخترقة لإعاقة الأنظمة المهمة (مثل حجز التذاكر عبر الإنترنت) بحركة المرور، مما يؤدي إلى تعطل النظام الأساسي. وقد يطلب المهاجمون أيضًا مبلغًا من الفدية من السلطات لمنع تعطيل مثل هذه الأنظمة الحساسة.

برنامج الفدية: نمت شعبية هذه الهجمات في السنوات القليلة الماضية، ولدينا بعض الهجمات المعوقة الحقيقية حيث يتمكن المهاجمون من الوصول إلى نظام المؤسسات وتشفير البيانات. وبعد النجاح في ذلك، يُطلب من الشركات دفع فدية لتتمكن من الحصول على مفتاح لفك تشفير البيانات.

تسريب البيانات: هذه هي الهجمات التي يتمكن فيها المهاجمين الضارين من الوصول إلى أنظمتك والبقاء هناك قدر الإمكان ومحاولة التعرف على البيانات الهامة وسرقتها خارج المؤسسة. وتشمل البيانات بيانات العمل بالإضافة إلى معلومات الضيوف (الشخصية / المالية (بطاقات الائتمان) وما إلى غير ذلك)

4.3 تأمين نظم معلومات الضيافة

يتزايد الاعتماد على التكنولوجيا في قطاع الضيافة حيث يكون الشكل والمزايا التنافسية مهمة بشكل كبير، ويتلخص الهدف النهائي من كل هذا في توفير تجربة مريحة وفاخرة للضيوف والزوار، ويمكن أن تكون أنظمة المعلومات عامل تغيير في تحقيق هذا الهدف.

ومع ذلك، فإنه ينشأ عن زيادة الاعتماد على التكنولوجيا، زيادة في مخاطر خرق أمن المعلومات (فقدان السرية، والسلامة، وتوافر بيانات العملاء). ويجب على قطاع الضيافة والكيانات التابعة له مراعاة النظافة الصحية لأمن المعلومات وأن توفر الحماية الكافية لنظم المعلومات والهياكل الأساسية.

وكجزء من الواجب المنوط بهم، يلزم عليهم توعية الموظفين على جميع المستويات بشأن التعامل مع بيانات العملاء. كما يلزم أن يصبح تنظيف أنظمة أمن المعلومات جزءًا من واجباتهم.

4.3.1 الحوكمة

إن تأسيس القيادة لبرنامج أمن المعلومات داخل المؤسسة أمر مهم للغاية. وقد أكدت عليها جميع معايير أمان البيانات مثل معيار تأمين المعلومات الوطنية.

ويلزم على كل مؤسسة تطوير إطار عمل شامل لأمن المعلومات وسياسات الخصوصية وإجراءات التنفيذ الفعال وإدارة أمن معلومات المؤسسة / نظام إدارة الخصوصية.

ويلزم أن يتضمن إطار العمل سياسة أمن معلومات الشركة (CISP)[1] التي تحدد التزام المؤسسات بتبني ممارسات أمن المعلومات / الخصوصية داخل الأعمال وتنفيذ نظام إدارة فعال لتحقيق الأهداف. ويلزم على رئيس المؤسسة التوقيع على السياسة.

يجب أن يكمل دليل السياسة الذي يغطي العمليات المختلفة ومجالات النطاق المحددة سياسة أمن معلومات الشركة.

التشريعات

يجب أن يحدد نظام الإدارة ودليل السياسة المرتبط به الضوابط بما يتماشى مع المتطلبات التنظيمية. وتشمل المتطلبات التنظيمية المتطلبات المحلية والدولية (إن وجدت).

وتتضمن بعض المتطلبات التنظيمية الرئيسية ما يلي:

[1] يتوفر نموذج لسياسة أمن معلومات الشركة على موقع الإلكتروني للوكالة الوطنية للأمن السيبراني

1. الالتزام بمعيار تأمين المعلومات الوطنية (قطر)
2. الالتزام بسياسة تصنيف البيانات الوطنية (قطر)
3. الالتزام بقانون حماية خصوصية المعلومات الشخصية (قطر)
4. الالتزام بقانون الجرائم الإلكترونية (قطر)
5. الالتزام بقانون المعاملات والتجارة الإلكترونية
6. الالتزام بالنظام الأوروبي العام لحماية البيانات إن أمكن

4.3.2 الخصوصية

حماية المعلومات الشخصية هي مطلب تنظيمي رئيسي على الصعيدين المحلي والدولي. وتنص اللائحة على عدد من الحقوق للأفراد مثل الحق في النسيان، والحق في المعلومات، والحاجة إلى الموافقة وما إلى غير ذلك. ومن الضروري أن يتم تصميم الأنظمة بما يتماشى مع المتطلبات التنظيمية الخاصة بالخصوصية. ويجب على المؤسسات جمع البيانات المطلوبة فقط للأعمال المتطلبة لتلك البيانات. تتمثل الاستراتيجية الرئيسية في إدارة الخصوصية الفعالة في ضمان الحد من المخاطر عن طريق تقليل كمية البيانات التي يتم جمعها، وضمان استخدامها بناءً على الموافقة المستلمة والتخلص من البيانات بمجرد الانتهاء من الحاجة (التجارية وكذلك القانونية / التنظيمية).

4.3.3 التأمين الإلكتروني

خرق أمن البيانات هو حادث يتم فيه المساس بسرية البيانات أو سلامتها أو توفرها (غالبًا ما يتم تخزينها إلكترونيًا)، بحيث تكون البيانات عرضة للوصول أو الحصول عليها من قبل أشخاص غير مصرح لهم. ولا يتسبب المهاجمون أو الأفراد الضارون في جميع وقائع انتهاكات البيانات؛ إذ أن بعضها ناتج عن الإهمال الفردي، مثل ترك جهاز كمبيوتر محمول غير آمن في مكان ما وتعريض البيانات لبيئة غير آمنة. باستخدام معلومات التعريف الشخصية - مثل أرقام البطاقة الشخصية أو أرقام الحسابات المالية أو بيانات اعتماد الوصول - من المحتمل أن يؤدي فقدان السرية إلى سرقة الهوية ورسوم بطاقات الائتمان أو بطاقات الخصم غير المصرح بها والاحتيال على الحساب المصرفي. وقد تتعرض المؤسسات لخسائر مباشرة وغير مباشرة، بما في ذلك الغرامات والعقوبات التي تفرضها اتحاد البطاقات الائتمانية. وقد تواجه الشركات أيضًا مسؤولية إزاء الغير في شكل دعاوى قضائية ومطالبات وغرامات تنظيمية، وفي بعض الحالات، حتى عقوبات مدنية وجنائية.

لا يعتبر التأمين الإلكتروني خط دفاع، ولكن في حالة حدوث خرق، يمكن أن يساعد المؤسسات في إدارة بعض الالتزامات على الأقل من منظور مالي. ويعتبر ذلك أمر منطقي في بيئة تنظيمية قوية حيث قد تكون المؤسسات مسؤولة عن الغرامات التأديبية و / أو التكاليف المتعلقة بإخطار الخرق.

ويلزم أن تكون الوكالات حذرة ويجب إجراء العناية الواجبة، بما في ذلك إشراك أصحاب المصلحة التجاريين مثل الإدارة القانونية أثناء التفاوض على بوليصة تأمين إلكتروني مناسبة للوكالة. يجب فحص جميع التعريفات وتفسيراتها من قبل كل من مالك السياسة ومزود التأمين السيبراني من قبل الإدارة القانونية. ويرد فيما يلي بعض العوامل التي يجب مراعاتها عند اختيار التغطية التأمينية الإلكترونية:

نوع التغطية التأمينية: عادة ما تغطي السياسة خسائر الطرف الأول والجهات الخارجية المتكبدة نتيجة لخرق الأمن الإلكتروني.

نطاق التغطية التأمينية: يمكن تصميم نطاق التغطية لمجموعة متنوعة من سيناريوهات المخاطر ويلزم أن يغطي ما يلي:

- تغطي إدارة الأصول أو الالتزامات نفقات استبدال الأصول الرقمية، وفقدان الدخل التجاري وتغطية خسارة دخل الأعمال المعتمدة، وتغطية تهديد الابتزاز السيبراني ومدفوعات المكافآت.
- تغطي مسؤولية حماية الشبكات أضرار الجهات الخارجية الناتجة عن الإخفاق في الحماية من تحريف البيانات الإلكترونية لطرف ثالث أو حذفها أو تلفها. وقد يكون هذا نتيجة لهجمات حجب

الخدمة ضد مواقع الويب أو أجهزة الكمبيوتر، أو من خلال نقل فيروس من أجهزة كمبيوتر والأنظمة التابعة لجهات خارجية.

- تغطي مسؤولية الخصوصية الأضرار التي تقع على عاتق الجهات الخارجية والتي تنتج عن الكشف عن المعلومات السرية التي تم جمعها أو التعامل معها من قبلك، أو التي تكون تحت وصايتك أو سيطرتك. وهذا يشمل تغطية المسؤولية غير المباشرة عندما يفقد البائع المعلومات التي عهدت بها إليهم.
- تغطي المسؤولية عن محتوى الوسائط الإلكترونية الضرر الشخصي ومطالبات العلامات التجارية / حقوق النشر التي تنشأ عن إنشاء المحتوى الإلكتروني ونشره.
- يغطي الدفاع التنظيمي والعقوبات التكاليف الناشئة عن الانتهاك المزعوم لقانون الخصوصية الناجم عن خرق أمني.
- يوفر ابتزاز الشبكة تعويضًا عن المدفوعات التي تتم تحت الإكراه استجابة لتهديد الابتزاز.
- يوفر انقطاع أعمال الشبكة تعويضًا عن خسارتك للدخل والنفقات الإضافية الناتجة عن انقطاع أو تعليق أنظمة الكمبيوتر. وهذا يشمل الحدود المفروضة- التابعة لخسائر انقطاع الأعمال.
- تغطي مصاريف حالات حدوث الخرق التكاليف المرتبطة بالامتثال لقواعد الخصوصية. وهذا يشمل الاحتفاظ بشركة لإدارة الأزمات، أو مستشار خارجي، أو تكاليف قانونية، أو غرامات تنظيمية، أو إخطار بالخرق، أو محققين جنائيين.
- تغطي حماية أصول البيانات استرداد التكاليف والنفقات التي قد تتكبدها لاستعادة بياناتك وغيرها من الأصول غير الملموسة أو إعادة إنشائها أو إعادة تجميعها.
- يمكن أن تتضمن أغطية مسؤولية الوسائط المتعددة / الوسائط تشويهًا محددًا لموقع الويب وانتهاك حقوق الملكية الفكرية.
- تغطي مسؤولية الابتزاز الخسائر الناجمة عن التهديد بالابتزاز، والرسوم المهنية المتعلقة بالتعامل مع الابتزاز.
- مطالبات الجهات الخارجية. وهذا يشمل المطالبات بالتعويضات المقدمة من العملاء أو المستهلكين أو الكيانات التجارية الخارجية ضد الأضرار التي تكبدوها بسبب خرق الشركة المؤمن عليها للأمان، ولا سيما خسائرهم الناشئة عن عدم القدرة على التعامل مع الأعمال التجارية، بما في ذلك التعويضات العقابية والتأديبية، والتسويات والتكاليف.

وتكون القوائم المذكورة أعلاه غير شاملة؛ وقد تقدم شركات النقل تغطية إضافية، خاصة للشركات ذات المخاطر المتخصصة.

المهلة الزمنية: تُعرّف على أنها مدة تغطية الإصلاح، وتكون المدة الزمنية الأكثر شيوعًا سنة واحدة بعد الخرق.

4.3.4 تحديد وتنفيذ العمليات

بعد وضع الحوكمة اللازمة، فإن الخطوة الأساسية هي إنشاء العمليات الصحيحة بشكل ملائم لتنفيذ برنامج فعال.

ويسلط القسم الوارد أدناه الضوء على بعض العمليات الرئيسية التي يلزم تنفيذها. يُنصح المؤسسات بمراجعة معيار تأمين المعلومات الوطنية إصدار 2.0 وأي لوائح صادرة عن المنظمين المحليين أو الدوليين وأي ممارسات أخرى خاصة بالقطاع مثل تلك الصادرة عن اتحاد النقل الجوي الدولي.

تصنيف أصول المعلومات ووضع العلامات عليها

1. إجراء جرد لجميع أصول المعلومات عبر الأعمال التجارية.

2. قم بتقييم القيمة الأمنية الإجمالية لأصل المعلومات باستخدام نموذج تصنيف أصول المعلومات[2]
3. قم بتحليل تأثير حماية خصوصية البيانات للتأكد مما إذا كان أصل المعلومات يحتوي على أي معلومات تعريف شخصية (PII).
4. قم بتسمية أصل المعلومات بناءً على تصنيفات السرية والخصوصية للأصل.
5. يجب أن تكون الملصقات واضحة وغير مبهمة ومرئية.
6. بالنسبة للبيانات الإلكترونية، يوصى أيضًا باستخدام علامات التعريف أو التنسيقات التي يمكن قراءتها آليًا.

إدارة التغيير

1. تحديد وتنفيذ عملية إدارة التغيير بما يتماشى مع معيار تأمين المعلومات الوطنية[3].
2. قم بإنشاء مجلس إدارة التغيير (CMB) أو مجلس استشاري للتغيير (CAB) لمراجعة أي تغييرات على النظام والموافقة عليها.
3. يشكل مجلس إدارة التغيير/ مجلس استشاري للتغيير أعضائه من قطاعات الأعمال، وقسم تكنولوجيا المعلومات، ورئيس أمن المعلومات، ورئيس استمرارية الأعمال وأي أعضاء آخرين حسب الاقتضاء.
4. يجب أن يوافق مجلس إدارة التغيير/ مجلس استشاري للتغيير على جميع التغييرات.
5. حدد عملية الموافقة في حالات الطوارئ لإجراء أي تغييرات طارئة، إذا لزم الأمر. وقد يشمل ذلك الموافقات الشفهية والموافقة المباشرة من الإدارة العليا وما إلى غير ذلك.
6. على الرغم من ذلك، يجب توثيق جميع التغييرات (بما في ذلك التغييرات الطارئة) في النظام.
7. يجب أن تتضمن أي طلبات تغيير عملية تراجع في حالة عدم نجاح التغيير المقترح.
8. يجب أن تتضمن العملية مراجعات منتظمة للتأكد من أن التغييرات المنفذة قد حققت أهدافها وتعمل بشكل جيد، بالإضافة إلى التراجع عن التغييرات التي كانت مؤقتة بطبيعتها.

قبول النظام والتشغيل التجريبي

1. حدد عملية للتحقق من صحة أي نظام جديد (برنامج / جهاز) يتم إدخاله في شبكة الأعمال.
2. يجب أن تتضمن عملية التحقق على الأقل ما يلي:
   أ. مسوغ تجاري والحاجة إلى أصول المعلومات داخل شبكة الأعمال.
   ب. تصنيف وتسمية أصول المعلومات.
   ت. الحد الأدنى من تقييم الأمان الأساسي الذي يتضمن:
      i. فحص للتأكد من تنفيذ ضوابط الأمان القياسية مثل حماية نقطة النهاية، التصلب وما إلى غير ذلك.
      ii. تمرين لتقييم الضعف أو تمرين اختبار الاختراق لأنظمة المواجهة الحاسمة والعامة (الإنترنت) لتحديد أي نقاط ضعف معروفة.
      iii. خطة تنفيذ إما للقضاء على نقاط الضعف المحددة أو التخفيف منها بما يتماشى مع الإقبال على المخاطر من جانب المؤسسة.
3. تحديث قائمة جرد الأصول بعد تشغيل النظام.
4. تحديث حلول مراقبة النظام لتجميع ومراقبة الأحداث الأمنية من الجهاز الخاضع للتجربة.

[2] يرجى مراجعة السياسة الوطنية لتصنيف المعلومات.

[3] قوالب خرائط عملية إدارة التغيير، وتكون نماذج إدارة التغيير متاحة على موقع الإلكتروني للوكالة الوطنية للأمن السيبراني

التسجيل والمراقبة

1. تحديد وتنفيذ عملية التسجيل والمراقبة بما يتماشى مع معيار تأمين المعلومات الوطنية[4].
2. تكوين جميع أصول المعلومات لتسجيل سجلات النظام والأمان الهامة. يجب أن تضمن المؤسسات تسجيل الأحداث المناسبة اللازمة لتحديد الحوادث الأمنية والمساعدة في التحقيق فيها.[5]
3. الاحتفاظ بالسجلات لمدة لا تقل عن 120 يومًا بما يتماشى مع قانون الجرائم الإلكترونية.
4. مراقبة سجلات الأمان على مدار الساعة طوال أيام الأسبوع، على الأقل فيما يخص الأنظمة المهمة.
5. يوصى بربط السجلات من الأنظمة المختلفة بشكل مشترك للحصول على نظرة شاملة للعمليات.
6. يجب أن تعمل عملية التسجيل والمراقبة بشكل وثيق مع عملية إدارة الحوادث، كما يلزم أن يكون نظام التسجيل والمراقبة قادرًا على توجيه الحوادث التي تم تحديدها من خلال نظام الاستجابة للحوادث.

التوعية الامنية

1. تحديد وتنفيذ برنامج توعية بأمن المعلومات للموظفين والمقاولين الذين يعملون داخل مؤسستك.
2. التأكد من تنفيذ برامج التوعية الأمنية على فترات منتظمة من خلال استخدام وسائل مختلفة.
3. يجب أن يتضمن برنامج التوعية الأمنية كحد أدنى ما يلي:
   أ. سياسات وإجراءات الأمن الداخلي للمؤسسات.
   ب. المتطلبات القانونية والتنظيمية
   ت. الاستخدام المقبول لمرافق معالجة المعلومات وأصول المعلومات.
   ث. معلومات عن إجراءات الإنفاذ والإجراءات التأديبية.
   ج. معلومات بشأن الإبلاغ عن الحوادث الأمنية.
   ح. معلومات حول الجهة التي يجب الاتصال بها في حالات الحوادث الأمنية.

الإبلاغ عن الحوادث وإدارتها

1. تحديد وتنفيذ عملية إدارة الحوادث بما يتماشى مع معيار تأمين المعلومات الوطنية.
2. وضع آليات للمستخدمين والموظفين للإبلاغ عن حوادث أمن المعلومات بطريقة مسؤولة.
3. تحديد اتفاقية مستوى الخدمة (داخليًا وخارجيًا) للاستجابة وإغلاق جميع الحوادث المبلغ عنها.
4. يشترط برنامج أمن المعلومات الإبلاغ عن جميع حوادث الأمن الإلكتروني إلى الوكالة الوطنية للأمن السيبراني والهيئة العامة للسياحة بقطر (إن أمكن).
5. الإبلاغ عن أي هجمات / حوادث إلكترونية في أسرع وقت ممكن، أو في غضون يومين من اكتشافها.

إخطار خرق البيانات

1. تُلزم اللوائح الخاصة في نطاق الخصوصية أصحاب البيانات بالإبلاغ في حالة حدوث خرق لمعلوماتهم الشخصية لدى المؤسسة.
2. حدد إجراءً لإخطار الأشخاص المعنيين بالبيانات عند اكتشاف حادث خرق للبيانات.

[4] يوفر معيار تأمين المعلومات الوطنية عناصر تحكم للتمكين من التسجيل والمراقبة.
[5] إرشادات لإدارة الحوادث - توفر الإجراءات المطلوبة مسبقًا أيضًا إرشادات إضافية خاصة بالنظام.

3. ويضمن الإجراء ما يلي:
   أ. تتكامل هذه العملية مع العمليات المؤسسية لإدارة الحوادث/إدارة الأزمات.
   ب. يجوز للوائح تحديد الفترة عند اكتشاف الخرق، والتي يتم خلالها تنفيذ هذا الإخطار.
   ت. لدى المؤسسة جرد فيما يخص أصحاب البيانات ممن ترد معلوماتهم الشخصية داخل بيانات أعمال المؤسسات.
   ث. تحدد المؤسسة وسائل وأدوات الاتصال المناسبة لإخطار أصحاب البيانات في حالة وقوع حادث خرق للبيانات محددة.

استمرارية الأعمال والمرونة

1. بالنظر إلى أن قطر تركز على أن تكون وجهة سياحية ورياضية، تعد صناعة الفنادق قطاعًا مهمًا لدولة قطر، ويتعين على المؤسسات ضمان تصميم الأعمال بشكل مرن يلائم مواجهة الكوارث الطبيعية / البشرية، والكوارث التكنولوجية و / أو الحوادث.
2. تعيين شخص لامتلاك وإدارة برنامج استمرارية الأعمال ونظام إدارة استمرارية الأعمال وثيق الصلة.
3. تطوير تخطيط استمرارية العمل الشامل (BCP) [6] الذي يغطي جميع الأنظمة الهامة.
4. يلزم أن يغطي تخطيط استمرارية العمل بشكل كاف الأشخاص (الأكثر أهمية) والعمليات والتكنولوجيا.
5. تصميم الأنظمة الحيوية لتكون متسامحة مع الأخطاء ومرنة.
6. اختبار تخطيط استمرارية العمل على فترات منتظمة بما في ذلك الاختبارات المباشرة وتجاوزات الفشل للتأكد من أن تخطيط استمرارية العمل سيعمل في حالة وقوع كارثة.

4.3.5 الضوابط الفنية

القسم أ: ضوابط تكنولوجيا المعلومات العامة

تصميم النظام والشبكة

تضمن المؤسسات أن الهندسة (تصميم الأنظمة والشبكات) بها قدر كبير جدا من الحماية عن طريق التصميم بدلاً من المحتويات الإضافية الموضوعة للتخفيف من عيوب التصميم. ويجب أن يتضمن تصميم النظام والشبكة كحد أدنى ما يلي:

1. التقسيم: فصل أصول المعلومات في قطاعات مختلفة (مناطق أمنية) بناءً على حساسيتها.
2. سطح الوصول: يقتصر الوصول فقط على أصول المعلومات على قنوات اتصال محدودة ومؤسسة. وعلاوة على ذلك، قم فقط بتوفير المعلومات المطلوبة. وقم بإخفاء جميع المعلومات الأخرى قدر الإمكان لتعزيز مفهوم "الأمن من خلال الغموض".
3. الدفاع في العمق: حماية أصول المعلومات على مستويات ونقاط متعددة باستخدام التقنيات والتكنولوجيات المتعددة. وتقييم أمان النظام على أساس الأصول الأقل أمانًا في النظام (الحلقة الأضعف).
4. الحماية الكافية: يجب أن تكون الضوابط الأمنية المختارة كافية ومناسبة بناءً على ملف المخاطر الخاص بالمؤسسة والمخاطر التي يتعرض لها الأصل نفسه بالإضافة إلى قيمة الأصل نفسه.
5. أقل امتياز /الحاجة إلى المعرفة يلزم التحكم في الوصول إلى أصول المعلومات بعناية وتقييده بناءً على مفاهيم أقل امتياز أو أساس الحاجة إلى المعرفة. ويجب إيلاء اهتمام خاص للحسابات الإدارية أو المميزة.

[6] راجع معيار تأمين المعلومات الوطنية ومعايير الصناعة مثل ISO 22301 للحصول على إرشادات إضافية.

6. الخصوصية حسب التصميم: حماية المعلومات الشخصية هي مطلب تنظيمي رئيسي على الصعيدين المحلي والدولي. وتنص اللائحة على عدد من الحقوق للأفراد مثل الحق في النسيان، والحق في المعلومات، والحاجة إلى الموافقة وما إلى غير ذلك. ومن الضروري أن يتم تصميم الأنظمة بما يتماشى مع المتطلبات التنظيمية الخاصة بالخصوصية.
7. الوفرة: الحماية من نقطة عطل مفردة، باستخدام العناصر الزائدة عن الحاجة ومفاهيم الوفرة العالية.

أمن النظام والشبكة

تغطي معيار تأمين المعلومات الوطنية ضوابط متعمقة لأمن النظام والشبكة. يرد في القسم أدناه أهم العناصر:

1. **التكوين:**
   أ. تأمين تكوين جميع أجهزة الشبكات والأمن.
   ب. ويلزم تخزين نسخة من التكوين المحدث والمختبَر في مكان آمن لاستخدامه في حالة وقوع كارثة.
2. **جدران الحماية / الخوادم الوكيلة:**
   أ. استخدم جدران الحماية لتقسيم الأنظمة وفقًا لمناطق الأمان المختلفة.
   ب. استخدم جدار حماية مناسبًا لتنظيم حركة المرور (التطبيق / الحزم / البروتوكولات / المنافذ) بناءً على نموذج الربط البيني للأنظمة المفتوحة.
   ت. قم بتكوين جدار الحماية بقواعد مناسبة ودقيقة.
   ث. قم بتوجيه أي حركة مرور من الإنترنت من خلال خادم وكيل.
3. **تزامن الساعة:**
   أ. قم بتكوين خادم الوقت لمزامنة جميع الأجهزة الموجودة على الشبكة مع نفس مصدر الوقت.
4. **أمن الشبكات اللاسلكية:**
   أ. احتفظ بقائمة جرد لنقاط الوصول اللاسلكية. فضلاً عن مراقبة واكتشاف وإزالة نقاط الوصول اللاسلكية المارقة.
   ب. تكوين النظام لاستخدام المصادقة والتشفير المناسبين.
   ت. استخدم جدار الحماية / أجهزة التوجيه لفصل الشبكات. استخدم معرف مجموعة خدمات وتكوينات مختلفة لشبكات مناطق الأمان المختلفة.
   ث. راجع أيضًا إرشادات الأمن السيبراني الخاصة بنا لتأمين أجهزة التوجيه[7] المنزلية والمكتبية الصغيرة فيما يخص أجهزة التوجيه وتوصيات إعداد نقاط الوصول.
5. **نظام اسم النطاق:**
   أ. استخدم خوادم نظام اسم النطاق المنفصلة لتحليل العناوين الداخلية والخارجية.
   ب. توقيع ملفات المناطق رقميًا، وتوفير المصادقة المتبادلة المشفرة وتكامل البيانات لعمليات نقل المنطقة والتحديثات الديناميكية. وكذلك توفير مصادقة أصل التشفير وضمان سلامة بيانات نظام اسم النطاق.
6. **شبكة خاصة افتراضية:**
   أ. يجب أن تكون أي اتصالات عن بُعد لأنظمة الأعمال من خلال شبكة خاصة افتراضية.
   ب. يجب أن تتم الاتصالات بالأنظمة الحيوية للأعمال من خلال شبكة خاصة افتراضية، حتى عند الاتصال من خلال الأنظمة اللاسلكية للأعمال.

[7] متوفر على الموقع الالكتروني للوكالة الوطنية للأمن السيبراني

ت. تعامل مع حركة المرور من خلال اتصال شبكة خاصة افتراضية بنفس طريقة التعامل مع حركة المرور التجارية وقم بتصفيتها من خلال نفس عمليات التحقق (المراقبة والتحكم).

7. تصلب النظام:

أ. يجب أن تتوافق جميع الأنظمة مع الحد الأدنى من الوضع الأساسي. ويشمل ذلك كحد أدنى ما يلي:

i. تطبيق جميع حزمة الأمان المعروفة.
ii. تعطيل جميع الخدمات غير المرغوب فيها وإلغاء تثبيت جميع التطبيقات غير المرغوب فيها.
iii. تمكين السجلات اللازمة للتدقيق ورصد النظام والأمن[8].
iv. قم بتثبيت برنامج حماية نقطة النهاية على سبيل المثال برامج مكافحة البرامج الضارة، ونظام كشف التسلل المرتكز على المضيف، جدار حماية التطبيقات، وما إلى غير ذلك.
v. تقييم الضعف (خاصة للخوادم) لتحديد نقاط الضعف المعروفة.

ب. يجب على المؤسسة تحديد ملفات تعريف التقوية للأنظمة المختلفة التي تستخدمها بناءً على متطلبات الأمان.

ت. ضمان الحماية ضد هجمات حجب الخدمة الموزعة. توفر إرشادات الأمن السيبراني لهجمات حجب الخدمة الموزعة[9] (DDoS) إرشادات وتوصيات لمواجهتها.

8. أمان نقطة النهاية

أ. سجل كل نقطة نهاية في سجل أصول المعلومات.
ب. قم بتثبيت برنامج تم اختباره لمكافحة البرمجيات الضارة على جميع الأنظمة.
ت. تسجيل ومراقبة وتوجيه التنبيهات من نظام أمان نقطة النهاية.
ث. قم بتكوين نظام كشف التسلل المرتكز على المضيف (HIDS) و / أو جدران حماية التطبيقات على الخوادم.
ج. قم بتقييم وتثبيت حلول الحماية من تسرب البيانات لنقاط النهاية التي يمكنها الوصول إلى البيانات المهمة للأعمال و / أو بيانات معلومات التعريف الشخصية لعملائك / موظفيك.

9. الخصوصية حسب التصميم

أ. مقابل كل أصول المعلومات الجديدة التي تم إدخالها في النظام، يلزم ما يلي:

i. تحديث سجل أصول المعلومات.
ii. تحديد معلومات التعريف الشخصية التي تنشئها أو تعالجها أو تخزنها.
iii. إجراء تحليل تأثير حماية خصوصية البيانات (DPIA) لتحديد مدى أهمية البيانات وضوابط الأمان المحتملة لتأمين معلومات تحديد معلومات التعريف الشخصية.

أمان المنتج

يغطي معيار تأمين المعلومات الوطنية ضوابط متعمقة لأمان المنتج. يرد في القسم أدناه أهم العناصر:

1. أي منتج يتم اختياره لحل مشكلة العمل أو تلبية متطلبات العمل يجب أن:
أ. الحصول على الدعم من بائع يتمتع بمكانة جيدة ويفي بالتزامه.

[8] الرجوع إلى إرشادات إدارة الحوادث - الإجراءات المطلوبة مسبقًا
[9] متوفر على الموقع الالكتروني للوكالة الوطنية للأمن السيبراني

ب. أن يتم الاختيار من خلال عملية مستقلة وغير متحيزة لاختيار البائعين / المنتج.
ت. الخضوع للاختبار بشكل مستقل للتأكد من أنه يلبي جميع متطلبات العمل والأمن الخاصة بالعمل.

2. يتم ضمان الحد الأدنى من مستويات ضمان الأمان للمنتجات المختارة لوظائف الأعمال الهامة.
3. تأكد من أن المنتجات لا تحتوي على أي أسماء مستخدمين وكلمات مرور مشفرة. تغيير جميع كلمات المرور الافتراضية قبل استخدامها في شبكات الأعمال.

أمن البرمجيات

يغطي معيار تأمين المعلومات الوطنية ضوابط متعمقة فيما يخص أمن البرمجيات. يرد في القسم أدناه أهم العناصر:

1. الالتزام بضوابط الأمان وإدراجها ضمن دورة حياة تطوير الأنظمة (SDLC).
2. تتضمن دورة حياة تطوير الأنظمة بناء نموذج نضج الأمن (BSIMM)ونموذج أواسب لنضج وضمان البرامج (OSAMM) من بين أمور أخرى.
3. اختبر أمان أي برنامج تم نشره في شبكات الأعمال. ويشمل هذا الاختبار، اختبار الثغرات الأمنية، واختبار الاختراق، ومراجعات الأكواد وما إلى غير ذلك. وقم بإجراء مراجعات للكود لأكثر التطبيقات أهمية. وفيما يخص التطبيقات المهمة و / أو التي تواجه الإنترنت، يجب إجراء الاختبار على فترات منتظمة (على الأقل على أساس نصف سنوي).
4. قم بمراجعة الإرشادات المقدمة من وزارة المواصلات والاتصالات[10]، والالتزام بها، إذا كانت المؤسسة تنوي استخدام برمجيات مفتوحة المصدر.

الأمن السحابي

تغطي معيار الأمن السحابي[11] ضوابط متعمقة تخص أمان البرنامج. علاوة على ذلك ، يوفر مستشار موقع البيانات[12] إرشادات إضافية حول استخدام موفري خدمات الحوسبة السحابية الموجودين خارج قطر.

1. يجب أن تستضيف المؤسسات بيانات الأعمال الهامة داخل قطر (إلى أقصى حد ممكن) أو في البلدان التي لديها علاقات ودية (سياسية) مع أنظمة تنظيمية مماثلة لدولة قطر.
2. تشفير البيانات المخزنة خارج قطر فيما يخص المتطلبات التنظيمية أو متطلبات استمرارية الأعمال.

يجب أن تفي معلومات التعريف الشخصية (PII) المخزنة / المعالجة في الأمن السحابي بالمتطلبات التنظيمية لخصوصية البيانات محليًا ودوليًا.

إدارة الهوية والوصول /إدارة امتياز الوصول

يوفر إطار عمل المصادقة الإلكترونية في قطر إطارًا [13] قويًا لبناء حل للمصادقة الإلكترونية داخل المؤسسة.

تغطي معيار تأمين المعلومات الوطنية ضوابط أمنية متعمقة لإدارة الهوية والمصادقة.

أمان الوسائط

[10] متوفر على الموقع الالكتروني للوكالة الوطنية للأمن السيبراني
[11] متوفر على الموقع الالكتروني للوكالة الوطنية للأمن السيبراني
[12] متوفر على الموقع الالكتروني للوكالة الوطنية للأمن السيبراني
[13] متوفر على الموقع الالكتروني للوكالة الوطنية للأمن السيبراني

تغطي معيار تأمين المعلومات الوطنية ضوابط متعمقة فيما يخص أمن الوسائط. يرد في القسم أدناه أهم العناصر:

1. يجب أن تراعي ضوابط الأمان للوسائط تأثيرات الخصوصية جنبًا إلى جنب مع اعتبارات الأمان.
2. حسب التصميم، لا تحتفظ بالبيانات / الوسائط بما يتجاوز ما هو مطلوب. وطالما يتم الاحتفاظ بالبيانات / الوسائط (طوال دورة حياتها وفي جميع الأشكال) يجب حمايتها وفقًا لملف تعريف الأمان الخاص بها.
3. يجب تطبيق وسائل عملية وكافية للتخلص من البيانات التي أفادت بالغرض ويلزم اتلافها.

استخدام جهازك الخاص

تغطي سياسة "استخدام جهازك الخاص"[14] ضوابط أمنية متعمقة لأي جهاز شخصي مستخدم في شبكة / نظام الأعمال. ويتضمن ذلك أي أجهزة مثل التخزين (يو إس بي) والموجهات اللاسلكية والهواتف المحمولة / الأجهزة اللوحية وما إلى ذلك. وبالإضافة إلى ذلك، تتضمن معيار تأمين المعلومات الوطنية أيضًا ضوابط أمنية فيما يخص نظام "استخدام جهازك الخاص".

تطوير وسائل التواصل الاجتماعي

تعتبر السمعة أمر بالغ الأهمية لصناعة الفنادق والترفيه. حيث تلعب وسائل التواصل الاجتماعي دورًا مهمًا في تحديد صورة المؤسسة وتصورها في العالم الافتراضي. وعلى هذا النحو، فمن المهم تأمين قنوات التواصل الاجتماعي ضد التهديدات السيبرانية المحتملة. إذ توفر إرشادات الأمن فيما يخص تأمين حسابات وسائل التواصل الاجتماعي توصيات مفصلة للشركات لمساعدتهم على تأمين قنواتهم على وسائل التواصل الاجتماعي.

النظام الحرج

الموقع الإلكتروني والحجز عبر الإنترنت

تكون أيضًا ضوابط الأمان المذكورة في قسم أمان البرنامج وأمان المنتج أعلاه، إلى جانب معيار تأمين المعلومات الوطنية، قابلة للتطبيق فيما يخص بوابة التجارة الإلكترونية (حجز الفنادق). يمكنك أيضًا الرجوع إلى "ضوابط أمن المعلومات" من أجل تطوير مواقع الويب وإرشادات الاستضافة[15] للحصول على معلومات إضافية. ويرجى الانتباه تحديدًا للجوانب التالية:

1. المصادقة: استخدام الشهادات الرقمية من جهات موثوقة (مزودي الخدمات السحابية، ويفضل مزودي الخدمات السحابية القطريين) للتحقق من هوية مزود خدمة البوابة.
2. الخصوصية:
   أ. جمع البيانات المطلوبة فقط. تخلص من البيانات بمجرد إنجاز المتطلبات (بما في ذلك المتطلبات التنظيمية).
   ب. تشفير البيانات طوال دورة حياتها من التجميع والمعالجة والتخزين وصولا إلى التخلص منها.
3. السلامة: يُقصد بسلامة المعلومات التأكد من أن الاتصال المستلم لم يتم تغييره أو العبث به. في بوابة التجارة الإلكترونية، يمكن تحقيق ذلك باستخدام الشهادات الرقمية «لتوقيع» الرسائل رقميًا.

[14] متوفر على الموقع الالكتروني للوكالة الوطنية للأمن السيبراني

[15] متوفر على الموقع الالكتروني للوكالة الوطنية للأمن السيبراني

4. التقسيم: تأكد من التقسيم المناسب بين خوادم الويب وخوادم قواعد البيانات. استخدم "منطقة منزوعة السلاح" (DMZ) للأصول التي تواجه الإنترنت لمنع المهاجم من الوصول المباشر إلى الأصول الداخلية في حالة حدوث خرق.
5. الوفرة: تحديد استراتيجية النسخ الاحتياطي لقواعد البيانات والتطبيقات. وإجراء التخزين خارج الموقع للبيانات الحرجة.
6. عدم الانكار: عدم الانكار هو القدرة على إثبات أن شخصًا ما قد أرسل بريدًا إلكترونيًا معينًا أو طلب خدمة أو وافق على الشراء من موقع ويب بشكل قانوني. ويتحقق عدم الإنكار، في مجال التجارة الإلكترونية باستخدام التوقيعات الرقمية.
7. الامتثال لمعيار أمان بيانات صناعة بطاقات الدفع: تأكد من أن بوابة الدفع الخاصة بك متوافقة مع عيار أمان بيانات صناعة بطاقات الدفع. ويلزم على المؤسسات توخي مزيد من الحذر في اختيار بائعي نظام نقاط البيع ومعالجات بطاقات الائتمان الخاصة بهم. وكذلك فحص اتفاقيات الطرف الثالث مع هذه الكيانات ويجب أن تصبح الالتزامات الأمنية جزءًا من هذه الاتفاقيات.
8. الاختبار: الاختبار المنتظم لبوابة التجارة الإلكترونية من أجل:

أ. التحقق من مواصفات متطلبات الأمان مثل موقع الأصل (الأصول)، وآلية التحكم في الوصول للأصول، والسياق التشغيلي للمؤسسة، وخدمات النظام الحالية وآليات التحكم في الوصول الخاصة بها، والاتصال داخل المؤسسة وربط المؤسسة بـالعالم الخارجي.
ب. التحقق من تكوين أدوات الأمان المحددة في البنية التحتية للأمان، أي ما إذا كانت أدوات الأمان مثبتة ومهيأة بشكل صحيح للحفاظ على أمان الأصل.
ت. التحقق من تحديث كافة حزم الأمان المعروفة أو التخفيف من حدتها بشكل مناسب.
ث. التحقق من وجود أي فجوة بين البنية التحتية الأمنية المقترحة والبنية التحتية الأمنية المطبقة.
ج. التحقق من قيود البنية التحتية الأمنية المقترحة فيما يتعلق بالثغرات الأمنية المعروفة

محطات نقاط البيع (المطاعم)

الاتجاه العام بين المستخدمين هو الاعتقاد بأن أجهزة الكمبيوتر فقط هي التي تتعرض للخطر السيبراني. وبناء على هذا الاعتقاد، يتم تجاهل الأجهزة الكهروميكانيكية مثل الطابعات والأجهزة متعددة الوظائف (الماسحات الضوئية للطابعة وآلات النسخ وما إلى غير ذلك) أو المحطات الطرفية الصغيرة (أجهزة نقاط البيع أو أنظمة العرض أو المعلومات) بشكل عام عندما يتعلق الأمر بحزم الأمان أو الحماية من نقاط الضعف على الرغم من أن هذه الأجهزة قد تكون متصلة بنفس الشبكة مثل أنظمة الأعمال.

وتعد محطات نقاط البيع مكانًا رائعًا للجهات الفاعلة الضارة التي تبحث عن معلومات شخصية مثل تفاصيل بطاقة الائتمان والتفاصيل الشخصية / المعلومات الخاصة بنزلاء الفندق. ونتيجة لذلك، تهاجم الجهات الضارة محطات نقاط البيع لاستغلال بيانات بطاقة الائتمان ومعلومات الضيف الموجودة عليها.

1. ضمان تطبيق سياسة كلمات السر المؤسسية على أنظمة نقاط البيع أيضًا.
2. تأمين أنظمة نقاط البيع (الأجهزة/البرامج) بانتظام للتخفيف من أي نقاط ضعف معروفة.
3. فصل أجهزة نقاط البيع على شبكة منفصلة لتقييد انتشار البرامج الضارة أو فقدان المعلومات من الأنظمة الأخرى في حالة حدوث خرق.
4. يصعب تحديد متغيرات البرامج الضارة لنقاط البيع، لذلك من المهم أن يكون لدى المؤسسات خبراء يجرون بانتظام اختراقًا عميقًا لاكتشاف نقاط الضعف المحتملة قبل أن يتمكن الفاعلون الضارون من الاستفادة منها.
5. تقييد الوصول إلى الإنترنت: تطبيق قوائم التحكم في الوصول على تكوين جهاز التوجيه للحد من حركة المرور غير المصرح بها من وإلى أجهزة نقاط البيع.

6. عدم السماح بالوصول عن بُعد: يمكن لمجرمي الإنترنت استغلال تكوينات الوصول عن بعد على أنظمة نقاط البيع للوصول إلى هذه الشبكات. ولمنع الوصول غير المصرح به لأنظمة نقاط البيع، لا تسمح بالوصول عن بعد إلى شبكة نقاط البيع في جميع الأوقات.
7. تعطيل البروتوكولات اللاسلكية غير المرغوب فيها مثل البلوتوث وخدمة الراديوية العامة للرزم إذا لم يكن ذلك مطلوبًا.
8. استخدم التعمية بين الطرفيات إن أمكن.

شبكة واي-فاي الضيف

الإنترنت اللاسلكي هو أحد أكثر الخدمات المرغوبة للنزلاء داخل الفندق. ويشمل ذلك الضيوف المقيمين في الفندق أو أولئك الذين يحصلون على خدمات / يستخدمون مرافق معينة (مثل استخدام المرافق الصحية / حضور الأحداث / المطاعم / زوار نزلاء الفندق وما إلى ذلك). ومع ذلك، فإن الخدمة معرضة لخطر إساءة استخدامها من قبل الضيوف أو الجهات الفاعلة الضارة الذين قد يتمكنون من الوصول إلى شبكة واي-فاي الفندق بطريقة أو بأخرى.

توفر إرشادات الأمن السيبراني لشبكات الواي-فاي العامة[16] توصيات لنشر نظام واي-فاي عام آمن. يرد في القسم أدناه أهم العناصر:

أ. احتفظ بقائمة جرد لنقاط الوصول اللاسلكية. فضلاً عن مراقبة واكتشاف وإزالة نقاط الوصول اللاسلكية المارقة.
ب. تكوين النظام لاستخدام المصادقة والتشفير المناسبين.
ت. استخدم جدار الحماية / أجهزة التوجيه لفصل الشبكات. استخدم معرف مجموعة خدمات وتكوينات مختلفة لشبكات مناطق الأمان المختلفة.
ث. راجع أيضًا إرشادات الأمن السيبراني الخاصة بنا لتأمين أجهزة التوجيه[17] المنزلية والمكتبية الصغيرة فيما يخص أجهزة التوجيه وتوصيات إعداد نقاط الوصول.

أمن إنترنت الأشياء

تضم صناعة الفنادق عددًا من تقنيات إنترنت الأشياء مثل التلفزيون الذكي، والثلاجة الصغيرة الذكية، وأدوات التحكم في الإضاءة الذكية، والأبواب الذكية وما إلى ذلك لتعزيز راحة ضيوفها. يغطي معيار الأمان القطري الذكي[18] ضوابط متعمقة تخص أمن إنترنت الأشياء.

[16] متوفر على الموقع الالكتروني للوكالة الوطنية للأمن السيبراني

[17] متوفر على الموقع الالكتروني للوكالة الوطنية للأمن السيبراني

[18] يمكن توفير معيار الأمان القطري الذكي عند الطلب.

5 الامتثال والإنفاذ

5.1 الامتثال والإنفاذ

تم نشر هذا الدليل الإرشادي لمساعدة المؤسسات في قطاع الضيافة على فهم التهديدات السيبرانية والمخاطر التي تتعرض لها أنظمة المعلومات الخاصة بهم بشكل أفضل، فضلاً عن فهم كيفية التخفيف من مثل هذه التهديدات.

الدليل الإرشادي يكمل معيار تأمين المعلومات الوطنية، وسياسة تصنيف البيانات الوطنية. يجب على المؤسسات الالتزام بالقانون رقم 13 لسنة 2016 بشأن حماية خصوصية البيانات الشخصية (PDPPL) عند تأمين أنظمتها..

6 المرفقات

6.1 الاختصارات

APT تهديد مستمر متقدم

DDoS هجمات حجب الخدمة الموزعة

ISP مزود خدمة الإنترنت

NCSA الوكالة الوطنية للأمن السيبراني

6.2 المراجع

لا توجد مراجع

6.3 قائمة الأشكال

لا يوجد رسومات توضيحية

6.4 الإبلاغ عن الحوادث إلى الوكالة الوطنية للأمن السيبراني

يمكن للمؤسسات التي تواجه هجوم حجب الخدمة الموزعة إبلاغ الوكالة الوطنية للأمن السيبراني عن الحادث بإحدى الطرق التالية:

الاتصال بالخط الساخن الخاص بالوكالة الوطنية للأمن السيبراني على رقم 16555 (خدمة على مدار الساعة طوال أيام الأسبوع)

إرسال بريد الإلكتروني على البريد الالكتروني الخاص بالوكالة الوطنية للأمن السيبراني ncsoc@ncsa.gov.qa

قد تجد المؤسسات أيضًا الإرشادات التالية مفيدة في الاستعداد لمواجهة أي هجوم / حادث.

إرشادات لإدارة الحوادث - الإجراءات المطلوبة مسبقًا