الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

مبادئ توجيهية

حول برامج الفدية

إخلاء المسؤولية/ الحقوق القانونية

قامت الوكالة الوطنية للأمن السيبراني بتصميم وإنشاء هذه الوثيقة، بعنوان "مبادئ توجيهية خاصة ببرامج الفدية" - النسخة 1.0- وهو مستند سري حالياً وسوف يتم نشره بعد الاعماد بهدف مساعدة المؤسسات على فهم ماهية برامج الفدية وطرق التخفيف من حِدتها.

تُعد الوكالة الوطنية للأمن السيبراني الجهة المسؤولة عن مراجعة وصيانة هذه الوثيقة.

وعلى كل من يقوم بأي عملية نسخ لهذه الوثيقة إما بشكل كامل أو بأجزاء وبغض النظر عن طريقة النسخ، التصريح بأن الوكالة الوطنية للأمن السيبراني هي المصدر والمالك للوثيقة "الإرشادات التوجيهية الأمنية السيبرانية الخاصة ببرامج الفدية".

أما فيما يخص عملية استنساخ هذه الوثيقة بنية التسويق، فيجب أن يتم عبر إذن كتابي من الوكالة الوطنية للأمن السيبراني وتحتفظ الوكالة بالحق في تقييمه وتقييم مدى قابلية تطبيقه لأغراض تجارية.

لا ينبغي تفسير التفويض من الوكالة الوطنية للأمن السيبراني بأنه تصديق على النسخة المّطورة ولا يجب على المطور أن يقوم بنشر أو إساءة تفسير هذه الوثيقة بأي شكل من الأشكال سواء في وسائل الاعلام أو في النقاشات الشخصية /الاجتماعية.

التفويض القانوني

ينص المرسوم الأميري رقم (1) لعام 2021 على إنشاء الوكالة الوطنية للأمن السيبراني، وإعطاءها سُلطة الإشراف على البنية التحتية الوطنية الحيوية وتنظيمها وحمايتها من خلال تقديم وإصدار السياسات والمعايير وضمان الامتثال.

وفي هذا السياق، فقد تم إعداد هذه الوثيقة مع الأخذ بعين الاعتبار القوانين المعمول بها في دولة قطر. في حال نشوء أي تعارض بين هذه الوثيقة (سواء أحكام أو بنود محددة) وأي من قوانين دولة قطر، فتكون الأولوية للقانون. وفي حال وجود أي حكم أو بند يتعارض مع القانون، يجب حذفه من هذه الوثيقة دون التأثير على بقية البنود. وفي هذه الحالة، يجب أن تُجرى التعديلات لضمان الامتثال مع القوانين ذات الصلة والمعمول بها في دولة قطر.

جدول المحتويات

1. المقدمة

1.1 السياق

تواجه نُظم المعلومات اليوم مخاطر غير مسبوقة من قِبل عوامل تهديد كثيرة تشمل الوصول الغير مُصرح به للمعلومات، التعديل غير المُصرح به للمعلومات، عدم توافر المعلومات وغيرها الكثير. تنشأ هذه المخاطر من الهجمات كهجمات البرمجيات الضارة وهجمات برامج الفدية والتي قد تؤدي إلى ضياع البيانات أو جعلها غير قابلة للاستخدام أو القيام بتشفيرها، بالإضافة إلى هجمات الحرمان من الخدمة، الهجمات المادية على نُظم المعلومات ومرافق المعالجة وغيرها..

تُعد برامج الفدية ضمن الهجمات التي تسببت أضراراً كبيرة بدءً من المؤسسات الصغيرة والمتوسطة إلى الشركات الكبيرة والمؤسسات الحكومية، فالعديد من المؤسسات والقطاعات المتنوعة وقعت ضحية لهذه الهجمات.

وخلاصة القول، إن نُظم المعلومات حالياً أكثر عُرضة لتسريب البيانات وانقطاع الخدمات أكثر من أي وقت مضى. وتُشكل هجمات برامج الفدية تهديداً كبيراً لجميع الشركات الكبيرة والصغيرة، وقد تزايدت مخاطر برامج الفدية من حيث الحجم والتعقيد والضرر. وباتت تمتلك القدرة على الوصول الغير مُصرح به للمعلومات (تسريب البيانات) وانتهاكات النزاهة (تشفير البيانات وإلغاء فائدتها)، مما يؤدي إلى عدم توافر المعلومات. ولهذا، تستطيع المؤسسات استخدام هذه الإرشادات التوجيهية لفهم مخاطر هجمات برامج الفدية وكيف يمكن تفاديها.

2. الهدف، النطاق والاستخدام

2.1 الهدف

تزويد المؤسسات في دولة قطر بالمعرفة اللازمة لفهم هجمات برامج الفدية وطريقة التصدي لها.

2.2 النطاق

جميع المؤسسات التي تتعامل مع أجهزة الكمبيوتر والأجهزة الرقمية للقيام بأعمالها.

2.3 الاستخدام

تُساهم الإرشادات المتوفرة في هذه الوثيقة في مساعدة المؤسسات لتأمين بُنيتهم الرقمية ضد هجمات برامج الفدية، كما ويقدم توضيحات حول مفهوم برامج الفدية وأنواعها وطُرق التعافي منها.

3. المصطلحات الرئيسية

المؤسسة	أي منظمة تجارية تعمل في دولة قطر، سواء كانت ربحية أو غير ربحية.
أجهزة الكمبيوتر	أي جهاز كمبيوتر أو جهاز طرفي أو جهاز شبكة أو خادم، وما إلى ذلك، يملكه أو يؤجره العميل.
الشبكة العميقة	أي جزء من المعلومات عبر الانترنت لا تتم فهرسته بواسطة محركات البحث، ويضمن ذلك على سبيل المثال مواقع الانترنت التي تفصل محتواها خلف جدران الدفع ومواقع الانترنت المحمية بكلمة مرور ومحتويات رسائل البريد الإلكتروني، وغيرها.
الشبكة المُظلمة	مجموعة فرعية من الشبكة العميقة، وترتبط عادة بالسلوك الإجرامي والأنشطة المشبوهة، ويتم إخفاء المحتوى على الشبكة المظلمة عن قصد حيث يتطلب برامج خاصة مثل أداة إخفاء الهوية وأداة التشفير، مثل متصفح (Tor) للوصول. وتميل هذه الشبكات إلى إبقاء مستخدميها ومواقعهم مجهولة الهوية.
فك التشفير	برنامج مُحدد يستخدم لإزالة التشفير الذي تسببت به هجمات برامج الفدية على البيانات.
البرامج الضارة	يُشير إلى أي برنامج تم تصميمة من أجل إلحاق الضرر في جهاز الكمبيوتر أو الخادم أو العميل أو شبكة كمبيوتر مثل تسريب المعلومات الخاصة أو السرية، أو التمكن من الوصول الغير مصرح به إلى المعلومات أو الأنظمة أو منع الوصول إلى المعلومات. أمثلة على البرامج الضارة: Viruses, worms, trojans, spyware, adware

4. المبادئ التوجيهية

4.1 ماهي برامج الفدية؟

برامج الفدية هي شكل من أشكال الابتزاز الإلكتروني وهي برامج ضارة تستخدمها الجهات الخبيثة بهدف ابتزاز الأموال من الآخرين. وتصنف حالياً على أنها من بين أكبر التهديدات العالمية كما ولوحظت أيضاً هجمات استهدفت المُؤسسات والشركات في دولة قطر.

تعمل برامج الفدية بطريقتين، إما بطريقة منع الوصول إلى النظام وتسمى برامج الفدية المزودة بقفل (Locker Ransomware)، أو بطريقة تشفير الملفات ويُطلق عليها اسم برامج الفدية المُشفِرة (Crypto Ransomware).

وضمن نطاق أوسع لأمن المعلومات، تؤثر برامج الفدية عادة على الركائز الثلاثة (السرية، النزاهة، والوفرة)، حيث لوحظ في بعض الحالات بأن المهاجم يقوم بسحب المعلومات ونشرها للعامة إذا لم يتم دفع الفدية المطلوبة مما يؤثر على ركيزة السرية.

4.2 أنواع هجمات برامج الفدية

4.2.1 برامج الفدية المزودة بقفل

يقوم هذا النوع من برامج الفدية بمنع جهاز الحاسوب من القيام بوظائفه الرئيسية، ويقوم بالسيطرة على الجهاز مما يمنع المتضررين من التمكن من الوصول إلى جهاز الكمبيوتر الخاص بهم. وبذلك،

يمكن للمتضررين التمكن فقط من رؤية شاشة القفل أو التفاعل مع شاشة تحتوي على برنامج الفدية. بعد ذلك، يقوم المهاجم بتنشيط الفأرة ولوحة المفاتيح جُزئياً حتى يقوم المتضرر بإجراء عملية الدفع لبرنامج الفدية. ولا تقوم برامج الفدية المُزودة بقفل بتدمير البيانات بصورة كاملة، حيث أن هدفها الأساسي هو منع المتضررين من الوصول إلى البيانات. إضافة على ذلك، يقوم برنامج الفدية بعرض مؤقت زمني يُحدد موعد تسليم الفدية بهدف الضغط على الضحية للقيام بعملية الدفع.

بعض الأمثلة الأكثر شيوعاً لبرامج الفدية المزودة بقفل هي: Petya/NotPetyag Bad Rabbit وغيرها..

4.2.2 برامج الفدية المُشفِرة

يقوم هذا النوع من برامج الفدية بتشفير البيانات أو المعلومات أو الملفات الموجودة على أجهزة المتضررين دون التدخل في وظائف جهاز الحاسوب الأساسية. إذ يمكم للمتضررين استخدام النظام ورؤية البيانات ولكن لا يمكنهم الوصول إلى بياناتهم بسبب تشفيرها. ويقوم برنامج الفدية بالطلب من المتضررين بدفع الفدية خلال فترة زمنية معينة وإلا سوف تُحذف جميع بياناتهم المُشفرة أو سيتم الكشف عنها للعامة بصورة دائمة.

بعض الأمثلة الأكثر شيوعاً لبرامج الفدية المُشفِرة هي: Cryptolocker و LockygWannacry

وهنالك نوع من برامج الفدية يُعرف باسم doxware أو leakware حيث يقوم فيها المهاجم بتصفية البيانات بدلاً من تدميرها ثم تهديد المتضررين بنشرها للعامة.

4.3 فهم مخاطر برامج الفدية

جميع أجهزة الحاسوب المُتصلة بالإنترنت مُعرضة لخطر برامج الفدية، وتتم الإصابة بهذه البرامج عادة عن طريق المرفقات الضارة المنتشرة عبر البريد الالكتروني الاحتيالي (phishing)، وعن طريق التنزيلات من خلال مواقع الشبكات الضارة، واستغلال المجموعات التي تستغل البرامج الغير مُصححة.

وعلى مر السنين، لوحظ أن المهاجمين لم يقوموا بنشر بيانات أي أحد، وبأن هذه الهجمات حدثت للمستخدمين والأفراد والمؤسسات الحكومية الصغيرة والمتوسطة والشركات الكبيرة. وفي الماضي القريب، كانت هناك حوادث في مؤسسة رئيسية لحاويات الشحن وعدة مستشفيات (حتى خلال فترة كوفيد)، وغيرهم.

أما بالنسبة للعوامل التي ساهمت في انتشار برامج الفدية، فهي الجهد مقابل العوائد والعملة المُشفرة التي ساعدت في إبقاء هوية المهاجم مجهولة، واستعداد المؤسسات لدفع الفدية خاصة في حالة توافر تأمين سيبراني. وأحد العوامل الأخرى المهمة هو التسهيلات التي تقدمها الخدمات المظلمة مثل خدمة الفدية (Ransomware As A Service - RAAS).

4.3.1 احتمالية التعرض للهجوم

هنالك الكثير من العناصر التي تساهم في رفع احتمالية التعرض لهجمات برامج الفدية، مثل المؤسسة وقوتها المالية والتي تزيد من احتمالية قيام أصحاب المؤسسات بدفع الفدية، بالإضافة إلى امتلاك المؤسسات لتأمين سيبراني يجعلهم أهدافاً جذابة لهجمات برامج الفدية. فقد تبين بأن الجهات الضارة تحاول معرفة ما إذا كانت ضحيتهم المحتملة تمتلك تأمين سيبرانياً أم لا مما يؤدي إلى زيادة احتمالية دفع الفدية.

4.3.2 من الذي يمكنه مهاجمة مؤسستك؟

يمكن أن تصدر هجمات برامج الفدية من عوامل تهديد داخلية أو خارجية. وتشمل عوامل التهديد الداخلية موظفي المؤسسة الدائمين أو اللذين تم التعاقد معهم مؤقتاً وذلك إما لعدم رضاهم لأسباب مختلفة أو لأغراض خبيثة. أما بالنسبة لعوامل التهديد الخارجية، فتشمل المجرمين السيبرانيين أو المجرمين المدعومين من دولة معينة، وترتبط عادةً هجمات برامج الفدية الصادرة من قِبل عوامل تهديد خارجية بدوافع مالية أو دوافع سياسية لاستهداف الدولة.

إن من شأن التعرف على نوعية عوامل التهديد، أن يساعد المؤسسة على فهم دوافع المهاجمين وقدراتهم ومدى تعقيد الهجوم مما يسهم في وضع استراتيجية مناسبة للتعامل مع مثل هذه الهجمات.

4.3.3 دوافع المهاجمين

بالرغم من أن الدافع الرئيسي لهجمات برامج الفدية هو الحصول على المال، إلا أن هنالك دوافع سياسية وأيديولوجية خصوصاً في حالة هجمات برامج الفدية لأغراض سياسية والمدعومة من قبل دول معينة.

مع ذلك، فقد لوحظ في بعض الحالات بأن المؤسسات المتضررة تتعرض لفقد البيانات رغم دفعهم لمبلغ الفدية (عند قيام المهاجم بتوفير المفتاح الخاطئ أو عدم توفير المفتاح)، ومع ذلك، يتم استهداف المؤسسة مرة أخرى للدفع لبرامج الفدية الضارة.

4.3.4 تحديد مناطق الخطر

يجب على المؤسسات القيام بالتالي لتتمكن من تحديد مناطق الخطر:

1. فهم المخاطر المتعلقة بالقطاع ككل.
2. معرفة قُدرات عوامل التهديد.
3. تحديد نُظم العمل وأصول البيانات الحرجة والضوابط التي يمكن القيام بها لتخفيف المخاطر.
4. معرفة حدود المنطقة المُعرضة للهجوم، مثل تحديد عدد نقاط الدخول وعوامل التهديد التي يمكن استغلالها في الهجوم.
5. تقييم الحد الأقصى للفترة المسموح بها للتوقف عن العمل والتكلفة المترتبة على ذلك.

ستساعد العوامل المذكورة أعلاه المؤسسات على تقييم المخاطر التي يشكلها تهديد هجمات برامج الفدية.

4.3.5 لماذا تعد هجمات برامج الفدية فعالة جداً؟

ساعدت عدة عوامل في نجاح وانتشار هجمات برامج الفدية، فالعامل المساعد الأول هو توفر "خدمة برامج الفدية" (RAAS) في الشبكة المُظلمة، مما يسمح للجهات الضارة باستئجار البرنامج وتنفيذ الهجمات بكل سهولة. أما العامل الثاني المُساهم في نجاح هذه الهجمات، فهو نمو العملة

المُشفرة (Cryptocurrency)، والتي تساعد المجرمين في استقبال الأموال دون الكشف عن هويتهم.

والغريب أيضاً أن شركات التأمين السيبراني ساهمت في زيادة هجمات برامج الفدية، وذلك بسبب سياسات شركات التأمين السيبراني التي تُحتم على الشركة القيام بدفع الفدية للمجرمين من أجل حماية المؤسسة.

4.3.6 تأثير برامج الفدية على المُتضررين

يعتمد تأثير برامج الفدية على نوع الهجوم، فيمكن أن يكون التأثير أحد الأمور التالية:

تعطيل الخدمات أو الأنظمة:

سيؤدي هجوم الفدية إلى جعل النظام غير قابلاً للاستخدام ما لم يتم تعطيل البرنامج الضار أو استعادة الأنظمة مما يسبب عُطلاً في الخدمات التي تقدمها أجهزة الكمبيوتر المتضررة. تخيل لو أن النظام المتضرر هو نظام البنية الوطنية التحتية فسوف يكون التأثير متعدد الجوانب وقد يمتد إلى ما وراء نطاق مؤسستك وقد يمتد أثره إلى المستوى الوطني.

فقدان البيانات:

في حال عدم قدرة المؤسسة على فتح النظام بعد التعرض لهجوم برنامج الفدية، فسوف تُفقد المؤسسة بعض البيانات حتى لو تم استرداد البيانات بنجاح من النسخة الاحتياطية، وذلك بسبب فترة (delta)، وهي الفترة الزمنية التي تقع بين النسخ الاحتياطي وبين الوقت الحالي.

اختراق البيانات (فقدان السرية):

لا يقوم بعض المهاجمين فقط بتشفير البيانات، بل بالتهديد بتسريبها على الانترنت إذا لم يقم الضحايا بدفع الفدية. لذلك، لا يكمن الخطر فقط في فقدان البيانات، بل أيضاً بتسريبها وبيعها عبر المنتديات السرية. بمجرد تسريب البيانات، فإن خطر استخدامها يرتفع إذ يمكن استخدام هذه البيانات من قبل الجهات الفاعلة الضارة الأخرى لشن هجمات جديدة، أو من قِبل المنافسين التجاريين للوصول إلى المعلومات السرية كالسجلات المالية أو معلومات العملاء أو معلومات تجارية سرية أخرى.

الخسارة المالية:

تتسبب حوادث برامج الفدية في بعض الخسائر المباشرة والغير مباشرة لأموال المؤسسة، إذ يمكن أن تشمل الخسائر المباشرة الفدية إذا تم دفعها، تكلفة استرداد الأنظمة، الغرامات المالية إن وجدت، زيادة أقساط التأمين وغيرها. أما الخسائر المالية الغير مباشرة فتشمل فقدان الإنتاجية وفقدان الإيرادات المحتملة وذلك بسبب عدم توافر النظام وفقدان الميزة التنافسية للمنافسين التجاريين وغيرها.

فقدان السمعة:

تؤثر الهجمات التي تكشف عن البيانات من قِبل المهاجم على سمعة المؤسسة، فقد يتسبب ذلك في فقد العملاء لثقتهم في المؤسسة.

الأثر القانوني:

قد تؤدي هجمات الكشف عن البيانات وخاصة البيانات الشخصية إلى تحقيقات وغرامات محتملة ويمكن أن يتسبب الهجوم في دعاوى قانونية من العملاء والشركات التي ربما تكون بياناتهم قد

انتُهكت من قِبل

التأثير الغير مباشر:

من المعروف أيضاً أن هجمات برامج الفدية لها تأثير نفسي وعاطفي على الأفراد (الموظفين داخل المؤسسات).

4.4 كيفية التخفيف من هجمات برامج الفدية

4.4.1 الضوابط العامة والاستعدادات اللازمة

يجب على المؤسسات التفكير المتعمق ووضع استراتيجية دفاع فعالة ضد هجمات برامج الفدية والتي تتضمن:

1. **التصميم**

أ. التأكد من أن النظام مصمم ليكون مرناً ضد الهجمات الالكترونية المحتملة.

ب. استخدم خاصية المصادقة الثنائية وتدوير كلمة المرور لضمان الحماية من اختراقها.

ت. تنفيذ نظام للتحكم في القدرة على الوصول يعتمد على (الحاجة إلى المعرفة) والامتيازات.

ث. تقسيم الشبكة بناءاً على احتياجات المؤسسة أو الأعمال التجارية، تجنب استخدام تصميم الشبكة المسطحة، استخدم جدار حماية أو جدار حماية لتطبيقات الويب (WAF)، أنظمة منع التسلل / كشف التسلل (PS/IDS) وغيرها من الضوابط الأخرى لمنع برامج الفدية من التواصل مع مراكز القيادة والتحكم.

ج. تثبيت عناصر تحكم ومراقبة إضافية في نقاط بوابة الشبكة مثل بوابات البريد وبوابات الإنترنت وذلك للبحث عن حركة المرور الضارة وحظر رسائل البريد الإلكتروني المشبوهة تلقائياً وحظر الروابط الضارة.

2. **التوثيق:**

أ. التأكد من أن المؤسسة لديها مجموعة موثقة من السياسات والإجراءات المعمول بها لإدارة مراقبة النظام، إدارة الحوادث، استمرارية الأعمال، إدارة الأزمات وأمن سلسلة التوريد وما إلى ذلك.

ب. يجب تخزين نسخ من الوثائق الهامة بما في ذلك استمرارية الأعمال وخطط التعافي من الكوارث في وضع عدم الاتصال، بحيث لا يمكن الوصول إليها في حالة حدوث هجوم برامج الفدية.

3. **التقنيات** :

أ. القيام بتقوية البنية التحتية الخاصة (الشبكات، المنصات، التطبيقات، أنظمة التشغيل، أجهزة الحوسبة وما إلى ذلك) باتباع ما يلي:

أ. تحديد عدد التطبيقات المثبتة على الجهاز. وإذا أمكن الامر القيام بتنفيذ

القائمة البيضاء للتطبيقات المثبتة على آلة حوسبة الخاصة بالشركات.

ii. القيام بإعدادات أمان المتصفح.

iii. تعطيلAdobe Flash والثغرات الأخرى في المتصفح.

iv. تعطيل وحدات الماكرو لمعالجة النصوص والتطبيقات الضعيفة الأخرى.

v. تقييد أذونات المستخدم لتثبيت تطبيقات البرامج وتنفيذها.

vi. تعطيل بروتوكول التحكم عن بُعد في سطح المكتب.

vii. التأكد من تصحيح الأنظمة وتحديثها.

viii. التأكد من تطبيق أمن الأجهزة للكشف عن الهجمات الخبيثة وإدارتها.

ب. التأكد من أن المؤسسة لديها استراتيجية نسخ احتياطية فعالة مع تحديد تواتر النسخ الاحتياطية المطلوبة ونُسخ التناوب التي يتعين الاحتفاظ بها، نوع التكنولوجيا المطلوبة لتلبية احتياجات المؤسسة من خلال دليل الأعمال (playbook) واختبار النسخ الاحتياطية عن طريق استعادتها على أنظمة الاختبار الخاصة بالمؤسسة.

ت. التأكد من أن خطط المرونة الخاصة بالمؤسسة بما في ذلك خطط استمرارية الأعمال، خطط التعافي من الكوارث، وخطط إدارة الأزمات يتم اختبارها بانتظام لضمان توافر النظم واستمراريتها.

ث. التأكد من أن أدوات الكشف الخاصة بالمؤسسة جاهزة للاستخدام ولديها القدرة على اكتشاف هجمات برامج الفدية.

ج. القيام بمسح ومراقبة أنشطة الملفات المشبوهة.

4. **الوعي السيبراني**

أ. تنفيذ برامج التوعية السيبرانية لتوعية أفراد المؤسسة بصورة مستمرة بالتهديدات السيبرانية السائدة وأحدث الاتجاهات في التصيد الاحتيالي، الهندسة الاجتماعية والحيل الإلكترونية و التي يجب اختبار فعاليتها من وقت لآخر.

5. **المراقبة**

أ. التأكد من تفعيل السجلات وجمعها وتحليلها.

ب. التأكد من إعداد نظام إدارة السجلات للتعامل مع الهجمات المعروفة وسرعة الكشف عن أي هجوم ضار محتمل.

ت. التأكد من أن المؤسسة مشتركة في برامج إرشادات التهديد الموثوقة والتي تمكن المؤسسة من الاطلاع على أحدث التهديدات وأحدث مؤشرات الاختراقات والأدوات والتكتيكات والإجراءات للجهات الفاعلة في مجال التهديد.

ث. القيام بإعداد البنية التحتية الأمنية الخاصة (كأجهزة مثل الجدران النارية وIDS/IPS

وغيرها) وذلك لحجب عناوين ونطاقات بروتوكولات الانترنت الضارة المعروفة.

ج. القيام بتحديد أداء البنية التحتية وذلك لاكتشاف الحالات المشبوهة بسرعة.

6. **جهات اتصال الطوارئ:**

أ. إنشاء قائمة جهات اتصال طوارئ للموظفين حتى يتمكنوا من الوصول إلى الفرق الداخلية وشركات الدعم أثناء وقوع الحوادث. يرجى مراجعة القسم 4-8 من إدارة الحوادث في المعيار الوطني لتأمين المعلومات.

ب. إنشاء قنوات تواصل مع الوكالة الوطنية للأمن السيبراني والمؤسسات القانونية ومزودي خدمة الإنترنت الخاصة بالمؤسسة.

7. **تقييم عروض الطرف الثالث:**

أ. يجب تحديد اتفاقيات خاصة عند طلب الجهات المتخصصة في التعامل مع حوادث برامج الفدية وخدمات استعادة البيانات.

ب. الاشتراك في المنتديات/الخدمات التي توفر معلومات استخباراتية عن التهديدات السيبرانية لهجمات برامج الفدية.

8. **أمن سلسلة التوريد**

أ. التأكد من أن الشركات تفهم معنى الأمن السيبراني وتقوم بتقييم المخاطر وإدارتها من خلال الضوابط المناسبة. أما بالنسبة للوظائف الحيوية، ينبغي فرض تقييم النظم داخل المؤسسة وتقييم مخاطر الأطراف الثالثة.

ب. يجب إطلاع الشركات على السياسات والإجراءات الأمنية التابعة للمؤسسة.

ت. يجب أن تشتمل عقود الشركات على التالي:

i. دمج متطلبات الأمن السيبراني في عقود واتفاقيات الشركات.

ii. إلزام الشركات بالإبلاغ عن أي خرق للبيانات أو للنُظم إلى المؤسسة في غضون اثنتي عشرة ساعة من الاكتشاف. كما وينبغي أن تكون الشركة مسؤولة عن أي تأثير يطرأ على المؤسسة وإعداد التقرير النهائي عند إغلاق الحادث.

4.4.2 مرحلة أثناء الهجوم

1. بمجرد اكتشاف الهجوم، يجب أن يكون التركيز الفوري على احتواء الحادث وتقييد انتشاره في الشبكة لتقليل الضرر.

2. يجب الإبلاغ عن الحادث إلى الوكالة الوطنية للأمن السيبراني. قم بمراجعة القسم 6.4 للحصول على بيانات الاتصال. إذا كنت ترغب في الإبلاغ عن جريمة إلكترونية، فقد تحتاج إلى تقديم تقرير إلى الجهات القانونية في وزارة الداخلية فيفي قسم التحقيق في الجرائم الالكترونية.

3. تحديد الأنظمة التي تأثرت بالهجوم وعزلها عن طريق فصلها عن الشبكة، فبرامج الفدية

تنتشر بسرعة في الشبكة.

4. تحديد نوع برنامج الفدية التي أصابت الأنظمة الخاصة بك والتحقق مما إذا كان هناك فك للتشفير متاحاً عبر الإنترنت. ففي السنوات الأخيرة، اجتمعت بعض الحكومات والمنظمات لمساعدة المؤسسات على محاربة خطر برامج الفدية من خلال توفير الموارد وحتى مفاتيح فك التشفير عبر الإنترنت.

5. من منظور إدارة الحوادث والجرائم الرقمية، فمن المهم جمع كافة المعلومات ذات الصلة التي تساعدك على تحليل الهجوم والتحقيق فيه والنظر في سلسلة الوصاية المناسبة للأدلة الرقمية التي يتم جمعها لتكون مقبولة في المحاكم القانونية في حال أنك قد قررت متابعة القضية في القانون والقضاء.

6. يجب أن تتضمن الأدلة الرقمية والسجلات التي سيتم جمعها وتأمينها على التالي:

أ. أجزاء من البيانات التي تمت مهاجمتها والتي لازالت موجودة.

ب. جميع معلومات السجلات المتاحة.

ت. اسم برنامج الفدية.

ث. الأنظمة المتأثرة.

ج. رسائل البريد الإلكتروني الأصلية بعناوينها الكاملة وأي مرفقات بداخلها وذلك إذا تم تنفيذ الهجوم عن طريق ايميل تصيد احتيالي.

ح. نُسخ من الملفات القابلة للتنفيذ أو الملفات الأخرى التي تم تنزيلها على النظام بعد الوصول إلى المرفقات الضارة، بما في ذلك صفحة البداية.

خ. أي نطاقات أو عناوين بروتوكولات انترنت تم تواصلها مع الأنظمة قبل أو أثناء الإصابة مباشرة.

د. العناوين التي تطلب دفع عملات افتراضية مع تحديد المبلغ المطلوب.

ذ. أي تقارير خاصة بالتحليل الجنائي أو الاستجابة للحوادث.

ر. لقطات للذاكرة أثناء الهجوم من قِبل البرامج الضارة.

ز. حالة الضرر.

س. توفير طوبولوجيا الشبكة (network topology)

7. إعطاء الأولوية لاستعادة الأنظمة بناءً على أهميتها. يجب التأكد من أن النسخة الاحتياطية المستخدمة نظيفة ولا تحتوي على ملفات ضارة.

8. التأكد من تنظيف الشبكة من البرمجيات الضارة مع القيام بمسح جميع الأنظمة والشبكات والسجلات باستخدام مؤشرات التسوية المحددة والأدوات والتكتيكات والإجراءات مع القيام تحليل السبب الجذري لتحديد نقاط الضعف التي استغلها المهاجم والقيام بإصلاحها.

9. إصلاح أي نقاط ضعف محتملة أخرى يمكن اكتشافها واستغلالها لاختراق الأنظمة في المستقبل إذ لوحظ في الماضي وجود حالات تم فيها استهداف ضحايا برامج الفدية مرة أخرى في تتابع سريع وذلك لأن الثغرات الكامنة لم تتم معالجتها.

10. إذا كانت مؤسستك ضحية لهجوم برامج الفدية، فلا تدفع الفدية. قد يبدو دفع الفدية حلاً سريعاً ولكن لا يضمن ذلك بأن المهاجم سيقوم بفك التشفير بعد دفع الفدية. ففي بعض الحالات، يقوم فيها المهاجم بطلب الفدية من الضحية مرة أخرى، حتى بعد دفع الفدية الأولى وذلك لأن الثغرات الأساسية لم يتم إصلاحها.

11. ينُص تعميم مصرف قطر المركزي رقم 6 لعام 2018 والتعميم رقم 46 لعام 2019 على أن التداول في العملة الافتراضية "البيتكوين" غير قانوني. علاوة على ذلك لا ينبغي لأي مؤسسة مالية أن تُسهل بأي شكل من الأشكال شراء أو بيع أو التعامل في أي أصول افتراضية. وعلى هذا النحو، يمكن اعتبار دفع الفدية جريمة مالية، وسيتخذ مصرف قطر المركزي إجراء قانونياً ضد ذلك.

12. في أكتوبر من ال عام2020، أصدر مكتب مراقبة الأصول الأجنبية (OFAC) التابع لمكتب الخزينة في الولايات المتحدة بنداً يحظر فيه دفع الفدية، كما حذر مستشار مكتب مراقبة الأصول الأجنبية من أن كل من يقوم بتيسير هذه المدفوعات نيابة عن الضحايا كالمؤسسات المالية وشركات التأمين الإلكتروني وغيرها من الشركات المشاركة في الاستجابة للحوادث والجرائم الجنائية الرقمية إذ يعد ذلك انتهاكاً لأنظمة مكتب مراقبة الأصول الأجنبية. ولذلك، فقد توقف عدد من مقدمي التأمين الإلكتروني في جميع أنحاء العالم عن القيام بدفع الفدية كجزء من إجراءاتهم التأمينية.

4.4.3 مرحلة ما بعد الهجوم

1. بعد انتهاء الحادث واستعادة الأنظمة، يجب القيام بتوثيق ما حدث وتحليل السبب الجذري للحادث لتحديد الخطأ الذي حدث وتحديد نقاط الضعف (مثل البرامج القديمة أو الأنظمة غير المُصححة أو ضعف ضوابط الوصول وغيرها)، والثغرات في العمليات (على سبيل المثال، عدم كفاية أو عدم وجود إجراءات أو اتفاقيات مستوى الخدمة واتفاقية مستوى العمليات التشغيلية وغيرها)، وأوجه القصور في سلوك الناس (مثل ثقافة العمل ونقص التدريب وغيرها)، التي ربما ساهمت في تعريض النظام للخطر.

2. وضع خطة لمعالجة الثغرات التكنولوجية وثغرات العمليات وأوجه القصور في سلوك الناس وذلك لمنع تكرار الهجمات في المستقبل.

3. تحديد مجالات التحسين التي ستساعد المؤسسة على تجنب أي حوادث من هذا القبيل في المستقبل بالإضافة إلى تحسين قدرات الاستجابة والتعافي خلال مثل هذه الهجمات.

5. الامتثال والتنفيذ

5.1 الامتثال والتنفيذ

تهدف هذه المبادئ التوجيهية لمساعدة المؤسسات على فهم خطر هجمات برامج الفدية بشكل أفضل وكيفية التخفيف من حدة هذه التهديدات.

تعتبر هذه المبادئ التوجيهية مكملاً معيار تأمين المعلومات الوطنية.

6. الملحقات

6.1 الاختصارات

NCSA	الوكالة الوطنية للأمن السيبراني
OLA	اتفاقية المستوى التشغيلي
RAAS	خدمة تقديم برامج الفدية
SLA	اتفاقية مستوى الخدمة
TTP's	الأدوات، التكتيكات، الإجراءات

6.2 المراجع

معيار تأمين المعلومات الوطنية النسخة 2.1

6.3 الموارد عبر الانترنت

مفاتيح فك التشفير:
https://www.nomoreransom.org/en/index.html
https://noransom.kaspersky.com/
https://www.avast.com/en-au/ransomware-decryption-tools#pc
https://www.emsisoft.com/en/ransomware-decryption/
https://www.trellix.com/en-au/downloads/free-tools/ransomware-decryption.html
https://www.cisa.gov/stopransomware
تحديد نوع برنامج الفدية:
https://id-ransomware.malwarehunterteam.com/index.php
https://www.nomorweransom.org/crypto-sheriff.php?lang=en

6.4 الإبلاغ عن الحوادث للوكالة الوطنية للأمن السيبراني

يمكن للمؤسسات التي تتعرض لهجوم سيبراني أو تلاحظ وجود أية أنشطة مشبوهة أن تقوم بتبليغ الوكالة الوطنية للأمن السيبراني بذلك عن طريق أحد الطُرق التالية:

الاتصال بالخط الساخن التابع للوكالة الوطنية للأمن السيبراني: 16555 (الذي يعمل على مدار الساعة)

إرسال بريد الكتروني للعنوان التالي: ncsoc@ncsa.gov.qa

كما ويمكن للمؤسسات أيضاً التواصل مع الوكالة الوطنية للأمن السيبراني من أجل التحقيق أو المساعدة في البحث عن أي تسريب للبيانات التي تتعلق بها أو بالشركات التي تعمل معها. كما ويمكن أيضاً الاطلاع على المبادئ التوجيهية التالية لمواجهة الهجمات / الحوادث السيبرانية:
Guidelines for Incident Management - Pre-requisite Measures