المركز الوطني
للأمن السيبراني
National Cyber
Security Center

الاستجابة للحوادث الإلكترونية

المحـــاور

- المقدمة
- ما هي خطة الاستجابة للحوادث السيبرانية؟
- طرق الاستجابة للحوادث السيبرانية
- مفهوم الإبلاغ عن الحوادث السيبرانية
- أهمية الإبلاغ عن الحوادث السيبرانية
- خطوات الإبلاغ عن الحوادث السيبرانية
- ما الذي يجب تضمينه في تقرير الحوادث السيبرانية؟
- ما نوع النشاط المشبوه الذي يجب عليك الإبلاغ عنه؟
- عواقب عدم الإبلاغ عن الحوادث السيبرانية

المقدمة

هناك حقيقة مطلقة لا يُمكن التغافل عنها وهي أن الحوادث السيبرانية سوف تحدث دائماً، بغض النظر عن التدابير والممارسات المتبعة...

- وذلك لسبب بسيط وهو التطور المستمر والسريع لأساليب وتقنيات الهجوم من جانب المهاجم من جهة، والأخطاء البشرية المستمرة من جانب المستخدمين - الموظفين - من جهة أخرى.

- لذلك مع تزايد وتيرة التهديدات السيبرانية وتأثيرها سلباً على الأصول المعلوماتية والتقنية بالجهة، يعّد وجود خطة استجابة محكمة من الجهة للتعامل مع الحوادث السيبرانية، بجانب الإبلاغ المبكر عن تلك الحوادث من جانب الموظفين درع وقاية وحماية من تأثيرها المُتصَاعد الذي يهدد سرية وسلامة وتوافر أصول المعلومات والأنظمة.

ما هي خطة الاستجابة للحوادث السيبرانية؟

تحدد تلك الخطة الممارسات والخطوات الواضحة التي يجب على الجهة اتباعها للتصدي والاستجابة للعديد من السيناريوهات المحتملة للحوادث السيبرانية، بما في ذلك تسريب وفقدان البيانات، البرامج الضارة، التهديدات الداخلية وغيرها...

أهميتها:

- اكتشاف الحوادث السيبرانية في مهدها المبكر.
- تقليل مقدار الضرر الذي يمكن أن يسببه حادث معين والتعافي منه.
- بالإضافة إلى منع وقوع حوادث مماثلة في المستقبل.

طرق الاستجابة للحوادث السيبرانية

تعتمد الكثير من الجهات على منهجية (OODA) وهي استراتيجية طورها الخبير العسكري جون بويد للاستجابة للحوادث، تتضمن 4 خطوات أساسية عند مواجهة أي تهديد:

- الملاحظة (Observe):

متابعة الأنظمة والشبكات لتوفير معلومات فورية عن أي أنشطة مشبوهة.

- التوجيه (Orient):

التفكير مثل المهاجم للتمكن من فهم دوافعه والاستراتيجيات المتبعة من قبله، مثلًا إذا كانت الجهة في صَدَدِ إنهاء عقد عدد من الموظفين وكانت هناك عِدة هجمات متتالية من IP محدد ومألوف، فمن المحتمل أن يكون التهديد داخليًا.

- اتخاذ القرار (Decide):

بمجرد تجميع المعلومات، يجب النقاش حول كيفية اتخاذ قرارات مستنيرة بشأن الاستجابة لتلك الحوادث السيبرانية.

- العمل (Act):

التطبيق الفعلي للقرارات بهدف التصدي للتهديدات وتقليل مخاطرها ومعالجة الأنظمة المتأثرة سريعًا وإعادتها لطبيعتها، بجانب منع تكرار الحوادث المماثلة المستقبلية.

مفهوم الإبلاغ عن الحوادث السيبرانية

توثيق أو تسجيل أي حادث سيبراني متوقع، أو حدث بالفعل، مثل اختراق الأجهزة والأنظمة، أو تسريب البيانات، أو أي تهديد يمكن أن ينتج عنه الكشف عن المعلومات الحساسة أو تهديد سلامة أو موثوقية أو سرية الأصول أو الأنظمة أو كلاهما وإعلام قسم الأمن السيبراني بالجهة على نحو سريع لاتخاذ الإجراءات اللازمة.

الهدف: المساعدة على فهم المشهد السيبراني على نحو أفضل وتجنب الأخطاء السابقة في التعامل مع الحوادث السيبرانية.

أهمية الإبلاغ عن الحوادث السيبرانية

يلعب الإبلاغ المبكر عن الحوادث السيبرانية دورًا لا يُمكن إغفاله في التصدي والوقاية من التهديدات السيبرانية، من حيث:

- يساعد الإبلاغ المبكر عن الحوادث السيبرانية على الاستجابة السريعة لها، ومن ثمَّ منع المزيد من الضرر.
- تحديد أنماط الهجمات الموجهة للجهة، ثم تنفيذ تدابير وقائية لإحباط الهجمات المستقبلية.
- الحفاظ على الأدلة المهمة فيما يتعلق بالحادث واستغلالها في تحديد مصدر الهجوم، وفهم أسلوبه ونطاقه، واتخاذ الإجراءات القانونية المناسبة إذا لزم الأمر.
- توفير معلومات قيمة لفريق الأمن السيبراني، وتحسين الممارسات السيبرانية لتظل الجهة متقدمة بخطوة على التهديدات المحتملة.

خطوات الإبلاغ عن الحوادث السيبرانية

- اكتشاف أو الاشتباه في حدوث تهديد سيبراني على سبيل المثال (وجود رسالة: تم تشفير ملفاتك) على شاشة جهاز العمل؛ مما يعني أن الجهاز قد تعرض لهجوم فيروس الفدية.
- جمع ملابسات الحادث من وقت وتفاصيل حدوثه وتأثيره، بجانب إدراج صور مرئية فعّلية من الحادث مثل (لقطة شاشة لرسالة الفدية وصور الملفات المغلقة).
- تضمين كامل البيانات في تقرير الحوادث السيبرانية بشكل مُفصل وواضح حتى لغير التقنيين.
- إرسال تقرير الحوادث السيبرانية لقسم الأمن السيبراني بالجهة خلال 72 ساعة من توقيت وقوع الحادث.
- إبلاغ زملاء العمل بشأن الحادث لاتخاذ الاحتياطات اللازمة وتجنب التعرض للحادث نفسه.
- في حالة استخدام أجهزة أخرى في العمل يجب فحصها في البداية ثم تأمينها جيدًا من خلال برنامج مكافحة الفيروسات وجدران الحماية وما إلى ذلك لمنع إصابتها.

ما الذي يجب تضمينه في تقرير الحوادث السيبرانية؟

ما هو تقرير الحوادث السيبرانية؟

مستند يعرض تفاصيل الهجوم السيبراني بشكل مُفصل، مما يمنح فريق الأمن السيبراني صورة فعّلية عن الحادث من كامل جوانبه، ويمكنهم من اتخاذ إجراءات التصدي والاستجابة لهذا الحادث في أسرع وقت ممكن.

ما الذي يجب تضمينه في تقرير الحوادث السيبرانية؟

الخطوة 1: توثيق التفاصيل

- تأكد من تجميع كامل التفاصيل ذات الصلة بالحادث، على سبيل المثال وليس الحصر، تاريخ ووقت الحادث، الأنظمة والشبكات المتضررة، الأفراد المعنيين، وأي ملاحظات أخرى.
- تذكر: كُن مفصلًا قدر الإمكان وتجنب كتابة أي تفاصيل عامة، تذكر أن أي معلومة بسيطة كانت أو معقدة قد تكون مفيدة...

ما الذي يجب تضمينه في تقرير الحوادث السيبرانية؟

الخطوة 2: وصف الحادث

- بعد خطوة تجميع التفاصيل، قم بكتابة تقرير مُفصل عن الحادث، يتضمن:

1. ملخص موجز يصف نوع الحادث وتأثيره.
2. وصف تفصيلي للحادث، بما في ذلك: نوع التهديد، توقيت ومكان وقوع الحادث. الأضرار الناجمة عن الحادث، الأنشطة المشبوهة أو الحالات الشاذة، أي تفاصيل أخرى متاحة، بجانب إرفاق أي أدلة تم جمعها، مثل سجلات النظام أو لقطات الشاشة.

- تذكر: تجنب استخدام المصطلحات التقنية المعقدة التي لن يفهمها سوى الأشخاص التقنيين، كُن بسيطًا بقدر الإمكان.

ما الذي يجب تضمينه في تقرير الحوادث السيبرانية؟

الخطوة 3: تحليل الحادث

- بعد وصف الحادث، من المهم تحليله. من خلال فهم السبب الجذري لحدوثه وأي نقاط ضعف أو ثغرات أمنية تم استغلالها، بجانب أي توصيات أو استراتيجيات علاجية يُمكن أن تساعد على التخفيف من شدة الحادث ومنع تكراره مثل تنفيذ ضوابط أمنية إضافية أو إجراء تدريب للموظفين على أفضل ممارسات الأمن السيبراني.

- تذكر أن الهدف ليس فقط الوقاية من الحادث الحالي، ولكن أيضًا تجنب وقوع حوادث مماثلة في المستقبل..

ما الذي يجب تضمينه في تقرير الحوادث السيبرانية؟

شكل تقرير الحوادث السيبرانية

الملخص التنفيذي:
ملخص سريع عن الحادث دون الخوض في التفاصيل الفنية.

التحليل:
تحليل الحادث لتحديد السبب الجذري له ونقاط الضعف التي تم استغلالها.

تفاصيل الحادث:
تضمين المعلومات الأساسية حول الحادث، مثل تاريخ الحادث ووقته ومكان حدوثه، بجانب الأنظمة المتضررة والأفراد المعنيين وأي ملاحظات أولية.

التوصيات:
كتابة توصيات قابلة للتنفيذ لمنع وقوع حوادث مماثلة في المستقبل مثل تعزيز إجراءات الأمان، أو تطوير السياسات، أو مبادرات تدريب الموظفين.

وصف الحادث:
كتابة وصف تفصيلي عن الحادث، بما في ذلك الجدول الزمني للأحداث وأي أدلة جُمِعَت أو تفاصيل مهمة.

الاستنتاج:
كتابة ملخص لتقرير الحادث، مع التأكيد على أهميته وضرورة اتخاذ إجراءات سريعة للتعامل معه.

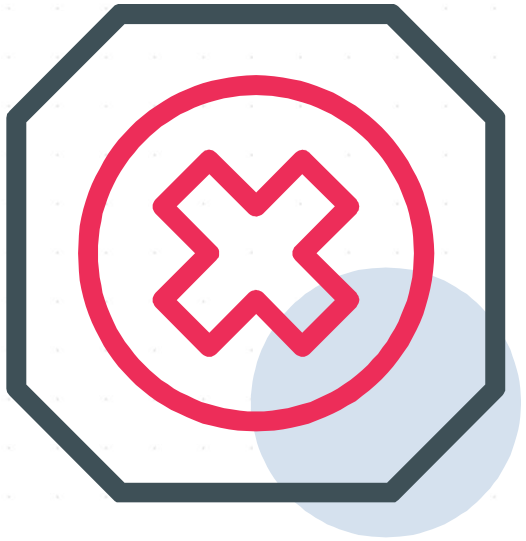
ما نوع النشاط المشبوه الذي يجب عليك الإبلاغ عنه؟

احرص على الإبلاغ السريع في حالة الاشتباه في حدوث التهديدات السيبرانية التالية:

- الوصول غير المُصرح به إلى أنظمة تكنولوجيا المعلومات الهامة
- فقدان وتسريب البيانات الحساسة
- الرسائل الاحتيالية المشبوهة
- اكتشاف البرامج الضارة على الأنظمة والأجهزة
- الوصول غير المُصرح به إلى المناطق السرية بالجهة
- الكشف غير المُصرح به عن المعلومات الحساسة
- أي حوادث أخرى من شأنها تعطيل خدمات الطيران والإضرار بالعملاء
- التهديدات الداخلية من الموظفين والأشخاص المألوفين بالجهة

عواقب عدم الإبلاغ عن الحوادث السيبرانية

عدم الإبلاغ عن الحوادث السيبرانية على نحو سريع يمكن أن يسبب عواقب وخيمة للموظفين والجهة بأكملها، من ناحية:



- عدم الإبلاغ عن الحوادث السيبرانية من المحتمل أن يتسبب في تفاقمها وزيادة الضرر الناتج عنها من اختراق الأنظمة وتسريب البيانات وما إلى ذلك.

- نقص المعلومات حول طبيعة الحوادث الموجهة للجهة، وبالتالي صعوبة تطوير التدابير الوقائية، أو طرق التعامل الاستباقي مع الهجمات المستقبلية الأخرى، لتظل الجهة عرضة للتهديدات المتكررة.

عواقب عدم الإبلاغ عن الحوادث السيبرانية

- تكبُّد الجهة الغرامات والعقوبات القانونية؛ بسبب عدم الامتثال للقوانين واللوائح التنظيمية.
- فقدان ثقة العملاء، بسبب عدم التزام الجهة بحماية بياناتهم الحساسة، خاصةً في حالة حدوث تسريب أو ضرر لتلك البيانات، يُمكن أن يسبب فقدان الثقة آثار طويلة الأمد على سمعة الجهة، ويُمكن أن يؤدي إلى خسائر مالية وتنظيمية.
- عدم الإبلاغ عن الحوادث يعرض الموظف إلى العقوبات المالية والتنظيمية من قِبل الجهة وفقاً للوائح والقوانين.

الخاتمة

تذكر في حالة الاشتباه أو التعرض لتهديد سيبراني، يُرجى التواصل مع قسم الأمن السيبراني بالجهة خلال 72 ساعة من وقت وقوع الحادث للتحقيق واتخاذ الإجراءات اللازمة على البريد التالي/.....

نتمنى لكم السلامة في

العالم الرقمي.