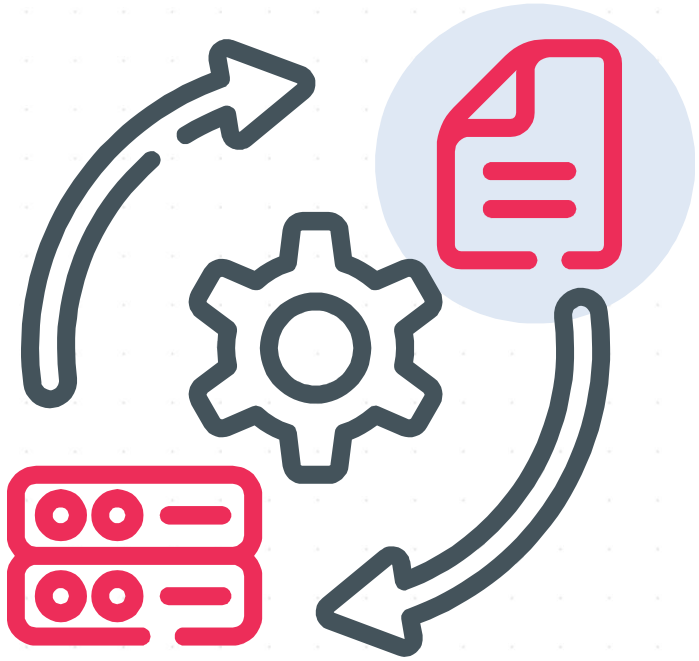
المركز الوطني
للأمن السيبراني
National Cyber
Security Center

حوادث وتهديدات الأمن السيبراني

المحـــــاور

- مقدمة في الحوادث والتهديدات السيبرانية
- الفرق بين الحوادث والتهديدات في مجال الأمن السيبراني
  - الحوادث في الأمن السيبراني
  - التهديدات في الأمن السيبراني
- التعامل مع الحوادث والتهديدات في الأمن السيبراني
- الخاتمة

مقدمة في الحوادث والتهديدات السيبرانية

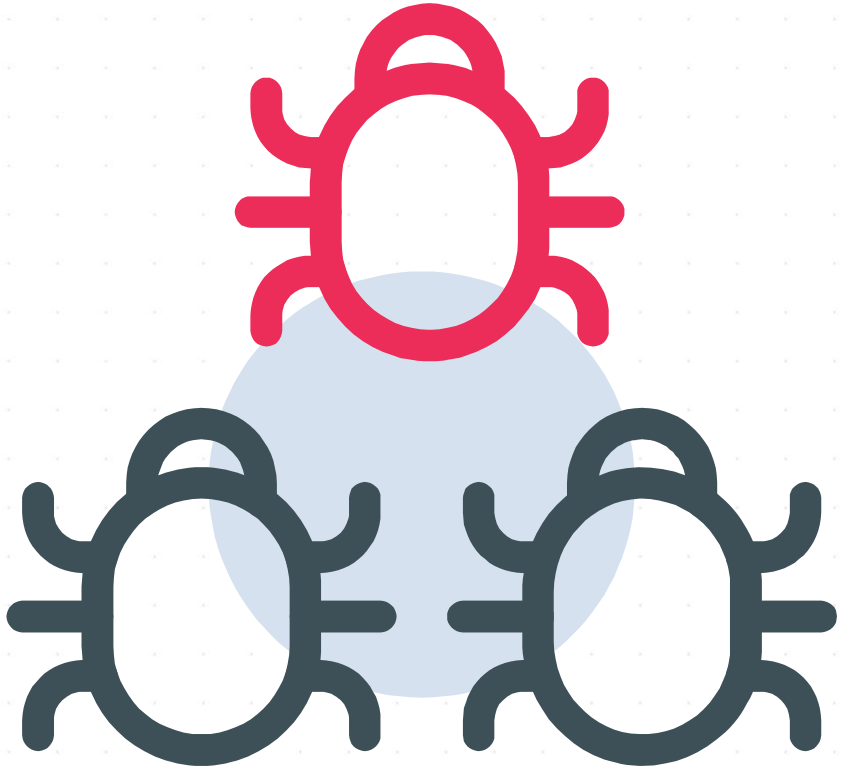


في ظل التحول الرقمي الكبير الذي تشهده جميع القطاعات وفي ظل التوجه المتزايد إلى استخدام التكنولوجيا في شتى المجالات فإن هناك علاقة طردية نشأت بين هذا التحول الرقمي وبين حجم ومقدار الخطر الناشئ عنه؛ فكلما ازداد الاعتماد على التكنولوجيا كلما زادت الفرصة للتعرض للهجمات والحوادث السيبرانية المختلفة.

الفـرق بـين الحـوادث والتهديـدات في مجال الأمن السيبراني

في حين يرتبط كل من مفهومي الحوادث والتهديدات في مجال الأمن السيبراني ارتباطاً وثيقاً ببعضهما البعض إلا أن لكل منهما تعريف تقني مختلف عن الآخر،كـالآتـــي:

الحوادث في الأمن السيبراني



يُشير مفهوم الحوادث في الأمن السيبراني إلى حدوث أحداث غير مرغوب بها وبشكل مفاجئ بحيث تتسبب تلك الأحداث بأثر ضار على سلامة الأنظمة أو المعلومات أو الأجهزة أو الشبكات أو غيرها من مكونات أنظمة تكنولوجيا المعلومات، ومن الأمثلة على الحوادث في الأمن السيبراني تسريب البيانات والمعلومات و انتشار البرمجيات الضارة وغيرها.

التهديدات في الأمن السيبراني

يُقصد بالتهديدات في الأمن السيبراني المُسببات أو الجهات التي عادة ما تُشكل خطراً على سلامة وأمان نظام المعلومات أو الشبكات أو غيرها مما قد يؤثر على السلامة الرقمية والأمن السيبراني للأفراد أو المؤسسات أو كليهما، ويُمكن أن تكون هذه التهديدات ناجمة عن أفراد أو جماعات أو حتى حكومات ودول، وقد تكون التهديدات هي أخطاء غير مقصودة من المُستخدِم نفسه ولكنها تؤدي إلى الإضرار بالأنظمة والمعلومات بأي شكل من الأشكال.

التعامل مع الحوادث والتهديدات في الأمن السيبراني

بصرف النظر عن طبيعة ما قد تواجهه المؤسسة من مشاكل متعلقة بالأمن السيبراني وسواء كانت حوادث أو تهديدات سيبرانية إلا أنها جميعا تُشكل تحدياً للمؤسسات والأفراد، ويُمكن الحد منها جميعاً من خلال مجموعة من السياسات والإجراءات التي يُمكن تنفيذها، ومنها:

التعامل مع الحوادث والتهديدات في الأمن السيبراني

تعزيز الوعي الأمني:

يُعتبر المُستخدِم خط الدفاع الأول في سبيل مواجهة التهديدات والحد من التعرض للحوادث السيبرانية لذا فإنه يتوجب توعية الموظفين بأبرز التهديدات السيبرانية كهجمات التصيد الاحتيالي والهندسة الاجتماعية وغيرها مما قد يعرضه للخداع والاستغلال عبر الإنترنت.

التعامل مع الحوادث والتهديدات في الأمن السيبراني

إعداد سياسات الأمان:

وذلك من خلال وضع مجموعة من القواعد وسلوكيات الأمان الرقمي التي يتوجب على المُستخدمين اتباعها بحيث يضمن تطبيقها وقاية كبيرة من التهديدات السيبرانية.

التعامل مع الحوادث والتهديدات في الأمن السيبراني

فحص الاختراقات:

من الأمور التي يتوجب الاهتمام بها لمواجهة تحديات الحوادث والتهديدات السيبرانية هو تنفيذ العديد من اختبارات اختراق الأنظمة والشبكات الخاصة بالمؤسسة وتحديد نقاط الضعف التي يُمكن أن تُشكل تهديدات، حيث يُساعد إجراء هذا الأمر وبشكل دوري على تقييم استراتيجية الأمن السيبراني المُتبعة في المؤسسة وتحسينها بشكل مُستمر.

التعامل مع الحوادث والتهديدات في الأمن السيبراني

استخدام أدوات الحماية:

يتوجب إتباع الإجراءات الفنية الصحيحة التي من شأنها تعزيز الأمن السيبراني سواء بالنسبة للأفراد أو المؤسسات كاستخدام برامج جدران الحماية وبرامج مكافحة الفيروسات وغيرها من تقنيات الحماية المختلفة.

التعامل مع الحوادث والتهديدات في الأمن السيبراني

تحديث البرامج والأنظمة:

يُعتبر مواكبة التحديثات التي تصدر من مُطوري البرامج والأنظمة المختلفة كأنظمة التشغيل من أهم المصادر الدفاعية لمقاومة التهديدات المختلفة وتجنُب وقوع الحوادث السيبرانية، وذلك أن هذه التحديثات تتضمن دوماً تحسينات أمنية يتم فيها معالجة أي نقاط ضعف أو ثغرات تم اكتشافها في إصدارات سابقة من تلك البرمجيات والنظم.

التعامل مع الحوادث والتهديدات في الأمن السيبراني

خطط الطوارئ والاستجابة:

حيث يتوجب أن يكون هناك خطة مكتوبة وخطوات معروفة يتم اتباعها بشكل تام من قبل الموظفين في حالة حدوث حادث سيبراني مُعين كانقطاع الإنترنت عن المؤسسة ثم إبلاغ الجهات المختصة بذلك.

الـخـــاتمــة

إن الحـوادث السـيبرانية واردة الحـدوث حتـى بالنسـبة لتلـك المؤسسـات والشـركات التـي تتبـع أقصـى درجـات الأمـان وقـد حدثت بالفعل لكبرى شركات تكنولوجيا المعلومات في العالم، إلا أن اتبـاع سياسـات الأمـن السـيبراني الوقائيـة والتنفيذيـة تحـد مـن آثارها وتقلل من تبعات حدوثها، وكذلك الأمر بالنسبة للتهديدات السيبرانية التي تزداد باستمرار كلما زاد اعتمادنا على استخدام العالم الرقمي، والحماية الفعالة للمؤسسات تتطلب جهداً وتعاوناً مشتركاً بين الجميع للوصول إلى فضاء سيبراني آمن وموثوق.

نتمنى لكم السلامة في

العالم

الرقمي.