الامن السيبراني

أ.م. إيمان محمد جعفر

قسم الحاسوب-كلية التربية للبنات

ما هو الامن السيبراني

الأمن السيبراني (Cybersecurity): يُطلق عليه أيضاً "**أمن المعلومات**" و"**أمن الحاسوب**"، وهو فرع من فروع التكنولوجيا يُعنى بحماية الأنظمة والممتلكات والشبكات والبرامج من الهجمات الرقمية التي تهدف عادة للوصول إلى المعلومات الحساسة، أو تغييرها أو إتلافها، أو ابتزاز المستخدمين للحصول على الأموال، أو تعطيل العمليات التجارية.

كذلك يعرف الامن السيبراني بأنه مجموع الوسائل التي من شأنها الحد من خطر الهجوم على البرمجيات أو أجهزة الحاسوب أو الشبكات ، و تشمل تلك الوسائل الادوات المستخدمة في مواجهة القرصنة و كشف الفيروسات الرقمية و وقفها و توفير الاتصالات المشفرة (Amoroso Edward)

وفي التقرير الصادر عن الاتحاد الدولي للاتصالات حول اتجاهات الإصلاح في الاتصالات لعام 2010-2011 عُرّف الأمن السيبراني بأنه: "مجموعة من المهمات مثل تجميع وسائل وسياسات وإجراءات أمنية ومبادئ توجيهية ومقاربات لإدارة المخاطر، وتدريبات وممارسات فضلى وتقنيات يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين".

وقدمت وزارة الدفاع الأمريكية "البنتاغون" تعريفاً دقيقاً لمصطلح الأمن السيبراني، فاعتبرته: "جميع الإجراءات التنظيمية اللازمة لضمان حماية المعلومات بجميع أشكالها المادية والإلكترونية، من مختلف الجرائم: الهجمات، التخريب، التجسس والحوادث

في حين اعتبر الإعلانُ الأوروبي الأمنَ السيبراني أنه يعني: "قدرة النظام المعلوماتي على مقاومة محاولات الاختراق التي تستهدف البيانات".

المفاهيم المرتبطة بالأمن السيبراني، ومن أهمها ما يلي:

- الفضاء السيبراني: وعرفته الوكالة الفرنسية لأمن أنظمة الإعلام ANSSI، وهي وكالة حكومية مكلفة بالدفاع السيبراني الفرنسي، بأنه: "فضاء التواصل المشكّل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية". فهو بيئة تفاعلية حديثة، تشمل عناصر مادية وغير مادية، مكوّن من مجموعة من الأجهزة الرقمية، وأنظمة الشبكات والبرمجيات، والمستخدمين سواء مشغلين أو مستعملين. كما أن هناك مَن عرّف الفضاء السيبراني بوصفه الذراع الرابعة للجيوش الحديثة.

- الردع السيبراني: يُعرف الردع السيبراني بأنه "منع الأعمال الضارة ضد الأصول الوطنية في الفضاء والأصول التي تدعم العمليات الفضائية"، ويرتكز الردع السيبراني على ثلاث ركائز هي عماد استراتيجية الدفاع السيبراني، تتمثل في: مصداقية الدفاع Credible Defense، والقدرة على الانتقام An Ability to Retaliate، والرغبة في الانتقام A Will to Retaliate.

- الهجمات السيبرانية: يمكن تعريفها بكونها: "فعلاً يقوّض من قدرات ووظائف شبكة الكمبيوتر لغرض قومي أو سياسي، من خلال استغلال نقطة ضعف معينة تُمكّن المهاجم من التلاعب بالنظام".

- الجريمة السيبرانية: مجموعة الأفعال والأعمال غير القانونية التي تتم عبر معدات أو أجهزة إلكترونية أو شبكة الإنترنت أو تبث عبرها محتوياتها، وهي ذلك النوع من الجرائم التي تتطلب الإلمام الخاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها". فهي الجريمة المتصلة باستخدام الكمبيوتر، أي تصرف غير قانوني، يرتكب باستخدام تقنيات المعلومات والاتصالات.

- القوة السيبرانية: يعد جوزيف.س ناي Nye.S Josephمن أبرز المهتمين بالقوة السيبرانية، حيث يعرّفها بأنها "القدرة على الحصول على النتائج المرجوة من خلال استخدام مصادر المعلومات المرتبطة بالفضاء السيبراني، أي أنها القدرة على استخدام الفضاء السيبراني لإيجاد مزايا للدولة، والتأثير على الأحداث المتعلقة بالبيئات التشغيلية الأخرى وذلك عبر أدوات سيبرانية".

أنواع الأمن السيبراني

يدافع متخصصو الامن السيبراني بإستمرار عن أنظمة الكمبيوتر ضد أنواع مختلفة من التهديدات السيبرانية. تصيب الهجمات الالكترونية الشركات والانظمة الخاصة كل يوم.

وتزايد تنوع الهجمات بسرعة. وفقًا للرئيس التنفيذي السابق لشركة Cisco ، جون تشامبرز ، "هناك نوعان من الشركات: تلك التي تم اختراقها ، وتلك التي لا تعرف حتى الآن أنها تعرضت للاختراق"

دوافع الهجمات الإلكترونية كثيرة. واحد منها هو المال ، حيث يجعل المهاجمون عبر الإنترنت النظام في وضع عدم الاتصال ويطلبون الدفع لاستعادة وظائفه.
برنامج الفدية ، وهو هجوم يتطلب الدفع لاستعادة الخدمات ، أصبح الآن أكثر تعقيدًا من أي وقت مضى.
الشركات معرضة للهجمات الإلكترونية ، لكن الأفراد مستهدفون أيضًا ،غالبًا لأنهم يخزنون المعلومات الشخصية على هواتفهم المحمولة ويستخدمون شبكات عامة غير آمنة.
يعد تتبع الهجمات الإلكترونية المتطورة و المتزايدة أمرا أساسيا لتحسين الامن السيبراني.

تهديدات الامن السيبراني

يشير تهديد الأمن السيبراني إلى أي هجوم ضار محتمل يسعى إلى الوصول غير القانوني إلى البيانات تعطيل العمليات الرقمية أو إتلاف المعلومات.
يمكن أن تنشأ التهديدات السيبرانية من جهات فاعلة مختلفة ، بما في ذلك جواسيس الشركات ونشطاء القرصنة والجماعات الإرهابية والدول القومية المعادية والمنظمات الإجرامية والمتسللين المنفردين والموظفين الساخطي.

في السنوات الأخيرة ، أدت العديد من الهجمات السيبرانية البارزة إلى الكشف عن بيانات حساسة.
على سبيل المثال ، أدى خرق Equifax لعام 2017 إلى اختراق البيانات الشخصية لنحو 143 مليون مستهلك، بما في ذلك تواريخ الميلاد والعناوين وأرقام الضمان الاجتماعي.
في عام 2018 ، كشفت شركة ماريوت الدولية أن المتسللين وصلوا إلى خوادمها وسرقوا بيانات حوالي 500 مليون عميل. في كلتا الحالتين ، تم تمكين تهديد الأمن السيبراني من خلال فشل المؤسسة في تنفيذ واختبار وإعادة إختبار الضمانات التقنية ، مثل التشفير والمصادقة والجدران النارية.

أنواع تهديدات الامن السيبراني

1. البرامج الضارة (MaleWare)

هي برامج ضارة مثل برامج التجسس وبرامج الفدية والفيروسات والديدان. يتم تنشيط البرامج الضارة عندما ينقر المستخدم على ارتباط
أو مرفق ضار ، مما يؤدي إلى تثبيت برامج خطيرة. تشير تقارير Cisco إلى أن البرامج الضارة ، بمجرد تنشيطها ، يمكنها:

- حظر الوصول إلى مكونات الشبكة الرئيسية (برامج الفدية ransomware)
- تثبيت برامج ضارة إضافية.
- الحصول على المعلومات سرا عن طريق نقل البيانات من القرص الصلب (برامج التجسس)
- تعطيل اجزاء من النظام ، مما يجعله غير صالح للعمل.

أنواع تهديدات الامن السيبراني

2- Emotet

تصف وكالة الأمن السيبراني وأمن البنية التحتية (CISA) برنامج (Emotet) بأنه "حصان طروادة (Trojan) مصرفي متقدم معياري يعمل بشكل أساسي ك(loader) لأحصنة طروادة المصرفية الأخرى. لا يزال برنامج Emotet من بين أكثر البرامج الضارة تكلفة وتدميرًا ."

أنواع تهديدات الامن السيبراني

2- Emotet

تصف وكالة الأمن السيبراني وأمن البنية التحتية (CISA) برنامج (Emotet) بأنه "حصان طروادة (Trojan) مصرفي متقدم معياري يعمل بشكل أساسي ك(loader) لأحصنة طروادة المصرفية الأخرى. لا يزال برنامج Emotet من بين أكثر البرامج الضارة تكلفة وتدميرًا ."

أنواع تهديدات الامن السيبراني

3- رفض الخدمة (Denial of Service DoS)

هو نوع من الهجمات الاليكترونية التي تغمر جهاز الكمبيوتر أو الشبكة بحيث لا يمكنه الاستجابة للطلبات. يقوم DoSالموزع (DDoS) بنفس الشيء، لكن الهجوم ينشأ من شبكة الكمبيوتر. غالبا ما يستخدم المهاجمون عبر الانترنيت هجوما طوفانيا لتعطيل عملية (المصافحة) وتنفيذ DoS يمكن إستخدام العديد من الاساليب الاخرى، ويستخدم بعض المهاجمين عبر الانترنيت
الوقت الذي يتم فيه تعطيل الشبكة لشن هجمات أخرى. الروبوتات هي نوع من DDoS حيث يمكن إصابة ملايين الانظمة ببرامج ضارة و التحكم فيها من قبل المتسللين.

أنواع تهديدات الامن السيبراني

4- Man in the Middle

يحدث هجوم (MITM) عندما يدخل المتسللون أنفسهم في صفقة بين طرفين بعد مقاطعة حركة المرور، يمكنهم تصفية البيانات و سرقتها. وفقا لشركة (Cisco) تحدث هجمات MITM غالبا عندما يستخدم الزائر شبكة Wi-Fi عامة غير أمنة. يدخل المهاجمون بين الزائر و الشبكة ثم يستخدمون البرامج الضارة لتثبيت البرامج واستخدام البيانات بشكل ضار

أنواع تهديدات الامن السيبراني

5- التصيد (Phishing)

تستخدم هجمات التصيد الاحتيالي إتصالات وهمية مثل البريد الالكتروني لخداع المتلقي لفتحه وتنفيذ التعليمات الموجودة فيه مثل تقديم رقم بطاقة الائتمان. الهدف هو سرقة البيانات و معلومات تسجيل الدخول أو تثبيت برامج ضارة على جهاز الضحية وفقا لتقارير Cisco.

أنواع تهديدات الامن السيبراني

SQL- Injection -6

يعد إدخال لغة الاستعلام الهيكلية (SQL) نوعا من الهجمات الالكترونية التي تنتج عن إدخال إيعازات برمجية ضارة (malicious code) في خادم (server) يستخدم SQL. عند الاصابة يقوم الخادم (server) بإصدار أو إطلاق المعلومات (release information) .

أنواع تهديدات الامن السيبراني

7- هجمات كلمات المرور (Password Attack)
بإستخدام كلمة المرور الصحيحة، يمكن للمهاجم الاليكتروني الوصول الى ثروة من المعلومات. تعتبر الهندسة الاجتماعية نوع من هجمات كلمات المرور التي والتي تعرف فيها (Data Insider) بأنها الاستراتيجية التي يستخدمها المهاجمون (attackers) عبر الانترنيت والتي تعتمد بشكل كبير على التفاعل البشري حيث تتضمن غالبا خداع الاشخاص لخرق الامان. تشمل الانواع الاخرى من هجمات كلمات المرور الوصول الى قاعدة بيانات كلمات المرور أو التخمين المباشر.

أنواع تهديدات الامن السيبراني

إنترنيت الاشياء (Internet of Things)

توفر الاجهزة الفردية التي تتصل بالانترنيت أو الشبكات الاخرى نقطة وصول للمتسللين (Hackers)
لقد أفادت Cytelligence أنه في عام 2019، إستهدف المتسللون بشكل متزايد أجهزة المنزل الذكي و إنترنيت الاشياء (IoT)، مثل أجهزة التلفزيون الذكي و المساعد الصوتي و شاشات الاطفال المتصلة والهواتف المحمولة. لا يتمكن المتسللون الذين نحجوا في إختراق المنزل المتصل بالانترنيت من الوصول الى بيانات إعتماد Wi-Fi للمستخدمين فحسب، بل يمكنهم أيضا الوصول الى بياناتهم مثل السجلات الطبية وكشوف الحسابات المصرفية و معلومات تسجيل الدخول الى مواقع الويب.

أنواع تهديدات الامن السيبراني

إنترنيت الاشياء (Internet of Things)

توفر الاجهزة الفردية التي تتصل بالانترنيت أو الشبكات الاخرى نقطة وصول للمتسللين (Hackers)
لقد أفادت Cytelligence أنه في عام 2019، إستهدف المتسللون بشكل متزايد أجهزة المنزل الذكي و إنترنيت الاشياء (IoT)، مثل أجهزة التلفزيون الذكي و المساعد الصوتي و شاشات الاطفال المتصلة والهواتف المحمولة. لا يتمكن المتسللون الذين نحجوا في إختراق المنزل المتصل بالانترنيت من الوصول الى بيانات إعتماد Wi-Fi للمستخدمين فحسب، بل يمكنهم أيضا الوصول الى بياناتهم مثل السجلات الطبية وكشوف الحسابات المصرفية و معلومات تسجيل الدخول الى مواقع الويب.

مؤخرا تم اختراق 533 مليون حساب فيسبوك ويعد الثاني من نوعه .
حسب المواقع حصة العراق 17 مليون حساب تم اختراقه.
أطلقت شركة موزيلا الشهيرة أداة بسيطة تقوم بتحليل حالة الإيميل لمعرفة انه ضمن قائمة التسريبات الأخيرة والتسريبات القديمة إيضاً.

صمم اثنين من الباحثين Lloyd Davies وcharlie موقع إلكتروني تم إطلاق عليه اسم Have I Been Zucked وذلك اقتباسا من اسم مؤسس الفيسبوك Mark Zuckerberg

من خلال الموقع تستطيع معرفة اذا كنت احد ضحايا التسريب الذي حصل مؤخرا،