الامن السيبراني اوكسجين التحول الرقمي

م.ايمان إسماعيل حامد

قسم الحاسوب

المقدمة

- يعد الأمن السيبراني مكوناً أساسياً من مكونات أي تحول رقمي؛ حيث إن حماية البيانات والبنية التحتية ستكون مصدر قلق كبير للحكومة والعامة والقطاع الخاص بسبب نمو الهجمات السيبرانية أصبح من الضروري التعامل مع مثل هذه الهجمات ومعالجتها بشكل مبتكر، والأمن السيبراني هو عبارة عن مجموع الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لمنع اختراق شبكات المعلومات، بالذات تلك التي تحتوي معلومات سرية، والحماية من هجمات التعطيل والهجمات الإلكترونية للهاكرز، والحماية من الجريمة الإلكترونية، والحماية من تهديدات الفيروسات وكذلك الحماية من اختراق ترددات المكالمات.

- الأمن السيبراني كلمة (سيبر) Cyberهي صفة لأي شيء له علاقة بالحواسيب وتقنيات المعلومات، والتي تستخدم بمجملها الواقع الافتراضي، وبالتالي فالسيبرانية هي فضاء الانترنت، أما الأمن السيبراني فهو الذي يهتم بأمن المعلومات على شبكات الحاسوب المرتبطة بالإنترنت، وحمايتها من أي دخول غير مصرح به أو أي تغير أو اختلال قد يحدث فيها، وكذلك من الجرائم السيبرانية التي تعد سلوك غير قانوني أو شرعي منافيًا للأخلاق يحدث على شبكة المعلومات العالمية، وللوصول لهذه الغاية تُستخدم مجموعة من الوسائل التقنية والإدارية لمنع هذا الدخول الغير مصرح به، إذ يعتبره البعض مجالاً جديداً للحروب الحديثة التي تهدد جميع شبكات الحاسوب الموجودة حول العالم، وتشمل الشبكات التي تستخدم الألياف البصرية واللاسلكية، فهو ليس فقط شبكة الانترنت، ولكنه شبكات أخرى تتصل بهذه الشبكة بطريقة أو بأخرى، كشبكات gps، Gsm، فالبنى التحتية وأنظمة الاتصالات الرقمية هي جزء مهم من هذا الفضاء.

- ارتفعت معدلات الإنفاق العالمية على الأمن الإلكتروني من ٧١.١ مليون دولار عام ٢٠١٤ إلى ٧٥ مليون دولار عام ٢٠١٥، وفق موقع FireEyeللأمن السيبراني، ويتوقع أن تصل إلى ١٠١ مليون دولار عام ٢٠١٨ خلال السنوات العشر القادمة، سترتفع هذه المعدلات بشكل مخيف جراء توجه العالم بشكل جذري نحو تكنولوجيا أجهزة الاستشعار وربطها بشبكة الإنترنت، حيث بالإمكان تتبع كلّ شيء من ضربات القلب، معدل الركض في اليوم، نوعية النوم وغيرها الكثير من المعلومات التي يجب حمايتها بشتى الوسائل للحفاظ على حقنا في الخصوصية.

خطر على الامن السيبراني

- يمكن تخيل الأمر بمقاربة بسيطة: تخيلوا منزلاً بباب قوي ومتين، ويأتي شخصٌ يريد الدخول إلى المنزل اكتشف هذا الشخص أن أحد جدران هذا المنزل لديه نافذة مقفلة ولكن ليس بإحكام، فيبتكر طريقة لفتح الباب والدخول هذا السيناريو يمثل اكتشاف الثغرات الأمنية بدقة بحيث يستطيع "المخترق" أن يكتشف نقاط ضعف في النظام تسمح له باختراقه يتم اكتشاف الثغرات من خلال المعارف التقنية التي يكتسبها هؤلاء الأشخاص ويتم استغلالها لمصالح خاصة أو لها علاقة بأنظمة دولية، وقد تكون هذه الثغرات أموراً بسيطة جداً مثل اكتشاف الجهة المعنية أن جميع أفراد هذه الشركة يستخدمون رمزاً سرياً واحداً للدخول إلى حواسيبهم في الشركة، أو أن تكون جميع أسماء المستخدمين تتألف من الحرف الأول من الاسم واسم العائلة.
- جزء كبير من الحروب اليوم تشن على الفضاء السيبراني، من اختلاس معلومات، إلى تعطيل أنظمة شديدة الحساسية تدرك الشركات أن القدرة على امتلاك الثغرات أصبحت أكثر سهولة عما كانت عليه في السابق، بسبب وجود أشخاص مهتمين حصرياً ومتخصصين في هذا المجال، بحيث بات بإمكان أي كان أن يصبح "مهاجماً سيبرانياً" وهذا ينعكس بازدياد سرعة وتيرة الهجمات السيبرانية وقد باتت هذه الهجمات "أكبر تهديد للشركات"، وفق ما أعلنت الرئيسة والمديرة التنفيذية لشركة IBM فرجينيا ماري روميتي عام ٢٠١٥.

أهمية الأمن السيبراني

- في عالمنا المترابط بواسطة الشبكة، يستفيد الجميع من برامج الدفاع السيبراني فمثلاً على المستوى الفردي يمكن أن يؤدي هجوم الأمن السيبراني إلى سرقة الهوية أو محاولات الابتزاز أو فقدان البيانات المهمة مثل الصور العائلي كما تعتمد المجتمعات على البنية التحتية الحيوية مثل محطات الطاقة والمستشفيات وشركات الخدمات المالية لذا فإن تأمين هذه المنظمات وغيرها أمر ضروري للحفاظ على عمل مجتمعنا بطريقة آمنة وطبيعية.

- يستفيد الجميع أيضًا من عمل الباحثين في مجال الأمن السيبراني ، فمثلاً يضم فريق تالوس ٢٥٠ باحثاً يحققون في التهديدات الجديدة والناشئة واستراتيجيات الهجوم السيبراني فهم يكشفون عن نقاط الضعف الجديدة، ويثقفون الجمهور بشأن أهمية الأمن السيبراني، ويعملون على تقوية أدوات المصادر المفتوحة مما يجعل العمل على الإنترنت أكثر أمانًا للجميع.

- هناك أنواع عديدة من التهديدات السيبرانية التي يمكنها مهاجمة الأجهزة والشبكات، ولكنها تقع عموماً في ثلاث فئات؛ وهي الهجمات على السرية، النزاهة، والتوافر.
- الهجمات على السرية Confidentialityتشمل سرقة معلومات التعريف الشخصية، والحسابات المصرفية، أو معلومات بطاقة الائتمان، حيث يقوم العديد من المهاجمين بسرقة المعلومات، ومن ثم بيعها على شبكة الإنترنت المظلمة Dark Webلكي يشتريها الآخرون، ويستخدموها بشكل غير شرعي.
- الهجمات على النزاهةIntegrity تتكون هذه الهجمات من التخريب الشخصي أو المؤسساتي، وغالباً ما تسمى بالتسريبات؛ إذ يقوم المجرم الإلكتروني بالوصول إلى المعلومات الحساسة، ثم نشرها، بغرض كشف البيانات، والتأثير على الجمهور لإفقاد الثقة في تلك المؤسسة أو الشخصيّة.
- الهجمات على التوافرAvailabilityالهدف منها هو منع المستخدمين من الوصول إلى بياناتهم الخاصة إلى أن يدفعوا رسومًا ماليّة، أو فدية معيّنة.

- اعلى ١٠ دول في العالم في الأمن السيبراني:
- ١- بريطانيا
- ٢- الولايات المتحدة الأميركية
- ٣- فرنسا
- ٤- ليتوانيا
- ٥- استونيا
- ٦- سنغافورة
- ٧- إسبانيا
- - ماليزيا
- ٩- كندا
- ١٠- النرويج

ترتيب الدول العربية

يرصد التقييم الذي شمل ١٧٥ دولة على مستوى العالم الممارسات والأدوات التي تستخدمها الدول لحماية الأنظمة والشبكات والبرامج من الهجمات الرقمية.

- السعودية
- عمان
- قطر
- مصر
- الإمارات
- الكويت
- البحرين
- الأردن
- تونس
- المغرب
- فلسطين
- السودان
- العراق
- الجزائر
- سوريا
- ليبيا
- لبنان
- موريتانيا
- الصومال
- جيبوتي
- اليمن
- جزر القمر

نشكر لكم حسن اصغائكم