العدد واحد وأربعون
تاريخ الإصدار: 2 – آذار – 2022 م
www.ajsp.net
ISSN: 2663-5798

"الأمن السيبراني واهميته في حماية الانظمة والبيانات"

إعداد الباحث:

عبدالمجيد صالح الحياري

بلدية السلط الكبرى

العدد واحد وأربعون
تاريخ الإصدار: 2 – آذار – 2022 م
www.ajsp.net
ISSN: 2663-5798

الملخص:

الأمن السيبراني عبارة عن تقنيات منصوص عليها بشكل عام في المواد المنشورة والتي تحاول حماية البيئة السيبرانية لمستخدم أو مؤسسة. يدير مجموعة التقنيات المستخدمة لحفظ سلامة الشبكات والبرامج والبيانات من الوصول غير المصرح به. يشير إلى مجموعة التقنيات والعمليات ، وقد يشار إليه أيضًا بأمن تكنولوجيا المعلومات. يزداد هذا المجال أهمية بسبب الاعتماد المتزايد على أنظمة الكمبيوتر ، بما في ذلك الهواتف الذكية وأجهزة التلفزيون والأجهزة الصغيرة المختلفة التي تشكل إنترنت الأشياء.

المقدمة:

لقد جعل الإنترنت العالم أصغر من نواحٍ عديدة ، لكنه فتح لنا أيضًا تأثيرات لم تكن من قبل بهذا التنوع والتحدي من قبل. مع نمو الأمن بسرعة ، نما عالم القرصنة بشكل أسرع. هناك طريقتان للنظر في مسألة الأمن السيبراني. الأول هو أن الشركات التي توفر الحوسبة السحابية تفعل ذلك فقط بحيث يتم تأمين هذه الشركات بشكل جيد للغاية باستخدام أحدث تقنيات التشفير المتطورة. يعد الإنترنت من أهم اختراعات القرن الحادي والعشرين التي أثرت على حياتنا. لقد تجاوز الإنترنت اليوم كل عوائق وغيرت الطريقة التي نستخدمها للتحدث ، ولعب الألعاب ، والعمل ، والتسوق ، وتكوين صداقات ، والاستماع إلى الموسيقى ، ومشاهدة الأفلام ، وطلب الطعام ، ودفع الفاتورة ، وتحية صديقك في عيد ميلاده / الذكرى السنوية ، وما إلى ذلك. سمها ، ولدينا تطبيق مطبق لذلك. لقد سهلت حياتنا بجعلها مريحة. لقد ولت الأيام التي نضطر فيها إلى الوقوف في طابور طويل لدفع فواتير الهاتف والكهرباء. الآن يمكننا دفعها بنقرة زر واحدة من منزلنا أو مكتبنا. لقد وصلت التكنولوجيا إلى حد أننا لا نحتاج حتى إلى جهاز كمبيوتر لاستخدام الإنترنت. الآن لدينا هاتف ذكي مزود بالإنترنت ، ما إلى ذلك يمكننا من خلاله البقاء على اتصال بأصدقائنا وعائلتنا ومكتبنا على مدار الساعة طوال أيام الأسبوع. لم يسهّل الإنترنت حياتنا فحسب ، بل جعل أيضًا العديد من الأشياء في متناول الطبقة الوسطى من خلال جعلها فعالة من حيث التكلفة. لم يمض وقت طويل إلى الوراء ، أثناء إجراء مكالمة ISD أو حتى مكالمة من الأمراض المنقولة بالاتصال الجنسي ، أصيبت العيون بمقياس النبض. كانت المكالمات مكلفة للغاية. تم استخدام ISD و STD لتمرير الرسائل العاجلة فقط وتم استخدام بقية الاتصالات الروتينية باستخدام الحروف لأنها كانت رخيصة جدًا نسبيًا. لقد أتاح الإنترنت الآن ليس فقط التحدث ولكن استخدام مؤتمر الفيديو باستخدام التطبيقات الشائعة مثل سكايب وما إلى ذلك بسعر منخفض للغاية إلى مستوى تكون فيه محادثة الفيديو لمدة ساعة واحدة باستخدام الإنترنت أرخص من تكلفة إرسال مستند من صفحة واحدة من دلهي إلى بنغالور باستخدام خدمة البريد السريع أو البريد السريع. ليس هذا فقط ، لقد غير الإنترنت استخدام الأجهزة النموذجية التي استخدمناها. يمكن استخدام التلفزيون ليس فقط لمشاهدة البرامج التلفزيونية والأفلام الشهيرة ولكن يمكن استخدامه للاتصال / الدردشة المرئية مع الأصدقاء باستخدام الإنترنت. لا يتم استخدام الهاتف المحمول فقط لإجراء مكالمة ولكن لمشاهدة أحدث فيلم. يمكننا أن نظل على اتصال مع الجميع ، بغض النظر عن موقعنا. يمكن للوالدين العاملين من المكتب مراقبة أطفالهم في المنزل ومساعدتهم في أداء واجباتهم المدرسية. يمكن لرجل الأعمال أن يراقب موظفيه ومكتبه ومتجره وما إلى ذلك بنقرة زر واحدة. لقد سهلت حياتنا بأكثر من طريقة. هل تساءلت يومًا من أين جاء هذا الإنترنت؟ دعونا نناقش التاريخ المختصر للإنترنت ونتعلم كيف تم اختراع هذا الإنترنت وكيف تطور إلى حد لا يمكننا الآن التفكير في حياتنا بدونه.

العدد واحد وأربعون
تاريخ الإصدار: 2 – آذار – 2022 م
www.ajsp.net
ISSN: 2663-5798

تاريخ الإنترنت

لا أعرف ما الذي أعطته الحرب الباردة بين الولايات المتحدة الأمريكية وروسيا للعالم ، ولكن بتحدٍ يعتبر الإنترنت أحد تلك الاختراعات المفيدة جدًا التي وُضعت أسسها خلال الحرب الباردة أيام. أطلقت روسيا أول قمر صناعي في العالم ، SPUTNIK إلى الفضاء في 4 أكتوبر 1957. كان هذا بوضوح انتصار روسيا على الفضاء السيبراني وكخطوة مضادة ، وكالة مشاريع الأبحاث المتقدمة ، الذراع البحثية لوزارة الدفاع ، المتحدة أعلنت الدول عن إطلاق شبكة ARPANET (وكالة مشاريع الأبحاث المتقدمة NETwork) في أوائل الستينيات. كانت هذه شبكة تجريبية وتم تصميمها لإبقاء أجهزة الكمبيوتر متصلة بهذه الشبكة للتواصل مع بعضها البعض حتى لو فشل أي من العقدة ، بسبب هجوم بالقنابل ، في الاستجابة. تم إرسال الرسالة الأولى عبر ARPANET ، وهي شبكة تبديل للتعبئة ، بواسطة مختبر ليونارد كلاينروك في جامعة كاليفورنيا ، لوس أنجلوس (UCLA). ستندهش من معرفة أن الرسالة الأولى التي تم إرسالها عبر الإنترنت كانت "LO". في الواقع ، كانوا يعتزمون إرسال العمل "LOGIN" ووصل الحرفان الأولان فقط إلى وجهتهما عند عقدة الشبكة الثانية في معهد ستانفورد للأبحاث (SRI) وقبل أن تصل الأحرف الثلاثة الأخيرة إلى الوجهة كانت الشبكة معطلة بسبب خلل. سرعان ما تم إصلاح الخطأ وتم إرسال الرسالة واستياءها المهمة الرئيسية التي يتعين على ARPANET لعبها هي تطوير قواعد الاتصال ، أي بروتوكولات الاتصال عبر ARPANET. أدى ARPANET على وجه الخصوص إلى تطوير بروتوكولات للعمل عبر الإنترنت ، والتي يمكن من خلالها ربط عدة شبكات منفصلة في شبكة من الشبكات. أدى ذلك إلى تطوير مجموعة بروتوكولات TCP / IP ، والتي تحدد قواعد الانضمام والتواصل عبر APRANET. بعد فترة وجيزة ، في عام 1986 ، تم إنشاء العمود الفقري NSF (مؤسسة العلوم الوطنية) وتم ربط خمس جامعات أمريكية بمراكز الحوسبة لتشكيل NSFnet. الجامعات المشاركة كانت:

1- جامعة برينستون – مركز جون فون نيومان الوطني للحواسيب العملاقة ، JvNC
2- جامعة كورنيل – مركز نظرية كورنيل
3- جامعة إلينوي في أوربانا شامبين – المركز الوطني لتطبيقات الحوسبة الفائقة ، NCSA
4- جامعة كارنيجي ميلون – مركز الحاسوب الفائق بيتسبرغ ، PSC

عنوان الإنترنت

مع وجود العديد من الأجهزة المتصلة بالإنترنت ، نحتاج إلى آلية ما للتعرف بشكل فريد على كل جهاز متصل بالإنترنت. كما أننا بحاجة إلى بعض المركزية النظام الذي يعتني بهذه الآلية بحيث لا تتكرر العلامات المستخدمة لتحديد كل جهاز ؛ وإلا فإن الغرض كله هزم. لرعاية ذلك ، لدينا سلطة مركزية تُعرف باسم هيئة الأرقام المخصصة للإنترنت (IANA) ، وهي مسؤولة عن تعيين رقم فريد يُعرف بعنوان IP (عنوان بروتوكول الإنترنت). عنوان IP هو رقم ثنائي 32 بت مقسم إلى أربع ثماني بتات وتتكون كل ثماني بتات من 8 أرقام ثنائية ويتم فصل هذه الثمانيات بنقطة (.). مثال على عنوان IP هويمكن أن تحتوي كل 8 بت في ثماني بتات على قيمتين ثنائيتين ، أي 0 و 1. لذلك ، يمكن أن يكون لكل ثماني بتات حد أدنى للقيمة 0. أي 00000000 إلى الحد الأقصى للقيمة 256 أي 11111111 ومجموعًا 28 = 256 مجموعة مختلفة. مرة أخرى ، من الصعب بعض الشيء تذكر عنوان 32 بت هذا ، لذلك من أجل فهم أفضل للإنسان ، يتم التعبير عنه بتنسيق عشري. لكن هذا التنسيق العشري مخصص لفهم الإنسان فقط ويفهمه الكمبيوتر في التنسيق الثنائي فقط. في النظام العشري ، يتم التعبير عن عنوان IP أعلاه كـ 123.45.78.125 تُستخدم هذه الثمانيات لإنشاء وفصل

العدد واحد وأربعون
تاريخ الإصدار: 2 – آذار – 2022 م
www.ajsp.net
ISSN: 2663-5798

فئات مختلفة. يتكون عنوان IP من جزأين. الشبكة والمضيف. يحدد جزء الشبكة الشبكة المختلفة للشبكة ويحدد الجزء المضيف جهازًا لشبكة معينة.

تخصيص عناوين IP في منطقتهم. تم سرد سجلات الإنترنت الإقليمية هذه جنبًا إلى جنب مع منطقة عملياتها أدناه:

1–APNIC– هذا RIR مسؤول عن خدمة منطقة آسيا والمحيط الهادئ

2– AfriNIC– هذا RIR مسؤول عن خدمة المنطقة الأفريقية

3– ARIN– هذا RIR مسؤول عن خدمة أمريكا الشمالية والعديد من جزر الكاريبي وشمال الأطلسي.

4– LACNIC– هذا RIR مسؤول عن خدمة أمريكا اللاتينية ومنطقة البحر الكاريبي.

5– RIPE NCC– هذا RIR مسؤول عن خدمة أوروبا والشرق الأوسط وأجزاء من آسيا الوسطى.

للاتصال والتنسيق بين هذه RIRs الخمسة ، هناك منظمة تسمى منظمة موارد الأرقام (NRO). هذه المنظمات.

البنية التحتية للإنترنت

الإنترنت ، كما يوحي الاسم ، في شبكة من الشبكات ، أي أنه عبارة عن مجموعة من عدة شبكات صغيرة ومتوسطة وكبيرة. يشير هذا بوضوح إلى حقيقة واحدة ، لا أحد هو مالك واحد للإنترنت وهو أحد الأمثلة المثبتة للنجاح التعاوني. الآن يجب أن تتفاجأ كيف يمكن لمثل هذه الشبكة الكبيرة المنتشرة عبر القارات أن تعمل دون أي مشكلة. نعم ، من الصحيح أنه لمراقبة مثل هذه الشبكة الكبيرة ، نحتاج إلى هيئة دولية يمكنها صياغة القواعد واللوائح والبروتوكولات للانضمام إلى هذه الشبكة واستخدامها. لذلك ، تم تشكيل منظمة دولية ، تُعرف باسم "مجتمع الإنترنت" في عام 1992 لرعاية مثل هذه القضايا دعونا نناقش الآن كيف يعمل هذا الإنترنت؟ كيف يتم تلقي البريد الإلكتروني الذي أرسلته إلى صديقك بواسطة كمبيوتر صديقك الموجود في بلد / قارة أخرى. عندما تعمل على الكمبيوتر المحمول / الكمبيوتر المكتبي في منزلك دون الاتصال بالإنترنت ، فإن جهاز الكمبيوتر الخاص بك هو نظام مستقل. ولكن عندما تتصل بالإنترنت عن طريق الاتصال بمزود خدمة الإنترنت (ISP) باستخدام المودم الخاص بك ، فإنك تصبح جزءًا من الشبكة. مزود خدمة الإنترنت هو الرابط بين العمود الفقري للإنترنت ، والذي من خلاله يتم توجيه البيانات بالكامل ، والمستخدم. يتصل مزود خدمة الإنترنت (ISP) بالعمود الفقري للإنترنت عند نقاط وصول الشبكة (NAP). يتم توفير برامج العمل الوطنية هذه من قبل شركات الاتصالات الكبيرة في مناطق مختلفة. تربط شركات الاتصالات الكبيرة هذه البلدان والقارات من خلال بناء وصيانة البنية التحتية الأساسية الكبيرة لتوجيه البيانات من NAP إلى NAP. ISPs متصلون بهذا العمود الفقري في NAP وهم مسؤولون عن بناء وإدارة الشبكة محليًا. لذلك عند الاتصال بالإنترنت من خلال المودم ، تصبح أولاً جزءًا من مزود خدمة الإنترنت المحلي ، والذي بدوره يتصل بالعمود الفقري للإنترنت من خلال NAP. يتم توجيه البيانات من خلال هذا العمود الفقري وإرسالها إلى الوجهة NAP ، حيث يوجد مزود خدمة الإنترنت لشبكة أصدقائك. بمجرد أن يطلب صديقك المودم الخاص به للاتصال بالإنترنت ، يتم تسليم البيانات إلى كمبيوتر صديقك.

العدد واحد وأربعون
تاريخ الإصدار: 2 – آذار – 2022 م
www.ajsp.net
ISSN: 2663-5798

شبكة الانترنت

في بعض الأحيان نستخدم مصطلح الإنترنت وشبكة الويب العالمية بشكل تبادلي أو ببساطة الويب ، كما يُعرف شعبياً باسم. لكن الويب ليست سوى واحدة من العديد من الأدوات المساعدة التي يوفرها الإنترنت. بعض الخدمات الشائعة التي يوفرها الإنترنت لغيرها هي البريد الإلكتروني ، والمستخدمين ، وخدمة الرسائل ، وبروتوكول نقل الملفات ، وما إلى ذلك. يستخدم الويب بروتوكول HTTP للتواصل عبر الإنترنت وتبادل المعلومات. تم تطوير الويب في (CERN (Europeen de Reserches Nucleaires ، سويسرا) بواسطة عالم بريطاني Tim Berners–Lee في عام 1989. وهو يتكون من جميع مواقع الويب العامة وجميع الأجهزة التي تصل إلى محتوى الويب. WWW هو نموذج لمشاركة المعلومات تم تطويره لتبادل المعلومات عبر الإنترنت. هناك الكثير من المواقع العامة ، وهي عبارة عن مجموعة من صفحات الويب ، متاحة عبر الإنترنت. تحتوي صفحات الويب هذه على الكثير من المعلومات في شكل نصوص ومقاطع فيديو وصوت وصورة. يتم الوصول إلى صفحات الويب هذه باستخدام برنامج تطبيقي يسمى متصفح الويب.

ما هو الأمن السيبراني

كونها محمية بواسطة أنظمة متصلة بالإنترنت ، بما في ذلك الأجهزة والبرامج والبيانات ، من الهجمات الإلكترونية. في سياق الحوسبة ، يشمل الأمن الأمن السيبراني والأمن المادي كلاهما تستخدمهما المؤسسات للحماية من الوصول غير المصرح به إلى مركز البيانات والأنظمة المحوسبة الأخرى. الأمان ، المصمم للحفاظ على سرية البيانات وسلامتها وتوافرها ، هو مجموعة فرعية من الأمن السيبراني. لماذا نحتاج إلى الأمن السيبراني يشمل نطاق عمليات الأمن السيبراني حماية المعلومات والأنظمة من التهديدات السيبرانية الرئيسية. تأخذ هذه التهديدات عدة أشكال. نتيجة لذلك ، يمكن أن تشكل مواكبة استراتيجية وعمليات الأمن السيبراني تحديًا ، لا سيما في شبكات الحكومة والمؤسسات حيث غالبًا ما تستهدف التهديدات السيبرانية ، في شكلها الأكثر ابتكارًا ، الأصول السرية والسياسية والعسكرية لدولة ما أو أفرادها بعض التهديدات الشائعة هي:

1- الإرهاب السيبراني: هو الاستخدام المبتكر لتكنولوجيا المعلومات من قبل الجماعات الإرهابية لتعزيز أجندتهم السياسية. اتخذت شكل هجمات على الشبكات وأنظمة الكمبيوتر والبنية التحتية للاتصالات.
2- الحرب السيبرانية: وهي تنطوي على استخدام الدول القومية لتكنولوجيا المعلومات للمرور عبر شبكات دولة أخرى لإحداث الضرر. في الولايات المتحدة والعديد من الأشخاص الآخرين الذين يعيشون في مجتمع ، تم الاعتراف بالحرب الإلكترونية على أنها المجال الخامس للحرب. يتم تنفيذ هجمات الحرب الإلكترونية في المقام الأول من قبل قراصنة مدربين تدريباً جيداً على الاستفادة من جودة تفاصيل شبكات الكمبيوتر ، ويعملون تحت رعاية ودعم الدول القومية. بدلاً من إغلاق الشبكات الرئيسية للهدف ، قد يُجبر هجوم الحرب الإلكترونية على وضع الشبكات في تعريض البيانات القيمة للخطر ، أو إضعاف الاتصالات ، أو إضعاف خدمات البنية التحتية مثل النقل والخدمات الطبية ، أو مقاطعة التجارة.
3- التجسس السيبراني: هي ممارسة استخدام تقنية المعلومات للحصول على معلومات سرية دون إذن من أصحابها أو حامليها. غالبًا ما يتم استخدامه لاكتساب ميزة استراتيجية واقتصادية وعسكرية ، ويتم إجراؤه باستخدام تقنيات التكسير والبرامج الضارة.

العدد واحد وأربعون
تاريخ الإصدار: 2 – آذار – 2022 م
www.ajsp.net
ISSN: 2663-5798

من هم مجرمين الإنترنت

أنها تنطوي على أنشطة مثل نشاط أو أعضاء جنسية مطبوعة للأطفال ؛ الاحتيال بواسطة بطاقات الائتمان؛ المطاردة السيبرانية تشويه سمعة شخص آخر عبر الإنترنت ؛ الحصول على وصول غير مصرح به إلى أنظمة الكمبيوتر ؛ تجاهل حقوق النشر وترخيص البرامج والعلامات التجارية الآمنة للحماية ؛ تجاوز التشفير لعمل نسخ غير قانونية ؛ قرصنة البرامج وسرقة هوية شخص آخر للقيام بأعمال إجرامية. مجرمو الإنترنت هم أولئك الذين يرتكبون مثل هذه الأفعال. يمكن تصنيفهم إلى ثلاث مجموعات تعكس دوافعهم.

مجرمو الإنترنت – متعطشون للاعتراف:

1- الهاكرز.
2- متخصصو تكنولوجيا المعلومات (الهندسة الاجتماعية هي أحد أكبر التهديدات) ؛
3- قراصنة ذوو دوافع سياسية.
4- التنظيمات الارهابية.

مجرمو الإنترنت – غير مهتمين بالاعتراف:

1- قراصنة ذوو دوافع مالية (تجسس الشركات).
2- القرصنة برعاية الدولة (تجسس وطني ، تخريب) ؛
3- المجرمين المنظمين.

مجرمو الإنترنت – المطلعون:

1- موظفون سابقون يسعون للانتقام.

2- الشركات المتنافسة التي تستخدم موظفين للحصول على ميزة اقتصادية من خلال التلف / أو السرقة.

كيفية الحفاظ على الأمن السيبراني الفعال

تاريخياً ، اتخذت المنظمات والحكومات نهج "المنتج النقطي" التفاعلي لمكافحة التهديدات السيبرانية ، وتنتج شيئًا ما معًا من تقنيات الأمان الفردية – واحدة فوق الأخرى لتأمين شبكاتها والبيانات القيمة بداخلها. هذه الطريقة ليست باهظة الثمن ومعقدة فحسب ، ولكن أخبار الانتهاكات السيبرانية الضارة لا تزال تهيمن على عناوين الأخبار ، مما يجعل هذه الطريقة غير فعالة. في الواقع ، بالنظر إلى مجال مجموعة الأشخاص الذين انتهكوا البيانات ، فقد تم إطلاق موضوع الأمن السيبراني على رأس قائمة أولويات مجالس الإدارة ، والتي سعوا إليها بقدر أقل من المخاطرة. بدلاً من ذلك ، يمكن للمؤسسات التفكير في نظام أساسي للأمان من الجيل التالي مُتكامل محليًا ومصمم خصيصًا لتوفير حماية متسقة قائمة على الوقاية – عند نقطة النهاية ، في مركز البيانات ، على الشبكة ، في السحابات العامة والخاصة ، وعبر Saabs البيئات. من خلال التركيز على الوقاية ، يمكن للمؤسسات منع التهديدات السيبرانية من التأثير على الشبكة في المقام الأول ، وتقليل مخاطر الأمن السيبراني بشكل عام إلى درجة يمكن التحكم فيها.

العدد واحد وأربعون
تاريخ الإصدار: 2 – آذار – 2022 م
www.ajsp.net
ISSN: 2663-5798

ما يمكن للأمن السيبراني منعه

يمكن أن يساعد استخدام الأمن السيبراني في منع الهجمات الإلكترونية وخروقات البيانات وسرقة الهوية ويمكن أن يساعد في إدارة المخاطر. عندما يكون لدى المؤسسة إحساس قوي بأمان الشبكة وخطة فعالة للاستجابة للحوادث ، فإنها تكون قادرة بشكل أفضل على منع هذه الهجمات وخطورتها. على سبيل المثال ، تدافع حماية المستخدم النهائي عن المعلومات والحماية من الضياع أو السرقة أثناء فحص أجهزة الكمبيوتر بحثًا عن التعليمات البرمجية الضارة.

أنواع تهديدات الأمن السيبراني: يعد استخدام مواكبة التقنيات الجديدة والاتجاهات الأمنية وذكاء التهديدات مهمة صعبة. ومع ذلك ، يجب أن يكون ذلك من أجل حماية المعلومات والأصول الأخرى من التهديدات السيبرانية ، والتي تتخذ أشكالًا عديدة.

1- أدوات الفدية هي نوع من البرامج الضارة التي تنطوي على مهاجم يقوم بقفل ملفات نظام الكمبيوتر للضحية عادةً من خلال التشفير والمطالبة بالدفع لفك تشفيرها وفتحها.

2- البرامج الضارة هي أي ملف أو برنامج يستخدم لإلحاق الضرر بمستخدم الكمبيوتر ، مثل الفيروسات المتنقلة وفيروسات الكمبيوتر وأحصنة طروادة وبرامج التجسس.

1-الهندسة الاجتماعية هي هجوم يعتمد على التفاعل البشري لخداع المستخدمين لخرق الإجراءات الأمنية من أجل الحصول على معلومات حساسة محمية عادة.

2- التصيد هو شكل من أشكال الاحتيال حيث يتم إرسال رسائل بريد إلكتروني احتيالية تشبه رسائل البريد الإلكتروني من مصادر موثوقة ؛ ومع ذلك ، فإن القصد من رسائل البريد الإلكتروني هذه هو سرقة البيانات الحساسة ، مثل بطاقة الائتمان أو معلومات تسجيل الدخول.

ماذا يفعل محلل الأمن؟

يعمل محللو أمن المعلومات على حماية أنظمة الشركة وشبكاتها من خلال التخطيط وتنفيذ إجراءات الأمان. إنهم ينشئون حلولًا تخريبية لمنع سرقة المعلومات الهامة أو إتلافها أو اختراقها. تتمثل مسؤوليتهم الأساسية في الحفاظ على بيانات الأعمال أو المؤسسات والعملاء والموظفين وأي معلومات افتراضية مخزنة آمنة من الهجمات الإلكترونية أو القرصنة من أي نوع.

ما هي عواقب الهجوم السيبراني؟

ستؤدي الهجمات الإلكترونية عبر الإنترنت إلى مزيد من الضرر المالي والسمعة للمنظمات الأكثر قدرة على الصمود. يتعين على المنظمة التي تعاني من هجوم إلكتروني أن تواجه الأصول الخاسرة والسمعة التجارية ومن المحتمل أن تواجه المنظمة غرامات تنظيمية واتخاذ الإجراءات القانونية وتكاليف الإصلاح. وجدت دراسة استقصائية أجرتها حكومة المملكة المتحدة حول الأمن السيبراني في عام 2017 ، أن متوسط تكلفة الأعمال التجارية الكبيرة هو 19600 جنيهًا إسترلينيًا وبالنسبة للشركات الصغيرة والمتوسطة الحجم هو 1570 جنيهًا إسترلينيًا.

أدوات القرصنة

هناك أدوات مختلفة هي أساليب الهجوم. ويتم استخدام البرامج الضارة لمجمل هذه الأدوات. الأمثلة هي الفيروسات والديدان. برامج الكمبيوتر التي تعيد إنتاج نسخ وظيفية لنفسها بتأثيرات متفاوتة تتراوح من التأكيد والإزعاج إلى المساومة على سرية أو سلامة المعلومات ، وأحصنة طروادة ، البرامج المدمرة التي تتظاهر بأنها تطبيقات حميدة ولكنها تنشئ بابًا خلفيًا حتى يتمكن المخترق من العودة لاحقًا وادخل النظام. غالبًا ما يكون اختراق النظام هو الهدف الرئيسي لاقتحام النظام وهو هجمات أكثر تقدمًا. إذا حصل المتسلل على سيطرة كاملة على النظام ، أو وصول إلى "الجذر" ، فسيكون لديه وصول غير مقيد إلى الأعمال الداخلية للنظام. نظرًا لخصائص المعلومات المخزنة رقميًا ، فإن الشخص ذو النية الإجرامية سوف يؤخر ، أو يعطل ، أو يفسد ، أو يستغل ، أو يدمر ، سرقة المعلومات وتعديلها. ستعتمد قيمة المعلومات أو أهمية التطبيق على المعلومات المطلوبة وأن مثل هذه الإجراءات سيكون لها تأثير مختلف بدرجات متفاوتة من الجاذبية.

مستوى المخاطر السيبرانية

هناك بعض الأسباب الإضافية للمبالغة في تقدير هذا التهديد. أولاً ، نظرًا لأن مكافحة التهديدات الإلكترونية أصبحت قضية مسيسة إلى حد كبير ، يجب أيضًا النظر إلى البيانات الرسمية حول مستوى التهديد في سياق الكيانات البيروقراطية المختلفة التي تتنافس فيما بينها على الموارد والنفوذ. يتم ذلك عادةً من خلال ذكر الحاجة الملحة لاتخاذ إجراء (وهو ما ينبغي عليهم اتخاذه) ووصف التهديد العام بأنه كبير ومتزايد. ثانيًا ، أظهر البحث النفسي أن إدراك المخاطر يعتمد بشكل كبير على الحدس والعواطف ، بالإضافة إلى تصورات الخبراء تتلاءم المخاطر السيبرانية ، لا سيما في شكلها الأكثر تطرفًا ، مع ملف المخاطر لما يسمى "المخاطر الرهيبة" ، والتي تبدو كارثية ومميتة وغير معروفة لا يمكن السيطرة عليها. هناك ميل للخوف من مخاطر احتمالية منخفضة ، وهو ما يترجم إلى ضغط لخدمة عمل ما مع كل أنواع الاستعداد لتحمل تكاليف عالية من الفوائد غير المؤكدة. فقط النظام الذي يهاجم بشكل مدمر أو تخريبي بما فيه الكفاية هو الذي يحتاج إلى اهتمام جهاز الأمن القومي التقليدي. الهجمات التي تعطل الخدمات أو التي تكلف بشكل أساسي إزعاج الكمبيوتر.

الحد من الأمن السيبراني

لقد تم تناول النقاشات الثلاث المختلفة حول العديد من المفاهيم وتم إنتاج تدابير مضادة مع التركيز عليها. شبكة الكمبيوتر التي تمتلك كيانات لديها ممارسة شائعة لتحمل مسؤولية حمايتها. ومع ذلك ، هناك بعض الأصول التي تعتبر بالغة الأهمية في القطاع الخاص لعمل المجتمع ويجب على الحكومات اتخاذ تدابير إضافية لضمان مستوى الحماية. وعادة ما يتم تضمين هذه الجهود تحت عنوان (المعلومات) الحرجة. ضمان المعلومات هو دليل لحماية البنية التحتية وإدارة المخاطر ، والتي تتعلق أساسًا بقبول أن الشخص (أو يظل) غير آمن: لا يمكن أبدًا خفض مستوى المخاطر إلى الصفر. هذا يعني أن الحوادث السيبرانية الصغيرة وربما الكبيرة لا بد أن تحدث لأنه لا يمكن تجنبها حتى مع إدارة المخاطر بشكل مثالي.

الخاتمه:

اعتمادًا على شدتها (المحتملة) ، ستستمر الحوادث التخريبية في المستقبل في تأجيج الخطاب العسكري ومعها مخاوف من حرب إلكترونية استراتيجية. من المؤكد أن التفكير (والتخطيط) في أسوأ السيناريوهات هو مهمة مشروعة لجهاز الأمن القومي. ومع ذلك ، من أجل تفضيل المشكلات الأكثر منطقية والأكثر احتمالية ، لا ينبغي لهم الحصول على مزيد من الاهتمام لذلك ، لا توجد طريقة لدراسة المستوى "الفعلي" للمخاطر الإلكترونية بأي طريقة سليمة لأنها موجودة فقط في وعبر تمثيلات مختلف الجهات الفاعلة في المجال السياسي.

المراجع:

Daniel, Schatz, Julie, Wall, (2017). "Towards a More Representative Definition of Cyber Security". Journal of Digital Forensics, Security and Law. 12 (2). ISSN 1558-7215. Archived from the original on 28 December 2017.

Rouse, Margaret. "Social engineering definition". Tech Target. Archived from the original on 5 January 2018. Retrieved 6 September 2015.

Schatz, Daniel; Bashroush, Rabih; Wall, Julie (2017). "Towards a More Representative Definition of Cyber Security". Journal of Digital Forensics, Security and Law. 12 (2). ISSN 1558-7215.

Reliance spells the end of the road for ICT amateurs", 7 May 2013, The Australian

Stevens, Tim. "Global Cyber security: New Directions in Theory and Methods". Politics and Governance. 6 (2). doi:10.17645/page. v6i2.1569.

"Computer Security and Mobile Security Challenges". researchgate.net. Archived from the original on 12 October 2016. Retrieved 4 August 2016.

"Distributed Denial of Service Attack". csa.gov.sg. Archived from the original on 6 August 2016. Retrieved 12 November 2014.

Wireless mouse leave billions at risk of computer hack: cyber security firm Archived 3 April 2016 at the Way Back Machine.

"Multi-Vector Attacks Demand Multi-Vector Protection". MSSP Alert. July 24, 2018.

Millman, Renee (December 15, 2017). "New polymorphic malware evades three-quarters of AV scanners". SC Magazine UK.

Turner, Rik (May 22, 2018). "Thinking about cyber attacks in generations can help focus enterprise security plans". Informa PLC. Ovum.

"Identifying Phishing Attempts". Case. Archived from the original on 13 September 2015.

Arcos Sergio. "Social Engineering" (PDF). Archived (PDF) from the original on 3 December 2013.

Scannell, Kara (24 February 2016). "CEO email scam costs companies $2bn". Financial Times (25 Feb 2016). Archived from the original on 23 June 2016. Retrieved 7 May 2016.

"Bucks leak tax info of players, employees as a result of email scam". Associated Press. 20 May 2016. Archived from the original on 20 May 2016. Retrieved 20 May 2016.

What is Spoofing? – Definition from Techopedia". Archived from the original on 30 June 2016.

spoofing". Oxford Reference. Retrieved 8 October 2017.

Marcel, Sébastien; Nixon, Mark; Li, Stan, eds. (2014). Handbook of Biometric Anti-Spoofing: Trusted Biometrics under Spoofing Attacks (PDF). London: Springer. doi:10.1007/978-1-4471-6524-8. ISBN 978-1-4471-6524-8. ISSN 2191-6594. LCCN 2014942635. Retrieved 8 October 2017 – via Penn State University Libraries.

Abstract:

Cyber security are techniques generally provided for in published materials that attempt to protect the cyber environment of a user or organization. Manages the set of technologies used to keep networks, programs, and data safe from unauthorized access. It refers to the set of technologies and processes, and may also be referred to as IT security. This field is becoming increasingly important due to the increasing reliance on computer systems, including smartphones, televisions, and the various small devices that make up the Internet of Things.