الأكاديمية العربية الدولية
Arab International Academy

إسم المادة :أساسيات الأمن السيبراني

إسم المدرس : محمد ماهر محمد سهلي

الأكاديمية العربية الدولية – منصة أعد

الأكاديمية العربية الدولية
Arab International Academy

محاور المحاضرة :

- مقدمة في الأمن السيبراني
- المقصود بأمن السيبراني
- أهمية الأمن السيبراني
- أساسيات الأمن السيبراني
- مجالات الأمن السيبراني
- أنواع الأمن السيبراني
- خصائص الأمن السيبراني
- أنواع تهديدات الأمن السيبراني -
- ما المقصود بالهجوم السيبراني
- الجريمة السيبرانية ونماذج التهديد
- ما هي هجمات DDOS
- طبيعة التهديدات
- اختراق البرامج الضارة
- الجمع بين الهندسة الاجتماعية و تقنيات البرامج الضارة
- المقصود بالجريمة الالكترونية وطرق الحماية منها و أهم منتجات الحماية

مقدمة في الأمن السيبراني

نظراً لأن حياتنا اليومية أصبحت أكثر اعتمادًا على الأدوات والخدمات المستندة إلى الإنترنت، وبما أن هذه المنصات تتراكم أكثر من بياناتنا الأكثر حساسية، فإن الطلب يزداد للخبراء في مجال الأمن السيبراني.

في هذا المساق، سوف تحصل على لمحة عامة عن مشهد الأمن السيبراني وكذلك وجهات النظر الدولية في هذا المجال. سنغطي البيئة القانونية التي تؤثر على الأمن السيبراني . ويعتبر هذا المساق بمثابة مقدمة لمجال الأمن السيبراني المثير.

مقدمة في الأمن السيبراني

يشتمل المساق على العديد من المواضيع الأساسية في الأمن السيبراني وسنتحدث عن مدخل تاريخي للأمن السيبراني اضافة الى أمن المعلومات والأطر العالمية لأمن المعلومات كما سنتطرق للتحدث عن الهياكل التنظيمية للأمن السيبراني، وتعد الجرائم الإلكترونية من أكثر المواضيع انتشار في وقتنا الحالي.

و مع التقدم التكنولوجي في شتى المجالات، زادت عمليات الاختراق والسرقة، مما دفع المبرمجين لوضع

الاستراتيجيات التي تحمي الأنظمة والشبكات من الهجمات الرقمية، وبعد مراحل كثيرة من التطور

جاء مفهوم الأمن السيبراني

ما المقصود بالأمن السيبراني Cyber security؟

يعرف الأمن السيبراني بكونه مجال من مجالات تكنولوجيا المعلومات والذي يعرف أيضًا باسم أمن المعلومات **Cyber security**، وفيه يتم حماية الأفراد والمؤسسات والأنظمة من حالات الاختراق الرقمي أو الدخول الغير مصرح به أو التهديدات الأمنية الخطيرة، والتي قد تؤثر على خصوصية البيانات والمعلومات لاسيما الحساسة منها وكذلك إدارة عملية الإنتاج ذاتها، خاصة إن الصناعات بمختلف أنواعها الآن أصبحت مرتبطة ارتباطًا وثيقًا بالتكنولوجيا.

الهدف الأساسي وراء ظهور الامن السيبراني هو ظهور ما يعرف بالهجمات الرقمية الخطرة أو الفيروسات المنيعة وفيها يتم الهجوم على الأنظمة الرقمية الخاصة بالأفراد أو المنشأة والسيطرة على ما تمتلكه من بيانات حساسة، وخضوعها لعمليات الابتزاز والسرقة وكذلك التخريب المتعمد للمعلومات

أهمية الأمن السيبراني

يعد الأمن السيبراني مهماً بسبب ارتفاع التكلفة المالية المخصصة لصد الهجمات الإلكترونية بمختلف أنواعها، حيث يعد متوسط الميزانية التي تم إنفاقها في صد الهجمات بـ 17 مليون دولار.

يوجد أكثر من 21.1 مليار جهاز مرتبط بالإنترنت حول العالم، أي ما يعادل 21.1 مليار هجمة محتملة في عالم الفضاء الإلكتروني وهو بدوره ما يمكن أن يحدث لولا الأمن السيبراني وتطوراته الحيوية التي تحدث بشكل متتابع ومتسارع في وقتنا الحالي.

تكمن أهمية الأمن السيبراني في كونه يحافظ على حساسية وأمان المعلومات الخاصة بالمستخدمين ولاسيما التي قد تعرض الأشخاص للخطر أو الدول التى يقيمون فيها، وذلك لأن أي معلومة قد تكون هامشية أو غير مهمة بالنسبة لبعض الأفراد قد تكون هي حلقة الوصل التي يحتاجها المخترق للقيام بعمله.

لذلك يرتبط مجال الأمن السيبراني Cyber security بأربع مفاهيم أساسية

1- الجريمة السيبرانية Cyber Crime

2- الهجمات السيبرانية Cyber attacks

3- الردع السيبراني Cyber deterrence

4- الفضاء السيبراني Cyber Space

أساسيات الأمن السيبراني

اساسيات الامن السيبراني هي المبادئ والتدابير التي تهدف الى حماية الأنظمة و الشبكات الرقمية من التهديدات السيبرانية وتشمل الأساسيات ما يلي:

1- الوعي و التثقيف

2- ادارة الهوية و الوصول

3- التشفير والتعتيم

4- حماية الشبكات والنظم

5- الكشف عن التهديدات والاستجابة

أساسيات الأمن السيبراني

6- التوعية بسياسة الأمن السيبراني

7- احترام الخصوصية والامتثال

8- النسخ الاحتياطي واستعادة البيانات

هذه هي بعض الأساسيات الرئيسية للأمن السيبراني وهناك العديد من المبادئ والتدابير الأخرى التي يمكن أن تكون جزءاً من استراتيجية الأمن السيبراني بناءاً على متطلبات كل منظمة أو نظام.

تتنوع مجالات العمل ما بين:

1- أمن التطبيقات

2- الأمان السحابي

3- الأمان المالي في التعاملات المالية

4- الأمان في البيئة التحتية الحرجة للنظام

5- أمان المعلومات والبيانات

6- أمان الشبكات

7- الأمان التشغيلي

8- الوعي الأمني للمستخدم النهائي

9- التعافي من الكوارث ولاسيما المتعلقة بالهجمات الإلكترونية أو الأسباب الطبيعية

أنواع الأمن السيبراني

1- أمن الشبكات:

أغلب الهجمات التي تحدث تكون عبر الشبكات الإلكترونية، لذلك تم وضع أنظمة أمنية تعمل كصمام أمان للشبكة

2- الأمن السحابي:

نظرًا لكون التوجهات الغالبة الآن لمعظم المؤسسات حول العالم هي استخدامها لتكنولوجيا الذكاء الاصطناعي والسحابات التخزينية

3- أمن التطبيقات:

تطبيقات الويب مثل أي شيء آخر متصل مباشرة بشبكات الإنترنت، وبالتالي فمن المنطقي أنها تكون مهددة بالهجمات على أمنها السيبراني

الأمن السيبراني

4- أمن إنترنت الأشياء:

رغم أن استخدام أجهزة إنترنت الأشياء (مثل الأجهزة الذكية وأدوات الذكاء الاصطناعي والمستشعرات الحساسة عبر شبكة عالمية واحدة) يوفر العديد من الفوائد الإنتاجية

5- أمن المستخدم النهائي:

أمان النقاط النهائية تكون عبارة عن مجموعة من الممارسات التقنية تُستخدم في حماية أجهزة المستخدمين النهائيين من الهجمات السيبرانية التي يكون مصدرها البرامج الضارة والغير مرغوب فيها.

6- أمن البنية التحتية:

يتم تعريف أمان البنية التحتية للمؤسسات بأنه إجراء أمني يقوم على أساس حماية البنية التحتية الحيوية للنظام والحد من نقاط الضعف في هذه الأنظمة من فساد وتخريب .

أنواع الأمن السيبراني

7- التعافي من حالات الكوارث المتعلقة بالهجمات الإلكترونية أو الأسباب الطبيعية :

التعافي من حالات الكوارث أو استمرارية العمل في ظروف التعافي من الهجمات الإلكترونية

8 -أمن المعلومات و البيانات :

أمن المعلومات هو عملية تصميم ونشر الأدوات الخاصة بحماية معلومات عملك الهامة من التدمير أو التعطيل أو التغيير، فهو العامل الحاسم في تأمين الأمن السيبراني.

9- الأمان المالي :

يظن البعض أن الأمن السيبراني وأمن البيانات غير مرتبطين بالدورة المحاسبية، ولكن بسبب تهديدات القرصنة على البيانات المالية الخاصة بالشركة .

خصائص الأمن السيبراني

للأمن السيبراني مجموعة من الخصائص التي تميزه عن غيره من المجالات، أهمها هم:

1- الثقة وعدم الثقة:

يمتلك جدار الحماية الخاص بنظام الأمن السيبراني بما يشبه مرشح إلكتروني لنوع وطبيعة البرامج والتقنيات المسموح بتفعيلها

2- الحماية من التهديدات الداخلية:

واحدة من أهم خصائص الأمن السيبراني هو حماية الجهاز من التهديدات الداخلية والتي قد تتم بناء على قلة ثقافة المستخدم أو جهله بمجال أمن المعلومات وفيه قد يقوم بالسماح ببرامج مجهولة المصدر.

خصائص الأمن السيبراني

3- الحماية من التهديدات الخارجية:

تمثل خاصية الحماية من التهديدات الخارجية أهم صفات الأمن السيبراني، حيث يتم فيها بناء جدار الحماية قادر على تصفية المخاطر الخارجية التي يسفر عنها التعامل مع العالم الرقمي .

4- رؤية شاملة:

تقوم الادوات الخاصة بالأمن السيبراني على منح مستخدميها أفراد كان أو شركات أو رؤية شاملة على ما يحتويه أنظمتهم من نقاط قوة وضعف

5- مراقبة مستمرة:

يقوم الأمن السيبراني على خاصية المراقبة المستمرة، حيث لا تقوم جدار الحماية الخاص به بالعمل لمرة واحدة أو في ساعات معينة .

خصائص الأمن السيبراني

6- الامتثال للسياسات والقوانين:

الهدف من الأمن السيبراني في المقام الأول هو الحفاظ على سرية وخصوصية البيانات والمعلومات، بالإضافة إلى مكافحة الفيروسات الضارة بجميع أنواعها

لذلك تعد خاصية الامتثال للقوانين والسياسات التشريعية الخاصة بأمن المعلومات واحدة من أهم خصائص الأمن السيبراني.

7- التنوع:

يجب أن يمتلك النظام الخاص بالأمن السيبراني حلول مجمعة تتعلق بالتعامل مع التهديدات السيبرانية .

ما المقصود بالهجوم السيبراني؟

يعد الهجوم السيبراني واحدًا من أحدث أنواع الأخطار الرقمية التى تواجه الإنسان في وقتنا الحالي، وفيه يتعرض الشخص أو الجهة أو المؤسسة أو حتى الدولة إلى هجمات إلكترونية الغرض منها تعطيل أو تدمير أو الدخول الغير مصرح إلى بيانات ذات قيمة أو حساسة للجهة أو الطرف الذي يتعرض للهجوم.

قد تحدث الهجمات الإلكترونية للأشخاص لا بسبب قيمة البيانات أو المعلومات التى يمتلكونها، ولكن بسبب كونهم حلقة وصل بين أطراف أخرى ذات قيمة يصعب الوصول إليهم، أو كونهم يمتلكون صلاحية للوصول إلى أجهزة وتقنيات يصعب اختراقها بطريقة مباشرة، وهو ذاته ما حدث لإحدى العيادات الجامعية في ألمانيا عندما تم اختراق نظامها بشكل كامل بسبب وجود ثغرة تكنولوجية في إحدى أجهزتها المستخدمة.

أنواع التهديدات في الأمن السيبراني

بعد التعرف على كل من مفهوم وخصائص الأمن السيبراني، يأتي الدور الآن لإلقاء الضوء على أشهر أنواع التهديدات فيه، والتي تمثل أكبر آفة يتعامل معها العالم الرقمي، والتي غالبًا ما تتسبب في خسائر فادحة يصعب التعامل معها، ودور الأمن السيبراني هنا ألا يقوم بالدفاع ضد هجماتها فحسب، بل أن يقوم بمنع حدوثها من الأساس كالآتي:

1- البرمجيات الخبيثة:

البرمجيات الخبيثة هي فيروسات متقدمة يتم تصميمها بهدف الالتفاف عن أنظمة الحماية المثبتة.

2- فيروس الفدية الخبيث:

يعد فيروس الفدية الخبيث واحد من أخطر الهجمات الإلكترونية في عالمنا الرقمي الحالي والتي طبقاً للإحصائيات العالمية الأخيرة فإن هناك هجوم من نوع الفدية الخبيث تقريبًا كل 10 ثواني على الأقل

أنواع التهديدات

3- التصيد للمعلومات:

فيها يتم استغلال قلة ثقافة الضحية الإلكترونية أو عدم انتباه لما يعرض أمامه من معلومات، وجعله يشارك بمحض إرادته معلومات حساسة خاصة ببطاقته الائتمانية أو معلومات سرية لا يجب مشاركتها مع العوام ككلمة السر الخاصة

4- استغلال البرامج الثنائية أو ما يعرف بهجوم الوسيط:

يعد هجوم الوسيط واحد من الأدوات الشائعة المستخدمة في عمليات الهجمات السيبرانية، وفيها يستغل المهاجم لجوء الضحية إلى مصدر تقني ثاني ضعيف الحماية .

5- التصيد المباشر أو ما يعرف بالتصيد بالرمح:

وفيه يتم استهداف فرد أو مؤسسة بحد ذاتها، والعمل على دراسة كل أنظمة الدفاع والحماية الخاصة بها بالتفصيل، ثم العمل على اكتشاف الثغرات التي يحتويها النظام وآلية تطويعها لصالح عملية اختراق وسيطرة ممنهجة.

ما المقصود بالهجوم السيبراني؟

6- التسلسل المتقدم طويل الأمد:

وفيها يتم اختراق أنظمة الحماية بشكل خفي وتدريجي، بحيث لا يتم اكتشافه إلا بعد مرور فترة زمنية طويلة، والتي من خلالها يكون الضرر قد تم بالفعل وتمت السيطرة الكلية على النظام بنجاح.

7- هجمات رفض الخدمة:

وفيها يتم إمطار النظام بوابل من حركات المرور والرسائل والمستخدمين الوهميين، بحيث ينشأ نوع من الضغط على الخوادم وتعطيلها أو التسبب في بطئها.

الجريمة السيبرانية

وتقوم الجريمة السيبرانية في الأساس على مجموعة من الهجمات المنظمة والتي يتم فيها التلاعب بالنظام الرقمي الخاص بالضحية والسيطرة التامة عليه فيما يعرف باسم الهجمات السيبرانية، ولكى يتم حماية الضحية من هذه الهجمات، يجب أن يتم وضع ما يعرف باسم الدرع السيبراني.

يعرف الدرع السيبراني بكونه جدار حماية فعال، يتم تفعليه على النظام الرقمي، بهدف سرعة اكتشاف أي ثغرة يمكن أن تمنح الفرصة لهجوم سيبراني خطير، حتى يتمكن الشخص أو المؤسسة في النهاية إلى التصفح في العالم الرقمي بحرية دون خوف من استغلال معلوماته أو التجسس عليه وهو ما يعرف بحرية التجول في الفضاء السيبراني.

نموذج لتهديد سيبراني أدى إلى الوفاة

في خريف 2020، تمكن فيروس الفدية الشهير من السيطرة على النظام التكنولوجي المتحكم في عيادة جامعية في ألمانيا، وعندما عان الدكاترة والأطباء من التواصل مع بعضهم البعض أو معرفة تاريخ سجلات المرضى يتعاملوا معهم بالطريقة الصحيحة، لاقت امرأة ما حتفها.

هذه الحادثة تمت بسبب اضطرار الممرضين بنقلها إلى مكان آخر جراء عدم توافر دكاترة كافية لتغطية التعامل مع هذه الأزمة. وهو ما أدى بدوره إلى تدهور الحالة ووفاتها، وكل هذا بسبب إهمال في أساليب الحماية الرقمية الخاصة بأنظمة العيادة، بالإضافة إلى جهل الضحايا بالثقافة التكنولوجية المطلوبة.

إذن عندما يخبرك خبير تقني أن البيانات التي تمتلكها يجب حمايتها بكل الصور، وتهز أنت رأسك دون اكتراث معللاً نك لست برئيس وزراء أو شخصية هامة لكل هذا التحفظ، فلا تستعجب أن تكون أنت طرفًا وسيطًا لعملية قتل إلكترونية أخرى أو وسيلة سهلة لابتزاز شخصًا ما أو السيطرة على امواله او السيطرة على حياتك أنت شخصيًا.

في النهاية، عالم الأمن السيبراني كبير ومليء بالتهديدات المختلفة، ومهما نجح مختصو الحماية من تجديد الدفاعات وعلاج الثغرات التقنية، إلا إن أكبر نقاط الضعف تتمثل في الاعتماد على الثغرة البشرية، وهي نقطة لن يتم حلها إلا بالتثقيف التكنولوجي المستمر المتمثل في ثقافة حماية المعلومات، فإذا كنت تخشى أن تكون ضحية جديدة من ضحايا اختراق الأمن السيبراني، فيجب عليك البدء في تثقيف نفسك من الآن .

ما هي هجمات DDoS

تتضمن الأهداف الاعتيادية لهجمات DDos

مواقع التسوق عبر الإنترنت

الملاهي عبر الإنترنت

أي شركة أو مؤسسة تعتمد على توفير الخدمات عبر الإنترنت

كيف يعمل هجوم DDoS

ضع موارد الشبكة، مثل خوادم الويب، لحدود معينة لجهة عدد الطلبات التي يمكن خدمتها في آن واحد. وبالإضافة إلى حدود قدرة الخادم، سيكون للقناة التي تربط الخادم بالإنترنت نطاق تردد / قدرة محدودة أيضًا. ومتى تجاوز عدد الطلبات حدود قدرة أي مكون من مكونات البنية التحتية، من المحتمل أن يتراجع مستوى الخدمة كما يلي:

- ستكون الاستجابة للطلبات أبطأ بكثير من المعتاد.
- سيتم تجاهل بعض، أو كل، طلبات المستخدمين تمامًا.

عادة ما يكون الهدف الأقصى للمتطفل هو منع العمل الطبيعي لمورد ويب تمامًا، أي "حجب الخدمة" تمامًا. وقد يطلب المتطفل أيضًا المال مقابل إيقاف الهجوم. وفي بعض الحالات قد يكون هجوم DDoS بهدف محاولة تشويه سمعة أعمال أحد المنافسين أو الإضرار بها.

اليوم طبيعة تهديدات

في الفترة من أوائل الألفينيات إلى منتصفها، كان هذا النوع من النشاط الإجرامي شائعًا جدًا. ومع ذلك، انخفض عدد الهجمات ، ومن المحتمل ان الزيادة في تراجع الهجمات ما يلي :

1- تحقيقات الشرطة التي أدت إلى اعتقال المجرمين في جميع أنحاء العالم.

2- الإجراءات المضادة الفنية التي كانت ناجحة في مواجهة الهجمات .

كيفية اختراق البرامج الضارة للحواسيب وأنظمة تكنولوجيا المعلومات

بالنسبة للكثير من منشئي فيروسات الحاسوب والمجرمين الإلكترونيين، الهدف هو توزيع الفيروس أو الفيروس المتنقل أو فيروس حصان طروادة على أكبر عدد ممكن من الحواسيب أو الهواتف المحمولة - بحيث يمكنهم زيادة اختراق البرامج الضارة إلى أقصى درجة. وهناك ثلاث طرق أساسية لتحقيق ذلك عن طريق :

اصابة النظام دون علم المستخدم

الهندسة الإجتماعية

بالإضافة إلى ذلك غالبًا ما يتخذ منشئو البرامج الضارة خطوات لمنع اكتشاف الاصابة بواسطة برامج مكافحة الفيروسات.

الجمع بين الهندسة الاجتماعية وتقنيات تطبيق البرامج الضارة

تساعد أساليب الهندسة الاجتماعية بما فيها هجمات التصيد الاحتيالي على جذب انتباه الضحايا المستهدفة.

تزيد البرامج الضارة من احتمالية اختراق العنصر المصاب لحاسوب الضحية.

من الأمثلة على ذلك:

Mimail

كان هذا أحد الفيروسات المتنقلة الأولى التي تم تصميمها لسرقة البيانات الشخصية من حسابات المستخدمين عبر الإنترنت. تم توزيع الفيروس المتنقل كمرفق بريد إلكتروني.

ما هو المقصود بالجريمة الإلكترونية

لعل أخطر انواع منشئي البرامج الضارة هم المتطفلون ومجموعات المتطفلين الذين ينشئون البرامج الضارة سعيًا إلى تحقيق أهدافهم الإجرامية. يقوم هؤلاء المجرمون الإلكترونيون بإنشاء فيروسات الحاسوب وبرامج أحصنة طروادة التي يمكنها :

سرقة رموز الوصول إلى الحسابات المصرفية

الإعلان عن منتجات أو خدمات على حاسوب الضحية

استخدام موارد الحاسوب المصاب بشكل غير قانوني، لتطوير وتشغيل حملات البريد الإلكتروني العشوائي

كيف تحمي نفسك من الجرائم على الإنترنت

مع استخدام المجرمين الإلكترونيين العديد من التقنيات لمهاجمة حواسيب المستخدمين وبياناتهم، أصبحت الحماية المتعددة الطبقات أمرًا لا غنى عنه. وبإمكان حلول الحماية من البرامج الضارة التي تضم تقنيات الكشف المستند إلى التوقيع والتحليل التجريبي الاستباقي والحماية السحابية تقديم المزيد من الحماية لأجهزتك وبياناتك من التهديدات الجديدة والمعقدة.

منتجات الحماية

تشتهر

Kaspersky Lab

بمنتجات الحماية من البرامج الضارة المتعددة الطبقات ذات المستوى العالمي التي يمكنها حماية مجموعة من الحواسيب والأجهزة من الجرائم على الإنترنت، ومنها:

الحواسيب الشخصية التي تعمل بنظام الويندوز

حواسيبlinux

أجهزة Apple Mac

الهواتف الذكية

الأجهزة اللوحية

نصائح لتحقيق الأمن السيبراني لك ولشركتك 10

1- إعطاء الأولوية للأمن السيبراني

2- لا تهمل حماية بيانات وخصوصية عملائك

3- اتباع سياسة حماية صحية ومناسبة

4- كلمات السر ليست كافية

نصائح لتحقيق الأمن السيبراني لك ولشركتك 10

5- لا تثق بأحد

6- احذر من الرسائل الخادعة للدعم الفني

7- إعطاء الأولوية لأمن شبكات الجيل الخامس

8- العمل عن بعد ومتطلبات الحماية

نصائح لتحقيق الأمن السيبراني لك ولشركتك 10

بناء علاقات أوثق بين المطورين وفريق الأمن السيبراني - 9

الاستعانة بمصادر خارجية للأمن السيبراني -10

أنواع جدران الحماية

- جدار فلترة الحُزم
- الجدار الناري من الجيل التالي
- جدار البروكسي
- جدران ترجمة عناوين الشبكة
- الجدار الناري متعدد الطبقات

شكراً لكم