تقنيات التعليم للجميع
مبادرة تطوعية؛ لمجتمع متعلم ذاتيا.
https://edutec4all.medu.sa

الشريك الاستراتيجي

جمعية الأنظمة التقنية
Association of Technology Systems
تحت إشراف وزارة الموارد البشرية و التنمية الإجتماعية
بترخيص رقم : ٢٠٩٨

أميـــره عبد الرحمن غـــوص
ماجستير تقنيات التعليم
مدرب وخبير مايكروسفت

IntSec

الأمن السيبراني
Cyber Security

IntSec

المقدمة

بعد الانتشار الكبير للإنترنت والأجهزة الذكية والأجهزة المحمولة، أصبح من الضروري في وقتنا الحالي الانتباه للأمن السيبراني وكيفية حماية أنفسنا في الفضاء الرقمي، ابتداء من المنزل إلى العمل وعلى مستوى الدولة ككل، ويعد الأمن السيبراني من أكثر المواضيع إنتشاراً في أيامنا هذه وتعلّمه أصبح ضرورة لابد منها أطلقت العديد من المبادرات والتشريعات لتعزيز هذا النوع من الأمن من خلال قيام المملكة العربية السعودية بتأسيس العديد من الهيئات الحكومية منها:

الهيئة الوطنية للأمن السيبراني بأمر ملكي رقم 6801 بتاريخ 11 /2 /1439 هـ الموافق 31 أكتوبر 2017 ويهدف عمل الهيئة إلى: تعزيز الأمن السيبراني للدولة واستقطاب الكوادر الوطنية وتأهيلها وتحفيز الابتكار والاستثمار في مجال الأمن السيبراني والاتحاد السعودي للأمن السيبراني والبرمجة والدرونز حيث يهدف الاتحاد إلى تطوير البرمجيات وحماية الشبكات وأنظمة تقنية المعلومات والأنظمة التشغيلية بالإضافة للائحة نظام مكافحة الجرائم المعلوماتية وتمت المصادقة عليه بموجب مرسوم ملكي توضح فيها الجرائم والعقوبات لمرتكب الجرائم المعلوماتية وذلك من أجل تحقيق الأمن المعلوماتي وحفظ الحقوق المترتبة على إستخدام المشروع للحاسبات الآليه والشبكات المعلوماتية، وحماية المصلحة العامة والأخلاق والآداب العامة ،كما أنشأت المملكة المركز الوطني الإرشادي لأمن المعلومات Certsa من أجل الحصول على دعم تقني لكيفية التعامل مع حوادث انتهاك أمن المعلومات

IntSec

مفهوم الأمن السيبراني وعناصره

حماية الحاسب الآلي والأجهزة الالكترونية المرتبطة بشبكة الأنترنت والمعلومات من أي تدخل غير مقصود أو غير مصرح به أو سرقتها أو تسريبها ومنع سوء الاستغلال واستعادة المعلومات الالكترونية التي تحتويها .

IntSec

مفهوم الأمن السيبراني وعناصره

عناصر الآمن السيبراني

السرية

أن تكون المعلومات الخاصة بالمؤسسة متاحة فقط للأشخاص المسموح لهم الاطلاع عليها ومنع وصول الأخرين الغير مصرح لهم مع تحديد صلاحية التعديل والحذف والاضافة

السلامة

أن تكون المعلومات صحيحة عند إدخالها حيث لن يتم تغيرها أو العبث بها أو تدميرها أو التلاعب بها

التوافر والاتاحة

أن تكون المعلومات متوفرة للمستخدم عند الحاجة إليها

IntSec

ماهية الامن السيبراني

بسبب الاستخدام المتزايد لشبكة الإنترنت والتطبيقات الخاصة بالتعليم عن بعد والتعاملات المالية والتسوق عبر الإنترنت وتطبيقات التواصل الاجتماعي والمكتبات الرقمية والألعاب الالكترونية عبر شبكة الإنترنت من قبل شرائح عمرية مختلفة بهدف تحقيق المتعة والتعبير عن الأفكار ومشاركة المعلومات مع الآخرين، فقد أصبح لا بد من توفر الوعي لدى جميع الأفراد بكيفية اتخاذ الإجراءات والاحتياطات اللازمة لحماية وسرية بياناتهم ومعلوماتهم عبر الشبكة من خلال التعرف على الاستخدامات الصحيحة والخاطئة للإنترنت؛ وأن الوجوه المتعددة للجرائم السيبرانية العربية السعودية ليست بمنأى عن التأثيرات العالمية حيث تعتمد هذه الخدمات على وجود كم كبير من المعلومات والتي يجب أن تحاط بسرية تامة وتحفظ بشكل يمنع وصول الغير المصرح لهم ، والأمن السيبراني هو التقنية المستخدمة لحماية أجهزة الكمبيوتر والشبكات من التطفل الإجرامي.

والآثار المترتبة لا تقف على حدود الأفراد والمؤسسات، بل تتعداها الى الدول والحكومات والمملكة العربية السعودية

IntSec

أهداف الأمن السيبراني

IntSec

الأمن السيبراني و أمن المعلومات

يعتبر مفهوم الأمن السيبراني وأمن المعلومات مصطلحان متشابهان إلا أن هناك بعض الاختلافات الأساسية بينهما فالأمن السيبراني يهتم بتأمين وتخزين المعلومات الرقمية والورقية وتبادلها بطريقة آمنة .

IntSec

وهناك اختلاف في وجهات النظر حول ايهما أعم وأشمل الأمن السيبراني أم أمن المعلومات؟

يعتبر أمن المعلومات أعم وأشمل في حفظ البيانات الورقية والرقمية والالكترونية، ولكن يتضمن الأمن السيبراني حماية شبكة الانترنت والأجهزة وحماية انترنت الأشياء وتشمل الأجهزة المنزلية وكاميرات المراقبة التي تعمل على شبكة الإنترنت

IntSec

هناك بعض الأعراض التي يمكن أن تظهر على الجهاز حتى يتم التعرف على وجود هجوم من أحد البرمجيات الخبيثة عليه مثل ما يلي:

ظهور تنبيهات من برنامج مكافحة الفيروسات

إرسال إيميلات عشوائية لأصدقائك ومعارفك لم تقم بإرسالها

كثرة ظهور إعلانات والنوافذ المنبثقة في متصفح الانترنت

عرض اعلانات غير لائقة أو تداخل إعلانات مع محتوى الصفحة

IntSec

هناك بعض الأعراض التي يمكن أن تظهر على الجهاز حتى يتم التعرف على وجود هجوم من أحد البرمجيات الخبيثة عليه مثل ما يلي:

- بطء النظام أو تعطله أو عرض رسائل خطأ متكررة .
- يمنع الطالب من إزالة البرامج الغير مرغوب فيها
- تظهر اشرطة جديدة أو أيقونا جديدة على سطح المكتب
- عرض صفحات ويب لم تقم بزيارتها
- حدوث تغيير مفاجئ أو متكرر في صفحة الانترنت

IntSec

البرمجيات الخبيثة

يتعرض الانسان للعدوى فيصاب بالمرض كذلك الأجهزة تصاب بالعدوى من خلال البرامج التالية :

فيروسات: هي عبارة عن برامج مشابهة للفيروس البشري حيث يقوم بنسخ نفسه والانتقال من جهاز إلى جهاز آخر عن طريق استخدام وسائط التخزين (فلاش ميموري) يحتوي على الفيروسات مثل فيروس الاختصارات لدى يجب فحصه بمكافح الفيروسات.

دودة: سميت بذلك لأنها قادرة على نسخ نفسها والانتشار سريعاً حيث تطلب من المستخدم فتح الملف المرفق بالرسالة في البريد الالكتروني فتعمل بعد ذلك على إتلاف البرامج والملفات وأنظمة التشغيل وتقوم بإرسال نسخ منها إلى جميع المضافين في القائمة البريدية.

البرمجيات الخبيثة

حصان طراودة : هوعبارة عن ملف مرفق عند تنزيل إحدى البرامج من المواقع الغير الرسمية ويقوم بإضعاف برامج الحماية في الحاسوب حتى يسهل اختراقه وسرقة البيانات وكشف كلمات المرور وعلى عكس الدودة لا يقوم بنسخ نفسه ، ولكن يفتح منافذ لبرامج أخرى خبيثة .

برمجيات الدعاية والاعلان: هي برمجيات تعمل على إظهار نوافذ منبثقة و إعلانات للمستخدمين تحدث عند تثبيت برامج من المواقع وسيطة أو غير موثوقة في الانترنت.

IntSec

اثراء

حصان طروادة
جاء هذا المصطلح لما حاصر الاغريق
مدينة طروادة لمدة عشر سنوات ففكر
الاغريق بحيلة للاستلاء على المدينة
فتظاهر جزء من الجيش بالانسحاب
ومغادرة المدينة تاركين هدية
للطرواديين عبارة عن حصان خشبي
عملاق خارج أسوار المدينة
ففرح الطراوديون لمغادرة الاغريق وتم
سحب الحصان الى داخل أسوار المدينة
في وسط احتفال كبير
كان داخل الحصان عدد من جنود الاغريق
الذين تسللوا إلى داخل المدينة عند
حلول الظلام وفتحوا البوابات للسماح
لبقية الجيش بدخول المدينة فنهبت
المدينة وقتل الرجال، وانتصر الإغريق
بالخدعة.
ومن هنا جاء مصطلح حصان طروادة

IntSec

كيف تحمي نفسك في الفضاء السيبراني؟

Cyber Security

IntSec

ثانيا: التحديثات

تثبيت نسخة محسنة وجديدة من البرنامج في الإصدار الأول لاي نظام تشغيل

ثالثا: تهديدات البريد الالكتروني:

يحتوي البريد على مرفقات مدموج ببرامج ضارة تؤدي الى الاضرار بجهازك
لذا يجب ارسال هذا النوع من الرسائل الى البريد الغير مرغوب به لمنعه من الوصول الي صندوق البريد

رابعا: تنصـــيب وتحديث برامج الحماية ومكافحة الفيروسات بشكل دوري مثل:

برنامج يكشف ويمنع البرامج الضارة والاعلانات المنبثقة مثل
anti-virus - ads block

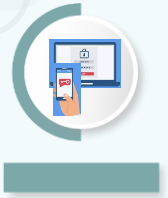
خامسا: الموثوقية

استخدام مواقع انترنت آمنة حيث يجب أن تبدأ
(https)

سادسا: احتفظ بنسخة من الملفات الهامة

حفظ نسخة احتياطية من الملفات في مكان آمن
مثل وسائط التخزين أو الاقراص المدمجة

IntSec



سابعا: المصادقة الثنائية

تعني المصادقة الثنائية لتأمين الحسابات من خلال تزويد المستخدم في كل مرة بعدد من الرموز ترسل نصياً إلى هاتفه

ثامنا: حذف التطبيقات عند الانتهاء منها

تاسعا: الحرص على وضع كلمات مرور على الشبكة اللاسلكية المنزلية

المراجع:

البار، عدنان مصطفى والسميري، عيسى رفاعي.(٢٠١٩).*أساسيات الأمن السيراني*.جدة.

أحمد، شاذلي صديق محمد، وأحمد، عوض حاج علي.(٢٠١٥). اكتشاف هجوم التصيد الإلكتروني لاستخدام خوارزمية تحسين الحد الأدنى التسلسلية. *مجلة الدراسات العليا: جامعة النيلين-كلية الدراسات العليا*، مج ٣

الدين، أسامة حسام.(٢٠١٧). مقدمة في الأمن السيبراني.

الربيعة، صالح. (٢٠١٩).الأمن الرقمي وحماية المستخدم من مخاطر الانترنت، هيئة الاتصالات وتقنية المعلومات، المملكة العربية السعودية: الرياض.