Tema 1

Monday, September 3, 2018 6:53 PM

Lo primero de debemos de saber y aclarar es que nada es completamente seguro, toda infraestructura puede verse afectada por un incidente de seguridad.

Muchas personal tienen la falsa creencia que existen sistemas infalibles, pero la realidad es que dicha impenetrabilidad de los sistemas no existe. Si les preguntara cuales empresas tienen los sistemas o infraestructura más seguras del planeta, muchos me dirán que los Bancos, las telefónicas o inclusos los casinos. La realidad es que ellos son los que más controles de seguridad aplican, pero los riesgos aunque sean mitigados por un control no desaparecen, lo único que se hace es disminuir la probabilIdad de Zaque ocurra.

Banco

Nacional

Sábado 09 junio de 2018 | Publicado a las 09:35 · Actualizado a las 20:52

Robaron US$10 millones en ataque informático al Banco de Chile: virus fue un distractor

Publicado por: Leonardo Casas

Recorte de pantalla realizado: 9/3/2018 7:49 PM
https://www.biobiochile.cl/noticias/nacional/chile/2018/06/09/robaron-us10-millones-en-ataque-informatico-al-banco-de-chile-virus-fue-un-distractor.shtml

Telefonica

SEGURIDAD

WannaCry, el ransomware del ataque a Telefónica

TWITTEAR COMPARTIR Javier Lacort - May 12, 2017 - 16:47 (CET)

Un mal viernes para la ciberseguridad que puede conseguir que salte más de una alerta en las empresas del país.

Recorte de pantalla realizado: 9/3/2018 7:51 PM
https://hipertextual.com/2017/05/wannacry-ransomware-ataque-telefonica

Casino

CH LO ÚLTIMO TECNOLOGÍA ENTRETENIMIENTO GAMING LIFE MOTOR INDUSTRIA PRODUCTOS

Home Noticias

Roban los datos de un casino a través del termómetro del acuario

Recorte de pantalla realizado: 9/3/2018 8:00 PM

https://computerhoy.com/noticias/software/roban-datos-casino-traves-del-termometro-del-acuario-79195

Todo el mundo

EL PAÍS INTERNACIONAL

EUROPA EE UU MÉXICO AMÉRICA LATINA ORIENTE PRÓXIMO ASIA ÁFRICA FOTOS OPINIÓN BLOGS TITULARES »

EE UU acusa al hacker norcoreano detrás del ciberataque 'WannaCry' y el de Sony

El Departamento de Justicia imputa a Pak Jin Kyok por los dos golpes informáticos que realizó "en nombre del Gobierno de Corea del Norte"

ANTONIA LABORDE

Washington - 6 SEP 2018 - 20:58 CEST

La fiscal federal asistente en Los Ángeles, Tracy Wilkison, anuncia los cargos contra el programador norcoreano Pak Jin

La fiscal federal asistente en Los Ángeles, Tracy Wilkison, anuncia los cargos contra el programador norcoreano Pak Jin Kyok. AFP

Estados Unidos finalmente dio con el cerebro detrás del mayor ataque de *ramsomware* de la historia. El Departamento de Justicia acusó este jueves al programador norcoreano Pak Jin Kyok y a la empresa Chosun Expo Joint Venture de los golpes informáticos del WannaCry en 2017 y el de Sony en 2014. El primero consistió en el cibersecuestro de casi 300.000 ordenadores en 170 países mediante un virus. El segundo, en la filtración de documentos internos y la

NEWSLETTERS
Recibe el boletín de Internacional

TE PUEDE INTERESAR

La Casa Blanca anuncia una segunda cumbre de Trump y Kim Jong-un

Los blogueros centrafricanos quieren unas redes sin odio

https://elpais.com/internacional/2018/09/06/actualidad/1536257762_840433.html

Ahora que se entiende que no hay ningún escenario perfecto, podemos pasar a algunos conceptos básicos de seguridad que pueden ayudar a construir una base sólida sobre una mitigación apropiada de los riesgos de seguridad.

Principio de Seguridad Informática

La seguridad informática tiene tres principios básicos que son la Confidencialidad, Integridad y Disponibilidad (CID).

Al emplear los conceptos de confidencialidad, integridad y disponibilidad de sus datos, una organización puede asegurar adecuadamente su hardware, software y comunicaciones.

Confidencialidad: este concepto se centra en prevenir la divulgación de información a personas no autorizadas. Como nuestra cedula, números telefónicos, resultados médicos, información de la licencia de conducir, cuentas bancarias y contraseñas, etc. Para las organizaciones esto puede incluir todo la información anterior, pero en realidad denota la confidencialidad de los datos.

Para que los datos sean confidenciales, la organización debe trabajar arduamente para asegurarse de que solo se puede acceder por personas autorizadas. Pasaremos una buena cantidad de tiempo discutiendo y mostrando cómo lograr esto. Por ejemplo, cuando usa un número de tarjeta de crédito en una tienda o en línea, el número debe ser cifrado con un cifrado fuerte para que el número de tarjeta no se vea comprometido.

El objetivo número uno de todo profesional de la seguridad es mantener la confidencialidad de los datos, mitigar las amenazas, subsanar las vulnerabilidades y reducir los riesgos.

Integridad: Esto significa que los datos no han sido manipulados. La autorización es necesario antes de que los datos puedan ser modificados de alguna manera; esto se hace para proteger el Integridad de los datos, Por ejemplo, si una persona borrara un archivo importante, por error o de forma malintencionada, se habrá violado la integridad de ese archivo. Debería asignar los permisos evitando que una persona elimine el archivo.

Consejo: Hay empresas que nunca eliminan datos, los permisos de eliminación de datos en muchas ocasiones están restringidos, para eliminar algún datos se lleva a cabo un proceso que integre varias personas y áreas. Además las auditorias en los sistemas deben generar alertas de los cambios.

Disponibilidad: La disponibilidad significa que los datos deben estar disponible para su uso sin importar la forma de almacenamiento, los recursos utilizados para acezar o los niveles de protección aplicados. También significa que los datos deben estar disponibles independientemente del ataque malicioso que podría ser perpetrado en él.

Autenticación: Es cuando la identidad de una persona se establece con la introducción de sus credenciales en un sistema. Por lo general, esto requiere una identidad digital de algún tipo, nombre de usuario / contraseña u otro esquema de autenticación.

Autorización: cuando un usuario tiene acceso a ciertos datos o áreas de un edificio.
La autorización ocurre después de la autenticación y se puede determinar en varios formas, incluyendo permisos, listas de control de acceso, restricciones de tiempo en el día, y otras restricciones de inicio de sesión y físicas.

Rastreo de cuentas: el seguimiento de los datos, el uso de la computadora y los recursos de la red.
A menudo significa registrar, auditar y monitorear los datos y recursos.

Los fundamentos de la seguridad de la información

La seguridad de la información es el acto de proteger los datos y los sistemas de información de acceso no autorizado, modificación e interrupción ilegal, divulgación, corrupción y destrucción. Discutimos cómo implementar la seguridad de la información en todo el todo el libro, pero por ahora hablemos de varios

Tipos básicos de amenazas

A lo largo de la clase discutiremos muchas aspectos importante que se necesita conocer sobre la seguridad de la información, pero por el momento veremos los tipos más básicos de amenazas que podemos ver a diario.

Software malicioso: conocido como malware, esto incluye virus informáticos, gusanos, caballos de Troya, spyware, rootkits, adware y otros tipos de virus. Todo el mundo ha oído hablar de un escenario en el que la computadora de un usuario era comprometida, aquí en la universidad lo vemos a diario con las memorias usb que son introducidas en la computadoras de los laboratorios.

Acceso no autorizado: acceso a recursos e información de la computadora sin consentimiento del propietario. Puede incluir acercarse al sistema, traspasar, comunicarse, almacenar y recuperar datos, interceptar datos o cualquier otro método que interferiría con el trabajo normal de una computadora. El acceso a los datos debe ser controlado para garantizar la privacidad. El acceso administrativo incorrecto también entra en esta categoría.

Falla del sistema: fallas de la computadora o falla de la aplicación individual. Esto puede suceda debido a varias razones, incluido el error del usuario, la actividad maliciosa o fallo de hardware.

Ingeniería social: el acto de manipular a los usuarios para revelar información confidencial. Casi todos recibe correos electrónicos hoy en día de entidades desconocidas que hacen afirmaciones falsas o preguntan para información personal (¡o dinero!); este es un ejemplo de ingeniería social.

Muchos conceptos de Seguridad pueden proteger contra, o ayudar a recuperarse de las amenazas anteriores.

La pregunta es ?Tenemos los recursos para implementarlos?, Incluso con un presupuesto bajo, la respuesta suele ser "si".

Todo comienza con la planificación, que es efectivamente gratuita.

Por lo general se debe crear un plan de seguridad proactivo que comienza con la implementación de controles de seguridad. Al crear el plan. Muchos profesionales de seguridad lo dividen en tres categorías de controles:

Físico: Alarmas, Cámaras de vigilancia, cerraduras, tarjetas de identificación, incluso hasta guardias de seguridad.

Técnico: Tarjetas inteligentes, lista de control de acceso, cifrado y autenticación.

Administrativo: Diversas políticas y procedimientos, campañas de concientización, planes de contingencia y planes de recuperación ante desastres.

Mas específicamente tenemos varias formas de prevenir y ayudar a recuperarse de las amenazas:

Conciencia del usuario: Cuanto más sabio es el usuario, menos posibilidades hay de violaciones de seguridad.

Autenticación: Verificar la identidad de una persona ayuda a proteger contra la presencia de personas con acceso no autorizadas.

La autenticación es una medida preventiva que se puede romper hasta en cinco categorías:

- Algo que el usuario sabe; por ejemplo, una contraseña o PIN
- Algo que el usuario tiene; por ejemplo, una tarjeta inteligente u otra seguridad
- Algo que el usuario es; por ejemplo, la lectura biométrica de una huella dactilar o exploración de la retina
- Algo que hace un usuario; por ejemplo, reconocimiento de voz o un escrito firma
- En alguna parte un usuario; por ejemplo, un individuo rastreado por GPS, o cuando un sistema se autentica a través de la ubicación geográfica

Software antimalware: el antimalware protege una computadora de los diversos formas de malware y, si es necesario, los detecta y elimina. Los tipos incluyen software antivirus y anti-spyware. Los ejemplos bien conocidos incluyen programas de Symantec y McAfee, así como del Windows Defender de Microsoft. Hoy en día, gran parte del software llamado "antivirus" puede proteger contra el spyware y otros tipos de malware también.

-