La seguridad de la información en la universidad

Rubén Aquino Luna
Universidad Nacional Autónoma de México

Seguridad de la Información UNAM-CERT
DGTIC, UNAM

DGTIC
DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Seguridad de la información

- “Si piensas que la tecnología puede solucionar tus problemas de seguridad, está claro que ni entiendes los problemas ni entiendes la tecnología"
  -- Bruce Schneier

Seguridad de la información

Para qué seguridad de información

- Gestión de riesgos
- Protección de activos/infraestructura
- Aprovechamiento de TIC

Dónde ubicar la seguridad de la información

Operación

- Monitoreo
- Redes/hosts
- Hardening
- Vulnerabilidades

Cumplimiento

- Auditoría
- Gestión
- Buenas prácticas
- Prevención

Sistema seguro

- "El único sistema seguro es aquél que está apagado en el interior de un bloque de hormigón protegido en una habitación sellada rodeada por guardias armados"
  -- Gene Spafford

Amenazas

- Desconocimiento
- Abuso de recursos
- Modificación de información
- Acceso a información no autorizada
- Desastres
- Denegación de servicio

ERES VULNERABLE

VERSIÓN EN ESPAÑOL

UNAM CERT

Nombres de usuario y contraseñas

Una vez que te han hackeado, los criminales cibernéticos pueden instalar programas en tu computadora que capturan las teclas que presionas y todas y cada una de las palabras que introduces en tu equipo, incluyendo tu nombre de usuario y contraseña. Esa información es usada para acceder a tus cuentas en línea, por ejemplo:

- *Tus cuentas financieras y/o bancarias, dentro de las cuales pueden robar o transferir tu dinero.*
- *Tus cuentas de iCloud, Google Drive, o Dropbox donde pueden acceder a todos tu datos confidenciales.*
- *Tus cuentas de Amazon, Walmart u otras cuentas de compras donde pueden adquirir bienes a tu nombre.*
- *Tus cuentas de UPS o DHL, donde pueden enviar bienes robados a tu nombre.*

Recolección de Email

Una vez que te han hackeado, los criminales cibernéticos pueden leer tu email en busca de información que pudieran vender a otros, por ejemplo:

- *Todos los nombres, direcciones de correo electrónico y números telefónicos de tu lista de contactos.*
- *Toda tu correspondencia electrónica personal o de trabajo.*

Bienes virtuales

Una vez que te han hackeado, los criminales cibernéticos pueden copiar y robar cualquier bien virtual que tengas y venderlo a otros, por ejemplo:

- *Tus personajes de juego en línea, los bienes que adquieres en el juego o el dinero virtual que usas para jugar.*
- *Cualquier licencia de software, números de licencia de sistemas operativos o licencias de juegos.*

Botnet

Una vez que te han hackeado, tu computadora puede ser conectada a toda una red de computadoras hackeadas controladas por los criminales cibernéticos. Esta red, llamada botnet, puede entonces ser usada para actividades como:

- *Envío de spam a millones de personas.*
- *Lanzamiento de ataques de denegación de servicio.*

Aunque no te des cuenta, tú eres un blanco para muchos criminales cibernéticos. Tu computadora, tus dispositivos móviles, tus cuentas y tu información; todos tienen un gran valor. Este poster demuestra las diferentes maneras que tienen los criminales cibernéticos para ganar dinero al hackearte. Afortunadamente, solo con tomar un par de medidas simples, puedes protegerte a ti y a tu familia. Si quieres aprender más, subscríbete a OUCH!: un boletín informativo diseñado para ayudar a personas como tú.

www.securingthehuman.org/ouch

Suplantación de identidad

Una vez que te han hackeado, los criminales cibernéticos pueden robar tu identidad en la red para cometer fraudes o vender tu identidad a otros, por ejemplo:

- *Tus cuentas de Facebook, Twitter o LinkedIn.*
- *Tus cuentas de correo electrónico.*
- *Tus cuentas de Skype u otras cuentas de mensajería instantánea.*

Servidores web

Una vez que te han hackeado, los criminales cibernéticos pueden convertir tu computadora en un servidor web, el cual pueden usar para cosas como:

- *Alojar sitios de phishing que roben nombres de usuario y contraseñas de otras personas.*
- *Alojar herramientas de ataque que hackearán las computadoras de las personas.*
- *Distribuir pornografía infantil, videos piratas o música robada.*

Finanzas

Una vez que te han hackeado, los criminales cibernéticos pueden revisar tu sistema en busca de información valiosa, por ejemplo:

- *Tu información de tarjeta de crédito.*
- *Tus registros de impuestos y antecedentes financieros.*
- *Información sobre tus planes de inversión y de retiro.*

Extorsión

Una vez que te han hackeado, los criminales cibernéticos pueden tomar el control de tu computadora y exigir dinero. Pueden hacerlo a través de:

- *Tomar fotos tuyas con la cámara de tu computadora y exigir un pago para destruir o no distribuir tus fotos.*
- *Cifrar toda la información en tu computadora y exigir un pago para poder recuperarla.*
- *Siguiendo todos los sitios web que visitas amenazando con difundir tu actividad.*

Este boletín informativo está basado en el trabajo original de Brian Krebs. Puedes aprender más acerca de los criminales cibernéticos en su blog: **http://krebsonsecurity.com**

DGTIC

DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Amenazas


Fecha: Sat, 1 Feb 2014 08:37:31
De: WorldCup2014@
Para: Destinatarios ocultos
Asunto: Usted es el ganador de u
Parte(s): Descargar todos los adju
Usted es el ganador de
Imprima su boleto y cor
IMPRIMA SU BOLETO
Revise la direcciyn del centr
SE HA BLOQUEADO SU NAVEGADOR - Mozilla Firefox
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
SE HA BLOQUEADO SU NAVEGADOR
consulmex.sre.gob.mx.id607632629-1415507771
/?flow_id=94878391469=35199/case_id=75786
Google
FEDERAL
Se han grabado todas las actividades de este ordenador. Todos sus ficheros están cifrados.
¡ATENCIÓN!
Ha violado la ley de derechos de autor (vídeo, música, software) y ha utilizado o distribuido ilegalmente contenidos con derechos de autor, infringiendo con ello el artículo 1, sección 8, cláusula 8, también conocido como derechos de autor del código penal de los México.
El artículo 1, sección 8, cláusula 8 del código penal prevé una multa de dos a quinientos salarios mínimos o la privación de libertad de dos a ocho años.
Ha estado viendo o distribuyendo contenido pornográfico prohibido (se encontraron fotos porno de niños etc. en su ordenador). Por violar el artículo 202 del código penal de los México, el artículo 202 del código penal prevé la privación de libertad de cuatro a doce años.
Se ha iniciado un acceso ilegal desde su PC sin su conocimiento o consentimiento, su PC puede estar infectado con malware, por lo que está violando la ley sobre el uso negligente del ordenador personal. El artículo 210 del código penal prevé una multa de hasta 100.000 Peso y/o la privación de libertad de cuatro a nueve años.
De conformidad con la enmienda al código penal de los México del 28 de mayo de 2011, esta infracción de la ley (en caso de que no se repita - primera vez) puede considerarse como condicional en caso de que pague la multa de los Estados Unidos.
Para desbloquear el ordenador y evitar otras consecuencias legales, está obligado a pagar unas tasas de 1000 Peso. Puede pagarlas a través de PAYSAFECARD (tiene que comprar una tarjeta PAYSAFECARD, cargarla con 1000 Peso e introducir el código). Puede comprar el código en cualquier tienda o gasolinera. PAYSAFECARD está disponible en tiendas a nivel nacional.
Su IP: .176
Ubicación: Mexico City, Distrito federal, Mexico
paysafecard
pay cash. pay safe
Beveiligd betalingsformulier
Por favor, introduzca el código PAYSAFECARD con el teclado numérico de
Región: Distrito Federal
Ciudad: Mexico
ISP:
Sistema Operativo: Windows XP (32-bit)
Nombre de Usuario: Administrador
Malware UNAM-
1 2 3 4 5 6 7 8 9 0
Pagar Ukash
Pagar PaySafeCard
¡ATENCIÓN! Su ordenador personal ha sido bloqueado por razones de seguridad vistos los motivos abajo detallados.
¿Dónde puedo adquirir un Ukash voucher?

Activos principales

Infraestructura TIC

- Telecomunicaciones
- Servidores
- Aplicaciones
- Servicios
- Equipo de cómputo

Activos principales

Información

- Registros escolares
- Datos de investigación
- Datos personales
- Publicaciones
- Administración
- Servicios a la comunidad

Algunos mitos

- No necesitamos seguridad de la información en la red abierta de la universidad
- No tengo problemas de seguridad en mi infraestructura
- Windows es inseguro/Linux es seguro
- Mac no tiene virus

Qué es lo importante (CID)

Gobierno de TI - SI

ITIL

CoBIT

ISO 27001

Protección de datos

ISO38500

Obstáculos más frecuentes

- No existen áreas específicas de seguridad
- Seguridad es un requerimiento “innecesario/prescindible”
- Mucho/poco involucramiento con otras áreas de TIC
- Resistencia al cambio
- Entorno heterogéneo

Algunos retos

- Movilidad
- Redes inalámbricas
- Protección de datos
- La nube
- Monitoreo, respuesta
- Desarrollo de aplicaciones
- Autenticación centralizada
- Firma electrónica

Lo que no funciona

- Alcances desmedidos
- Propiciar antagonismos
- Considerar seguridad al final

Lo que ayuda

Seguridad de la información

La tecnología

- Autenticación (doble factor)
- Controles de acceso
- Seguridad perimetral (FW, IPS, WAF, DB FW)
- Seguridad en dispositivos móviles
- Seguridad en aplicaciones
- Gestión de vulnerabilidades
- Correlación de eventos (SIEM)

MALA SEGURIDAD

Descripción Gráfica

Lo indispensable

Seguridad de la información

Cumplimiento

- Auditorías
- Prevención
- Gestión
- Respuesta

Operación

- Respuesta
- Gestión
- Monitoreo de TI

Lo que implica

- Gestión de riesgos
- Establecer políticas
- Planes de Recuperación de Desastres
- Continuidad del negocio
- Incorporar medidas y pruebas de seguridad a los procesos de TIC
- Concientización

Colaboración

- Implementación de buenas prácticas
- Prevención (contenidos, campañas)
- Intercambio de conocimiento/experiencias
- Evaluación de tecnología
- Desarrollo de tecnología
- Respuesta a incidentes

¿Preguntas?

UNAM-CERT

Twitter: @unamcert

Facebook: Seguridad de la Información/UNAM-CERT