CIBERSEGURIDAD

Violación de datos

Cyberoam

Avira

CRYPTOPHONE

NEXXT SOLUTIONS

open source

Índice

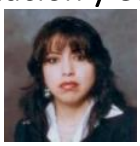
“La Seguridad no es solo un proceso Tecnológico. Es un proceso Organizacional que requiere invertir en tecnología, capacitación y recursos humanos”

— Anónimo —

CRÉDITOS:

Revista virtual de seguridad informática, recopilación de los mejores artículos de la prensa internacional.

Recopilación y edición:



Consuelo de la Torre
c.delatorre@scprogress.com (+593 979003123)

Marco de la Torre
m.delatorre@scprogress.com (+593 998053611)

Revisado por:

Arturo de la Torre
adltorre@scprogress.com (+593 999025294)

Síguenos en:

SCProgress

www.scprogress.com

Facebook

Twitter

Violación de datos

En ediciones anteriores, hemos tratado temas como el robo de datos, los Ciberstalkers, que se encuentran relacionados por ser delitos informáticos, los cuales en la mayoría de países son severamente sancionados, de igual forma, realizamos un análisis sobre la forma en la que nosotros, sin intención, dejamos impresa nuestra huella digital, mediante todas las actividades que realizamos en Internet y sobre todo en las redes sociales.

Hoy en día se habla continuamente sobre el robo de datos, la violación de datos, los ciberataques, refiriéndonos a una misma acción, es decir, al robo de nuestra información, la cual es utilizada en varias ocasiones para actos ilícitos,

La metodología utilizada para este tipo de actividad es la misma, y continuamente observamos que el uso avanzado de la tecnología, les permite a los ciberdelincuentes acceder más rápida y eficientemente a nuestra información.

SCProgress, en esta ocasión presenta a sus lectores, la recopilación de información sobre la “violación de datos”.

La acción de acceder a un computador, sin la debida autorización de su propietario o responsable, para extraer información de diferentes formas, se convierte en un delito informático, esta actividad no siempre es realizada por un experto informático.

Razón por la cual, iniciaremos con los conceptos básicos para que nos ayuden a tener mayor claridad sobre la definición de violación de datos.

“Una violación de datos es la liberación intencional o no intencional de información segura, privada o confidencial a un entorno no confiable”.

Los incidentes van desde ataques asociados por el crimen organizado, activistas políticos o gobiernos nacionales, hasta la eliminación descuidada de equipos informáticos usados o medios de almacenamiento de datos.

Otros términos para este fenómeno incluyen divulgación no intencional de información, fuga de datos, también conocido como derrame de datos, y en inglés Data Breach (violación de datos) o Breaking Down (Infracción de datos).

Definición de "Infracción de datos".

Acceso y recuperación no autorizada de información confidencial por un sistema individual, de grupo o de software. Una violación de datos es un percance de ciberseguridad que ocurre cuando los datos, intencionalmente o no, caen en manos equivocadas sin el conocimiento del usuario o propietario.

La creciente disponibilidad de datos debido al aumento de los productos digitales ha puesto una abrumadora cantidad de información en manos de las empresas.

Aunque parte de la información no es sensible, muchos de ellos son datos confidenciales y sobre todo, confidencial sobre individuos y empresas. El enfoque en las herramientas basadas en la tecnología, tales como las plataformas de computación en nube, también ha hecho que la información esté fácilmente disponible, accesible y compartida por pocos costos. Las empresas comparten y usan estos datos para mejorar sus procesos y satisfacer las demandas de una creciente población de tecnología avanzada. Sin embargo, algunas personas malvadas buscan tener acceso a esta información para usarla en actividades ilegales. El aumento de los incidentes de violaciones de datos registrados en empresas de todo el mundo ha puesto de relieve la cuestión de la ciberseguridad y la privacidad de los datos, razón por la que muchos organismos reguladores están emitiendo nuevas leyes.

Una violación no intencional de datos ocurre cuando un custodio legítimo de información tal como un empleado, pierde o utiliza negligentemente herramientas corporativas. Un empleado que accede a sitios web sin garantía, descarga un programa de software comprometido en un portátil de trabajo, se conecta a una red WiFi no segura, pierde un portátil o un teléfono inteligente en una ubicación pública, etc., corre el riesgo de que se rompan los datos de su empresa.

En 2015, Nutmeg, una empresa de gestión de inversiones en línea, tuvo sus datos comprometidos cuando un código defectuoso en el sistema dio como resultado el envío por correo electrónico de la información personal identificable (PII) de 32 cuentas a los destinatarios equivocados. La información que se envió incluyó nombres, direcciones y detalles de inversión y puso a los titulares de cuenta en riesgo de robo de identidad.

Una violación intencional de datos se produce cuando un ciberataque invade el sistema de un individuo o de una compañía con el propósito de acceder a la información personal y de propiedad. Los hackers cibernéticos utilizan una variedad de maneras de entrar en un sistema. Algunos programas maliciosos incrustados en sitios web o archivos adjuntos de correo electrónico que, cuando se accede, hacen que el sistema informático sea vulnerable a la entrada fácil y la accesibilidad de los datos por parte de los hackers. Algunos hackers utilizan botnets, que son computadoras infectadas, para acceder a los archivos de otros ordenadores.

Las botnets permiten a los perpetradores acceder a varios ordenadores al mismo tiempo utilizando la misma herramienta de malware. Los hackers también pueden utilizar un ataque de la cadena de suministro para acceder a la información.

Cuando una empresa tiene una medida de seguridad sólida e impenetrable en su lugar, un hacker puede pasar por un miembro de la red de la cadena de suministro de la empresa que tiene un sistema de seguridad vulnerable. Una vez que el hacker entra en el sistema informático del usuario, también puede tener acceso a la red de la empresa objetivo.

Los piratas informáticos no tienen que robar información confidencial como los números de seguridad social, a la vez para revelar la identidad de un usuario y obtener acceso a su perfil personal.

En el caso de robar información para el robo de identidad, los hackers con conjuntos de datos de cuasi-identificadores pueden juntar bits de información para revelar la identidad de una entidad. Los cuasi-identificadores como el sexo, la edad, el estado civil, la raza, y la dirección, se pueden obtener de diversas fuentes. En 2015, el IRS confirmó que se había producido una violación de datos de más de 300.000 contribuyentes. Los ciberdelincuentes habían utilizado cuasi-identificadores para acceder a la información de los contribuyentes y llenar las solicitudes de reembolso de impuestos. Esto dio lugar a que el IRS distribuyera más de $ 50 millones en cheques de reembolso a los ladrones de identidad.

Los propietarios y usuarios de un sistema o red quebrantados no siempre saben inmediatamente cuando ocurrió la violación. En 2016, Yahoo anunció lo que podría ser el mayor incumplimiento de la seguridad cibernética, aun cuando afirmó que se estima que 500 millones de cuentas fueron violadas. La investigación posterior reveló que la violación de datos había ocurrido realmente dos años antes, en 2014.

Mientras algunos ciberdelincuentes usan información robada para acosar o extorsionar por dinero a compañías e individuos, otros venden la información violada en mercados subterráneos de la Web que comercian con activos ilegales.

Ejemplos de información que se compran y venden en estas webs oscuras incluyen información de tarjetas de crédito robadas, propiedad intelectual de negocios y secretos comerciales de compañías.

SCProgress, cuenta con el único Firewall de Siguiente Generación del mercado (CYBEROAM NEXT GENERATION FIREWALL) que utiliza la identificación de Usuarios (Capa 8) a través de las capas 2 – 7, permitiendo a las empresas tener un mejor control y seguridad en sus redes.

La Capa 8 actúa como una capa abstracta que une las capas reales 2 – 7, permitiendo a las empresas obtener el control de seguridad perdido, habilitando la posibilidad de establecer controles en cualquiera de estas capas así como tener visibilidad de estos usuarios y las actividades de red.

Para una demostración, escriba directamente a **ventas@scprogress.com**

FUENTES:

- http://occidente.co/delito-informatico-la-violacion-de-datos-personales/
- http://wwwcomputacion95.blogspot.com/2011/04/tipos-de-violacion-la-seguridad.html
- https://translate.google.com.ec/translate?hl=es-419&sl=en&u=https://en.wikipedia.org/wiki/Data_breach&prev=search
- https://translate.google.com.ec/translate?hl=es-419&sl=en&u=http://www.investopedia.com/terms/d/data-breach.asp&prev=search
- http://www.dpoitlaw.com/notificacion-de-violacion-de-datos-personales-en-un-plazo-de-24-horas/#prettyPhoto/0/

Capacitación en Ciberseguridad y Antimalware

"La necesidad de capacitación surge por la diferencia entre lo que uno debería saber y lo que sabe realmente"

El personal responsable de las áreas de sistemas, así como los usuarios, deben conocer sobre la infinidad de ataques informáticos amenazas, ataques a la información y a las infraestructuras tecnológicas, los mantienen como áreas vulnerables permanentes, facilitando las actividades fraudulentas de hackers, quienes han visto como un gran negocio lucrativo, la sustracción de datos, ya sea personal, financiera, confidencial, etc.

La capacitación en seguridad informática, se vuelve relevante e importante para evitar que las empresas e instituciones, se vean afectadas ante este tipo de amenazas.

SCProgress cuenta con asesores altamente especializados a nivel internacional, lo que nos permite brindar cursos de capacitación en diversos temas tecnológicos, especialmente en el área de seguridad informática, su amplia experiencia y conocimientos, les ha permitido participar en eventos nacionales e internacionales como la conferencia organizada por la CEPOL Research & Science Conference (Organismo acreditado de la Unión Europea), realizada en Budapest el año 2016.

En esta ocasión SCProgress, consiente de la importancia que prestan las instituciones a la seguridad de la información, y ante el incontrolable crecimiento de las amenazas, ha organizado y pone a disposición de sus lectores y clientes, capacitación en los siguientes temas:

Certificación en Ciberseguridad de la RED	Introducción al análisis y comportamiento del malware
Contenido: • Fundamentos de red de computadoras y defensa • Amenazas, vulnerabilidades y ataques a la red • Controles, protocolos y equipos para la seguridad de la red Diseño e implementación de políticas de seguridad en la red • Seguridades físicas • Seguridades en los Host • Configuración y administración segura de Firewalls • Configuración y administración segura de IDS • Configuración y administración segura de VPNs • Protección de redes inalámbricas • Monitoreo y análisis del tráfico de la red • Gestión de riesgos y vulnerabilidades • Data backup y recuperación de datos • Respuesta y manejo de incidentes	**Contenido:** • Análisis de malware • Indicadores de infección • Malware signatures • Categorías de malware • Mass vs Targeted malware • Metodología de análisis de malware • Herramientas Antimalware • Malware empaquetado y oculto • DLL Hijacking • Magic labels • Formatos de archivos • Dynamic Link Libraries • Detección de virtualización de malware • Dependency Tracing • Modificación de registros • Manipulación de archivos del sistema • Análisis de tráfico de la red • Sandboxes

Los cursos se dictan en las instalaciones de SCProgress ubicadas en el edificio Plaza de Vizcaya, tercer piso, en La Pradera E7-21 y Mariana de Jesús,

Para mayor información visite nuestra página web: **www.scprogress.com**, o comuníquese directamente al correo electrónico: **ventas@scpgrogress.com**.

La violación de Datos Personales. Estar prevenidos por si nos toca.

En nuestra sociedad, cada vez más virtual, no podemos eludir un hecho tan desconcertante como la posible violación de datos personales dentro de nuestra compañía. Prácticamente, cada semana, nos encontramos con una empresa afectada por un nuevo caso de este tipo.

En el mundo empresarial es más que evidente que la violación de datos personales es un hecho, y que su prevención es la clave para procurar que los daños sean mínimos.

Afecta desde a las altas instituciones del Estado, a centros de negocio de las compañías de medios más grandes del mundo, hasta las más pequeñas, en las que se puede pensar que son demasiado insignificantes como para que los ciberdelincuentes puedan tener cierto interés en atacar las mismas. Nadie se libra. El daño y coste, como consecuencia del hack no hace más que crecer.

Es crucial tener un plan

Nuestra empresa necesita tener un plan preparado para abordar de inmediato las consecuencias de un hecho de esta dimensión. El plan debe incluir a todos los interesados clave dentro de la organización. Desde el Departamento TI al de Recursos Humanos, al de Comunicación y hasta a la cúpula ejecutiva.

Pero esta lista debe comenzar por un asesor legal que pueda guiarnos con la difícil tarea de informar a las partes involucradas. Alguien que nos oriente sobre cómo tratar con proveedores, localizar el incumplimiento y proporcionar información valiosa sobre el fraude.

La violación de datos es particularmente insidiosa, porque a menudo abarca la información confidencial de un individuo. Los gobiernos tienen regulación estricta sobre como una empresa debe tratar la información confidencial de los usuarios, con anexos sobre violación de datos. Pero hay numerosos aspectos de esta regulación que deben ser abordados con un experto legal, así cualquier plan de respuesta contra la violación de datos debe incluir asesoramiento legal completo. Si no se sigue una regulación de respuesta frente a una violación, nos podríamos enfrentar a sanciones.

Difunde el mensaje con cuidado

Después de preparar la ejecución del plan, es

importante transmitir el mensaje sobre la violación de datos a todos los implicados incluyendo:

- Cumplimiento de La Ley (Servicios de Seguridad)
- Compañías de Tarjetas de Crédito y Procesadores.
- Clientes.
- Proveedores.
- Usuarios.
- Empleados.

Tu plan debe detallar quienes son los contactos principales, y cuando llegar a ellos. No toque estos grupos sin una primera consultoría legal es posible que existan regulaciones sobre cuándo y cómo estos grupos necesitan estar informados.

Pon tu plan a prueba

La implementación del plan alertará a los empleados sobre la gravedad de este tipo de intrusión, les ayudará a estar más preparados de cara a un posible suceso real, y tal vez aumente su conciencia sobre el riesgo, reduciéndose las posibilidades de que se produzca un hecho de esta índole.

Compromiso y Profesionalidad

Se debe mostrar un nivel de compromiso y profesionalidad sobre cómo manejar la violación en sí, pero también sobre la gestión de la información sensible. Estar mejor preparados y saber exactamente qué hacer no sólo es una acción inteligente, sino que también te protege a ti y a tus clientes de un daño mayor.

Ecuador frente a la violación de datos

En el Ecuador también se han tomado medidas contra la violación de datos. En el mes de febrero de 2016, se creó una Unidad Especial en la Policía Nacional, para enfrentar los delitos cibernéticos, con efectivos dedicados a la investigación, de las denuncias realizadas en las diferentes Fiscalías.

Así también, los delitos informáticos se encuentran tipificados en el Código Orgánico Integral Penal (COIP), en la Sección Sexta: Delitos contra el derecho a la intimidad personal y familiar, en su Artículo 178.- "Violación a la intimidad.- La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años".

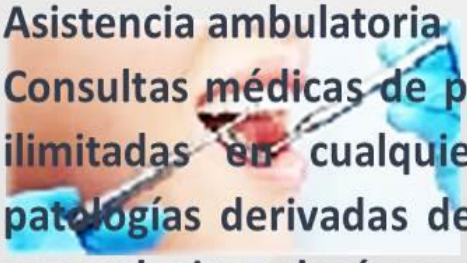
FUENTES:

- http://willisupdate.com/la-violacion-de-datos-personales-estar-prevenidos-por-si-nos-toca/
- http://www.policiaecuador.gob.ec/delitos-informaticos-o-ciberdelitos/
- http://willisupdate.com/la-violacion-de-datos-personales-estar-prevenidos-por-si-nos-toca/
- http://www.andes.info.ec/es/noticias/ecuador-crea-unidad-especial-enfrentar-ciberdelitos.html
- http://www.justicia.gob.ec/wp-content/uploads/2014/05/c%C3%B3digo_org%C3%A1nico_integral_penal_-_coip_ed._sdn-mjdhc.pdf
- https://es.slideshare.net/cesardav1/delitos-informaticos-15240484
- http://newalcatec.blogspot.com/2012/06/violacion-de-intimidad-en-redes.html
- https://es.slideshare.net/hectorrevelo/clase-02-delitos-informticos-en-ecuador-coip-20142015

Cooperativa de Ahorro y Crédito "General Rumiñahui"

Promoviendo el desarrollo y bienestar de sus socios militares y civiles desde 1993.

- Créditos sin garante hasta 3.000 dólares.
- Otorgamos créditos para consumo, emprendedores y microempresarios.
- Las tasas de interés más bajas del mercado.
- Inversiones a plazo fijo.
- Pagos de créditos y ahorros, a través de ventanillas o con autorización de débitos bancarios del Banco Pichincha, General Rumiñahui e ISSFA.



- Asistencia ambulatoria.
- Consultas médicas de primer nivel ilimitadas en cualquiera de las patologías derivadas de: medicina general, ginecología y pediatría.
- Cobertura en asistencia dental.
- Examen clínico y diagnóstico.
- Higiene dental, alivio del dolor.
- Rayos X periapical, profilaxis (Limpieza dental profunda).
- Restauraciones en resina simple.
- Extracciones simples.

Calle Manuel Cabeza de Vaca N53-240 y Av. Los Pinos a 30 mts. Del Cuartel Rumiñahui.
Teléfonos: 2411-731 / 2406-117 / 0984977204

www.cooprumi.fin.ec

Malware en TPV, un gran problema para empresas y clientes

Los terminales de puntos de venta (TPV) se han convertido en un gran objetivo para los cibercriminales en medio de ataques generales contra compañías de venta al por menor.

Con ello, el malware en TPV se ha convertido en un gran problema para las empresas y sus clientes, la presencia de software malicioso en estos terminales de punto de venta (conocidos en inglés por su acrónimo POS) está aumentando de forma alarmante.

La instalación de malware en los TPV tiene una motivación esencialmente económica y su objetivo preferente es el robo de los datos de las tarjetas de pago de los clientes. Para ello, los ciberdelincuentes aprovechan cualquier vulnerabilidad de los terminales, de su sistema operativo o de los protocolos utilizados para ejecutar las transacciones entre TPV y los servidores, para introducir software malicioso que permita el robo de datos, por cualquier técnica de ataque.

Un caso conocido es el que afectó a la cadena de hoteles y resorts Starwood, que opera 1.200 establecimientos de las marcas Westin o Sheraton en América del Norte. La cadena informó que los TPV de 54 de sus hoteles estaban infectados con un malware diseñado para desviar la información, incluyendo nombres de los clientes, números de tarjetas de pago, códigos de seguridad y las fechas de vencimiento.

Lo peor del caso es que el malware estuvo activo en algunos de los hoteles durante

varios meses sin que fuera detectado. Se cree que el software malicioso utilizado es el ModPOS, uno de los más sofisticados jamás creado para terminales de punto de venta. Además de la cadena Starwood, podría haber estado atacando en secreto a servicios de comida, hospitales y compañías de salud en Estados Unidos.

Los ataques contra estos puntos de venta y en general contra empresas y minoristas están a la orden del día y son un objetivo preferencial para los cibercriminales. Se encuentra entre las peores violaciones de seguridad con los ataques a Target, Home Depot o eBay, un ataque contra VTech comprometió a 5 millones de clientes.

A mediados de junio de 2016 se dio a conocer la existencia de un malware o software malicioso llamado PunkeyPOS que afecta a los terminales TPV y permite que los datos de las tarjetas de débito o crédito de los clientes sean robados.

Hasta ahora han detectado 200 terminales infectados, localizados sobre todo en restaurantes de Estados Unidos, aunque también hay casos reportados en Reino Unido y Francia. Los investigadores no descartan que el número y la localización geográfica aumenten con el paso del tiempo.

Cómo opera el malware PunkeyPOS sobre los TPV

El malware está formado por dos componentes, un keylogger que almacena los datos digitados por el cliente en el teclado y un ram - scraper que lee los datos almacenados en la banda magnética y los procesos internos que se llevan a cabo cuando se realizan los pagos.

Una vez los datos eran capturados por el software eran enviados a servidores remotos en donde eran almacenados para ser vendidos en la darkweb, donde los ciberdelincuentes los adquieren para cometer fraudes.

Afortunadamente, en esta ocasión el servidor en el que se almacenaban los datos tenía vulnerabilidades que permitieron a los investigadores tener acceso a él y descubrir exactamente cómo operaba PunkeyPOS.

Cómo evitar que se infecte tu datafono

Para evitar que tu terminal TPV se infecte con este y otros malware debes ser muy cuidadoso en la selección de las personas que lo manipulan, pues un dependiente malintencionado podría instalar software para alterarlo y robar los datos de tus clientes.

Otra medida que debes tomar es adquirir estos equipos con un proveedor de confianza y estar atento a todas las recomendaciones de seguridad que te haga tu banco. Por último, cuidar que el computador que se conecta al terminal TPV sea dedicado únicamente a este propósito, y si no fuera posible entonces mantener el antivirus y el firewall debidamente actualizados.

Avira Endpoint, te ofrece protección de primera clase y en tiempo real, en todos tus equipos y servidores de empresas, confía la seguridad de tus datos al antivirus más galardonado del 2016.

Recuerda que en caso de que se descubra que desde tu establecimiento se comete fraude los costos en imagen y reputación serían incalculables, y que puede tardar mucho antes de que logres recuperar la confianza de tus clientes.

Las brechas de seguridad también llegan a los TPV conectados a la nube

Los puntos de venta TPV conectados a la nube se vuelven más vulnerables a sufrir brechas de seguridad con robo de información relacionada con los clientes. El último suceso de la compañía canadiense Lightspeed podría haber afectado a 38.000 clientes.

Un operador de servicios basado en la nube podría haber sido el último en sufrir un ataque en el que 38.000 clientes se habrían visto afectados tras ser alterados los terminales punto de venta de sus establecimientos. La compañía canadiense Lightspeed informó de la brecha de

seguridad, destacando que se habrían visto afectados los puntos de venta que utilizan tablets, smartphone o cualquier otro dispositivo similar.

Lightspeed tiene una clientela de negocios que le permiten alcanzar los 12.000 millones de dólares en transacciones anuales. Estos clientes están formados por pequeños minoristas que venden ropa, joyas, libros y equipo deportivo. El servicio funciona con un sistema de bases de datos conectadas a la nube, con el fin de poder trabajar en remoto desde dispositivos móviles.

El incidente se produce en un momento en el que cada vez más, el sector retail es blanco de los hackers.

Los puntos de venta siguen convirtiéndose en un objetivo atractivo para los delincuentes cibernéticos, dado que un ataque a estos sistemas puede significar el acceso a información de decenas y cientos de tiendas al por menor.

FUENTES:

- https://www.gestiontpv.com/blog/alertan-sobre-nuevo-virus-que-ataca-los-tpv
- http://muyseguridad.net/2015/12/05/malware-en-tpv/
- http://cso.computerworld.es/cloud/las-brechas-de-seguridad-llegan-a-los-tpv-conectados-a-la-nube

Rincón de los expertos

Hoy existen más razones que nunca para comprender y aplicar formas de proteger nuestra información. A continuación les damos algunos procedimientos y consejos para alcanzar este objetivo.

1. Descarguen e instalen Signal, desarrollada por Open Whisper Systems, o en su lugar utilicen WhatsApp para enviar mensajes de textos.
2. Protejan el disco duro de su computador con FileVault o BitLocker.
3. Cambiar frecuentemente las contraseñas de los sistemas, es una de las mejores opciones de proteger nuestra información, pero es una de las más complicadas, en especial cundo utilizamos passwords combinados, por esta razón recomendamos utilizar Avira Vault, 1Password o KeePass.
4. Protejan sus cuentas de correo electrónico y otras similares, con al menos sistemas de dos factores de autentificación.
5. Utilizar el navegador de Internet siempre con el plug-in llamado HTTPS en todas partes.
6. Invierta en el uso y personalización de VPNs para su organización.
7. Recuerde que el modo incognito de su navegador, no siempre es privado y por tanto seguro. Tenga cuidado con la información que ahí maneja.
8. Realizar las búsquedas de información sensitiva en el sitio DuckDuckGo.
9. Cuando no sea necesario mantenga su webcam tapada con taipe.

Estas medidas con toda seguridad le ayudaran a mantener su sistema más seguro.

Novedades

Reconocimiento internacional a SCProgress por calidad, productos y servicios.

En el mes de abril, Latin American Quality Institute (LAQI) reconoció y premió a la empresa SCProgress, por sus altos estándares de calidad, productos y servicios a nivel Latinoamérica, LAQI es una organización privada sin ánimo de lucro, calificada como la institución de mayor relevancia en lo referente a desarrollo de normas y patrones de calidad en Latinoamérica, y una de las más importantes en el mundo.

Los avances tecnológicos desafían a las empresas a cumplir con óptimos estándares de calidad para fortalecer su desarrollo y perfeccionamiento, SCProgress, cumplió con todos los niveles requeridos por LAQI, confirmando que los productos y servicios proporcionados a todos sus clientes, son los mejores y están en sitiales altamente reconocidos a nivel internacional.

Felicitamos sobremanera a todos sus directivos y personal técnico, por la obtención de tan merecido reconocimiento, este premio, será la motivación para continuar en tan ardua labor y mantener el lugar que tan exitosamente hemos conseguido. También agradecemos a todos nuestros clientes, por la confianza brindada a lo largo de todos estos años.

¡Demuestra tus conocimientos!

La tecnología se encuentra al alcance de todos y se ha convertido en una herramienta indispensable para el desarrollo y aprendizaje permanente de los niños.

SCProgress en homenaje a los niños por su día y, conscientes del interés que tienen los padres por proporcionar a sus hijos las herramientas para su desempeño, desafía una vez más sus conocimientos y obsequia dos tablets Samsung de última generación, síguenos en nuestra página web y redes sociales Facebook y Twitter, donde encontrarás el enlace de la encuesta, en la que dos participantes con las mejores puntuaciones serán los ganadores. La encuesta se encontrará activa hasta el día viernes 26 de mayo de 2017.

Participa y gana, no puedes perder la oportunidad de llevarte totalmente gratis una tablet.

Noticias

La nueva guerra fría se juega en el espionaje cibernético

Angela Merkel y Vladimir Putín, se cruzaron. El presidente ruso le juró a la alemana que no está detrás de los hackeos.

Como una sombra apocalíptica, la pregunta retumba en todos los rincones del planeta. Los analistas internacionales se topan a menudo con ella: ¿viene la Tercera Guerra Mundial? Al temor lo alimenta que las palancas de las grandes maquinarias militares estén en manos de personajes que irradian desmesura y temeridad.

En la Casa Blanca está la impredecible creación de Steve Bannon, un ideólogo extremista que lleva tiempo predicando la necesidad de reconquistar en una guerra el liderazgo global de Washington. Para el ventrílocuo de Trump, no se trata de ser "el policía del mundo", sino de marcar el terreno a gigantes como China, que se expande en el Mar Meridional y avanza a paso redoblado en la conquista de mercados y socios económicos, mientras invade el mundo con sus productos.

En el Kremlin está el nuevo "zar de todas las Rusias", relanzando el expansionismo territorial que inició Iván el Terrible a partir del Gran Ducado de Moscovia, y agigantaron Pedro el Grande, Catalina II y Joseph Stalin.

El Bannon de Vladimir Putin es Aleksandr Dugin, autor de "La Geopolítica de Rusia" e ideólogo del "neo-euroasianismo". La búsqueda del "lebensraum" ruso está detrás de las conquistas de Osetia a costa de Georgia y de Crimea a costa de Ucrania, además de alimentar la expansión hacia el Donbass y la actual amenaza a los países bálticos, acrecentando a niveles de infarto las tensiones con la OTAN.

Para colmo, el custodio del Palacio del Sol es Kim Jong-Un, el muchachote robusto que parece decidido a ir más lejos que su padre en materia de generar tensiones bélicas. El

heredero de la estrambótica dinastía comunista que aspira a ser la versión moderna de la Dinastía Joeson, cuyo reinado se extendió desde el siglo XIV hasta el siglo XX, quiere mostrarse dispuesto a lo que hizo su abuelo al iniciar, en 1950, la guerra que lo enfrentó con Estados Unidos.

En aquel momento, Kim Il-sung actuó por cuenta propia, sin acatar la orden soviética de no invadir el sur de la península. China es hoy la potencia que le ordena a Kim Jong-un cesar las pruebas nucleares y balísticas, pero el gobernante norcoreano muestra la misma indómita temeridad de su abuelo.

En Washington, de momento, al extremismo de Bannon lo está neutralizando el establishment republicano, que logró reemplazarlo en el Consejo de Seguridad Nacional por un experto como el general Herbert McMaster.

Rusia

Tampoco se sabe hasta dónde puede llegar Putin, en su afán por reconstruir el imperio euroasiático y evitar que la influencia mundial de Rusia se diluya ante el poderío avasallante de la economía china.

Menos predecible aún es el "líder supremo" de la sociedad más militarizada del mundo. Es difícil entender por qué se arriesga a perder el petróleo que recibe de China y las exportaciones norcoreanas de carbón a Beijing y Seúl, sufriendo una nueva tanda de sanciones económicas, justo cuando la tenue pero persistente reforma económica iniciada por Kim Jong-il empieza a mostrar buenos resultados. El hecho es que estos liderazgos, más la proliferación de gobiernos extremistas y líderes impresentables han generado la sensación de que se avecina una nueva guerra mundial.

Según el Papa, esa guerra ya está ocurriendo. ¿Es así? En el imaginario del hombre contemporáneo, la idea de una III Gran Guerra tiene dos formas posibles. La primera se desprende de las dos conflagraciones anteriores que fueron calificadas como "mundiales". En ambos casos, la calificación surgió de una cuestión numérica: la gran cantidad de países que participaron en los conflictos.

Hoy es improbable que ese formato se repita. Quienes quieren ver tal rasgo en la guerra civil siria porque involucra a varios países, deben tener en cuenta que algo similar ocurrió en la guerra civil que desangró al Líbano entre 1975 y 1990. Tampoco se habló de Guerra Mundial durante la trágica desintegración de Yugoslavia, a pesar de que la OTAN entró en acción contra Serbia.

La otra posibilidad que justificaría la calificación de "mundial" para un conflicto en este tiempo, sería un choque nuclear entre dos potencias. De hecho, durante la Guerra Fría fue ese el fantasma que llevó el título "Tercera Guerra Mundial".

Ciberataque

Lo que más temen hoy las superpotencias no es un ataque con ojivas atómicas o neutrónicas. El riesgo más temido, en particular por Washington, es un devastador "ciberataque". De haber una III Guerra Mundial, lo más probable es que sea cibernética.

Del mismo modo que los espías que existieron hasta los tiempos de la Guerra Fría, fueron reemplazados por los ciberespías que actúan en la web, la guerra entre superpotencias se desarrollaría en el ciberespacio.

Los espías de hoy no usan microfilms, sino laptops. El espionaje ya no tiene personajes como James Bond, sino como Edward Snowden. A los mayores daños causados por espías a Estados Unidos, los infligieron los ciberespías de China y de Rusia, además de Julian Assange con WikiLeaks.

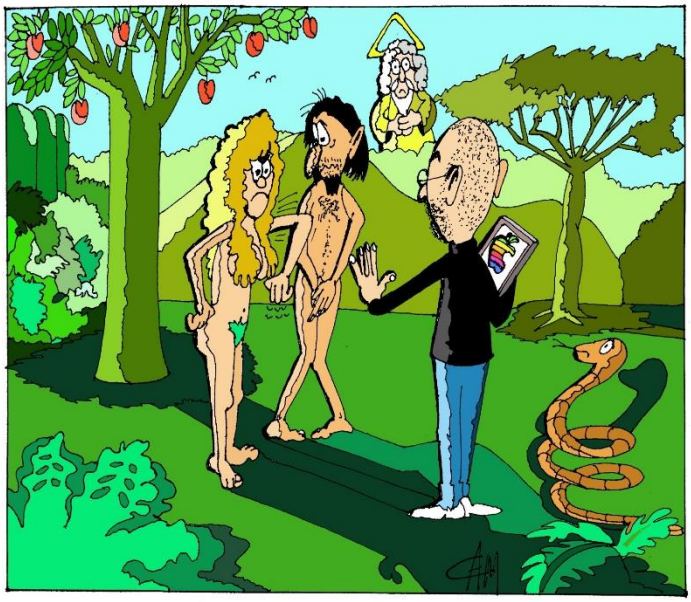
Un ejemplo de las armas que actuarían en una III Gran Guerra es Stuxnet, el "gusano" cibernético que, en el 2010, tomó el control de mil centrifugadoras que producían uranio enriquecido en la central iraní de Natanz, y les ordenó autodestruirse. Un virus similar provocó estragos en Bushehr, otro de los puntos donde se desarrollaba el plan nuclear de la teocracia persa.

¿Podría un equipo de hackers intervenir los sistemas que activan lanzamientos de misiles intercontinentales?.. De momento, la pesadilla del Pentágono no es una lluvia de misiles, sino un ataque cibernético que paralice las centrales nucleares, hidroeléctricas y termoeléctricas, dejando sin energía el país. O que un ataque masivo a las redes haga caer el sistema a nivel nacional. La consecuencia sería la generalización del pánico y de la histeria colectiva. Un caos devastador como el que no podría causar a Estados Unidos ningún ataque con ejércitos, aviaciones o misiles.

FUENTE:

- http://noticias.perfil.com/2017/05/06/la-nueva-guerra-fria-se-juega-en-el-espionaje-cibernetico/

Humor



Espionaje Cibernético

El espionaje cibernético se ha convertido en una nueva mina de oro para los criminales.

Es por eso que el gobierno de Estados Unidos presentó una nueva estrategia para contrarrestar el dramático aumento de la amenaza que representan los piratas cibernéticos y el espionaje en internet.

Con el presente contexto, iniciaremos por conocer el concepto de espionaje cibernético:

"Espionaje cibernético, es el acto o práctica de obtener secretos sin el permiso del poseedor de la información (personal, sensible, propietaria o de naturaleza clasificada), de individuos, competidores, rivales, grupos, gobiernos y enemigos para ventaja personal, económica, política o militar usando métodos en Internet, redes o computadoras individuales a través del uso de técnicas de cracking y software maliciosos incluyendo Troyanos y spyware.

Puede ser totalmente perpetrado en línea desde las computadoras de escritorio de profesionales en las bases, en países muy lejanos o puede implicar la infiltración en el hogar por espías convencionales entrenados en computación, o, en otros casos puede ser la obra criminal de un hacker malicioso amateur y programadores de software.

Recientemente, el espionaje cibernético supone el análisis de la actividad pública en redes sociales como Facebook, Twitter entre otros.

El ciberespionaje también es considerado como la práctica de utilizar las redes de computadores para obtener información que se considera de otra manera privada.

El espionaje cibernético puede tener lugar en diferentes niveles. Por ejemplo, las personas pueden realizar espionaje cibernético contra otro individuo en particular, o los países

pueden utilizar ciberespionaje como una forma de espionaje para obtener información clasificada de otros países.

El ciberespionaje es esencialmente el mismo que normal, excepto que el espionaje cibernético tiene lugar en Internet. Por la piratería en la red informática de la meta, o poner en peligro su seguridad a través de otros medios, los espías informáticos son capaces de interceptar y descargar la información que pueda ser útil, muy privado, o relativa a la seguridad nacional.

Espionaje cibernético a gran escala

Cuando el espionaje cibernético tiene lugar en un gran nivel, por ejemplo, entre los países, la práctica puede ser referida como el espionaje cibernético. Muchos países de todo el mundo tienen las agencias de inteligencia que se dedican a la práctica de espionaje en nombre de la seguridad nacional. Con la llegada de Internet, muchas de estas agencias ahora realizan la vigilancia rutinaria con otros países.

Operación Shady Rat

Un claro ejemplo de espionaje cibernético, fue el detectado en agosto de 2011, una operación denominada "Operación Shady Rata" que probablemente financiado por el gobierno chino, lleva una década de espionaje ininterrumpido a gobiernos y empresas en el sudeste asiático y la India, una operación de espionaje cibernética de larga duración. Se centraron en objetivos de gobierno y comercial, que tienen la información política, económica y militar clave de la región.

No fue posible medir el daño causado, ya que había tenido lugar durante un período tan largo, aunque el impacto podría ser "masivo".

Métodos

Los métodos utilizados para el ciberespionaje involucran diferentes niveles de complejidad. Algunos métodos de espionaje cibernético pueden ser tan simples como adivinar la contraseña de un objetivo y el acceso a sus archivos sin permiso, o tan complejo como la plantación de código oculto en el ordenador

de un objetivo y hacer que la computadora cargue automáticamente cierta información a un servidor remoto.

Espías cibernéticos utilizan cualquier medio a su alcance con el fin de infiltrarse en el objetivo deseado, incluyendo los esquemas de phishing, piratería, clave de registro de software y puertas traseras en los sistemas informáticos.

FUENTES:

- http://www.voanoticias.com/a/internet-espionaje-cibernetico-amenaza-dinero/1607862.html
- http://es.viva-read.com/article/qu-es-el-ciber-espionaje
- https://es.wikipedia.org/wiki/Ciberespionaje
- https://sites.google.com/site/espionajeindustrialcibernetico/introduccion/definicion
- http://www.ubiquitour.com/5OJbjXNO/
- http://www.lr21.com.uy/mundo/1109794-europa-inerme-e-indefensa-ante-el-espionaje-de-ee-uu-a-cualquier-ciudadano
- https://mediatelecom.com.mx/~mediacom/index.php/agencia-informativa/noticias/item/84743-fireeye-identifica-espionaje-chino-persistente-por-10-a%C3%B1os

Recomendaciones para proteger de ataques cibernéticos a los centros de datos

Con el cambiante entorno de las amenazas, vale la pena revisar si las políticas, metodologías y tecnologías utilizadas aún protegen los datos, sin importar dónde se encuentren. Aquí le ofrecemos algunos consejos de expertos para asegurar la información de su empresa.

Son acciones básicas y sencillas de realizar que pueden ser de suma utilidad para proteger a la empresa y su reputación. Además, la mayoría de ellas no necesitan una gran inversión.

1. **Simplificar el sistema**: La complejidad aumenta el número de superficies de ataque. Una forma fácil de reducir este número es desactivando las funciones que no estén siendo utilizadas, así como apagando o desconectando el equipo que no esté en uso o no tenga una función básica.
2. **Fortalecer los accesos**: Partir de la base de que los usuarios y contraseñas predeterminados se encuentran 100 por ciento expuestos y, por ende, se deberán cambiar al momento de configurar los dispositivos. De la misma forma, es recomendable eliminar las credenciales predeterminadas (contraseñas, cadenas de comunidad SNMP, etc.). Hay que construir contraseñas fuertes y, cuando sea posible, usar distintos usuarios y accesos para diferentes personas.
3. **Aislar la red**: Separe la red de las instalaciones de la red corporativa y desarrolle una red física independiente para el centro de datos, ocultándola detrás de un firewall físico. Al no estar conectada a la red corporativa, es posible mantener a los hackers alejados del equipo crítico para la misión de la empresa.
4. **Actualización constante**: Asegúrese de que el firmware más reciente se encuentra instalado en todos los dispositivos y no olvide realizar esta actividad con frecuencia para estar al tanto de los parches de seguridad más recientes.
5. **Acceso físico controlado**: Proteja de manera física al equipo crítico y utilice un plan de control de acceso. Algunos de los protocolos de seguridad que se usan en el equipo tienen treinta años de antigüedad y fueron desarrollados en una época en la que no teníamos tantos problemas de seguridad. Al colocar el equipo tras una puerta bloqueada con control de acceso, se tiene ventaja en cuestión de protección.

6. **Correcto reciclaje de computadores:** Elimina los datos de la computadora de forma

permanente. Una vez que hayas guardado toda la información importante, lo más inteligente es borrarla de la computadora para que los futuros usuarios o ladrones de identidad no puedan acceder a ella. Borrar datos enviándolos solo a la papelera de reciclaje o la herramienta equivalente que tengas en tu computadora, puede dejar estos archivos en el disco duro, de forma que cualquier persona con conocimientos informáticos podrá recuperarlos. Esto quiere decir que, por lo general, para vaciar toda la información personal de la computadora tendrás que formatear el disco duro.

El formateo del disco duro es irreversible y, básicamente, dejará tu computadora "en blanco" (eliminando no solo los datos, sino, prácticamente, toda la información), así que asegúrate de haber guardado todos los archivos importantes antes de iniciar este proceso.

Desarrollamos estas recomendaciones asumiendo que las herramientas activas de digitalización (escáneres de red, detección de intrusos y registros de penetración, escáneres de correo electrónico y software antivirus) son implementadas por el Departamento de TI como parte de las medidas de seguridad necesarias para proteger a la empresa, pero si trabaja en el centro de datos y no está seguro de esta situación, es clave que lo verifique.

FUENTES:

- http://searchdatacenter.techtarget.com/es/opinion/Cinco-recomendaciones-para-proteger-de-ataques-ciberneticos-a-los-centros-de-datos
- http://es.wikihow.com/deshacerte-de-una-computadora-sin-peligro
- http://www.huffingtonpost.es/2017/05/12/consejos-para-evitar-un-ciberataque_a_22083669/

SCProgress cuenta con todo lo que necesita para su infraestructura de cableado estructurado

Los sistemas de cableado estructurado constituyen una plataforma universal para la transmisión de voz, datos y video, el diseño e implementación de infraestructuras de fibra óptica y cableados que cumplan con los estándares se vuelven cada vez más imprescindible para el éxito de sus empresas.

SCProgress brinda el mejor servicio en:

- Diseño e instalación de sistemas de cableado estructurado con las mejores marcas.
- Certificación de sistemas de cableado estructurado
- Diseño e instalación de fibra óptica.
- Asesoría técnica para la implementación de sistemas de cableado estructurado.
- Personal altamente calificado, certificado y con amplia experiencia.

En caso de requerimiento del cliente, nuestro personal cuenta con experiencia en marcas como Panduit, Dexon, así como marcas nacionales.

Para más información no dude en contactarnos en ventas@scprogress.com

GESRICA
COMPAÑÍA DE GESTIÓN DE RIESGO Y CAPACITACIÓN S.A.

Nuestro país se encuentra ubicado sobre el cinturón de fuego del pacífico, por lo que nos encontramos expuestos a eventos naturales que pueden afectar nuestras actividades, razón por la cual, debemos tomar acciones y ejecutar procedimientos para mitigar posibles siniestros, ya sean causados por la fuerza de la naturaleza o por accidentes humanos.

Contamos con personal especializado en la gestión, planificación, capacitación e implementación de estrategias para la reducción de riesgos y ponemos a su disposición , asesoramiento en la elaboración de planes de gestión de riesgos, diseñados exclusivamente para las características de su empresa, así como, capacitación en áreas a fines, principalmente en:

- ***Primeros auxilios.***
- ***Brigadas de emergencia.***
- ***Prevención de incendios***
- ***Seguridad industrial.***
- ***Normas de seguridad.***
- ***Prevención y manejo de emergencias y evacuaciones.***

www.gesrica.com
E-mail: info@gesrica.com
Teléfonos: 0984489267 - 0996620889 – 0979003123
Dirección: 18 de Septiembre 07-04-009 y Panamericana Norte.

www.scprogress.com

Mayo 2017