Número 80

Notibytes

1

Octubre de 2017
Año 11

Universidad Distrital Francisco José de Caldas - Facultad Tecnológica
Proyecto Curricular Tecnología en Sistematización de Datos e Ingeniería en Telemática.

EDITORIAL

Cuatro consejos sencillos para hacer 'back-up'

Si su teléfono se daña de repente o si al tratar de utilizar su computador una mañana le pide una clave que no conoce, ¿qué información perdió? Aunque no exista un método infalible **las prácticas de autocuidado o 'higiene digital' pueden reducir vulnerabilidades**. Entre ellas se cuenta cambiar las contraseñas con frecuencia, activar la verificación de dos pasos y realizar (copias de seguridad).

Si desea hacer una copia de seguridad de su sistema, estas son algunas recomendaciones:

1. Cree un hábito: Procure que se vuelva un hábito como lavar sus dientes u organizar su escritorio. Usted define qué tan seguido realizar el proceso, pero trate de mantener esa periodicidad. No solo tendrá su información actualizada, sino que también optimizará el espacio de memoria y facilitará la recuperación de versiones recientes.

2. Establezca una lógica de almacenamiento: Con frecuencia cuando se guardan las fotos de un celular para recuperar espacio, simplemente se arrastran y se acumulan en su computador. Pero, definir un orden (por fechas, por temas o por importancia) le permitirá encontrar más fácilmente sus archivos, actualizarlos y borrar lo que no necesite.

3. Depure la información y actualice: Para conocer qué información posee y cuál necesita cuidar más, es importante priorizar qué va a almacenar. Difícilmente puede prestar atención a unas fotografías si las tiene en medio de miles de archivos sin clasificar. Puede ser útil preguntarse cuándo fue la última vez lo utilizó la información y qué valor tiene para usted.

4. Seleccione el lugar de almacenamiento: Los volúmenes de información y las rutinas para el proceso pueden ser significativamente diferentes para empresas y para individuos. Identifique si sus contenidos solo necesitan un disco duro de almacenamiento externo o si necesita un servicio en la nube. Es importante verificar las posibilidades de acceso a su información que tendrán terceros y considerar cifrar archivos delicados.

Resumen tomado de: eltiempo.com, tecnosfera, 22 de Octubre/ 2017
http://www.eltiempo.com/tecnosfera/novedades-tecnologia/consejos-para-hacer-back-up-y-protegerse-digitalmente-143668

Comité Editorial:
Carlos Alberto Vanegas,
Sonia Alexandra Pinzón,
Edwin Ávila.

"Las tácticas preferidas por los cibercriminales".

¿Le asusta que criminales encripten los datos de su celular o su PC? Imagine que, además, lo amenacen con enviar a sus contactos todas las fotos del dispositivo si no paga rescate.

El panorama de la ciberdelincuencia empeora con la emergencia del internet de las cosas, que multiplica las amenazas. Según Kaspersky, en el segundo que tarda leyendo esta línea hay 33 ataques en América Latina.

"Puede que la información de una sola persona no sea llamativa, pero, sumada a los de otras 100, se vende por 30 dólares", explica David Pereira, de Etek International. Estas son las armas preferidas por los cibercriminales.

- El correo falso de la Fiscalía.
- El 'phishing' (correos que aparentan provenir de entidades legítimas y esconden código malicioso) **no es una estrategia nueva, pero sigue siendo de las más usadas.** Según la firma de ciberseguridad VU, es la modalidad de cibercrimen más frecuente en la región.

"El correo va personalizado y es un mensaje de una cita con la Fiscalía en el que adjuntan un PDF. También pueden ser multas de tránsito, y al descargar el archivo ejecutan código para robar datos", explica Pereira.

- Recomendación: **no abra enlaces de desconocidos y verifique que la dirección de correo sea legítima** (por ejemplo, fiscalia.gov.co).

'Malware' en móviles: **Los atacantes modifican una 'app' para que se asemeje a otra.** Le inyectan un código y la suben con nombres ligeramente cambiados. De este modo pueden robar contraseñas, tomar fotos, espiar o hacer grabaciones. Según Dmitry Bestuzhev, director de investigación en Latinoamérica de Kaspersky, "van a ser los nuevos dueños del teléfono, sin que el verdadero lo sepa".

Otra táctica común es el envío de mensajes que proponen juegos. Al contestar, el usuario se suscribe sin saberlo a un servicio de mensajería que le hace cargos a su factura.

- Recomendación: implemente la doble autenticación en las redes y revise los permisos que se les dan a las apps.

Redes wifi públicas: Buscar acceso al wifi gratuito de un restaurante o un café puede ser riesgoso. "Un atacante podría manipular el tráfico de red (o sea, la navegación de la víctima) y tener acceso a los datos", explica Bestuzhev.

- Recomendación: **cuando acceda a una red pública, no realice transacciones y nunca ingrese la información de inicio de sus redes.**

'Ransomware': La técnica de 'secuestrar' archivos para pedir un rescate ha tomado fuerza luego de ataques como Wannacry, que afectaron a varias multinacionales. Según Kaspersky, Brasil, México y Colombia lideran la lista de países latinoamericanos más afectados por este fenómeno. De acuerdo con Andrés Galindo, de Digiware, **el aumento de estos ataques se ve potenciado por los avances tecnológicos.** "El mundo se está digitalizando y cada vez está más interconectado. Eso implica que los ataques sean más potentes", dijo.

- Recomendación: realizar copias de respaldo de la información de todos los dispositivos y NO pagar el rescate.

Criptomonedas: **Las criptomonedas no son ilegales, pero, al no estar reguladas, son usadas para acciones ilegales,** explica Giusto. "Las usan para comprar herramientas que son fraudulentas, para alquilar servicios ilegales o para recibir dinero de víctimas que han sufrido algún ataque. Con su existencia se está propiciando el cibercrimen", afirma.

- Recomendación: no ceda a extorsiones que le exijan pagar con bitcoines.

Resumen tomado de: eltiempo.com, Tecnosfera, 22 de octubre de 2017 http://www.eltiempo.com/tecnosfera/novedades-tecnologia/las-tacticas-preferidas-por-los-cibercriminales-143368.

CONOZCAMOS NUESTROS PRINCIPIOS...

Tecnología en Sistematización de Datos

Visión:
El proyecto curricular de Tecnología en Sistematización de Datos deberá consolidarse como un programa académico de reconocimiento local, nacional e internacional, caracterizado por el aporte permanente al desarrollo tecnológico e investigativo, soportados en el uso de las herramientas tecnológicas suficientes para mantenernos ubicados en la frontera del conocimiento de los sistemas modernos de procesamiento y transmisión de información

Misión:
Formación de Tecnólogos íntegros, críticos e idóneos, altamente calificados en el área de los sistemas informáticos, capaces de identificarlos y mejorarlos empleando la ciencia y la tecnología para optimizar su funcionamiento.

Ingeniería en Telemática

Visión:
El proyecto curricular de Ingeniería en Telemática deberá consolidarse como un programa académico de reconocimiento local, nacional e internacional, caracterizado por el aporte permanente al desarrollo tecnológico e investigativo, soportado en la capacidad de convertir sistemas convencionales de comunicaciones en otros que puedan calificarse de avanzados, tanto por sus características teleinformáticas actuales como por sus proyecciones de mejoramiento y crecimiento.

Misión:
La misión del Proyecto curricular de Ingeniería en Telemática constituye la formación de profesionales con un alto nivel académico e investigativo, humanamente formados, científicamente fundamentados y tecnológicamente calificados en el área de telemática, capaces de servir a la sociedad y dar soluciones convenientes a sus requerimientos y necesidades mediante la creación, desarrollo y adaptación de tecnologías, promoviendo el cambio y la innovación

La seguridad es un tema estratégico.

La transformación digital está impulsando a las empresas a adoptar la nube, el Internet de las Cosas (IoT), el big data y otras iniciativas digitales en oleadas cada vez mayores, obligándolas a reinventar y automatizar todo, desde la toma de decisiones hasta el servicio al cliente.
Con estas oportunidades vienen nuevos desafíos de ciberseguridad. La amenaza es real. Gartner prevé que el 60% de las empresas sufrirán grandes fallas de servicio debido a la incapacidad de los equipos de seguridad para gestionar el riesgo digital. Parte del problema gira en torno al hecho de que la seguridad no es vista como un problema de negocio crítico por los altos ejecutivos y miembros del consejo directivo.

Ciberseguridad, no es todavía un foco de la alta dirección

Este tema se enfatiza en nuestra Encuesta Global de Seguridad Empresarial. Al encuestar a más de 1.800 tomadores de decisiones en tecnología informática, Fortinet encontró que aproximadamente la mitad de los encuestados cree que la seguridad todavía no es una discusión de máxima prioridad para la junta directiva. Al mismo tiempo, sostienen fuertemente que la ciberseguridad debe convertirse en una prioridad de la alta dirección, con el 77% de los encuestados indicando que la junta tiene que poner la seguridad de TI bajo un mayor escrutinio.

Se podría asumir que ha habido un alza sustancial en el interés de los altos ejecutivos en la ciberseguridad como resultado de algunos de los ataques de seguridad más recientes y de las terribles implicaciones que tuvieron en las empresas víctimas. Sin embargo, aunque las juntas directivas reaccionan cuando ocurren ataques de seguridad, sus acciones son generalmente reactivas y no preventivas. Específicamente, los altos ejecutivos parecen estar más implicados en la gestión posterior a la violación que en la prevención. Por ejemplo, el 77% de las juntas directivas exigen saber qué sucedió después de que ocurre un evento de seguridad y el 67% revisa o aumenta los presupuestos de seguridad. Los líderes de seguridad todavía tienen mucho trabajo por hacer en la priorización de la seguridad a nivel de la junta directiva.

Ninguna organización es inmune a la amenaza de violaciones, ataques de ransomware o interrupciones operacionales. Las empresas de todo tamaño y forma, así como todos los segmentos de la industria, son objetivos. Los hallazgos de la encuesta de toma de decisiones de TI de Fortinet corroboran esto. El 85% de los encuestados sufrió una violación de seguridad en los últimos dos años y casi la mitad reportó un ataque de malware o ransomware.

Por qué la ciberseguridad va en camino a convertirse en una prioridad

Hay una serie de factores que están llevando a las juntas directivas, altos ejecutivos y responsables de TI a hacer de la ciberseguridad una prioridad en el 2018. Aquí algunos de los aspectos más significativos:

Violaciones de seguridad y ataques globales. La gran mayoría de las organizaciones han experimentado algún tipo de violación o ataque de seguridad en los últimos dos años. El 49% de los encuestados dijeron que sus organizaciones aumentaron su enfoque en la seguridad después de un ataque global como WannaCry. El aumento de la publicidad y la concientización, junto con las implicaciones sobre la reputación de la marca y las operaciones del negocio, pone a estos problemas al nivel de la dirección en lugar de ser solamente responsabilidades operativas de TI.

Superficie de ataque. La adopción de la nube, la aparición del IoT y el crecimiento del big data expanden tanto la superficie de ataque como su complejidad. El 74% de los encuestados indica que la seguridad en la nube es una prioridad creciente para sus organizaciones. La mitad dice que sus organizaciones planean inversiones en seguridad en la nube durante los próximos 12 meses. IoT es otro gran factor cuando se trata de la superficie ataque en constante expansión, se prevé que el número de dispositivos IoT conectados aumentará a más de 8,4 billones a finales de año, según Gartner. De éstos, 3,1 billones pertenecen a empresas. Como muchos dispositivos IoT son difíciles de proteger, los expertos predicen conjuntamente que más del 25% de todos los ataques de seguridad apuntarán a los dispositivos IoT para el 2020.

Cumplimiento regulatorio. Las nuevas regulaciones de gobierno y de industria también están aumentando la relevancia de la seguridad en el negocio. El 34% de los encuestados indicó que estas regulaciones aumentan la conciencia de la seguridad por parte de la junta directiva. La aprobación del Reglamento General de Protección de Datos en la Unión Europea, que entrará en vigor en 2018, es un ejemplo.

Estas tendencias están obligando a considerar la ciberseguridad como un asunto clave dentro de la estrategia más amplia de gestión de riesgos de una organización, en lugar de una simple inversión en tecnología.

Para tener éxito en sus esfuerzos de transformación digital, los líderes de seguridad de TI deben repensar su enfoque de ciberseguridad con el objetivo de extender la visibilidad a través de la superficie de ataque, acortar la ventana de tiempo entre la detección y la mitigación, ofrecer un rendimiento robusto, y automatizar la inteligencia y la administración de la seguridad.

Resumen tomado de: https://computerworld.co, *Patrice Perche, vicepresidente ejecutivo sénior de Ventas Globales y Soporte de Fortinet,* 25 de Octubre 2017.
https://computerworld.co/la-ciberseguridad-es-un-tema-estrategico/

Pare Oreja

Dicen que….

- **Las fechas límite para la captura de notas son:**
  - Segundo corte: Noviembre 18 de 2017.
  - Examen final: Diciembre 9 de 2017**.**
- **Finalización del segundo semestre:** Noviembre 18 de 2017.

Link de Interés:

- **¿Por qué la computación de alto rendimiento está creciendo en diferentes sectores?**
- https://www.elespectador.com/tecnologia/por-que-la-computacion-de-alto-rendimiento-esta-ocupando-nuevos-sectores-en-la-sociedad-articulo-719588

- **¿Qué es, cómo funciona y qué hacer para protegerse de Krack, la falla que ataca las redes Wi-fi?**

- https://www.elespectador.com/tecnologia/que-es-como-funciona-y-que-hacer-para-protegerse-de-krack-la-falla-que-ataca-las-redes-wi-fi-articulo-718559

- **Cómo convertir texto en audio utilizando Bloc de notas**

  http://computerhoy.com/paso-a-paso/software/como-convertir-texto-audio-utilizando-bloc-notas-67351

SI QUIERES FORMAR PARTE DE LA ELABORACIÓN DE ESTE BOLETÍN PREGUNTA EN LA COORDINACIÓN DE LA CARRERA tecsistematizaciondatos@udistrital.edu.co