CIBERSEGURIDAD: más que una moda

Los problemas de seguridad de la información se remontan a los orígenes de la civilización, cuando se inició la escritura y los individuos sintieron la necesidad de mantener su información sensible en secreto.

El nacimiento de la computación en el siglo pasado trajo consigo una mejora significativa en los procesos que los individuos y las organizaciones llevaban a cabo. En sus inicios, la seguridad de la información que almacenaban y procesaban las computadoras se limitaba a restringir el acceso a los edificios donde se alojaban los centros de procesamiento donde estaban ubicados esos grandes equipos de cómputo.

Más allá del cómputo, lo digital habilita el almacenamiento y la comunicación de datos. Al avanzar la tecnología, en las últimas dos décadas del siglo XX, la informática llega a los hogares y a la mayoría de las organizaciones. Con ello, surge la necesidad de conectar los equipos para compartir información y para facilitar los procesos: nacen las redes de computadores y con ellas la Internet.

Con el desarrollo de las redes de computadores aparece un nuevo reto: ya no es suficiente tener la seguridad de la información circunscrita a la seguridad física de un centro de procesamiento de datos, sino que ahora es necesario proteger también la información que es transportada a través de redes de computadoras. Así, al arrancar el siglo XXI, empezamos a hablar de **ciberseguridad**.

La seguridad de la información es la protección de todo tipo de información, sin importar su ubicación o el medio en que esta se encuentre. La ciberseguridad es parte de la seguridad de la información, pero se refiere a aquella información que compartimos por medio de redes de computadoras y, principalmente, cuando es expuesta en Internet.

Internet nació neutra, como una 'red de redes', sin mayor seguridad: cualquiera puede conectarse a ella. Por ser abierta, actores malévolos pueden aprovechar las debilidades de seguridad de Internet para perpetrar ataques contra otros equipos que estén conectados a dicha red.

La ciberseguridad procura introducir seguridad en un ambiente que - por su naturaleza - es inseguro. Se requiere blindar la información que compartimos en la red, dependiendo de sus grados de sensibilidad y confidencialidad.

Desde hace un par de décadas, la preocupación por garantizar razonablemente la seguridad de la información que compartimos ha hecho imperativo formar y capacitar a profesionales que puedan llevar a cabo las tareas de fortalecimiento de la ciberseguridad de la información.

¿Por qué está de moda el término 'Ciberseguridad', si tenemos muchos años de luchar y combatir en esta guerra en el ciberespacio? La respuesta es simple: el ser humano es muy propenso a pensar que a nosotros nunca nos va a pasar algo similar a lo que vemos en otras latitudes. Hasta que tenemos un ataque real, que paraliza muchos de los procesos del país, sentimos que somos parte de una ciberguerra.

Soren Skou, CEO de Maersk, refiriéndose al ataque que sufrió hace pocos años esa multinacional, nos recalca que "hasta que usted no haya experimentado algo como esto, no se da cuenta de lo que puede suceder, de lo grave que puede ser. No tenía una idea de cómo seguir adelante".

Así de serio puede ser un ataque y lo hemos experimentado en nuestras instituciones; no ha sido algo que pueda recuperarse en un par de días: han pasado semanas y aún existe incertidumbre de cuándo se volverá a la normalidad.

El golpe que le dio a la humanidad la pandemia hizo ver que la mayor parte de las organizaciones, sin importar su tamaño, no contaba en su gestión de riesgos la continuidad operativa (si es que tenían una gestión de riesgos). El peligro de sufrir ciberataques debe ser una prioridad importante en la gestión de riesgos de toda organización. Debemos estar preparados y saber cómo actuar si somos atacados, a fin de garantizar el funcionamiento de empresas e instituciones.

Nunca se debe bajar la guardia. Si no hemos sido víctimas de un ciberataque, no sabemos si es porque nuestras defensas son suficientemente robustas o porque no hemos estado en la mira de los ciberdelincuentes.

Tanto las organizaciones como los individuos ven hoy, más que nunca, la necesidad de contar con sistemas de defensa que coadyuven en la seguridad de la información, principalmente aquella que se considera confidencial.

Nuestro sistema primario de defensa es el más sencillo y el que menos inversión requiere: es capacitarnos, tomar conciencia de que la seguridad empieza en nosotros, en estar alertas, en no brindarle a nadie información con la que pueda vulnerar nuestras cuentas de correo, bancarias, entre otras, además de contar con contraseñas robustas. Entre los principales consejos para fortalecer las contraseñas se recomienda que sean de al menos 10 caracteres, incorporando números, letras, caracteres especiales, sin incluir nombres o fechas. Las claves y las contraseñas no deben ser compartidas con nadie más, ni escribirlas en lugares que tengan acceso otras personas. Las contraseñas deben ser cambiadas con regularidad y - en la medida de lo posible – ser complementadas con otros factores de autenticación, como enviar claves de un solo uso a nuestro correo o celular, usar certificados digitales, recurrir a medios biométricos que robustezcan los procesos.

Los delincuentes cibernéticos buscan primero romper la línea de defensa más débil: los individuos que mantienen en sus computadoras información sensible (números de cuenta, de tarjetas, información personal, entre otros). Como trabajadores en las organizaciones, tenemos acceso a la información sensible corporativa y de sus socios comerciales o clientes. El ataque a los individuos para hacerlos caer en error y brindar información privilegiada es conocido como ingeniería social.

Los atacantes siempre han existido, no es nada nuevo. Cada día intentan infiltrarse en formas novedosas. Un porcentaje alto de ataques corresponden a personal interno de las organizaciones que facilitan o perpetran los ataques. No podemos confiar en nadie, los sistemas deben mantener la consigna de cero confianza.

Uno de los ataques que cobrado fuerza en la vida diaria es conocido como ransomware. Este consiste en un secuestro de la información que está en nuestros computadores o en los servidores de la organización. El atacante logra acceso a la información y la cifra o encripta (la pasa a una forma que requiere de una llave para poder acceder a la información) y pide un rescate para proveer la llave que vuelva a abrir esa información. En algunas ocasiones, copia la información y amenaza con publicarla si no llevamos a cabo el pago. Para este tipo de ataque lo mejor es tomar previsiones, reforzar nuestras defensas y estar alertas para no caer en los engaños del delincuente. Si esto fallara, debemos tomar dos sencillas medidas de seguridad: mantener encriptada la información sensible y tenerla respaldada. Si llegaran a robarnos o a secuestrar nuestra información, no podrán publicarla pues estará en un formato incomprensible para quien no tenga la llave y, por otro lado, si nos encriptan la información, tenemos un respaldo que nos permite recuperarla a partir de la copia que tenemos guardada.

La ingeniería social es el método preferido por los ciberdelincuentes para tener acceso a nuestra información y poder utilizarla para atacarnos o estafarnos. Puede tomar la forma de un mensaje de correo electrónico o de una llamada telefónica, en que intentarán ponernos en una situación de urgencia para que caigamos en la trampa y les brindemos información. También pueden llevarnos a una página de una organización luce idéntica a la original, pero es falsa (esto se conoce como phishing), en la cual intentarán que digitemos nuestras credenciales para robarlas y con ellas perpetrar su ataque.

Debemos mantenernos alertas, verificar la procedencia de todo correo o mensaje que nos llegue, desconfiar de las ofertas que llegan a nuestros correos o celulares, en que nos solicitan información o nos envían una dirección de red para que ingresemos datos. Prefiramos digitar nosotros la dirección de red de nuestro banco o de la página de cualquier empresa donde necesitemos ingresar para realizar alguna transacción, nunca confiemos en las direcciones que nos mandan.

La ciberdelincuencia ha estimulado que varias universidades se aboquen a formar especialistas en ciberseguridad. Hoy en día existen más de veinte especializaciones profesionales diferentes en este campo: inteligencia de amenazas, hackeo ético, respuesta a incidentes, investigación forense, seguridad en la nube, son algunas de las especializaciones.

En Costa Rica algunas universidades están preparando profesionales en ciberseguridad. Como parte de su labor social, ciertas universidades cooperan con el país ofreciendo charlas y talleres, frecuentemente gratuitos o a muy bajo costo – a fin de sensibilizar y alfabetizar a los ciudadanos y a las organizaciones en cuanto a los riesgos que tienen la información y nuestras vidas, ante ciberataques.

Los profesionales especializados pueden apoyar a las organizaciones para establecer y fortalecer las defensas contra los ciberdelincuentes. La Universidad Cenfotec ofrece programas educativos en Ciberseguridad desde el 2012: carreras técnicas, planes de estudio a la medida de las organizaciones para capacitar a sus funcionarios en estos campos, cursos profesionales conducentes a certificaciones internacionales y la primera Maestría en Ciberseguridad de la región centroamericana (desde el año 2014). El TEC abrió, en abril de este año, una Maestría Profesional en Ciberseguridad – con cursos bimestrales. La Universidad Fidélitas ofrece una carrera de grado: Bachillerato en Ingeniería de Seguridad Informática. La Ciberseguridad es promovida en los gremios profesionales y empresariales por el Colegio de Profesionales en Informática y Computación, el Capítulo Costa Rica de la Asociación profesional ISACA y la Cámara Costarricense de Tecnologías de Información y Comunicación. La Organización de Estados Americanos (OEA) ofrece regularmente capacitación en Ciberseguridad a entidades públicas en América Latina y el Caribe. El Banco Interamericano de Desarrollo (BID) ha estimulado el desarrollo de programas especializados de formación o capacitación en Ciberseguridad en varios países latinoamericanos y del Caribe– con el apoyo de la Universidad Carlos III de Madrid (UC3M).

Agradecimiento

Ing. Miguel Pérez Montero, M.Sc., es Fiscalizador en la Contraloría General de la República, fue Consultor del Programa de las Naciones Unidas para el Desarrollo, Director de Informática, Empresario y Gerente de empresas tecnológicas e Ingeniero de Sistemas en el Banco Nacional y en Recope. Miguel es Director de la Escuela de Ciberseguridad de la Universidad Cenfotec y Profesor de su Maestría en Ciberseguridad. Miguel es Auditor de Ciberseguridad y de Sistemas de Información y cuenta con varias certificaciones profesionales.

Ing. Ignacio Trejos Zelaya,M.Sc. es profesor de Informática en el Instituto Tecnológico de Costa Rica y en la Universidad Cenfotec. Su investigación se centra en Lenguajes de programación, Ingeniería del software y Educación en Informática. Es Representante de Costa Rica en el Consejo Hispanoamericano de Pruebas de Software (HASTQB). Ignacio es Ingeniero Certificado en Calidad.