Realidad Empresarial
Administración • Mercadeo • Finanzas • Operaciones

Realidad Empresarial N° 19, Especial 2024, pp.43-50
URL: https://revistas.uca.edu.sv/index.php/reuca/index
ISSN 2789-2689 (en línea) - ISSN 2415-5721 (impreso)

Ensayo

Cuando la escuela no nos alcanza....

When school doesn't reach us....

DOI: https://doi.org/10.51378/reuca.vi19.8713

Fecha de recibido: 12 de junio de 2024
Fecha de aceptado: 17 de septiembre de 2024

Elisa Cristina Aldana Calderón
Académica
Universidad Centroamericana José Simeón Cañas
ealdana@uca.edu.sv
ORCID: https://orcid.org/0009-0006-6764-6000
El Salvador

Resumen

Actualmente, ciberseguridad es una palabra en auge de la que hay muchas interpretaciones como: defender, cuidar, proteger, entre otras. Pero, ¿qué es lo que debe protegerse? ¡Nuestra información!, muchas veces, los datos personales se ven expuestos a terceros ya que no se les otorga el valor que deberían a su uso en la web, o sencillamente no se sabe cómo protegerlos. Diariamente los noticieros presentan ejemplos de distintas clases de ataque cibernético, tales como: robo de credenciales, malware, phishing, ransomware, entre otros. Los ciberdelitos avanzan de un ámbito personal al empresarial. No tener conciencia de la importancia de proteger nuestra información puede ocasionar problemas en los ambientes laborales, donde las medidas de seguridad tienen que ser más estrictas para evitar robo de datos, caída de servicios, pérdida de equipos y hasta secuestro, o privación pérdida definitiva de la información de la empresa, golpes tan grandes de los que en muchos casos las instituciones no se recuperan fácilmente. En este artículo se exponen las razones que debieran movernos a proteger nuestra información personal, se examina algunos de los ciberdelitos más frecuentes en el hurto de información privada, profundizando en tres de ellos. Este es un artículo de opinión basado en la revisión de bibliografía sobre el tema. Los conocimientos y datos que se exponen son de conocimiento público, pero dirigidos a una comunidad de aprendizaje que vive inmersa en el uso de redes sociales y plataformas virtuales, por tanto, expuesta a los ciberdelitos; personas que necesitan conocer las formas en que actúan los ciberdelincuentes para poder protegerse a título personal, institucional o empresarial.

Palabras claves: seguridad, protección de datos, cibernética. Security, Data Protection

Summary

The word cybersecurity is booming these days, and we find many definitions of this word such as: defend, care for, protect, etc. But what is it that we must protect? Our information. Many times we lose our data because we do not give it the true value it has or we do not know how to do it! We see in the news that we are presented with different attacks day after day, for example: credential theft, malware, phishing, ransomware, among others. Cybercrimes advance from a personal to a business environment. Not being aware of the importance of protecting our information can cause problems in work environments, where security measures have to be stricter to avoid data theft, service failure, loss of equipment and even kidnapping and permanent loss of company information, which in many cases have been major blows where institutions are not easily recovered. In this article we will explain the reasons that will move us to take care of our personal information, we will examine some of the most frequent cybercrimes that are used to obtain private information and we will delve into three of them. This is an opinion article based on a review of the literature on the subject. The knowledge and data presented are public knowledge, but are aimed at a learning community that lives immersed in the use of social networks and virtual platforms and is therefore exposed to cybercrime and needs to know the ways in which cybercriminals act so that they can protect themselves personally, institutionally or corporately.

Keywords: security, data protection, cyber. Security, Data Protection

Introducción

Existe hoy un amplio vocabulario que inicia con el prefijo Ciber-, por ejemplo: cibernauta, ciberespacio, ciberproductos y cibercultura. También vemos palabras como ciberseguridad, ciberdelito y ciberdelincuencia.

Algunas personas consideran los términos relacionados con la cibernética como algo que no es tangible y no se puede explicar, otros, sin embargo, como construcciones lingüísticas para definir todo lo que estamos viviendo. Un ejemplo es el acceso a comunicación que existe, pues resulta tan fácil comunicarnos con una persona al otro lado del océano, ya sea por mensajes de texto e imágenes, llamadas y videollamadas, éstas últimas provocan la sensación de cercanía, aunque no haya contacto físico, se dice que están ciberconectados.

Estos avances que datan de mediados de los 80, cuando la tecnología era accesible solo para algunos. Con el tiempo, se fue expandiendo hasta llegar al punto en el que estamos: ciberconectados; sumergidos en tecnologías que hace diez años solo eran un sueño. Ahora es tan real que la utilizan los niños, ya no es un privilegio de algunos adultos está al alcance de todos, desde una persona de 90 años hasta el bebé de 5 meses; yno solo para el ser humano, también se desarrollan herramientas y aplicaciones que ayudan a entretener a las mascotas. Es por eso que este ensayo busca exponer los ciberdelitos más frecuentes en el ciberespacio, además de crear conciencia sobre la importancia de proteger los datos personales.

Nuestro entorno personal

Cada vez es más necesario estar conectados a internet, con el fin de informarse sobre noticias, tendencias, estudiar u otras actividades de entretenemiento; ya que puede encontrar cualquier tema en la red. Por mucho tiempo, navegar en el ciberespacio no implicaba ninguna situación desagradable, se vivía en un ambiente, como de leyenda, es decir en completa armonía.

Pero lo cierto es que el uso de internet se popularizó facilitando para la gran mayoría de personas, empresas, instituciones educativas de todos los niveles y hasta el gobierno, el uso de muchas herramientas, no solo Google, Wikipedia, YouTube, sino correos electrónicos, almacenamiento en la nube, al punto que las empresas ya no necesitan tener físicamente un área de servidores en sus edificios para brindar sus servicios. Esto llamó la atención de personas curiosas que vieron como un reto eludir las medidas de ciberseguridad. Al principio, quizás era por diversión, pero después las acciones adquirieron un efecto negativo, provocando distintos grados de daño, no físico, llegando incluso a comprometer sus bienes.

De esta manera se introduce el concepto de ciberseguridad, que se define a continuación:

Según la empresa internacional Kaspersky, especialistas en ciberseguridad, se define como: "la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos". (Kaspersky, 2024)

Ya no es solo la computadora la que se debe de proteger, sino todo su entorno, y así existen múltiples definiciones, todas resumidas en defender, cuidar, proteger y mitigar los daños potenciales.

Sin embargo, surgen interrogantes como: ¿Soy propenso a recibir un ataque? ¿Por qué debo tomar precauciones?

> La importancia de proteger los datos personales, según el (Instituto de Acceso a la Información y Protección de Datos Personales de Quinta Roo [IDAIPQROO], (2024) es directamente para: evitar que los datos sean utilizados para una finalidad distinta para la cual la proporcionaste y con ello se afecten otros derechos o libertades; así como para evitar la comisión de delitos en tu contra, tal como el robo de identidad" (Instituto de Acceso a la Información y Protección de Datos Personales de Quintana Roo [IDAIPQROO], 2024).

Es evidente que la identidad y los datos personales son valiosos y deben protegerse. Esto también se aplica a la información que poseen las empresas sobre sus clientes y empleados, así como a las instituciones gubernamentales.

La ciberseguridad surge como una reacción a los ataques que se presentaron a algunas empresas con la finalidad de evidenciar algún error en sus configuraciones, o bien para sustraer datos, modificarlos o eliminarlos. Así puede enlistarse una cantidad de ataques diarios a nivel mundial.

En algunos casos hay carencia de estadísticas certeras debido a que no se reportan, tal es el caso de Facebook, en donde si la cuenta es hackeada a veces se reporta y otras veces las personas la dan por perdida. Pero ¿por qué no luchamos por recuperar nuestra información?

Será por falta de interés, desconocimiento, o porque no se logran valorar adecuadamente los datos personales que se comparten en la Web. Y esta cadena se complica cuando se ve en las empresas, dado que las instituciones, privadas y públicas, invierten mucho en aplicaciones, equipos, antivirus, firewall, servidores, capacitaciones, sin embargo, de igual modo sufren ataques cibernéticos de gran impacto.

Algo que debe de aclararse y tener por seguro, es que nada es completamente infalible; ninguna empresa puede garantizar que nunca va a sufrir un ataque, ya que los movimiento del mercado presentan cambios en la seguridad de un minuto a otro. Las razones pueden ser varias: apareció un nuevo virus, surgió una brecha de seguridad y debe instalar la actualización para evitar un ataque al servidor de la empresa o su celular le está indicando que tiene que actualizarlo, debido a que se ha presentado una vulnerabilidad. Hoy en día su celular es su oficina, en muchos casos todo lo que necesita para trabajar está en ese dispositivo y por ende es blanco de ataques para los hackers.

Aunque tengamos una lista de los posibles ataques a los que somos susceptibles y estemos prevenidos para ellos, siempre habrá problemas con diferentes amenazas, unas en mayor escala que otras en las cuales hay una incidencia directa de una persona, por ejemplo: un clic donde no se debía, abrir un correo malicioso, entrar a sitios que no son seguros, entre otros.

En algunas literaturas sobre el tema de ciberseguridad se menciona que el eslabón más débil, en el proceso, es el ser humano, que se puede tener lo último en tecnología, pero si las personas no son conscientes del tema de seguridad, ese eslabón siempre será el más vulnerable.

Debe tenerse en cuenta que hacer conciencia no es sinónimo de amenazar o adoctrinar en el sentido que si no siguen indicaciones tendrán consecuencias. Se trata de educar, de que las personas entren en un proceso de reflexión y deconstrucción de un nuevo valor: ***proteger la información***.

Durante la niñez se aprenden normas en casa, en la escuela se aprende el abecedario y finalmente la lectura, matemáticas, ciencias, historia; sin embargo, la escuela no enseña el valor de la información personal, al menos no de momento. A lo largo de la vida la información hace su aporte a formar la identidad en las personas, desde el aprendizaje de su nombre, en donde vive, quienes conforman su núcleo familiar, hasta las calificaciones y logros que se suman al expediente académico, que luego se vuelve una parte primordial en la vida de cada persona.

Actualmente, los datos personales quedan expuestos, no existe plena conciencia de las medidas que deben tomarse para no caer en los diferentes tipos de ataques cibernéticos existentes.

Algunos tipos de ataques

Malware: un programa malicioso, que se instala en una computadora, celular, tablet y desconfigura, deshabilita o daña los equipos, según la página de WatchGuard "en el 2023 se tuvo 1,000 millones de malwares activos" (WatchGuard, 2024), convirtiéndose en una de las tres modalidades más populares de ataques; dentro de los malwares hay diferentes categorías.

Phishing: el objetivo de esta práctica es hacer que la víctima revele información personal como credenciales de acceso a un sistema, información financiera, entre otros datos. Se busca engañar a la persona para que ejecute una acción, que suele terminar en dar acceso a información confidencial, por ejemplo, envían un correo electrónico a la víctima, donde le indican que dé clic a un enlace para verificar sus datos personales, debido a que se ha registrado una actividad irregular en su tarjeta de crédito, y la persona da clic, llena el formulario y le roban los datos. Estos casos son tan frecuentes que para el año 2023 se reportó: "14.261 incidentes" (Instituto Nacional de Ciberseguridad de España [INCIBE], 2024) relacionados con este tipo de fraude y no solo utilizando correo electrónico, sino por mensajes de texto, WhatsApp, llamadas, entre otros.

Ransomware: consiste en un programa que encripta los archivos de cualquier dispositivo, "es un tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y exige el pago de un rescate

para recuperar el acceso. Aunque algunas personas podrían pensar que un virus bloqueó mi ordenador, el ransomware se clasificaría normalmente como una forma de malware distinta de un virus" (malwarebytes, 2024) Esto se analizará en profundidad más adelante.

Pero el usuario común, que es víctima de este tipo de secuestro, debe estar consciente que una vez cifrados los archivos la probabilidad de recuperarlos es ínfima. .

Los ataques cibernéticos se auxilian incluso de los dispositivos que forman parte de IoT (internet de las cosas) que pueden ser cámaras y sensores que se instalan en las casas para vigilar, entre otros, para robar información. Se acostumbra conectar sin revisar las configuraciones que por defecto traen estos dispositivos, pero al hacerlo se expone información familiar y personal.

Los ataques a nivel empresarial

Los ataques cibernéticos no solo se presentan a nivel personal o familiar, se presentan también en empresas, instituciones educativas de todo nivel, instituciones financieras y de gobierno. En algunos casos, las consecuencias han consistido en la pérdida de millones de dólares.

En este punto deben quedar en claro las aristas que cubre la ciberseguridad: servidores, aplicaciones móviles, sistemas informáticos, redes, computadoras, tabletas, sensores, dispositivos, sitios web, firewall, nube, correo electrónico, todo lo que de una forma u otra recolecta, procesa, guarda y elimina información. Además, tomar en cuenta la parte de riesgos en la cual puede encontrarse una gran variedad de situaciones que se describen a continuación.

El estudio profundiza en tres tipos de ataque: primero, el Ransomware que en 2023 fue una de las modalidades que más se disparó; el malware encripta los archivos de una empresa, detiene por completo la producción de la misma y para liberarla se exige el pago de un rescate. Según la página de Panda mediacenter (2023) en los últimos años se ha llegado a tener alrededor de "4,000 ataques por día" y llega a pérdidas que rondan los "400 millones de dólares en todo el mundo" (Panda mediacenter, 2023), como consecuencia de la pérdida de la información. Se pueden presentar dos situaciones cuando no se paga el rescate en los Ransomware: la primera, usted no paga el rescate de la información y nunca la recupera; la segunda, dependiendo del tipo de información que maneje, si no paga, entonces los datos se hacen públicos, causando una variedad de daños, como daño reputacional para la empresa, porque después de ese acontecimiento será difícil que las personas puedan confiar nuevamente en la institución, la recuperación de toda la información que se perdió, que en algunos casos no se puede reconstruir, porque ya no se tienen los documentos de donde se tomaron los datos y por supuesto, el daño a las personas que han visto vulnerada su privacidad. Por ejemplo, si es un hospital el que ha sufrido este tipo de ataque, el secuestro de los expedientes médicos ocasiona un gran problema para el paciente al no poder dar seguimiento a un tratamiento, respuesta de exámenes o su historial como tal. Los Ransomware, como mencionaba la página Panda mediacenter (2023), van en aumento, nuestro país ha sido víctima de estos secuestros, por lo que las medidas para prevenirlos se hacen urgentes y de carácter obligatorio.

El segundo tipo de ataque de especial atención es el ***phishing***, al igual que el Ransomware buscan una forma de entrar a los sistemas de las empresas para después capturar datos. Comúnmente engañan a las personas y no a los sistemas de seguridad. Se hacen pasar por un familiar, un jefe, el representante de una empresa para que la víctima entregue la información requerida, aquí también entran en acción los ataques de ingeniería social que buscan de diferentes formas conseguir información para llegar a su objetivo y aunque en algunos casos no puede imaginarse lo que hacen los hackers, en la gran mayoría, mediante estudios, se definen los pasos que siguen para conseguir información. Algunas películas lo han puesto en evidencia, por ejemplo en una película se presenta el caso que están buscando en la basura de una casa y lo que encuentran ahí son los estados de tarjetas tirados sin triturar, el papel, recibos de servicios básicos, los cuales después son usados en contra del protagonista; eso le puede pasar a cualquier directivo de una empresa porque es un blanco y un punto de acceso a la información de esa empresa.

Un tercer ciberdelito muy particular para las instituciones es el DDoS (Ataque de Denegación de Servicios Distribuidos), el cual consiste en atacar los sitios web y lanzar cientos, miles de peticiones de múltiples fuentes de manera que el servidor no pueda responder y termina colapsando, "el atacante inunda un servidor con tráfico de Internet para evitar que los usuarios accedan a servicios y sitios en línea conectados" (Fortinet, 2024). El usuario común percibe que la página no se muestra o no termina de cargar la información, sin embargo, actualmente la caída de un sitio web se refleja en perdidas monetarias porque la gran mayoría de personas hace transacciones en línea, y si no está habilitada la banca en línea de una institución financiera ocasiona pérdidas para el banco, clientes y empresas, ya que paraliza por completo las operaciones.

Los delitos como el phishing, el DDoS y el Ransomware son la causante del papel protagónico que ha tomado la ciberseguridad tratando de cubrir todas las áreas posibles para proteger la información. Sin embargo, a pesar de la probada importancia que tiene la seguridad, en muchas ocasiones cuando se desarrollan diferentes productos tecnológicos, el presupuesto o valor que se le da al tema es mínimo, lo que más adelante ocasiona problemas.

Una de las áreas que ha tomado fuerza dentro de la ciberseguridad es la parte del análisis de los riesgos, no pretende predecir el futuro, sino poder tener opciones para afrontar diferentes situaciones, para mantener la continuidad del negocio. Un ejemplo palpable y real fue la pandemia: muy pocas empresas estaban preparadas a nivel mundial para continuar sus operaciones en ese escenario. Era inimaginable la idea de abandonar los puestos de trabajo y que los hogares se volvieran el centro de operaciones en pleno confinamiento sanitario, la única idea era tratar de sobrevivir a algo que no mirábamos y que existía. Fue en ese escenario que lastimosamente los ciberataques se incrementaron en un 200 % aproximadamente, fue un proceso lento y doloroso que ayudó a lo que debería de ser una fase que evolucionaría muchos servicios que llevaran entre cinco y ocho años para instalarlos y que todos trabajaran en ellos. Eso, en algunos casos, se aceleró a cumplimentarse en cinco meses , en otros casos, las empresas se vieron forzadas a cerrar porque no se pudieron recuperar de esa pérdida. Por eso es importante analizar los riesgos a los que se enfrenta cada institución y hacer un plan adaptado a las mismas. Esa es una de las muchas ventajas de la ciberseguridad.

¿Pero qué puede hacerse? La respuesta es la misma, educar, hacer que las personas tomen conciencia de su papel en proteger su información del mismo modo que ayudan a proteger la información de otros y tomar participación en las instituciones sobre este tema.

Además, tomar las medidas que estén al alcance de todos para no ser blanco de ataques, por ejemplo, para las personas: se les pide activar la doble autenticación ya que eso permite asegurar la identidad de quien intenta acceder a su información y que está consciente de los dispositivos que está utilizando para realizar esa acción. Algunas recomendaciones para los usos individuales son:

- No se conecte a redes públicas, no conoce realmente quién está detrás de esa conexión wifi que le está ofreciendo internet.
- Utilice contraseñas robustas que no sea una palabra sino una frase y que tenga mayúsculas, minúsculas, números y caracteres especiales.
- Cambie las contraseñas cada cierto tiempo. No las comparta con nadie.
- Actualice sus dispositivos, tanto una actualización del sistema operativo como una de su antivirus.
- Lea con cuidado los correos electrónicos y qué le solicitan, repórtelos si puede, pero no entregue sus datos a nadie, elimínelos para no tenerlos en su bandeja.
- No deje sus dispositivos con las contraseñas que vienen de fábrica, cámbienselas.
- No responda mensajes que le parezcan sospechosos.
- Tenga cuidado al navegar en internet, en especial en ciertos sitios que de primera vista contienen demasiada publicidad.
- Busque los sitios oficiales para la descargar deprogramas

En el caso de las instituciones pueden tomarse las siguientes medidas:

- Mantener todos los sistemas actualizados: instalando las actualizaciones de sistemas operativos y aplicaciones.
- No utilizar librerías que se encuentren desfasadas.
- No utilizar configuraciones por defecto; por ejemplo, rutas que ya vienen por default en los programas.
- Utilizar contraseñas robustas, utilización de algoritmos fuertes para la encriptación de datos.
- Si se tiene servidores físicamente en la empresa, asegurar el área donde se encuentran los servidores.
- Revisar configuraciones de los servidores, tanto físicos como en la nube. Por ejemplo: diferentes niveles de permisos, contraseñas robustas, servicios que no se utilicen, desinstalarlos, tener habilitado solo los puertos en uso, entre otros.
- Chequear los contratos de los servicios que se tengan en la nube y de terceros, cuales herramientas ofrecen en esta área.
- Tener en cuenta niveles de permisos en los usuarios.
- Monitoreo de la red (comportamiento de los dispositivos y firewall).
- Revisión de los logs de los servidores para ver si se ha presentado alguna actividad irregular.
- Tener copia de respaldo de toda la información de su institución
- Tener a personas expertas en el área de seguridad y en especial de ciberseguridad en las empresas.
- Mantener los dispositivos de los empleados actualizados, por ejemplo, el antivirus.
- Capacitar a todo el personal en temas de ciberseguridad con especial atención en temas: de ingeniería social, malware y correo electrónico.
- Identificar los posibles riesgos a los cuales se puede ver expuesto cualquier miembro de la empresa, analizarlos y preparar un plan de cómo minimizar esos riesgos.
- Estar pendiente de publicaciones que se presenten en el área de ciberseguridad con respecto a este tipo de ataques.

Conclusión

En conclusión, es imperante que las personas desarrollen conciencia de lo importante que es proteger los datos, a pesar de no ser algo que se aprende en la escuela pero que ya es parte del día a día en las distintas aplicaciones con las que interactuamos.

De igual manera, los entornos empresariales deben mantener una actualización continua en el tema de ciberseguridad para sus empleados, dado que cada día surgen nuevos tipos de ataques los cuales afectan directamente a las instituciones y la forma de protegerlas es conocer muy bien lo que se tiene y a partir de eso ejecutar acciones puntuales para el resguardo de la información.

Esto es solo una pincelada sobre el gran tema de ciberseguridad, un área en crecimiento y constante evolución que involucra muchas otras de la tecnología.

Referencias Bibliográficas

Fortinet(2024) *¿Qué es un ataque DDoS?* https://www.fortinet.com/lat/resources/cyberglossary/ddos-attack#:~:text=Significado%20de%20ataque%20DDoS,y%20sitios%20en%20l%C3%ADnea%20conectados

Instituto de Acceso a la Información y Protección de Datos Personales de Quinta Roo [IDAIPQROO], (2024) *¡Por tu derecho a la protección de datos personales!* http://www.idaipqroo.org.mx/proteccion-de-datos-personales/

Instituto Nacional de Ciberseguridad (2024). *Balance de ciberseguridad relativo al año 2023*

https://www.incibe.es/incibe/sala-de-prensa/los-incidentes-de-ciberseguridad-de-2023-gestionados-por-incibe-aumentan-en

Kaspersky (s.f.) *¿Qué es la ciberseguridad?* Recuperado el 12 de octubre de 2024, de https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Malwarebytes (2024). *Todo sobre los ataques deransomware* https://www.malwarebytes.com/es/ransomware

Panda mediacenter (2023). *Prevención de amenazas. Ransomware: datos y tendencias que debes conocer para 2023*. https://www.pandasecurity.com/es/mediacenter/ransomware-datos-2023/

WatchGuard (2024). *Cada 39 segundos se produjo un ciberataque en 2023*. https://www.watchguard.com/es/wgrd-news/blog/cada-39-segundos-se-produjo-un-ciberataque-en-2023