Autor: Jorge Orillac

La evolución de la ciberseguridad en las empresas en la era digital

Cada día las amenazas y peligros ante ciberataques son más sofisticados y la ciberseguridad juega un papel crucial.

La protección de su negocio es primordial. Por eso, alrededor del mundo, cientos de empresas invierten importantes sumas de dinero cada año en sistemas de vigilancia, protección y prevención de posibles riesgos a la seguridad y a la continuidad de sus negocios.

Sin embargo, ¿qué sucede cuándo estas transgresiones son invisibles o imperceptibles? ¿Cómo hacer cuando dichos ataques han vulnerado la raíz misma de nuestro negocio mediante una serie de intrincadas redes digitales capaces de capturar datos de importancia crítica? Ahí es donde entra la ciberseguridad.

El tema de la ciberseguridad quizás hace unos quince o diez años, aunque era considerado de importancia, no necesariamente era un punto crucial en la administración de las empresas.

Hoy en día, la realidad es otra. Ya sea una empresa, una firma de abogados o un comercio al por menor, la ciberseguridad se ha convertido cada vez más en un aspecto esencial, ya que cada vez más la sostenibilidad de los negocios depende de sistemas, redes y programas digitales para ser eficientes y llevar el negocio a la velocidad que hoy se requiere para ser competitivo.

Cada día más se capturan datos, ya sea de ventas, facturación de clientes, y en el caso de firmas de abogados o bancos; el manejo y administración de datos sensitivos y confidenciales; lo que convierte a los ataques digitales en verdaderas amenazas para la seguridad y continuidad del negocio.

Para una firma de abogados, por ejemplo, se capturan datos necesarios para una debida diligencia como pasaportes, cartas de referencias bancarias, los roles que las diferentes personas tienen en las sociedades y fundaciones, con lo cual uno tiene por fuerza que tener mayor cuidado.

Es por eso por lo que la ciberseguridad va mucho más allá de lo que uno se solía preocupar.

En el pasado los ataques primordialmente se centraban en la saturación o bombardeo de requisiciones a los servidores, al punto que entraban en cortocircuito colapsando el servicio e interrumpiendo su capacidad de hacer negocios.

Hoy en día la preocupación es más que nada poder retener los datos de manera privada y segura.

De acuerdo con un artículo sobre ciberseguridad de la revista Forbes, el 2020 batió todos los récords en la pérdida de datos por infiltraciones (data breach) así como por una enorme cantidad de ataques cibernéticos a empresas, gobiernos e individuos.

Además, destaca, la sofisticación de amenazas aumentó a partir de la aplicación de tecnologías emergentes como el aprendizaje automático o machine learning, la inteligencia artificial y la tecnología 5G.

> HOY EN DÍA LA PREOCUPACIÓN MÁS RELEVANTE ES PODER RETENER LOS DATOS DE MANERA PRIVADA Y SEGURA

Protección de datos en Panamá

Ante la importancia de este tema, el 28 de mayo de 2021, Panamá reglamentó la Ley 81 de Protección de Datos Personales, la cual establece principios, derechos, obligaciones y procedimientos para regular la protección de datos personales en Panamá, cuya entrada en vigencia se dio el pasado 29 de marzo de 2021, dos años después de su sanción y promulgación en Gaceta Oficial.

Con estas regulaciones se les exige a las empresas que almacenan datos personales o privados de empresas o clientes, que vayan un paso más allá. Esto quiere decir que, no solo debes preocuparte por la protección de datos de tu propia empresa o de la interrupción de tus servicios, sino que debes preocuparte por proteger los datos de tus clientes.

Para conseguirlo es necesaria una gestión proactiva y constante. Una tendencia que ha cambiado con el tiempo. Antes la tendencia era que uno contrataba una empresa de auditoría externa para que revisara anualmente los sistemas o que llevara a cabo pruebas de penetración para constatar si las medidas de seguridad podían resistir un ataque.

Sin embargo, esa prueba arrojaba resultados que te indicaban vulnerabilidades en un período de tiempo. Algo que hoy no es suficiente.

En la actualidad estas pruebas tienen que hacerse constantemente, ya que la tecnología se mueve a una velocidad vertiginosa y del mismo modo, los riesgos y las amenazas.

Los propios hackers, desarrollan nuevas herramientas que van aprendiendo de sí mismas para atacar más inteligentemente; por lo tanto, tienes que tener herramientas de defensa que utilicen también machine learning para que aprendan al mismo ritmo o más rápido; de modo que las posibilidades de defenderte contra esas amenazas sean mayores.

Herramientas de protección

Es saludable que una empresa mantenga evaluaciones anuales de todos sus sistemas, pero es aún más importante adoptar una gestión interna en tiempo real que le permita mantener la seguridad de sus sistemas el resto del año.

Existen herramientas denominadas SIEM (System Information Event Monitoring) las cuales emiten alertas ante cualquier cambio en los sistemas o posibles amenazas por cambios en alguna configuración. Estas herramientas son administradas por un centro de operaciones de seguridad o SOC (Security Operation Center), una empresa dedicada a monitorear las alertas que surjan en tiempo real.

Adicionalmente es recomendable que las empresas cuenten con un sistema de escaneo y parchado de vulnerabilidades, que lleve a cabo una revisión al menos semanalmente.

Mediante este método, como su nombre sugiere, se escanean los equipos de una red dentro de la empresa, y si se advierte que le falta algún parche - de Windows, por ejemplo - que haya detectado una vulnerabilidad se envía y se instala de inmediato.

El factor humano

Una de las mayores vulnerabilidades que existe es el factor humano. Los usuarios con acceso a una red o un sistema dentro de la empresa pueden abrir una puerta a posibles amenazas, como sucede con el uso de las contraseñas.

La tendencia hasta hace poco había sido pedir al personal que utilizara contraseñas seguras, y que las cambiaran con regularidad cada tres meses. Pero, lo que en la práctica termina sucediendo - ante los reiterados llamados a cambio de contraseña - es que los usuarios aplican las mismas contraseñas con ligeras variaciones.

Esto los hace mucho más vulnerables a que tuvieran una sola contraseña robusta y segura, pero se puede evitar con la aplicación de un segundo factor de autenticación, como un token que cambie cada 30 segundos o con un mensaje de texto al celular validado que incluya un código temporal para loguearte en ese momento.

Por eso el tema de las contraseñas protegidas a través de un factor múltiple de autenticación, conocido como multifactor authentication, es lo más recomendable.

Capacitación en ciberseguridad

Cabe destacar que, aunque una compañía tenga todos estos sistemas de vigilancia, si un usuario no está capacitado para reconocer un correo de phishing y con un "click", puede abrir un formulario, poner su usuario y contraseña, y de inmediato enfrentar una amenaza.

Aquí es donde cobra mucha importancia la capacitación constante de los usuarios. Hacer ejercicios conocidos como ingeniería social, en los que se les pone a prueba a través de un sistema con un correo de phishing controlado para ver si lo creen y son vulnerables.

Política Informática

Toda empresa debe contar con una política informática interna que indique para qué se pueden usar los sistemas, cuáles son las políticas de contraseñas, de token, qué se puede instalar y qué no, en las computadoras.

Esta política se enfoca en los usuarios y, en el departamento de tecnología; que la usará como manual para poder aplicar las configuraciones en los sistemas que van de acuerdo con esa política.

Además de esto hacer quincenal o mensualmente estos ejercicios con el usuario para que esté en constante capacitación y en constante estado de alerta de estar pendiente de los correos potencialmente maliciosos.

La realidad es que los correos phishing y las maneras de atacar cambian todo el tiempo por lo cual, todas las empresas deben mantenerse al día, cumplir con las certificaciones nacionales e internacionales en materia de ciberseguridad para ofrecer a los clientes externos la seguridad para sus datos que ellos buscan.

Visita: www.focusalcogal.com