NEXTVISION

Ciberseguridad Inteligente

UNICERO

Creando una cultura cibersegura

Somos unicero. Nuestras organizaciones, nuestra información
y hasta nosotros mismos estamos en dimensiones digitales.
La forma de hacer negocios, inevitablemente, se está transformando.

¿Qué cambios sufrió la ciberseguridad en este proceso?
¿Qué rol ocupa en la toma de decisiones?

nextvision.com

Los ciberataques no paran de aumentar.
Y ante esto, ¿Cómo se están defendiendo las organizaciones?

Actualmente, las organizaciones no han podido igualar a los cibercriminales en efectividad: un ataque tarda entre 2 y 48 horas en tener éxito, mientras que las empresas pueden tardar hasta 200 días en detectar estos ataques, dándole tiempo a los atacantes para desarrollar su estrategia.

Estos son tan sólo un par de ejemplos de las víctimas más famosas del Cibercrimen en los últimos años.

YAHOO!

Perdió datos de 3 mil millones de cuentas de correo, teniendo como consecuencia la disminución de hasta 350 millones de dólares de su valor en su posterior venta a Verizon.

EQUIFAX

Extravió 143 millones de registros de sus clientes, ocasionando el despido del CEO.

Para afrontar este contexto tan complejo en el que el ritmo de los atacantes es mucho mayor que la velocidad de detección y respuesta de las organizaciones, es necesario contar con una estrategia en Ciberseguridad.

Definiendo la Ciberseguridad

Cuando pensamos en definir la Ciberseguridad, el público general puede pensar en varios controles, como firewalls, antivirus, etc; pero en realidad para definir esta disciplina hay que pensar de forma más global: **la Ciberseguridad es la gestión del riesgo para mitigar el impacto de los ataques.**

¿Qué es el riesgo para la Ciberseguridad?

Podemos identificar 3 pilares que componen el riesgo cuando hablamos de Ciberseguridad, que afectan directamente los activos digitales de las empresas: la amenaza, la vulnerabilidad y el impacto.

La amenaza

• Organizaciones de cibercriminales.
• Hacktivistas.
• Estados.

Todos usan distintas técnicas y herramientas para penetrar en las organizaciones: desde ingeniería social, hasta malware y ransomware.

La vulnerabilidad

Las amenazas no surten efecto si no hay vulnerabilidades.

Tenemos que pensar en las amenazas como una lluvia: cada día las empresas se enfrentan a miles y miles de amenazas, cada vez más sofisticadas y difíciles de detectar. En este sentido, para que la lluvia de amenazas no surta efecto es necesario pensar en la Ciberseguridad como un paraguas que mitiga las vulnerabilidades por las que las amenazas se pueden filtrar.

El impacto

Es aquello que ninguna organización quiere sufrir: fraudes, pérdida de patentes, o pérdida de bases de datos de clientes que implican pérdidas económicas, daños a la reputación, y no pocos dolores de cabeza que pueden afectar la continuidad de la organización.

Estos son los componentes del riesgo que tenemos que gestionar. Pero para hacerlo de forma adecuada, es necesario derribar algunos mitos. Veamos algunos:

Mitos de la Ciberseguridad

Mito #1: Los ataques sólo son perpetrados por agentes externos

En realidad, el 70% de las fuentes de todos los ataques provienen del interior de las organizaciones. Irónicamente, el pensar que solo los hackers pueden explotar nuestras vulnerabilidades hace que muchas empresas descuiden sus protocolos de seguridad internos y sean mucho más vulnerables.

Nos enfrentamos a 3 tipos de intrusos internos:

Descuidados o negligentes

Aquellos empleados que toman información a la que tienen acceso y, sin ningún tipo de precaución, la envían a clientes, proveedores o a compañeros no autorizados.

Happy Clickers

Son los empleados que le hacen click a todo correo o archivo que reciben. Este comportamiento provoca que el dispositivo sea capturado por el atacante, dándole la oportunidad de conocer las credenciales de acceso a la red.

“Desleales” o maliciosos

Los empleados que intencionalmente buscan alterar o robar información.

Mito #2: Debo proteger todos los activos por igual

Si bien toda la información de una empresa es crítica y valiosa, no toda tiene la misma importancia, por lo que es importante ejecutar un proceso para clasificar la información, determinar su valor y criticidad para la organización, tomando en cuenta variables como su antigüedad o confidencialidad. Por ejemplo, el plan de marketing del 2018 no tiene la misma importancia que el del 2015. Debemos variar el grado de protección según la influencia que tenga en la continuidad de las operaciones.

Mito #3: La Ciberseguridad es un tema técnico

La Ciberseguridad es un área que suele ser relegada a segundo plano, y debería tener protagonismo en la mesa estratégica de las empresas ya que de ella depende también la continuidad (o incluso la supervivencia) de los negocios. Idealmente, el personal de Ciberseguridad debe contar con acceso al management de la empresa para ofrecer asesoría inteligente y darle las pautas que necesita para que sepa asumir los riesgos en los que la seguridad de sus activos está implicada.

Si hablamos de mitos, también hablamos de verdades

Verdad #1: Estamos yendo desde el perímetro hacia el flujo

La información ya no se encuentra alojada únicamente en servidores, ahora fluye y se dispersa en distintos formatos: celulares, la nube, objetos conectados a Internet… ¡Y en sitios que ni sabemos dónde están ubicados!
Nuestro reto es proteger el flujo de la información, lo que nos lleva a la siguiente verdad...

Verdad #2: Pasamos de proteger activos físicos a proteger el unicero

Tenemos que dejar de preocuparnos únicamente por los dispositivos que albergan la información, y extender la protección a la información que contienen. Esta debe ser considerada como un activo más de la organización y darle la protección que necesita para evitar que su filtración interrumpa la continuidad de sus operaciones.

Verdad #3: Dejamos de ser usuarios para ser productos

Los servicios que compañías como Google y Facebook nos brindan no son “gratis” como aparentan ser: nosotros tenemos que dar nuestros datos a cambio para poder abrir nuestras cuentas en estas plataformas, y una vez que aceptamos los términos y condiciones, perdemos el control de nuestra información, del uso que le van a dar y del nivelde seguridad que van a usar.

Un ejemplo muy famoso y reciente es el escándalo de la filtración de 50 millones de datos de usuarios por parte de Facebook a la consultora Cambridge Analytica, durante las últimas elecciones presidenciales de Estados Unidos.

Verdad #4: Dejamos de ser solo humanos a tener un doble digital

Hoy en día, los objetos se conectan entre sí, los usuarios con objetos o los usuarios entre sí. Muchos de los comportamientos pueden modelizarse, creando un doble digital que simule su comportamiento. Por ejemplo, objetos como un motor o un avión pueden ser digitalizados para hacer simulaciones, el mismo caso aplica con los seres humanos: todos tenemos dobles digitales o avatares con los que nos desenvolvemos en la red.

En este sentido, ninguno de nosotros tiene certeza de quién se está comunicando con nosotros cuando navegamos en la red, y los hackers se aprovechan de ello para secuestrar los dobles digitales que les interesan para sus objetivos.

Hemos hablado mucho de las amenazas y sus consecuencias pero, ¿Qué podemos hacer para protegernos?

Hay una luz al final del túnel: el 97% de los ataques pueden ser detenidos si hacemos una buena gestión de las herramientas con las que ya cuenta la mayoría de las empresas. Por los general, los atacantes no tienen una víctima en la mira, solo están buscando la red más vulnerable, y al primer obstáculo con el que se topan al intentar vulnerar una red, suelen retirarse sin insistir demasiado ya que se arriesgan a perder su anonimato e impunidad.

Sabiendo esto, es momento de reflexionar sobre las bases de una buena estrategia de Ciberseguridad

1. **Hacer una buena gestión de los riesgos:**
   estableciendo la prioridad de protección de nuestros activos.

2. **Capacitar a todo el equipo:**
   la improvisación no vale cuando hablamos de Ciberseguridad. Todo el personal de la organización debe tener consciencia de su rol y estar entrenado para manejar y cuidar la información de la forma adecuada.

3. **Fomentar una cultura cibersegura:**
   proveer de conocimientos a los usuarios es sólo la base: es necesario promover un cambio de comportamiento para que adopte hábitos más responsables en el uso de la información y activos digitales del negocio.

Y, ¿Cómo se debe cuidar la información?

La protección de la información consta de 4 fases:

Predicción

La misma puede ser provista por información, ya sea de organismos, empresas o redes sociales. La ciberinteligencia es otro instrumento para conocer cuando se planean ataques dirigidos a nosotros o para identificar la información crítica disponible por otros.

Prevención

El awareness es una de las claves de la prevención. Los ciberataques suelen ser exitosos por la falta de cuidados de los usuarios. El fortalecimiento de los segmentos de redes y servicios, o aplicaciones críticas harán junto al awareness que los atacantes desistan y salgan en búsqueda de otros objetivos.

Detección

Los ataques son inevitables: la clave está en detectarlos antes de que se propaguen y causen estragos, con ayuda de herramientas de monitoreo y control.

Respuesta

Debemos estar en condiciones de remediar lo dañado, así como de identificar las evidencias para poder aprender de los ataques para iniciar un proceso de mejora continua. La formación de equipos que hayan planificado su comportamiento en escenarios de ciberataques es una de las claves de la resiliencia. La improvisación nunca da buenos resultados, de modo que un equipo que ya conozca quienes lo integran, sus roles, responsables y actividades en una crisis, debe ser estratégico para la organización. De lo contrario, el funcionamiento va resultar descoordinado y el tiempo en debatir las acciones va a ser aprovechado por los ciberatacantes.

La respuesta: UNA CULTURA CIBERSEGURA

No podemos pensar lo digital de una manera aislada. Este mundo unicero es inevitable, y ya no debemos entender lo binario cómo algo estricto y exacto sino como una dimensión que se conecta, integra y confluye con el mundo físico.

La transformación digital nos exige repensar nuestra estrategia para continuar haciendo negocios bajo este nuevo paradigma. Y la ciberseguridad atraviesa todo el negocio: empleados, procesos, clientes, proveedores y reguladores.

Estos 4 pilares necesarios para la ciberseguridad no se cumplirán en las empresas si no se cuenta con el personal capacitado. Si tu organización no cuenta con los recursos humanos ni económicos para ejecutar un protocolo de Ciberseguridad adaptado al nuevo contexto digital, existen proveedores de servicios tercerizados en Ciberseguridad que te darán la asesoría experta que necesitás, sin necesidad de invertir tiempo ni dinero en armar un área de seguridad in house.

Contar con una estrategia de Ciberseguridad entonces ya no es una opción si no queremos sufrir daños a nuestra reputación o penalidades por el mal uso de los datos que nos ceden nuestros clientes. Debemos contar con una visión transversal y compartida (que involucre a todas las áreas que manejan información crítica) para enfrentar este nuevo paradigma. Las organizaciones que dominarán el futuro serán aquellas que desarrollen resiliencia y se conviertan en empresas capaces de adaptarse, evitando que los ataques afectan su operatividad o, en el caso de sufrir un ataque de mayor gravedad, puedan recuperarse rápidamente con el menor daño para el negocio.

NEXTVISION

Ciberseguridad Inteligente

AYUDAMOS A GESTIONAR LOS RIESGOS DE CIBERATAQUES DE MANERA INTELIGENTE

El 97% de los ataques son controlables con una buena administración de las herramientas tecnológicas y educación de los usuarios. Erradicamos la improvisación, priorizando correctamente los activos a proteger para mantener la continuidad del negocio.

PROMOVEMOS UNA CULTURA CIBERSEGURA

Ayudamos a transformar los hábitos de toda la organización con programas integrales, para que todos los colaboradores cuiden la información crítica y activos digitales del negocio.

nextvision.com