¿Qué es la ciberseguridad?

Obtén información sobre la ciberseguridad y cómo defender a tus usuarios, datos y aplicaciones contra el número creciente de amenazas a la ciberseguridad que hay actualmente.

Descubrir la protección contra amenazas integrada

“ ”

Ciberseguridad definida

Tipos de amenazas a la ciberseguridad

¿Por qué es tan importante la ciberseguridad?

Procedimientos recomendados de ciberseguridad

Soluciones de ciberseguridad

Soluciones de Seguridad de Microsoft

Ciberseguridad definida

La ciberseguridad es un conjunto de procesos, procedimientos recomendados y soluciones de tecnología que ayudan a proteger tus sistemas críticos y redes contra ataques digitales. A medida que los datos han proliferado y cada vez más personas trabajan y se conectan desde cualquier lugar, los infiltrados han respondido desarrollando métodos sofisticados para obtener acceso a tus recursos y robar datos, sabotear tu negocio y extorsionar. Cada año, el número de ataques aumenta y los adversarios desarrollan nuevos métodos para evadir detecciones. Un programa de ciberseguridad efectivo incluye a personas, procesos y soluciones de tecnología que en conjunto reducen los riesgos de interrupción de actividad comercial, pérdida financiera y daño de reputación a causa de un ataque.

Tipos de amenazas a la ciberseguridad

Una amenaza a la ciberseguridad es un intento deliberado de obtener acceso al sistema de una organización o usuario individual. Los infiltrados están desarrollando constantemente sus métodos de ataque para evadir la detección y explotar nuevas vulnerabilidades, pero confían en algunos métodos comunes para los que puedes prepararte.

Malware

Malware es un término amplio para cualquier software malintencionado, como gusanos, ransomware, spyware y virus. Está diseñado para causar daño a los ordenadores o redes alterando o eliminando archivos, extrayendo información confidencial como contraseñas y números de cuenta, o enviando tráfico o correos electrónicos malintencionados. El malware lo puede instalar un atacante que obtiene acceso a la red, pero a menudo, los usuarios implementan sin querer el

malware en sus dispositivos o la red de la empresa tras hacer clic en un vínculo incorrecto o descargar datos adjuntos infectados.

Ransomware

El ransomware es una forma de extorsión que usa malware para cifrar archivos y hacerlos inaccesibles. Los atacantes suelen extraer datos durante un ataque de ransomware y pueden amenazar con publicarlos si no reciben un pago. A cambio de una clave de descifrado, las víctimas tienen que pagar un rescate, normalmente en criptomoneda. No todas las claves de descifrado funcionan, por lo que el pago no garantiza que los archivos se recuperarán.

Ingeniería social

En ingeniería social, los atacantes aprovechan la confianza de las personas para engañarlas para que les entreguen información de su cuenta o descarguen malware. En estos ataques, hay infiltrados que se hacen pasar por un marca conocida, un compañero de trabajo o amigo, y usan técnicas psicológicas como crear un matiz de urgencia para que las personas hagan lo que ellos quieren.

Phishing

El phishing es un tipo de ingeniería social que usa correos electrónicos, mensajes SMS o correos de voz que parecen provenir de una fuente fiable para convencer a las personas para que cedan su información confidencial o hacer clic en un vínculo desconocido. Algunas campañas de phishing se envían a un gran número de personas con la esperanza de que una persona hará clic. Otras campañas, llamadas phishing de objetivo definido, son más específicas y se centran en una sola persona. Por ejemplo, un adversario puede fingir ser un solicitante de empleo para engañar a un contratante para que descargue un CV infectado.

Amenazas internas

En una amenaza interna, las personas que ya tienen acceso a algunos sistemas, como los empleados, contratistas o clientes, provocan una vulneración de seguridad o pérdida financiera. En algunos casos, este daño es involuntario, como cuando un empleado publica accidentalmente información confidencial en una cuenta de la nube personal. Pero algunos infiltrados actúan de manera malintencionada.

Amenaza persistente avanzada

En una amenaza persistente avanzada, los atacantes obtienen acceso a los sistemas, pero se mantienen sin detectar durante un período prolongado de tiempo. Los adversarios investigan los sistemas de la empresa objetivo y roban datos sin desencadenar ninguna contramedida defensiva.

¿Por qué es tan importante la ciberseguridad?

El mundo de hoy está más conectado que nunca. La economía global depende de que las personas puedan comunicarse en diferentes zonas horarias y tener acceso a información importante desde cualquier lugar. La ciberseguridad facilita la productividad e innovación al darles a las personas confianza para trabajar y socializar online. Los procesos y las soluciones adecuadas permiten que los negocios y gobiernos aprovechen la tecnología para mejorar la forma en que se comunican y entregan sus servicios sin aumentar el riesgo de ataques.

Cuatro procedimientos recomendados de ciberseguridad

Adopta una estrategia de seguridad de Confianza cero

Con más organizaciones que adoptan modelos de trabajo híbrido que les dan a los empleados la flexibilidad para trabajar en la oficina y remotamente, se necesita un nuevo modelo de seguridad que proteja a las personas, los dispositivos, las aplicaciones y los datos, independientemente de donde se encuentren. Unmarco de Confianza cero empieza con el principio de que ya no puedes confiar en una solicitud de acceso, incluso si viene de dentro de la red. Para mitigar el riesgo, asume que has tenido una vulneración y comprueba explícitamente todas las solicitudes de acceso. Usa el acceso con privilegios mínimos para darles a las personas acceso solo a los recursos que necesitan y a nada más.

Realiza formaciones en ciberseguridad con regularidad

La ciberseguridad no solo es la responsabilidad de los profesionales de seguridad. Hoy, las personas usan dispositivos personales y de trabajo indistintamente, y muchos ciberataques inician con un correo electrónico de phishing dirigido a un empleado. Incluso las empresas grandes y bien dotadas de recursos caen presas de las campañas de ingeniería social. Para confrontar a los ciberdelincuentes, es necesario que todos trabajen en colaboración para que el mundo online sea más seguro. Enséñale a tu equipo cómo proteger sus dispositivos personales y ayúdale a reconocer y detener ataques con formación periódica. Supervisa la eficacia de tu programa con simulaciones de phishing.

Establece procesos de ciberseguridad

Para reducir el riesgo de ciberataques, desarrolla procesos que ayuden a impedir, detectar y responder a un ataque. Revisa periódicamente el software y el hardware para reducir

vulnerabilidades y proporcionar directrices claras a tu equipo, de modo que conozcan las medidas que deben tomar cuando sufran un ataque.

No tienes que crear tu proceso desde cero. Obtén instrucciones de marcos de ciberseguridad como la International Organization for Standardization (SOC) 2700 o el National Institute of Standards and Technology (NIST).

Invierte en soluciones integrales

Las soluciones de tecnología que ayudan a resolver los problemas de seguridad mejoran cada año. Muchas soluciones de ciberseguridad usan IA y automatización para detectar y detener ataques automáticamente sin intervención humana. Otras tecnologías ayudan a comprender qué está sucediendo en tu entorno con análisis e ideas. Obtén una vista integral de tu entorno y subsana interrupciones de cobertura consoluciones completas de ciberseguridad que trabajen juntas y con el ecosistema para proteger tus identidades, aplicaciones y nubes.