Guía de supervivencia de ciberseguridad:

Cómo responder a las ciberamenazas modernas

El mundo digital se ha convertido en una selva peligrosa donde cada clic, cada descarga y cada inicio de sesión pueden ocultar una trampa.

El contexto cibernético actual está más plagado de amenazas que nunca, ya que los ataques de ransomware y DDoS, las estafas de phishing y las filtraciones de copias de seguridad cada vez se sofistican más. Ahora, los hackers aprovechan la IA para burlar las defensas tradicionales, y lo que antes eran solo ataques oportunistas se han convertido en amenazas calculadas y persistentes con capacidad de provocar graves perjuicios a las organizaciones.

Varios clientes de Dell han denunciado ataques basados en IA en los que los hackers habían extraído datos de redes sociales para redactar mensajes convincentes que podían engañar incluso a los empleados más concienciados sobre esta cuestión.

Esto es un duro recordatorio de que los atacantes utilizan tecnologías avanzadas con una precisión nunca vista para manipular, engañar e infiltrarse en empresas.

Para navegar por este entorno hostil, las organizaciones necesitan una estrategia de ciberseguridad integral que comprenda herramientas de última generación, estrategias de prevención y una vigilancia constante. Esta guía explica los componentes que debe tener esta estrategia para ayudar a las empresas a aumentar su resiliencia contra las ciberamenazas más graves de hoy en día.

Cómo proteger su empresa: principio de confianza cero

En el contexto actual de amenazas basadas en IA, es fundamental adoptar una infraestructura de confianza cero. Los atacantes utilizan IA para automatizar los sistemas de reconocimiento, robar credenciales y adaptar sus técnicas rápidamente, por lo que las defensas tradicionales resultan poco efectivas. El principio de confianza cero se basa en la idea de que cada intento de acceso puede ocultar una amenaza, así que se verifican todas las solicitudes y se implementan procesos estrictos de autenticación para minimizar los riesgos.

Con este principio, se supervisa activamente tanto a los usuarios como los dispositivos y las aplicaciones, de forma que se reduce la probabilidad de accesos no autorizados y vulneraciones de datos. Se trata de un enfoque moderno y unificado para gestionar las identificaciones.

Mantenga el entorno seguro y minimice el área de ataque potencial

Los atacantes suelen aprovechar vulnerabilidades en los puntos finales, las API y la cadena de suministro, así que, si quiere evitar las amenazas basadas en IA, es esencial reducir el área de ataque potencial. Los puntos finales y las API sirven como vías de entrada a las redes y los atacantes suelen utilizarlos para introducir malware o robar datos confidenciales.

Para proteger estas áreas se requieren varias capas de defensa: un sistema de autenticación estricto, cifrado de datos en tránsito, pruebas regulares de vulnerabilidad, herramientas de detección y respuesta de puntos finales (EDR), gestión de parches y refuerzos en los dispositivos.

Las soluciones de supervisión de puntos finales y la detección constante de amenazas pueden ayudar a identificar y bloquear actividades maliciosas en tiempo real.

Las organizaciones deben adoptar estrategias preventivas para proteger las cadenas de suministro y el ciclo de vida de desarrollo del software. La estrategia de acceso con privilegios mínimos asegura que solo ciertas aplicaciones y usuarios autorizados puedan interactuar con sistemas críticos, mientras que la detección de amenazas y las respuestas automatizadas pueden resolver vulnerabilidades en cuanto surgen.

Avance con la máxima seguridad: detección y respuesta proactivas ante amenazas

Los ataques basados en IA aprovechan vulnerabilidades, imitan comportamientos legítimos y se van adaptando continuamente para intentar burlar las medidas de seguridad, por lo que son muy difíciles de detectar. Para combatir estas sofisticadas amenazas, no basta con tener medidas de respuesta, sino que se necesitan sistemas de detección de amenazas avanzadas y herramientas de respuesta rápida. A través de la IA y el aprendizaje automático, los equipos de seguridad pueden analizar patrones de conducta, detectar anomalías y reaccionar en tiempo real ante las amenazas, corrigiendo los incidentes antes de que se produzcan problemas de mayor gravedad.

Un sistema de detección y respuesta efectivo debe absorber grandes cantidades de datos operativos para poder detectar riesgos y reaccionar a ellos de forma automática. Esta inteligencia contra amenazas se va desarrollando por sí misma, de forma que el sistema se vuelve más inteligente y más hábil a la hora de identificar amenazas emergentes y atajarlas de forma proactiva.

Asegúrese un refugio antes de la tormenta: reacción ante incidentes y recuperación

Si bien la prevención de ataques es un primer paso, las empresas deben actuar como si los ataques fueran inevitables. El objetivo es sobrevivir con el menor número de daños posible. En este sentido, una estrategia efectiva debe contemplar dos aspectos:

- Un plan sólido de respuesta a incidentes y recuperación (IRR).
- Medidas tecnológicas centradas en la copia de seguridad de aplicaciones y datos críticos.

Los planes de recuperación ante incidentes deben abarcar varios escenarios. Si se produce un ataque potente, se verían afectadas la mayoría de las operaciones de la empresa (si no todas). El plan debe detallar qué va a hacer cada departamento en caso de ciberataque e indicar qué medios va a utilizar la empresa para comunicarse, tanto a nivel interno como externo, con plantillas ya preparadas. El plan también debe revisarse y actualizarse regularmente. Por último, el plan solo es útil si se ha puesto en práctica previamente. Cuando se produzca un ataque, todo el mundo debería estar listo para actuar según lo establecido.

Desde un punto de vista tecnológico, las empresas deben determinar desde un buen principio cómo será su **viabilidad mínima (MVC)**: por ejemplo, ¿qué sistemas deben mantenerse operativos aunque esto implique trabajar con papel y bolígrafo?, ¿las ventas deben seguir en marcha?, ¿y el servicio de atención al cliente?

Una vez que se hayan establecido estas prioridades, deben desarrollarse las copias de seguridad y los mecanismos de recuperación correspondientes. Al tener la capacidad de trabajar solo con los datos correctos conocidos, la empresa no solo puede reemprender su funcionamiento rápidamente, sino que evita que los agentes maliciosos secuestren los datos. Además, las estrategias modernas de recuperación de información deben ir más allá de los enfoques tradicionales. Los sistemas de IA y LLM como los chatbots y los agentes virtuales deben tratarse como prioritarios, al mismo nivel que los sistemas de pagos o los datos de clientes.

Para combatir las amenazas avanzadas, los planes de recuperación de información deben combinar la automatización con las comprobaciones manuales. Es fundamental saber cómo funcionará la empresa si se produce una interrupción total del sistema. ¿Y si hay que volver a trabajar con papel y bolígrafo?

Todo el mundo debe contribuir: concienciación del personal

Los empleados son su primera línea de defensa ante los ciberataques, como quienes encabezan una expedición en la selva. Cada miembro del personal tiene un papel fundamental a la hora de identificar posibles amenazas y proteger los recursos. Para reforzar esta defensa, las empresas deben crear programas de concienciación en los que se trabaje con simulaciones de ataques con IA, como phishing o deepfakes avanzados.

Un buen programa debe combinar una formación continua junto con una comunicación clara, simulaciones de casos reales y una cultura de responsabilidad compartida. Cuando todo el mundo, desde operarios hasta ejecutivos, es consciente de las amenazas tanto tradicionales como con IA, la empresa está preparada y alerta ante cualquier eventualidad. Si se fomenta el trabajo en equipo y se prepara al personal, la organización podrá adelantarse a las amenazas en constante evolución y construir una defensa resiliente contra posibles ataques.

Prácticas recomendadas para mantener la resiliencia frente a los ataques basados en IA

Para mantener la resiliencia frente a los ataques con IA, las empresas deben adoptar un enfoque estratégico y proactivo. Presentamos 10 prácticas recomendadas:

Arquitectura de confianza cero

Cree un sistema de verificación continua, controles estrictos de acceso y segmentación de redes para que todos los usuarios y los dispositivos deban autentificarse antes de obtener acceso. Esto le ayudará a frenar y limitar los ataques con IA más sofisticados.

Refuerzo de la gestión de identidades y accesos:

Establezca un sistema de autenticación sólido (MFA, RBAC) y aplique políticas de credenciales estrictas para minimizar los ataques de phishing y relleno de credenciales.

Detección e inventario automatizados de activos:

Explore y supervise constantemente todos los activos, como la cloud, el IoT y la shadow IT, para evitar amenazas ocultas.

Microsegmentación y controles de acceso a la red:

Segmente y aísle las redes y las cargas de trabajo para evitar ataques de movimiento lateral y limitar las amenazas.

Refuerzo de puntos finales y API:

Utilice protección avanzada de puntos finales (EDR/XDR) y puertas de enlace de API seguras, además de un sistema de autenticación, limitación de velocidad, validación de entradas y cifrado seguros.

Gestión rigurosa de parches y vulnerabilidades:

Automatice los análisis y la aplicación rápida de parches para sistemas operativos, firmware, aplicaciones, API y software externo.

Detección y control de amenazas basada en IA:

Detecte anomalías y conductas sospechosas con tecnología de IA o ML para identificar amenazas sutiles o automatizadas en tiempo real.

Respuesta automatizada ante incidentes:

Utilice cuadernos de estrategias automatizados para aislar, contener y corregir amenazas rápidamente, lo que minimizará el tiempo de permanencia de los atacantes.

Simulaciones realistas regulares y mejora continua:

Realice ejercicios de simulación, equipos rojos y phishing; actualice también los planes de recuperación de información y los modelos de detección en función de los resultados.

Copias de seguridad inmutables con cámara de aire y recuperación:

Mantenga copias de seguridad antimanipulaciones (idealmente con sistema de cámara de aire y sometidas a pruebas regulares) para garantizar una recuperación rápida y sin obstáculos.

DELL Technologies

Dell Technologies: una guía para moverse en territorio desconocido

Para proteger a su empresa de las ciberamenazas más avanzadas, deberá disponer de las herramientas y los conocimientos adecuados para adelantarse a los posibles riesgos. En el complejo panorama de ciberseguridad de hoy en día, es imprescindible contar con una estrategia sólida para proteger los datos, los sistemas y la reputación de la organización. Aquí es donde entra Dell Technologies: ofrecemos un conjunto completo de soluciones diseñadas para satisfacer las necesidades de todo tipo de empresas.

Dell le proporciona la tecnología necesaria para defenderse de los ciberataques modernos, desde una cadena de suministro segura hasta detección de amenazas avanzadas y protección de puntos finales para mantener los datos a salvo. Con un conocimiento y una experiencia líderes en el sector, el equipo de Dell le ayuda a crear una estrategia de seguridad a medida. Dell cuenta con funciones como supervisión en tiempo real, respuestas automatizadas a amenazas y una arquitectura de confianza cero para garantizar la resiliencia y la defensa activa de su empresa.

Tanto si se enfrenta a un ataque de ransomware como a una estafa de phishing o a cuestiones de cumplimiento normativo, Dell Technologies le ayuda a superar las amenazas de hoy en día con máxima seguridad. Colabore con Dell para proteger su negocio y crecer en la era digital. Cuide de la seguridad y la eficiencia y manténgase siempre un paso por delante.

> "Su plan de respuesta ante incidentes debe imprimirse en papel, ya que es posible que los sistemas no estén operativos durante un ataque".
>
> ***Rachel Tyler***
> *Consultora de ciberseguridad, Dell Services*

Productos y soluciones Dell para ayudarle

Solución Dell destacada	Descripción
Infraestructura de confianza de Dell	Una combinación de servidores, redes y soluciones de almacenamiento y ciberresiliencia de Dell que, en conjunto, ofrecen una base moderna y segura para innovar.
Ciberresiliencia	Una cartera completa de soluciones diseñadas para proteger los datos y garantizar una recuperación segura. Incluye dispositivos, software y opciones como servicio.
Servicios de ciberseguridad	Un conjunto de herramientas para ayudarle a desarrollar e implementar una estrategia de seguridad integral en todas las tareas. Entre las prestaciones se incluyen servicios de asesoramiento, vCISO, el servicio Managed Detection and Response, pruebas de penetración y vulnerabilidad, respuestas a incidentes y recuperación.
Dell Trusted Workspace (seguridad de los puntos finales)	Una combinación de funciones complementarias integradas y opcionales diseñadas para proteger los PC. La solución está desarrollada con procedimientos seguros de la cadena de suministro y funciones integradas como SafeBIOS y SafeID con TPM. Los complementos opcionales incluyen la verificación de componentes seguros SecureD, SafeID con ControlVault y software de socios CrowdStrike y Absolute para maximizar la seguridad del espacio de trabajo.

Descubra cómo afrontar algunos de los principales retos de ciberseguridad actuales en **dell.com/cybersecuritymonth**