DELL Technologies

Amenazas internas: reforzar la ciberseguridad y la resiliencia con Dell Technologies

La amenaza en auge de ataques maliciosos internos

Una de las amenazas de ciberseguridad más serias en el panorama empresarial actual son los ataques maliciosos internos. A diferencia de las amenazas externas, los agentes internos ya cuentan con cierta confianza y acceso al sistema de una empresa, así que sus acciones pueden ser más difíciles de detectar y tener un impacto especialmente grave. Los ataques internos, desde el acceso a datos confidenciales hasta el sabotaje de los sistemas, pueden paralizar operaciones clave y provocar grandes daños financieros y de reputación.

Dell Technologies es consciente de la amenaza creciente que suponen estos ataques y, por eso, desarrolla soluciones innovadoras y adaptables para ayudar a las empresas a identificar, prevenir y mitigar los riesgos procedentes de agentes maliciosos internos. Combinamos la tecnología más punta con servicios desarrollados por expertos para que las organizaciones puedan adelantarse a estas amenazas.

¿Qué son los ataques maliciosos internos?

Los ataques internos se producen cuando una persona de una empresa utiliza su acceso para exponer datos, interrumpir operaciones u obtener información confidencial para fines personales, financieros o competitivos. Esta persona puede ser desde un empleado hasta un contratista, un socio o cualquiera con acceso legítimo al sistema y las redes de la empresa.

Cómo funcionan los ataques maliciosos internos

Los agentes internos aprovechan su posición de confianza para superar las barreras de seguridad tradicionales. Estas son algunas de las técnicas más comunes:

1. **Robo de datos:** obtención de datos confidenciales de clientes, contenido con propiedad intelectual o registros financieros.
2. **Sabotaje:** daño intencionado de los sistemas de TI para obstaculizar el funcionamiento de la empresa o afectar negativamente a su reputación.
3. **Abuso de credenciales:** uso de credenciales robadas o apropiadas para ofrecer acceso privilegiado a terceros o crear cuentas falsas.
4. **Colaboración con atacantes externos:** compartición de acceso o información confidencial con ciberdelincuentes externos a cambio de beneficios económicos.

Al disponer de la confianza de la empresa y de conocimientos restringidos, los atacantes internos son mucho más peligrosos en comparación con las amenazas externas.

El impacto en las empresas

Los ataques internos pueden tener un impacto muy grave y causar daños que van mucho más allá de las pérdidas económicas. Estas son algunas de las consecuencias que pueden tener que afrontar las empresas:

Pérdidas económicas

El robo de información confidencial, el fraude o el sabotaje pueden generar unos costes de recuperación de millones de dólares.

Interrupción operativa

El sabotaje del sistema o la destrucción de datos pueden interrumpir las operaciones y ocasionar retrasos, la pérdida de oportunidades y una reducción de la productividad.

Daño reputacional

Los ataques o vulneraciones de datos por parte de personal interno minan la confianza de los clientes y las partes interesadas, lo que reduce a su vez la fidelización y la percepción de la empresa en el mercado.

Incumplimiento normativo

En función del sector, los ataques internos pueden dar lugar a multas y penalizaciones cuantiosas si se produce una brecha de datos sanitarios o financieros.

Ejemplo real

En 2020, un contratista de TI que trabajaba para una entidad financiera importante eliminó intencionadamente varias configuraciones clave del sistema, lo que provocó interrupciones de más de **10 horas** en la conexión. A causa de este acto de sabotaje, la empresa perdió **millones** de dólares, no solo en daños económicos directos, sino también en costes de recuperación e impacto en la reputación. Los incidentes como este demuestran el gran potencial que tienen las amenazas internas y ponen de relieve la urgencia de implantar medidas eficaces de detección y prevención.

83 %

de las empresas tuvieron al menos un ataque interno en el último año

Fuente: Informe de Cybersecurity Insiders de 2024

Costes estimados

Según un estudio del instituto Ponemon de 2024, el coste medio de los incidentes relacionados con ataques internos se calcula en **4,99 millones de dólares**. Según el mismo estudio, este tipo de ataques supone casi el **55 %** de todas las vulneraciones. Estas cifras representan los costes de detección, recuperación y mitigación, y revelan la necesidad imperiosa de invertir en soluciones preventivas contra amenazas internas.

Combatir los ataques maliciosos internos con Dell Technologies

Dell Technologies ofrece un ecosistema integral de herramientas y servicios para combatir ataques maliciosos internos y garantizar que la empresa esté preparada contra posibles amenazas.

Protección de puntos finales con Dell Trusted Devices

Los puntos finales suelen ser la vía de entrada de las amenazas internas. Dell Trusted Devices integra funciones de seguridad pioneras en el hardware para reforzar los puntos finales y proteger los datos confidenciales.

- **Dell SafeBIOS** garantiza la integridad del firmware impidiendo manipular el sistema a nivel de hardware.
- **SafeID** protege los datos de credenciales y evita su robo y el acceso no autorizado a los mismos.
- **SafeData** cifra los datos confidenciales de forma integral, lo que garantiza que, en caso de que algún agente interno extraiga o intercepte información, no pueda leerla.

Al implementar estas soluciones, las empresas protegen completamente los puntos finales, tanto si las amenazas provienen de dentro como de fuera de la entidad.

Detección preventiva de amenazas con CrowdStrike

Para identificar amenazas internas, se debe vigilar y supervisar la actividad de los usuarios. El sistema de CrowdStrike se integra con las soluciones de Dell y utiliza inteligencia artificial y análisis de comportamiento para detectar anomalías indicativas de amenazas internas.

Por ejemplo, el sistema avisa inmediatamente si identifica transferencias anormales de datos fuera del horario de trabajo o el acceso no autorizado a áreas clave de la red, lo que permite actuar rápidamente. Recientemente, una organización sanitaria de EE. UU. pudo identificar y evitar el intento de extraer datos de pacientes por parte de un empleado gracias a la detección proactiva de amenazas, y esto impidió lo que habría sido una costosa vulneración de datos.

Protección de datos mejorada con Dell PowerProtect

Dell PowerProtect ofrece una línea de defensa sólida a través de copias de seguridad, almacenamiento con cámara de aire y copias inmutables de datos críticos. La información confidencial queda protegida contra intentos de modificación o eliminación, y los ataques internos resultan fallidos.

Tenemos el ejemplo de una empresa manufacturera donde un empleado descontento intentó sabotear varios archivos de diseño. El vault de recuperación de Dell PowerProtect permitió restablecer las operaciones en cuestión de horas, lo que evitó interrupciones y mantuvo el funcionamiento.

Recuperación rápida ante incidentes con Dell Professional Services

Cuando una amenaza interna se convierte en un incidente, la recuperación rápida es esencial. Dell Professional Services incluye soluciones de recuperación remota de datos y respuesta ante incidentes para garantizar el restablecimiento rápido de datos y sistemas. Los expertos de Dell siguen innovando para reducir al máximo el tiempo de inactividad y mitigar los impactos.

Estos son solo algunos ejemplos de la gama de soluciones que puede ofrecer Dell contra amenazas maliciosas internas.

Seguridad de red avanzada y microsegmentación con las redes de Dell PowerSwitch y SmartFabric OS

La segmentación de red avanzada, los controles de acceso estrictos y los análisis de tráfico en tiempo real en toda la infraestructura fortalecen las defensas contra ataques de día cero.

La importancia de una seguridad multicapa

Para defender los sistemas de forma efectiva contra ataques internos, no basta con una capa de protección. Con una estrategia de seguridad multicapa, evitará que las vulnerabilidades se conviertan en puntos débiles. Estos son algunos pasos clave:

Pasos clave para fortalecer sus defensas

- **Principios de confianza cero:** verifique constantemente todas las solicitudes de acceso y no confíe automáticamente en ninguna entidad, incluso dentro del perímetro de la empresa.
- **Controles de acceso basado en funciones (RBAC):** limite el acceso de los empleados a los sistemas y datos necesarios para sus funciones.
- **Soluciones de cifrado avanzado:** cifre los datos en tránsito y en reposo para impedir el robo de información.
- **Formación y concienciación de los empleados:** implemente programas frecuentes de concienciación sobre seguridad para evitar que el personal participe de forma accidental en actividades maliciosas.
- **Pruebas periódicas del sistema:** realice pruebas de penetración y análisis de vulnerabilidades para comprobar que las defensas sigan siendo seguras.

Estas prácticas, reforzadas con las soluciones de Dell, crean una increíble infraestructura de protección integral contra ataques maliciosos internos.

Fortalecimiento de las defensas mediante colaboraciones estratégicas

Dell colabora con proveedores de ciberseguridad líderes en el sector, como **CrowdStrike** y **Secureworks**, para reforzar aún más sus soluciones. CrowdStrike potencia la seguridad de los puntos finales y aporta inteligencia valiosa sobre indicadores de riesgo, mientras que Secureworks ofrece una detección avanzada de amenazas y servicios de respuesta. Gracias a estas colaboraciones, los clientes de Dell pueden disfrutar de un ecosistema de tecnologías integradas y de última generación.

Por qué elegir Dell Technologies para la ciberseguridad

Dell Technologies sigue siendo un referente en cuanto a soluciones de ciberseguridad multicapa. Los conocimientos expertos, las colaboraciones y la innovadora gama de productos de Dell se adaptan al panorama actual de amenazas constantes para ayudar a las empresas. Desde la protección de los puntos finales hasta la detección de amenazas internas y la recuperación ante incidentes, Dell proporciona una infraestructura completa y resiliente de soluciones para fomentar la confianza y el crecimiento.

Cree un futuro resiliente con Dell Technologies

Proteja su empresa frente a amenazas maliciosas internas con las soluciones integrales y adaptables de Dell Technologies. Al colaborar con Dell, no solo protegerá sus operaciones, sino que también garantizará la continuidad del negocio, aumentará la confianza de sus clientes y preparará a su organización de cara al futuro. Póngase en contacto con nosotros para obtener más información sobre cómo implementar soluciones de defensa proactiva hoy mismo.

Dell Technologies es su aliado de confianza para combatir amenazas internas, proteger activos críticos e impulsar a su empresa para que pueda prosperar en un entorno digital dinámico. La seguridad es la clave del futuro, y ese futuro empieza con Dell.

Descubra cómo afrontar algunos de los principales retos de ciberseguridad actuales en **Dell.com/SecuritySolutions**

Más información acerca de las soluciones Dell

Póngase en contacto con un experto de Dell Technologies

Ver más recursos

Únase a la conversación con #HashTag.

DELL Technologies