ENERO 2025

NEWSLETTER

Tendencias para el 2025

En el 2025, el panorama de la ciberseguridad continúa evolucionando a un ritmo acelerado. Las amenazas se vuelven más sofisticadas y los atacantes encuentran nuevas formas de comprometer nuestras infraestructuras críticas. En este contexto, es esencial estar al tanto de las tendencias emergentes y adoptar estrategias proactivas para proteger nuestros datos y comunicaciones.
En esta edición siendo la primera del año, exploraremos las predicciones más importantes para 2025 en el ámbito de la ciberseguridad que nos brinda Blackberry. Desde el cambio de enfoque de los atacantes hacia las redes de telecomunicaciones hasta las crecientes vulnerabilidades en aplicaciones de comunicación gratuitas, pasando por la sofisticación de los ataques de suplantación de identidad con IA y deepfakes, y la importancia de la seguridad en la cadena de suministro. También abordaremos cómo la difuminación de los límites entre la vida personal y profesional de los empleados puede aumentar los riesgos de ciberseguridad.

1 Redes de Telecomunicaciones como objetivo principal

En 2025, los actores de amenazas están cambiando su enfoque hacia la infraestructura de comunicaciones, como los operadores inalámbricos y los proveedores de servicios de Internet (ISP). Este cambio se debe a la interconectividad de las redes y los valiosos datos que contienen. Según Wiseman, vicepresidente de Comunicaciones Seguras de BlackBerry, comprometer estas redes permite a los atacantes eludir el malware específico del dispositivo y centrarse en vulnerabilidades de infraestructura más amplias.
El reciente incidente de escuchas telefónicas de Salt Typhoon, que interceptó comunicaciones ordenadas por tribunales, ilustra cómo las redes de telecomunicaciones se están convirtiendo en un vector principal para los atacantes. En el próximo año, las naciones y las organizaciones empresariales deben priorizar las estrategias de seguridad a nivel de red e infraestructura para salvaguardar los sistemas de comunicación críticos de ataques dirigidos en tiempo real.

2 Vulnerabilidades en aplicaciones de comunicación gratuitas

En 2025, el espionaje a nivel de red será solo una de las muchas preocupaciones relacionadas con las comunicaciones. Las aplicaciones de mensajería "gratuitas" como WhatsApp y Signal enfrentarán un escrutinio mayor debido a sus vulnerabilidades. Wiseman advierte que la seguridad percibida de estas aplicaciones se enfrentará a un escrutinio cada vez mayor a medida que sus vulnerabilidades se hagan más evidentes.
Recientemente, se descubrió que el grupo APT41 está utilizando actualizaciones de la campaña de malware LightSpy para infiltrarse en sistemas de comunicaciones comunes, en particular WhatsApp. Esto deja los metadatos y la información personal de los usuarios en riesgo de exposición o uso indebido por parte de terceros.

3 Suplantación de identidad con IA y Deepfakes

La tecnología de IA y los deepfakes están avanzando rápidamente, lo que permite a los atacantes crear suplantaciones de identidad más convincentes. En 2025, la suplantación de identidad sofisticada debería ser una preocupación importante para todas las organizaciones. Las tecnologías y tácticas de IA y deepfake están avanzando rápidamente para hacer que las voces, las imágenes y los vídeos sean más convincentes y fáciles de crear que nunca.
Los atacantes continuarán aprovechando los metadatos personales y los "datos de escucha", como la voz y el texto de las violaciones de la red de telecomunicaciones, que les brindan información actualizada para dirigirse mejor a las víctimas. Esto podría permitir a los actores de amenazas adaptar sus ataques en función de las comunicaciones anteriores, lo que dificultaría la detección de sus suplantaciones.

4 Suplantación de identidad con IA y Deepfakes

La tecnología de IA y los deepfakes están avanzando rápidamente, lo que permite a los atacantes crear suplantaciones de identidad más convincentes. En 2025, la suplantación de identidad sofisticada debería ser una preocupación importante para todas las organizaciones. Las tecnologías y tácticas de IA y deepfake están avanzando rápidamente para hacer que las voces, las imágenes y los vídeos sean más convincentes y fáciles de crear que nunca.
Los atacantes continuarán aprovechando los metadatos personales y los "datos de escucha", como la voz y el texto de las violaciones de la red de telecomunicaciones, que les brindan información actualizada para dirigirse mejor a las víctimas. Esto podría permitir a los actores de amenazas adaptar sus ataques en función de las comunicaciones anteriores, lo que dificultaría la detección de sus suplantaciones.

5 Difuminación de límites personales y profesionales

El uso de dispositivos personales para tareas profesionales aumenta los riesgos de ciberseguridad. En 2025, los empleados seguirán estando en riesgo y pueden exponer fácilmente a su organización si mezclan su vida personal y profesional en sus dispositivos. Esto crea nuevos puntos de entrada para las ciberamenazas.
Wiseman señala que el uso de dispositivos personales y redes inseguras mientras se viaja o se realizan comunicaciones confidenciales puede exponer vulnerabilidades críticas dentro de las organizaciones. Muchos empleados de alto valor pueden pasar por alto estos riesgos, asumiendo que sus dispositivos personales están seguros, pero prácticas simples como la sincronización con ID personales de Apple/Google pueden exponer inadvertidamente datos confidenciales.

Reflexión empresarial

Debido a que hay grietas en cualquier armadura, este es un buen momento para evaluar sus métodos de comunicación y fortalecerse contra las tácticas de intercepción generalizadas tanto a nivel de red como de dispositivo. Proteger sus comunicaciones ya no es opcional, sino una parte crucial de cualquier estrategia integral de ciberseguridad en 2025.

Implementar medidas como la autenticación multifactor (MFA), los servicios de campo avanzados (Field Services 2.0), la microsegmentación basada en el modelo de Zero Trust, la gestión de dispositivos móviles (MDM) y políticas de seguridad claras y mejoradas son pasos fundamentales para asegurar la integridad de nuestras comunicaciones.

Por eso, Grupo BelT junto a sus partners líderes en ciberseguridad e infraestructura, está comprometido a proporcionar soluciones integrales y personalizadas que aborden los desafíos de protección (Ciberseguridad). Contando con experiencia y enfoque en la innovación en los diversos sectores económicos, hemos ayudado a las organizaciones a proteger sus infraestructuras críticas, garantizar la privacidad de los datos y mantener la continuidad operativa en un entorno de amenazas en constante evolución.

Hasta la próxima semana, ciberlectores

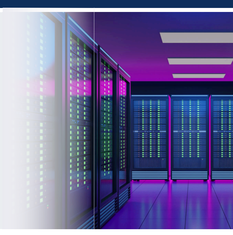
Referencias
Hart, G. (2024). 5 predicciones para 2025 y la próxima frontera de las ciberamenazas. BlackBerry Blogs.

admmarketing@buromc.com
Contáctanos ahora

DICIEMBRE 2024

NEWSLETTER

1 Transformación de los Centros de Datos: La Visión de Dell Technologies para 2025



En un mundo donde la inteligencia artificial (IA) está revolucionando la tecnología, Dell Technologies anticipa una transformación significativa en la arquitectura de los centros de datos. Según Steve Young, Vicepresidente Senior y Director General de Dell Technologies en el Reino Unido, la adopción de sistemas de IA está pasando de la fase de prueba a la implementación completa, lo que requiere cambios sustanciales en la infraestructura de TI.

La evolución de los centros de datos

Dell Technologies prevé que para 2025, los centros de datos tradicionales serán reemplazados por arquitecturas desagregadas. Este cambio permitirá que los sistemas de computación, almacenamiento y redes escalen de manera independiente, optimizando el rendimiento y la eficiencia.

La empresa estima que para 2026, las cargas de trabajo de IA constituirán más de la mitad de los requisitos de procesamiento de los centros de datos.

La importancia de la IA en la infraestructura

La IA no solo está transformando los centros de datos, sino también los dispositivos de punto final. Dell proyecta un aumento en la adopción de PCs con unidades de procesamiento neuronal (NPUs), diseñadas específicamente para manejar cargas de trabajo de IA. Estos dispositivos permitirán procesar datos directamente en el punto de creación, mejorando la eficiencia y reduciendo los costos asociados con la transmisión de datos a centros de datos centralizados.

Sectores clave para la implementación de IA

Los sectores de salud, educación, gobierno y comercio minorista son los principales objetivos para la implementación de IA. Estos sectores manejan grandes volúmenes de datos y requieren una infraestructura robusta para soportar sus operaciones. Dell Technologies destaca que el 70% de las empresas del Reino Unido ya han obtenido retornos de inversión significativos de sus implementaciones de IA generativa tras las pruebas iniciales en 2024.

El futuro de la computación en el borde

La computación en el borde, que procesa datos en el punto de creación en lugar de en instalaciones centralizadas, se expandirá a través de dispositivos habilitados para IA. Dell ha introducido una cartera de PCs Copilot+ AI, que permiten procesar datos en tiempo real directamente en el dispositivo, lo que potencialmente reduce costos y mejora la seguridad.

Reflexión empresarial

La visión de Dell Technologies para 2025 subraya la necesidad de una infraestructura flexible y escalable para soportar el crecimiento de la IA. Las empresas que no adopten una estrategia y arquitectura adecuadas para la IA estarán en desventaja. La transformación de los centros de datos y la adopción de dispositivos de punto final habilitados para IA son pasos cruciales para mantenerse competitivos en un entorno tecnológico en rápida evolución.

Grupo BeIT, a través de sus marcas BuróMC y Elit Infrastructure Services, ofrece una amplia gama de soluciones diseñadas para abordar los desafíos actuales y futuros de los centros de datos. Estas soluciones incluyen:

1. **Infraestructura hiperconvergente:** Elit Infrastructure Services proporciona soluciones de hiperconvergencia que permiten a las empresas escalar sus recursos de manera eficiente y reducir la complejidad de la gestión de TI.
Estas soluciones integran computación, almacenamiento y redes en una única plataforma, mejorando la eficiencia y reduciendo los costos operativos.

2. **Ciberseguridad avanzada:** BuróMC Seguridad Informática se especializa en la creación de arquitecturas de seguridad robustas para proteger los activos digitales de las organizaciones.
Con un enfoque en la protección perimetral y la gestión de amenazas, Grupo BeIT asegura que los centros de datos estén protegidos contra ataques cibernéticos sofisticados.

3. **Servicios en la nube:** BuróMC Seguridad Informática ofrece servicios de infraestructura como servicio (IaaS), permitiendo a las empresas evitar el gasto y la complejidad de la compra y administración de servidores físicos.
Estos servicios en la nube proporcionan flexibilidad y escalabilidad, adaptándose a las necesidades cambiantes del negocio.

4. **Monitoreo y soporte continuo:** Con su Centro de Operaciones de Red (NOC) y Centro de Operaciones de Seguridad (SOC), BuróMC Seguridad Informática ofrece monitoreo proactivo y soporte continuo para garantizar la disponibilidad y seguridad de los centros de datos.
Estas capacidades permiten a las empresas detectar y responder rápidamente a cualquier incidente, minimizando el impacto en las operaciones.

Hasta la próxima semana, ciberlectores

Referencias
Dell predice un cambio importante en la arquitectura del centro de datos para la IA

admmarketing@buromc.com

Contáctanos ahora

Grupo BeIT

ENERO 2025

NEWSLETTER

Planificación del presupuesto de ciberseguridad para 2025, guía esencial para CISOs empresariales

La planificación del presupuesto de ciberseguridad para 2025 presenta nuevos desafíos y oportunidades para los CISOs empresariales.
Con el costo promedio de una brecha de datos alcanzando aproximadamente los $4.8 millones en 2024 y proyectado a aumentar, la planificación estratégica del presupuesto de ciberseguridad nunca ha sido más crucial.

1 Crecimiento proyectado en el gasto de ciberseguridad

Según el pronóstico de Gartner, se espera que el gasto global en seguridad de la información alcance los $212 mil millones en 2025, lo que representa un aumento del 15.1% respecto a 2024 (Toll, 2024). Este aumento refleja la creciente priorización de la seguridad a nivel de la junta directiva y su reconocimiento como un habilitador de negocios.

2 Cambio en la asignación del presupuesto: Software y servicios en el centro del escenario

Una tendencia clave en la planificación del presupuesto de ciberseguridad para 2025 es el continuo cambio hacia el software y los servicios. Las encuestas recientes indican que el software ahora representa aproximadamente el 35.9% de los presupuestos globales de ciberseguridad, con un énfasis particular en las soluciones basadas en la nube. Para las grandes empresas, esta cifra puede alcanzar hasta el 39.4% del presupuesto total de ciberseguridad (Toll, 2024).

3 Alineación de los presupuestos de ciberseguridad con los objetivos empresariales

Los CISOs modernos están viendo cada vez más la ciberseguridad como una inversión estratégica en lugar de solo un centro de costos. Este cambio está impulsando una planificación del presupuesto de ciberseguridad que no solo se enfoca en la protección contra amenazas, sino que también apoya las iniciativas de transformación digital y habilita nuevos modelos de negocio. Como resultado, estamos viendo una mayor alineación entre el gasto en ciberseguridad y los objetivos empresariales generales en los planes presupuestarios de 2025 (Toll, 2024).

Desglose del Presupuesto de Ciberseguridad 2025

Participación de la ciberseguridad en los presupuestos de TI

Para las grandes empresas que planifican sus presupuestos de ciberseguridad para 2025, es crucial notar que se espera que la seguridad represente el 13.2% de los presupuestos de TI en promedio, frente al 8.6% en 2020. Este aumento subraya la creciente importancia de la ciberseguridad frente a las amenazas en evolución y las iniciativas de transformación digital.

Desglose detallado de las asignaciones del presupuesto de ciberseguridad para 2025

Basado en los puntos de referencia de la industria, aquí hay un desglose típico de las asignaciones del presupuesto de ciberseguridad para grandes empresas en 2025.

- **Software: 32%** (21% fuera de las instalaciones, 11% en las instalaciones)
- **Servicios: 28%** (incluyendo servicios de seguridad gestionados y consultoría)
- **Hardware: 15%** (incluyendo infraestructura en la nube y sistemas en las instalaciones)
- **Personal: 37%** (incluyendo salarios, beneficios y capacitación)

Estrategias para optimizar el presupuesto de ciberseguridad

Inversión en Soluciones Basadas en la Nube

Dado el aumento en la adopción de soluciones basadas en la nube, las empresas deben considerar la inversión en tecnologías que ofrezcan escalabilidad y flexibilidad. Las soluciones en la nube no solo proporcionan una protección robusta contra amenazas, sino que también permiten una gestión más eficiente de los recursos de TI (Toll, 2024).

Enfoque en la seguridad Zero Trust

La implementación de un modelo de seguridad Zero Trust es esencial para proteger las infraestructuras críticas. Este enfoque asegura que cada acceso a la red sea verificado y autenticado, minimizando el riesgo de brechas de seguridad.

Capacitación y desarrollo del personal

Invertir en la capacitación y el desarrollo continuo del personal de ciberseguridad es crucial para mantener una postura de seguridad fuerte. La formación en nuevas tecnologías y prácticas de seguridad ayuda a los equipos a estar preparados para enfrentar las amenazas emergentes.

Reflexión empresarial

La planificación del presupuesto de ciberseguridad para 2025 requiere una estrategia bien pensada que alinee las inversiones en seguridad con los objetivos empresariales. Con el aumento de las amenazas cibernéticas y la creciente complejidad de los entornos de TI, los CISOs deben asegurarse de que sus presupuestos no solo protejan contra las amenazas actuales, sino que también habiliten la innovación y el crecimiento empresarial.
En este contexto, BuróMC Seguridad Informática se presenta como el aliado estratégico ideal para dimensionar adecuadamente las necesidades de ciberseguridad de tu organización. Con un enfoque especializado y adaptable, podemos ayudarte a ajustar tu presupuesto de manera eficiente, incluso cuando no se está claro de cuál debería ser. Nuestro departamento de compliance, en colaboración con los departamentos de TI y comercial, están listos para ofrecerte el soporte necesario y que mereces para proteger tus activos digitales y fomentar el desarrollo continuo de tu empresa.

Hasta la próxima semana, ciberlectores

Referencias
Hart, G. (2024). 5 predicciones para 2025 y la próxima frontera de las ciberamenazas. BlackBerry Blogs.

admmarketing@buromc.com

Contáctanos ahora

Grupo BeIT

ENERO 2025

NEWSLETTER

Planificación del presupuesto de ciberseguridad para 2025, guía esencial para CISOs empresariales

La planificación del presupuesto de ciberseguridad para 2025 presenta nuevos desafíos y oportunidades para los CISOs empresariales.
Con el costo promedio de una brecha de datos alcanzando aproximadamente los $4.8 millones en 2024 y proyectado a aumentar, la planificación estratégica del presupuesto de ciberseguridad nunca ha sido más crucial.

1 Crecimiento proyectado en el gasto de ciberseguridad

Según el pronóstico de Gartner, se espera que el gasto global en seguridad de la información alcance los $212 mil millones en 2025, lo que representa un aumento del 15.1% respecto a 2024 (Toll, 2024). Este aumento refleja la creciente priorización de la seguridad a nivel de la junta directiva y su reconocimiento como un habilitador de negocios.

2 Cambio en la asignación del presupuesto: Software y servicios en el centro del escenario

Una tendencia clave en la planificación del presupuesto de ciberseguridad para 2025 es el continuo cambio hacia el software y los servicios. Las encuestas recientes indican que el software ahora representa aproximadamente el 35.9% de los presupuestos globales de ciberseguridad, con un énfasis particular en las soluciones basadas en la nube. Para las grandes empresas, esta cifra puede alcanzar hasta el 39.4% del presupuesto total de ciberseguridad (Toll, 2024).

3 Alineación de los presupuestos de ciberseguridad con los objetivos empresariales

Los CISOs modernos están viendo cada vez más la ciberseguridad como una inversión estratégica en lugar de solo un centro de costos. Este cambio está impulsando una planificación del presupuesto de ciberseguridad que no solo se enfoca en la protección contra amenazas, sino que también apoya las iniciativas de transformación digital y habilita nuevos modelos de negocio. Como resultado, estamos viendo una mayor alineación entre el gasto en ciberseguridad y los objetivos empresariales generales en los planes presupuestarios de 2025 (Toll, 2024).

Desglose del Presupuesto de Ciberseguridad 2025

Participación de la ciberseguridad en los presupuestos de TI

Para las grandes empresas que planifican sus presupuestos de ciberseguridad para 2025, es crucial notar que se espera que la seguridad represente el 13.2% de los presupuestos de TI en promedio, frente al 8.6% en 2020. Este aumento subraya la creciente importancia de la ciberseguridad frente a las amenazas en evolución y las iniciativas de transformación digital.

Desglose detallado de las asignaciones del presupuesto de ciberseguridad para 2025

Basado en los puntos de referencia de la industria, aquí hay un desglose típico de las asignaciones del presupuesto de ciberseguridad para grandes empresas en 2025.

- **Software: 32%** (21% fuera de las instalaciones, 11% en las instalaciones)
- **Servicios: 28%** (incluyendo servicios de seguridad gestionados y consultoría)
- **Hardware: 15%** (incluyendo infraestructura en la nube y sistemas en las instalaciones)
- **Personal: 37%** (incluyendo salarios, beneficios y capacitación)

Estrategias para optimizar el presupuesto de ciberseguridad

Inversión en Soluciones Basadas en la Nube

Dado el aumento en la adopción de soluciones basadas en la nube, las empresas deben considerar la inversión en tecnologías que ofrezcan escalabilidad y flexibilidad. Las soluciones en la nube no solo proporcionan una protección robusta contra amenazas, sino que también permiten una gestión más eficiente de los recursos de TI (Toll, 2024).

Enfoque en la seguridad Zero Trust

La implementación de un modelo de seguridad Zero Trust es esencial para proteger las infraestructuras críticas. Este enfoque asegura que cada acceso a la red sea verificado y autenticado, minimizando el riesgo de brechas de seguridad.

Capacitación y desarrollo del personal

Invertir en la capacitación y el desarrollo continuo del personal de ciberseguridad es crucial para mantener una postura de seguridad fuerte. La formación en nuevas tecnologías y prácticas de seguridad ayuda a los equipos a estar preparados para enfrentar las amenazas emergentes.

Reflexión empresarial

La planificación del presupuesto de ciberseguridad para 2025 requiere una estrategia bien pensada que alinee las inversiones en seguridad con los objetivos empresariales. Con el aumento de las amenazas cibernéticas y la creciente complejidad de los entornos de TI, los CISOs deben asegurarse de que sus presupuestos no solo protejan contra las amenazas actuales, sino que también habiliten la innovación y el crecimiento empresarial.
En este contexto, BuróMC Seguridad Informática se presenta como el aliado estratégico ideal para dimensionar adecuadamente las necesidades de ciberseguridad de tu organización. Con un enfoque especializado y adaptable, podemos ayudarte a ajustar tu presupuesto de manera eficiente, incluso cuando no se está claro de cuál debería ser. Nuestro departamento de compliance, en colaboración con los departamentos de TI y comercial, están listos para ofrecerte el soporte necesario y que mereces para proteger tus activos digitales y fomentar el desarrollo continuo de tu empresa.

Hasta la próxima semana, ciberlectores

Referencias
Hart, G. (2024). 5 predicciones para 2025 y la próxima frontera de las ciberamenazas. BlackBerry Blogs.

admmarketing@buromc.com

Contáctanos ahora