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