NOVIEMBRE 2024

NEWSLETTER

1 Ransomware y las vulnerabilidades, cómo funcionan, cómo nos afectan y cómo podemos protegernos

El Ransomware sigue siendo una de las amenazas cibernéticas más persistentes y devastadoras en 2024. Este tipo de malware cifra los datos de las víctimas y exige un rescate para restaurar el acceso. A medida que las tácticas de los ciberdelincuentes evolucionan, es crucial entender cómo funcionan estas amenazas, cómo nos afectan y qué medidas podemos tomar para protegernos.

¿Cómo funciona el Ransomware?

El Ransomware se infiltra en los sistemas a través de varios vectores, como correos electrónicos de phishing, vulnerabilidades en software no parcheado y descargas maliciosas. Una vez dentro, cifra los archivos del usuario y muestra un mensaje de rescate. **Los ataques de ransomware han evolucionado para incluir tácticas de doble y triple extorsión, donde los atacantes no solo cifran los datos**, sino que también amenazan con publicarlos o utilizarlos para atacar a terceros.

Impacto del Ransomware

El impacto del ransomware es significativo y multifacético. Según IBM, **el coste promedio de una vulneración de ransomware es de 5,13 millones de dólares, sin incluir los pagos de rescate.** Además, los ataques pueden desestabilizar operaciones empresariales críticas, como se ha visto en sectores de infraestructuras críticas y tecnología operacional.

Sophos reporta que el 59% de las organizaciones fueron afectadas por ransomware en el último año, con un incremento en las facturas de rescates y un 70% de los ataques resultando en el cifrado de datos. Fortinet destaca que los cibercriminales están explotando nuevas vulnerabilidades un 43% más rápido que en el primer semestre de 2023, lo que subraya la necesidad de una gestión proactiva de parches y una higiene cibernética rigurosa.

Cómo protegernos del Ransomware

Actualización y parches: Mantener todos los sistemas y aplicaciones actualizados es fundamental. Las vulnerabilidades no parcheadas son una de las principales vías de entrada para el ransomware.

Copias de seguridad: Realizar copias de seguridad regulares y almacenarlas de manera segura puede ayudar a recuperar los datos sin pagar el rescate.

Educación y concienciación: Capacitar a los empleados sobre los riesgos del phishing y las prácticas seguras en línea puede reducir significativamente el riesgo de infección.

Soluciones de seguridad avanzadas: Utilizar soluciones de seguridad que incluyan detección y respuesta de endpoints (EDR), inteligencia artificial y análisis de amenazas, detectar y responder a ataques de ransomware.

Enfoque Zero Trust: Implementar un enfoque de seguridad de confianza cero, que verifica continuamente la identidad y el contexto de los usuarios y dispositivos, puede ayudar a prevenir accesos no autorizados.

Conclusión

El ransomware y las vulnerabilidades asociadas continúan siendo una amenaza crítica en 2024. Sin embargo, con una combinación de tecnología avanzada, buenas prácticas de seguridad y una cultura de concienciación, las organizaciones pueden mitigar estos riesgos y proteger sus activos más valiosos.

En Grupo BeIT, nos posicionamos como su aliado estratégico para solventar las vulnerabilidades de ransomware. Nuestras soluciones de seguridad están diseñadas para detectar y neutralizar amenazas antes de que puedan causar daño, asegurando que sus datos y operaciones permanezcan seguros. Además, nuestras estrategias de copia de seguridad y recuperación garantizan que sus datos puedan ser restaurados rápidamente sin necesidad de pagar rescates.

Nuestro enfoque proactivo y nuestras alianzas con líderes del sector como IBM, Dell, Fortinet, Sophos, Bitdefender, Vicarius entre otros, nos permiten ofrecer soluciones de vanguardia, respaldadas por las mejores tecnologías y prácticas del mercado. Con nuestro soporte continuo y asesoramiento especializado, su empresa estará mejor preparada para enfrentar las amenazas cibernéticas del presente y del futuro.

admmarketing@buromc.com

SUSCRIBETE
DE MANERA GRATUITA