Publicado en Madrid el 12/07/2022

DXC Technology lanza una suite de soluciones para la protección del Directorio Activo

El servicio, que incluye una suite de soluciones basadas en IA y herramientas avanzadas como CyberArk DNA y Tenable.ad, contempla tres niveles de alcance que permiten detectar y corregir los gaps más relevantes, identificar vulnerabilidades en las cuentas privilegiadas y proteger de manera continuada la exposición del Directorio Activo

DXC Technology ha lanzado un innovador servicio de Consultoría que permite conocer el estado del Directorio Activo (AD) de las empresas y evitar ataques y fallas de seguridad. El servicio, que incluye una suite de soluciones basadas en IA y herramientas avanzadas como CyberArk DNA y Tenable.ad, contempla tres niveles de alcance que permiten detectar y corregir los gaps más relevantes, identificar vulnerabilidades en las cuentan privilegiadas y proteger de manera continuada la exposición del AD.

Más del 90% de las empresas de más de 1.000 empleados utilizan el Directorio Activo y, a pesar de ser el núcleo de la seguridad de cualquier organización, su administración adolece a menudo de los criterios de gestión adecuados y de las medidas de seguridad necesarias. Una debilidad que aprovechan los ciberdelincuentes hasta el punto de que el 60% de los ataques malware se dirigen contra el directorio activo. Uno de los casos más destacados es el del ransomware Ryuk, que se aprovecha de una vulnerabilidad común partiendo de un phishing para, en apenas 5 horas, paralizar grandes entidades tanto públicas como privadas.

El Directorio Activo está conformado por una base de datos (directorio) y un conjunto de servicios que conectan a los usuarios con los recursos de red que necesitan utilizar para realizar su trabajo. La base de datos contiene información crítica sobre su entorno, incluidos los usuarios y los equipos utilizados y qué puede hacer cada usuario.

Servicio escalable

El nuevo servicio de Auditoría del AD de DXC contempla tres alcances que se complementan. El Crítico, incluye el análisis básico y estático en todas las cuentas de la infraestructura para comprobar su estado y el contenido del AD y Azure AD principal con la finalidad de detectar los gaps más relevantes para permitir su corrección. El Avanzado amplía la auditoría crítica con la avanzada solución de CyberArk DNA, una herramienta que permite descubrir las cuentas privilegiadas de los servidores y de la totalidad del Azure AD. Con ella es posible detectar las vulnerabilidades en las cuentas privilegiadas minimizando los Pass The Hash (robo de credenciales). Finalmente, el alcance Total utiliza la herramienta Tenable.ad para proteger de manera continuada la exposición de todo el AD, detectar sus gaps y toda configuración errónea. Además, permite la trazabilidad de los ataques para poder correlacionar en tiempo real eventos y cambios de manera inteligente.

Síntomas de alerta

Según DXC, hay cuatro factores de alerta claves relacionados con la seguridad del Directorio Activo: contar con más de 4 administradores de dominio, no realizar auditorías del directorio activo, no poder

visualizar los cambios en tiempo real del directorio activo y no disponer de un plan de contingencia ante la pérdida de control del administrador de dominio.

“Las empresas que estén en esta situación pueden tener graves problemas de seguridad que puede, incluso, afectar a su viabilidad de futuro”, afirma Mikel Salazar, Director de Ciberseguridad para Iberia de DXC Technology. “En la mayoría de las organizaciones -añade- se supera con creces el número de administradores de dominio, que no debe ser superior a cuatro. Además, son muy pocas las que realizan auditorías de su Directorio Activo y las que cuentan con herramientas de monitorización continua del Directorio Activo. La realidad es que la mayoría de ellas no serían capaces de evitar un ciber ataque, lo que resulta muy preocupante”.

Inestabilidad global

Las tensiones geopolíticas y económicas actuales son aprovechadas por los ciber delincuentes y el Directorio Activo es uno de sus principales objetivos. Para Pablo Parra, Cybersecurity Business Developer de DXC Technology, “La seguridad del directorio activo no es un evento único sino un proceso continuo. Se sabe que el 60% del nuevo malware incluye código específico dirigido contra el directorio activo y según estudios recientes, el 80% de las organizaciones auditadas presentan errores críticos de configuración en su directorio activo”.

El nuevo servicio de Auditoria del Directorio Activo, que ofrece una visión holística y un alcance end to end, se ha diseñado para dar una respuesta eficaz a estas amenazas. “Hemos definido un servicio escalable, con tres alcances – Crítico, Avanzado y Total –, que nos permite definir las actuaciones necesarias para proteger el Directorio Activo y reducir los vectores de ataque a las empresas mitigando su exposición y vulnerabilidad. El objetivo es proteger y monitorizar el directorio activo de manera integral, detectando y tratando las amenazas y configuraciones erróneas para minimizar los riesgos operativos, regulatorios y reputacionales”, concluye Mikel Salazar.

Más de 200 especialistas

El equipo de Ciberseguridad de DXC cuenta con más de 200 especialistas en España, con equipos dedicados en Madrid, Barcelona, Avilés, Zaragoza y Lisboa. Además, DXC es uno de los principales partners en Ciberseguridad de Microsoft, en Iberia y en el mundo.

Datos de contacto:
María Guijarro
622836702

Nota de prensa publicada en: Madrid

Categorías: Nacional Inteligencia Artificial y Robótica E-Commerce Software Ciberseguridad Recursos humanos

NotasdePrensa
https://www.notasdeprensa.es