Publicado en Madrid el 23/09/2021

DXC Technology: El enemigo en casa: los ataques de insiders han crecido un 31% en los últimos tres años

El teletrabajo ha incrementado de manera exponencial el riesgo debido al uso de conexiones inseguras y la difuminación del perímetro, problemas que se añaden al ya complicado panorama de amenazas de la prepandemia

Los daños causados por los ataques internos -insiders- a los sistemas de información de las empresas en EE.UU. crecieron un 31% en los últimos tres años, con un coste medio de más de 11 millones de dólares, según el estudio 2020 Cost of Insider Threats: Global. También aumentó un 47% la frecuencia de los incidentes que, de media, tardan 77 días en contenerse. De los tres grandes perfiles de insiders: usuarios negligentes, los infiltrados y los ladrones de credenciales, éstos últimos son los que causan más daño, si bien representan solo una cuarta parte de los ataques.

Para ayudar a frenar esta amenaza emergente, AUTELSI ha elaborado un Trabajo que analiza esta problemática, que ha servido de base para el encuentro “Amenazas Internas de Ciberseguridad: Insiders” en el que Mikel Salazar Peña, Responsable de Ciberseguridad para Iberia de DXC Technology presentó una hoja de ruta y las mejores prácticas y tecnologías para combatir a los insiders.

Aumento del área de exposición

El teletrabajo ha incrementado de manera exponencial el riesgo debido al uso de conexiones inseguras, el uso de dispositivos personales y la difuminación del perímetro, problemas que se añaden al ya complicado panorama de amenazas de la prepandemia.

Para Mikel Salazar Peña, en la batalla contra los insiders es necesario enfocar tres principios clave. El primero es Reducir la complejidad. Identificar y entender el riesgo al que se exponen las organizaciones teniendo claro el nivel de madurez de partida y los vectores de entrada. Además del cumplimiento con la normativa, es fundamental tener preparado un plan por si la organización se ve comprometida y disponer de protocolos de gestión de impacto reputacional y operacional.

El segundo es Proteger el dato. “Hay que cambiar el chip -señala Mikel Salazar-, antes el foco estaba en la securización de la red ahora lo urgente es prestar atención al dato y la identidad. Recomendamos la implementación del modelo Zero Trust donde cualquier usuario o elemento es una posible amenaza, independientemente de si es interno o externo. Gracias a Zero Trust tendremos una autenticación reforzada, procesos de verificación y mejora en la visibilidad del uso del dato de una manera transversal”.

Su implementación requiere una autenticación fuerte (apoyada en soluciones de acceso Multifactor y condicional), en un dispositivo confiable (libre de vulnerabilidades y con sistemas avanzados de respuesta EDR). También será fundamental asegurar el principio de mínimo privilegio. En el caso de la verificación, será fundamental incorporar sistemas de Análisis del comportamiento de usuarios y entidades (UEBA) apoyados en inteligencia artificial y machine learning para la detección avanzada de este tipo de insiders.

El tercer foco es situar la Seguridad en el centro. El empleado es la primera línea de defensa y es fundamental un buen plan de formación y concienciación que contemple políticas reforzadas,

actualizaciones de seguridad y formación continua. A nivel corporativo, es fundamental la esponsorización de la dirección, creando una cultura de seguridad, aplicando la máxima del principio “secure by design”, (personas, procesos, tecnología).

Gestión de identidad e identidad privilegiada

Las soluciones de gestión de la identidad e identidad privilegiada ayudan a implementar las mejores prácticas en identidad para mitigar estas amenazas internas como segregación de funciones, privilegio mínimo, facilitando solo el acceso necesario para realizar un trabajo, que limita la exposición de datos confidenciales o secretos.

“En DXC -señala Mikel Salazar- tenemos gran experiencia y referencias en la implementación de estas herramientas, en clientes de todos los sectores, apoyándonos en socios tecnológicos tan potentes como Cyberark o Sailpoint, entre otros que nos permiten implementar el modelo Zero Trust de manera eficiente”.

Según el responsable de Ciberseguridad para Iberia de DXC, las soluciones de Gestión de identidad ayudan en 5 puntos clave contra los insiders. La implementación del ciclo de vida de la identidad permite asegurar la correcta baja de permisos una vez finalizada la relación laboral, evitando accesos no deseados, eliminación de archivos o fugas de información. Por su parte, las políticas de segregación de funciones impiden que una identidad acumule permisos incompatibles o que consiga una composición de permisos que supere un nivel de riesgo determinado.

La Implementación del modelo de control de acceso basado en roles (RBAC) garantiza que no se acumulen permisos heredados y permite hacer campañas de certificaciones de acceso en las que, periódicamente, los propietarios de los datos o aplicaciones validen si esos accesos son necesarios pudiéndose revocar en el caso de no ser necesarios.

Finalmente, la gestión de identidad ayuda a identificar identidades y grupos de riesgo derivados de acumulación de permisos o de accesos a sistemas críticos del negocio que puedan aconsejar la ejecución de campañas de recertificación o segregación de funciones adicionales. Además, la posibilidad de su integración dentro de la Gestión de Eventos e Información de Seguridad (SIEM), permite la creación de casos de usos personalizados para ciertos perfiles sospechosos.

En el caso de la Gestión de accesos privilegiados es necesario asegurar que nadie conozca las contraseñas de los sistemas objetivo, disponiendo de un punto único de acceso y centralizado. También se podrá controlar unívocamente quién hace uso de esas cuentas privilegiadas cada momento, protegiéndolas. Y, por último, gracias a la posibilidad de grabación de las sesiones de usuarios privilegiados se tendrá una capacidad completa de registros de auditoría de cara a posibles investigaciones forenses.

Securización de infraestructuras, detección y respuesta

Según Salazar, la transformación digital hacia la nube es imparable y su adopción entraña diferentes riesgos como la aparición de permisos excesivos. “En este nuevo paradigma aparecen nuevos permisos asociados a su gestión (cloudops, devops) y desde DXC recomendamos la adopción de herramientas CSPM que nos dan visibilidad sobre roles, nivel de acceso, acciones realizadas para localizar y remediar permisos incensarios asignados a roles personales o de aplicación. Además, pueden posibilitar remediaciones automáticas minimizando el riesgo de respuesta”.

En paralelo, en esta nueva realidad, donde el perímetro se ha difuminado para proteger a los empleados es necesario proteger todas las actividades realizadas desde sus puestos de trabajo. Aquí,

las soluciones de arquitectura Secure Access Service Edge (SASE) pueden ayudar, ya que no se centran en redes origen ni destino como antiguamente, sino que tienen un foco directo en la identidad independientemente de su localización. “En DXC somos expertos en este nuevo enfoque SASE y trabajamos con los principales partners referentes en este ámbito como Palo Alto, Netskope o Zscaler”, añade Salazar.

En cuanto a la detección y respuesta, el uso de técnicas o soluciones tradicionales como DLP, SIEM o PAM no son suficientes para poder detectar a estos actores. Muchas compañías tratan de realizar una buena clasificación de la información confidencial o de negocio, pero la manera cada vez más descentralizada en la que se manejan los datos complica mucho la detección.

Para DXC las dos principales amenazas a monitorizar frente a los insiders son la exfiltración de datos que constituye la más recurrente junto el abuso de credenciales privilegiadas. En el caso de la exfiltración, antes se utilizaban los USBs y los discos duros para principal medio de robo de información, hoy se hace utilizando el correo electrónico mediante reenvío a cuentas personales, cargando la información en sitios de colaboración en la nube.

En este contexto tan complicado hay que recurrir a sistemas UEBA que cuentan con algoritmos de detección avanzado apoyados en inteligencia artificial y machine learning. Esta detección avanzada se logra gracias al uso de patrones de detección basados en diferentes variables tales como el análisis del comportamiento, rareza del evento, geolocalización, análisis de volumetrías, comparativas con pares, entre otros.

En el ámbito de la detección avanzada y respuesta automatizada mediante sistemas SOAR, DXC trabaja con líderes del mercado como Securonix o Microsoft Sentinel donde apoya sus servicios de detección y respuesta 24x7. “Gracias a su potencia y su posibilidad de automatización podemos detectar comportamientos extraños como los derivados de la presencia de insiders, de la ejecución de comandos de Windows PowerShell injustificados, de la compartición de cuentas o de escalados de privilegios que puedan desencadenar en un incidente”, concluye Mikel Salazar.

Datos de contacto:
María Guijarro
622836702

Nota de prensa publicada en: Madrid

Categorías: Nacional Telecomunicaciones Emprendedores E-Commerce Ciberseguridad Recursos humanos