¿Cómo detectar y protegerse de las amenazas de identidad?

nexus aggity

Los avances tecnológicos nos han permitido evolucionar hacia un mundo virtual donde, día a día, construimos una identidad digital que cobra vida paralelamente a nuestra realidad, con la diferencia de que la web no descansa y la información que nos describe circula constantemente, sin que lo podamos controlar.

Desde las páginas y las aplicaciones que visitamos a diario se obtienen datos de gran valor que van desde las preferencias de navegación, las compras, la ubicación GPS, la dirección IP, el nombre de usuario y el tipo de dispositivo hasta información de fechas importantes, lugar donde laboramos, amigos y familiares con los que interactuamos y más.

La responsabilidad de los CIO

Todo lo anterior adopta una gran relevancia al ocupar el cargo de CIO, en una organización cuya responsabilidad es proteger los activos de información de la empresa, incluyendo la plantilla de colaboradores y sus diferentes alternativas para interconectarse, lo que involucra los accesos al correo corporativo, además de sistemas y aplicaciones que se usan para la actividad laboral.

Desde 2021 se alertó sobre la necesidad de que los CIO ampliarán la visibilidad en la actividad de sus usuarios y sus sesiones asociadas con aplicaciones web, tras una encuesta global a 900 líderes de seguridad empresarial.

Y es que hoy, el uso indebido de credenciales es uno de los principales vectores de ataque que está poniendo en jaque a decenas de organizaciones.

Según esa investigación, en **70%** de las organizaciones, el usuario final tiene acceso a más de 10 aplicaciones de negocio, muchas de las cuales contienen datos de alto valor, por lo que el robo de credenciales y/o la suplantación de identidad es una excelente oportunidad para los ciberdelincuentes, quienes buscan hacer “rapiña digital”.

¿Qué hacer para protegerse?

Los CIO deben implementar controles de seguridad que mitiguen el riesgo de errores humanos o intenciones maliciosas. Uno de ellos es la Detección y Respuesta a las Amenazas de Identidad, tendencia de ciberseguridad para 2023 de acuerdo con Gartner, que integra un conjunto de herramientas y mejores prácticas para defender los sistemas de identidad de diferentes ataques.

La primera infraestructura a evaluar es el IAM (Sistemas de gestión de accesos e identidades) a fin de identificar áreas de oportunidad para mejorar la identificación, la investigación y la contención ante amenazas digitales. Asimismo, se sugiere a los CIO utilizar el marco ATT&CK (tácticas y conocimiento común de adversarios) de MITRE para correlacionar técnicas de Identity Threat Detection and Response (ITDR) con los escenarios de ataque habituales.

Es recomendable realizar la modernización y/o la implementación de las mejores prácticas de seguridad de higiene en la infraestructura las cuales están basados en los estándares actuales como el OAuth 2.0, estructura de autorización que permite a las aplicaciones tener acceso limitado a cuentas de usuarios de determinados servicios. Esto fungirá como un escudo contra los intentos de intrusión cibernética mediante las identidades que, desde 2021, atacan a los usuarios finales, incluidos los usuarios comerciales con acceso a datos confidenciales, según el **56%** de los CIO encuestados en el Informe CISO View 2021: Zero Trust y acceso privilegiado de CyberArk.

Los segundos blancos de ciberataques son directivos **(48%),** proveedores externos **(39%),** así como ingenieros Cloud y DevOps **(33%).**

Fuente de información: cio.com.mx