Preguntas para reforzar la seguridad empresarial

Los ciberataques son cada vez más rápidos y se dirigen a múltiples superficies de amenaza simultáneamente, utilizando una amplia gama de técnicas para evadir la detección y acceder a datos valiosos. Una de las estrategias de ataque favoritas de los hackers es utilizar diversas técnicas de ingeniería social, phishing, ransomware y malware para obtener credenciales de acceso. Una vez en una red corporativa, los actores maliciosos se mueven lateralmente por la organización, buscando los datos más valiosos para exfiltrarlos, venderlos o utilizarlos para hacerse pasar por altos ejecutivos.

El perímetro tradicional centrado solo en el manejo de los passwords e infraestructura es, en muchos sentidos, de otra época. Este enfoque se basa en la creencia de que es posible proteger todo dentro de la empresa. Ahora los profesionales de la seguridad deben tener en cuenta no sólo los usuarios, sino también las aplicaciones y las máquinas. Los usuarios ahora pueden tener múltiples identidades a través de más cuentas, los usuarios pueden ser máquinas y robots, y los usuarios humanos pueden tener múltiples dispositivos en los que conectarse con diferentes versiones o generaciones de aplicaciones. Todos ellos pueden moverse para acceder a los recursos desde diferentes puntos de acceso y sistemas.

Por ello, recomendamos priorizar el acceso basado en la identidad: por ejemplo, ¿Quién es este usuario?, ¿A qué debería tener acceso? ¿Qué hace con esta autorización? y ¿Cuándo deberían cambiar sus derechos? Este punto es aún más relevante y clave cuando se trata de grandes empresas ya que tiene más de 25 diferentes sistemas para manejar los accesos a los datos.

En Quest Software brindamos los siguientes consejos para reforzar la seguridad de tus datos:

1) Al menos Dos Factores de Autentificación: Una excelente manera de hacer que tu organización sea menos vulnerable a ataques es restar importancia a las contraseñas individuales. La forma más común de lograrlo es agregar un segundo factor a las contraseñas. Hay muchos sistemas diferentes de autenticación de dos factores, desde mensajes SMS (que no son tan recomendables), hasta aplicaciones de autenticación y claves FIDO (Fast Identity Online).

Las plataformas de autenticación como Azure AD también ofrecen inicios de sesión “sin contraseña”. En estos sistemas, el dispositivo de acceso se vuelve muy importante. La combinación de un dispositivo debidamente registrado junto con un PIN local o un identificador biométrico se utiliza en lugar de una contraseña para

2) Refuerza tus “endpoints” o terminales: Para que los cyber ataques tengan éxito, las terminales deben estar disponibles para un atacante. Normalmente, un cibercriminal buscará una terminal en el que se pueda generar un script y validar si un nombre de usuario y una contraseña funcionaron. No se lo pongas fácil a tus atacantes. Audita regularmente todos tus dispositivos y, si es posible, agrégales autenticación al menos de dos factores.

3) Utiliza herramientas de auditoría más inteligentes: Muchas herramientas de auditoría

pueden ver que, si bien una cuenta individual puede no tener una cantidad inusual de fallas de autenticación, la organización en su conjunto sí lo tiene.

Para que esto funcione, las herramientas de auditoría deben poder establecer automáticamente actividades que sean “normales” para que puedan detectar acciones que sean “anormales”. Después de todo, lo “típico” no solo evoluciona constantemente, sino que puede variar mucho según la hora y el día de la semana.

Si tu organización usa varios directorios al mismo tiempo, como Azure Active Directory y Active Directory, es una buena idea que tu herramienta de auditoría pueda considerar el comportamiento y monitoreo de ambos. De lo contrario, es posible que te encuentres en una situación en la que tengas un punto ciego significativo.