Recientemente me preguntaron: "¿Qué consejo tiene para que las empresas protejan sus negocios y sistemas financieros de phishing, violaciones de datos e ataques cibernéticos?"

Las mejores prácticas de seguridad cibernética se han expandido, ya no se trata solo de capacitación y conciencia.

Un periodista le preguntó a Mike Tyson si estaba preocupado por el plan de lucha de Evander Holyfield. Tyson dijo: *"Todos tienen un plan hasta que alguien los golpea en la boca".*

El costo promedio de una violación de datos hoy en los Estados Unidos es de ~ 8.19 millones de dólares. Los ataques de ransomware ocurren cada 14 segundos y cada 11 segundos para 2021. Aproximadamente el 73% de las copias de seguridad críticas fallan durante un ataque cibernético. El costo promedio de un registro comprometido es de $242 por registro expuesto durante una violación de datos. Las nuevas leyes de privacidad de datos promulgadas, como GDPR, CCPA y la ley NY-SHIELD, están imponiendo sanciones sustanciales a las organizaciones que no son cibernéticas. Es importante tener en cuenta que una empresa no necesita estar en Europa, California o Nueva York, por ejemplo, para hacerse responsable de las violaciones de la privacidad de datos.

Es un error pensar que las violaciones de datos ocurren solo para cobrar un rescate. Los ciberataques modernos a menudo persiguen algo más que un rescate. Aunque la capacitación puede ayudar a reducir el número de usuarios que son víctimas de intentos de phishing (suplantación de identidad), ciertamente no es la solución. Tenga en cuenta que si un solo usuario es víctima de un correo electrónico de phishing, toda la organización puede verse afectada. Ese único usuario no necesita ser un administrador de TI con credenciales de administrador de dominio o superusuario para todo el entorno y / o para que los activos comerciales críticos se vean comprometidos.

Las intrusiones cibernéticas se refieren a la confidencialidad, disponibilidad e integridad de los sistemas y datos. Las amenazas cibernéticas modernas para las empresas son piratas informáticos externos e incluso actores internos de amenazas, así como acciones gubernamentales y legales en forma de violaciones y sanciones.

En términos de actores de amenazas internas, se realizó una encuesta independiente durante COVID-19 que encontró que ~ 57% de los empleados sentían que podían participar en actividades nefastas contra la empresa para la que trabajan y salirse con la suya, simplemente porque estaban trabajando desde hogar. Las empresas deben comprender que durante COVID-19 y la Nueva Normalidad, la superficie de ataque de su organización se ha expandido significativamente, especialmente con una fuerza de trabajo y tecnología distribuidas.

No espere hasta que ocurra un incidente.
Para obtener información adicional sobre los servicios de seguridad cibernética de Withum, comuníquese con nuestros expertos ahora.

La nube no equivale automáticamente a una mejor seguridad. La nube es simplemente la computadora de otra persona. Simplemente porque su proveedor de la nube es seguro, no hace que su empresa sea segura. Si le dicen algo diferente, solicite a su proveedor de la nube que asuma toda la responsabilidad en nombre de su empresa en caso de que el sistema o los datos se vean comprometidos en su nube impenetrable.

Los ciberataques de próxima generación ya están aquí, y tampoco son ciencia ficción. Se llaman ataques cibernéticos. Estos tipos de ataques causan daños físicos a los entornos. Entonces, independientemente de si las copias de seguridad son "buenas", los ataques cibernéticos pueden obstaculizar los entornos y por lo tanto, hacer que los equipos físicos, electrónicos y los datos sean inútiles como un ladrillo físico. *Asegure su entorno a través de auditorías independientes de terceros.*

Deben adoptarse consideraciones adicionales:

- Aplicar controles de seguridad y filtrado con integración de inteligencia artificial
- Tripwires virtuales (identifica anomalías en el entorno). Implemente copias de seguridad inteligentes de autocuración (self healing) (las copias de seguridad suelen estar envenenadas por intrusos)
- Realice una emulación de amenazas de terceros, también conocida como piratería autorizada del entorno, continuidad del negocio y evaluación de brechas de seguridad para verificar la confidencialidad, disponibilidad e integridad de la empresa.
- 24/7/365 Tercero independiente Monitoreo y validación de entornos para proporcionar un constante "control y equilibrio" contra personas, procesos y tecnologías. Esto asegura la política interna y externa, la privacidad de los datos y la adherencia al cumplimiento.

ARTICULO POR: WITHUM SMITH + BROWN, PC
AUTOR: MATTHEW FERRANTE
TRADUCCIÓN: MV CONSULTORES S.C.