Enfrentando **la disrupción** y sus **riesgos emergentes**

CIBERSEGURIDAD

LA CIBERSEGURIDAD COMO PUNTO NEURÁLGICO PARA LA CONTINUIDAD DEL NEGOCIO

La pandemia por el COVID-19 ha obligado a muchas organizaciones a desarrollar forzosamente métodos de trabajo alternativos, como el trabajo en casa. De esta forma y en tiempo récord, pequeñas, medianas y grandes empresas han puesto su foco en "seguir funcionando" y la realidad es que la gran mayoría no han evaluado en detalle las ciber amenazas que eso implica.

Si bien resulta clave proteger la salud de los empleados durante este tiempo de crisis por la pandemia, también es crítico proteger la salud de la ciberseguridad de su organización.

Los atacantes maliciosos de todo el mundo están aprovechando la oportunidad de explotar debilidades tecnológicas. Por ejemplo, la Organización Mundial de la Salud (OMS) ha advertido que los criminales la están suplantando, enviando mensajes usando su logotipo y la información disponible públicamente para robar dinero e información sensible.

Ahora más que nunca es primordial que su organización tome las medidas adecuadas para protegerse de las ciber amenazas y se debe actuar rápidamente.

Muchos de los riesgos asociados a trabajar desde casa no son nuevos; sin embargo, la rápida migración de millones de usuarios (desde redes empresariales y universitarias que se monitorean y protegen corporativamente) a redes Wi-Fi domésticas (en gran parte no supervisadas y a menudo inseguras) crea una gran oportunidad para los cibercriminales y cambia claramente el perfil de riesgo, debiéndose considerar ahora los siguientes factores para dicho análisis:

- Aumento del riesgo por uso de terminales y/o redes no corporativas fuera del control del área de TI (posibles versiones desactualizadas del software, carencia de antivirus o falta de controles de acceso robustos, entre otros).

- Descentralización del acceso, lo que difumina el perímetro de seguridad.
- Aumento de los ataques provenientes de hackers, grupos activistas y crimen organizado que tratarán de aprovechar las debilidades tecnológicas y el temor y/o necesidad de información de las personas acerca de la pandemia.
- Aumento de factores de estrés que afecta de manera diferente a los colaboradores como desmotivación, angustia o tedio, lo cual incrementa el riesgo de factor humano en errores o materialización de brechas de seguridad de la información.

Las organizaciones deben ser proactivas contra los ciberataques y se deben fortalecer los mecanismos de seguridad. Algunas medidas que recomendamos son las siguientes:

- Asegurar que exista una política de acceso remoto (o equivalente) indicando las condiciones de seguridad mínimas requeridas.
- Si se utiliza un cliente de escritorio remoto, asegurarse de las condiciones de seguridad.
- Implementar la autenticación multifactorial para los sistemas y recursos de acceso remoto (incluidos los servicios en la nube). Si la autenticación multifactorial no está habilitada, adaptar controles compensatorios para mitigar este riesgo.
- Fortalecer las políticas y campañas de sensibilización-concientización de seguridad informática con todo el personal, intentando que estén informados y educados en las mejores prácticas de seguridad cibernética como, por ejemplo: la detección de mensajes de ingeniería social y posibles ataques provenientes de servicios de soporte de TI falsos.
- Asegurar que los sistemas (incluyendo las VPN y firewalls) están al día con los parches de seguridad más recientes.
- Asegurar que los dispositivos de trabajo como ordenadores portátiles y teléfonos móviles tienen una configuración mínima de seguridad. Si el dispositivo utilizado por un colaborador no es de la organización, desarrollar un plan para que el mismo pueda ser asegurado de forma apropiada.
- Revisar y actualizar los procesos de gestión de incidentes y asegurarse que es posible contener cualquier ataque rápidamente y minimizar las pérdidas económicas y posibles efectos colaterales como daños reputacionales.
- Es clave continuar evaluando la seguridad de los sistemas. La mayoría de las pruebas (incluida una prueba de penetración interna) se pueden realizar de forma remota y ahora es más importante que nunca probar la seguridad del acceso remoto.

La comunicación regular sobre el trabajo a distancia de forma segura, las amenazas actuales (en particular correos electrónicos de phishing COVID-19, algunos incluso simulando comunicaciones internas de la alta dirección), la implementación de controles y actualizaciones en materia de seguridad resultan clave para mantener la salud de la ciberseguridad de una organización.

CARLOS ALBERTO GIRALDO | carlosalberto.giraldo@rsmco.co
SOCIO DE RISK ADVISORY SERVICES – RSM COLOMBIA

BERNARDO VITALE | bernardo.vitale@rsm.uy
SOCIO DE RISK ADVISORY SERVICES – RSM URUGUAY

RSMLatinAmerica
rsm.global

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM