El trabajo remoto en tiempos del Coronavirus

COVID-19

La declaración del COVID-19 como una pandemia, ha obligado a empresas de todo tipo a adoptar modelos de trabajo remoto, algunos de estos improvisados, que minimícen los riesgos de contagio por el virus y garanticen la continuidad de sus negocios.

Sin embargo, es necesario tener en cuenta una serie de recomendaciones para que las redes empresariales, no terminen siendo las afectadas por ataques informáticos.

SITUACIONES DE CIBER-RIESGO

Uso de equipos
personales, no corporativos

Uso de redes
públicas o no seguras

Falta de un plan
de continuidad del negocio

Falta de políticas
de seguridad internas

MEDIDAS DE CIBERPREVENCIÓN

Realizar conexiones
a través de VPN

Usar contraseñas
seguras (alfanúmericas)

Precaución ante
e-mails desconocidos

Concientizarse
sobre ciberseguridad

SÍNTOMAS DE CIBERCONTAGIO

Datos extraviados
o secuestrados

Identidad
suplantada

Servicios
fuera de línea

Con las recientes declaraciones de la OMS que confirman el Coronavirus como una pandemia, las medidas gubernamentales para la no propagación del virus y la decisión de algunas organizaciones que han optado por el trabajo desde casa para la prevención y cuidado de sus colaboradores, es indispensable prevenir cualquier amenaza para la seguridad de las compañías y los usuarios.

Según el estudio, Tendencias de cibercrimen en Colombia liderado por la Cámara Colombiana de Informática y Telecomunicaciones (CCIT) y otras entidades, de 2017 a hoy se reportaron 52.901 denuncias de las cuales el mayor número de hurtos se realizan a través de medios informáticos (31.058), seguido por robo de identidad (8.037), donde Bogotá fue la ciudad que más incidentes reportó (5.308), luego Cali (1.190) y Medellín (1.186).

Con esta medida, las empresas aumentan el nivel de exposición y el nivel de riesgo frente a fugas de información y accesos no autorizados. Como el colaborador no se encuentra en la oficina, que generalmente es un ambiente más controlado, el proceso de apoyo y respuesta a incidentes de ciberseguridad se hace más lento, ocasionando que el robo de información se vuelva inminente. Por lo tanto, ya no estamos hablando solo de ciberseguridad sino de la ejecución de todo un plan de continuidad del negocio, que se vuelve crítico e indispensable para cualquier organización sin importar su tamaño.

Aunque no es posible garantizar que esto no suceda, si se pueden minimizar los riesgos y la exposición de los datos, por lo que el experto en ciberseguridad ofrece las siguientes recomendaciones, tanto para las empresas como para sus colaboradores:

Diseñe una política corporativa de trabajo desde casa que defina mínimo los siguientes puntos:

- ¿Cómo van a acceder a la información de mi empresa? VPN, escritorio remoto, etc.
- ¿Quiénes tienen acceso a esta medida de trabajo remoto, y bajo qué circunstancias?
- ¿Con qué equipos van a acceder a mi información y qué protecciones de seguridad deben tener?
- Equipos propios, equipos corporativos, celulares, tablets, etc.
- ¿Cómo se debe manejar la información en esta modalidad de trabajo en casa?
- ¿Uso de medios externos? ¿Los prohibo?
- ¿Almacenamiento de información?, ¿Copia local, en la nube, en servidores corporativos?
- Procedimiento de atención y soporte en caso de requerirse.
- Responsabilidades y obligaciones del trabajador en cuestiones de seguridad de la información.

Concientice a sus empleados

Este debe ser un pilar importante en las organizaciones para que todos los usuarios sean conscientes de los riesgos a los cuales pueden verse expuestos. Si el usuario no conoce los riesgos a los cuales expone la información de la empresa y/o propia, puede ser víctima con más facilidad de muchas amenazas existentes.

Revise su conexión a internet

- Evite utilizar las redes inalámbricas gratuitas de cualquier zona pública. Estas conexiones no poseen medidas de seguridad y cualquier persona conectada a la misma puede interceptar el tráfico e incluso manipularlo.
- Si se realiza la conexión a internet desde casa, es necesario cambiar la contraseña de la red inalámbrica antes de conectarse a la red corporativa. Esto puede denegar acceso a equipos anteriores que quizá no se hayan actualizado o que simplemente usted no sabía que se conectaban a esta.
- Notifique al personal de tecnología de la empresa desde qué dirección IP se va a conectar a los sistemas, en algunas empresas se restringe el acceso a la información por medio de controles de acceso por IP a través de un Firewall u otros dispositivos de seguridad informática.

Acceso remoto a información corporativa

- Si se requiere mayor seguridad, implemente en casa del empleado soluciones de nueva generación (NGFW), existen soluciones de bajo costo que le pueden evitar muchos dolores de cabeza a futuro (robo de información, impactos económicos, entre otros).
- Evite acceder a la información de la empresa a través de conexiones vía escritorio remoto, ya que este protocolo es muy vulnerable a ataques informáticos y existen innumerables técnicas para acceso no autorizado a través de este.
- Siempre que acceda a información corporativa debe hacerse a través de una VPN para conectarse de manera segura. En lo posible que la navegación del empleado se force a través de la misma VPN para que pase por infraestructura de ciberseguridad de la empresa.
- Use contraseñas seguras. Es necesario revisarlas y fortalecerlas, recuerde que lo ideal es que sean mínimo de 10 caracteres alfanuméricos y con caracteres especiales, no deben ser relacionadas con algo que lo pueda identificar a usted, por ejemplo: fechas de nacimiento, nombres de sus hijos, mascotas, etc; las cuales debe estar cambiando de forma periódica.
- Use el doble factor de autenticación, es un sistema que complementa el método tradicional en los sistemas de acceso. A parte de requerir un usuario y una contraseña, también requiere de un tercer dato, como puede ser un código de seguridad o una huella digital. Se utiliza un código generado de manera aleatoria, como puede ser un token o una aplicación en el celular.

Asegure los equipos de cómputo

- En la medida de lo posible asigne un equipo corporativo para uso en modalidad de trabajo en casa.
- Implementar medidas de seguridad en el equipo de cómputo como antivirus de nueva generación o EDR (End point Detection and Response, como sus siglas en inglés), va a minimizar el riesgo de infección, detectando de manera proactiva, cualquier tipo de amenaza, evitando robo de información, cifrado (ransomware) y otros códigos maliciosos.
- Se debe cifrar la información corporativa para que esta esté segura en caso de robo de equipo de cómputo o dispositivo móvil del empleado.
- Mantener todos los dispositivos actualizados, tanto en sistema operativo como en sus aplicaciones.
- Contar con una protección anti robo o seguros asociados.

Además, en infraestructura empresarial se deberían seguir algunas recomendaciones en ciberseguridad, teniendo en cuenta necesidades particulares y presupuesto, que le permitirán minimizar el riesgo de robo de datos:

- Control de acceso a la red: la empresa debería contar con un sistema de control de accesos NAC (Network Access Control) para poder vigilar qué equipos pueden acceder a la red, según políticas de gestión de dispositivos y políticas corporativas.
- Firewall de Nueva Generación (NGFW): la empresa debería contar con un dispositivo de nueva generación para protegerse ante amenazas y minimizar los riesgos que comprometan la información corporativa, en este dispositivo es imperativo revisar constantemente su capacidad, ya que al aumentar el trabajo desde casa (a través de VPN), aumenta el requerimiento de recursos de este equipo.
- Prevención frente a la pérdida de datos (Data Lost Prevention - DLP): las soluciones DLP se utilizan en el proceso de monitoreo de sucesos que pueden ocasionar la filtración de información, con el fin de evitar fuga de información confidencial.
- Análisis de tráfico de red autónomo, de aprendizaje automático (Network Traffic Analysis - NTA): detecta amenazas nuevas o internas que surgen de comportamientos maliciosos y evita exfiltraciones de datos.

Por último, le recomendamos prestar especial atención a toda la información que se recibe sobre coronavirus o COVID-19. Evite hacer clic en los enlaces que parecen sospechosos y solo descargue contenido de fuentes confiables que puedan verificarse, haciendo búsquedas directamente en las páginas de las entidades y asegurarse que no proviene de ciberdelincuentes.

GammaCSOC

By Gamma Ingenieros

Si está interesado en implementar una estrategia de trabajo en casa para su equipo de trabajo, no dude en contactarnos. Contamos con soluciones y servicios soportados en un equipo de expertos que estarán prestos a asesorarlo en la implementación de un plan de continuidad para su negocio.

Expertos en Ciberseguridad
e Infraestructura Tecnológica

Bogotá: Calle 166 No. 20-45 — PBX: +5714076000

Cali: Carrera 18 No. 10-38 — PBX: +57 2 5574147

Medellin: Calle 15 No. 35-1 Edificio C34 — PBX: +57 4 3229906

Barranquilla: Carrera 49C No. 75 - 47 — PBX: +57 2 5574147

www.gammaingenieros.com