DECALOGO PARA MINIMIZAR LOS RIESGOS CIBERNÉTICOS EN EL TELETRABAJO

Con motivo del Estado de Alarma decretado por el Gobierno de España, muchas empresas han implementado **medidas de teletrabajo** para mantener su actividad. Esto supone que muchos **trabajadores/as accederán a servidores y a datos confidenciales desde conexiones que no están bajo el control de la empresa**. En este contexto, desde Grupo S4 invitamos a tomar medidas preventivas para evitar ciberataques ya que, en el caso de que se produzcan, es fundamental reaccionar en menos de 24 horas.

Para blindar los datos y la información que se maneja en las conexiones remotas y evitar ser víctima de los hackers o minimizar los efectos de los mismos, el **Departamento de Ingeniería y Empresas de S4** recomienda:

1. La contratación de un Seguro de Riesgos Cibernéticos

El Seguro de Riesgos Cibernéticos contempla una serie de coberturas que aportan la tranquilidad de saber que, en caso de ataque, existirá una actuación rápida y eficaz. Para ello, antes de su contratación, se realiza un estudio preliminar de la organización, analizando los sistemas informáticos de los que dispone para detectar posibles vulnerabilidades en el ámbito de las telecomunicaciones e Internet. Una vez reconocidas las debilidades de este sistema, se ofrecen soluciones y protecciones óptimas a través de un proyecto a medida cuyo fin es reducir las consecuencias en el caso de que se produjese. Entre otras coberturas, se pueden incluir:

- Asistencia técnica 24 horas, 365 días al año
- Cobertura de las pérdidas procedentes de la interrupción
- Recuperación de los datos borrados y restablecimiento de los accesos digitales
- Reparación de los equipos dañados y descontaminación de virus
- Servicio forense: gastos de investigación para la obtención de evidencias con valor legal
- Costes legales que puedan derivarse del ataque
- Gestión de crisis y recuperación de la reputación
- Comprobación del funcionamiento adecuado de todos los sistemas

2. Usar de herramientas tecnológicas corporativas

Los dispositivos facilitados a los trabajadores/ as deben disponer de todas las herramientas necesarias para garantizar el acceso seguro desde casa: firewall, protección antivirus, acceso VPN, entre otros. Debe concienciarse a todos los miembros del equipo de la necesidad de cumplir con los protocolos indicados.

3. Evitar descargas improvisadas

Los/as empleados/as a menudo trabajan en equipo y eso puede significar el uso de herramientas colaborativas como plataformas de videoconferencia. Se debe dotar a todos los dispositivos de estas herramientas para evitar descargas particulares: una ejecución de software indebida puede abrir la puerta a alguien no autorizado.

4. Conectar a través de VPN

Una VPN (Red Privada Virtual) puede ayudar a proteger los datos que se envían y reciben mientras se teletrabaja. Puede proporcionar un enlace seguro entre empleados/as y empresas

encriptando datos y escaneando dispositivos para detectar software malicioso como virus y ransomware. Oculta lo que se hace en línea durante la conexión remota: acceso a datos financieros, documentos estratégicos o datos de clientes entre otros.

5. Definir medidas de actuación ante emails falsos

Los ciberdelincuentes están explotando el brote de coronavirus para enviar correos electrónicos falsos con enlaces peligrosos, suplantando incluso la identidad de miembros del equipo, simulando que se envían desde la propia compañía. Ante cualquier duda, no hacer click sin previa autorización de informáticos/as expertos/as.

6. Mantener el equipo y el software actualizado

Los avisos de actualización deben ejecutarse, preferiblemente de manera automática. Saltarse dichas actualizaciones puede derivar en fallos de seguridad, haciendo que los dispositivos se vuelvan más vulnerables ante ataques. Además, suelen corregir errores, agregar nuevas funciones que blinden todavía más la información que se maneja y eliminar aquellas obsoletas

7. Precaución ante las aplicaciones de chat

A pesar de que pueden resultar útiles en las relaciones entre los miembros del equipo a nivel profesional, es necesario controlar el tipo de información que se envía a través de los chats colaborativos. En muchas ocasiones no queda claro cómo de segura es la plataforma que almacena la información, existiendo algunas que nunca eliminan el historial y, en caso de hackeo, se podría acceder a los datos enviados en un periodo de tiempo concreto.

8. Monitorizar los activos de IT

Mantener bajo control e inspeccionar continuamente los activos internos de IT. Los hosts, sistemas y servidores internos pueden ser más susceptibles a ataques debido a que los empleados/as en remoto acceden a ellos desde dispositivos, ubicaciones y redes nuevas y desconocidas.

9. Realizar una copia de seguridad de los datos

La mayoría de compañías hacen copias de seguridad de sus redes habitualmente, por lo que durante la modalidad de teletrabajo, es necesario comprobar que se siga realizando.

10. Recordar las normas

Es recomendable que, de manera habitual, se recuerden las políticas y mejores prácticas de seguridad informática a distancia para garantizar un trabajo en remoto seguro.

Desde **S4** seguimos ofreciendo un servicio que **asegure** la **excelencia**, caminando a vuestro lado más cerca que nunca. Para obtener más información sobre los Seguros de Riesgos Cibernéticos, facilitamos el correo electrónico empresas@s4net.com, estando también disponibles a través de **nuestro formulario web** o perfiles sociales de **Linkedin**, **Facebook** o **Twitter**.