Publicado en Madrid el 20/05/2020

La ciberseguridad, clave para la reputación de la empresa, según The Valley

El "boom" repentino del teletrabajo y el incremento de la actividad online puede impactar en la vulnerabilidad de empresas y particulares y en el desarrollo de la economía digital

La pandemia ha sacado lo mejor de la tecnología, pero también lo peor. Si bien es cierto que internet y el entorno digital ofrecen infinitas ventajas, también se debe tener en cuenta que, el “boom” repentino del teletrabajo y el incremento de la actividad online, podrían tener un impacto en la vulnerabilidad tanto de particulares como de empresas ante los riesgos digitales. La buena noticia es que la pandemia del COVID-19 ha aumentado el grado de concienciación sobre la importancia de la ciberseguridad, según el Centro Criptológico Nacional (CCN-CERT).

En este contexto de digitalización es importante que las empresas se centren en garantizar la seguridad en todos los procesos de trabajo, de su información y de sus sistemas, y que también, los propios usuarios tomen conciencia y sean responsables de la información que comparten y los sitios web, aplicaciones o herramientas con las que interactúan. Un ciberataque puede impactar en la empresa no solo a nivel económico sino también en su reputación.

Los expertos del ecosistema de conocimiento The Valley han identificado algunos factores a tener en cuenta de cara a reducir la vulnerabilidad a riesgos digitales:

La transformación digital y “cultural” debe incluir ciberseguridad

Es sumamente importante que al momento de transformar los procesos de una empresa se prepare a los empleados para convivir y trabajar con estas nuevas herramientas y procesos, y la ciberseguridad es una materia clave que se debe abordar a la hora de implementar medidas como el teletrabajo. La empresa debe informar a los empleados las “buenas prácticas” a seguir para efectuar el trabajo sin riesgos, formarles para identificar técnicas de phishing u otros riesgos que pueden encontrar en el entorno online. Por su parte, los profesionales deben ser conscientes de los riesgos digitales y tener cuidado con qué información comparten en sitios públicos o en sus propias redes sociales, asegurar que sus contraseñas cumplen los mínimos de seguridad y demás recomendaciones básicas.

Reuniones virtuales y videollamadas seguras

En las últimas semanas se ha cuestionado la seguridad de las herramientas disponibles para hacer videollamadas y las medidas de seguridad que se deben cumplir para ello. El Centro Criptológico Nacional (CCN-CERT) ha definido algunas pautas de seguridad para realizar reuniones virtuales entre las que se incluye no aceptar llamadas/chats de usuarios que no se conozcan, no compartir datos sensibles como contraseñas durante las videollamadas, descargar las aplicaciones únicamente de markets oficiales o programar las videollamadas con el número exacto de participantes, entre otras.

Expertos de IT, agentes imprescindibles en la digitalización

Los expertos de IT suelen ser los más concienciados sobre los riesgos que existen en la red y los que tienen los conocimientos para garantizar la seguridad. Además, también es importante que los líderes de negocios y de innovación estén al tanto con la seguridad de las infraestructuras con las que se trabaja en la empresa de cara a garantizar que todos los protocolos de trabajo sean seguros.

El teletrabajo no es algo temporal sino un cambio que ha venido para quedarse
El teletrabajo va para largo y si bien algunas empresas ya estaban preparadas para este cambio de paradigma que ha traído la pandemia, muchas otras han tenido que ir tomando medidas de forma espontánea para poder seguir con su actividad normal. Es importante que las empresas refuercen ahora -más que nunca- sus medidas de seguridad, pues ya el trabajo en remoto y la distancia laboral no se presenta como una solución pasajera o temporal, sino que es un cambio que ha venido para quedarse.

Trabajar siempre con los dispositivos administrados por la empresa y con las aplicaciones corporativas
Los portátiles, móviles de trabajo y demás dispositivos ofrecidos por la empresa para realizar la actividad laboral suelen estar configurados con medidas de seguridad especiales que les hacen más seguros. Una estrategia común es bloquear el acceso a páginas webs que puedan ser peligrosas o incluso, hacer necesaria la “solicitud” de descarga de alguna aplicación de trabajo que esté fuera del “application hub” de la empresa.

Una VPN segura y redes wifi privadas para asegurar la información
Es muy importante garantizar que la VPN mediante la cual se conectan los empleados en remoto para trabajar diariamente sea segura y privada. Las empresas deben evitar vulnerabilidades a toda costa para prevenir que su información y sus servidores puedan ser hackeados. De la misma forma, cada empleado es responsable de que las redes wifi a las que se conecten desde su lugar personal de trabajo sean redes privadas y personales protegidas bajo contraseña, y no redes públicas o de acceso común.

Datos de contacto:
Redacción

Nota de prensa publicada en: Madrid

Categorías: Nacional Marketing E-Commerce Ciberseguridad Recursos humanos