Los verdaderos riesgos en ciberseguridad para las empresas en época de teletrabajo

La insólita situación de la pandemia ha obligado a todas las industrias a volcar sus esfuerzos en la búsqueda de estrategias para mantener su operatividad a pesar de la crisis. Como consecuencia, uno de los primeros retos fue el salto repentino al trabajo remoto.

El factor de obligatoriedad que llevó a las empresas a activar esta modalidad evidenció, por un lado, que muchas no estaban preparadas para ese esfuerzo y, por el otro, que aunque algunas ya lo realizaban de forma parcial, no contaban ni con la capacidad para sostener esta forma de trabajo para todos sus colaboradores, ni con la información apropiada sobre cómo hacerlo.

De ahí la proliferación de textos, asesorías y seminarios enfocados a cómo enfrentar la situación, a través de discursos sobre la importancia del teletrabajo, las rutinas del colaborador para un trabajo remoto llevadero, e incluso tips para la conectividad. Sin embargo, hay un aspecto de mayor o igual relevancia en las empresas, y del cual no se ha hablado lo suficiente: la ciberseguridad.

Los datos son más vulnerables

El afán de implementarlo no solo ha mostrado algunas carencias o fallas en la disposición de los recursos, sino que, al no asegurar los canales y medios de conexión para la continuidad en el manejo de información y datos de los colaboradores, las vulnerabilidades aumentaron de forma exponencial.

Factores como pasar a usar un dispositivo personal, computador o celular, o conectarse a la red del hogar (muchas veces compartido por varias personas en simultáneo), son algunos de los escenarios que exponen a las empresas a inminentes riesgos en materia de cibercrimen, y que vuelve urgente la necesidad de garantizar la seguridad de los teletrabajadores durante su labor remota.

Phishing, malware, robo: riesgos a los que me enfrento

Desde que surgió la pandemia se ha registrado un incremento de amenazas que facilitan el fraude, intentos de phishing, ataques relacionados con malware y el robo de credenciales, haciendo uso de dominios relacionados con el coronavirus (algunos muy parecidos a instituciones oficiales).

Esto demuestra, básicamente, la importancia de que las organizaciones aumenten sus esfuerzos para proteger tanto a la empresa como a sus colaboradores, con el fin de evitar la entrada de agentes maliciosos que pueden terminar afectando de formas irreversibles los datos e información.

axity | CISCO Partner Gold Certified

Durante el Q1 de 2020 el Anti-Phising Working Group ha arrojado datos relevantes sobre este tema:

Se detectaron
165772
sitios de phishing

El objetivo de los ataques han sido principalmente usuarios de webmail y SaaS.

El 75%

de los sitios de phising ahora usan SSL, pasando como sitios seguros ante los usuarios.

En marzo de 2020 se recibieron
8 reportes
de ataques phising

contra Zoom y sus usuarios, sin embargo, en abril se recibieron **1054** reportes.
Algunos de los ataques envían invitaciones falsas a reuniones de Zoom que los llevan a páginas falsas para robar sus cuentas y passwords. Otros ataques dan la oportunidad de descargar el cliente Zoom pero en cambio descargan malware.

Era de esperar que el cibercrimen aprovechara la situación de pánico ocasionado por la pandemia e incrementaran los ciberataques, comprometiendo la seguridad de empresas y usuarios.

Soluciones al alcance

Además de los desafíos en soporte, conectividad y adaptación, garantizar la seguridad es primordial para un desempeño adecuado y confiable del teletrabajo y se deben aplicar las soluciones adecuadas que mejor soporten a la compañía.

Y aunque algunas empresas ya cuentan con políticas corporativas, el confinamiento ha permitido una flexibilización de las mismas que debe analizarse con cuidado. Por ello, algunos expertos en ciberseguridad de Axity aconsejan no solo conservar estas políticas sino hacer revisión y asegurar el cumplimiento de las mismas, desde el acceso a los recursos corporativos.

Adicionalmente a la conexión a través de concentradores de VPN, también aconsejan fortalecer o establecer, por medio de soluciones de protección, una política de filtrado de contenido, y robustecer la autenticación con un doble factor (haciendo uso de tokens, por ejemplo) que permitan una navegación segura, una información protegida, evitando la entrada de los agentes maliciosos.

Ya sea que los colaboradores trabajen con los dispositivos brindados por la empresa, o hagan uso de recursos propios, la seguridad debe primar.

La seguridad también es cultural

La implementación de un teletrabajo seguro es, además de todo, un asunto cultural. Al aceptar que el trabajo remoto conlleva peligros y riesgos, se empieza un proceso por identificar las amenazas y bloquearlas. Pero, para lograrlo, las organizaciones deben garantizar la formación de sus empleados, con el fin de que ellos también puedan identificar vulnerabilidades, comprender la importancia de asegurar su privacidad, adoptar buenas prácticas y crear un entorno más confiable, en medio del proceso de adaptación complejo.

El teletrabajo será exitoso en su organización
cuando logre ser realmente seguro.

axity | Cisco Partner Gold Certified

Fuentes consultadas:

Anti-Phishing Working Group. (Abril de 2020). Phishing activity trends reports. https://apwg.org/trendsreports/

Security Boulevard. (6 de abril de 2020). A Round-up of Data Breaches in March 2020. https://securityboulevard.com/2020/04/a-round-up-of-data-breaches-in-march-2020/

Quiroga, M. (15 de mayo de 2020). La covid-19 acelera la implementación de soluciones criptográficas. Dinero. https://www.dinero.com/tecnologia/articulo/la-covid-19-acelera-la-implementacion-de-soluciones-criptograficas/286364

Axity. (2 de abril de 2020). Seguridad Axity-Cisco: Incrementa la seguridad para tus trabajadores remotos. Youtube. https://www.youtube.com/watch?v=cYoxlQ9ovno&t=621s