Las empresas españolas desprotegidas por el aumento de las vulnerabilidades a raíz del COVID-19

Muchas compañías, ante el Estado de Alarma, necesitan que sus empleados lleven a cabo su trabajo en remoto con la "mayor normalidad" posible, sin embargo, no son conscientes de las vulnerabilidades que traen consigo la improvisación y el desconocimiento, así como del aumento desmesurado de los ciberataques de los últimos días

Madrid, 20 de marzo de 2020.- OneseQ, el área de ciberseguridad de Alhambra IT, advierte de la necesidad de proteger los sistemas empresariales en la crisis originada por el coronavirus y el consiguiente aumento desproporcionado de los ciberataques.

Tras el cierre de centros docentes y la posterior declaración del Estado de Alarma en el país, los departamentos de TI de las compañías han estado buscando soluciones de trabajo remoto con el objetivo de garantizar la continuidad de sus negocios. Sin embargo, las vulnerabilidades generadas por la "inexperiencia" sobre el teletrabajo seguro y el aumento de los ciberataques hacen que la situación sea poco alentadora para las compañías. Ya que, todo ello coloca a las empresas en una situación de sobreexposición hacia los ciberatacantes.

Según investigadores de Proofpoint, el volumen de los ciberataques vía correo electrónico relacionados con el COVID-19 representa uno de los mayores volúmenes de ataques en la historia bajo un mismo tema, aunque materializados en distintos tipos de amenazas: phishing, adjuntos y enlaces maliciosos, compromiso de cuentas de correo empresarial, landing pages falsificadas, donwloaders, spam, malware, etc.

"Muchas compañías se encuentras desesperadas en este momento de crisis—asegura José María Ochoa, Area Manager de OneseQ— por lo que recomendamos fervientemente que no tomen medidas precipitadas y que, antes de actuar, sopesen las consecuencias a corto, medio

y largo plazo. Desde nuestra compañía aconsejamos a nuestros clientes evitar una serie de actos que podríamos considerar como temerarios: configuraciones débiles de firewalls, hacer uso de equipos (de la compañía o personales) sin protección, conectarse a Internet sin control a través de redes domésticas o wifis compartidas, etc.".

Desde OneseQ, compañía especializada en identificar, proteger, detectar, responder y recuperar en el ámbito de la seguridad de las compañías, aconsejan seguir una serie de recomendaciones básicas:

- No lanzar servicios empresariales que se expongan a Internet por primera vez. No abrir ERP, CRM, etc. que no estén bien diseñados y preparados para ser accedidos de manera segura desde Internet. Si no hay más remedio, limitar las conexiones, protegiéndolo detrás de un FW, WAF, etc.
- Hacer que el desktop corporativo siempre lance la VPN al arrancar y no dejar la opción en manos el usuario, que además puede no estar acostumbrado a su uso.
- Activar la protección de EndPoint a todos los equipos remotos y procurar que no sea el antivirus gratuito.
- Intentar que la navegación de esos usuarios sea controlada, a través de la salida corporativa, para así que sea filtrada por los equipos corporativos de seguridad de la compañía.
- Revisar las reglas del Firewall
- Seguir las políticas de permisos que estén activadas, elevarlas y controlarlas, evitando hacer nuevos grupos y permisos para que no queden en el olvido y sean una posterior puerta de entrada.
- Preparar una pequeña guía de uso a los usuarios.
- Mantener informados a los usuarios en buenas prácticas IT.

Ochoa destaca la importancia de realizar las cosas lo más serenamente posible: "Lo más importante es identificar los riesgos que van surgiendo y asumir que cuando volvamos a la situación de partida podamos recuperar todo el control sin dejar abiertas cosas por distracción, prisas e improvisaciones. Es más, desde OneseQ, nos ponemos a disposición de todas aquellas compañías que precisen asesoramiento o necesiten implantar servicios de ciberseguridad activa en estos momentos tan cruciales para todos".