

Ciberseguridad en tiempos de la COVID-19: IBM alerta de un incremento de los ciberataques durante el primer trimestre de 2020

- El equipo de seguridad de IBM ha detectado un aumento del 40% en los ataques de ciberdelincuentes a nivel mundial
- Desde el pasado mes de marzo también se ha experimentado un crecimiento de más del 5.000% en el spam relacionado con el COVID-19
- En muchos casos los ciberdelincuentes han aprovechado el contexto del trabajo en remoto, totalmente nuevo para muchas organizaciones, para atacar

Madrid, 1 de junio de 2020 – La crisis generada por la COVID-19 ha obligado a transformar el modo en el que trabajan las empresas. Según [datos](#) del Instituto Valenciano de Investigaciones Económicas, uno de cada tres españoles ocupados han teletrabajado como consecuencia del avance del virus durante los últimos meses.

El trabajo en remoto, totalmente nuevo para muchas organizaciones, ha sido aprovechado por los ciberdelincuentes para explotar vulnerabilidades y atacar los sistemas de las empresas. Según datos de [IBM X-Force IRIS](#), durante los tres primeros meses de 2020 se ha detectado un incremento global del 40% en la cantidad de ciberataques en comparación con el mismo período del año anterior. En el caso específico de la zona de Europa, Oriente Próximo y África, que fue una de las primeras áreas en verse impactada por el virus, este aumento ha sido de un 125%.

Los criminales se han servido de la incertidumbre generada por la pandemia y el cambio al teletrabajo para lanzar ataques muy centrados en los usuarios que trabajan desde casa, utilizando malware, campañas de spam, de phishing y ransomware.

Una de las técnicas que más están utilizando los cibercriminales para atacar está siendo el spam. IBM X-Force ha identificado un incremento enorme en las cifras de ataques de spam, en muchos casos centrados en la suplantación de entidades bancarias, ofreciendo ayuda financiera falsa o notificaciones engañosas relacionadas con transferencias y pagos, aprovechando la situación generada por la pandemia. Desde el pasado 1 de marzo, se ha detectado un aumento de más del 5.000% en el spam relacionado con la COVID-19. Las pequeñas empresas están siendo uno de los objetivos preferidos de este tipo de ataques; los cibercriminales contactan con las organizaciones fingiendo ser entidades gubernamentales para compartir falsas ofertas de ayuda. Al abrir archivos adjuntos, los usuarios ejecutan un malware que, mediante un troyano de acceso remoto, permite al atacante acceder al dispositivo de la víctima.

Los expertos de IBM han observado que este tipo de emails fraudulentos detectados contenían algunas faltas de ortografía y frases mal construidas. Unas erratas que pueden dar pistas para detectar una información falsa, pero que en ocasiones el usuario pasa por alto debido al contexto de preocupación y crisis actual. “Los cibercriminales tienden a aprovechar la actualidad en beneficio propio. En un momento como el que vivimos, en el que recibimos tanta información, resulta muy fácil que un usuario pueda hacer clic inadvertidamente en archivos adjuntos o en enlaces dentro de correos electrónicos relacionados con la COVID-19. La confusión y la incertidumbre son la combinación perfecta para lanzar este tipo de ciberataques”, ha señalado Susana del Pozo, directora de servicios de seguridad en IBM España, Portugal, Grecia e Israel.

Con tal de hacer frente a este tipo de ataques de spam, los expertos de seguridad de IBM recomiendan utilizar siempre fuentes de información fiables, no abrir archivos adjuntos no solicitados, estar alerta con los mensajes con una ortografía extraña o con errores tipográficos, y ser extremadamente cuidadosos con aquellos correos o mensajes relacionados con la COVID-19 no solicitados, especialmente aquellos relacionados con fondos de ayuda o cheques de desempleo. También se recomienda no utilizar la dirección de correo de la empresa para registrarse en servicios que se utilicen de forma privada, y evitar proporcionar información bancaria o de la tarjeta de crédito por teléfono. Además, para cualquier duda relacionada con el avance de la pandemia, la OMS ha creado [una web](#) con información oficial y detalles sobre spam, estafas y ciberseguridad.

Los desafíos de ciberseguridad en el contexto actual

La situación que se está viviendo actualmente en todo el mundo provoca que las empresas se estén enfrentando a desafíos sin precedentes que, en muchos casos, pueden comprometer su seguridad. Por ejemplo:

- Pérdida de tiempo: las empresas que no teletrabajaban han tenido que centrar sus esfuerzos en movilizar a sus empleados. Esto ha supuesto que bajen la guardia y hayan dejado de hacer seguimiento

sobre posible actividad maliciosa, lo que ha sido aprovechado por los cibercriminales para llegar hasta sus redes corporativas, y mantenerse sigilosamente en ellas con el objetivo de perpetrar un ataque futuro.

- Falta de visibilidad: Aquellas empresas que no habían migrado a la nube tienen por delante el reto de actualizar sus soluciones de seguridad para adaptarse al teletrabajo y obtener la visibilidad que se necesita para monitorizar su red.
- Falta de herramientas: al trabajar desde casa, muchas empresas se encontrarán sin herramientas como *Endpoint Detection Response* (EDR) y *Managed Detection and Responses* (MDR) con las que se hacen análisis forenses de sus sistemas. Hacer estos análisis desde un ordenador portátil lleva días.
- Falta de recursos: Al trabajar en entornos remotos ocurre, también, que los responsables de seguridad no cuentan con los mismos equipos y pantallas que cuando están físicamente en la oficina, con lo que la falta de recursos también supone una desventaja.
- Por último, el teletrabajo conlleva utilizar herramientas de colaboración a las que los equipos pueden no estar acostumbrados, de forma que en algunos casos puede haber más dificultad para comunicarse e intercambiar ideas o problemas. Aquellas organizaciones que ya trabajaban con este tipo de herramientas, como Slack o Teams, y que además ya habían adoptado soluciones Cloud y servicios SaaS, han podido hacer una transición al teletrabajo mucho más fluida y segura.

Claves para mejorar la seguridad durante el teletrabajo

Los expertos del área de seguridad de IBM han desarrollado una serie de recomendaciones para que empleados y organizaciones puedan actuar y tomar medidas para garantizar un entorno de trabajo más seguro, también cuando se está teletrabajando.

En el caso de los empleados trabajando desde casa es importante:

- Tener el router actualizado con la última versión de firmware.
- Conectarse únicamente a una red wifi de confianza y, si es posible, a la VPN de la empresa.
- Asegurar que el antivirus está actualizado.
- Contar con una autenticación multifactor siempre que sea posible, que nos permita confirmar el inicio de sesión a través de mail o mensaje de texto.
- Asimismo, en caso de que se trabaje con un ordenador personal, es necesario que la empresa lo haya puesto a punto para poder trabajar de manera segura.
- No descargar archivos corporativos en nuestros dispositivos personales sin la autorización necesaria.

Por otro lado, si hablamos de indicaciones para las empresas es recomendable:

- Utilizar un endpoint seguro, e implementar herramientas que lo protejan de dominios maliciosos, malware y phishing.

- Es clave, también, apostar por herramientas de colaboración seguras, y verificar que aquellos empleados que trabajan con sus dispositivos personales siguen las políticas de seguridad de la empresa.
- También puede ser muy útil ensayar el plan de respuesta a incidentes que tenga la empresa, y formar constantemente a los empleados para que estén familiarizados con la seguridad en el entorno de trabajo.
- Otra medida recomendable es implementar sistemas para filtrar el correo no deseado o spam que pueda poner en peligro la seguridad de la organización y los empleados.

For further information: Patricia Núñez Comunicación Externa patricia.nunez@es.ibm.com Tlf. 637 893 754
