NOTA DE PRENSA
28 / 11 / 2019

Concienciación y anticipación, claves de Ingecom y Secura para evitar un ataque ransomware

> Coincidiendo con el Día Internacional de la Seguridad de la Información, el próximo día 30 de noviembre, ambas firmas especializadas en el ámbito de la ciberseguridad aconsejan sobre las mejores medidas para evitar este tipo de ataques

Los ataques de ransomware se han convertido en la principal preocupación de las organizaciones durante el último tramo de 2019, debido al incremento del número de empresas afectadas y la popularidad de las mismas, pero ¿cómo es posible hacer frente a este tipo de ataques cada vez más común? **INGECOM**, mayorista de valor de soluciones de seguridad IT y ciberseguridad, y **SECURA**, integrador especialista en ciberseguridad, han analizado –coincidiendo con el Día Internacional de la Seguridad de la Información que se celebra este sábado 30 de noviembre– las mejores prácticas para evitar estos ciberataques.

Un correo electrónico malicioso suele ser la antesala de un ataque ransomware. “El elemento humano sigue siendo el eslabón más débil de la cadena de la seguridad y el vector de ataque más frecuente. Técnicas como el phishing son usadas para intentar engañar a nuestros usuarios y robarles sus credenciales o tentarles a abrir un fichero con el malware de aspecto inocente. Un email confirmando la llegada de un paquete, una factura falsa o una invitación a una reunión con el jefe buscan llevar a la confusión del usuario y hacer que éste caiga en la trampa propuesta. A partir de ahí, aprovechando vulnerabilidades de los sistemas o usando las credenciales robadas, los atacantes pueden llegar a secuestrar o robar datos corporativos, con el consecuente daño para la compañía”, comenta Israel Zapata, COO de Secura.

Y es que más del 90% de los ciberataques explotan la debilidad humana, siendo el correo electrónico el principal vector de infección. Por este motivo, integrador y mayorista señalan que es importante la educación y la concienciación de los trabajadores para que sean capaces de reconocer dichos

ataques cuando se produzcan de verdad y así evitar un fatal error humano.

“Cualquier compañía puede sufrir un ciberataque de esta tipología. Sin embargo, aquellas con información de mayor criticidad se llevan la peor parte debido a la importancia y privacidad de los datos robados. Esto conlleva, además de grandes pérdidas económicas, daños tanto a su imagen como a la confianza de los clientes en las organizaciones atacadas, lo que afecta directamente a su reputación corporativa”, apunta Javier Modúbar, CEO de Ingecom.

Mantenimiento adecuado y herramientas de simulación

INGECOM y SECURA recomiendan contar con tecnologías punteras como son los antimalware de nueva generación y herramientas basadas en análisis de comportamiento que permiten detectar exploits y técnicas de ofuscación de malware en la etapa previa a la ejecución de un ataque ya sea dirigido, con archivos y tráfico de red sospechosos. “Además de tener instaladas este tipo de soluciones vanguardistas, es fundamental su correcta configuración y actualización para anticiparse a un ataque. No vale de nada contar con la última tecnología si no se mantiene adecuadamente y se afina continuamente para bloquear nuevos ataques y minimizar la exposición en caso de brechas de seguridad. Para eso es importante contar con un partner con experiencia en seguridad gestionada, que conozca bien nuestros sistemas y aporte ese conocimiento, que será clave a la hora de aparecer o no en los periódicos por ser víctimas de un ataque.”, señala Israel Zapata, COO de Secura.

Otro punto que marca la diferencia a la hora de estar prevenido ante un ataque ransomware es la formación continua del personal de una organización. “Además de poner más capas defensivas, es muy importante la formación de los trabajadores con herramientas de simulación. Así, cuando ocurra un ataque, serán capaces de identificarlo y evitarlo. En este sentido, existen herramientas de simulación automatizadas que ayudan a los responsables técnicos a ahorrar tiempo en su día a día a la vez que forman al resto de trabajadores sobre los peligros que puede acarrear un solo clic”, concluye Javier Modúbar, CEO de Ingecom.

En definitiva, en este Día Internacional de la Seguridad tanto SECURA como INGECOM coinciden “en que el reto de las empresas está en combinar el hecho de contar con tecnologías adecuadas que prevengan este tipo de ataques con la concienciación del personal, que sigue siendo el punto más débil y principal vector de entrada de ataques, y enmarcarlo dentro de la estrategia global de seguridad”.

Contacto de prensa:

JAVIER MODUBAR ALVAREZ
info@ingecom.net
944395678
http://www.ingecom.net