



Chema Alonso afirma que las empresas tardan hasta 6 meses en detectar intrusos en su red

Masterhacks - El español José María Alonso, mejor conocido como Chema Alonso, ingresó a Telefónica hace cuatro años y desde entonces es el CDO (Chief Data Officer) de la compañía a nivel global.

En un viaje por Buenos Aires, Chema tuvo una entrevista con periodistas, entre ellos BIZ, donde dió un diagnóstico preocupante acerca de la situación de los ataques informáticos. Afirma que *«la escalada es cada vez más agresiva»*.

En mayo pasado la seguridad de miles de personas se vio afectada por el ataque masivo de WannaCry, y muchos de los afectados ya no pudieron recuperar su información.

Para Chema, el problema real no son los ataques que publican los medios, sino los que quedan en el anonimato.

*«Realmente hay muchos tipos, muy profesionales, que están haciendo los famosos APT (Advanced Persistent Threat) que son muy sibilinos. Se están colando en las organizaciones con malware dirigido»*, advirtió el hacker.

Los piratas informáticos utilizan este tipo de malware para infiltrarse en redes de empresas y pedir rescate a cambio de la liberación de los archivos.

*“No hay una estimación de cuantos ataques se reportan, lo que hay es una estimación de que las empresas tardan hasta 6 meses en detectar que hay un intruso en su red”, agregó. “los tipos que están son muy profesionales. Saben todo de cómo funciona la empresa. ¿Por qué? Porque se cuelan y están durante mucho tiempo analizando, y cuando se van, se van con mucha plata. Y de esos hay una escalada altísima. Esos son los que no salen en los medios de comunicación. Los intrusos hacen cosas como leer tu correo electrónico, saben tus contratos, tu cuentas bancarias, el día que vas a cobrar algo, puede ocurrir que tomen un texto con tus palabras y le digan al que te tiene que pagar que deposite en otra cuenta y*



Chema Alonso afirma que las empresas tardan hasta 6 meses en detectar intrusos en su red

*así se llevan fortunas”.*

*“Muchas empresas cuando sufren estos ataques no los denuncian por miedo a la exposición pública. Y si no lo denuncian, no salen en las estadísticas”.*

Afirma que todos estos incidentes deben ser reportados, porque *«ayuda a que se conozca bien el problema y a tomar las medidas adecuadas para resolver el problema».*

*“No hay tecnología 100% segura y efectiva”* y debe asumirse que *“no se puede evitar el 100% de los ataques”*, dice Chema, y afirma que es indispensable tomar precauciones para resguardar la información. *“No sirve invertir en sistema súper desarrollados de detección y prevención si no haces lo básico, que es tener copias de seguridad de los archivos”.*

Refiriéndose a WannaCry, Chema opinó que *«fue más mediático que otra cosa»*, y agregó que Telefónica ya había neutralizado la amenaza a una hora de haberla detectado.

*«El impacto fue prácticamente mínimo»*, dijo. Sin embargo, no descartó la teoría de que el virus pudo *«habérsele escapado»* a su creador, debido a que *«no estaba terminado»*, su sistema de cifrado presentaba fallas y no contaba con medidas sofisticadas contra especialistas en ciberseguridad. *«Si hubiese sido más profesional hubiese sido mucho más grave»*, agregó.

Finalmente, consideró que deben desarrollarse sistemas de seguridad *«más fáciles para todo el mundo»*, que se puedan utilizar sin complejidad por personas que no tienen ni siquiera mínimas nociones de informática.

Dijo que Telefónica lanzará para fin de año sistemas de protección directamente en la red como servicio de valor agregado, y el usuario sólo deberá activarlo.

*«Creo que los que trabajamos en ciberseguridad hemos hecho mal las cosas durante mucho tiempo»*, concluye.