

Experto acerca de hackeo a EMC0: “Es sorprendente que tengan 10 años de correos disponibles online”

https://radionuevomundo.cl/wp-content/uploads/2022/10/ANCHAS-A LAMEDAS-092922-mp3cut.net_.mp3

Frente a los ataques cibernéticos sin precedentes que afectaron a organismos de alto nivel institucional, Alejandro Barros, Investigador del Centro de Sistemas Públicos (CSP) de Ingeniería Industrial, Universidad de Chile, explica el tipo de eventos que desestabilizaron tanto al sistema de información del Estado Mayor Conjunto del Ejército, como al del Poder Judicial.

En el caso del ataque que afectó a la documentación reservada del Ejército, el experto identificó una finalidad política que junto con extraer información secreta por parte del grupo Guacamaya, se buscó exponer que aquella no estaba siendo administrada adecuadamente.

En cambio, en el caso del Poder judicial existiría un propósito económico, dado el tipo de programa utilizado que requeriría un pago para el rescate de la información: “Lo que hacen es que con un software de tipo malware, se toma el control del equipo donde llegó, se replica en otros intentando invadir la red de equipos conectados cifrando la información, para pedir luego *un rescate*, un ransomware, habitualmente por medio de pago de criptomonedas buscando la menor trazabilidad, y con eso llegar una clave que permite descifrar los archivos”, explicó.

Acerca de los varios reportes de riesgo que recibió el EMC y de la falta de recursos como argumento esgrimido por el órgano

asesor, el profesor Barros observó que resulta sorprendente que tengan 10 años de correos disponibles online “porque uno podría restringir la cantidad de información si los hubieran atacado y hubieran tenido 1 mes de correo, se hubiesen robado 1 mes de correo y no 10 años”, precisó.

Si bien no es posible certificar completamente el resguardo de los datos, el académico señaló que ante eventos que reflejan el descuido en medidas mínimas para proteger datos del estado, se suma un lento avance en modernizar el marco jurídico de ciberseguridad: “antes de estos casos rara vez nos preocupa. Lo que nos ha ido ocurriendo es que no hemos logrado una política pública consistente en esta materia, tener una institucionalidad que dé cuenta de los riesgos que tenemos, si nos comparamos con países que tienen instruccionalidad bastante robusta”, observó Barros.

“Este año recién se aprobó una nueva ley de delitos informáticos la que teníamos era del año 92, 30 años atrás antes de que existieran redes sociales”, indicó.