PUBLICIDAD

GUERRA EN UCRANIA Rusia asegura que EEUU ha entrado en la guerra al entrenar soldados ucranianos

OPINIÓN / DESPUÉS DE LA PANDEMIA

¿Debe pagar el seguro los ciberataques por negligencia?

por Enrique Dans · 11 enero, 2023 - 02:36 GUARDAR

Mario Greco, CEO de una de las mayores aseguradoras europeas, Zürich, ha advertido en un artículo en el *Financial Times* que los riesgos derivados de los ciberataques a compañías están convirtiéndose cada vez más en imposibles de asegurar, y que suponen un riesgo para la industria mucho más importante que las catástrofes naturales.

La advertencia de Greco tiene, sin duda, mucho sentido. Las catástrofes naturales, en una era en la que la insistencia de muchos en no hacer nada para paliar la emergencia climática las está convirtiendo en más frecuentes e intensas, han crecido de manera significativa. Hasta el punto que superan por segundo año consecutivo los 100.000 millones de dólares. Pero la verdadera amenaza para la industria no es esa, sino la posibilidad de ciberataques con efectos dirigidos hacia partes especialmente sensibles de las infraestructuras, lo que Greco considera "ataques a la civilización".

Ciberataques que impactan hospitales e impiden su funcionamiento, contra infraestructuras de distribución eléctrica que generan enormes apagones, contra oleoductos o contra departamentos enteros de gobiernos, pueden dan lugar a daños imposibles de cubrir.

Y lo peor, además, es que hablamos de daños que son, en muchos casos, relativamente sencillos de prevenir, o cuando menos, de dificultar. Es, básicamente, como intentar asegurar a un mono cuando le das una pistola cargada y con el seguro quitado: sabes perfectamente que más tarde o más temprano, se va a pegar un tiro.

> *"Hablamos de daños que son, en muchos casos, relativamente sencillos de prevenir, o cuando menos, de dificultar"*

Las pólizas que aseguran **riesgos relacionados con los ciberataques** han ido elevando sus precios a lo largo de los últimos años. Esto es debido al incremento cada vez mayor de ataques como el *ransomware*, que suelen impactar de manera importante en la capacidad de las compañías o de las instituciones para seguir funcionando con normalidad.

Algunas aseguradoras están empezando a plantearse el uso de bonos, tradicionalmente utilizados para la prevención de catástrofes naturales, para prevenir las posibles responsabilidades derivadas de ciberataques. Otras tratan de **introducir exenciones en sus contratos** cuando se pueda demostrar que el ciberataque proviene de un gobierno, aunque ese tipo de cláusulas suelen ser frágiles debido a las frecuentes dificultades para atribuir el origen de este tipo de esquemas delictivos.

[Europa pone el foco en la regulación de la ciberseguridad]

¿Cómo actuar ante una amenaza creciente, cuando sabemos que en gran medida es el propio comportamiento de las víctimas el que la hace posible? El incremento de los ataques de *ransomware* se debe a un problema muy simple: un elevado número de compañías **prefieren, en muchos casos, pagar el rescate a los delincuentes**, aun cuando saben que están, efectivamente, tratando con delincuentes y que, por tanto, nada les asegura ni que sus sistemas volverán a funcionar tras el pago, ni que ese pago sea el único que demanden.

> *"¿Cómo actuar cuando sabemos que en gran medida es el propio comportamiento de las víctimas el que la hace posible?"*

Pero la cuestión es aún peor si sabemos que, en muchos casos, **los ciberataques se producen por actuaciones negligentes** en el lado del cliente: empleados que utilizan contraseñas extremadamente débiles o directamente absurdas como "*password*" o "12345678", o políticas corporativas directamente estúpidas como la obligación de cambiar de contraseña cada tres meses y fijar una imposible de recordar, que termina o bien con contraseñas de nuevo demasiado sencillas, o con notas adhesivas pegadas detrás de la pantalla.

¿Qué deberían hacer las aseguradoras? Fundamentalmente, **convertir la ciberseguridad en una responsabilidad compartida.** Si una compañía prefiere ahorrarse el coste de un gestor de contraseñas y martirizar en su lugar a sus empleados, o no fijar política alguna en ese sentido, debería perder su derecho a reclamar daños en caso de ciberataque.

Si la compañía decide no implementar sistemas de autenticación en dos pasos porque le parecen incómodos, lo mismo. Si por la razón que sea no actualiza puntualmente su software y, al no hacerlo, abre la puerta a ataques de todo tipo, lo sentimos, no estamos aquí para **asegurar que no le roben cuando deja la llave debajo del felpudo**.

Las medidas de ciberseguridad más básicas son esas tres, y deben estar desplegadas en toda compañía que tenga un mínimo de sentido común: en primer lugar, usar un gestor de contraseñas, algo que convierte las contraseñas en mucho más robustas, y asegurarse que los empleados entienden su uso y fijan una contraseña maestra con los adecuados niveles de seguridad.

Incluso ahora, tras el importante ataque sufrido por LastPass, uno de los gestores de contraseñas más conocidos, se sigue demostrando que usar un gestor de contraseñas, incluso cuando este es atacado, sigue siendo mucho más seguro que no usarlo.

[Esta app promete traer la privacidad del iPhone a tu Android, bloqueando el rastreo de las apps]

En segundo lugar, usar un sistema de **verificación en dos pasos**, y no mediante un correo electrónico o un SMS, sino uno seguro: una aplicación de verificación. Es fácil de instalar, fácil de usar, y genera códigos cada pocos segundos que el usuario simplemente tiene que teclear.

Y en tercero, **actualizar el software puntualmente**. Un gran número de ataques responden a vulnerabilidades ya publicadas, ya conocidas y ya corregidas, pero que muchas compañías no se molestan en actualizar.

Que sí, que **es un trabajo pesado y recurrente en sí mismo, pero es necesario** y fundamental en ciberseguridad. Lo siento, pero si tu empresa continúa utilizando un vetusto Windows XP (o cualquier cosa anterior a Windows 8), merece cualquier ataque que pueda recibir, y ninguna aseguradora debería tener que pagar por ello.

Si eres un incompetente en ciberseguridad, la responsabilidad debería ser tuya, y no deberías poder descargarla en una aseguradora. Y eso, además, permitiría ofrecer mejores coberturas a quienes realmente hacen sus deberes y se preocupan de intentar reducir su exposición a este tipo de ataques. La ciberseguridad era algo muy complejo y de especialistas, pero desde hace tiempo, sus reglas básicas están cada vez más claras. Si renuncias a ponerlas en práctica, el problema es tuyo.

SIGUE LOS TEMAS QUE TE INTERESAN

CIBERATAQUES · CIBERSEGURIDAD · COLUMNAS DE OPINIÓN · SEGUROS

PUBLICIDAD

COMENTA

PUBLICIDAD

MÁS DE ENRIQUE DANS

- Lo que dicen los números del coche eléctrico
  4 enero, 2023 - 02:47
- Las criptomonedas sí son el dinero del futuro
  28 diciembre, 2022 - 02:42
- La importancia (relativa) de ChatGPT
  21 diciembre, 2022 - 02:29
- Emergencia climática, es tarde para decir 'me quedo como estoy'
  14 diciembre, 2022 - 03:31

LOS ÚLTIMOS

Notas digitales
Aprovechar el valor presente que nos ofrece la inteligencia artificial
Paco Bree

CONVERGENCIA DIGITAL ESG
Caldo de huesos y circularidad
Lluis Altés

EL ESPÍRITU SOPLA DONDE QUIERE
Epístolas, profecías y la Reserva Federal
Juan Ignacio Crespo

LAS SIETE Y MEDIA
La cuesta de enero desnuda el eslogan de la menor desigualdad
María Vega

Ahora en portada

LA TRIBUNA
Por qué los candidatos del PSOE piden a Sánchez bajar impuestos
María Vega

DESPUÉS DE LA PANDEMIA
¿Debe pagar el seguro los ciberataques por negligencia?
Enrique Dans

LA TRIBUNA
Rebajar el IVA: una medida con efectos limitados?
Cristóbal Montoro

Sé el primero en comentar

Escribe tu comentario

NORMAS DE USO

ENVIAR

PUBLICIDAD

Operar con instrumentos financieros o criptomonedas conlleva altos riesgos, incluyendo la pérdida de parte o la totalidad de la inversión, y puede ser una actividad no recomendada para todos los inversores. Los precios de las criptomonedas son extremadamente volátiles y pueden verse afectados por factores externos como el financiero, el legal o el político. Operar con apalancamiento aumenta significativamente los riesgos de la inversión. Antes de realizar cualquier inversión en instrumentos financieros o criptomonedas debes estar informado de los riesgos asociados de operar en los mercados financieros, considerando tus objetivos de inversión, nivel de experiencia, riesgo y solicitar asesoramiento profesional en el caso de necesitarlo.

Recuerda que los datos publicados en Invertia no son necesariamente precisos o ernitidos en tiempo real. Los datos y precios contenidos en Invertia no se proveen necesariamente por ningún mercado o bolsa de valores, y puedan diferir del precio real de los mercados, por lo que no son apropiados para tomar decisión de inversión basados en ellos. Invertia no se responsabilizará en ningún caso de las pérdidas o daños provocadas por la actividad inversora que nérices basándole en datos de este portal. Queda prohibido usar, guardar, reproducir, mostrar, modificar, transmitir o distribuir los datos mostrados en Invertia sin permiso explícito por parte de Invertia o del proveedor de datos. Todos los derechos de propiedad intelectual están reservados a los proveedores de datos contenidos en Invertia.

© 2023 El León de El Español Publicaciones S.A.