

Síguenos en



FUENTES ABIERTAS Y CIBERSEGURIDAD: EL GRAN RETO DE LAS COMPAÑÍAS

## El 80% de los ciberataques corporativos están dirigidos a los empleados

Ante la mayor oleada de ataques cibernéticos a compañías, desde Grant Thornton advierten de que empleados y proveedores son dos de los eslabones más débiles de la cadena

El Centro Criptológico Nacional registra la cifra de 940.776 cibercrímenes en los últimos nueve meses, lo que supone un incremento del 21,5% respecto al año anterior

Para Grant Thornton las fuentes abiertas -OSINT, por sus siglas en inglés- pueden prevenir casos de cibercrimen y evitar suplantaciones

“En España no somos nada preventivos. La inversión en ciberseguridad es muy necesaria y eficaz”, destacan desde la firma



*Cristina Muñoz-Aycuens, directora de Forensic de Grant Thornton*

Síguenos en



03/06/2024

**Las fuentes abiertas** -OSINT, Open Source INTelligence, por sus siglas en inglés- **ofrecen en internet grandes volúmenes de información** sobre las empresas y sus empleados, lo cual, con la inteligencia adecuada, **brinda oportunidades infinitas**, pero también **riesgos importantes a nivel de seguridad y reputación** que las compañías deben tener en cuenta a la hora de tratar la información, más si cabe ante el incremento de ataques cibernéticos corporativos que se han producido en los últimos meses.

Al respecto, desde la firma aseguran que es vital que **las empresas tengan bien controlada la información que ofrecen en internet**, para evitar la exposición a riesgos de ciberseguridad y de reputación; en un contexto, en el que varios estudios señalan que los ciberataques han aumentado entre un 25 y un 30%. En el caso de nuestro país, **el Centro Criptológico Nacional registra la cifra de 940.776 cibercrímenes en los últimos nueve meses**, lo que supone un incremento del 21,5% respecto al año anterior, y según datos del Ministerio del Interior, en 2023

“El **OSINT es una herramienta muy útil para las empresas que consiste en obtener e interpretar la información** que está disponible en canales abiertos o que supongan cierto pago. Es decir, no solo es buscar a través de los canales habituales, como Google, sino también hacerlo con herramientas muy avanzadas en Deep Web, Dark Web o registros. Todo ello tiene una gran utilidad para las corporaciones, pero **también supone grandes riesgos, si no se hace de manera adecuada**, con los conocimientos y protocolos necesarios”, asegura Cristina Muñoz-Aycuens, directora de Forensic de Grant Thornton.

El OSINT, entre otras ventajas, permite analizar **la reputación de una compañía**; así, por ejemplo, en el supuesto de una adquisición se puede estudiar la reputación para operaciones de compra o la trazabilidad de activos. En el caso de la **desinformación o fake news**, permite confirmar la veracidad de las informaciones y evitar así una crisis mayor. Asimismo, **las fuentes abiertas también pueden prevenir casos de cibercrimen** y evitar suplantaciones, ya que los ciberdelicuentes suelen buscar información en estas fuentes: “**La tecnología al servicio de la ingeniería social en la lucha contra el cibercrimen**”, recuerda Muñoz-Aycuens.

### **El 80% de los ciberataques corporativos están dirigidos a los empleados**

En este sentido, la directora de Fosenic de Grant Thornton también alertó de que **ocho de cada diez ataques cibernéticos que sufren las empresas están dirigidos a empleados, a través malware o phishing**. “Parece que la ciberseguridad no es un problema hasta que ocurre y en España no somos nada preventivos en este sentido. **La**

Síguenos en



**inversión en ciberseguridad es muy necesaria y eficaz**, ya que, si ocurre cualquier problema y no hemos tomado precauciones, la empresa tiene que afrontar muchos gastos, entre lo que pueden estar los de detener su producción durante cierto tiempo”, advierte.

En este sentido, **una de las mayores amenazas es el de la suplantación de la identidad** que no solo ocurre a nivel particular, sino también en el ámbito de las compañías. Las empresas pueden tener un gran volumen de información accesible a cualquiera, con la que “los cibercriminales se pueden hacer pasar por un director financiero de cualquier compañía y llegar a generar un problema muy grave”, asegura Muñoz-Aycuens.

Otro de los riesgos comunes suele venir también por parte de los **proveedores**. Es de hecho el **ataque cibernético que ha sufrido Iberdrola**, la principal eléctrica de nuestro país, recientemente, **que ha comprometido la información de 850.000 clientes**, y que se suma a los de otras multinacionales españolas como Banco Santander o Telefónica, o incluso instituciones públicas como la DGT, que tampoco se han librado de este tipo de ataques que **pueden llegar a poner en riesgo información sensible de la compañía y terminar impactando en su reputación de forma sustancial**.

Para Cristina Muñoz-Aycuens, **“la mejor herramienta para luchar contra estos ciberataques es la prevención**, contar con una adecuada inteligencia de datos que nos permita tener toda la información disponible en internet y hacerlo de forma segura, algo en lo que el OSINT puede contribuir a evitar esas brechas de seguridad y entornos proclives a los hackeos”.

---

#### Sobre Grant Thornton

Grant Thornton es una Firma de servicios de auditoría, consultoría y asesoramiento fiscal, legal y financiero. Pertenece a una de las organizaciones mundiales líderes en servicios profesionales, Grant Thornton Internacional, con 68.000 profesionales presentes en más de 140 países. En España cuenta con un equipo de más de 900 profesionales multidisciplinar, transversal, con experiencia y visión empresarial, que da servicio a más de 3.500 clientes en 12 oficinas repartidas por el territorio nacional: Madrid, Barcelona, Bilbao, Castellón, Las Palmas, Málaga, Murcia, Pamplona, Sevilla, Valencia, Vigo y Zaragoza.

---

Para ampliar información o hablar con profesionales de Grant Thornton, no dudes en llamarnos:

Síguenos en

**DEPARTAMENTO COMUNICACIÓN  
GRANT THORNTON****POLICARPO AROCA**

Director de Comunicación

T 91 576 39 99

M 650 71 31 21

[Policarpo.aroca@es.gt.com](mailto:Policarpo.aroca@es.gt.com)**RAFAEL GIL**

Supervisor de Comunicación

T 91 576 39 99

M 681 15 65 13

[Rafael.gil@es.gt.com](mailto:Rafael.gil@es.gt.com)**Roman****Tamara Raposo**

+34 690 358 123

[t.raposo@romanrm.com](mailto:t.raposo@romanrm.com)**Ignacio Marín**

+34 602 254 999

[i.marin@romanrm.com](mailto:i.marin@romanrm.com)

Síguenos en

