

Versión en CASTELLANO

ARTÍCULO: “Por qué es necesaria una formación en ciberseguridad para Pymes y la Administración Pública”

A día de hoy la ciberdelincuencia es un tipo de delito que se está llevando a cabo con mayor frecuencia, CrowdStrike advierte que entre 2023 y 2024 los ciberataques han aumentado un 75%. Esto puede deberse a su facilidad (desde el propio domicilio de los atacantes sin la necesidad de desplazarse y solo con un nivel mínimo de conocimientos informáticos) o también a su rapidez (basta con un simple clic).

Son muchos los objetivos que persiguen los ciberatacantes, pero el principal suele ser el económico, que consiguen mediante el daño a los datos que gestionan las empresas. Además, la mayoría de los ciberataques tienen su origen en errores humanos: configuraciones incorrectas, apertura de correos maliciosos, uso de contraseñas débiles, entre otros. Estudios recientes revelan que el error humano es responsable de hasta el 95% de las violaciones de seguridad en empresas.

Uno de los ataques hacia las empresas que está creciendo de forma considerable es el que se dirige a la cadena de suministro, el cual aprovecha las vulnerabilidades de los proveedores o socios para acceder a los sistemas. Por ello, la gestión de la ciberseguridad en la cadena de suministro será un reto ineludible.

Con todo lo dicho, se podría deducir que una buena protección y formación en ciberseguridad podría evitar o limitar el daño de estos ataques. Sin embargo, todavía hay empresas (tanto pymes como la Administración Pública) que tienen esta asignatura pendiente, ya que no cuentan con medidas de seguridad para hacer frente a este tipo de amenazas diarias y cada vez más difíciles de detectar (debido en gran parte al uso de la IA por los atacantes).

Las pequeñas empresas tienden a tener el pensamiento del tipo “*somos pequeños, a nosotros no nos van a atacar*”, o “*nosotros no somos tan interesantes como las grandes empresas*”, pero todo esto es falso. Debemos tener en cuenta que:

- Los atacantes en muchas ocasiones prefieren a las pequeñas empresas, ya que suelen tener una menor protección y capacidad de respuesta frente a estos ataques, lo que las hace más atractivas.
- El pensamiento de “*nosotros no somos tan interesantes...*” es completamente erróneo, ya que las pymes tienen datos que interesan especialmente a los atacantes como: datos de los clientes (DNI, cuentas bancarias, direcciones...), facturas, acceso a banca online, etc.
- El impacto para una pyme es doble que para una gran empresa debido a sus menores recursos. En ocasiones un simple ciberataque a llevado a la pequeña empresa a cerrar sus puertas debido a las terribles consecuencias. Por el contrario, las grandes empresas tienen mayor facilidad para hacer frente a los ataques. Además, como señala Cybersecurity Magazine, que el 83% de las pequeñas y

medianas empresas no están preparadas para recuperarse de los daños financieros de un ciberataque.

Por lo tanto, es muy importante y necesaria la formación en ciberseguridad. Ello solo nos puede traer ventajas como:

- Reducción de los ciberataques causados por error del factor humano (empleados).
- Endurecimiento de las medidas de seguridad contra los ataques.
- Ser capaces de anticiparse a las amenazas y detectarlas con mayor facilidad.
- Mejorar la capacidad de respuesta ante los ciberataques.
- Se fomentan las buenas prácticas en ciberseguridad tanto dentro como fuera de la empresa.
- Protección de los propios datos personales y de los clientes y proveedores.
- Refuerzo de la confianza de la población.

Fórmate en ciberseguridad – Protege tu empresa