MONRAK

Servicio de Operaciones de Seguridad Informática para PYMES

NIS2

Redefiniendo los estándares de ciberseguridad en toda la UE, las organizaciones deben asumir requisitos de cumplimiento

La Directiva NIS2 (Normativa de Seguridad de Redes y Sistemas de Información) establece sanciones significativas para las empresas que no cumplan con los requisitos de ciberseguridad. Estas sanciones son proporcionales al impacto del incumplimiento, con un enfoque en sectores esenciales y críticos para la sociedad y la economía.

1. **Multas económicas**: Las sanciones pueden llegar a ser de hasta el 2% del volumen de negocio anual global de la entidad infractora o 10 millones de euros, lo que sea mayor. Esto depende de la gravedad de la infracción y el tipo de empresa afectada (entidades esenciales o importantes). *Cita de S2 / GRUPODIG ABOGADOS.*

2. **Responsabilidad adicional**: Además de las multas, los responsables legales de las empresas pueden enfrentar consecuencias personales si no supervisan adecuadamente las medidas de ciberseguridad, como pérdida de confianza o incluso inhabilitación para ejercer ciertos roles. *Cita de DIG ABOGADOS / DELOITTE UNITED STATES.*

3. **Otras sanciones**: En algunos casos, las autoridades pueden ordenar medidas correctivas inmediatas o imponer restricciones temporales en las operaciones de la empresa. *Cita de DELOITTE UNITED STATES.*

Estas sanciones buscan reforzar la importancia de la ciberseguridad en infraestructuras críticas y reducir el riesgo de ciberataques que puedan afectar a la sociedad. Las empresas están obligadas a notificar incidentes significativos en plazos estrictos (por ejemplo, dentro de las 24 horas siguientes a la detección del incidente)
S2 GRUPO DELOITTE UNITED STATES.

Es necesaria ayuda específica para adaptar la empresa a la normativa, siendo recomendable realizar auditorías de ciberseguridad y establecer planes claros de gestión de incidentes.

ESCENARIO GENERALIZADO

Diariamente estamos inundados por noticias sobre ataques a sistemas de información, sustracción, cifrado y rescate, o bien fraude y estafa con los datos obtenidos

«

¿Estás preparado para hacer frente a los ataques informáticos?

»

TU PRIORIDAD

Como PYME debes de anteponer la seguridad de tu información, y solo no puedes

Ofrecemos servicios de centro de operaciones de seguridad de la información y sistemas de defensa de respuesta única y común

Cada día tenemos más casos de ataques a los más vulnerables, vosotros

UN CASO CUALQUIERA QUE LE PASA A CUALQUIERA

ME ACABAN DE ESTAFAR 42.000 EUROS 💶

Así, como suena, tal y como dice la Policia ha sido un ataque casi perfecto (esperemos que lo de casi sea verdad)

Os lo voy a explicar por si ayuda o incluso por si alguien puede ayudarme y conoce a alguien que se haya encontrado con este problemón 👇

El caso es que han suplantado el mail de un proveedor nuestro, con el que tenemos muchísima confianza, le hackearon el sistema de tal manera que leían todos sus mails.

El tema es que estábamos en el proceso de pago de un servicio grande y ahí es dónde actuó el pirata; nos mandó un mail desde su propio dominio (proveedor) pasándonos unas facturas iguales, mismo PDF, todo exacto... menos el número de cuenta...

¡Que había puesto el suyo! 😣

Fuente;
https://www.linkedin.com/feed/update/urn:li:activity:7268174747543162880/

Es un caso real que ha sufrido

MARCACONDAL

CUBRETE ANTE UN ATAQUE

Asesoramiento Jurídico y Legal

Monitorización Alertas

Integración Sistemas

Consultoría, Formación y Administración de Seguridad

No estás solo para hacer frente a los ciberdelincuentes

NUESTRO VALOR

- Contamos con un área de seguridad de los sistemas para PYME´s
- Evitamos los ataques mediante nuestros servicios especializados en detección y defensa
- Descubrimos amenazas y vulnerabilidades

www.monrak.es