CYBERWAY

Telefónica Seguros
SUCURSAL EN ESPAÑA

Asegura el futuro del negocio de tus clientes con Telefónica Seguros. El seguro imprescindible para proteger a las PYMES y Autónomos de los efectos económicos y legales de los Ciberriesgos

PYMES AUTÓNOMOS

ESPAÑA Y LA CIBERDELINCUENCIA

+120.000
Ataques en 2019

68%
Infección de equipos a través de programas maliciosos

15%*
Accesos no autorizados

11%*
Fraudes

3ª
Ranking global en Ciberincidentes

ASÍ ATACAN LOS CIBERDELINCUENTES UN NEGOCIO

Con el **uso diario de dispositivos conectados a internet**, un negocio se expone a potenciales riesgos que pueden llegar a **limitar o incluso detener** su actividad empresarial

ATAQUES DDOS

Ataques DDOS o Denegación de Servicio es un tipo de ataque que consiste en denegar el acceso a una web o servidor a su legítimo propietario. También puede provocar una pérdida sustanciosa de datos

GUSANO
Se autoreproduce y busca otros equipos vulnerables

SPYWARE
Software oculto que una vez instalado obtiene información confidencial que entrega a terceros

PHISHING
Modalidad de estafa por la cual se solicitan datos personales como contraseñas a través del correo

VIRUS
Llegan a través de correos o imágenes y pueden borrar todos los archivos del dispositivo

TROYANO
Programa que se oculta en la memoria y se autoactualiza

EXPLOTACIÓN DE VULNERABILIDADES
Agujero de seguridad o vulnerabilidad es una falla en un sistema de información que se puede explotar para violar la seguridad del sistema

RANSOMWARE
Impide el acceso a determinados archivos o partes del sistema pidiendo un rescate para liberar la información. El ciberdelincuente accede al servidor de la empresa, encriptra la información y vende la clave a la víctima para recuperar los datos y no ser destruidos

Y ASÍ LO PUEDEN HACER A TRAVÉS DE SUS EMPLEADOS

VULNERACIÓN DE LA PRIVACIDAD

Situaciones en las que se sustrae un ordenador con información privada de la empresa, o actos de un empleado en los que envía o publica datos de los clientes de la empresa (ya sea por extorsión, correo falso...)

CONSECUENCIAS PARA SU NEGOCIO

COSTES

102.000€
Coste medio por ataque en España

- Costes de infraestructuras o software
- Consultores seguridad TI
- Auditores, contables
- Abogados
- Consultores gestión de riesgo
- Consultores imagen de marca

NEGOCIO

14.000
Millones de euros de pérdidas al año para las empresas españolas

- Pérdida de acceso a información crítica
- Pérdida de capacidad de comerciar
- Menor solvencia
- Daño reputacional
- Pérdida de oportunidades de negocio

***ACCESO NO AUTORIZADO**

Fallos o deficiencias de un programa que pueden permitir que un usuario no legítimo acceda a la información o lleve a cabo operaciones no permitidas de manera remota. Los agujeros de seguridad pueden ser aprovechados por atacantes para acceder a los sistemas con fines maliciosos.

***FRAUDES**

El fraude cibernético e informático se refiere al fraude realizado a través del uso de un ordenador o de Internet. La piratería informática (hacking) es una forma común de fraude, en la que el delincuente usa herramientas tecnológicas sofisticadas para acceder a distancia a un ordenador con información confidencial. Otra forma de fraude se realiza mediante la intercepción de información en una transmisión electrónica, que puede ocasionar el robo de contraseñas, el número de cuentas bancarias o de tarjetas de crédito, u otra información confidencial sobre la identidad de una persona.

FUENTES

Instituto Nacional de Ciberseguridad (INCIBE), Centro de Respuesta a Incidentes de Seguridad e Industria (CERTSI), Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC), Global Corporate IT Security Risk survey, B2B International with Kaspersky Lab, Eset, Encuesta Mundial de Seguridad de la Información 2018 elaborada por PwC.

CYBERWAY

ebroker