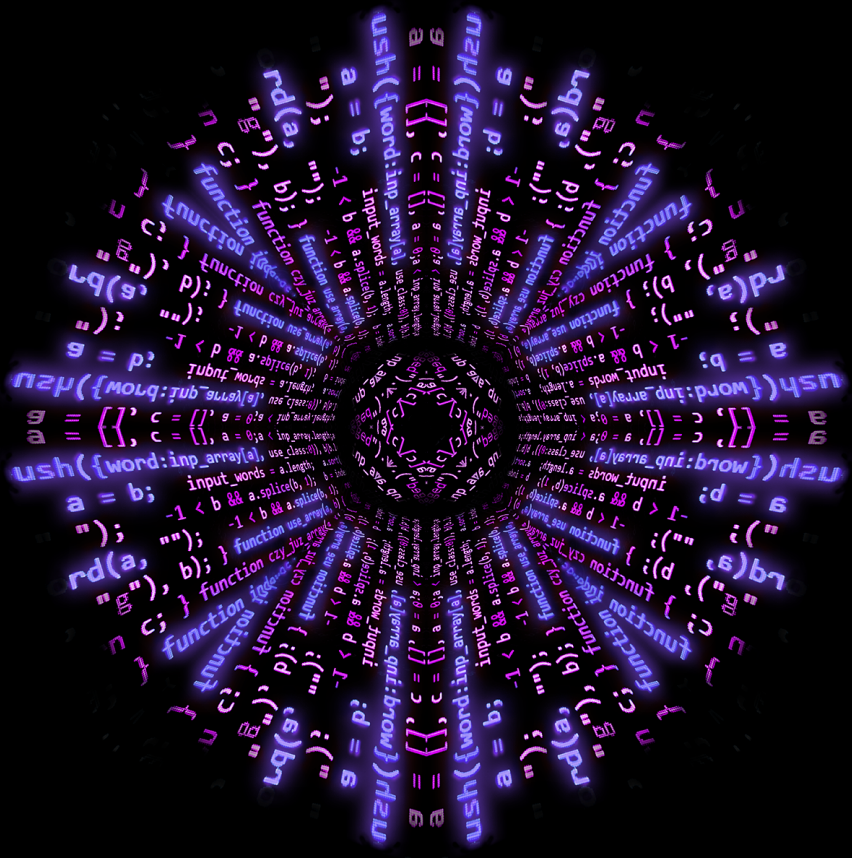
Deloitte.



Empresa manufacturera cierra por completo sus operaciones debido a un ataque cibernético

Risk Newsletter

Empresa manufacturera cierra por completo sus operaciones debido a un ataque cibernético.

De acuerdo a estudios realizados por Deloitte se ha comprado la afectación de un ciberataque que existe entre actuar en minutos y días, ver Figura 1.

Este es el caso de Pilz una empresa de automatización alemana que fue víctima de una infección de ransomware por más de una semana las operaciones de la misma se han visto interrumpidas debido a la infección del malware de crifrado conocida como BitPaymer la cual consiste en secuestrar la mayoría de los archivos almacenados en los servidores.

En un comunicado publicado en su sitio web indicaron: "*Pilz ha sido víctima de un ciberataque dirigido específicamente contra nuestros sistemas que ha paralizado las operaciones en todos los puestos de trabajo basados en servidores y equipo de cómputo, incluyendo las redes de comunicación de la compañía*". Por el momento Pilz trabaja apresuradamente para cumplir con sus encargos adquiridos previamente, además de restablecer todas las operaciones afectadas.

El lunes 21 de octubre se cumplió una semana después de la detección de la infección. Aunque Pilz ya ha logrado restablecer algunos sistemas que le permiten realizar las entregas programadas entre otras funciones, muchos de los sistemas siguen paralizados, la compañía ha indicado "*Hemos integrado un equipo de seguridad informática para resolver algunos problemas técnicos, identificar el origen del ataque, entre otras actividades*".

De acuerdo a lo mencionado por los funcionarios de la compañía, el restablecimiento total de las operaciones de Pilz se demorarán algunos días más.

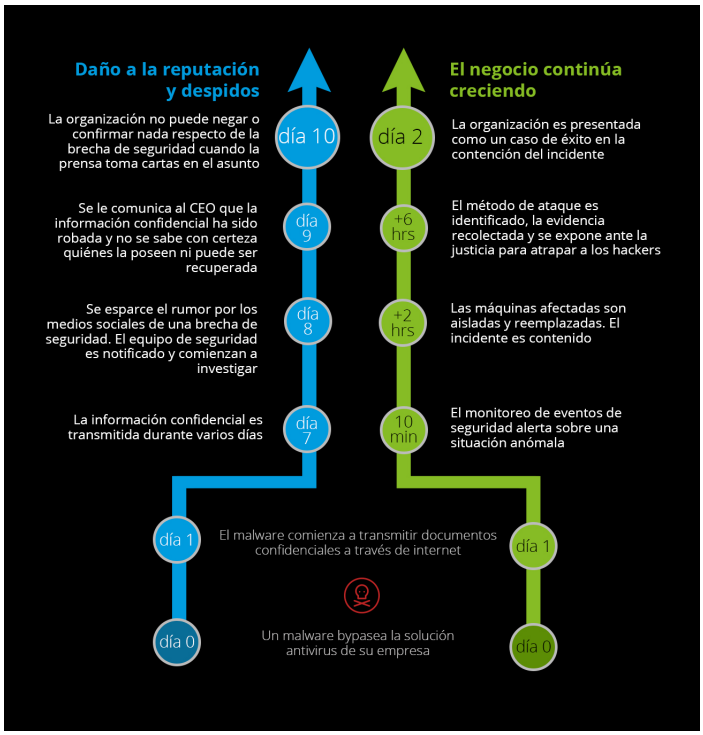


Figura 1. Diferencia entre actuar en minutos y días

El experto en seguridad informática Maarten Van Dantzig comentó que este es el típico ataque es vinculado al grupo de hackers conocido como BitPaymer. El experto afirma que descubrió algunas muestras del malware usado por este grupo en la plataforma VirusTotal, incluyendo la nota de rescate usada durante este incidente, con detalles personalizados relacionados con la compañía alemana. Finalmente, el experto añade que, por lo general, el ransomware BitPaymer es entregado a las víctimas usando el troyano conocido como Dridex (es un malware especializado en el robo de credenciales que utiliza un botnet ya establecido para expandirse ejecutando ataques de tipo mando y control).

Especialistas del Instituto Internacional de Seguridad Cibernética (IICS) agregan que este troyano se dirige contra usuarios de Windows desprevenidos mediante un documento adjunto enviado por email. Al ser abierto, Dridex es descargado, abriendo la puerta a otras amenazas, como en el caso de la compañía afectada.

Se desconoce el monto del rescate, sin embargo expertos en seguridad indicaron que los operadores de esta variante de ransomware pueden llegar a exigir un rescate de hasta un millón de dólares en criptomoneda.

Según estudios realizados por **Deloitte**, el 70% de las organizaciones afirma no tener certeza de la efectividad de su proceso de respuesta ante incidentes de ciber seguridad y sólo un 3% realizar simulaciones para probar sus capacidades efectivas de respuesta ante un evento cyber.

Y el 60% de las organizaciones tarda meses en responder y recuperarse ante un ataque. Ver Figura 2.

¿Estás preparado para un ciberataque?
Nuestros expertos te pueden ayudar.

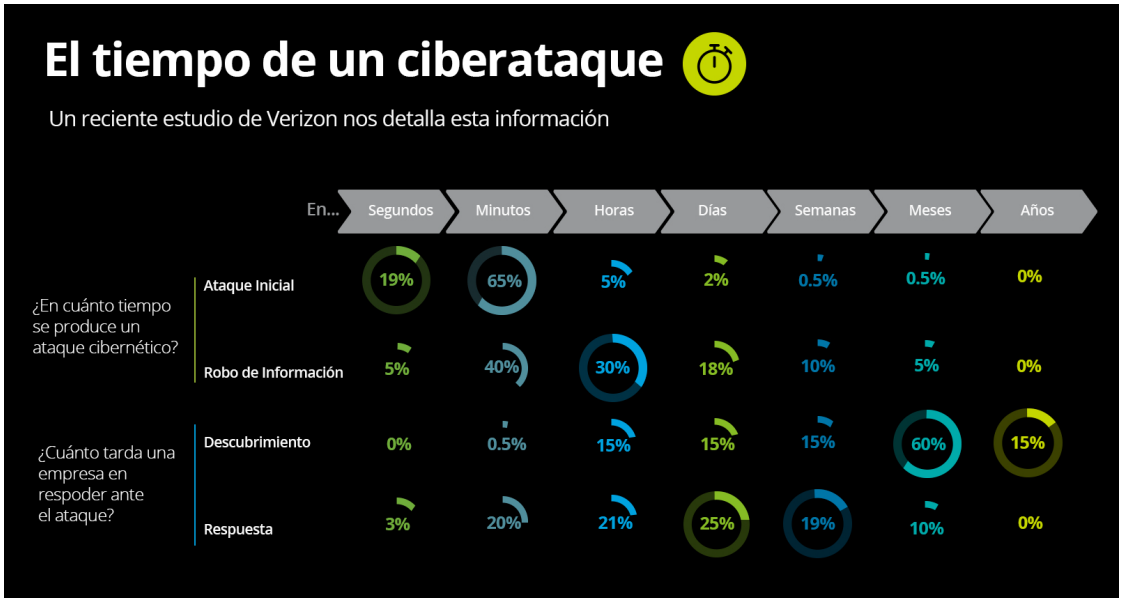


Figura 2. El tiempo de un ciberataque

Nuestros expertos

Renato Campos
Director
Risk Advisory
rencampos@deloitte.com

Evelyn Donis
Gerente
Risk Advisory | Cyber
edonis@deloitte.com

2384 6500 deloitte.com/gt @deloittegt

Deloitte.