

JORNADAS DE #CIBERSEGURIDAD EN EL ENTORNO INDUSTRIAL



ORGANIZACIONES INDUSTRIALES HAN TENIDO UN INCIDENTE DE CIBERSEGURIDAD EN LOS ÚLTIMOS 12 MESES

CONCIENCIACIÓN

Falta de concienciación en ciberseguridad desde puestos directivos



TECH OBSOLETEA

Mayoría de sistemas anticuados que difícilmente se pueden parchear o sustituir



54%



FALTA DE RESPUESTA

No se cuentan con mecanismos que permitan atribución o rápida recuperación tras un incidente.



PHISHING

Ataques como la "estafa del CEO" pueden ser devastadores si no se tienen los conocimientos adecuados.

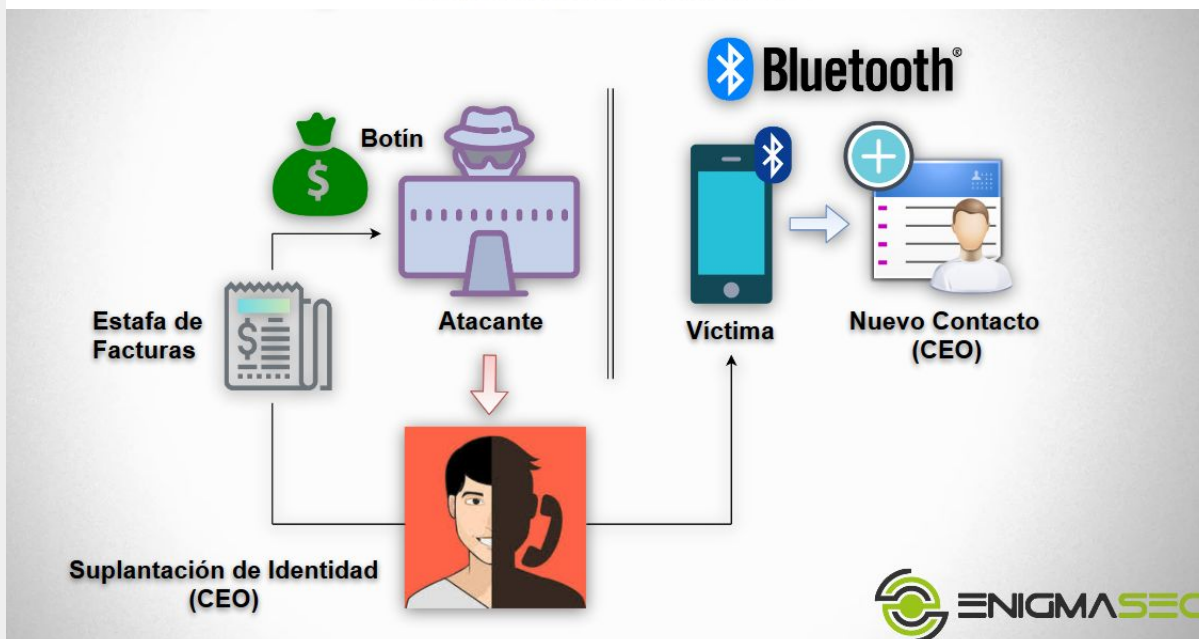
INGENIERÍA SOCIAL

¿POR QUÉ TAN IMPORTANTE?

LA MAYOR AMENAZA RESIDE EN EL ENGAÑO AL USUARIO POR CUALQUIER MÉTODO DE COMUNICACIÓN



EN LA ESTAFA DEL CEO, EL ATACANTE SUPLANTA UN PROVEEDOR LEGÍTIMO DESVIANDO EL PAGO HABITUAL A OTRAS CUENTAS BANCARIAS



EMPRESAS CANARIAS HAN SUFRIDO TRANSFERENCIAS ILEGÍTIMAS CON VALORES SUPERIORES A LOS 150.000€



73 % CASOS DE PHISHING

EN EL 2018



30% CASOS DE RANSOMWARE

EN 12 MESES

MALWARE AUTOCAD

TÁCTICA EN AUJE PARA ROBAR PLANOS EN ENTORNOS INDUSTRIALES





4

Recomendaciones MEJORAR TU Ciberseguridad

PARA ORGANIZACIONES INDUSTRIALES

1 EVALUAR ESCENARIOS



Cada organización es diferente y no todas comparten un mismo escenario de cara a una posible explotación

Conoce tu terreno, revisa tus puntos de exposición a internet y ponte en el peor de los supuestos. Sólo así podrás ver en donde necesitas invertir

2 PROTEGER



Con la información anterior, actualiza, parchea o sustituye aquellos equipos o servicios en los que se pueda intervenir

Si no es posible, protege aquellos servicios en los que necesitas tolerar ese riesgo, para que la explotación o post explotación sea la mínima posible

3 DESAFIAR LA POLÍTICA



Aunque tengas tu infraestructura controlada, todavía no ha terminado el trabajo. Es hora de desafiar las medidas adoptadas y corregirlas

Dos ojos ven mejor que uno

ENIGMASEC dispone de soluciones de Pentesting totalmente adaptables a cualquier tipo de cliente

4 RESPUESTA INCIDENTES



ENIGMABOX



Tras un incidente de ciberseguridad el tiempo de respuesta y de vuelta a la normalidad es crucial

Tener un plan de respuesta nos ayuda a atribuir el incidente y minimizar el tiempo de explotación al ataque. Pudiendo ahorrar costes en el proceso de recuperación



Enigmabox almacena evidencias y alerta en base a comportamientos sospechosos asociados a una intrusión al sistema exitosa.

Anímate a probarla sin compromiso



WWW.ENIGMASEC.COM

CONTACTO



OFICINAS

Santa Cruz de Tenerife
2ª Transversal Darsena Los Llanos 38003
Las Palmas de Gran Canaria
Avenida de los Consignatarios S/N 35008



TELÉFONO

902 - 101 - 997
610 - 410 - 110



TWITTER

@enigmasecteam



WEB

www.enigmasec.com

