TOP 10
CYBER RISKS

Grupo de Trabajo de Ciberriesgos de

AGERS – ISMS FORUM

agers | Asociación Española de Gerencia de Riesgos y Seguros

ISMS forum spain

TOP 10 CYBER RISKS

Grupo de Trabajo de Ciberriesgos de
AGERS – ISMS FORUM

AGERS - Asociación Española De Gerencia de Riesgos y Seguros
C/Príncipe de Vergara 86, 28006 Madrid

Depósito legal: M-12170-2018

ISBN: 978-84-09-01375-3

COPYRIGHT: DEP636588625615983611

COLABORADORES AGERS

Iván Alcauza – Vodafone

Javier Bastarreche Bengoa- Indra

Juan Pedro Gago – Deutsche Bank

Juan Gayá – El Corte Inglés

Álvaro González la Calle – Aena

Belén Medina – Globalvia

José Molina – Red Eléctrica Española

Eva Pérez – Transfesa

Fernando Vegas – Universidad Politécnica de Madrid

Alfredo Zorzo – One eSecurity

COLABORADORES ISMS FORUM

Concepción Cordón Fuentes, Emasa

Daniel Largacha Lamela, Mapfre

Francisco Lázaro Anguis, Renfe

Jacinto Muñoz Muñoz, Mapfre

ÍNDICE

PRESENTACIÓN

La tecnología es en estos momentos algo imprescindible en los negocios y en nuestras vidas. Cada vez está más extendida, es más fácil de utilizar y está al alcance de todos. Nos hace la vida más cómoda y la gestión de las empresas más eficiente. Pero esa sencillez de uso contrasta con lo complejo que es entenderla. Su comprensión solo está al alcance de expertos.

Esta tecnología genera nuevos e importantes riesgos. Conocer y gestionar estos riesgos no es un trabajo exclusivo de técnicos en informática. Son muchas las personas que deben intervenir para garantizar la seguridad de la información. En unos casos autorizando presupuestos económicos, en otros implantando medidas técnicas, desarrollando procedimientos, formando al personal, elaborando planes de continuidad de negocio, etc.

Difícilmente puede el personal no técnico realizar correctamente sus funciones relacionadas con la seguridad de la información si no tiene un conocimiento básico sobre esta materia.

Este es el objetivo de este documento. Facilitar el entendimiento entre el experto y el no experto en materia de ciberseguridad. Este trabajo complementa la GUIA DE TERMINOLOGÍA DE CIBERSEGURIDAD, elaborada también por AGERS e ISMS y publicada en 2017.

En esta ocasión se exponen 10 tipos de ataques. La lista se ha obtenido de una encuesta realizada por ISMS entre sus socios a finales de 2017.
Todos los ataques seleccionados tienen al menos dos características en común: son frecuentes y su impacto económico puede ser muy alto.

Algunos de los ataques enumerados pueden estar relacionados entre sí. Por ejemplo el phishing (caso 3) puede tener como objetivo final robar datos (caso 1).

Cada caso se analiza en detalle. Comienza con una descripción y casos reales para a continuación realizar un análisis que comprende el motivo, la causa, el método utilizado (cuya descripción se puede encontrar en la GUÍA DE TERMINOLOGÍA DE CIBERSEGURIDAD), el tipo de riesgo afectado, el impacto económico y los sectores más afectados. El último apartado contiene las lecciones aprendidas: que podemos hacer para prevenir ese tipo de incidentes y cómo debemos gestionarlos, incluyendo las coberturas de seguro que deberían tener las pólizas para transferir los riesgos.

Este probablemente no será el único documento que publiquemos con este título. El mundo está en constante evolución y los ciberriesgos van por delante. Surgirán nuevos casos y algunos de los publicados en este documento dejarán de ser frecuentes o tener gran impacto.

Esperamos que este documento sea una pequeña contribución para hacer el ciberriesgo más entendible facilitando su gestión.

1. FUGA DE INFORMACIÓN

1. FUGA DE INFORMACIÓN

DESCRIPCIÓN

La fuga/ robo de información se define como la filtración de información (deliberada o involuntaria) a un medio o persona que no debería conocerla.

Es uno de los mayores ciber-riesgos que tienen las empresas, derivadas del valor que la información ha tomado en las organizaciones, convirtiéndose en uno de los activos más importantes de las mismas.

Las consecuencias, y por tanto el impacto de una fuga de información son importantes en cualquier empresa ya que casi siempre derivan en daños reputacionales, daños a las operaciones, perdidas de oportunidades de negocio y/o sanciones penales, civiles, administrativas o deontológicas, en ocasiones de elevado importe.

CASOS

Una empresa podría sufrir robo/fuga de información si alguno de sus directivos pierde un dispositivo móvil sin las debidas medidas de protección, pudiendo ser accedida por cualquiera que encuentre dicho dispositivo.

Otro caso que se puede dar es cuando la empresa tira sus muebles sin asegurarse que no queda ningún soporte de información dentro de los mismos.

También cuando un atacante se introduce en los sistemas de información de la empresa.

Uno de los casos con mayor repercusión fue el de Wikileaks que en noviembre de 2010 comunicó a la prensa internacional una colección de más de 250.000 cables entre el Departamento de Estado estadounidense y sus embajadas por el mundo, transformándose en la mayor filtración de documentos secretos de la historia.

Otro caso, es Yahoo que entre 2013 y 2016 ha declarado que se habría tenido acceso a la base de datos de sus cuentas de correo afectando a más de 1.000 millones de cuentas de correo.

En septiembre 2017, Equifax declaro que unos hackers habían tenido acceso a su base de datos y, por tanto, al nombre de sus clientes, sus números de la seguridad social, fechas de nacimiento y direcciones. La filtración afecto a 145, 5 millones de cuentas y duró más de un mes, desde mediados de mayo hasta finales de julio de 2017.

MÓVIL

Europol indica que hasta el 89% del robo de datos tiene un motivo financiero o de espionaje.

En este sentido, según los últimos datos contrastados, crecieron considerablemente los casos con propósitos económicos, obtención de credenciales para desarrollar acciones de contra-espionaje chantaje en los siguientes sectores: centros hospitalarios, formaciones políticas y gobiernos de países occidentales, hostelería y comercio, o intercambiadores de divisas virtuales.

CAUSA DEL INCIDENTE

Fallos de seguridad en los sistemas de información.
Descuido por parte de los usuarios de información.

MÉTODOS DE ATAQUE

Malware, puerta trasera, rootkit, etc.
Ingeniería social.

TIPO DE RIESGO AFECTADO

Daños patrimoniales, daños reputacionales, pérdida de competitividad (robo de información confidencial), responsabilidad civil (reclamaciones de terceros), penal (por la falta de diligencia en la aplicación de medidas de diligencia debidas), etc.

IMPACTO ECONÓMICO DEL INCIDENTE

Determinar el impacto es una tarea compleja que depende de muchos factores, siendo el principal la criticidad de la información filtrada para la empresa (confidencialidad, datos personales, secretos comerciales, información técnica, etc.).

SECTORES MÁS AFECTADOS POR ESTE TIPO DE INCIDENTES

Sectores que dispongan de información de medios de pago, información confidencial valiosa, etc.

LECCIONES APRENDIDAS		
MEDIDAS PREVENTIVAS	Establecimiento de un Modelo de Gobierno Corporativo de Ciberriesgos Clasificar la información para que las medidas de protección que se apliquen sean proporcionales a la confidencialidad de la información. Aplicación del principio de mínimos privilegios: adecuar los accesos a la información a los usuarios que realmente la necesiten. Cortafuegos, sistemas de detección de intrusos, etc. Encriptación de datos. Formación en seguridad de información y mejorar los controles de política interna y de seguridad de la información. Campañas de concienciación en seguridad de información.	
MEDIDAS CORRECTIVAS	**GESTIÓN**	Análisis forense para determinar el alcance y causa del incidente. Campaña de relaciones públicas (cuando se pueda producir pérdida de reputación). Posible cierre del sistema hasta que se determine y elimine la causa.
	TRANSFERENCIA (Cobertura de seguros)	Gastos de mitigación y análisis forense. Violación de datos personales y violación de información. Multas y sanciones. Ciber extorsión. Gastos de reputación. Responsabilidad Civil . CRIME / Infidelidad de empleados (cuando la información se filtra de forma deliberada). Consejeros y Directivos.

2. RANSOMWARE

2. RANSOMWARE

DESCRIPCIÓN

El ransomware es un tipo de "malware" (malicious software) o programa malicioso, cuyo principal objetivo es infiltrarse en los sistemas informáticos de las empresas para dañarlos, bloquearlos o cifrarlos. Se caracteriza porque inutiliza y bloquea determinados archivos del sistema pidiendo un rescate (normalmente en moneda virtual) para recuperar la información. Su nombre le viene de esta peculiaridad, "ransom", rescate en inglés y "software", de programa.

Normalmente este tipo de programas se camuflan dentro de otros programas o aplicaciones de uso habitual (por ejemplo archivos adjuntos en correos electrónicos, links de anuncios, videos, actualizaciones de programas fiables etc.) que invitan a la víctima hacer clic para combinar con otras técnicas de ataques que consiguen instalarse en los quipos informáticos pasando desapercibidos para el usuario.

Existen muchos tipos de ransomware, entre los que destacan el que provoca el secuestro del ordenador (imposibilidad de usarlo), y el cifrado de sus archivos (criptoware), sea cual sea el soporte en que esté (equipos individuales, en red, en nube, etc.)

Cabe reseñar la proliferación de ransomware diseñado específicamente para atacar dispositivos conectados a internet, siendo denominados RoT (Ransomware of Things).

Durante los últimos años numerosos estudios, consultoras expertas y organismos estatales a nivel mundial coinciden en afirmar que ha sido la gran amenaza que se ha materializado en las empresas, y lo se prevé que siga siéndolo durante el 2018, adoptando formas más sofisticadas y complejas, dificultando su detección y subsanación.

CASO

Ejemplos de este tipo de ciber-riesgo son los famosos Wannacry, cuyos costes se estimaron entorno a los 200 millones euros, NotPetya, especialmente sangrante para algunas compañías como la farmacéutica americana MSD con 310 millones de dólares, la logística FedEx con 300 millones de dólares.

Un ejemplo de ataque y sus consecuencias sería por ejemplo un correo con una factura señuelo que llega al departamento de contabilidad de una gran empresa. El usuario abre la factura e infecta a su equipo y todos los equipos que están conectados en la misma red. El atacante toma todos los activos digitales empresariales como rehenes, cifrando la información.

Pide un pago a la empresa a cambio de la clave de cifrado, además usa técnicas de presión para que la víctima pague amenazando con dejar datos irrecuperables pasado un tiempo, publicar información, eliminar todos los datos, incrementar cantidad a pagar pasado un tiempo, etc.

MÓVIL

Económico.

CAUSA DEL INCIDENTE

Descuido o negligencia de un usuario al aceptar un correo, actualizar una aplicación o cualquier otra tarea cotidiana.

MÉTODOS DE ATAQUE

Ransomware.
Ingeniería social, suplantación de identidad, uso de Botnets.

TIPO DE RIESGO AFECTADO

Daños Patrimoniales, Responsabilidad Civil (reclamaciones de terceros por la falta de servicio), Daño Reputacional (en caso de falta de servicio), Responsabilidad de Administradores y Directivos, etc.

IMPACTO ECONÓMICO DEL INCIDENTE

El impacto total de este tipo de ataque resulta difícil de calcular, no sólo por los costes directos e inmediatos (sin contar el pago del rescate, hecho que no garantizaría la recuperación de la información) como remediación de sistemas y restablecimientos de los servicios afectados, sino por el conjunto de daños provocados, como el reputacional, ventas no realizadas, pérdida de confianza de los clientes e inversores, sanciones, penalizaciones de contratos, etc., incluso pérdidas de vidas.

Debido a las características del ataque, puede asegurarse que este tipo de ciber-riesgo es de los más costosos para las empresas, incluyendo el supuesto pago por rescate, cuyo promedio ha ido aumentado, siendo el último corroborado por el Internet Crime Complaint Center (IC3) del FBI, en 679 dólares en 2016. Téngase en cuenta que este es el coste por equipo; multiplíquese esta cantidad por el número de equipos afectados dentro de una organización.

SECTORES MÁS AFECTADOS POR ESTE TIPO DE INCIDENTES

Los ataques por este tipo de ciber riesgo han crecido exponencialmente a todo tipo de usuarios, destacando en los últimos años los sectores de energía (persiguiendo la interrupción del suministro), gubernamentales, sanitario, telecomunicaciones, domésticos, negocios, gobiernos e incluso servicios críticos como hospitales o centrales energéticas.

LECCIONES APRENDIDAS

MEDIDAS PREVENTIVAS		Establecimiento de un Modelo de Gobierno Corporativo de Ciberriesgos. Copias de seguridad y procedimientos que permitan restaurar los datos y archivos en un periodo de tiempo específico. Políticas de contratación con fabricantes de HW y SW más estrictas (Security by default). Instalación de software anti-ransomware. Aplicación del principio de mínimos privilegios: adecuar los accesos a la información susceptible de ser cifrada a los usuarios realmente necesarios. Formación en seguridad de información y mejorar los controles de política interna y de seguridad de la información. Campañas de concienciación en seguridad de información.
MEDIDAS CORRECTIVAS	**GESTIÓN**	Análisis forense para determinar la veracidad del incidente y su tamaño. Recuperar las bases de datos de las copias de seguridad en el tiempo adecuado. Comunicación del hecho delictivo a los Cuerpos y Fuerzas de Seguridad. Campaña de relaciones públicas (cuando se produzca pérdida de reputación).
	TRANSFERENCIA (Coberturas de seguros)	Gastos de mitigación y análisis forense. Pérdida de beneficios. Ciber extorsión. Gastos de reputación. Gastos legales. Multas y sanciones. Responsabilidad Civil (aunque en general es difícil encontrar pólizas que cubran las reclamaciones por este tipo de incidente). Consejeros y Directivos.

3. PHISHING

3. PHISHING

DESCRIPCIÓN

El término phishing se refiere a las técnicas utilizadas por cibercriminales para suplantar la identidad de un sitio web con objeto de sacar algún tipo de beneficio engañando a las víctimas.

El modus operandi más sencillo del phishing se divide en tres fases:

1) **Relación de una imagen de la página web**. Consiste en crear un sitio web falso similar al que se quiere imitar. Hoy en día existen herramientas automatizadas que directamente simulan la navegación que haría un usuario para descargar el contenido completo de la página web. A partir de los datos descargados, estas herramientas crean un código web y las imágenes necesarias, para poder publicar dicha página.

2) **Colocación de la página web**. Para que una página web pueda ser accedida debe estar publicada en un servidor web.

Existen dos principales métodos que utilizan los delincuentes bien hackear un servidor web legítimo de alguna empresa y añadirle la página web falsa, de forma silenciosa dentro de los contenidos de la página web. Esta primera opción no tiene coste directo, pero la disponibilidad de la página web falsa tendrá un tiempo de publicación limitada que va desde que se coloque la página web hasta que la empresa propietaria de la página web se percate de este uso indebido.

La segunda opción pasa por la compra de un dominio similar al que se quiere copiar (por ejemplo supongamos el nombre de una empresa Karla que tiene una página web www.karla.com, posibles dominios de suplantación serían www.kaarla.com, www.karlaa.com, www.karlaweb.com, etc.) y la compra de los servicios de publicación en la nube, para colocar la página web falsa. Los delincuentes suelen aprovecharse de la escasa colaboración internacional existente seleccionando países con una escasa legislación al respecto. El inconveniente de esta técnica es que conlleva unos pequeños costes asociados al registro del dominio y la contratación de la página web.

3) **Distribución de la dirección web falsa.** Esta es la última fase de este tipo de ataques y consisten en hacer llegar la página web falsa al mayor número de usuarios posible, de forma que se incremente al máximo las probabilidades de éxito. A tal fin los delincuentes suelen comprar bases de datos con direcciones de emails que suelen ir clasificadas por nacionalidades del usuario de cara a acotar el tipo de engaño lo máximo posible.

CASO

A mediados de 2010 el propietario de una pequeña empresa de Estados Unidos recibió una llamada de alerta del director de la sucursal del pequeño banco con el que trabajan. El director le comentaba que en la cuenta bancaria no había dinero suficiente para hacer frente al pago de las nóminas. El propietario de la pequeña empresa se sorprendió, aunque no había sido de lejos el mejor año las ventas se estaban comportando bien y la situación financiera de la empresa era buena. Lo más probables es que se tratara de un error del banco por lo que acordó con el director de la sucursal acercarse para analizar la situación y buscar soluciones.

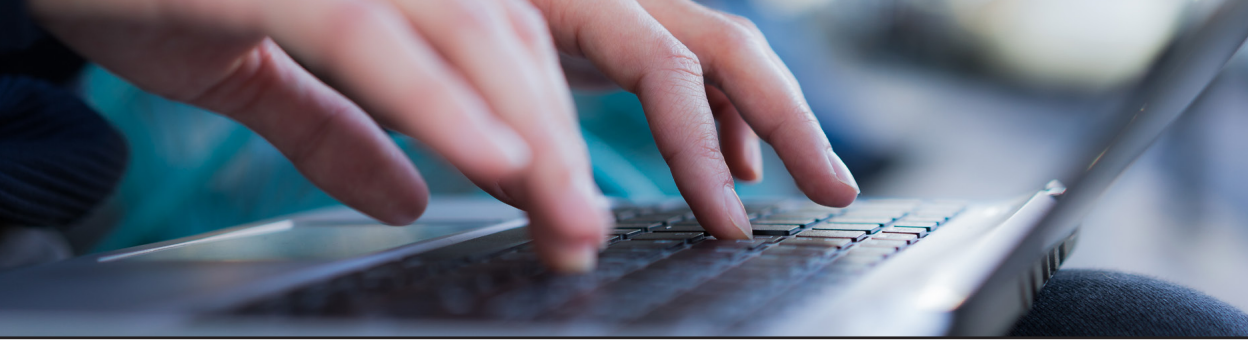
Una vez en la sucursal el director le mostraba al propietario de la empresa el listado de movimientos de la cuenta sobre la que se realizaban los pagos de las nóminas. Durante toda la semana se habían registrado pequeñas transferencias de dinero a distintas cuentas que habían disminuido los casi 20.000$ que se disponían a poco más de 3.000$. El director del banco le aseguraba que habían chequeado las transferencias y que todas se habían realizado con el usuario del que disponen.

Una vez en la empresa el propietario habló con las pocas personas que tenían acceso a los usuarios que manejan las cuentas bancarias, todos confirmaron que no habían realizado dichas transferencias. En ese momento el propietario de la empresa decidió poner en conocimiento de las autoridades los hechos para denunciarlo. Desde la Policía le recomendaron adquirir los servicios de una empresa especializada de seguridad.

La empresa especialidad de seguridad inició una investigación enfocando el caso hacia los ordenadores de aquellas personas que manejan las cuentas. Tras la investigación se identificó que uno de los trabajadores de la compañía había recibido un mensaje como el siguiente:

Cuando los especialistas hablaron con el trabajador les comentó que había abierto el correo, siguiendo los pasos que le habían indicado (cambio de contraseña), pero que esta no se llegó a realizar porque la página le mostró un error. Los especialistas de seguridad no consiguieron acceder a la página web del mensaje porque ésta ya no estaba disponible.

El propietario de la empresa tuvo que hacer frente en primera instancia a la pérdida económica de las transacciones realizadas, aunque con la colaboración del banco se pudieron retroceder algunas de las últimas transacciones realizadas.



Asimismo el propietario de la empresa acordó con el banco reforzar el acceso a las cuentas de la empresa mediante el uso del modo de acceso seguro que implica el utilizar un código de verificación en el acceso.

MÓVIL DEL INCIDENTE

Económico.
Robo de Información confidencial.
Daño Reputacional.

CAUSA DEL INCIDENTE

Engaño a un empleado mediante el empleo de técnicas de ingeniería social por los delincuentes con la finalidad de acceder a los datos confidenciales de la víctima (claves y contraseñas) para realizar pagos y transferencias de dinero a través de Internet

MÉTODOS DE ATAQUE

Phishing y sus diversas tipologías y evoluciones: Pharming, Wi-Phishing, Spear Phishing, Smishing y Vishing.
Ingeniería Social.
Suplantación de identidad.

TIPO DE RIESGO AFECTADO

Daño patrimonial
Información.
Daño reputacional.

IMPACTO ECONÓMICO DEL INCIDENTE

De cientos de euros a millones de euros.

SECTORES MÁS AFECTADOS POR ESTE TIPO DE INCIDENTES

Existe una tendencia a la baja en la aplicación de este método para grandes empresas, pero se mantiene para particulares y Pymes.

LECCIONES APRENDIDAS		
MEDIDAS PREVENTIVAS	Establecimiento de un Modelo de Gobierno Corporativo de Ciberriesgos. Sistemas de seguridad de filtrado de web y de email. Procedimientos: nunca responder a ninguna solicitud de información personal a través de correo electrónico, llamada telefónica o mensaje corto (SMS). Autentificación por doble o triple factor. Formación en seguridad de información y mejorar los controles de política interna y de seguridad de la información. Campañas de concienciación en seguridad de información.	
MEDIDAS CORRECTIVAS	**GESTIÓN**	Tratar con la entidad bancaria informándola de lo sucedido. Análisis forense para determinar el alcance y causa del incidente. Denunciar ante las autoridades. Restablecer contraseñas.
	TRANSFERENCIA (Coberturas de seguros)	Gastos de mitigación y análisis forense. Robo de identidad (si bien no repone el dinero robado). Gastos Reputacionales. Gastos legales. Crime. Consejeros y Directivos.

4. SUPLANTACIÓN DE IDENTIDAD

4. SUPLANTACIÓN DE IDENTIDAD

DESCRIPCIÓN

Pese a las múltiples variantes que presenta, con carácter general podemos decir que la suplantación de identidad es un tipo de ataque mediante el cual una persona consigue hacerse pasar por otra, típicamente engañando al elemento (persona o sistema) encargado de verificar la identidad de la misma en el proceso de registro o acceso.

Lo anterior se logra, generalmente, demostrando que se conoce información o se poseen determinadas características de la persona suplantada, que pueden ir desde datos personales (fecha de nacimiento, DNI, nombre de los hijos, etc.) hasta, en el caso extremo, sus credenciales de acceso.

También puede utilizarse ingeniería social (o ausencias de control) para lograr engañar al elemento encargado del registro o acceso y conseguir la suplantación sin necesidad de conocer la información que normalmente se requiere.

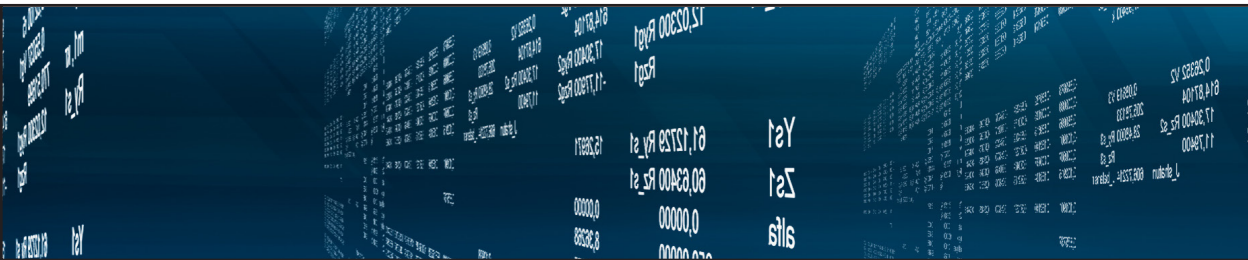
CASOS

Imaginemos que en la compañía ACME se despide a un trabajador, con buenos conocimientos tecnológicos, por conductas no acordes con el código ético y que éste trabajador busca venganza. Para llevarla a cabo, se le ocurre suplantar la identidad del CEO de ACME en una red social de amplia difusión y comenzar a difundir información falsa de la compañía.

Inicialmente, utiliza herramientas automáticas que permiten obtener la lista de todos los contactos que tiene el CEO en su cuenta, y descarga su foto de perfil y la información que aparece publicada. Después crea un perfil falso, idéntico al perfil original y posteriormente, utilizando también librerías automáticas, va agregando uno a uno a todos los contactos del CEO de ACME, personalizando la solicitud de tal modo que diga “Por favor, ten en cuenta que a partir de este momento esta es mi nueva cuenta en la red social”.

Una vez que va recibiendo las aceptaciones de los contactos, comienza a difundir información aparentemente normal y, en un momento dado, publica que deja ACME porque éticamente no puede soportar por más tiempo las directrices del dueño encaminadas a publicar noticias falsas de una determinada tendencia.

Otro ejemplo de suplantación de identidad sería el que podría sufrir una persona normal que, pese a ser un usuario habitual de Internet y realizar habitualmente transacciones de comercio electrónico (con un poder adquisitivo medio), tiene poca conciencia de seguridad.



Esta persona está registrada en un foro web de aficionados al motor. Esta web, muy popular y con un elevado número de usuarios, llama la atención de un grupo de hackers, que comienzan a analizar las vulnerabilidades del sitio, encontrando una que les permite acceder a los servidores. Una vez dentro, son capaces de acceder a las bases de datos y obtienen las cuentas de los usuarios registrados, que incluyen la dirección de correo y sus contraseñas de acceso al foro, y cuelgan esta información en un sitio específico utilizado habitualmente por hackers de diversa índole.

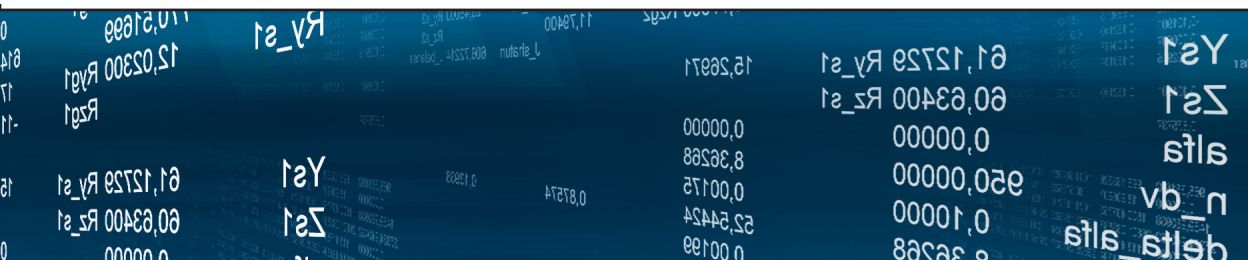
Como el usuario reutilizaba en el foro la misma contraseña que en su cuenta de correo electrónico personal, las herramientas automáticas utilizadas habitualmente por otros hackers detectan las cuentas comprometidas y prueban a acceder a la cuenta de correo electrónico de la víctima, lo que consiguen dado que el usuario utilizaba, por comodidad, la misma contraseña. Posteriormente, los hackers, dentro de la cuenta de correo de la víctima, listan los e-mails existentes con el objetivo de identificar servicios habituales de compra a través de Internet. Tras esto, resetean la contraseña de acceso a estos sitios (generalmente el proceso consiste en enviar un enlace al correo del usuario para poder llevar a cabo la operación de reseteo), acceden a estas webs de compras y, reseteando las contraseñas, se dedican a comprar con las tarjetas de crédito allí almacenadas, enviando la mercancía a puntos de recogida públicos con destinatarios ficticios.

MÓVIL

Una vez realizada la suplantación, y dependiendo de la entidad o medio en el que se haya logrado llevar a cabo la misma, el atacante puede comenzar a actuar en nombre de la persona suplantada, buscando en la mayoría de las ocasiones obtener algún tipo de beneficio económico o comprometer la reputación de la víctima o de terceros relacionados con él.

En este sentido, algunas de acciones habituales suelen ser solicitar un crédito o préstamo hipotecario, extorsionar a la víctima, solicitar transferencias, contratar servicios en nombre de un tercero beneficiándose de los mismos, difundir información u opiniones falsas buscando un determinado efecto o enmascarar acciones delictivas.

Dentro de las acciones de suplantación que buscan conseguir un beneficio económico o dañar la reputación de la víctima, se podría destacar el caso en el que empresas competidoras utilicen estos medios para suplantando la identidad de algún directivo o empleado con acceso a información confidencial y sensible ya sea de carácter económico o de otro tipo, y utilizarla en su provecho.



CAUSA DEL INCIDENTE

Para lograr la suplantación de identidad, se puede contar con la obtención de las claves y los datos personales a través del Phishing o la suplantación web y otras formas de ciber ataque que conlleven la revelación o el robo de datos personales, para su posterior explotación.

También se podría producir cuando se rompe la cadena de confidencialidad, identificación y verificación de la identidad personal.

Por otro lado, en muchas organizaciones esto se puede producir ante una mala educación organizativa en lo referente a la seguridad cibernética.

MÉTODOS DE ATAQUE

Los modos más habituales mediante los que los atacantes consiguen obtener los datos de las víctimas suelen ser los de explotar la información publicada en redes sociales (LinkedIN, Twitter, Facebook, etc.) , realizar "hackeos" directamente a la víctima, bien comprar en el mercado negro registros robados a compañías hackeadas o llevar a cabo ataques de ingeniería social en los que el atacante se hace pasar (por ejemplo) por un empleado de fuerzas del orden o de una compañía de suministros básicos para solicitar información privada a la víctima.

Con estos "hackeos" se consigue acceder a claves y accesos personales y confidenciales remitidos o almacenados por el propio usuario en sus bases de datos y/o correo electrónico, y a través de esas claves de usuario cometer la suplantación de identidad.

También se pueden conseguir a través del Phishing y de la suplantación del correo/web.

TIPO DE RIESGO AFECTADO

Daño reputacional, daño patrimonial, responsabilidad civil (en el caso de revelación de información crítica).

IMPACTO ECONÓMICO DEL INCIDENTE

Muy variado, el impacto directo e indirecto puede llegar a alcanzar elevadas cantidades.

SECTOR MÁS AFECTADO POR ESTE TIPO DE INCIDENTES

Cada vez son más usuarios los afectados por este tipo de ciber ataque.

De hecho según el Eurostat, España es uno de los países de la Unión Europea donde más suplantaciones/robos de identidad se tenían registrados, con un 7% de los cibernautas en los últimos 12 meses analizados.

Los sectores más afectados varían desde instituciones bancarias, hasta instituciones estatales, pasando por el sector sanitario.

Además con la influencia de las Redes Sociales, cada vez está más extendido este tipo de amenaza.

LECCIONES APRENDIDAS

MEDIDAS PREVENTIVAS		Establecimiento de un Modelo de Gobierno Corporativo de Ciberriesgos. Herramientas de tecnología de la información que reduzcan los posibles efectos de este tipo de ataques. Campañas de concienciación en seguridad de información (no establecer la misma contraseña para todo, crear contraseñas seguras, cambiarlas regularmente, no enviar información personal susceptible vía correo electrónico u otro tipo de vías sensibles, navegación solo por lugares oficiales, realización de transacciones seguras…).
MEDIDAS CORRECTIVAS	**GESTIÓN**	Análisis forense para determinar el alcance y causa del incidente. Denunciar ante las autoridades. Comunicación a las partes afectadas (bancos, instituciones estatales, etc.). Campaña de relaciones públicas (cuando se produzca pérdida de reputación).
	TRANSFERENCIA (Coberturas de seguros)	Gastos de mitigación y análisis forense. Suplantación de identidad. Crime. Pérdida de Beneficios. Gastos reputacionales. Ciber extorsión. Responsabilidad Civil. Consejeros y Directivos.

5. APT (Amenaza Persistente Avanzada)

5. APT (Amenaza Persistente Avanzada)

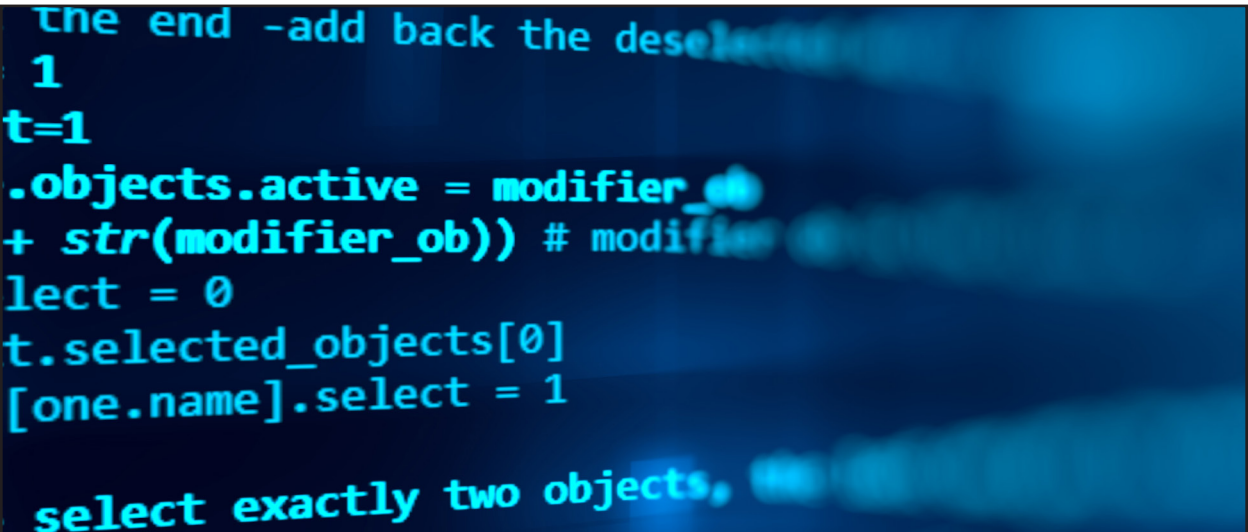
DESCRIPCIÓN

APT es abreviatura de las siglas del término inglés “Advanced Persistent Threat” traducido al español como “Amenaza Avanzada Persistente”.

Se trata de un ataque dirigido contra una organización concreta (la víctima) por parte de un adversario (el atacante) altamente capacitado en conocimientos técnicos y recursos financieros y humanos, que mediante la combinación de diferentes métodos de ataque (por ejemplo, cibernético, físico e ingeniería social), consigue infiltrarse y expandirse en la infraestructura tecnológica de la víctima con el propósito de sustraer información sensible o perjudicar los procesos críticos de la organización de forma continuada en el tiempo.

Lo que hace diferentes a las APT de otros ciber riesgos es que los atacantes estudian minuciosamente la organización para personalizar el ataque. El tiempo y los recursos empleados no son un obstáculo si la recompensa merece la pena; los atacantes perseguirán su objetivo con determinación hasta conseguirlo. Utilizan técnicas altamente sofisticadas y complejas, e incluso vulnerabilidades desconocidas (llamadas “día 0”). Los criterios de seguridad habituales no rigen ante una amenaza de tal envergadura, y los sistemas de protección de la organización (Cortafuegos, IDS/IPS, antivirus...) resultan insuficientes para detectar y bloquear una APT, de forma que para cuando ésta se percata de la situación, el daño puede haber sido catastrófico. Un despliegue de medios de tal magnitud sólo está al alcance de estados o de grupos organizados altamente capacitados, en ocasiones auspiciados en la sombra por gobiernos de algunos países.

Algunos grupos de APT conocidos por ser especialmente activos son “FancyBear” y “CozyBear”, supuestamente vinculados al gobierno ruso, “OceanLotus” posiblemente de origen vietnamita, “Codoso Team”, supuestamente vinculado al gobierno chino y “Lazarus Group”, supuestamente vinculado al gobierno de Corea del Norte.



CASOS

Los primeros casos de los que se tiene conocimiento se remontan a los años 90. Durante ésta década, el Pentágono, la NASA, el Departamento de Energía de los EEUU y varios laboratorios y universidades fueron víctima de diferentes campañas de APT.

Desde entonces y hasta la fecha, han sido muchos los casos que han visto la luz espoleados por un impacto nunca antes conocido. Casos como "Buckshot Yankee" (2008) que afectó al Departamento de Defensa de los EEUU, "Operación Aurora" (2009) con Google como víctima, "Stuxnet" (2010) que afectó a varias centrales nucleares iraníes, poniendo de manifiesto que una APT era capaz de traspasar de lo cibernético a lo físico, son buenos ejemplos de ello.

Recientemente "Carbabank" (2015), una campaña de APT dirigida a una centena de instituciones financieras en 30 países que supuso unas pérdidas estimadas a nivel global de unos mil millones de dólares. El ataque había durado cerca de dos años antes de ser detectado por las compañías. Y por último, los supuestos compromisos por parte de dos grupos de APT rusos del "Comité Democrático Nacional" (DNC) estadounidense, en 2016, y su potencial influencia en los resultados de la campaña electoral. Todos estos casos y otros que se han conocido, dan buena cuenta del porqué las APT están entre las principales preocupaciones de la organizaciones.

MÓVIL

Cada vez son más usuarios los afectados por este tipo de ciber ataque.

De hecho según el Eurostat, España es uno de los países de la Unión Europea donde más suplantaciones/robos de identidad se tenían registrados, con un 7% de los cibernautas en los últimos 12 meses analizados.

Los sectores más afectados varían desde instituciones bancarias, hasta instituciones estatales, pasando por el sector sanitario.

Además con la influencia de las Redes Sociales, cada vez está más extendido este tipo de amenaza.

CAUSA DEL INCIDENTE

Engaño a un empleado.
Vulnerabilidades de los sistemas de información.

MÉTODOS DE ATAQUE

El ordenador de cualquier empleado, una vez ha sido comprometido y tomado el control por parte del atacante, puede servir como punto de entrada a la red de la organización para, a través de éste, moverse internamente hasta llegar a los recursos informáticos de mayor interés.

El ordenador de cualquier empleado, una vez ha sido comprometido y tomado el control por parte del atacante, puede servir como punto de entrada a la red de la organización para, a través de éste, moverse internamente hasta llegar a los recursos informáticos de mayor interés.

TIPO DE RIESGO AFECTADO

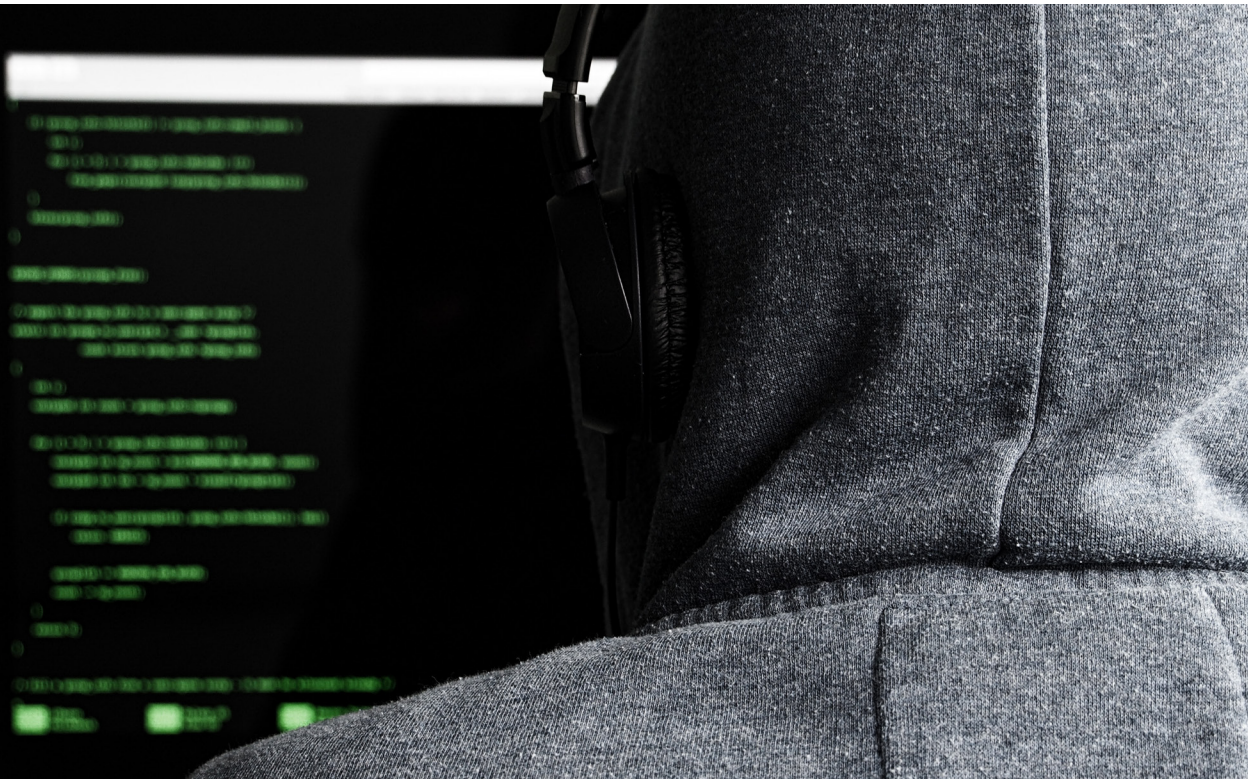
Estratégicos para el país.

IMPACTO ECONÓMICO DEL INCIDENTE

No es mucha la información disponible sobre el impacto de ataques utilizando APTs. De hecho, es probable que muchas organizaciones que hayan sido, o estén siendo víctimas, no sean conscientes de tal situación. Por otra parte, el impacto en la imagen hace que las organizaciones afectadas sean reticentes a hacer pública la información.
Sin embargo, queda claro que hablar de APTs es sinónimo de ciberespionaje o ciberguerra; su impacto puede alcanzar dimensiones económicas incalculables para una organización o incluso afectar al funcionamiento de un país en el caso de ataques contra sectores estratégicos.

SECTORES MÁS AFECTADOS POR ESTE TIPO DE INCIDENTES

Servicios estratégicos.



LECCIONES APRENDIDAS		
MEDIDAS PREVENTIVAS	Establecimiento de un Modelo de Gobierno Corporativo de Ciberriesgos. Planes de continuidad de negocio. Formación en seguridad de información. Campañas de concienciación en seguridad de información.	
MEDIDAS CORRECTIVAS	**GESTIÓN**	Análisis forense para determinar el alcance y causa del incidente. Comunicación a las autoridades. Campaña de relaciones públicas (cuando se produzca pérdida de reputación). Activación de planes de continuidad de negocio y de respuesta al incidente.
	TRANSFERENCIA	Gastos de mitigación y análisis forense. Pérdida de beneficios. Ciber extorsión. Gastos de reputación. Responsabilidad Civil. Cobertura de daños (si el ataque provoca daños materiales. Nota: la mayoría de las pólizas excluyen daños materiales de origen ciber). Consejeros y Directivos. Aunque es posible contar con coberturas que permitan la transferencia económica del riesgo, la envergadura del siniestro puede hacer que los capitales asegurados estén muy por debajo del valor económico del daño causado.

6. FRAUDE DEL CEO

6. FRAUDE DEL CEO

DESCRIPCIÓN

También conocido en inglés como “Whaling Attack” (“Caza de ballenas” o “Caza del pez gordo”) o “BEC Attack” (Business Email Compromise), es una de las formas de ciberdelincuencia más recientes y con un mayor crecimiento.

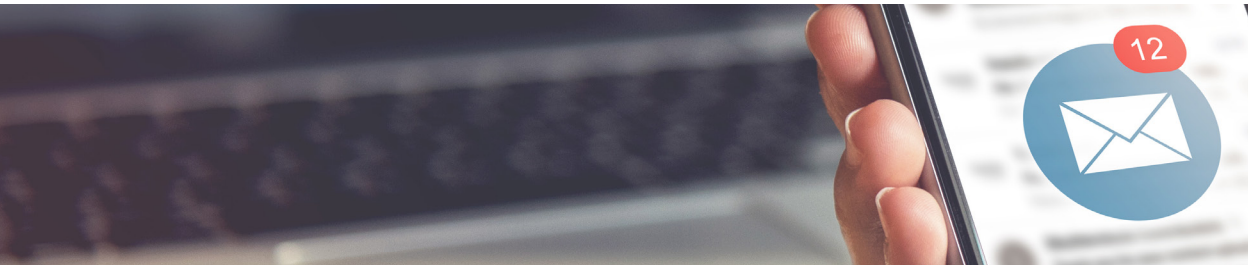
Se trata de un tipo de fraude en el que los cibercriminales aprovechan la facilidad de suplantación de identidad inherente a los medios de comunicación electrónicos (en particular el correo electrónico) que combinan con técnicas de engaño (ingeniería social) para incitar a un empleado, previamente elegido como víctima, a realizar algún tipo de transacción sensible (financiera o de información), hacia un destino controlado por los atacantes, pasando a su poder. Los controles y procedimientos internos de las compañías, en ocasiones demasiado laxos, no logran detectar el fraude hasta que se ha llevado a efecto.

En el caso más simple, los estafadores envían un correo electrónico a un empleado incauto elegido como víctima, perteneciente al área Financiera o Contable de la compañía. El correo, que viene de una dirección supuestamente legítima de alguna persona de la alta dirección, como el Director General (o CEO, de ahí el nombre del fraude), apremia al empleado para que envíe dinero o realice el pago de una factura a una determinada cuenta bancaria. Esta cuenta, bajo el control de los ciberdelincuentes, estará ubicada en algún país donde resulte prácticamente imposible seguir su rastro de forma que si la operación se lleva finalmente a efecto, no se podrá recuperar el dinero.

Bajo este mismo esquema han aparecido otras variantes; en unos casos, los ciberdelincuentes solicitan al empleado el envío de información sensible de la compañía (que será luego empleada con otros fines maliciosos), o también se hacen pasar por un proveedor de la compañía que solicita un cambio en la cuenta bancaria en la que se abonan los servicios o suministros prestados por otra nueva (que por supuesto estará bajo su control).

Si bien el vector de ataque principal es el correo electrónico, también se utiliza el teléfono, mensajes de texto, servicios de mensajería electrónica como Telegran o Whatsapp, e incluso una combinación de varios de esto medios (por ejemplo, iniciar el contacto con la víctima con una primera llamada telefónica, para continuar posteriormente con el correo electrónico).

Es un tipo de un fraude muy dirigido y bien preparado para el que los ciberdelincuentes se toman tiempo estudiando a la víctima (a partir de informaciones disponibles en internet, publicaciones en redes sociales, investigación de los empleados, etc.) hasta tener la información suficiente para hacer que el ataque sea lo más realista y exitoso posible.



CASOS

También conocido en inglés como “Whaling Attack” (“Caza de ballenas” o “Caza del pez gorEl pasado 12 de agosto de 2016, Leoni, el mayor fabricante de cables eléctricos de Europa con más de 81.000 empleados repartidos por 31 países, anunció públicamente que había sido víctima del “fraude del CEO” por un importe cercano a los 40 millones €. La Directora Financiera (CFO) de una fábrica de la compañía ubicada en Bistrita (Rumanía) recibió un correo electrónico que parecía provenir de uno de los altos ejecutivos de la compañía en Alemania.

La Dirección General para la Investigación de la Delincuencia Organizada y el Terrorismo de Rumanía (DIICOT) informó que los estafadores tenían un amplio conocimiento sobre los procedimientos internos para aprobar y procesar transferencias ya que, de las cuatro que Leoni tiene en Rumanía, esta fábrica es la única autorizada para transferir dinero.

En enero de 2016 el fabricante francés de maquinaria industrial Etna Industrie, con unos 50 empleados, fue víctima del fraude del CEO por importe de unos 100.000 €. Una empleada de la compañía recibió una llamada telefónica indicándole que en breve recibiría un correo de la Directora General de la Compañía, Carole Gratzmuller, dándole instrucciones; se trataba de una operación confidencial de adquisición de una compañía en Chipre; tenía que seguir las indicaciones que le darían desde un despacho de abogados. En breve recibió varios correos y llamadas telefónicas desde el supuesto despacho. Finalmente se llegaron a realizar transacciones de unos 500.000 € si bien gracias a la intervención de los bancos, “sólo” 100.000€ llegaron a su destino final.

MÓVIL DEL INCIDENTE

Económico.

CAUSA DEL INCIDENTE

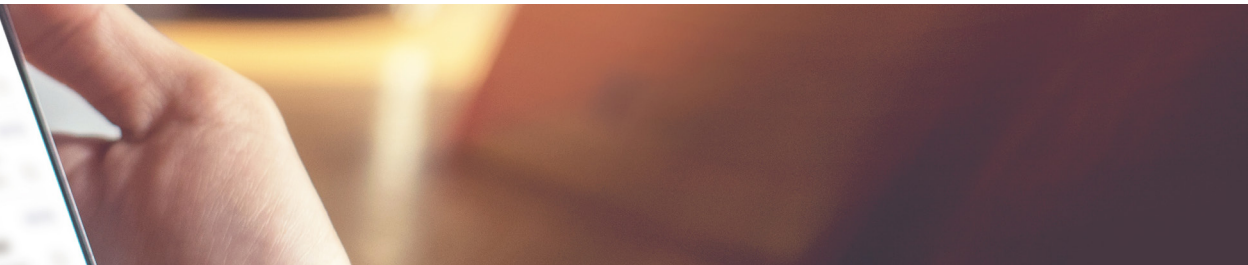
Engaño a un empleado.
Controles inadecuados dentro de la organización.

MÉTODOS DE ATAQUE

Ingeniería social.

TIPO DE RIESGO AFECTADO

Daño patrimonial.



SECTORES MÁS AFECTADOS POR ESTE TIPO DE INCIDENTES

Según publicó en febrero de 2017 el Centro de Denuncias de Delitos en Internet (IC3) del FBI, "el fraude del CEO continúa creciendo, evolucionando y apuntando a negocios de todos los tamaños. Desde enero de 2015, ha habido un aumento del 1.300 % en las pérdidas identificadas, que ahora suman más de 3 mil millones de dólares".

El dinero sólo se ha podido recuperar en un 4% de casos. El fraude afecta desde pequeñas empresas hasta grandes corporaciones y en cualquier ámbito de actividad (compañías privadas, administraciones públicas, universidades, hospitales, escuelas...).
En la mayoría de los casos, el dinero se ha traspaso a cuentas en China y Hong Kong.

En los últimos tres años se han reportado fraudes en más de 100 países. Es una de las formas de delincuencia de mayor crecimiento.

LECCIONES APRENDIDAS

MEDIDAS PREVENTIVAS	Establecimiento de un Modelo de Gobierno Corporativo de Ciberriesgos. Procedimientos internos de autorización de operaciones. Formación en seguridad de información y mejorar los controles de política interna y de seguridad de la información. Campañas de concienciación en seguridad de información.	
MEDIDAS CORRECTIVAS	**GESTIÓN**	Tratar con la entidad bancaria. Denunciar ante las autoridades.
	TRANSFERENCIA (coberturas de seguros)	Crime.

7. ATAQUE DDOS

7. ATAQUE DDOS

DESCRIPCIÓN

El término Distributted Denial of Service (DDOS) se asocia para aquellos incidentes de seguridad en los que se impide la prestación de un servicio (de los sistemas de información) a una organización. La manera de llevarlo a cabo puede ser muy diversa, aunque lo más habitual suele ser mediante la generación de un consumo de dicho servicio de manera artificial y maliciosa, impidiendo que otros usuarios o empresas puedan hacer uso de este servicio. Una analogía en el mundo físico podría darse en aquellas situaciones de huelga y protesta en estaciones de tren y aeropuertos, en los que usuarios que no van a hacer uso de los medios de transporte abarrotan de manera no forzosa las infraestructuras impidiendo el normal desarrollo y uso de las mismas.

En la actualidad los ataques de DDOS están muy extendidos en el ámbito cibernético, y aunque se han utilizado con motivos hacktivistas y terroristas, la causa más extendida de motivación de este tipo de ataques es el de la extorsión.

El modus operandi suele consistir en una saturación inicial de los servicios de forma momentánea y puntual, para posteriormente solicitar una cantidad económica al a cambio de no saturar el canal online.

Para llevar a cabo esta saturación, previamente el criminal suele hacerse con el control de una red de equipos informáticos infectados que son controlados de manera centralizada (botnet) por el cibercriminal sin que los usuarios de estos equipos se percaten. Existen organizaciones que alquilan estas redes con estos fines.

CASOS

Corría el año 2015, parecía una tarde de domingo cualquiera en una compañía de juego online. El área de operaciones monitorizaba los sistemas y redes de la compañía sin que se advirtiera ninguna anomalía ni situación adversa que pudiera conllevar un problema. En un momento dado el número de operaciones de acceso a la página principal empezó a incrementarse de forma drástica. Casi sin tiempo para poder analizar las causas de ese incremento drástico los canales de comunicación de la principal página web quedaron saturados por completo.

El estado de los servidores web principales no era mucho mejor, los sistemas no estaban preparados para una demanda de acceso de tanto volumen. Adicionalmente algunos de los sistemas internos (bases de datos, servidores de aplicación, etc.) también presentaban un alto grado de saturación.

El operador de la sala de control, siguiendo los procedimientos previamente establecidos, realiza una llamada al responsable de operación para comentarle la situación. Sin que tuviera mucho tiempo para poder tomar decisión alguna el tráfico empieza a cesar.

No obstante el nivel de saturación a los que habían llegado algunos servidores había dejado a los sistemas en su conjunto completamente inconsistentes. Dada la situación, el responsable de operación tuvo que activar el procedimiento de emergencia que implica llamar a los principales equipos de sistemas para la parada y puesta en marcha de los sistemas, ya habría tiempo para analizar después que había pasado.

La situación en el exterior tampoco era buena, Twitter, Facebook y otras redes sociales se habían hecho eco del problema en la página web. Cientos de usuarios mostraban su descontento con la empresa de apuestas online debido a la indisponibilidad en un día en el que se juegan gran parte de los eventos deportivos que son objeto de apuesta. La dirección de la empresa, tampoco era ajena a la situación y ya era conocedora de los hechos. Ese análisis que el responsable de operación había valorado en posponer tendría que adelantarse, además incorporando a especialistas de seguridad.

Durante las primeras horas del lunes, una persona del departamento de marketing se puso en contacto con los especialistas de seguridad. Había recibido en su correo electrónico un extraño correo que pensó que podía tener relación con el incidente del domingo.

Hello,
To introduce ourselves first:
https://blogs.akamai.com/2014/12/dd4bc-anatomy-of-a-bitcoin-extortion-campaign.html
http://bitcoinbountyhunter.com/bitalo.html
http://cointelegraph.com/news/113499/notorious-hacker-group-involved-in-ex-coin-theft-owner-accusesccedk-of-withholding-info
Or just google "DD4BC" and you will find more info.
Recently, we were DDoS-ing Neteller. You probably know it already.
So, it's your turn!
<site> is going under attack unless you pay 20 Bitcoin.
Pay to 18NeYaX6GCnibNkwyuGhGLuU2tYzbxvW7z
Please note that it will not be easy to mitigate our attack, because our current UDP flood power is
400-500 Gbps, so don't even bother.
Right now we are running small demonstrative attack on your server.
Don't worry, it will stop in 1 hour. It's just to prove that we are serious.
We are aware that you probably don't have 20 BTC at the moment, so we are giving you 48 hours to get it and pay us.

We do not know your exact location, so it's hard to recommend any Bitcoin exchanger, so use Google.
Current price of 1 BTC is about 250 USD.

IMPORTANT: You don't even have to reply. Just pay 20 BTC to 18NeYaX6GCnibNkwyuGhGLuU2tYzbxvW7z – we will know it's you and you will never hear from us again.
We say it because for big companies it's usually the problem as they don't want that there is proof

El correo original fue recibido el 6 de abril, y en éste se solicitaba el pago de 20 bitcoins con objeto de evitar un ataque web. En principio el equipo de marketing hizo caso omiso al correo electrónico al considerar que se trataba de algún tipo de fraude.

El departamento de operaciones, junto con los especialistas en seguridad no tuvo duda alguna de que se trataba de un intento de extorsión por parte de un grupo cibercriminal denominado DD4BC.

El incidente había costa miles de dólares en ingresos a la organización, a lo que había que añadir el imponderable del coste reputacional que había tenido en las redes sociales. La dirección decidió que la empresa tenía que tomar medidas para atajar un problema que consideraban crítico por la naturaleza online del negocio, por lo que dejaron en manos de los especialistas de seguridad y el responsable de operaciones el tomar medias que limitaran el impacto de este tipo de incidentes.

Los especialistas de seguridad analizaron la información que habían recogido de los sistemas y definieron una batería de medidas de seguridad que ayudaran a mejorar la situación de la compañía ante estas situaciones. Entre esta batería de medidas destacaba como medida principal la contratación de servicios específicos anti DDOS que ofertaba la empresa que le gestionaba la conexión a Internet de sus sistemas.

MÓVIL DEL INCIDENTE

Económico.
Existe una variante que tiene por objetivo es demostrar la vulnerabilidad de determinados servicios.
Activismo (muy frecuente como respuesta social a una organización a la que se le quiera castigar).

CAUSA DEL INCIDENTE

Los sistemas de información de las organizaciones no están dimensionados para gestionar un tráfico desproporcionado.

MÉTODOS DE ATAQUE

Ataque DDOS.

TIPO DE RIESGO AFECTADO

Daño patrimonial (pérdida de beneficios).
Daño reputacional.
Responsabilidad civil (reclamaciones por falta de servicio).

IMPACTO ECONÓMICO DEL INCIDENTE

De miles a millones de euros.

Actualmente con el incremento de dispositivos conectados el riesgo ha aumentado, puesto que cualquier dispositivo que esté conectado a Internet puede ser utilizado para cometer ataques DDOS.

SECTORES MÁS AFECTADOS POR ESTE TIPO DE INCIDENTES

El principal objetivo de este tipo de incidentes suelen ser empresas, no necesariamente grandes, generalmente pequeñas, con una alta dependencia del canal online, por ejemplo portales de compra/venta de productos, servicios de apuestas, juego online, etc.

LECCIONES APRENDIDAS

MEDIDAS PREVENTIVAS	Establecimiento de un Modelo de Gobierno Corporativo de Ciberriesgos. Monitorización del tráfico y contratación de servicios específicos anti DDOS.	
MEDIDAS CORRECTIVAS	**GESTIÓN**	Servicios específicos anti DDOS. Campaña de relaciones públicas (cuando se produzca pérdida de reputación).
	TRANSFERENCIA (coberturas de seguros)	Pérdida de beneficios. Cyber extorsión. Gastos de reputación. Responsabilidad Civil.

8. SUPLANTACIÓN / MODIFICACIÓN DE WEB

8. SUPLANTACIÓN / MODIFICACIÓN DE WEB

DESCRIPCIÓN

Este tipo consiste en la alteración de una página web mediante la modificación de forma no autorizada del código de la página. El motivo de un atacante puede variar pero lo más habitual es que persiga uno de estos tres objetivos:

1) Alterar el contenido de un sitio web, de manera perceptible, para el usuario con el objetivo de manifestar algún tipo de protesta o reivindicación.

2) Alterar el contenido de un sitio web, de manera imperceptible del usuario logrando instalar código dañino en el dispositivo de navegación (ordenador, móvil, etc.) que el usuario esté utilizando.

3) Hacerse pasar por el sitio web legítimo, dando la falsa sensación a los usuarios de que acceden y navegan por el mismo, aunque realmente no lo hagan, buscando lograr el obtener información confidencial del usuario.

CASO

Como ejemplo ilustrativo, imaginemos que la página web del periódico local ACME tiene un gestor de contenidos basado en código abierto, con una pieza de código (plugin) que permite que los usuarios puedan votar las noticias que mayor interés les despierten, funcionalidad que interesa mucho a ACME, dado que le permite priorizar sus contenidos en función de los gustos de sus lectores.

Este plugin se muestra vulnerable a un ataque de Inyección SQL (vulnerabilidad), del que existe un parche para solucionarlo, pero nadie lo ha actualizado ya ACME no cuenta con personal específico en materia de seguridad y no ha sido capaz de detectarlo.

Con el paso del tiempo, la vulnerabilidad del sitio es detectada por programas automáticos (arañas) que rastrean Internet en busca de sitios vulnerables basados en tecnologías populares de amplia difusión. La araña en cuestión, está programada para que, una vez detectada la vulnerabilidad, dispare automáticamente un ataque que, utilizando funciones de base de datos, permita lograr el control total del servidor que aloja el sitio web. De este modo, los atacantes toman el control del sitio web de ACME.

Una vez tomado el control, los atacantes tienen total libertad de actuación, pudiendo desde publicar contenidos con noticias falsas, hasta modificar los archivos del sitio web e inyectar programas maliciosos.

El software malicioso que pudieran incluir los atacantes, estaría programado para buscar vulnerabilidades que pueda tener el usuario en su navegador para infectar el equipo desde el que accede el lector que navega por ACME, convirtiéndolo en "zombie" e ingresándolo en las filas de una Botnet, o, también muy habitual hoy en día, cifrando el contenido de su disco duro y pidiendo un rescate a la víctima para recuperarlo.

MÓVIL

Los objetivos de este tipo de ataques son múltiples: utilizar los ordenadores de las víctimas para realizar acciones maliciosas sin su conocimiento, robarles sus credenciales de acceso a los servicios proporcionados por la compañía propietaria del sitio web, dañar la reputación de la compañía o el medio propietario del sitio web, difundir contenidos o noticias falsas, revindicar ideas o mensajes, etc.

CAUSA DEL INCIDENTE

Para lograr modificar o suplantar al sitio legítimo, los atacantes típicamente emplean fallos conocidos en los productos tecnológicos de las páginas web (conocidos como vulnerabilidades), con el fin de lograr el acceso para modificar el contenido web y/o instalar después a su antojo el código malicioso que mejor sirva a sus propósitos.

MÉTODOS DE ATAQUE

Inyección SQL.

TIPO DE RIESGO AFECTADO

Daño reputacional dado que puede haber personas que no se hayan dado cuenta del engaño y reclamen a la empresa auténtica pidiéndole responsabilidades de lo ocurrido, daño patrimonial (pérdida de ventas que se dirigen a otra plataforma), responsabilidad civil (en el caso de modificación de la web, y en caso de que los productos suministrados tenga problemas de calidad, de etiquetado, etc.).

IMPACTO ECONÓMICO DEL INCIDENTE

Daño reputacional dado que puede haber personas que no se hayan dado cuenta del engaño y reclamen a la empresa auténtica pidiéndole responsabilidades de lo ocurrido, daño patrimonial (pérdida de ventas que se dirigen a otra plataforma), responsabilidad civil (en el caso de modificación de la web, y en caso de que los productos suministrados tenga problemas de calidad, de etiquetado, etc.).

SECTORES MÁS AFECTADOS POR ESTE TIPO DE INCIDENTES

Principalmente los sectores con mayor número de clientes web (retail, transporte, medios de comunicación, banca, eléctricas, fundaciones, ONGS) o los de ámbito institucional o gubernamental.

<table>
<tr><th colspan="3">LECCIONES APRENDIDAS</th></tr>
<tr><td>MEDIDAS PREVENTIVAS</td><td colspan="2">Establecimiento de un Modelo de Gobierno Corporativo de Ciberriesgos.
Actualización continua de parches que eliminan vulnerabilidades.
Contratar o crear internamente servicio de rastreo diario en la red de información / noticias que puedan estar relacionadas / afectar a la empresa.

El software malicioso que pudieran incluir los atacantes, estaría programado para buscar vulnerabilidades que pueda tener el usuario en su navegador para infectar el equipo desde el que accede el lector que navega por ACME, convirtiéndolo en “zombie” e ingresándolo en las filas de una Botnet, o, también muy habitual hoy en día, cifrando el contenido de su disco duro y pidiendo un rescate a la víctima para recuperarlo.</td></tr>
<tr><td rowspan="2">MEDIDAS CORRECTIVAS</td><td>GESTIÓN</td><td>Análisis forense para determinar el alcance y causa del incidente.
Campaña de relaciones públicas (cuando se produzca pérdida de reputación).
Denuncias en los foros que correspondan para solicitar la retirada de la página fraudulenta.</td></tr>
<tr><td>TRANSFERENCIA (coberturas de seguros)</td><td>Es difícil encontrar pólizas de seguros que permitan transferir este tipo de riesgos. Podría negociarse de forma puntual para dar respuesta a algún hecho concreto.</td></tr>
</table>

9. IOT (Internet of Things) PRIVACIDAD Y SEGURIDAD

9. IOT (Internet of Things) PRIVACIDAD Y SEGURIDAD

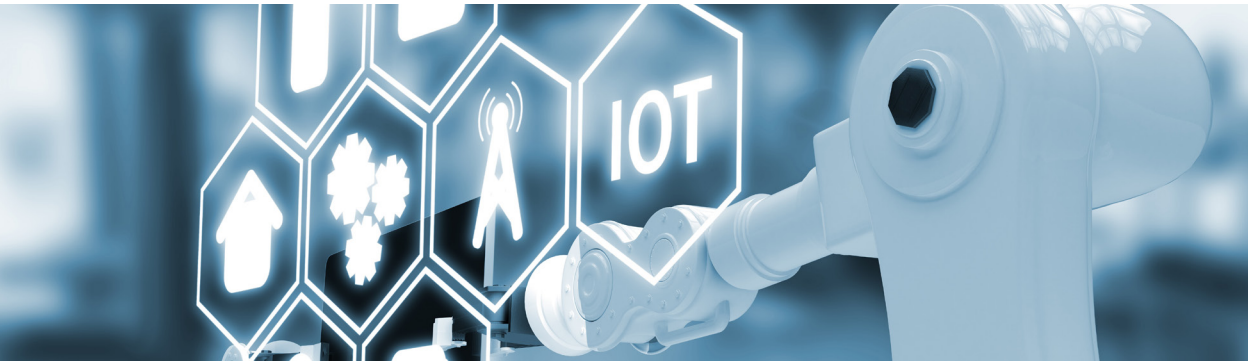
DESCRIPCIÓN

Internet de las cosas (IoT, en sus siglas en inglés) viene a amplificar los actuales riesgos que como individuos, como compañías y como sociedad sufrimos; durante años hemos percibido, que en nuestro entorno más cercano, existían altos niveles de seguridad y privacidad por el hecho de estar desconectados de la Red. Mientras que el acceso a Internet suponía cruzar la línea de riesgo que nos exponía a innumerables peligros, la vida off line, tanto en comunicaciones personales como de máquinas, parecía ser un lugar seguro.

Esta situación, ha cambiado en un mundo hiperconectado dónde cada vez más objetos cotidianos disponen de una dirección IP para interactuar de una forma más efectiva con nuestro contexto (nuestro entono) y donde los sistemas ya no sólo se utilizan, sino que además se portan, se implantan, se tragan o se inyectan, dependiendo en muchos casos la vida del anfitrión de los mismos.

Estos dispositivos los encontramos por ejemplo en:

- Televisiones conectadas que obtienen y procesan nuestra voz para dar órdenes al dispositivo o realizar interacciones con informaciones que están fuera del televisor o que recogen nuestros gustos y horarios.
- Coches conectados que en base a nuestro próximo destino nos informa del mismo o que escucha nuestras ordenes vocales para cumplirlas o que nos “asisten” en la conducción (la cual en muchos casos ya está programada para ser autónoma).
- Termostatos que recogen y actúan en base a nuestros gustos térmicos, neveras que nos informan de la agenda del día cuando sacamos el tetrabrik de leche, o colchones que nos enseñan a dormir mejor o avisan de infidelidades.
- Pulseras deportivas que recogen nuestros signos vitales y nuestros hábitos de desplazamiento ya sea para nuestro uso particular o que comparten con otros nuestra posición como parte de nuestra vida social.
- Robots, marcapasos, bombas de diálisis, prótesis, que comienzan a formar parte del mundo de la salud
- Compañeros que en forma de juguetes o de asistentes, ayudarán a niños y ancianos, a relacionarse y estar vigilados y cuidados.



Perdida de la privacidad

Todos estos objetos en el día a día acaban conformando un pulcro y detallado perfil sobre usuarios y empresas. Información al instante sobre gustos, consumos, constantes vitales, patrones de movimiento…

Esos micrófonos en televisores, coches y juguetes, registran y suben nuestras conversaciones, las procesan y como salió en la prensa son objetivo de los servicios secretos, que mejor que un micrófono en cada hogar, para procesar de forma automática millones de conversaciones.

Nuestra voz e imágenes ya forman parte del "etiquetado" actual, identificándonos en cualquier fuente a la que tengan acceso fabricantes, gobiernos y atacantes.


MENÚ BUSCAR elPeriódico EDICIÓN CATALUNYA EDICIÓN GLOBAL INICIAR SESIÓN

ÚLTIMA HORA El Barça pincha contra el Getafe en el Camp Nou (0-0)

TECNOLOGÍA Y SEGURIDAD

Una 'app' de fitness revela ubicaciones secretas del Ejército de EEUU

El fallo es especialmente sensible en países como Irak, Afganistán o Siria

En los coches conectados surge rápidamente la duda ¿de quién son los datos?; la respuesta obvia es del propietario; pero, ¿incluido los de los ocupantes?. Cuestiones como la cesión por descuentos o sus uso en investigaciones criminales y de seguros, abren nuevas dudas.

Amenazas a la Seguridad

No todos estos dispositivos cuentan en su diseño e implementación con un responsable de seguridad, con requisitos y pruebas para este tipo de amenazas. Es más, si nos fijamos que la innovación surge habitualmente de la capacidad de pequeñas startups (empresas emergentes) y que en otros es mediante la incorporación de estas en empresas mayores (por adquisición o integración), nos daremos cuenta porqué está resultando tan fácil, hacer ataques como:

- Engañar a sensores de coches autónomos con pegatinas en señales o punteros láser,
- causando accidentes selectivos o no.
  Tomar el control de servidores en la nube que están recogiendo la posición, imágenes y sonidos de drones o de cámaras (vigilancia, de bebes, de juguetes, webcams,..).
- Utilizar los IoTs como dispositivos controlados en redes de generación de ataques de Denegación de servicio o para la minería de Bitcoins; no hay nada más barato y rentable que disponer de la capacidad de cómputo y comunicaciones de millones de equipos por los que no pagas nada.
- Hacer intrusiones físicas en domicilios gracias al control de la información de los robots o drones de vigilancia de los dueños y de los sistemas de alarma y apertura.

CASO

Imaginemos un individuo Mr. ACME (la victima) y un atacante Mr. Robot.

Mr. ACME que dispone de los siguientes elementos tecnológicos:

- Un coche conectado
- Un contrato inteligente de alquiler de una maravillosa casa. El contrato inteligente rige que con cada pago mensual, la cerradura inteligente se activa para su uso por un mes más.
- Una aspiradora conectada.

Mr. ACME sabe (o intuye) que su aspiradora ha trazado un plano de su casa y por eso es eficiente, también sabe que tiene una cámara y que la aspiradora se comporta como un fiel vigilante cuando él no está. Mr.ACME no sabe (tampoco le interesa) es que el plano y las imágenes son subidas para su procesamiento a la nube.

Mr. ACME sabe que su magnífico coche se conecta internet, le hace diagnósticos en tiempo real, se actualiza sólo, le da el tiempo (climatológico y de desplazamiento) de su futuro trayecto, le reserva restaurantes y hoteles, le lee su correo, sus mensajes y un sinfín de informaciones y acciones.

Mr. ACME no conoce (tampoco le interesa) es que su coche tiene contraseñas por defecto que dan acceso al vehículo, que es accesible su posicionamiento por terceros y que no hay una correcta separación de las redes de entretenimiento e información de usuario, de la de control del vehículo.

Mr. ACME sabe que las cerraduras de su casa son de última tecnología, que cuando llega el trabajador del hogar le abré ya sea con su código personal o remotamente . Sabe que le da un reporte perfecto de entradas y salidas.

Mr. ACME no sabe (tampoco le interesa) que los datos son subidos a la nube tanto para su control como para ser tratados por el fabricante para identificar fallos o demandas.

Lo que sabe Mr. ROBOT (nuestro atacante) es como obtener el plano del hogar (en realidad buscó por una zona determinada en la web del fabricante de la aspiradora) y como es y a qué horas está ocupada la casa y por cuantos personas (gentileza de las imágenes). Con la vulnerabilidad de la aspiradora se conecta a la red local de la casa e identifica la marca y modelo de la cerradura y si dispone de sistema de alarma. Una vez fijado el objetivo, y por simple inspección ocular identifica que Mr. ACME es un feliz propietario de un coche conectado de marca y modelo X. Con toda esa información Mr. ACME localiza las vulnerabilidades en internet, del coche y de las cerraduras.

Mr. ROBOT gracias a la cámara ve que no está ocupada la casa, la visita desactivando la cerradura y la vigilancia de la aspiradora, además bloquea el vehículo de Mr. ACME por si cambia de horario, así es Mr. ROBOT un hombre de nuestro tiempo o mejor dicho, es un niño de su tiempo; tiene solo 14 años.

Mr. ROBOT gracias a la cámara ve que no está ocupada la casa, la visita desactivando la cerradura y la vigilancia de la aspiradora, además bloquea el vehículo de Mr. ACME por si cambia de horario, así es Mr. ROBOT un hombre de nuestro tiempo o mejor dicho, es un niño de su tiempo; tiene solo 14 años.

≡ EL PAÍS TECNOLOGÍA

Roomba, la aspiradora que te espía

El fabricante del robot de limpieza reconoce que quiere vender los planos de los hogares

DIGITAL TRENDS ES Secciones + Features Opinión Videos Más +

La cámara y la cerradura de Amazon pueden ser hackeadas

HOME TECNOXPLORA 〉 INTERNET EL PODER DE UN CIRCUITO CASERO

Un chico de 14 años hackea un coche inteligente

Un 'hackaton' con los coches inteligentes como protagonistas ha sido el lugar de la proeza: un joven de tan solo 14 años ha sido capaz de 'hackear' un vehículo inteligente. Para ello, solo ha necesitado fabricar un circuito casero que ha puesto en jaque la seguridad de los coches del futuro.

MÓVIL

El beneficio económico se basa en la venta a gran escala de información (bases de datos de clientes con todo lujo de detalle, históricos de consumos energéticos de barrios enteros, etc.) y en ataques selectivos con un alto beneficio.

CAUSA DEL INCIDENTE

Pocas o nulas medidas de seguridad de los dispositivos IOT.

MÉTODOS DE ATAQUE

Toma de control del dispositivo.

TIPO DE RIESGO AFECTADO

Es muy variado (pero sobre todo se trata de riesgo patrimonial y reputacional):

- robo de información (ocupación del inmueble, por equipos que se conectan automáticamente al entrar en el mismo)
- vulneración de la intimidad por espionaje en dispositivos de uso diario (tv, cámaras IP, aspiradoras, pulsera deportiva, juguetes)
- salud (marcapasos u otros elementos vitales anexados a nuestro cuerpo)
- suplantación en control en vehículos inteligentes
- DDos

En la mayoría de los casos, la principal finalidad es preparar otros ataques más importantes.

IMPACTO ECONÓMICO DEL INCIDENTE

Muy variado, pudiendo provocar daños funcionales o de privacidad en los dispositivos del propietario (daños directos) o indirectos al estar controlado por un atacante y servir como pasarela de ataque u ofuscación (como proxy) contra terceros.

SECTORES MÁS AFECTADOS POR ESTE TIPO DE INCIDENTES

Infraestructuras críticas y Ámbito personal residencial.

<table>
<tr><th colspan="3">LECCIONES APRENDIDAS</th></tr>
<tr><td>MEDIDAS PREVENTIVAS</td><td colspan="2">Establecimiento de un Modelo de Gobierno Corporativo de Ciberriesgos.
No adquirir equipos que no cuenten con unas medidas de seguridad mínimas (preferiblemente equipos diseñados Security by default).
Cortafuegos .
Sistemas de detección de intrusos.
Planes de continuidad de negocio.
Formación en seguridad de información.
Campañas de concienciación en seguridad de información.</td></tr>
<tr><td rowspan="2">MEDIDAS CORRECTIVAS</td><td>GESTIÓN</td><td>Análisis forense para determinar el alcance y causa del incidente.
Activar planes de continuidad de negocio.
Campaña de relaciones públicas (si se produce daño reputacional).</td></tr>
<tr><td>TRANSFERENCIA (coberturas de seguros)</td><td>Gastos de mitigación y análisis forense.
Ciberextorsión.
Pérdida de Beneficios.
Gastos legales.
Gastos reputacionales.
Daños (si se producen daños materiales, la mayoría de las pólizas excluyen los daños con origen ciber).
Responsabilidad Civil.
Consejeros y Directivos.</td></tr>
</table>

10. ATAQUES A INFRAESTRUCTURAS CRÍTICAS

10. ATAQUES A INFRAESTRUCTURAS CRÍTICAS

DESCRIPCIÓN

Hace ya más de 15 años, todos los países industrializados y en especial los estados miembros de la Unión Europea constaron que se enfrentaban a lo que en aquel momento identificaron como nuevos desafíos; terrorismo internacional y la proliferación de armas de destrucción masiva. Lo que en aquel momento fueron nuevas amenazas, conferían a la Seguridad Nacional un carácter cada vez más complejo, lo que unido a la mayor dependencia que la sociedad tiene del sistema de infraestructuras que aseguran el mantenimiento de los servicios esenciales y a la entrada de nuevos agentes de amenaza tales como el ciberhacktivismo, el cibercrimen, el ciberespionaje o los ciberejércitos (oficiales, y grupos afines), hacen que su protección sea una prioridad para las diferentes naciones, situación en la que España no es una excepción.

Una idea que nace a principios de los 90 fruto del grupo Cult of the Dead Cow. Sus creadores la definen como «hacer hacking o crear tecnología en pos de un objetivo político o social». La primera acción de esas características fue el gusano Wank que penetró en el sistema del Departamento de Energía Americano en protesta contra la energía nuclear en 1989.

Nuestra forma de vida e incluso nuestra vida misma depende de sectores esenciales como el del Agua, Alimentación, Energía, Espacio, Industria Química, Industria Nuclear, Salud, Sistema Financiero y Tributario, Tecnologías de la Información y las Comunicaciones (TIC) o Transporte, entre otros, dependen a su vez de las tecnologías de la información y en consecuencia se exponen a los riesgos de su uso.

Esa dependencia tecnología es además constante y no admite fallos prolongados (y en muchos casos ni durante espacios muy cortos de tiempo); debe estar siempre disponible y ser fiable sin fallos en la integridad de la información. La confidencialidad de actividades, planos, esquemas, manuales, protecciones, debilidades, personas y recursos es atendiendo a los tipos de ciberatacantes antes enunciados un elemento crítico.

La durabilidad y la fiabilidad forman parte intrínseca de los componentes industriales, puesto que deben ser elementos funcionalmente fiables. Las redes de producción y gestión industrial de todos esos sectores no son ajenas a la necesidad de ser más eficaces, eficientes y competitivas (con costes comedidos, buscando menores precios en el desarrollo / adquisición, despliegue y sobre todo en la operación). Ese abaratamiento de coste, hace por ejemplo concentrar las tareas de mantenimiento y en muchos casos las de gestión en puntos remotos ahorrando duplicidades en costes locales de personal o en desplazamientos para el mantenimiento. Es en este punto donde la necesidad de la conectividad se hace necesaria.

En los últimos años hemos visto en los medios como los estados han utilizado los ciberataques contra intereses de sus enemigos o simplemente para desestabilizar a sus competidores, también hemos visto como los criminales han conseguido cientos de millones con un solo golpe o incluso con una sola transacción.

CASO

El troyano BlackEnergy ataca a una planta de energía eléctrica en Ucrania

POR ROBERT LIPOVSKY Y ANTON CHEREPANOV PUBLICADO 5 JAN 2016 - 10:34AM

INVESTIGACIONES

El 23 de diciembre de 2015, unas 80.000 personas se quedaron en Ucrania sin electricidad durante 6 largas horas, abandonadas al frío que típicamente es de -2 y-6 grados.

El apagón fue provocado por un virus denominado BlackEnergy. Este fue una de las piezas usadas en el ataque, llevado a cabo por mercenarios informáticos del más alto nivel y supuestamente trabajando para Rusia. Ucrania, después de dos años de guerra con Rusia, no dudó en señalar a este país como culpable.

El timeline del ataque sería como sigue: un día, un empleado de una central eléctrica de Ucrania recibió un mensaje de correo electrónico que le animaba a pinchar en un documento adjunto. Al hacerlo, se instaló un código malicioso en su ordenador, que lo conectó al ordenador de los criminales y abrió una puerta trasera. Por esta puerta entró BlackEnergy, un virus del tipo troyano que se instaló en tantos ordenadores como pudo y allí se quedó, en silencio, espiando los movimientos en la central.

En un momento dado, los atacantes instalaron a distancia un nuevo módulo a BlackEnergy, llamado KillDisk.

KillDisk está programado para destruir archivos vitales de los ordenadores de una central eléctrica. Después manipularon remotamente los ordenadores para provocar los apagones y, acabado el trabajo, activaron KillDisk, que destruyó los discos duros borrando así las huellas de los hackers en el sistema.

Para provocar más confusión, orquestaron un bombardeo cibernético de los sitios web y centrales telefónicas de la compañía, de forma que los clientes no podía llamar a la misma ni ser informados por web sobre lo que había pasado.

MÓVIL

Generalmente los objetivos de estos ataques suelen ser políticos o sociales (desestabilizar a la competencia, desestabilizar un país, región o sector de actividad) en lugar de económicos (ciberextorsión).

CAUSA DEL INCIDENTE

Aunque las compañías destinan importantes partidas presupuestaria a la seguridad informática, las características propias de los negocios (utilización de telemandos, SCADA's etc.) así como su implantación en diferentes países, y la interrelación no sólo con sus empleados sino también con outsorcers facilitan diferentes puntos de acceso, que en a veces la seguridad informática no evoluciona tan rápido como los posibles ataques.
Falta de concienciación de empleados.

MÉTODOS DE ATAQUE

Malware.
Descuido o negligencia de algún empleado.

TIPO DE RIESGO AFECTADO

Daño reputacional, patrimonial, estabilidad del país, etc.

IMPACTO ECONÓMICO DEL INCIDENTE

Difícil de cuantificar, ya que estos incidentes, generalmente no suelen producir daños materiales o patrimoniales directos, sino que suelen generar paralización de funcionamiento, pérdida de información confidencial, pérdida de contratos licitaciones, pérdidas de tiempo y recursos destinados en volver a la situación inicial de la empresa etc…

SECTORES MÁS AFECTADOS POR ESTE TIPO DE INCIDENTES

A diferencia de otro tipo de negocios, los ataques a este tipo de industrias no son aleatorios, sino que son objetivos seleccionados tanto por Estados como por organizaciones. Fundamentalmente se trata de infraestructuras críticas.

LECCIONES APRENDIDAS

MEDIDAS PREVENTIVAS	Establecimiento de un Modelo de Gobierno Corporativo de Ciberriesgos. Cortafuegos, sistemas de detección de intrusos, etc. Planes de continuidad de negocio. Formación en seguridad de información y mejorar los controles de política interna y de seguridad de la información. Campañas de concienciación en seguridad de información.	
MEDIDAS CORRECTIVAS	**GESTIÓN**	Análisis forense para determinar el alcance y causa del incidente. Comunicación a las autoridades. Campaña de relaciones públicas (cuando se produzca pérdida de reputación). Activación de planes de continuidad de negocio y de respuesta al incidente.
	TRANSFERENCIA (coberturas de seguros)	Gastos de mitigación y análisis forense. Pérdida de beneficios. Ciberextorsión. Gastos de reputación. Responsabilidad Civil. Cobertura de daños (si el ataque provoca daños materiales, la mayoría de las pólizas excluyen daños de originen ciber). Consejeros y Directivos.

NOTA: CNPIC

El Centro Nacional para la Protección de las Infraestructuras y Ciberseguridad (CNPIC) es competente en la protección de las infraestructuras críticas según la Ley 8/2011 y el Real Decreto 704/2011.

La Secretaría de Estado de Seguridad y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información han suscrito un acuerdo en el que, entre otros aspectos, se sientan las bases para la colaboración del CNPIC e Instituto Nacional de Ciberseguridad (INCIBE) en materia de Respuesta a Incidentes para las Tecnologías de la Información de las Infraestructuras Críticas ubicadas en España.

Ambas entidades han puesto en marcha un Equipo de Respuesta a Incidentes de Seguridad especializado en el análisis y gestión de problemas e incidencias de seguridad tecnológica. De este modo, este Equipo de Respuesta se convierte en el CERT especializado en la gestión de incidentes relacionados con las infraestructuras críticas a nivel nacional.

En caso de que una Infraestructura Crítica sufra un problema de seguridad cibernético, el operador responsable de la misma podrá beneficiarse de los servicios del equipo de respuesta, informando de la incidencia a través del Punto de Contacto Único habilitado para esta finalidad respuesta, informando de la incidencia a través del Punto de Contacto Único habilitado para esta finalidad.

Los principales beneficios de este centro de respuesta para el operador de infraestructura crítica son:

- El acceso a un equipo técnico especializado.
- Contar con un servicio de notificación de alerta temprana de riesgos, amenazas o incidentes que puedan afectar a los sistemas de información del operador.
- Aumentar la capacidad de mitigación del incidente a través de la coordinación con los diferentes agentes implicados, como proveedores de servicios en internet, Fuerzas y Cuerpos de Seguridad del Estado u otros CERTs, incluso en el ámbito internacional en el caso de incidentes originados en fuera de la jurisdicción española.
- Contar con un soporte jurídico y legal en todo el ciclo de vida del incidente,- El seguimiento de los incidentes en base a un protocolo de actuación común.
- Además de estas medidas correctivas, también se contará como medida preventiva, con acceso a servicios orientados a proteger de una manera más eficiente las infraestructuras nacionales.

INFOGRAFÍA CYBER RISKS TOP TEN

CYBER RISKS TOP 10

1 FUGA DE INFORMACIÓN

Móvil: económico, espionaje.
Causa: fallos de seguridad, descuido de usuarios.
Cobertura: FOR, VIO, MyS, EXT, REP, RC, CRI, D&O

2 RANSOMWARE

Móvil: económico.
Causa: descuido y/o negligencia de usuario.
Cobertura: FOR, PB, EXT, REP, LEG, MyS, RC, D&O

3 PHISHING

Móvil: económico, daño reputacional, robo info confidencial
Causa: engaño a empleado.
Cobertura: FOR, ROB, REP, LEG, CRI, D&O

4 SUPLANTACIÓN DE IDENTIDAD

Móvil: económico, daño reputacional, fake news.
Causa: suplantación, descuido, fallos de seguridad.
Cobertura: FOR, ROB, CRI, PB, REP, EXT, RC, D&O

5 AMENAZA PERSISTENTE AVANZADA (APT)

Móvil: espionaje, robo de propiedad industrial o intelectual, daño reputacional.
Causa: engaño, vulnerabilidad.
Cobertura: FOR, PB, EXT, REP, RC, DM, D&O

6 FRAUDE DEL CEO

Móvil: económico.
Causa: engaño, controles internos inadecuados.
Cobertura: CRI

ageRS | Asociación Española de Gerencia de Riesgos y Seguros

ISMS forum spain

7 ATAQUE DDOS

Móvil: económico, daño reputacional, hacktivismo.
Causa: tráfico desproporcionado en la red.
Cobertura: PB, EXT, REP, RC

8 SUPLANTACIÓN / MODIFICACIÓN WEB

Móvil: daño reputacional, fake news.
Causa: vulnerabilidad del sistema.
Cobertura:N/A

9 IOT

Móvil: económico, venta datos.
Causa: bajo nivel de seguridad.
Cobertura: FOR, EXT, PB, LEG, REP, DM, RC, D&O

10 ATAQUES A INFRAESTRUCTURAS CRÍTICAS

Móvil: políticos, sociales.
Causa: vulnerabilidad del sistema, mala praxis de empleados.
Cobertura: FOR, PB, XT, REP, RC, DM, D&O

COBERTURAS:

EXT: Ciber extorsión
CRI: Crime
DM: Daños materiales
D&O: D&O
LEG: Gastos legales
FOR: Gastos de investigación y análisis forense
REP: Gastos de reputación
MyS: Multas y sanciones
PB: Pérdida de Beneficios
RC: Resp.Civil
ROB: Robo de identidad
VIO: Violación de datos personales/información

SECTORES:

Alimentación
Energía
E-commerce
Financiero
Gobierno
Medios de pago
Mercancías peligrosas
Nuclear
Particulares
Pymes
Retail
Salud
Teleco
Transporte

PATROCINADORES AGERS

PLATINO

HERBERT SMITH FREEHILLS

MAPFRE

GOLDEN

AIG

AON

AXA

CLYDE&CO

DAC beachcroft

GENERALI

grupo addvalora

MARCH JLT

Munich RE

QBE

Swiss Re Corporate Solutions

ventiv

Willis Towers Watson

XL CATLIN

ZURICH

SILVER

CHUBB

EY Construyendo un mejor entorno de negocios

F·B·A sociados

HIGHDOME

INTERNATIONAL SOS WORLDWIDE REACH. HUMAN TOUCH.

LLOYD'S

MARSH

RSA

PATROCINADORES ISMS FORUM

Realizado por:

AGERS - Asociación Española de Gerencia de Riesgos

ISMS Forum - Asociación Española para el Fomento de la Seguridad de la Información

agers | Asociación Española de Gerencia de Riesgos y Seguros

isms forum spain