# ATAQUE CIBERNÉTICO

## QUÉ ES

A diferencia de las amenazas físicas que requieren acción inmediata, las amenazas y los ataques cibernéticos a menudo son difíciles de identificar o entender. La seguridad informática implica prevenir, detectar y responder a incidentes cibernéticos. Prácticamente todas las organizaciones modernas (incluyendo gobiernos, hospitales, corporaciones, bancos y empresas de servicios públicos) confían en sistemas informáticos para sus operaciones y gestión de datos y, por lo tanto, son vulnerables a los ataques cibernéticos.

La denominada "superficie de ataque" cuya vulnerabilidad es conocida por delincuentes puede incluir equipos informáticos, tabletas, teléfonos y muchos otros dispositivos y artefactos con acceso a Internet en la denominada "Internet de las cosas". Entre los peligros de los ataques cibernéticos están los intrusos que borran sistemas enteros, guardan datos o sistemas operativos para pedir un rescate, roban información confidencial o personal, ingresan a sistemas y modifican archivos o usan una computadora o dispositivo para acceder a listas de contacto y atacar o infectar a otros.

## TÉRMINOS CLAVE

- Un **ataque cibernético** puede ser provocado por individuos, grupos de redes de contactos, grupos terroristas o países, y puede generar problemas graves (y peligrosos) para el gobierno, el comercio, las empresas de servicios públicos y el público en general.
- El **hackeo** es un ataque directo contra un sistema "a través de los cables" en el cual un atacante (ya sea mediante un "bot conversacional" en vivo o automático) accede de modo directo a datos u operaciones seguras/restringidas. Con frecuencia, las vías que permiten estos ataques se abren a través de la suplantación de identidad o "*phishing*" o correos electrónicos fraudulentos (*scams*) de descarga.
- La **Internet de las cosas (IoT)** incluye dispositivos conectados a Internet y artefactos como refrigeradores, sistemas de sonido, relojes, termostatos, sistemas de seguridad, cafeteras, etc.
- La **suplantación de identidad o *phishing*** consiste en la revelación masiva de comunicaciones por correo electrónico o texto con la esperanza de que algunos destinatarios hagan clic en algún lugar del mensaje (por ejemplo, en un adjunto, enlace o botón para "habilitar macros") que active un virus u otro programa malicioso. Una campaña de *phishing* dirigida; por ejemplo, contra un servicio público o gobierno en particular, se denomina estafa o *spear-phishing*.
- La **ingeniería social** involucra la explotación de las vulnerabilidades de un usuario, en lugar de su sistema, para burlar las medidas de seguridad informática. Algunos ejemplos son la suplantación de identidad, correos electrónicos fraudulentos y otros inconvenientes. Los usuarios suelen ser los elementos que pueden derrotarse más fácilmente dentro de la arquitectura de seguridad informática.

## QUÉ HACER

### Antes (Preparación/Mitigación)

- ❑ Mantenga el *firewall* activado y actualizado.
- ❑ Instale o actualice los programas de antivirus/antispyware.
- ❑ Use contraseñas únicas y difíciles, y cámbielas periódicamente.
- ❑ Busque e instale inmediatamente todas las actualizaciones en su sistema operativo, *firmware*, *software* y antivirus.
- ❑ Sea cuidadoso con lo que descarga. Nunca haga clic en un adjunto, enlace o macro de un correo electrónico o mensaje de texto no solicitado.
- ❑ Apague su computadora cuando no la usa.
- ❑ Siempre verifique el origen de los correos electrónicos y, si tiene dudas, elimínelos.
- ❑ Sospeche de correos electrónicos de contactos conocidos que parezcan "extraños" (errores de ortografía, uso extraño de vocabulario o sintaxis, lenguaje genérico, URL con enlaces poco comunes); muchas campañas de hackeo imitan correos electrónicos conocidos.
- ❑ Para su análisis, tome una captura de la pantalla del contenido sospechoso antes de eliminarlo.
- ❑ Guarde, periódicamente, una copia de seguridad de todos los datos en un disco externo o en Cloud; habilite la función "Time Machine" (Máquina del tiempo) si usa una Mac.

### Durante (Respuesta)

- ❑ Desconecte un dispositivo infectado de la red.
- ❑ Si está en el trabajo, informe al personal del departamento de Tecnología de la Información (TI) de cualquier sospecha de ataque o ataque confirmado a sus dispositivos y envíe una captura de pantalla.
- ❑ Si un incidente provoca la pérdida de información financiera, personal o médica, haga la denuncia ante la policía.

### Después (Recuperación)

- ❑ Informe a todos quienes podrían verse afectados negativamente; entre ellos, cuentas de crédito, cuentas bancarias, clientes, empleados, familiares y amigos. Cambie sus cuentas y todas las contraseñas.
- ❑ Corra escaneos y funciones adecuadas para eliminar todo tipo de infecciones.
- ❑ Supervise su informe crediticio, resúmenes bancarios, inversiones y resúmenes de tarjeta de crédito.
- ❑ Asegúrese de que su dispositivo no esté infectado; borre el disco duro y vuelva a instalar todos los programas si tiene alguna duda.