MÓDULO 5

GESTIÓN DE RIESGO EN EL NEGOCIO

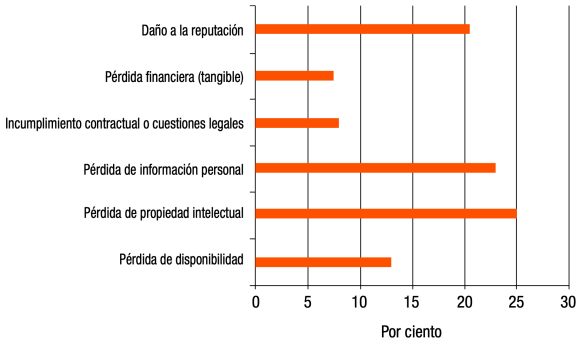
Prof. Mg. Rafael Mellado S.
rafael.mellado@pucv.cl
COM5163 – Sistemas de Información 3
Escuela de Comercio

AMENAZA PERSISTENTE AVANZADA (APT)

- Comprensión de una APT
  - Visión general
  - ¿Qué es un APT?
  - ¿Cómo responden otras empresas?

AMENAZA PERSISTENTE AVANZADA (APT)

- El mayor riesgo para la empresa relacionado con un ataque de APT exitoso, según los encuestados en la encuesta de ISACA:



TERMINOLOGÍAS SOBRE APT

Malware
También conocido como software mal intencionado

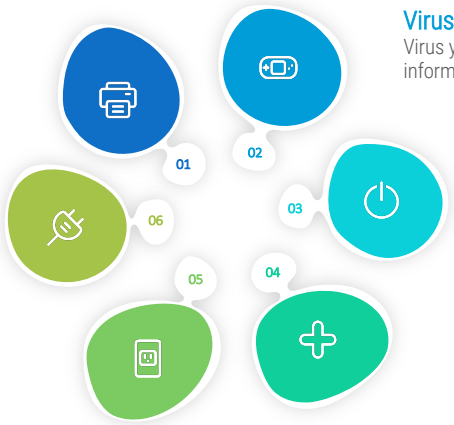
Virus
Virus y gusanos informáticos

Troy horse
Caballos de troya o troyanos

Día cero
Vulnerabilidades de día cero

Botnet
Botnets o robot network

Drive-by
Descargas de software tipo drive-by



RESPONSABLES DE ATAQUES APT

Amenaza	Lo que buscan	Impacto al negocio
Agencias de inteligencia	Política, defensa o secretos comerciales	Pérdida de secretos comerciales, ventaja competitiva
Grupos criminales	Las transferencias de dinero, oportunidades de extorsión, información de identidad personal o cualquier secreto para su posible venta posterior	Pérdida financiera, acceso a datos de clientes a gran escala o pérdida de secretos comerciales
Grupos terroristas	Generación de terror generalizado a través de la muerte, destrucción y trastornos	Pérdida de producción y servicios, irregularidades en el mercado de valores y posible riesgo para la vida humana
Grupos activistas	Información confidencial o interrupción de servicios.	Violación de datos grave o pérdida del servicio.
Fuerzas armadas	Inteligencia o posicionamiento para apoyar futuros ataques contra las infraestructuras nacionales críticas.	Graves daños a las instalaciones en caso de conflicto militar.

IMPACTOS DE ATAQUES APT

- Daño generado por un ataque APT
- Características de un ataque de APT:
  - Buena investigación
  - Sofisticado
  - Furtivo
  - Persistente
  - Excepciones

EVALUACIÓN DE RIESGO DE UN APT

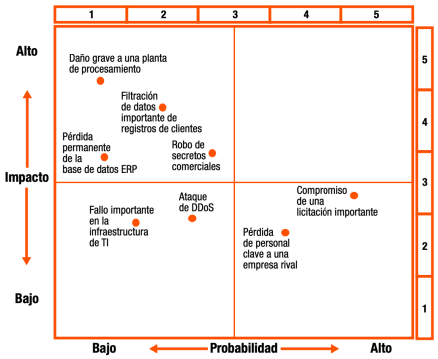
- Identificación de los activos en riesgo:
  - Activos físicos
  - Activos financieros
  - Activos intelectuales
  - Información
  - Conocimiento
  - Relaciones
  - Reputación y valor de la marca

EVALUACIÓN DE RIESGO DE UN APT

- Identificación de las amenazas específicas de APT para los activos:
  - Existe un posible gran riesgo de APT relacionado con las empresas modernas, así que la selección cuidadosa y las prioridades claras son esenciales para evitar generar demasiadas acciones menores que reducirían la atención prestada a los riesgos más grandes e importantes.

EVALUACIÓN DE RIESGO DE UN APT

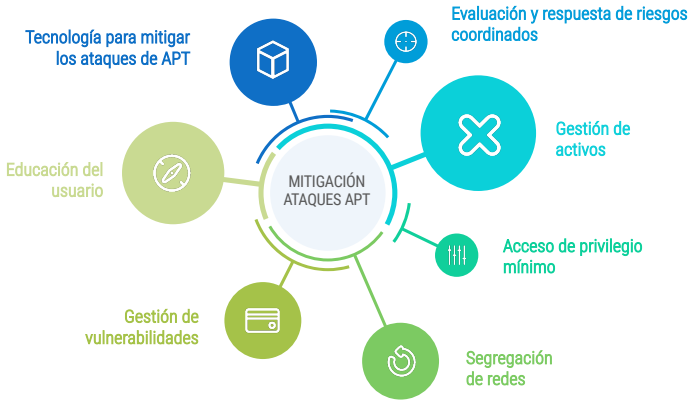
- Evaluación del riesgo de APT



GESTIÓN DE LA SEGURIDAD PARA AMENAZAS APT

- Sistema de gestión de seguridad de la información (ISMS)
- Proceso de gestión de riesgos
- Seguridad de las personas
- Seguridad física
- Arquitectura de redes
- Gestión de redes
- Detección de software malintencionado
- Gestión de plataformas informáticas
- Control de acceso de la aplicación
- Desarrollo y mantenimiento de sistemas.
- Proceso de informe de incidentes
- Gestión de la continuidad del negocio + gestión de crisis

MEDIDAS CLAVE PARA MITIGAR ATAQUES APT



SIGNOS DE UN ATAQUE APT

- La naturaleza oculta de los ataques de APT hace de su detección una tarea difícil, la cual se refleja en el gran número de intrusiones.
- Signos:
  - Comportamiento sospechoso
  - Comportamiento humano
  - Actividad de la red

MEDIDAS DE SEGURIDAD

- Medidas básicas de seguridad:
  - Sistemas antivirus
  - Sistemas de detección de intrusiones
  - Cortafuegos (firewalls)
  - Pruebas de intrusión
  - Autenticación fuerte

MEDIDAS DE SEGURIDAD

- Medidas de seguridad avanzadas:
  - Prevención de intrusiones
  - Prevención de fuga de datos
  - Escaneo de vulnerabilidades
  - Simulación en entorno de pruebas
  - Supervisión de actividad de la base de datos
  - Pruebas de seguridad de las aplicaciones

MEDIDAS DE SEGURIDAD

- Contramedidas específicas para APT:
  - Inspección profunda de paquetes
  - Coincidencia de patrones de comunicaciones
  - Supervisión de la integridad de los archivos
  - Gestión de la configuración de seguridad
  - Información de seguridad y gestión de eventos

MEJORES PRÁCTICAS DE SEGURIDAD

Ciclo de vida de desarrollo de seguridad

El ciclo de vida de desarrollo de seguridad (SDL) de Microsoft es un proceso de desarrollo de software que ayuda a los desarrolladores a crear software más seguro.

Honeypots

Un honeypot es una trampa diseñada para atraer a los intrusos.

Informática confiable

La informática confiable (TC) es una tecnología basada en un conjunto de estándares abiertos desarrollados por el Grupo para la Informática Fiable, una alianza de los principales vendedores que incluye a HP, IBM, Microsoft e Intel.

Inspecciones forenses

Las inspecciones forenses periódicas de las máquinas que puedan ser objeto de un ataque APT son un medio efectivo para identificar los ataques APT o para dar seguridad de que las plataformas que contienen datos críticos o sensibles no están comprometidos.

Lista blanca de aplicaciones

En lugar de intentar bloquear el malware en la lista negra se mantiene una lista blanca

GESTIÓN DE UN INCIDENTE APT

- Creación de un CSIRT
  - Rol del CSIRT
- Creación de un centro de operaciones de seguridad
- Interconexión del CSIRT con otros equipos de crisis
  - Varias estructuras de equipos
  - Equipos
  - El valor de la preparación y los ejercicios
- Identificación de incidentes
- Evaluación de daños

GESTIÓN DE UN INCIDENTE APT

- Gestión de crisis
- Contención
- Recuperación
- Investigación
- Aprendizaje a partir de incidentes
- Informe post mortem

REVISIÓN DE CONTROLES APT

ESCUELA DE COMERCIO
PONTIFICIA UNIVERSIDAD CATÓLICA DE VALPARAÍSO

MÓDULO 5

GESTIÓN DE RIESGO EN EL NEGOCIO

Prof. Mg. Rafael Mellado S.
rafael.mellado@pucv.cl
COM5163 – Sistemas de Información 3
Escuela de Comercio