Estado Actual de la Cibersecuridad: Amenazas y activos involucrados

Ing. Carlos Luis Vidal, CISSP, CISA, CISM, CRISC, CIA, CFE, CobiT, ITIL

Past President- ISACA Lima Perú

Agenda

- Descripción de las principales amenazas a la ciberseguridad.
- Activos Involucrados
- Descripción de los principales Controles

Carlos Eduardo Luis Vidal

Master of Business Administration (MBA) por Centrum Católica e Ingeniero Informático por la Pontificia Universidad Católica del Perú. Es Auditor Senior de Tecnologías y Sistemas de Información en Interbank. Asimismo, es miembro del Consejo Directivo de la Asociación de Auditoría y Seguridad de Sistemas del Perú (ISACA Lima) como Past President. Ha sido Presidente de ISACA Lima. Cuenta con más de 10 años de experiencia en Auditoría y Seguridad de Sistema de Información. Adicionalmente, ha brindado cursos de Auditoría y Seguridad de Sistemas para empresas de diversos rubros, así como en ISACA Lima y Instituto de Auditores Internos del Perú. Cuenta con las certificaciones internacionales de Auditor de Sistemas Certificado (CISA), Gerente de Seguridad de Sistemas (CISM), Profesional de Seguridad de Sistemas (CISSP), Auditor Interno Certificado (CIA), Examinador de Fraude (CFE), entre otras.

- Ciberseguridad:

  La ciberseguridad, se ocupa de la protección de los **activos digitales**, desde las redes al hardware y la información que es procesada, almacenada o transportada a través los sistemas de información interconectados.

  Mientras que la **seguridad de información** trata con la información, **independientemente de su formato** - incluye los documentos en papel, propiedad digital e intelectual en las mentes de las personas, y las comunicaciones verbales o visuales.

  Fuente: Manual de Preparación CSX Cybersecurity 2014

- Principales amenazas a la ciberseguridad.

Estado Actual de la Ciberseguridad: Amenazas y activos involucrados

5

- Principales amenazas a la ciberseguridad.
  Cobra cada vez mayor relevancia.

Fuente: ISACA Internacional. 2017

Estado Actual de la Ciberseguridad: Amenazas y activos involucrados

6

- APT:

  El término "amenaza persistente avanzada" (APT) denota un tipo de amenaza y ataque que es técnicamente sofisticado y usualmente presente en el contexto del ciberdelito o la ciberguerra. Los APTs van más allá del ataque o amenaza estándar.

  Los APT están diseñados para infiltrarse en un entorno de TI protegido utilizando técnicas y vectores avanzados. El objetivo de un ataque basado en el APT es establecer y mantenerse secreto.

  Fuente: ISACA 2017

- APT: Ciclo de Vida

Ejemplos:
Stuxnet (Ataque a central nuclear iraní)
Aurora (Ataque a Google inc.)
Etc..

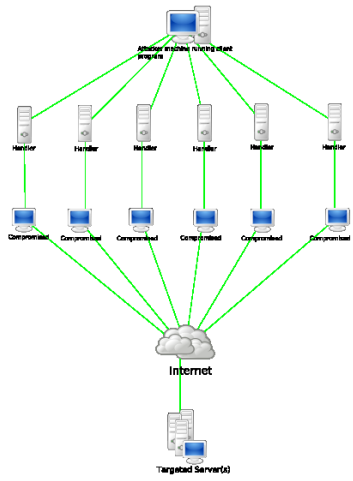
- Ddos (Distribuited Denial of Service)

El término "denegación de servicio" denota generalmente un ataque, o una serie de ataques, en un entorno de TI, con el fin de interrumpir o deshabilitar los servicios proporcionados por ese entorno.

En un escenario DDoS , requieren recursos significativos puestos a la tarea de atacar simultáneamente el entorno de destino. En la mayoría de los casos, estos recursos se montan a nivel mundial mediante el secuestro y/o *autorización* del usuario final.

Fuente: ISACA 2017

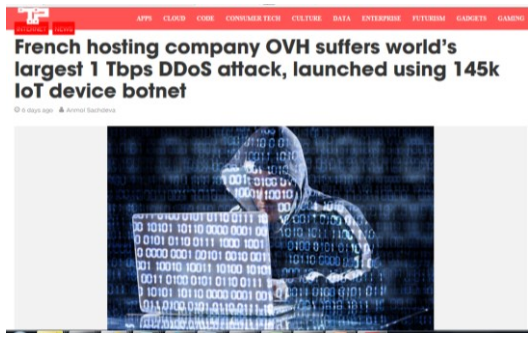
- Ddos (Distribuited Denial of Service)



Fuente: ISACA 2017

- Ddos (Distribuited Denial of Service)

- Ddos (Distribuited Denial of Service)



IoT: no solo se usa host, sino también camaras ip y grabadoras de video digital

- **Agente Interno (Genérico)**

Una amenaza interna se define como el potencial de un acto u omisión adverso dentro de la organización, es decir, cometido por empleados o individuos con un conjunto específico de privilegios y derechos que se asemejan a los de los internos. Como con todas las formas de comportamiento negligente o deliberado, las amenazas internas pueden variar en términos de impacto y sofisticación

Fuente: ISACA 2017

- **Agente Interno (Genérico)**

Ejemplos:

Caso de Tamara Moon / Citigroup:

Empleado usó acceso privilegiado y brechas de seguridad para robar dinero a los clientes del banco; Daños totales de unos US $ 750.000

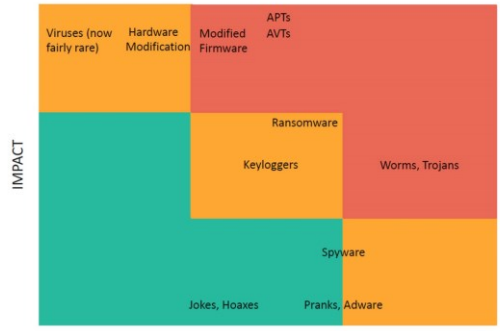
Caso Jerome Kerviel / Société Générale
Empleado utilizó el acceso privilegiado adquirido durante un período de años para eludir los límites de negociación, causando daños de más de € 4.000.000.000. Este caso ilustra la delgada línea entre el ataque interno y el daño interno no intencionado. Kerviel dirigió inicialmente una cartera de negociación muy exitosa (más allá de los límites, pero con aprobación de la administración tácita) hasta que los cambios en el mercado provocaron las pérdidas repentinas.

Caso "Outsourcing"
El desarrollador contrató a una persona en China para hacer el trabajo. Un caso atípico de mala conducta que implícitamente creó una amenaza significativa al revelar información a terceros desconocidos

Fuente: ISACA 2017

- Malware

El término "malware" denota cualquier software malicioso utilizado con el propósito de atacar sistemas y entornos de TI. Hay un gran número de tipos de malware. Normalmente, el malware se clasifica según su impacto y su prevalencia en la naturaleza, como se muestra en la siguiente figura:



Fuente: ISACA 2017

- Malware
  - 10 Top Malware:
    - Kovter
    - ZeuS/Zbot
    - Ursnif
    - DNSChanger
    - Ponmocup
    - Emotet
    - PCRat/Gh0st
    - Hancitor
    - Tinba
    - Virlock

- Fuente:Center for Internet Security ® 2017

- Ransonware

El término "ransomware" se refiere la inserción de malware que está diseñado para solicitar un rescate en dinero o dinero equivalente del usuario final (bitcoin)

Esto se logra generalmente en una de dos maneras:

a) El primer enfoque consiste en cifrar los datos del usuario o en el acceso corrupto a partes o todo el entorno de TI del usuario final.

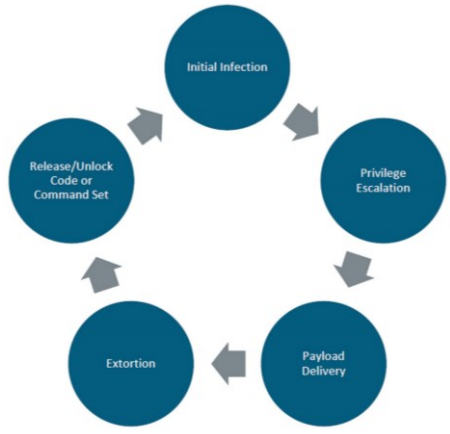
b) El segundo enfoque consiste en presentar información incriminatoria y amenazar al usuario final con la aplicación de la ley, por lo general a través de denuncias de carácter penal grave como la posesión de pornografía infantil.

En la práctica, el ransomware es un **fenómeno generalizado**. Tiende a afectar a los usuarios de forma no segmentada, dado que los canales de distribución masiva se utilizan para desplegar ransomware.

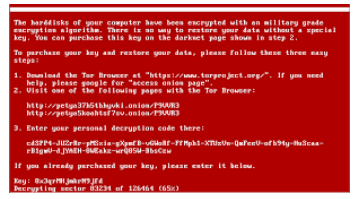
En contraste con APT o malware complejo, ransomware es un tipo de ataque de mercado masivo que apunta a recoger cantidades relativamente pequeñas de dinero.

Fuente: ISACA 2017

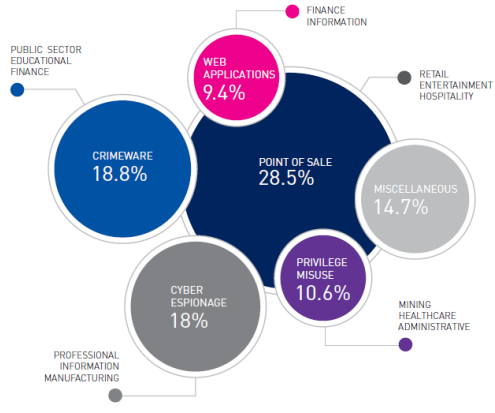
- Ransonware : Ciclo de Ataque



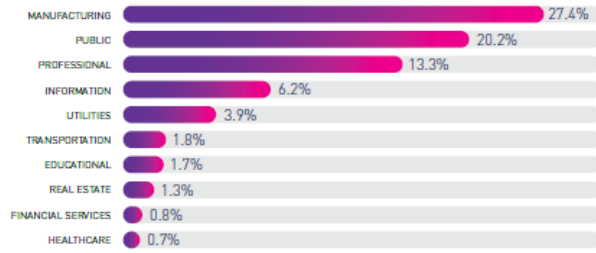
- Ransonware : Ejemplos.
- **WannaCry:** Los países más afectados que han sido reportados son Rusia, Ucrania, India y Taiwán, pero partes del servicio nacional de salud de Gran Bretaña (NHS), Telefónica de España, FedEx, Deutsche Bahn, y las aerolíneas LATAM también fueron afectadas; junto con muchos otros blancos a nivel mundial (incluyendo perú)
- **Petya:** Foco empresas ucranianas, pero llegó afectar a empresas peruanas



- Principales Industrias y tipos de servicio afectadas por ataques informáticos



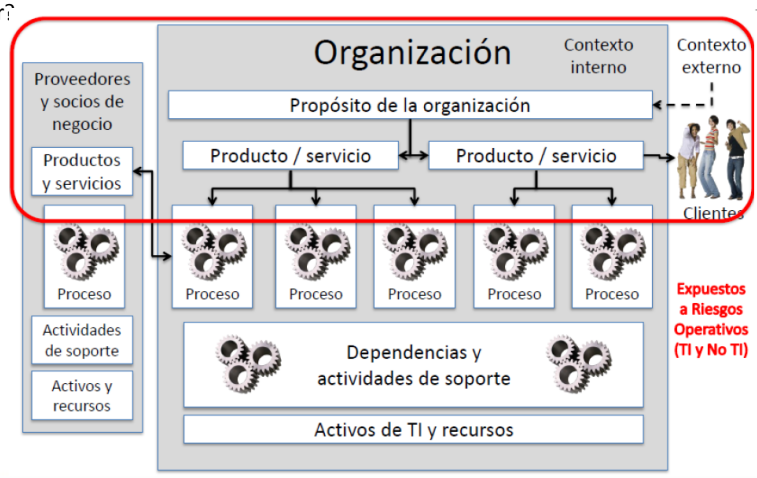
- Principales Industrias afectadas por ataques informáticos



Estado Actual de la Cibersecuridad: Amenazas y activos involucrados

21

- Primer Paso: Establecer contexto – ¿Qué proteger? y ¿cuánto tengo que proteger?



Fuente: Mario Ureña, 2015

Estado Actual de la Cibersecuridad: Amenazas y activos involucrados

22

- Principales controles

  Control : Aquello que permite reducir la probabilidad y/o impacto de un riesgo de ciberseguridad

Fuente: ISACA, 2015

Los controles perimetrales

Están diseñados para proporcionar protección en el límite exterior de la empresa, o su esfera de interés.

El perímetro real a menudo se extiende a partes del entorno de TI que son administradas por terceros (por ejemplo, en la subcontratación o las relaciones de servicio administrado). Técnicamente, los controles perimetrales previenen el acceso no autorizado, proporcionan señalización y alertas (por ejemplo SIEM) y separan el entorno empresarial extendido de la Internet pública. Ejemplos de defensa perimetral incluyen cortafuegos, zonas desmilitarizadas, dispositivos de monitoreo de eventos, etc.

Fuente: ISACA 2017

La defensa en profundidad

La defensa en profundidad proporciona capas secuenciales de protección contra ataques, a saber, mediante la formación de zonas (como capas de cebolla) de densidad de control creciente y mecanismos de defensa más sofisticados.

Las configuraciones típicas de defensa en profundidad suelen incluir la definición de un perímetro exterior (por ejemplo, una zona semipública con interacción entre el cliente o el público en general), un perímetro interior (por ejemplo, sólo para empleados) y zonas protegidas (por ejemplo, sólo para investigación y desarrollo)).

Algunas de estas capas pueden incluir mecanismos de defensa específicos tales como honeypots para agregar a la fuerza defensiva total.

Fuente: ISACA 2017

Gestión de backups

Los controles y la protección de la seguridad cibernética deben incluir siempre una estrategia de respaldo apropiada (y completa) para el hardware/datos que pueda haber sido objeto de un ataque cibernético.

Mientras que el componente del hardware sí mismo puede todavía ser funcional después de un reajuste, se toma a menudo fuera de la circulación para el forense, así creando la necesidad de un reemplazo inmediato. Para dispositivos de hardware particularmente críticos o sensibles, es buena práctica duplicar el dispositivo. Y sobre todo de la información de la organización.

Fuente: ISACA 2017

Gestión de parches

El parcheado en ciberseguridad es una actividad vital, así como un conjunto de control en la aplicación, el sistema operativo y las capas de firmware.

Los parches actualizados proporcionados por el proveedor o programador del software son una parte esencial de la administración general del cambio. Cuando los parches no se aplican de manera oportuna, existe un riesgo significativo de explotar las debilidades conocidas. En la práctica, el parche se combina a menudo con sistemas de endurecimiento para salvar la brecha entre la publicación de una debilidad y la entrega del parche. Por lo general, el parche se realiza con mucha frecuencia, con un ligero retraso debido a las pruebas corporativas antes de implementar el parche. Las aplicaciones y sistemas sin parches se encuentran entre los puntos de entrada más frecuentes para ataques cibernéticos, al igual que los sistemas operativos y aplicaciones de fin de vida útil.

Fuente: ISACA 2017

Controles de punto final

Los terminales típicos incluyen dispositivos de escritorio y móviles, a menudo con sistemas operativos estándar que difieren del mundo de host / backend (server)

Los controles incluyen los entornos administrados (incluyendo sandboxes), los datos encapsulados, la segregación en dispositivos de entornos empresariales y privados, etc. Los conjuntos de control de punto final siempre deben equilibrar la necesidad de seguridad contra el interés legítimo del usuario del punto final, particularmente en un escenario BYOD.

Fuente: ISACA 2017

- Ataques «client side»

Fuente:Center for Internet Security ® 2017

Concientización de Usuario/Gerencia

Los usuarios finales, incluida la gestión, deben ser conscientes de la seguridad cibernética, incluidos los riesgos y amenazas típicos, así como las contramedidas y el buen mantenimiento.

En cuanto a los controles, la sensibilización de los usuarios debe fomentarse informando, comunicando y probando la seguridad cibernética en todos los niveles de usuarios. Dependiendo de su misión, los empleados y los gerentes deben recibir educación y capacitación regulares sobre requisitos legales, regulatorios e internos. En la práctica, esto se hace a menudo mediante sesiones de formación obligatorias (por ejemplo, basadas en la web).

Otros controles sobre la concienciación incluyen incentivos, inclusión de la ciberseguridad en las evaluaciones anuales e información / educación sobre eventos pasados. Este último ha resultado ser un control particularmente eficaz, ya que a menudo los empleados encuentran más fácil relacionarse con una historia "real" y posteriormente adoptar una actitud de cautela y vigilancia.

Fuente: ISACA 2017

FIN

Ing. Carlos Luis Vidal, CISSP, CISA, CISM, CRISC, CIA, CFE, CobiT, ITIL
cluis@pucp.edu.pe