ASIS INTERNATIONAL
Capítulo 215 - Buenos Aires, Argentina

KNOWHOW SECURITY
SABEMOS QUE HACER

Desafíos de la Convergencia en Ciberseguridad

CAP 4 - Manual de Protección de Activos
CONVERGENCIA? → “dos o más eventos concluyen en un mismo espacio“

Christian Vila
CTO Director de Tecnología
KnowHow Security Labs

C|EH Certified Ethical Hacker, EC Council.
Director KnowHowSecurity
Sub Inspector (r) de la Policía de Seguridad Aeroportuaria
Especialista Investigación de Homicidios (MAT N° 510, ACRA)
Agente de Inteligencia (FAA)

christian.vila@knowhowsec.com

KNOWHOW SECURITY
SABEMOS QUE HACER

KNOWHOW SECURITY

Investigaciones y estudios , exposiciones y congresos en Latinoamérica

- Identificación de Posición Absoluta Temporal de dispositivos móviles, Universidad INACAP Chile (Patagonia Hacking), enlace aquí.
- Herramientas digitales de fuentes abiertas para la investigación criminal (CIBSI 2017), enlace aquí.
- Ciberseguridad Financiera – Criptomonedas, Centroamérica, enlace aquí.
- SHODAN.io como herramienta de seguridad y pentesting, Google GDG Neuquén, enlace aquí.
- Análisis técnico del ataque de ransomware WannaCrypt (iCoaching), enlace al trabajo aquí.
- Técnicas de OSint “Le ocurrió a un amigo”, (Infosecurity), enlace al trabajo aquí.
- Ciberdelitos, desde la escena hasta la corte (Universidad de Río Negro, Infosecurity), enlace al trabajo aquí.
- Laboratorio “Metadata Exposed”, Instituto Prueger, Neuquén (ARG), enlace al trabajo aquí
- IoT Security, Google GDG Neuquén, enlace al trabajo aquí.

iSEC

INSTITUTO PRUEGER

REPUBLICA ARGENTINA
PSA
POLICÍA DE SEGURIDAD AEROPORTUARIA

4.1 Riesgos para la red ¿de qué estamos hablando?

KNOWHOW SECURITY
SABEMOS QUE HACER

- Converger en ciberseguridad implica la integración formal, colaborativa y estratégica, de los recursos de seguridad de la organización.
- Converger en ciberseguridad permitirá:
  - reducir el riesgo
  - aumentar la eficiencia y efectividad operacional
  - ahorrar costos!!!
- Y si estas tres características CONVERGEN…

habrá muchos jefes contentos!!

KNOWHOW SECURITY
SABEMOS QUE HACER

Es la SEGURIDAD FÍSICA un riesgo para la red ????

KNOWHOW SECURITY
SABEMOS QUE HACER

Denegaciones de Servicio

https://computerhoy.com/listas/tecnologia/mayores-ataques-ddos-historia-internet-555187

MIRAI la DOS más grande de la historia, IoT el causante

Es la SEGURIDAD FÍSICA un riesgo para la red ????

KNOWHOW SECURITY
SABEMOS QUE HACER

- **Ejemplo 2 →** Contales el caso de la Compañía Mayorista de Energía que era accesible a través de sus servicio de control de **presentismo por proximidad.**

- **Ejemplo 3 →** COVID 19, En hospital de Alemania muere una paciente en la sala de espera porque el hospital "se ovidó" de ella, el sistema de ticketeras de admisión estaba infectado de un ransonware. (ver más)

Medidas de CONTROL

- Algunas veces **implementar sistemas de control o medidas de seguridad física** puede dejar puertas de acceso a los sistemas de información de la compañia.
- Entonces cuando **PROYECTEMOS** estas medidas → tendremos que considerar medidas que **NO PERMITAN:**
  - **Denegación de servicios (y DDOS)**
  - **Robo de datos**
  - **Acceso indebido a los Datos (Inserción, Modificación o Destrucción)**
  - **ATAQUES A LA INFORMACIÓN DE LA COMPAÑÍA.**

Medidas de CONTROL → QUE

- Justamente lo que dice el Manual en el punto 4.1:

„Cuando los profesionales de seguridad física ponen tecnología de seguridad física en la red, abren la puerta a importantes riesgos de seguridad basados en la red...“

  - **Denegación de servicios (y DDOS)** → detener el funcionamiento de un sistema informático
  - **Robo de datos** → Hurto de información sensible de la Empresa
  - **Acceso indebido a los Datos → Inserción, Modificación o Destrucción**
- En definitiva el QUÉ se refiere a todos los **ATAQUES A LA INFORMACIÓN DE LA COMPAÑÍA.**

Medidas de CONTROL → COMO

- Todo se trata de una correcta **gestión de riesgo** que se centra en tres elementos básicos: CIA
  - **Confidencialidad**
  - **Integridad**
  - **Disponibilidad**
- Entonces vamos a identificar que elemento corresponde a que riesgo:
  - **Denegación de servicios (DOS) → disponibilidad**
  - **Inserción de datos inexactos → integridad**
  - **Robo de datos → confidencialidad**
  - **Modificación de Datos → integridad**
  - **Destrucción de Datos** → disponibilidad

Resumiendo...

- Dice el manual→ "Para hacer frente a los riesgos de**seguridad provocados por la convergencia**, los profesionales de **seguridad física deben ser capaces de clasificar el riesgo** del ISS (information security system)conforme a la tríada CIA.
- Este enfoque ayuda a **evaluar rápidamente los tipos de riesgos** que se enfrentan y luego aplicar las **estrategias adecuadas** para mitigar esos riesgos."

Gestión de riesgo → ¿dónde estamos parados?

KNOWHOW SECURITY
SABEMOS QUE HACER

Lo que nos prometen

La realidad...

ESTUDIO DE CASO DE RED → CCTV

KNOWHOW SECURITY
SABEMOS QUE HACER

Como funciona?

ESTUDIO DE CASO DE RED → CCTV DESPLIEGUE
LAN, circuito más antiguo y muy utilizado

Como funciona?, Cómo se rompe?, Cómo se ataca?

COMPONENTES de red utilizados:

- Switch
- Firewall
- NetVideoRec (NVR)
- Ethernet
- Wifi
- BT (lue Tooth)

ESTUDIO DE CASO DE RED → CCTV DESPLIEGUE
LAN, circuito más antiguo y muy utilizado

KNOWHOW SECURITY
SABEMOS QUE HACER

Como funciona?, **Cómo se rompe?, Cómo se ataca?**

Debilidades:

- Todo el sistema se conecta a internet y es accedido desde dispositivos a través de VPN → (la clave esta en una cartelera o es compartido por todos en la oficina!)
- Todo el sistema está conectada en la LAN → todos los ataques de LAN (lo que vamos a ver en hacking directo)

ESTUDIO DE CASO DE RED → CCTV
DESPLIEGUE LAN, principales riesgos

KNOWHOW SECURITY
SABEMOS QUE HACER

Denegación de servicios → Inhibidores WIFI que se usan para cámaras y alarmas, el mismo sistema tira abajo la red (jammers)

Inserción de datos inexactos → Videos antiguos o videos captados con otros circuitos para encubrimiento (por acá no pasó nadie, contar ejemplo de femicidio río limay que duplicaron un archivo)

ESTUDIO DE CASO DE RED → CCTV
DESPLIEGUE LAN, principales riesgos

KNOWHOW SECURITY
SABEMOS QUE HACER

Robo de datos→ video accedido por pesonas NO autorizadas (ej. secuestro extorsivo en Neuquén)

Modificación de datos → Modificación de los metadatos para encubrimiento

Destrucción de datos → Borrado de evidencia para encubrimiento, y la tipica se pisó el video!.

ESTUDIO DE CASO DE RED → CCTV DESPLIEGUE LAN, SOLUCIONES!!!

KNOWHOW SECURITY
SABEMOS QUE HACER

- **Analizar** y **RE definir** los riesgos.
- **Cuantificarlo** → posibilidad de ocurrencia y gravedad.
- Definir **medidas de protección** y PROBARLAS!!!!.
- Incluirlas en las **auditorías** de seguridad.
- **¿cómo hacer todo esto?** → Como funciona?, Cómo se rompe?, Cómo se ataca?

- INGENIERÍA SOCIAL :):):)
- MALWARE :(
- HACKING DIRECTO :)
- WEB ATTACK :)

4.2 ATAQUES DE COMUNICACIÓN
Ingeniería Social

KNOWHOW SECURITY
SABEMOS QUE HACER

4.2 ATAQUES DE COMUNICACIÓN
Ingeniería Social

KNOWHOW SECURITY
SABEMOS QUE HACER

Hola... Tu eres elempleado lindo del tercer piso no?, estamos haciendo un relevamiento de la privacidad en las camaras; podrías darme el acceso al sistema de videos por favor?

4.2 ATAQUES DE COMUNICACIÓN
Ingeniería Social

KNOWHOW SECURITY
SABEMOS QUE HACER

- **INGENIERÍA SOCIAL**→ son técnicas de manipulación que se usan para obtener información confidencial de los usuarios.
- **Un ataque de IS completo implica tres etapas → ENGAÑO → MANIPULACIÓN → ATAQUE PURO**
- 1.**Engaño**: el atacante simula distintas actividades **distractoras** y **confiables, tambien podría ser** vía mail, mensajerías (wapp, telegram, redes sociales), sms o cualquier otro medio de comunicación

4.2 ATAQUES DE COMUNICACIÓN
Ingeniería Social

KNOWHOW SECURITY
SABEMOS QUE HACER

- **2. Manipulación:** la víctima está distraída y tiene confianza –tambien se usa en la mayoría de las estafas- entonces simula solucionar problemas graves de la víctima
- " ...de esta forma podrá reanudar de nuevo suscripción y así poder seguir utilizando nuestro servicio"
- "...necesitamos que verifique su información cuanto antes, y así evitar perdidas/demoras en sus futuras operaciones"

4.2 ATAQUES DE COMUNICACIÓN
Ingeniería Social

KNOWHOW SECURITY
SABEMOS QUE HACER

- **3. Ataque Puro:** ahora que la víctima está **distraida + confiada + necesitada**, y el atacante le ofrece la solución!!!!!.
- Si no sospechó al momento inicial menos va a sospechar ahora! y el atacante va a resolver su necesidad de distintas formas→ le dice que se baje e instale este archivo..., que vea la siguiente imagen..., que siga el link y deje los datos de tarjeta de debito/crédito...

4.2 ATAQUES DE COMUNICACIÓN
Malware

KNOWHOW SECURITY
SABEMOS QUE HACER

- MALWARE es similar a los virus en medicina, el código malicioso -malware- es un programa que intenta corromper sistemas, redes, dispositivos, archivos; **casi siempre con la colaboración del usuario,** posterior a ser ejecutados intenta distribuirse y propagarse a otros dispositivos, equipos.
- Categorías:
  - troyanos y rootkits
  - virus: necesita ser ejecutado por el usuario
  - gusanos: -worms- se autoejecuta y se autopropaga

4.2 ATAQUES DE COMUNICACIÓN
Malware

KNOWHOW SECURITY
SABEMOS QUE HACER

- Algunas soluciones para mitigar el riesgo del MALWARE:
- instalar software antivirus para **detección y remoción**; y definir procedimientos de upgrades.
- definir políticas de avir que cumpla **todo** el parque de equipos.
- definir **medidas de control para bajar y abrir archivos** de internet, email, dvd, usb, etc.
- realizar **copias limpias** de la información de la compañía (escanear antes del backup)
- programar **escaneos regulares** en los sistemas.
- **educar** a los empleados de la compañía.

4.2 ATAQUES DE COMUNICACIÓN
Ataques Web (Web Attacks)

KNOWHOW SECURITY
SABEMOS QUE HACER

- Los ataques web se realizan en los **extremos** de la comunicación del sistema cliente ↔ server
- Entonces pueden centrarse en los **clientes** (estaciones de trabajo de los usuarios, por ejemplo) o en los **servidores** (obtienen acceso directo no autorizado a los recursos e información del sistema).

4.2 ATAQUES DE COMUNICACIÓN

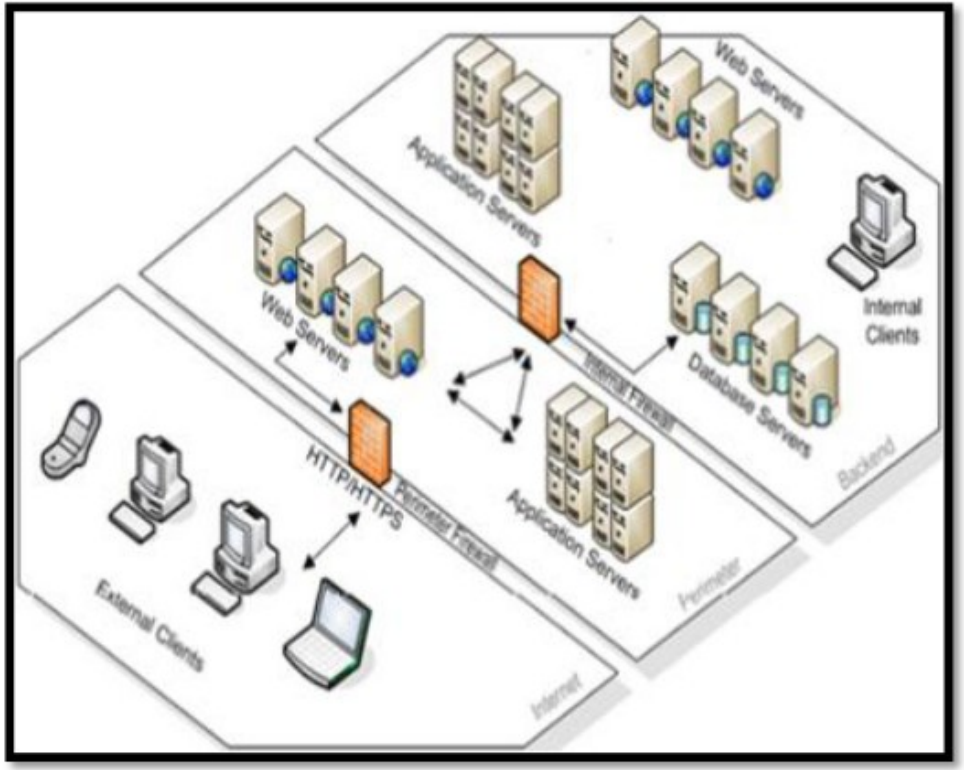
Ataques Web (Web Attacks)

KNOWHOW SECURITY
SABEMOS QUE HACER

¿Cómo funciona, cómo se rompe, cómo se ataca?

componentes de la arquitectura

- webapp son **aplicaciones que corren en un webserver** remoto
- **interactúan** usuarios de internet, servidores de app web, servidores de bases de datos, wan, dmz, lan...
- **compenentes claves**; hypertext transfer protocol (http), hypertext markup language (html), tcp port 80



4.2 ATAQUES DE COMUNICACIÓN
Ataques Web (Web Attacks)

KNOWHOW SECURITY
SABEMOS QUE HACER

- Ataques a más comunes a clientes → troyanos, phishing, ransonware, otros virus, ingenierías social,soulder surfing (¡si ha vuelto!), brute forcing, diccionario...

- ¿cuál piensa que es es eslabón más débil???→

4.2 ATAQUES DE COMUNICACIÓN
Ataques Web (Web Attacks)

KNOWHOW SECURITY
SABEMOS QUE HACER

- Ejemplos de ataques a Webservers: todos los definidos en el estandard de OWASP(https://owasp.org/www-project-top-ten/)

4.2 ATAQUES DE COMUNICACIÓN
Ataques Web (Web Attacks)

KNOWHOW SECURITY
SABEMOS QUE HACER

¡Mejor que ver es hacer! → Vamos a hackear websites en vivo, prepare el teclado y caliente las manos!!!

```
intitle:index.of claves.txt .

intitle:index.of /awstats/ .

intitle:index.of @pwcache .

intitle:index.of logs/ .

intitle:index of .bash_history
.

intitle:index.of /etc/ .
```

4.2 ATAQUES DE COMUNICACIÓN
Hacking directo

KNOWHOW SECURITY
SABEMOS QUE HACER

hacking directo, un hacker trabaja con herramientas digitales para obtener el acceso a la red.

Ataques comunes →

- Cracking
- Ataques de Fuerza Bruta
- Ataques de Ingeniería Social
- Ataques de Diccionario
- Ataques con malware (APT incluidas)
- Ataques OSint
- **Ataque de lateralización!**
- La lista es larga (+500)

4.2 ATAQUES DE COMUNICACIÓN
Hacking directo

KNOWHOW SECURITY
SABEMOS QUE HACER

hacking directo, un hacker trabaja con herramientas digitales para obtener el acceso a la red.

Ataques comunes →

- Cracking
- Ataques de Fuerza Bruta
- Ataques de Ingeniería Social
- Ataques de Diccionario
- Ataques con malware (APT incluidas)
- Ataques OSint
- **Ataque de lateralización!**
- La lista es larga (+500)

Algunos tips después de +20 años en ciberseguridad

- Algo hay que hacer no? → Entonces por que no hacerlo de **forma ordenada** a través del SGSI (tambien ISMS ó sistema de gestión de la seguridad de la información).
- Primer actividad → El primer trabajo de **CIBERSEGURIDAD** de la organización es crear un ISMS **adecuado a LA REALIDAD** de la organización
- Principales Estándares CONVERGENTES (FISICO/DIGITAL) → ISO/IEC 27001:2013, NIST → CIS Critical Security Controls V8, Guía de Ciberseguridad en la nube → CSA – Cloud Security Aliance

eof()

powered by Cvila

Cada una de las partes protegerá la información obtenida durante el desarrollo del curso de la misma manera en que protege su propia información confidencial, haciéndose responsable por cualquier daño/perjuicio que se pudiera ocasionar por el uso indebido de la información obtenida.

Todas las herramientas, técnicas y metodologías utilizadas tienen un fin UNICAMENTE EDUCATIVO.

Nuestros documentos entregables y papeles de trabajo serán de acceso exclusivo para los alumnos, quien podrá disponer para su uso de todos los entregables, que no incluyen metodología ni software utilizado.

PROHIBIDA SU REPRODUCCIÓN PARCIAL O TOTAL DEL MATERIAL

https://knowhowsec.com/ - christian.vila@knowhowsec.com