Ciberseguridad y Ciberdefensa

M.A. Manuel I. Quintero.
GISP, GCWN, GCUX, MCITP, PMP

Cyberseguridad

- ¿En que pensamos al hablar de cyberseguridad?
  - IDS
  - IPS
  - Antivirus
  - WIPS
  - IPSec
  - SSL
  - TLS
  - Estándares
  - Etc.

Ciberseguridad

If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

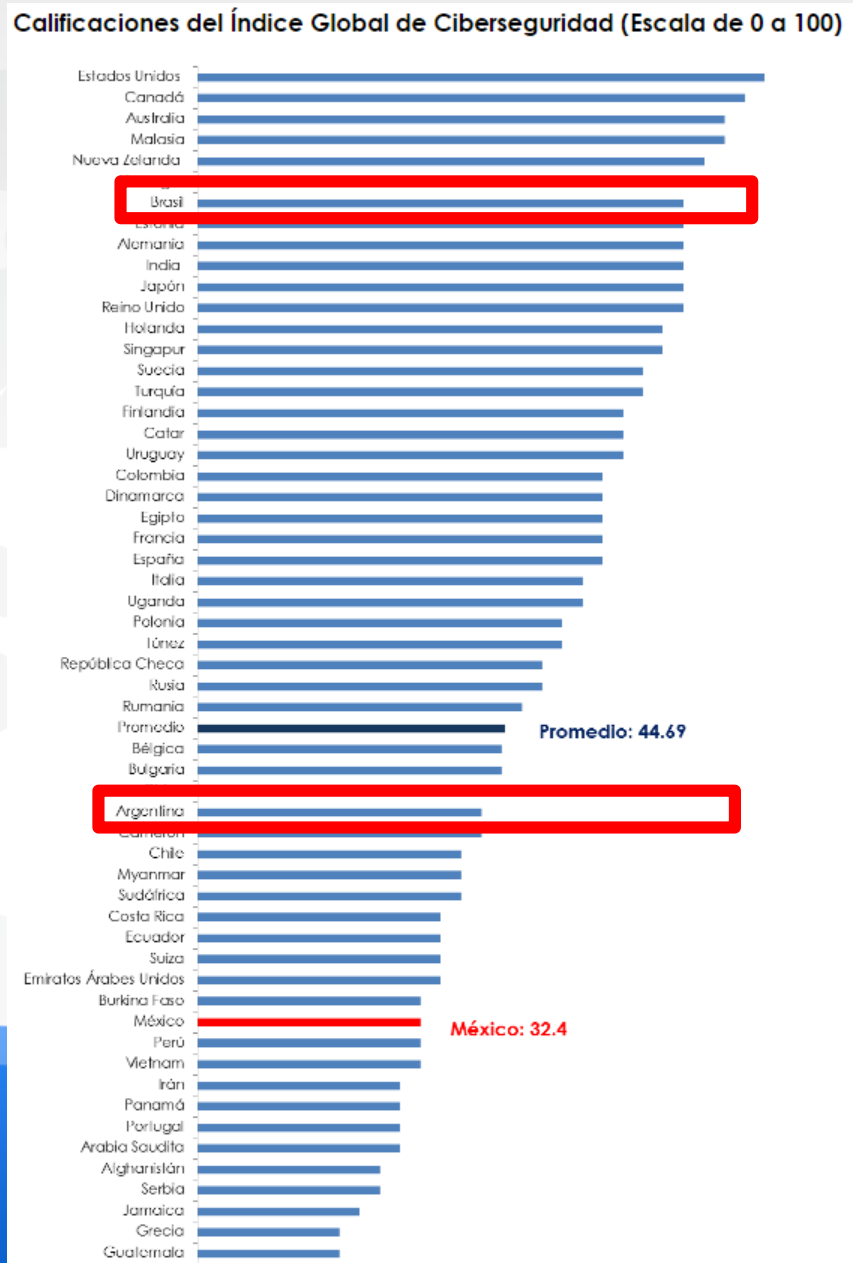
Bruce Schneier

Frases comunes al pensar en seguridad

- “Este appliance resolverá todos sus problemas de seguridad”.
- “Esta es la mejor solución en el mercado”.
- “Mi política de contraseñas es muy buena”.
- “No he tenido problemas de seguridad en los últimos *n* meses”

Tendencia local

- El informe del observatorio de Ciberseguridad de la OEA realiza análisis sobre el estado de cada país miembro.
  - México se encuentra muy por debajo de la media
  - Su mayor fortaleza se encuentra en la capacidad técnica
  - ¿Cómo interpretamos esto?



Como asumir la seguridad

- La seguridad es un proceso, no un resultado ni un producto.
  - Si alguien les preguntara: ¿Es segura su red?, ¿Cuál sería su respuesta?
  - No tenemos algo seguro, aseguramos nuestros activos.
- No existe ningún hardware/software que pueda prevenir cualquier tipo de ataque.
  - ¿Zero days?
  - APT
- Muchos desarrolladores de soluciones venden un *producto* como la solución *integral*. La única solución integral es asumir que nunca se está lo suficientemente seguros.

Lo verdaderamente seguro…

Cuando hablamos de seguridad, no se trata de si tendré un incidente o no, se trata sobre cuándo llegará ese incidente…

y si lo detectaré y podré responder a él.

Cyberseguridad

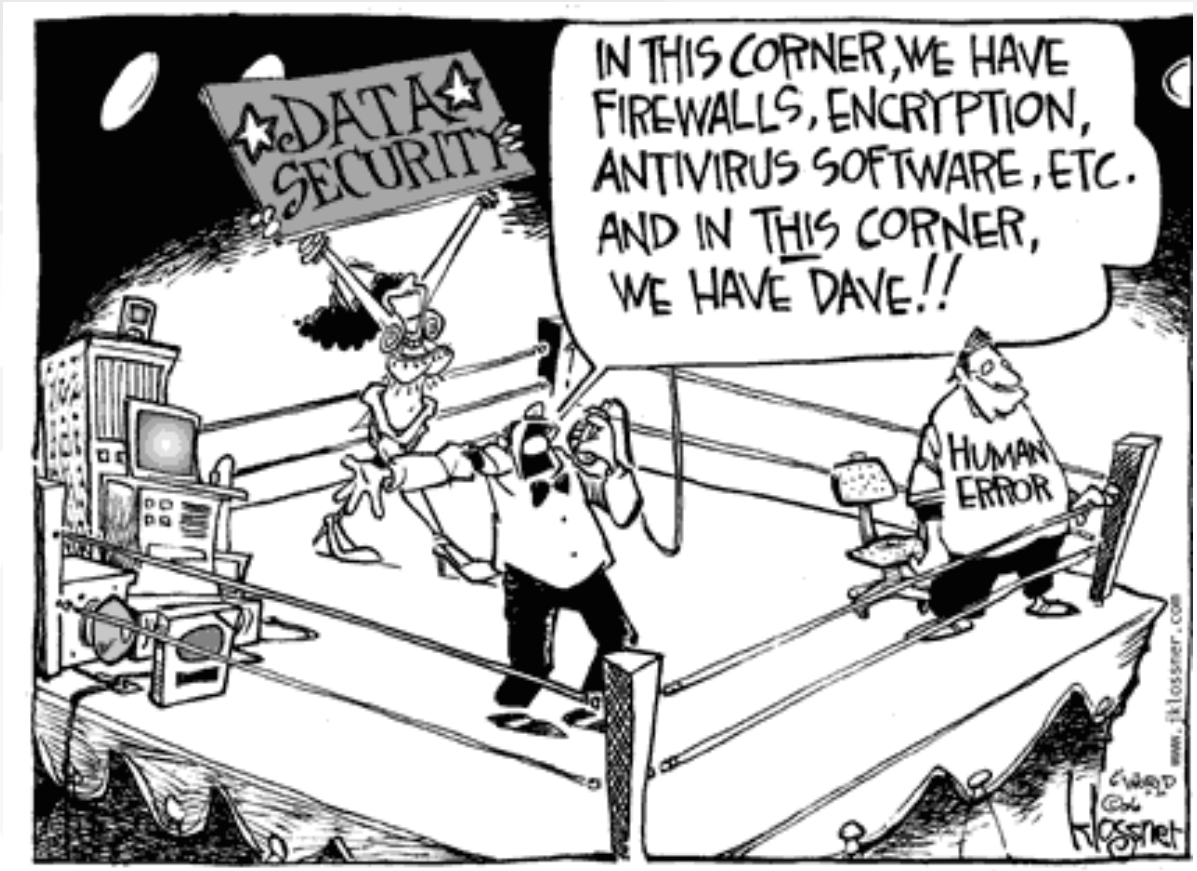
- Esto agrega dos elementos más a la prevención y la seguridad ofensiva.
  - Monitoreo
    - ¿Sabemos todo lo que pasa en la red/usuarios/sistemas?
  - Respuesta
    - ¿Cuál es el plan cuando se presente un incidente?

Monitoreo

- ¿Es sólo el registro de los logs?
- ¿Es sólo esperar respuestas de un IDS/IPS/UTM/etc.?
- ¿Qué nos interesa monitorear?
  - ¿Qué se está haciendo con sus logs?
    - Correlación de eventos
  - ¿Se están monitoreando cambios en los equipos/servicios/sistemas?
    - ¿Alguien verifica estas alertas?
  - Aún más importante…

Monitoreo

- Como regularmente se sabe, la mayor fuente de problemas son los usuarios (22%)*.
  - Los usuarios siempre encuentran como *sobrepasar* los controles técnicos



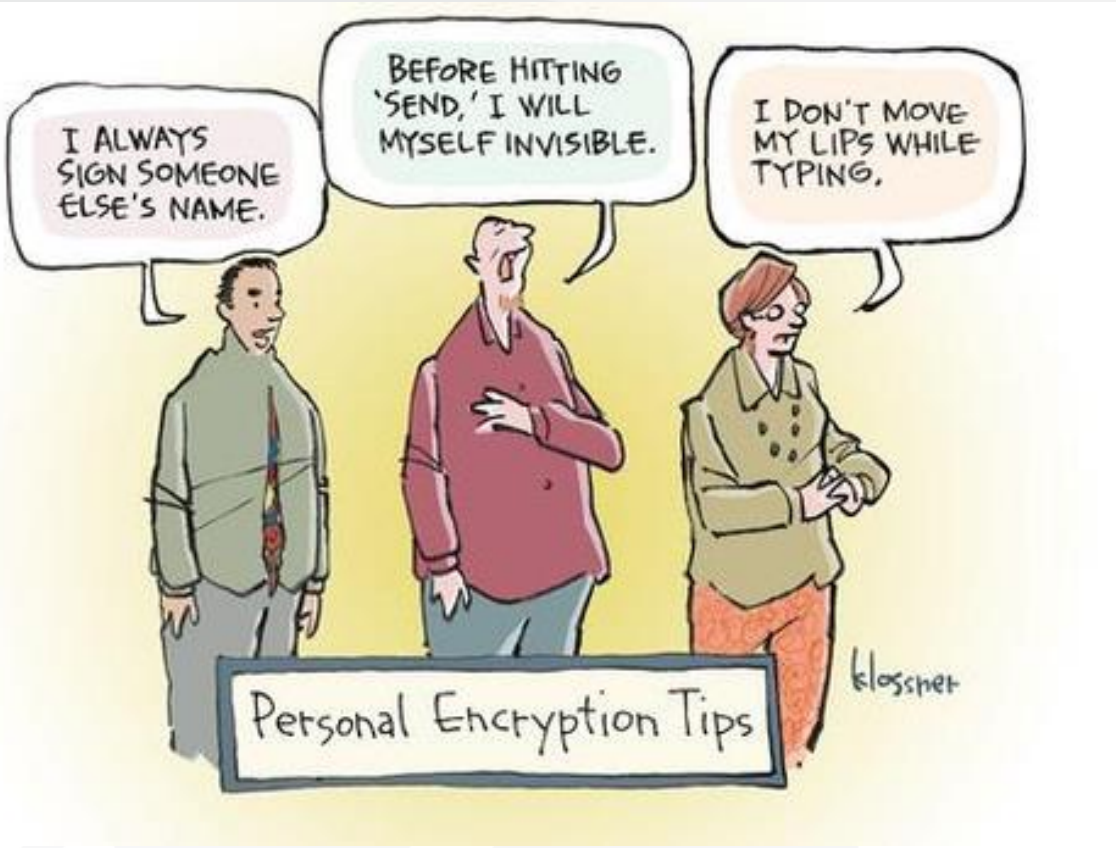
Monitoreo

- ¿Cómo prevenimos que los usuarios sean una brecha?
  - La respuesta común será:
    - Capacitación

http://www.darkreading.com/perimeter/cartoon-end-user-security-prayer/d/d-id/1316122

Monitoreo

- Pero…
- ¿Verificamos como lo hacen en el día a día?
- Es importante hacer revisiones de lo que los usuario saben, pero sobre todo, de cómo lo aplican.



http://www.darkreading.com/application-security/cartoon-e2c$y5tion/d/d-id/1204582

Problemas con la capacitación

- Security Awareness Report 2016, menciona que los retos más comunes son:
  - Recursos (19%)
  - Adopción (19%)
  - …
  - Métricas (0.05%) ← Es como asumir que el alumno aprende, y nunca nos preocupamos por saber si realmente lo hace.

Monitoreo

- 22%* de los problemas de seguridad vienen de los usuarios internos, pero…
- Otro 22%* se atribuyen a *partners*.
  - ¿Tienen algún tipo de control o monitoreo con ellos?
  - La tendencia más común, es confiar en que ellos hacen su parte.
  - ¿Cómo aseguran sus activos en la nube?

The Global State of Information Security Survey 2016

http://www.darkreading.com/cloud/cartoon-cloud-conundrum/d/d-id/1279063

Respuesta a incidentes

- Por ejemplo
  - Sabemos que el Ransomware es uno de los mayores problemas en las organizaciones:

El ransomware Crysis emplea la fuerza bruta para infectar equipos

Detalles
Publicado: 21 Septiembre 2016

Investigadores de seguridad afirman haber descubierto una nueva campaña de distribución del ransomware Crysis, que lleva a cabo ataques de fuerza bruta a RDP (Remote Desktop Protocol) para comprometer equipos.

Los ciberdelincuentes están lanzando ataques de fuerza bruta en un intento de adivinar la contraseña de administrador del equipo expuesto. Si lo logran, instalan el ransomware Crysis en el equipo, además de extenderse a otros dispositivos de la misma red, como impresoras o routers, que luego propagan la amenaza a otros usuarios.

Con anterioridad otros ransomware también hicieron uso de esta técnica, como por ejemplo Apocalypse, Bucbi, DMA Locker o Smrss32, entre otros.

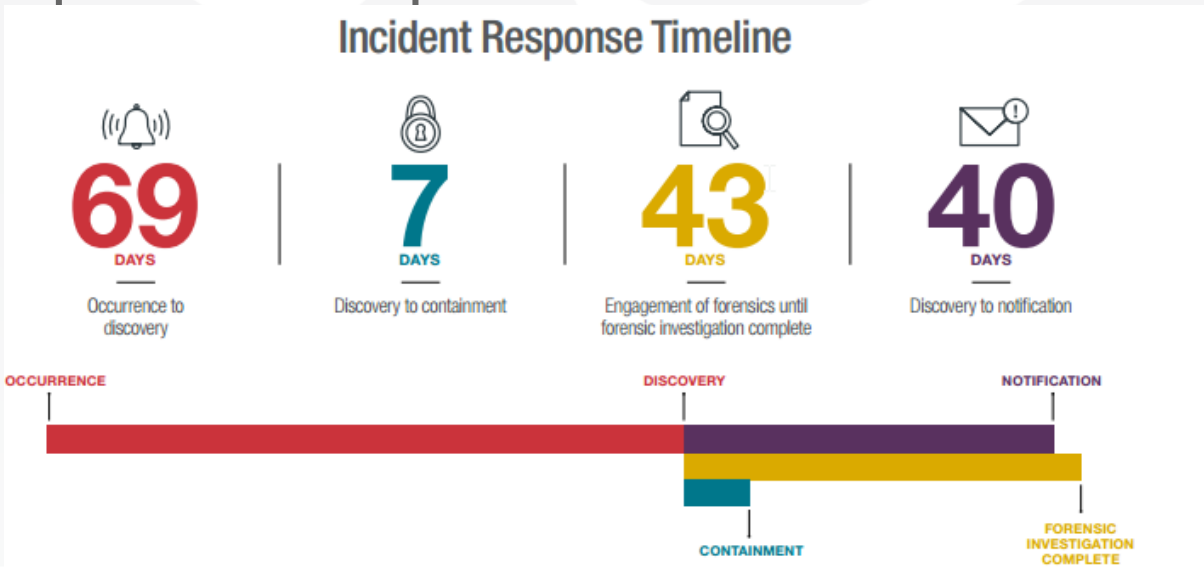
Debido a que Crysis utiliza una fuerte combinación de algoritmos de cifrado AES y RSA, no se conoce aún ninguna manera de desbloquear los archivos cifrados por éste ransomware (también conocido como Virus-Encoder).

y

usuarios lo es?

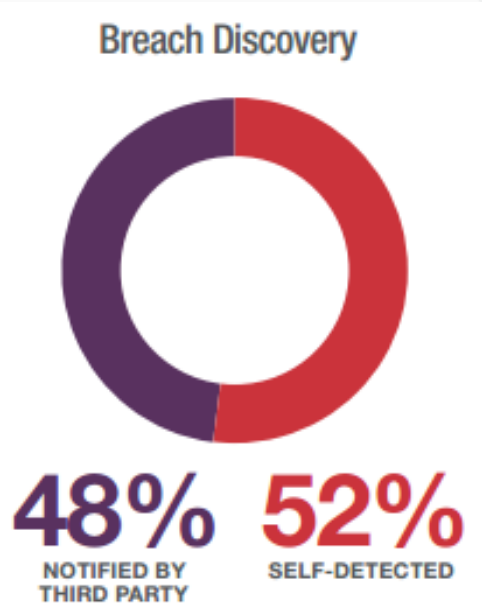
Respuesta a incidentes

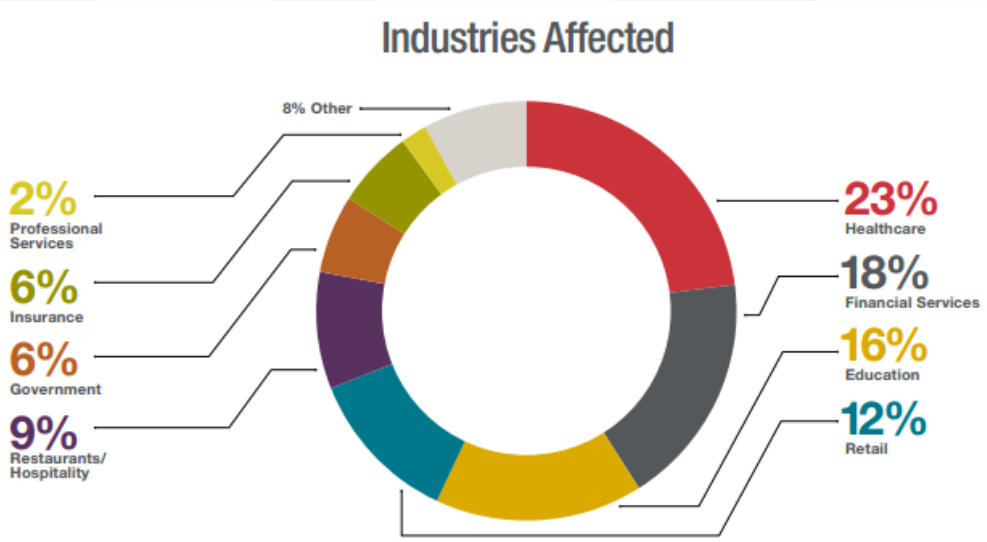
- "Tengo ***n*** meses sin incidentes…"
  - En promedio pasan 112 días antes de que pueda completarse un proceso.



2016 Data Security Incident Response Report

Respuesta a incidentes





Respuesta a incidentes

- ¿Cómo saber si tenemos elementos para responder?
  - Capacidades en seguridad preventiva y de detección.
  - Generación de información sobre amenazas en el entorno.
  - Capacitación y entrenamiento a usuarios.
  - Evaluación proactiva de seguridad, identificando activos críticos implementando **medidas de detección razonables**.
  - Evaluar y supervisar a otros actores.
  - Desarrollar, actualizar y **practicar** respuesta a incidentes.
  - Entender las tendencias.
  - Evaluar la adquisición de un seguro de responsabilidad cibernética.

Respuesta a incidentes

- No es necesario redescubrir el hilo negro
  - ISO/IEC 27035:2011 Information technology
  - GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA (proyecto AMPARO)

Conclusiones

- La seg… solo un proces…
- Si bien… técnicos, existen… organi… oceso.
- NUNC…
- **Y recuerden que hacer seguridad, es no tener una zona de confort.**

UNAM-CERT

M.A. Manuel I. Quintero

manuel.quintero@cert.unam.mx

Coordinación de Seguridad de la Información

DGTIC, UNAM

DGTIC

DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN