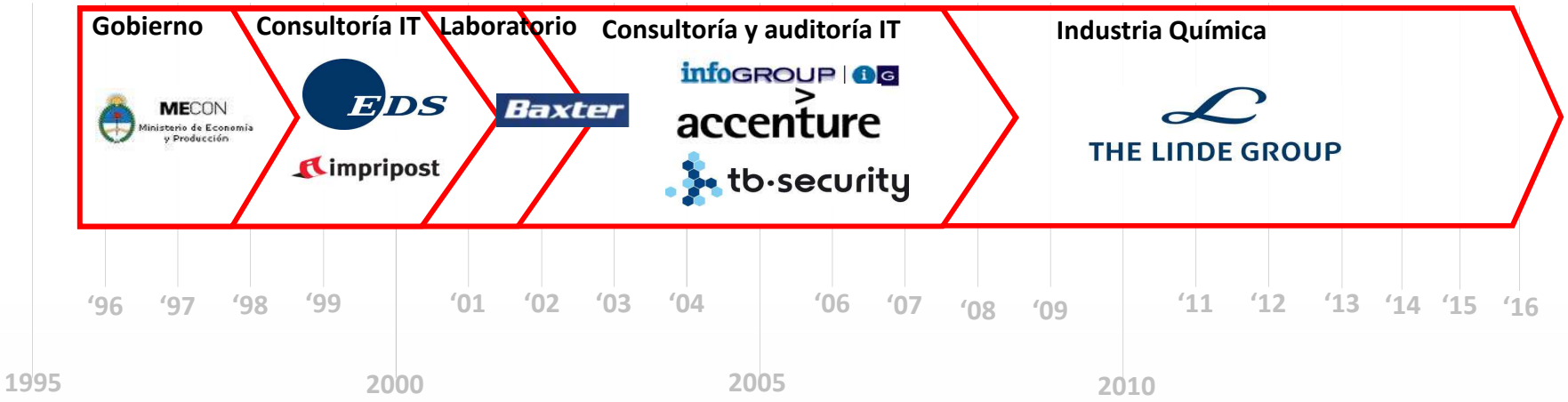
¿Cuáles son los peligros a los que se enfrenta su sistema informático?

Ramiro Cid
CISM, CGEIT, ISO 27001 LA, ISO 22301 LA, ITIL(f)
Region Europe South IT Security Officer & IT Manager - Linde

Bio y experiencia laboral

Ramiro Cid | ramiro@ramirocid.com | @ramirocid

- ✓ Region Europe South IT Security Officer & IT Manager en Linde
- ✓ Miembro del Linde EMEA Regional Security Officers Team en Linde
- ✓ Postgrado en Dirección de Empresas (UPF Barcelona School of Management)
- ✓ Licenciado en Sistemas de Información (Universidad de Buenos Aires)
- ✓ Certificaciones: CISM®, CGEIT®, ISO 27001:2013 LA , ISO 22301:2012 LA, ITIL®(f)
- ✓ Profesional con casi 20 años de trayectoria en la industria de TI en diferentes sectores: Industria química, Laboratorio, Banca, Gobierno, Consultoría de sistemas, etc., en diferentes empresas trabajando en España, Argentina y Andorra.



Indice

1. Evolución de las amenazas	Slide 4
2. Algunos ataques producidos durante 2016	Slide 7
3. Tipología de las amenazas más comunes	Slide 8
4. Orígenes de los ataques a nuestra red	Slide 10
5. ¿Dónde se producen los ataques?	Slide 11
6. Trazabilidad del ataque	Slide 12
7. ¿Qué está sucediendo en el mercado de la seguridad?	Slide 13
8. Soluciones ofrecidas en el mercado	Slide 14
9. Posibles soluciones (técnicas)	Slide 17
10. Posibles soluciones (no técnicas)	Slide 19
11. ¿Cómo comprobar si sus datos de cuenta alguna vez se han filtrado?	Slide 20
12. Acercamiento al término resiliencia	Slide 22
13. ¿Cómo debemos entender actualmente la seguridad?	Slide 23

1. Evolución de las amenazas

Cada vez es mayor el reto que supone proteger nuestros activos TI frente a las crecientes amenazas y ataques.

Una vez que alguna aplicación maliciosa entra en nuestras redes, puede desplazarse rápidamente con el tráfico y causar estragos en toda la red.

Estos ataques pueden ser **devastadores.**

¿Cuáles son los peligros a los que se enfrenta su sistema informático?

1. Evolución de las amenazas

1. Evolución de las amenazas

2014:

• El coste **medio** total de una vulneración de datos ascendió para las empresas estadounidenses a **U$S 5,85 millones** *(*)*

• Se confirmaron **80.000 incidencias de seguridad** en todo el mundo *(*)*

• Hubo más de **2.000 casos confirmados** en los que se pusieron en **riesgo datos confidenciales** *(**)*

2015:

• El uso del cifrado como herramienta para secuestrar los datos más importantes de las empresas y los usuarios individuales aumentó en un 35 % *(***)*

(*) Fuente: "2014 Cost of Data Breach Study" del Ponemon Institute.
(**) Fuente: "2015 Data Breach Investigation Report" de Verizon.
(***) Fuente: "ISTR" de 2015 de Symantec.

2. Algunos ataques producidos durante 2016

Yahoo: *>500 millones de contraseñas comprometidas (*)*

MySpace: *427 millones de contraseñas comprometidas*

Gmail: *272 millones de contraseñas comprometidas*

LinkedIn: *164 millones de contraseñas comprometidas*

Dropbox: *68 millones de correos de acceso y contraseñas encriptadas aparecieron a la venta en Internet (**)*

Twitter: *33 millones de contraseñas estaban a la venta.*

TOTAL: > 1.605.000.000 contraseñas comprometidas !!

(sería el ~20% de la población mundial si cada una de las cuentas fuera de una persona distinta)

(*) Publicado en agosto 2016 pero los datos provienen de una brecha de seguridad producida en 2014

(**) Publicado en agosto 2016 pero los datos provienen de una violación que tuvo lugar en 2012, pero en ese entonces se reveló que únicamente las direcciones de correo electrónico habían sido filtradas, no las contraseñas.

3. Tipología de las amenazas más comunes

- **Data Breach/Data leak:** Múltiples formas (automáticas o no)
- **DDoS:** Denial-of-service attack. Ataque de denegación de servicio
- **Programa malicioso:** Virus, troyano, ransomware, etc.
- **APT:** Amenaza persistente avanzada. Es una amenaza sofisticada y muchas veces se trata de un exploit 'Zero-day'. conjunto de procesos informáticos sigilosos y continuos, dirigidos a penetrar la seguridad informática de una entidad específica.
- **Puertas traseras:** Backdoors: Una puerta trasera en un sistema informático, un sistema de cifrado o un algoritmo, es un método para evitar la autenticación normal, garantizar el acceso remoto, obteniendo acceso mientras se pasa desapercibido.
- **Ataques de "Man-in-the-middle":** Con capacidad de leer, insertar y modificar a voluntad los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado.
- **Ingeniería social:** Fraude bancario, "Fraude del CEO", etc.

3. Tipología de las amenazas más comunes

- **Exploits:** Un exploit es un elemento de software, fragmento de datos, o secuencia de comandos que se aprovechan de un "error" o "fallo" de la aplicación con el fin de provocar un comportamiento no deseado o imprevisto.

- **Ataques de acceso directo:** Alguien que ha tenido acceso a un ordenador instalando diferentes tipos de dispositivos para comprometer la seguridad, incluyendo las modificaciones del sistema operativo de software, gusanos, keyloggers, y dispositivos de escucha encubiertas. El atacante también puede descargar fácilmente grandes cantidades de datos.

- **Ataques indirectos:** Es un ataque lanzado por un equipo de terceros mediante el uso de un ordenador de otra persona para lanzar un ataque, se hace mucho más difícil de localizar al atacante real.

- **Espionaje:** Es el acto de escuchar a escondidas una conversación privada, típicamente entre hosts en una red (ej. “Man-in-the-middle”).

4. Orígenes de los ataques a nuestra red

- **Aplicaciones de cloud corporativo**: Interfaces y API poco seguros, fuga de información, secuestro de sesión*.

- **Aplicaciones de cloud no corporativo** (Dropbox, Google Drive, etc).

- **Amenazas provenientes del IoT**: Cualquier dispositivo susceptible de ser conectado a nuestra red corporativa posee un riesgo inherente por vulnerabilidades en su OS (cámaras IP, televisores, dispositivos wearables, etc).

- **Móviles o tablets** corporativos o no (BYOD o no) infectados (por tener jailbreak, aplicaciones maliciosas, etc.) que se conecten a nuestra Wifi interna si esta está mal segmentada (o no posee ninguna segmentación).

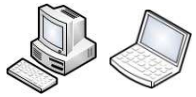
- **Pendrives infectados**

- **Webs** infectadas/comprometidas, cookies, códigos incrustados en webs legítimas.

Fuente: "Riesgos y amenazas en Cloud Computing" INTECO-CERT

5. ¿Dónde se producen los ataques?

¿Dónde están nuestros endpoints?

- **PC's y portátiles** 
- **Smartphones y tablets**
- **Discos externos, pendrives**
- **Cabinas de discos, NAS**
- **Servidores**
- **IoT devices**

- **Personas**

6. Trazabilidad del ataque

Desde el exterior: Los ataques explotan los puntos débiles inherentes en las estrategias de seguridad de redes centradas en el perímetro (FW, IPS, etc.) para infiltrarse en el corazón de los data center de las empresas.

Después de esquivar con éxito las defensas del perímetro del centro de datos, un ataque puede desplazarse lateralmente en el data center, saltando de una carga de trabajo a otra, con pocos controles, si es que hay alguno, que impidan su propagación.

Desde el interior: Con un pendrive o disco externo infectado, con un dispositivo móvil (Smartphone, Tablet) infectado conectado a la red, etc.

7. ¿Qué está sucediendo en el mercado de la seguridad?

Convergencia de muchas marcas para ofrecer una “solución única”:

a) Fabricantes provenientes de los entornos endpoints (Symantec, McAfee, etc.)

b) Provenientes del perimetral (Checkpoint, Palo Alto*(*)*, etc.)

c) Fabricantes de soluciones no relacionadas con seguridad (Wmware*(**)*, otros)

Actualmente la solución no pasa únicamente por securizar el viejo perímetro (FW, IPS, VPN en los portátiles, etc.) si no también por la monitorización constante de la red, herramientas para controlar el data leak, monitorización de red, etc.

(*) Fuente: ‘Are you Secure against threasts with cybersecurity?’. Palo Alto Networks
(**) Fuente: ‘Qué puede hacer la microsegmentación por su centro de datos?’ VMWare

8. Soluciones ofrecidas en el mercado

Algunas soluciones encontradas en el mercado con la actual hiperconvergencia de fabricantes para ofrecernos una "solución única":

- **Symantec:** Symantec Embedded Security: Plataforma de securización de IoT para entornos críticos protegiendo dispositivos con sistemas operativos embebidos.

- **McAfee:** Protección en la Nube, neutralización de amenazas, protección de datos, optimización de las operaciones de seguridad.

8. Soluciones ofrecidas en el mercado

Algunas soluciones encontradas en el mercado con la actual hiperconvergencia de fabricantes para ofrecernos una "solución única":

- **VMWare: "**Microsegmentación", reduce significativamente la propagación lateral de las amenazas dentro del CPD VMware NSX, es la plataforma de virtualización de redes para CPD definido por software reproduciendo el entorno de red. Mediante NSX se proporciona un conjunto completo de elementos y servicios de red lógicos entre los que se incluyen switchs lógicos, enrutamiento, protección de firewall, balanceo de carga, red privada virtual (VPN, Virtual Private Network), calidad de servicio (QoS, Quality of Service) y monitoreo.

- **Checkpoint:** FW + endpoints + DLP prevention + DDoS prevention + SandBlast Zero-Day Protection (una sandbox) + Mobile Threat prevension + Threat Prevention Appliances & Software

8. Soluciones ofrecidas en el mercado

- **BSI:** Entropy™, Software que ayuda a obtener rendimiento de los sistemas de negocio y de gestión. Proporciona una solución de software y gestión para ayudarle a gestionar de forma proactiva los riesgos, la sostenibilidad y el rendimiento, reduciendo el coste y el esfuerzo que se dedica a estas actividades, al tiempo que mejora la visibilidad global dentro de su organización.

- Muchas soluciones integrales de gestión de nuestro SGSI, SGCN o SGPD pudiendo combinar controles provenientes de distintas normativas como COBIT, ISO 27001, ISO 22301 como legislación: Protección de Datos, etc.

  En el año 2007 he realizando un estudio de mercado donde se encontraron 29 soluciones en el mercado (Babel Enterprise, Modulo Risk Manager, Proteus Enterprise, Meycor, y un largo etc.). Actualmente muchas más presentes.

9. Posibles soluciones (técnicas)

- Soft token/hard token: Para accesos desde fuera de nuestra red corporativa vía VPN
- FW + IPS en la red interna (puede ser implementado en el propio FW)
- Segmentación de red (subneting, definiendo distintas VLANs para distintos usos y con un firewall que gestione los accesos): Ejemplo: botnets para nuestras visitas, proveedores, etc.
- Antivirus endpoints + servers de firma + consola web
- Ante ataque de DDoS: Honey pots, etc.
- Criptografía
- Certificados de autentificación a la wifi instalados en los portátiles
- Reportes de IT Compliance (mensuales, etc.): Antivirus, fixes, encryptación

9. Posibles soluciones (técnicas)

- Monitorización de equipos de red (NAGIOS, etc.)
- Monitorización del tráfico de la red: Sniffer
- Correlación de eventos, monitorización y gestión de logs y alertas
- Soluciones combinadas (incidencias de seguridad y eventos): SIEM
- Monitorización de permisos en los shares departamentales
- Monitorización de DLP (Data Loss Prevension): Distintas soluciones de distintos fabricantes para prevenir el Data Leak

10. Posibles soluciones (no técnicas)

- Formación interna/awareness: Los usuarios deben estar al corriente de las amenazas actuales y como proceder ante ellas (plan de formación + newsletters + simulacros de phishing, etc.)
- Sentido común
- Buenas prácticas en seguridad TI (políticas internas, etc.)
- Normas relacionadas: COBIT 5, ISO/IEC 27001:2013, etc.
- División de funciones: Diferentes personas para gestión de TI y para seguridad TI (no siempre posible por falta de recursos o cultura organizacional)
- Aplicación de metodologías de GRC*(*)*, herramientas y facilitadores en las diferentes industrias como Archer, BWise, Metric Stream, BPS, Chase Cooper, Paisley

(*) GRC significa: Governance, Risk & Compliance

11. ¿Cómo comprobar si sus datos de cuenta alguna vez se han filtrado?

¿Dónde?

-> Una respuesta fácil es HaveIbeenPwned.com un servicio gratuito que debe ser considerado un **"deber-tener (must)** como parte de su higiene online, para comprobar si sus cuentas están a salvo.

¿Cómo?

La página web recoge datos filtrados y tiene información sobre más de mil millones de cuentas filtradas desde diferentes sitios web. Para averiguar si sus datos de cuenta se han filtrado, haga clic en el enlace mencionado, escriba su dirección de correo electrónico y pulse intro.

11. ¿Cómo comprobar si sus datos de cuenta alguna vez se han filtrado?

Sí su dirección de correo electrónico aparece en sus registros, debe cambiar su contraseña en las cuentas afectadas inmediatamente. El seleccionar una contraseña segura y teniendo una contraseña única para cada cuenta es, por supuesto, un requisito previo esencial

También puede suscribirse para recibir notificaciones en caso de que sus datos de cuenta se filtraron en el futuro o puede probar servicios similares en leakedsource.com o hacked-db.com

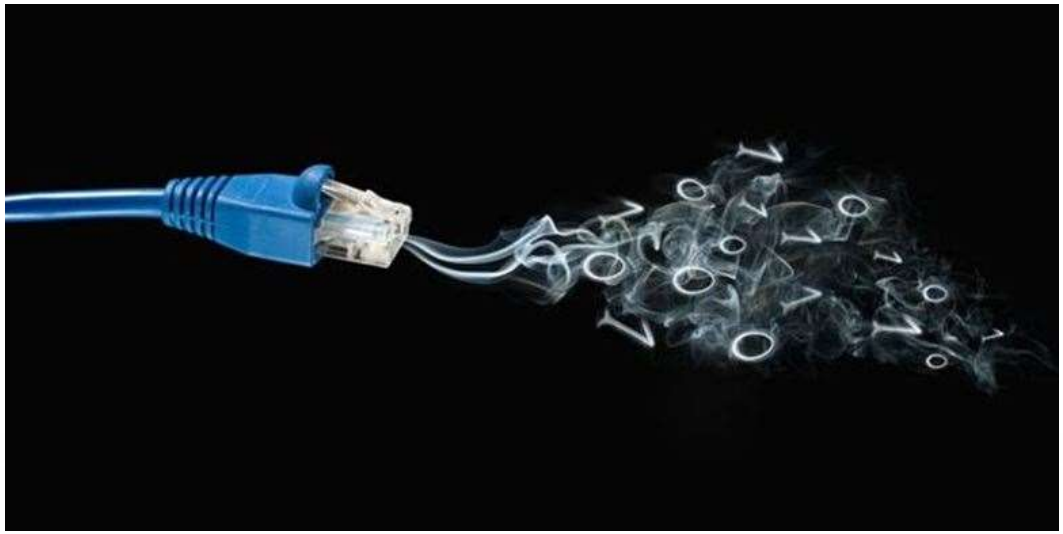


Imagen de cortesía de SRI Data Leak

12. Acercamiento al término resiliencia

Desde la física: Se llama resiliencia de un material a la energía de deformación (por unidad de volumen) que puede ser recuperada de un cuerpo deformado cuando cesa el esfuerzo que causa la deformación. La resiliencia es igual al trabajo externo realizado para deformar un material hasta su límite elástico.

Desde la psicología: Es la capacidad para afrontar la adversidad y lograr adaptarse bien ante las tragedias, los traumas, las amenazas o el estrés severo.

Las personas resilientes poseen 3 características principales:

a) saben aceptar la realidad tal y como es

b) tienen una profunda creencia en que la vida tiene sentido

c) tienen una inquebrantable capacidad para mejorar.

13. ¿Cómo debemos entender actualmente la seguridad?

Un estado de **"seguridad"** es un concepto ideal, conceptual que está conformado por el uso de los tres procesos:

1) La prevención de amenazas
2) La detección
3) La respuesta

La clave actualmente está en potenciar la última.

¿Dónde está el **nuevo perímetro**? -> Posiblemente en los **datos.**

13. ¿Cómo debemos entender actualmente la seguridad?

¿Cuál la nueva **filosofía** de seguridad?

Pasamos de repeler ataques a tener **resiliencia organizacional** (*), entendiendo que **NO** es posible detener todas las amenazas, por lo que la organización tiene poder sobreponerse a los impactos **para poder sobrevivir.**

(*) Capacidad de una organización para anticipar, prepararse y responder y adaptarse al cambio incremental y las interrupciones repentinas con el fin de sobrevivir y prosperar.

¿Dudas? ¿preguntas?

¡ Muchas gracias !

Ramiro Cid

CISM, CGEIT, ISO 27001 LA, ISO 22301 LA, ITIL

ramiro@ramirocid.com

http://ramirocid.com

@ramirocid

http://www.linkedin.com/in/ramirocid

http://es.slideshare.net/ramirocid

http://www.youtube.com/user/cidramiro