



OWASP

Open Web Application
Security Project

Panorama de la ciberseguridad

OWASP Latam Tour 2017

Jorge Córdova Pelayo

Abril 2017

Agenda

- Introducción
- Antecedentes
- Eventos relevantes
- Principales amenazas
- ¿Hacia dónde va la ciberseguridad?
- ¿Qué nos espera?
- Siguiendo pasos



Introducción



OWASP
Open Web Application
Security Project

Introducción

Eso nunca ha pasado, ni
pasará en la empresa

Nosotros tenemos la
tecnología para detener
cualquier ataque

Nuestra organización no
está en la mira de los ciber
delincuentes

Lo real es que todas
organizaciones y personas
están expuestas a un ciber
ataque



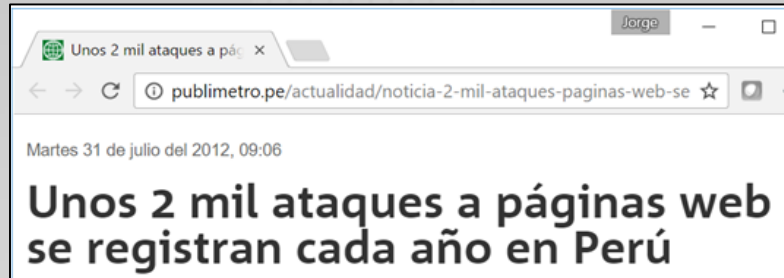
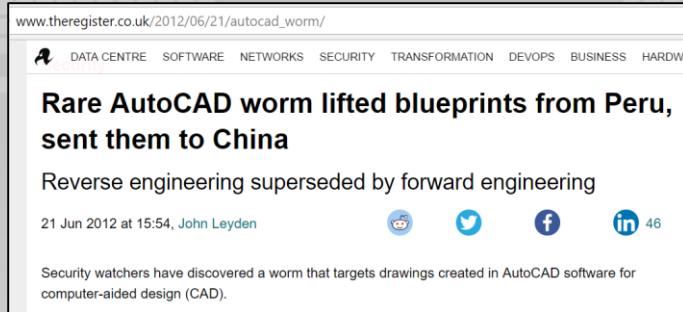
Antecedentes



OWASP
Open Web Application
Security Project

Antecedentes

Incidentes de seguridad que vemos en internet.



Antecedentes: lo que no vemos en las noticias

- **Caso 1: Campañas de phishing a entidades financieras**
 - Identifican vulnerabilidades en los procesos y sistemas de información.
 - Explotan las vulnerabilidades. El fraude se materializa.
 - Buscan otras organizaciones con las mismas vulnerabilidades.
 - El ciclo se repite.
- **Consecuencias**
 - Impacta directamente en el cliente de la entidad.
 - Afecta la reputación y cumplimiento normativo.
 - Costos por el fraude: multas, investigación, reposición, pérdida del cliente, entre otros.



Antecedentes: lo que no vemos en las noticias

- **Caso 2: Fuga de datos**

- Exfiltración de datos sensibles por empleados, terceros/proveedores.
- Acceso a carpetas compartidas sin restricciones, acceso a reportes de los sistemas, USB perdidas/robadas, entre otros.
- Ausencia de controles para prevenir y detectar: DLP, políticas, revisión de antecedentes de empleados/proveedores, ausencia de controles de acceso, entre otros.

- **Consecuencias**

- Afecta la reputación e imagen
- Costos por el fraude: pérdida de oportunidades, la competencia sacó el producto antes, entre otros.



Antecedentes: lo que no vemos en las noticias

- **Caso 3: Clonación de tarjetas**
 - Comercios con controles básicos de seguridad.
 - La tarjeta con chip es posible clonarla. Aún mantiene la banda magnética.
 - Medios inseguros de transmisión, almacenamiento y procesamiento: computadoras sin parches, sin antivirus, aplicación de pago legacy, tramas enviadas sin cifrado, almacenamiento de datos de tarjetas, entre otros.
 - Malware dedicado a robar datos de tarjetas (memory scraping).
- **Consecuencias**
 - Clonación de la tarjeta y pérdida de dinero para el cliente y entidad emisora.
 - Disponibilidad. El cliente no podrá utilizar la tarjeta cuando lo requiera.
 - Costos por el fraude: multas, investigación, reposición, pérdida del cliente, entre otros.



Antecedentes: lo que no vemos en las noticias

- **Caso 4: Espionaje avanzado (APT – Advanced Persistent Threat)**
 - Ciberdelincuentes (casi profesionales – crime as a service).
 - Motivos: dinero, información confidencial/sensible, generar pérdidas a las empresas.
 - Diferentes modos de operar: spear phishing, ransomware, ingeniería social, explotación de vulnerabilidades 0-day, troyanos, vulnerabilidades en aplicaciones web/móviles.
 - Ocultan su identidad, se dedican a la investigación, utilizan bitcoins, deep web o foros underground, entre otros.
- **Consecuencias**
 - Fuga de datos.
 - Costos asociados: investigación, pérdida de información, pérdida de clientes, pérdida de oportunidades, entre otros.



Antecedentes

- Todo lo anteriormente mencionado sucede en Perú.
- En los medios se destacan algunos debido a su contenido de interés, sin embargo, la gran mayoría nunca salen a la luz.
- Si las consecuencias son similares, ¿por qué no se toman las debidas acciones?

“El pueblo que no conoce su historia,
está condenado a repetirla”



Eventos relevantes



OWASP
Open Web Application
Security Project

Eventos relevantes

Millions of Americans Use Medical Devices That May Be Vulnerable to Hacking



HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT



COMPUTERWORLD

NEWS ANALYSIS

Researchers hack a pacemaker, kill a man(nequin)



Credit: C&E Healthcare

Researchers decided you don't need to be a pen tester to wirelessly hack a pacemaker, to successfully launch brute force and denial of service attacks that can kill 15tan simulated humans.

Pasamos de un mundo de ciencia ficción, a ver que todo lo que nos rodea puede ser vulnerado.



WIRED

IS IT POSSIBLE FOR PASSENGERS TO HACK COMMERCIAL AIRCRAFT?



OWASP
Open Web Application
Security Project

Eventos relevantes

- Robo de datos personales por contener información muy valiosa.
- Medios de comunicación, debido al alcance de público.



updated 5th Jan 2017)



latest

2016

2015

Fuente:
<http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

Principales amenazas



OWASP
Open Web Application
Security Project

Principales amenazas

- Aumento de **ciberataques** entre naciones.
- Crecimiento de ataques **ransomware**.
- Incremento de ataques **DDoS**.
- Aumento de **ataques a Internet de las cosas (IoT)**.
- Wearables, carros, software con **fallas**.
- Ingeniería social aprovechándose de los **errores humanos**.

Fuentes:

- <http://www.zdnet.com/article/the-top-security-threats-of-2016/>
- <http://www.techrepublic.com/article/experts-predict-2017s-biggest-cybersecurity-threats/>
- <http://cybersecurityventures.com/cybercrime-infographic/>

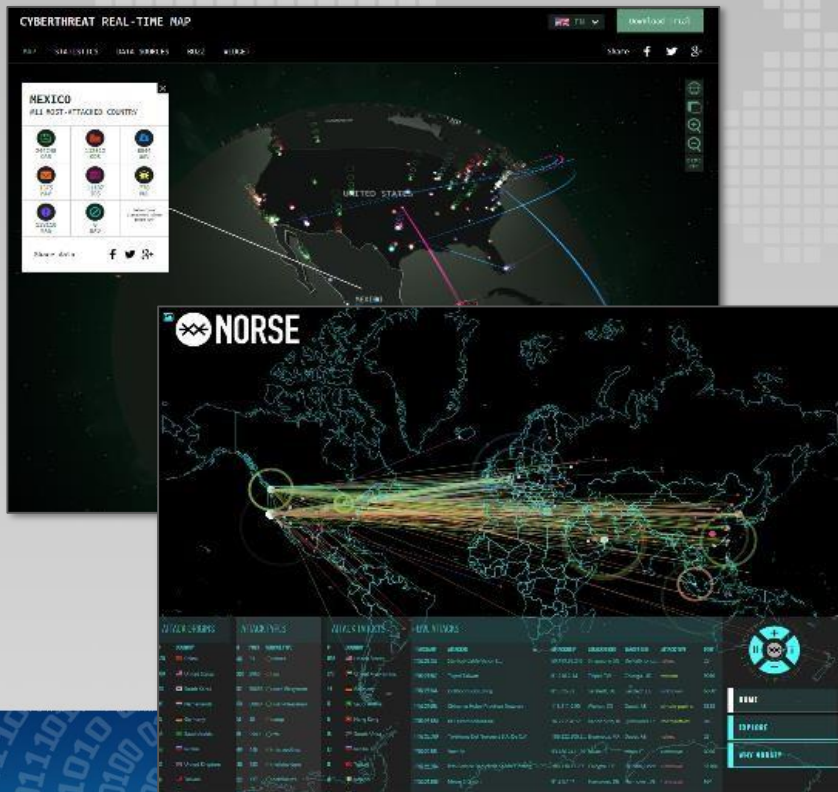


¿Hacia dónde va la ciberseguridad?



OWASP
Open Web Application
Security Project

¿Hacia dónde va la ciberseguridad?

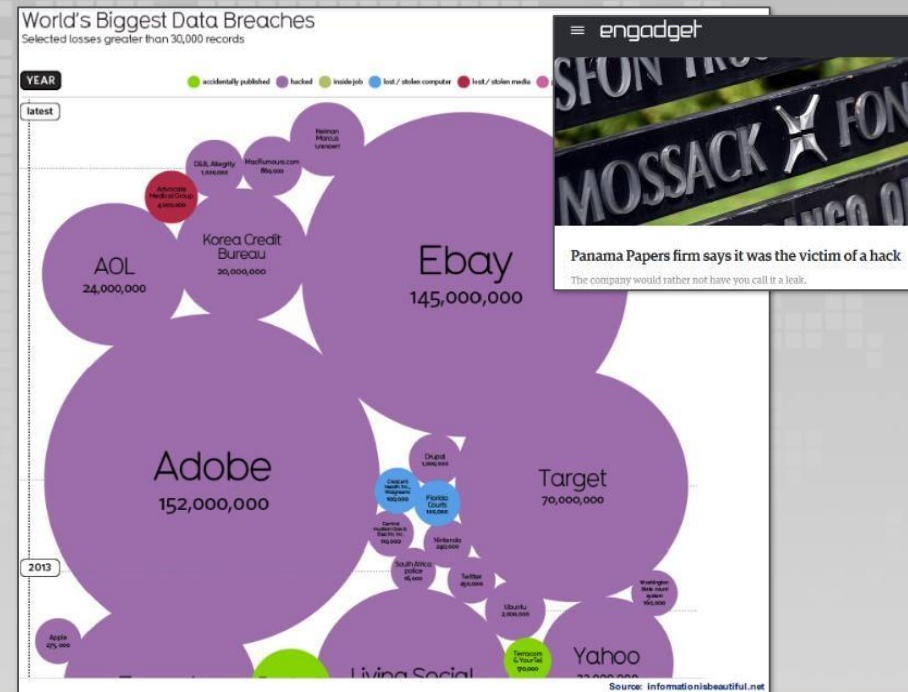


Los ciber ataques van en aumento en el mundo con distintos objetivos:

- Denegación / Interrupción de servicios
- Robo de propiedad intelectual
- Robo de datos de usuario
- Robo de identidad
- Secuestro de bases de datos
- Ciber guerra / terrorismo

¿Hacia dónde va la ciberseguridad?

- La información se ha convertido en el principal objetivo de los atacantes.
- Ninguna organización está exenta a riesgos cibernéticos. El robo de información seguirá creciendo en sectores como el retail y el financiero.



¿Hacia dónde va la ciberseguridad?



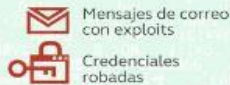
El crimen organizado y el terrorismo están adoptando recursos tecnológicos para llevar a cabo sus actividades.

¿Hacia dónde va la ciberseguridad?

Los APT evaden los controles de seguridad de las organizaciones.

Carbanak: un robo de 1.000 millones de dólares Un ataque dirigido contra un banco

1. Infección



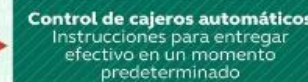
Cientos de equipos infectados
en busca del PC admin



2. Obtención de inteligencia Intercepción de las pantallas



3. Suplantación del empleado Cómo robaron el dinero



¿Hacia dónde va la ciberseguridad?

Existe un cambio global en los vectores, patrones y capacidades de ataque:

- Los vectores de ataque son cada vez más dirigidos a las personas y menos a la tecnología.
- Los patrones de los ataques cada vez parecen más de “comportamiento normal” y son más sofisticados.
- Las vulnerabilidades pueden estar en modo inactivo, y activarse sólo de forma temporal, haciendo más difícil su detección.



¿Hacia dónde va la ciberseguridad?

- Las redes criminales, los gobiernos e incluso los grupos hacktivistas están desarrollando redes de inteligencia robustas y siendo más sofisticados.
- Las capacidades de ataque se vuelven difíciles de estimar al existir plataformas de “crime-as-a-service”.
- Las vulneraciones a través de la cadena de suministro o de los socios de negocio se hacen cada vez más frecuentes.



A collage of blue icons representing various smart devices and systems connected by lines, illustrating the Internet of Things (IoT). The central text reads "INTERNET of THINGS". Icons include a key, a potted plant, a mobile phone, a bicycle, a battery, a car, a car with a sensor, a fan, an airplane, a foot scanner, a computer monitor, a trash bin, a syringe, a clock, a speaker, a train, a light bulb, a bus, a television, a gear, a propeller, a drone, and a radiation symbol.

-

¿Hacia dónde va la ciberseguridad?

ESTRATEGIA

Impulsar la alineación de la estrategia de ciber riesgo con el negocio, innovar e iniciar la transición para administrar el riesgo a través de inversiones de valor

CISO

ASESOR

Ser parte integral del negocio para educar, asesorar e influenciar en las actividades con implicaciones de ciber riesgo.

GUARDIAN

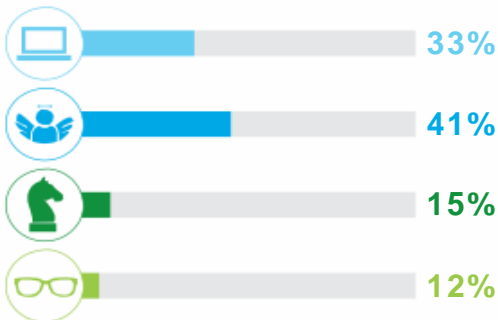
Proteger los activos del negocio al entender el entorno de amenazas y administrar la efectividad del programa de ciber riesgos.

TECNÓLOGO

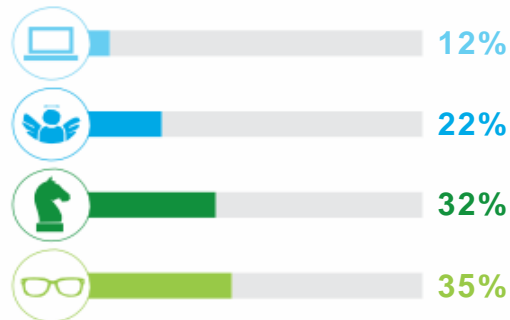
Evaluar e implementar tecnologías y estándares de seguridad para construir capacidades organizacionales



Actual



Deseado



¿Qué nos espera?



OWASP
Open Web Application
Security Project

¿Qué nos espera?



Los retos de ciberseguridad para nuestro país incluyen afrontar:

- Organizaciones carentes de cultura/conciencia de riesgo.
- Ausencia de políticas y estándares de seguridad.
- El enfoque tradicional solo asegura el perímetro.
- Involucramiento de la alta gerencia.
- Sistemas legados que no han sido asegurados.



¿Qué nos espera?

- Pocos cuentan con defensas antimalware.
- Las capacidades de respuesta a incidentes son deficientes, o no existen.
- Confianza en tecnología, sin considerar controles.
- No se consideran los riesgos en la gestión de terceros.
- Estar alineados al negocio y tendencias emergentes.



¿Qué nos espera?

A nivel regulatorio:

- Fortalecer y mantener actualizados los marcos regulatorios con tendencias actuales: **transformación digital, cloud, entre otros.**
- Algunos marcos para impulsar la seguridad en las organizaciones y a considerar son:
 - SBS G140: Gestión de la Seguridad de la Información.
 - SBS 6523-2013: Reglamento de Tarjetas de débito y crédito.
 - Ley de Protección de datos personales.
 - NTP ISO/IEC 27001:2014



¿Qué nos espera?

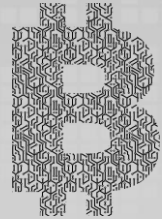
A nivel educación:

- Ausencia de especialistas: capacidades técnicas y experiencia.
- La falta de personal calificado no será resuelta de forma rápida, sin embargo, ya hay universidades/instituciones que están desarrollando diplomados, maestrías.



¿Qué nos espera?

- El gasto en seguridad seguirá creciendo.
- Algunos drivers:
 - Sistemas más complejos e interconectados
 - Nuevas tendencias / nuevos riesgos
 - Protección de datos sensibles
 - Cumplimiento regulatorio
 - Reducción de incidentes y brechas



Siguientes pasos



OWASP
Open Web Application
Security Project

Siguientes pasos



Definir o reforzar programas de ciberseguridad:

- Cambiando el enfoque reactivo por un **enfoque proactivo**.
- Reforzando las **habilidades de personas** (no sólo tecnología y procesos).
- Desarrollar **capacidades de ciber inteligencia** para anticipar los vectores de ataque e identificar las vulnerabilidad de forma eficaz y a tiempo.
- **Reportar riesgos cibernéticos** a los niveles de Dirección.
- Extendiendo sus programas de ciber seguridad a **terceros y socios de negocios**.
- **Integrando capacidades** extendidas a través de servicios de tipo “Security-as-a- Service”.



Recursos



OWASP
Open Web Application
Security Project

Recursos

- Seguridad en aplicaciones:
https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project
- Desarrollo seguro:
https://www.owasp.org/index.php/Category:OWASP_Guide_Project
- Cyber security framework:
https://www.owasp.org/index.php/OWASP_Open_Cyber_Security_Framework_Project
- Riesgos de privacidad:
https://www.owasp.org/index.php/OWASP_Top_10_Privacy_Risks_Project
- Modelado de amenazas:
https://www.owasp.org/index.php/Threat_Risk_Modeling
- Seguridad en aplicaciones móviles:
https://www.owasp.org/index.php/OWASP_Mobile_Security_Project



Preguntas



Contacto



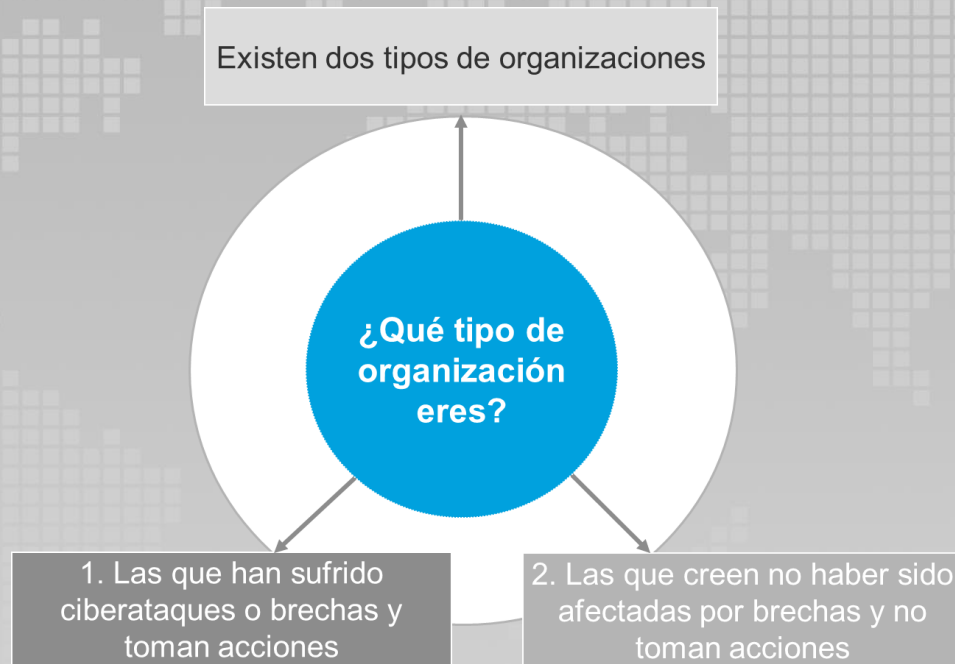
Jorge Córdova Pelayo

CISSP, CISM, ISO 27001 LA, C|EH, C)PTE,
BNS, MCSA+M, MCTS

Correo: jacppe@gmail.com



OWASP
Open Web Application
Security Project



“Eso nunca ha pasado (pasará) en la empresa”, “nosotros tenemos la tecnología para detener cualquier ataque” o “nuestra organización no está en la mira de los delincuentes”. Lo real es que todas organizaciones y personas están expuestas a un ciber ataque.