



Seguridad y Auditoria a los Cyberataques

***Ing. Carlos Luis Vidal, CISA, CIA, MBA,
CISM CISSP, CFE, QAR, COBIT5F, ITIL3,
Security+***

***Past President
ISACA Capítulo de Lima***

ACERCA DE ISACA

- Asociación internación profesional sin fines de lucro.
- Posee más de 40 años de fundación y es reconocida a nivel internacional y local.
- **Una Oficina Central en Illinois, USA**
- **205 Capítulos en 86 Países**
- Miembros que en su mayoría son:
 - *Profesionales en Auditoría de TI*
 - *Profesionales Seguridad de Información*
 - *Profesionales en Riesgos y cumplimiento*
 - *Profesionales en Gerencia y Gobierno de TI*



ACERCA DE ISACA LIMA



- Asociación profesional sin fines de lucro.
- Es el **capítulo local y oficial** de ISACA Internacional en el Perú.
- Fundado en 1997.
- En la actualidad cuenta con **más de 570 miembros** sus miembros son profesionales de auditoría, seguridad, control, gestión y gobierno de TI.

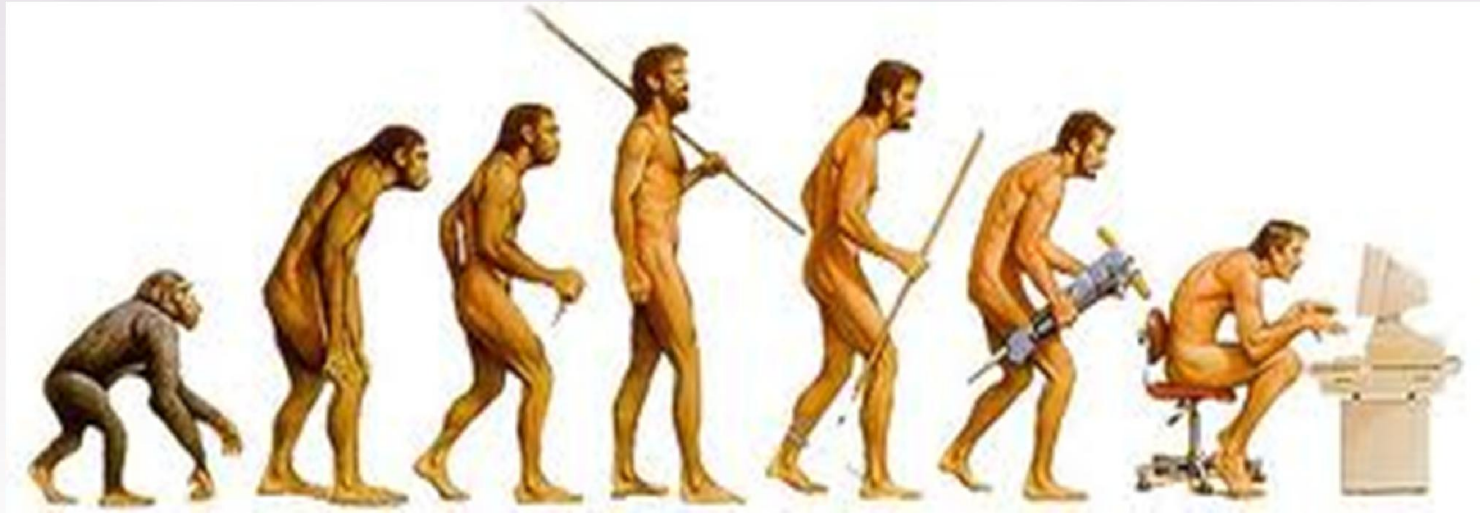


Agenda

1. EVOLUCIÓN DE CYBER ATAQUES
2. DEFINICION DE CLIENTE SIDE ATTACK(Cyber ataques del lado del cliente)
3. ¿POR QUE ES EXITOSO UN CLIENT SIDE ATTACKS
4. RECOMENDACIONES A:
 - a) GERENCIAS DE TI(CIO's)
 - b) SEGURIDAD DE SISTEMAS DE INFORMACIÓN
 - c) AUDITORIA DE SISTEMAS DE INFORMACIÓN

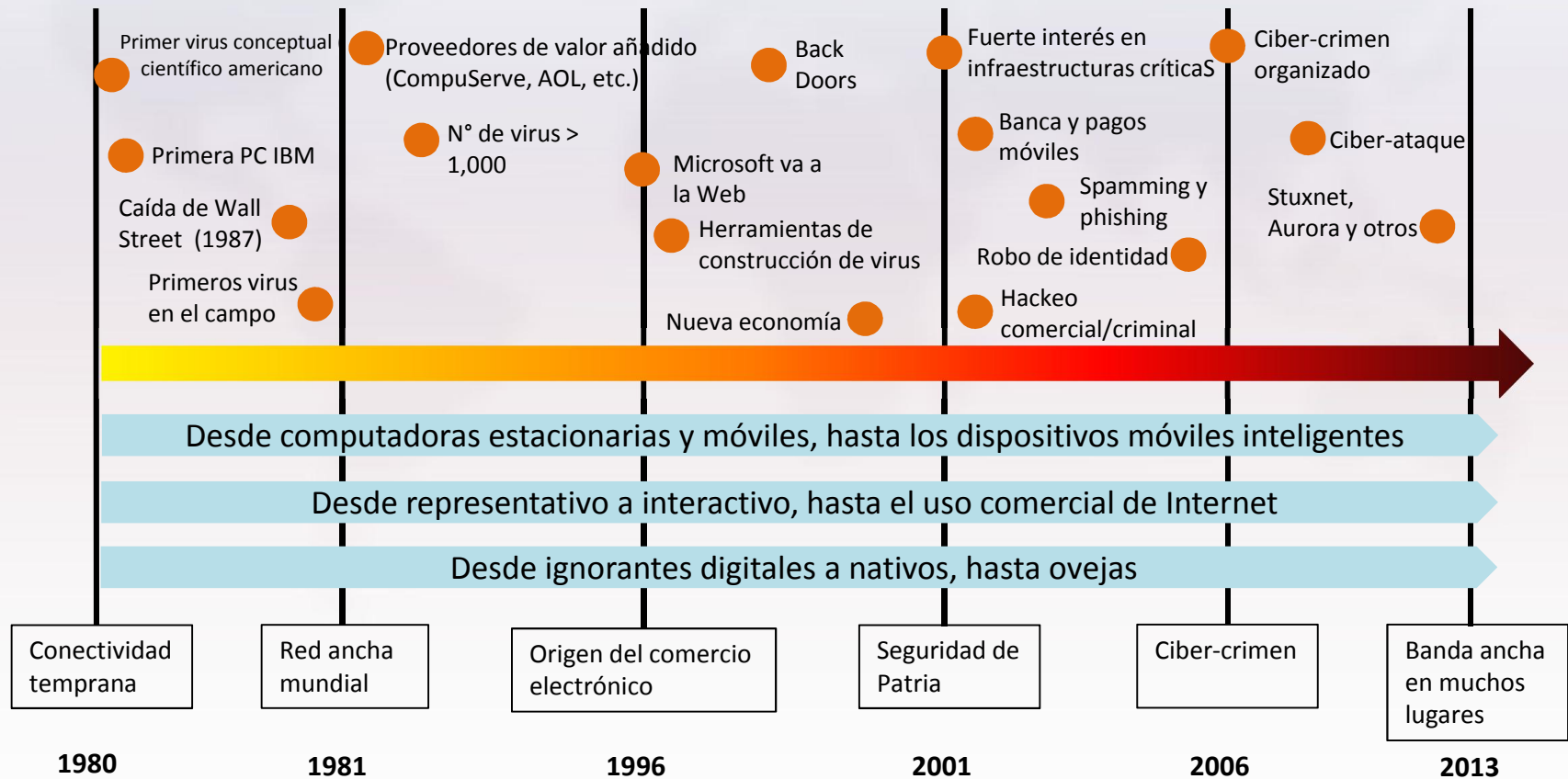
INTRODUCCION

EVOLUCION DE LOS ATAQUES



INTRODUCCION

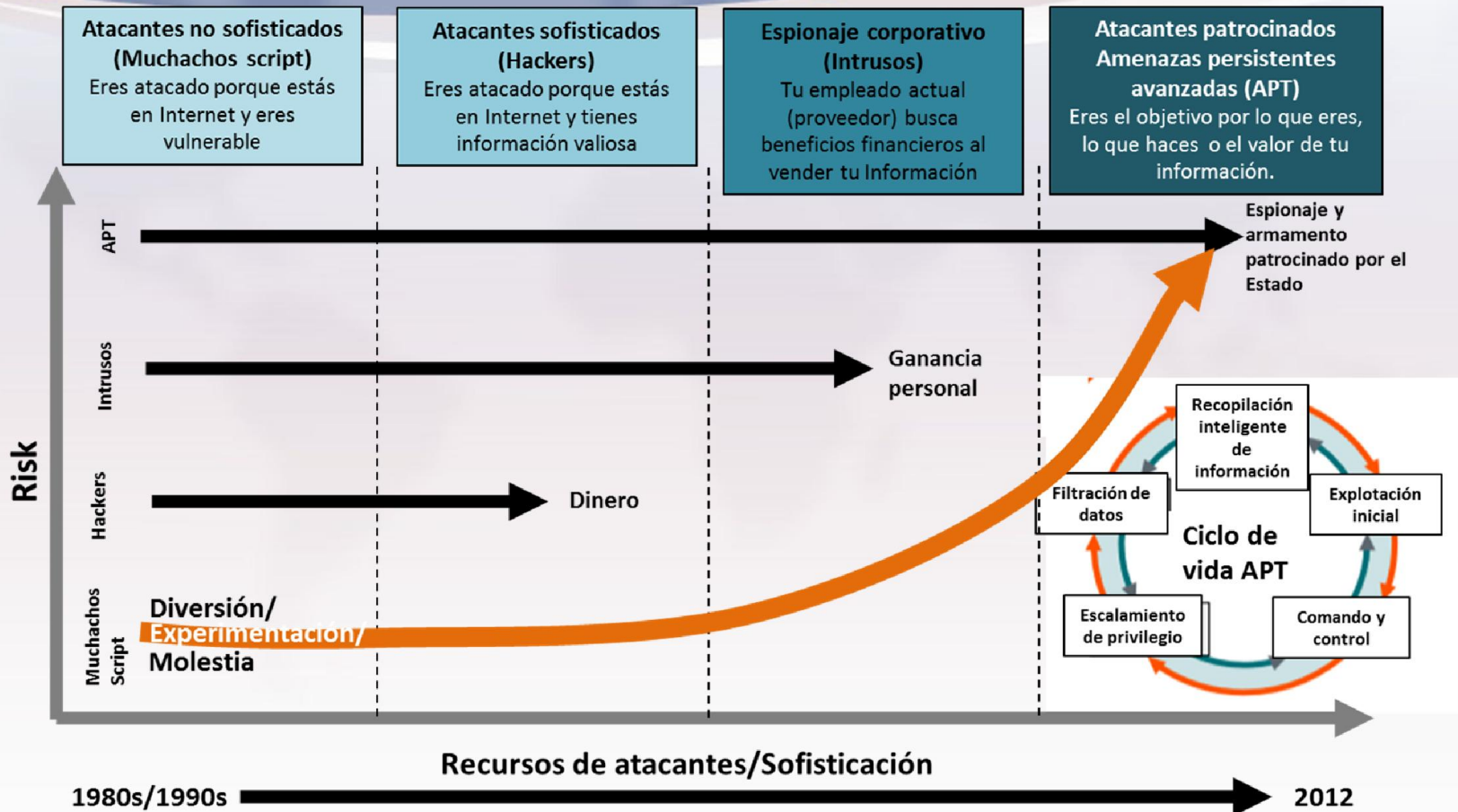
¿DONDE ESTAMOS EN LINEA DE TIEMPO DE CIBERATAQUE?



Fuente: Transformando la Ciberseguridad usando COBIT 5- ISACA HQ- 2014

INTRODUCCION

Evolución del panorama de amenazas



- Morris Worm
- Virus polimorfos
- MiguelAngel
- Concepto de macro virus
- Melissa
- "Te amo"
- Anna Kornikova
- Sircam
- Código rojo y Nimda
- MyDoom
- Netsky
- Sasser
- Storm bonet
- Koobface
- Conflicker
- Aurora
- Mariposa
- Stuxnet
- Wikileaks
- Anonymous
- LutzSec
- SpyEye/Zeus
- Duqu
- Flame

Para tomar en cuenta

Cybersecurity Skills Crisis

Too Many Threats

 **62%**
INCREASE
IN BREACHES
IN 2013¹

1 IN 5 
ORGANIZATIONS
HAVE EXPERIENCED
AN APT ATTACK⁴

US \$3 TRILLION
TOTAL GLOBAL
IMPACT OF
CYBERCRIME³

 **31 7½ MONTHS**
IS THE AVERAGE TIME
AN ADVANCED THREAT
GOES UNNOTICED ON
VICTIM'S NETWORK²

2.5 BILLION 
EXPOSED RECORDS AS
A RESULT OF A DATA BREACH
IN THE PAST 5 YEARS⁵

Too Few Professionals

 **62%**
OF ORGANIZATIONS
HAVE NOT INCREASED
SECURITY TRAINING
IN 2014⁶

 **1 OUT OF 3**
SECURITY PROS ARE
NOT FAMILIAR WITH
ADVANCED PERSISTENT
THREATS⁷

 **<2.4%**
GRADUATING STUDENTS
HOLD COMPUTER
SCIENCE DEGREES⁸

 **1 MILLION**
UNFILLED SECURITY
JOBS WORLDWIDE⁹

83% 
OF ENTERPRISES CURRENTLY
LACK THE RIGHT SKILLS AND
HUMAN RESOURCES TO PROTECT
THEIR IT ASSETS¹⁰

Enterprises are under siege from
a rising volume of cyberattacks.

At the same time, the global demand for skilled professionals sharply outpaces supply. Unless this gap is closed, organizations will continue to face major risk. Comprehensive educational and networking resources are required to meet the needs of everyone from entry-level practitioners to seasoned professionals.

SOURCES: 1. 2014 Internet Security Threat Report, Volume 19, Symantec, April 2014; 2. M-Trends 2014: Attack the Security Gap, Mandiant, April 2014; 3. Increased Cyber Security Can Save Global Economy Trillions, McKinsey/World Economic Forum, January 2014; 4. ISACA's 2014 APT Study, ISACA, April 2014; 5. An Executive's Guide to 2013 Data Breach Trends, Risk Based Security/Open Security Foundation, February 2014; 6. ISACA's 2014 APT Study, ISACA, April 2014; 7. ISACA's 2014 APT Study, ISACA, April 2014; 8. Code.org, February 2014; 9. 2014 Cisco Annual Security Report, Cisco, January 2014; 10. Cybersecurity Skills Haves and Have Nots, ESG, March 2014



Retos Actuales en Seguridad de TI

- **62%** incremento en brechas de seguridad de TI durante el 2013.
- **1 de cada 5** organizaciones han sufrido un ataque avanzado de cómputo.
- **3 Trillones de \$** es el impacto anual por Cibercrimen.
- **7 y ½ meses** es el tiempo que permanece en promedio una ataque avanzando de cómputo sin detectarse
- **2.5 Billones** registros han sido expuestos debido alguna brecha en los últimos 5 años.

Fuente: Internet Security Theat Report 2014.

¿Qué es una APT?

- Las amenazas persistentes avanzadas son fenómenos relativamente nuevos para muchas organizaciones.
- Un APT es una amenaza que es avanzada y persistente. Es un ataque con un objetivo específico que busca mantenerse en la víctima.

CASO AURORA

- *Se le considera como uno de los ciberataques más sofisticados, pues se trata de un robo detalladamente planeado y muy bien dirigido hacía Google y otras más de 30 empresas para robar información usando un malware.*
- *Se trató de sabotaje corporativo*

**HAZ CLICK AQUÍ
PARA ACCEDER**



Noticias

Europe News

ECB hacked: Data stolen from central bank

Mark Smith (@marksmith1)

Thursday, 24 Jul 2014 | 3:15 AM EBCNDC.com

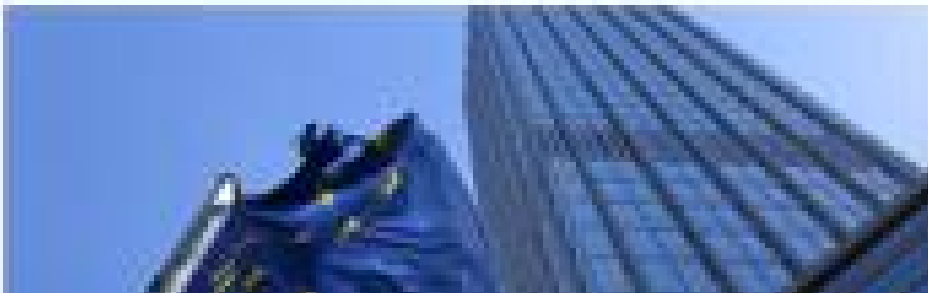
SHARES

Email addresses and other contact information stored at the [European Central Bank \(ECB\)](#) have been stolen, the organization confirmed on Thursday.

Security that protects a database serving its public website has been breached, it said in a statement published on its website, meaning users registering for information on conferences and visits at the ECB have been compromised.

[Read More: Euro zone business activity rebounds, France lags](#)

It stated that no "critical systems or market-sensitive" information had been part of the data theft and was physically separate from the compromised data.



Noticias

Information Systems & Security | News | Target breach may have started with email phishing

Target breach may have started with email phishing

By [ANNE HOGAN](#) | [@ANNEHOGAN](#) | [February 12, 2014, 10:01 AM](#)

1 / Shares | 11 / Tweets | 0 / Stumble | 0 / Email

For the millions of victims of [Target's \(TGT\) data and credit-card hack](#), some answers are emerging about how the crime was committed, but it might not prove reassuring.

A Pennsylvania-based heating and air conditioning company appears to have been the victim of the "phishing" attack, which allowed the criminals to access Target's systems, reports security expert Brian Krebs, who was the first to alert consumers in December about the hack that has affected as many as 116 million customers.



Play [VIDEO](#)

In a typical phishing attack, fraudsters try to lure people into divulging passwords, credit card details and other confidential information by sending them an email that appears to be from a legitimate organization, such as a bank or retailer. Messages may also include a link that, if the recipient clicks on it, introduces a computer virus that secretly collects data.

Market Data

Moneywatch Spotlight

Top 10 international places to invest in real estate

Introducción- Premisa

La ciberseguridad es un área en constante cambio y crecimiento.

Es crucial que los conceptos centrales que enmarcan y definen esta área sean entendidos por los profesionales que están involucrados con las implicaciones de seguridad.

ATAQUES DE LADO CLIENTE

- Antes: Server Side Attack

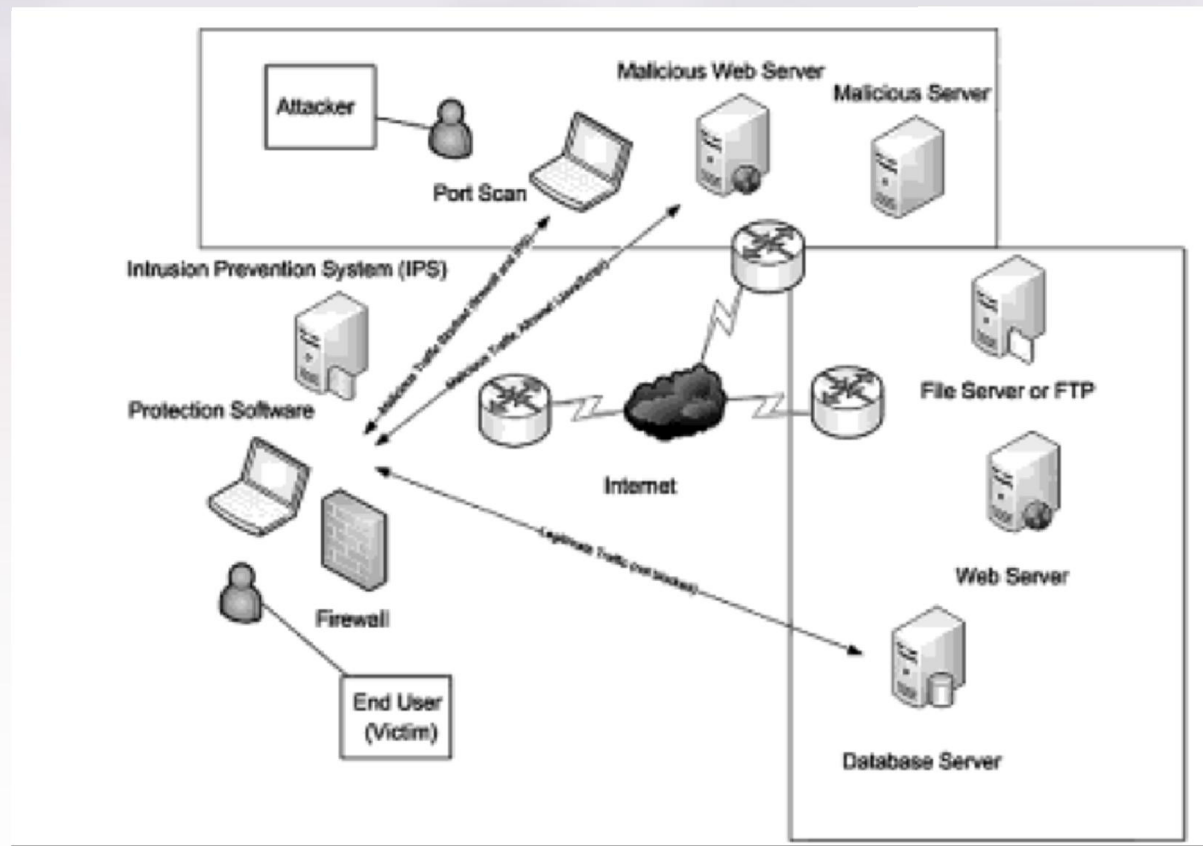
Router, Servidor Web, Servidor Base de Datos,
Servidores Aplicaciones y similares.



Fuente: Client Side Attacks, 2012

ATAQUES DE LADO CLIENTE

Ahora también: Cliente Side Attack



Fuente: Client Side Attacks, 2012

ATAQUES DE LADO CLIENTE

Navegadores, Lectores PDF, Aplicaciones Ofimáticas, entre otras.



ATAQUES DE LADO CLIENTE

Tipos de Client Side Attack

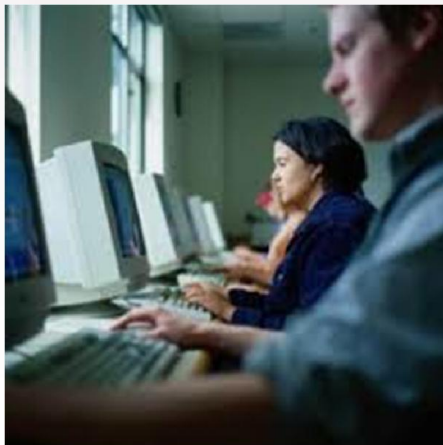
i) CSA asociados a una vulnerabilidad técnica



ATAQUES DE LADO CLIENTE

Tipos de Client Side Attack

ii) CSA que utilizan también la ingeniería social



ATAQUES DE LADO CLIENTE

¿Que será mejor tener cualquier cuenta de usuario o la de los administradores y altos funcionarios de los sistemas de una empresa?



ATAQUES DE LADO CLIENTE

¿En este tipo de ataque sólo se aprovechan de temas técnicos?

NO, Sino además los atacantes buscan la motivación de las personas que quieren atacar, así como su falta de concientización en seguridad de información.

ATAQUES DE LADO CLIENTE

Vulnerabilidad

Es la debilidad de un sistema que permite que un atacante logre concretar sus ataques.

P.E: Tener instalado sistemas con fallas de seguridad, no tener o tener un antivirus desactualizado, otros



Vulnerabilidades

Busqueda de vulnerabilidades

Base de Vulnerabilidades:

<http://web.nvd.nist.gov/view/vuln/search>

NVD - Search

web.nvd.nist.gov/view/vuln/search

NVD - Search

Sponsored by
DHS National Cyber Security Division/US-CERT

NIST
National Institute of
Standards and Technology

National Vulnerability Database
automating vulnerability management, security measurement, and compliance checking

Vulnerabilities Checklists 800-53/800-53A Product Dictionary Impact Metrics

Home SCAP SCAP Validated Tools SCAP Events About

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

- 64813 [CVE Vulnerabilities](#)
- 250 [Checklists](#)
- 248 [US-CERT Alerts](#)
- 3360 [US-CERT Vuln. Notes](#)
- 10286 [OVAL Queries](#)
- 97158 [CPE Names](#)

Last updated: 9/22/2014 6:35:54 AM

CVE Publication rate: 29.17

Email List

Search CVE and CCE Vulnerability Database

([Advanced Search](#))

Keyword search:

Try a product or vendor name
Try a [CVE](#) standard vulnerability name or [OVAL](#) query
Only vulnerabilities that match ALL keywords will be returned
Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions

Search All
 Search Last 3 Months
 Search Last 3 Years

Show only vulnerabilities that have the following associated resources:

Software Flaws (CVE)
 Misconfigurations (CCE), under development

US-CERT [Technical Alerts](#)
 US-CERT [Vulnerability Notes](#)
 [OVAL](#) Queries

NVD now maps to CWE! See [NVD CWE](#) for more details.

Exploits

Búsqueda de vulnerabilidades y exploits

Base de Exploits On-Line:

<http://www.exploit-db.com>



The screenshot shows the Exploit Database website. The main navigation includes Home, Exploits, Shellcode, Papers, Google Hacking Database, Submit, and Search. The main content area features the "Offensive Security Exploit Database Archive" with 34733 exploits archived. A prominent banner for the "Google Hacking Database" is displayed, describing it as a collection of interesting Google searches. Below this, the "Remote Exploits" section is shown, including a table of recent exploits.

Date	D	A	V	Title	Platform	Author
2015-10-14	✓	-	✓	Linux/MIPS Kernel NetUSB - Remote Code Execution Exploit	multiple	blasty
2015-10-13	✓	-	✓	ZHONE < S3.0.501 - Multiple Vulnerabilities	hardware	Lyon Yang
2015-10-05	✓	-	✓	Zemra Botnet CnC Web Panel Remote Code Execution	multiple	metasploit

ATAQUES DE LADO CLIENTE

Búsqueda de vulnerabilidades y exploits

Base de Exploits On-Line:

<http://www.cvedetails.com>

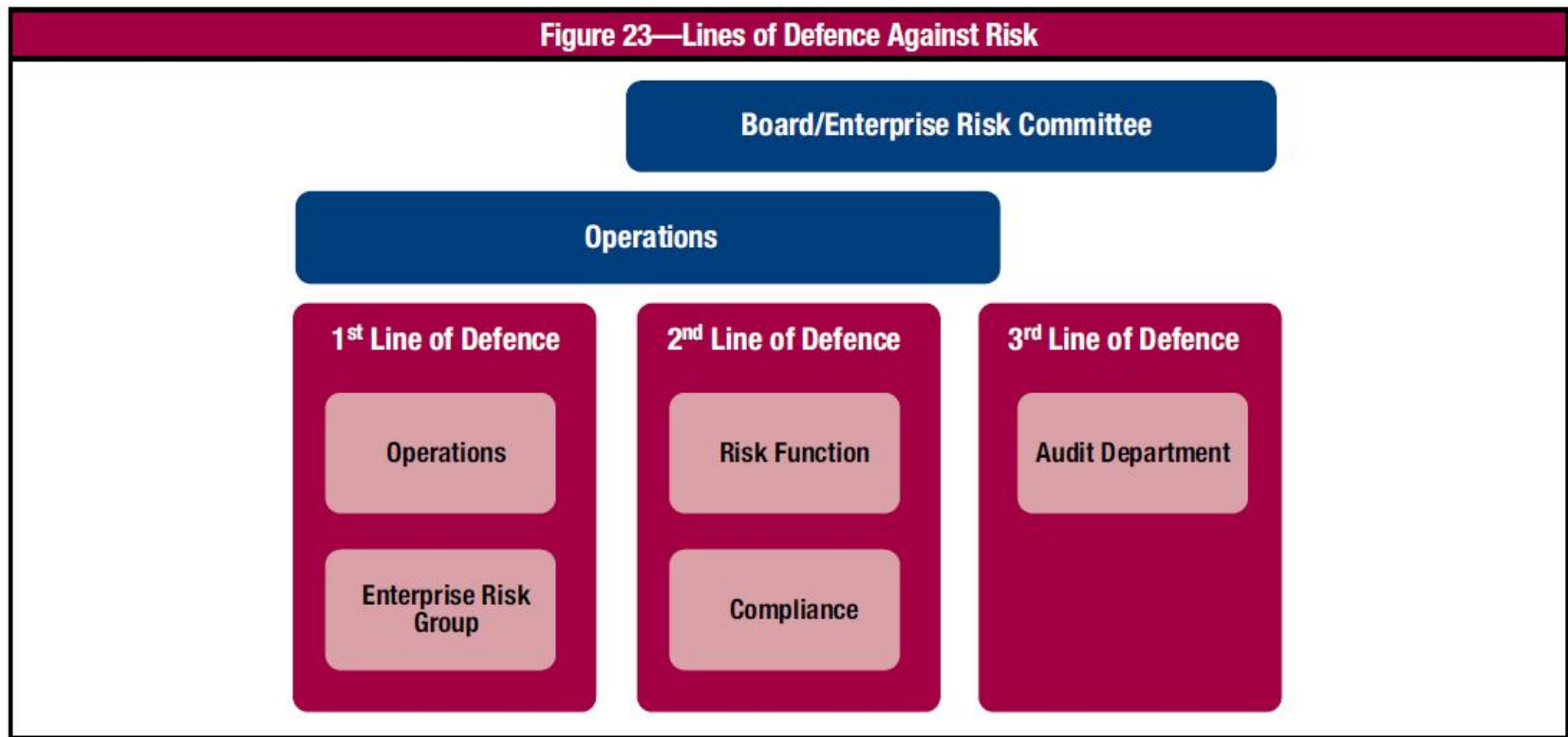
The screenshot shows the CVE Details website interface. The main heading is "CVE Details" with the tagline "The ultimate security vulnerability datasource". The page includes a search bar, navigation links, and a section for generating custom RSS feeds or widgets. A prominent feature is the "Current CVSS Score Distribution For All Vulnerabilities" section, which includes a table and a bar chart.

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	160	0.20
1-2	478	0.70
2-3	2697	4.20
3-4	1334	2.10
4-5	12438	19.40
5-6	12517	19.50
6-7	7567	11.80
7-8	17444	27.20
8-9	258	0.40
9-10	9269	14.40
Total	64162	

The bar chart titled "Vulnerability Distribution By CVSS Scores" shows the following data points: 0-1 (160), 1-2 (478), 2-3 (2697), 3-4 (1334), 4-5 (12438), 5-6 (12517), 6-7 (7567), 7-8 (17444), 8-9 (258), and 9-10 (9269).

RECOMENDACIONES Y CONCLUSIONES- CSA

Primero tomar es importante tomar en cuenta:



RECOMENDACIONES Y CONCLUSIONES- CSA

CIOS(Gerentes de Sistemas y Tecnologías de información

- Actualizar y ejecutar un programa antivirus y un programa anti spyware.
- Actualizar el sistema operativo y los navegadores web de forma regular.
- Actualizar (por ejemplo: Flash, Quicktime), lectores (por ejemplo. Acrobat), y complementos con regularidad.
- Tener cuidado con sitios web sospechosos (por ejemplo. Sitios que ofrecen videos gratuitos y torrent)
- No navegar por la web y abrir correos utilizando la cuenta de administrador(cuenta con altos privilegios).

RECOMENDACIONES Y CONCLUSIONES- CSA

CISO(Oficiales de Seguridad de Información)

- Definir lineamientos en la política de seguridad de información que establezca la responsabilidad de actualización de los agentes de antivirus, anti malware, sistemas operativos, base de datos y aplicaciones clientes
- Monitoreo de la consola de antivirus tanto en los servidores, estaciones de trabajo y en la actualidad incluso dispositivos móviles.
- Verificar la actualización:
 - Sistemas operativos(servidores y estaciones)/ BD's
 - Aplicaciones cliente(navegadores, ofimáticas, reproductores de audio, lectores pdf, etc.)
- Verificar que no exista tráfico a sitios web sospechosos (por ejemplo. Sitios que ofrecen videos gratuitos y torrent)
- Verificar el uso de las cuentas privilegiadas
- Realizar análisis de vulnerabilidades en servidores y estaciones de trabajo

RECOMENDACIONES Y CONCLUSIONES- CSA

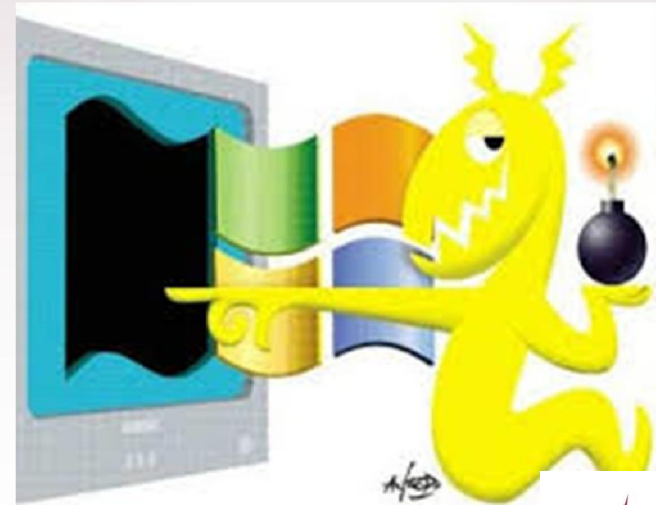
Auditor de Sistemas

- Revisar la existencia y suficiencia de lineamientos en la política de seguridad relacionadas a controlar los cyber ataques tales como la actualización de la infraestructura tecnológica y antivirus/antimalware.
- Verificar el cumplimiento de los lineamientos definidos en la política(incluso a pesar que no se hayan definido), sino igual revisar que se realice la actualización tanto en servidores , estaciones de trabajo(pcs') y MOBILES de: agentes de anti virus/malware, S.O, BD, aplicaciones finales, navegadores.
- Revisar que se hayan implementado controles de web content (por ejemplo. Sitios que ofrecen videos gratuitos y torrent)
- Verificar los controles en la cuenta de administrador(cuentas con altos privilegios).
- Solicitar el sustento de las charlas de concientización/educación tanto a personal de TI como a usuarios finales, clientes, partners.

RECOMENDACIONES Y CONCLUSIONES

Pero NO OLVIDAR:

CONCIENTIZAR A TODOS LOS USUARIOS
Y CLIENTES



MAYOR INFORMACION

<http://www.isaca.org/cyber/Pages/default.aspx>

(Como implementar la ciberseguridad en la organizacione)

<http://www.offensive-security.com/community-projects/kali-linux/>

(Descarga de Kali)

<http://www.exploit-db.com>

(Base de datos de exploits)

<http://www.cvedetails.com>

(Base de datos de vulnerabilidades)

<http://web.nvd.nist.gov/view/vuln/search>

(Base de datos de vulnerabilidades)

PREGUNTAS



ISG PUCP

Conferencias: QAR en AI, Seguridad Web, INFOSOFT 2012, 2013, 2014



Muchas Gracias!!!

**Ing. Carlos Luis Vidal, CISA, CIA, MBA, CISM CISSP, CFE, QAR,
COBIT5F, ITIL3, Security+
Past President- ISACA Lima**

cluis@pucp.edu.pe

celv_83@hotmail.com

cluis@isaca.org.pe

(ISACA LIMA)

[E-mail informacion@isaca.org.pe](mailto:informacion@isaca.org.pe)

Facebook: ISACALima

Web: www.isaca.org.pe

(ISACA Internacional)

www.isaca.org

Proxima conferencia de ISACA Lima

"Infraestructuras Críticas y Sistemas de Control Industrial - Cómo clasificarlos y protegerlos «

Objetivos:

- Conocer cuál es la clasificación del DHS (Departamento de Seguridad Interior) para las diferentes infraestructuras críticas
- Distinguir las diferencias de la información entre TICs y SCIs
- Conocer los servicios de un CSIRT de ICS versus uno de ICT.

DIRIGIDO A:

CIOS - Gerentes de TI / Sistemas

Audidores Internos y de TI

Oficiales de Gobierno de TI

Oficiales de cumplimiento

Consultores en seguridad de TI

FECHA: Martes 20 de octubre de 2015

LUGAR: Hotel José Antonio - Sala Larco Piso 9 Av. 28 de Julio 398 - Miraflores

Asociados a ISACA : Sin costo*

No Asociados a ISACA : S/ .170.00 (Incluye IGV)

Inscripción al: informacion@isaca.org.pe