ActivosTI

Tecnología e Información Segura

Seguridad Informática
algo mas que un firewall y un antivirus

Héctor Herrera, Director ActivosTI
hector.herrera@activosti.com

Bogotá, 2016.

ActivosTI
Tecnología e Información Segura

Conferencia

Hackers al acecho de su información. Como atacan

Recopilación de información acerca de los ataques informáticos a las empresas. Como los delincuentes informáticos pueden hacerse con la información de su empresa y su información personal. Que tan fácil podemos hacerle el trabajo y que se debe hacer para asegurar la información.

Héctor Herrera

Para los que le gusta la lectura.

Ingeniero de sistemas egresado de la Universidad Industrial de Santander, Especialista en Gerencia de Proyectos de Sistemas – Universidad del Rosario. Especialista en Auditoría de Sistemas – UAN. Certified Ethical Hacker CEH – ECCouncil. Red Hat Certified Engineer RHCE. Ha desarrollado proyectos de seguridad informática a nivel gerente/lider en empresas como: Ecopetrol, Avianca, “Elecciones 2011 – Registraduría Nacional de Colombia”. , Ministerio de Comercio Industria y Turismo. Trabajó como asesor de Despacho del Director de Sistemas en el Ministerio de Hacienda y Crédito Público 2014-2015. En la actualidad se desempeña como Director de ActivosTI, empresa consultora en productos de seguridad como Nessus, Acunetix, Sophos y Nagios entre otros, servicios de evaluaciones del estado de la seguridad en las empresas, pruebas análisis de vulnerabilidades, pruebas de hacking ético, ingeniería social, auditoria de código fuente, pruebas perimetrales de seguridad y consultoría en seguridad de la información.

Presentación - ActivosTI

Somos consultores en productos y servicios de seguridad informática.

ActivosTI fue fundada en la ciudad de Bogotá Colombia, el 5 de octubre de 2011

Objetivo: Viabilizar el cierre de las brechas de seguridad informática.

Ofrecer herramientas y métodos para implantar, mantener, gestionar y auditar controles de seguridad informática.

Empresas con las cuales ActivosTI ha realizado trabajos

Trabajos tercerizados
- Avianca
- Ecopetrol
- Min. de Hacienda
- Min. de Industria y Comercio
- Min. de Educación
- Alcaldía de Itagüí

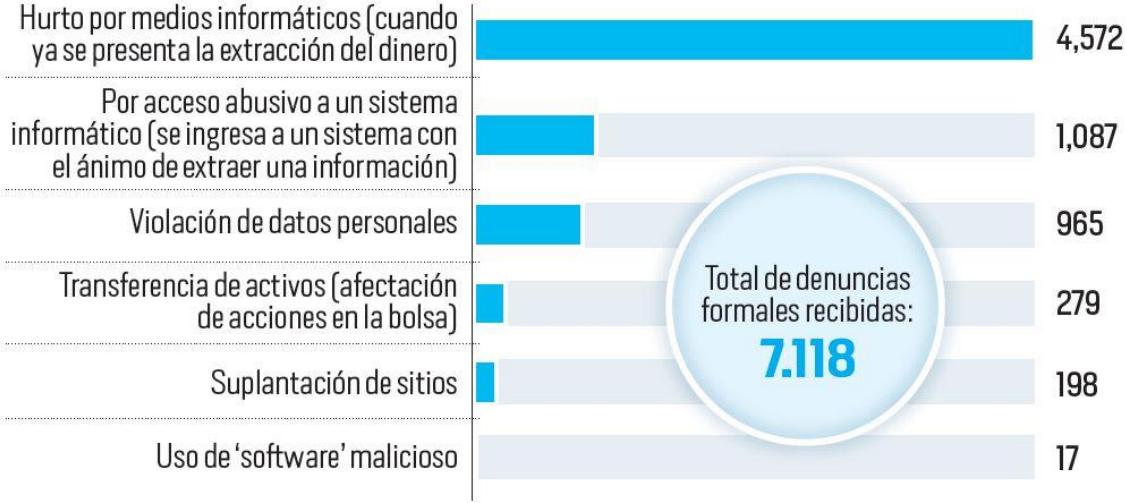
Nos han contratado:
- Sonda de Colombia
- Gamma Ingenieros
- INDRA
- Compufacil
- Grant Thorton y Fast Auditores.

Clientes directos:
- Claro Telmex
- EMTELCO
- Comfenalco Cartagena, OlimpiaIT
- Alianza Valores
- Alianza Fiduciaria
- Asesorías e Inversiones

Radiografía de los delitos informáticos en Colombia en 2015

Fuente: Unidad de Delitos informáticos de la Dijín, Panda Security, Microsoft

El **64 por ciento** de las denuncias correspondió a hurtos por medios informáticos



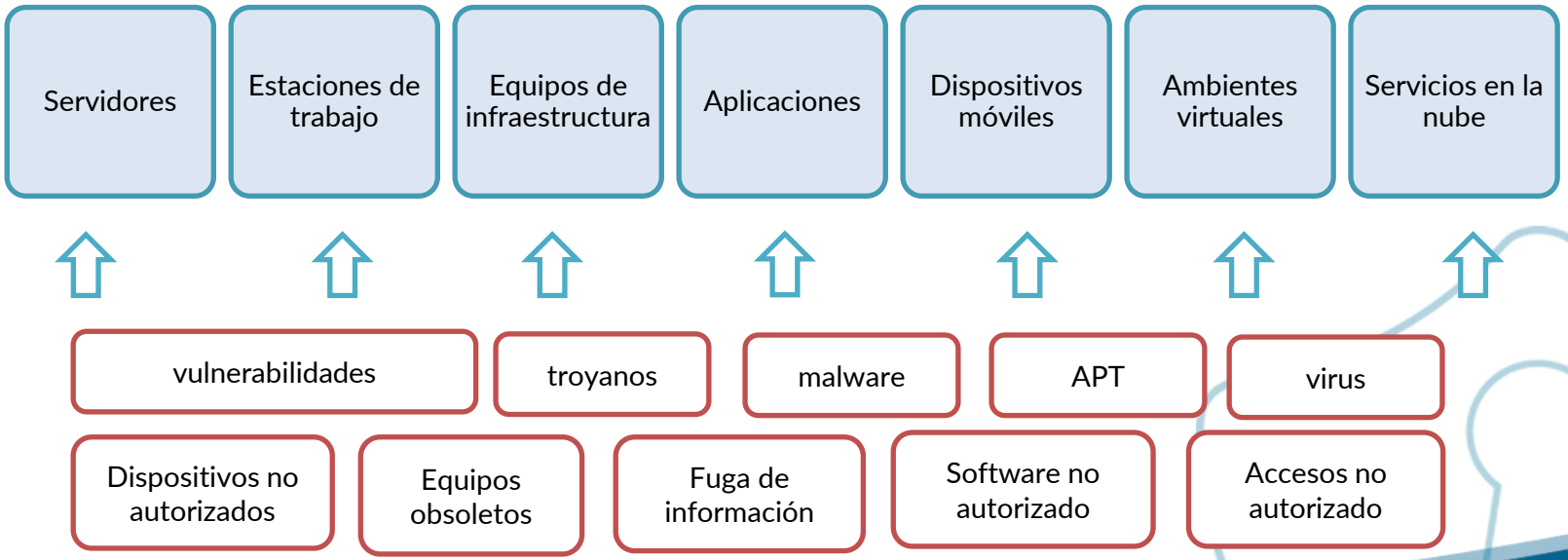
A diario, se crean más de **160.000** tipos de programa malicioso.

Actores interesados en la información de su empresa

- Delincuentes
- Crimen organizado
- Su competencia
- Caza recompensas
- Accidentes informáticos
- Descuidos informáticos
- Espionaje industrial
- Principiantes
- empleados deshonestos
- …

http://www.eltiempo.com/tecnosfera/tutoriales-tecnologia/cuantos-delitos-informaticos-se-denuncian-en-colombia/16493604

Elementos en infraestructura



Areas de acción de amenazas informáticas

Hackers al ataque ?

Hacker

cracker

pentester

Hacker ético

Delincuente informático

Hackers al ataque ?
Definiciones

Hacker: experto en técnicas relacionadas con las tecnologías de la información y las telecomunicaciones: programación, redes, sistemas operativos.

Cracker: es alguien que viola la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que a diferencia de este último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño a su objetivo.

Hackers al ataque ?
Definiciones

Black hats
Individuos con habilidades computacionales empleadas para actividades maliciosas o destructivas. Conocidos como ‘Crackers.’

White Hats
Individuos que profesan habilidades de hackers y las utilizan con fines defensivos.

Gray Hats
Individuos que trabajan tanto ofensiva como defensivamente en varias ocasiones.

¿Hackers al ataque?
Definiciones

Hacker ético: profesionales de la seguridad que aplican sus conocimientos de hacking con fines defensivos (y legales).

¿Hackers al ataque?
Elementos esenciales de la seguridad.

Confidencialidad	Solo el autorizado tiene acceso.
Integridad	Identificación y garantía del origen de la información.
Disponibilidad	La información que contiene no ha sido modificada
Autenticidad	Solo el autorizado tiene acceso.

¿Hackers al ataque?

¿Hackers al ataque?

1. Reconocimiento

Previo a cualquier ataque

- Información sobre el objetivo.
- Reconocimiento pasivo:
  - Google Hacking
  - Ingeniería social
  - Monitorización de redes de datos. Por ejemplo, sniffing, etc.

2. Escaneo

es una fase de pre-ataque.

- Se escanea la red pero ya con información de la fase previa.
- Detección de vulnerabilidades y puntos de
- entrada.
- El escaneo puede incluir el uso de scanners de puertos y de vulnerabilidades.

2. Escaneo (cont)

Reconocimiento activo
Probar la red para detectar:

- hosts accesibles
- puertos abiertos
- localización de routers
- Detalles de sistemas operativos y servicios

3. Ataque – garantizar acceso.

Obtención de acceso – Se refiere al ataque propiamente dicho.

- Vulnerabilidades
- ataques man-inthe_middle (spoofing)
- exploits (buffer overflows)
- DoS (denial of service)
- Fuerza bruta
- SQL Injection
- XSS Cross Site Scripting

4. Mantener acceso.

Se trata de retener los privilegios obtenidos.

A veces un hacker blinda el sistema contra otros posibles hacker, protegiendo sus puertas traseras, rootKits y Troyanos.

5. Borrado de huellas.

Eliminación de evidencia para no ser descubierto.
Hay que tener claro que hay técnicas más intrusivas (y por lo tanto delatoras) que otras.
Análisis forense

Principios de ciberseguridad

- Identificar: implica obtener una comprensión de los recursos y los niveles de riesgo asociado a los activos.
- proteger y detectar: control de acceso y supervisión de la seguridad.
- responder y recuperar: buscan la forma de reaccionar en caso de un incidente de seguridad.

Identificar

Proteger

Detectar

Responder

Recuperar

VISIBILIDAD COMPLETA

Conozca “toda” su Red

Alcance de Sensores
Colecte & integre data critica a través de su empresa

MEJOR CONTEXTO

Sepa, que hacer

Analice y Reporte
Priorice seguridad, basándose en inteligencia con la que puede reaccionar mejor

COBERTURA TOTAL

Sepa, que esta seguro

Monitoreo Continuo
Analítica mas avanzada y en tiempo real

Búsqueda de vulnerabilidades

Framework de seguridad

Dispositivos desconocidos

Gestión de vulnerabilidades

Monitoreo continuo

Que software ayuda en seguridad informática?

tenable network security

SecurityCenter CV
continuous view

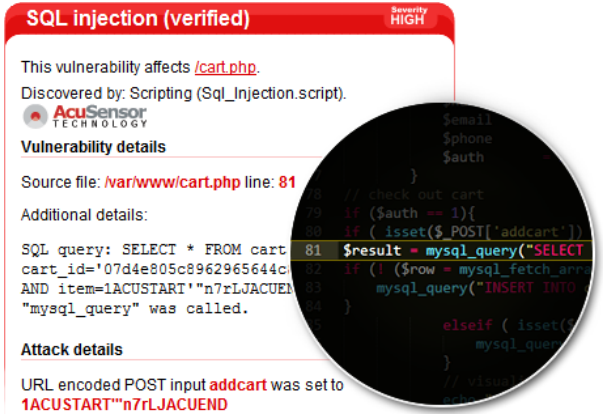
SecurityCenter

Nessus manager

Nessus cloud

Nessus professional

acunetix



SOPHOS

Nagios®

Aerohive NETWORKS

Barracuda

Servicios

- Monitoreo continuo de seguridad
- Evaluaciones de seguridad informática
- Auditoría de seguridad informática
- Análisis y gestión de vulnerabilidades
- Pruebas de hacking ético
- Pruebas perimetrales de seguridad
- Monitoreo de plataforma TI

Cual es su postura frente a los nuevos ataques de seguridad hacia los datos de su empresa:

- Proactiva
- Reactiva

¿Que pasa si no tiene monitoreada adecuadamente la seguridad de su empresa?

Tres cosas pueden pasar:

- Los ataque han sucedido y no se ha enterado.
- Los ataque pueden estar pasando y no se ha dado cuenta.
- A futuro pueden suceder ataques y no esta preparado.

¿Interesado en ver una postura completa de la seguridad de su empresa hacia Internet?

Llámenos:
5161878
6386220
3152301090
Bogotá Colombia

ActivosTI

Tecnología e Información Segura

Cr. 18 Nº 86A-14 Chicó
PBX: (+571) 6386220 Fax: (+571) 6163030
Bogotá - Colombia
www.activosti.com