the Internet is for everyone

Algunas Perspectivas de Ciberseguridad

Shernon Osepa

Gerente Asuntos Regionales Para America Latina y el Caribe

4TO Foro Regional Sobre Interconectividad y Reduccion de Precios de los Telecomunicaciones y Acesso a Internet

Tegucigalpa, Honduras

12 de Agosto de 2016

Internet Society

InternetSociety.org

Agenda

- Sobre Internet Society
- Tres Niveles de Operación de Internet
- Temas de Seguridad Cibernética

Internet Society

- Fundada en 1992 por pioneros de Internet.

- Organización internacional sin fines de lucro que trabaja por el uso, desarrollo y evolución abiertos de Internet para todas las personas del mundo, mediante el trabajo en las áreas de estándares técnicos, educación y desarrollo de capacidades, así como políticas públicas.

Visión

- Internet es para todos

Misión (1)

Para avanzar hacia nuestra misión, Internet Society

- Facilita un desarrollo abierto de normas, protocolos, administración e infraestructuras técnicas de Internet.
- Apoya la educación, en especial en países en vías de desarrollo, o en aquellos lugares donde haga falta.
- Promociona el desarrollo profesional y crea una comunidad para fomentar la participación y el liderazgo en temas que son importantes para la evolución de Internet.
- Ofrece información fiable sobre Internet

Misión (2)

Para avanzar hacia nuestra misión, Internet Society

- Ofrece foros para discutir temas que afectan a la evolución de Internet, su desarrollo y uso en cuestiones técnicas, comerciales, sociales y otros contextos
- Fomenta un entorno de cooperación, internacional, comunidad y una cultura que crea un autogobierno que funciona
- Sirve como punto central para los esfuerzos cooperativos que promueven Internet como herramienta positiva para que toda la gente del mundo se beneficie.
- Ofrece administración y coordinación para las iniciativas estratégicas en curso y los esfuerzos de difusión en el contexto humanitario, educativo, social y en otros contextos

Grandes Objetivos de ISOC

- Desarrollo de Estándares vía IETF
- Desarrollo de Políticas Públicas
- Educación y desarrollo de capacidades

¿Cómo se administra la Internet?

- Algunos datos sobre Internet y su economía
- > 3 mil millones de usuarios
- > 950 millones de sitios web
- Miles de redes autónomas conectadas
- > 284 millones de nombres de dominio registrados (> 120 millones de .com , > 100 millones de ccTLD)
- Los últimos 30 segundos > USD 1,2 millones de dólares gastados en el comercio electrónico

¿Cómo se administra la Internet?

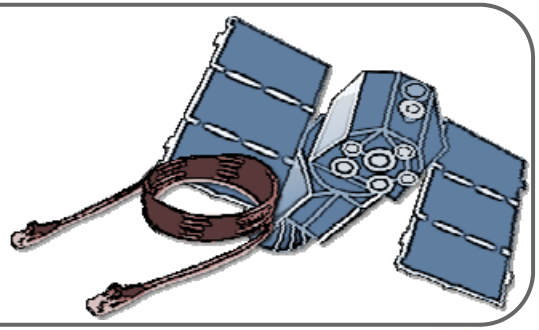
- Ningún organismo de control central (caos?)
- El foco inicial no estaba en control, pero para crear algo que podría crecer a una escala mucho mayor
- modelo de múltiples partes interesadas (apertura, colaboración y toma de decisiones orientado hacia el consenso)
- Los gobiernos, las empresas, la sociedad civil , Comunidad Técnica
- "Poder" se gana por méritos y no de jerarquía
- Eficacia
- Cómo ha crecido y qué tan estable es

Tres Niveles de Operación de Internet

Estándares de contenido y aplicaciones (HTML, XML, Java) - Promueve la creatividad y la innovación en las principales aplicaciones de correo electrónico, la World Wide Web, Wiki, Skype, Twitter, Facebook, Yahoo, Google, YouTube y mucho más.

Protocolos y estándares de Internet (TCP / IP, DNS, SSL) - TCP / IP, controla el flujo de tráfico dividiendo datos de correo electrónico y la web en paquetes antes de su transmisión a través de Internet.

Infraestructura de Telecomunicaiones- Red física formada por cables submarinos, líneas telefónicas, fibra óptica, satélites, microondas, wifi, etc. facilita la transferencia de datos electrónicos a través de Internet**.**



Definiciones de seguridad cibernética

- “La seguridad cibernética se refiere a los métodos preventivos para proteger a la información de ser robada, comprometida o atacada de alguna otra forma”

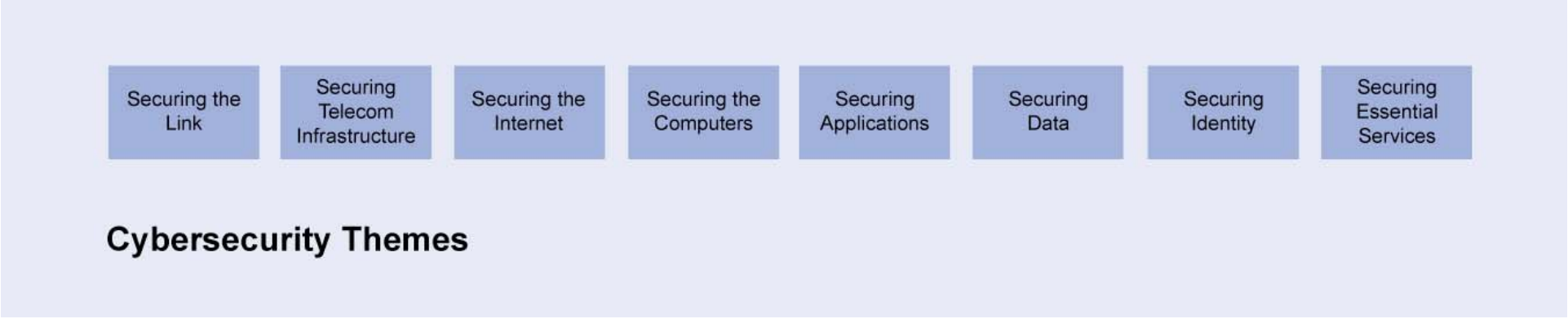
- A los efectos de esta presentación, la seguridad informática se define como: " cualquier cosa que incluya problemas de seguridad específicos en Internet y sus soluciones técnicas y no técnicas”.

- No todos los delitos que se producen en Internet están contenidos en el término seguridad cibernética. Un crimen es un crimen, solo por ejecutarlo mediante Internet no lo hace especial.

Internet Society
InternetSociety.org

Temas de Seguridad Cibernética

- El ámbito de la seguridad cibernética es muy amplio, por lo que es mejor descomponerlo en categorías:



Asegurar el enlace

- Los paquetes de Internet por sí no tienen seguridad.
- Para evitar escuchas no “autorizadas” la información con datos sensibles debe estar encriptada.
- En 2010 Eric Butler, demostró con " Firesheep " que el tráfico no encriptado de FB podría ser espiado en las WiFi públicas
- Formas de realizar la encriptación:
  - A nivel de data link layer(MACSec and Wifi Protected Access);
  - A nivel de IP layer(IPSec);
  - A nivel de application layer(SSL/TLS and SSH etc).

Asegurar las infraestructuras de telecomunicaciones y de Internet

- Tradicionalmente se hace una distinción entre Internet e infraestructuras de telecomunicaciones porque se utilizan diferentes tecnologías y organismos de normalización (UIT -T/IETF)
- Telecomunicaciones (altamente regulada, actores importantes en todos los mercados, los monopolios naturales, etc.) que se centran en la obtención de la red:
  - Localidades (donde se encuentran los “switches” o centrales)
  - Sitios celulares
  - Satélite
  - Instalaciones de transmisión de microondas
- Internet (sin órgano de control central, sistemas abiertos no regulados, construida sobre multiples redes nac./int.)
  - DNS (DNSSEC)
  - Rutas (RPKI)

Asegurar a Internet

Internet se compone de miles de redes todas interconectadas entre si

Los dos elementos críticos son el **DNS** y las **Rutas**

- El DNS
  - DNSSEC (asegura los nombres)

- Las Rutas
  - RPKI (asegura las rutas)

Asegurar a las computadoras

- Siempre que un dispositivo está conectado a Internet, es susceptible de ser atacado.
- Los ataques más exitosos de los hackers, criminales y otros actores maliciosos se realizan contra los servidores y equipos de los usuarios finales.
- Muchas organizaciones instalan firewalls y sistemas de seguridad de punto final o herramientas llamadas "anti-malware“ o "anti-virus"
- ¡Controversia! los propietarios de ordenadores que desean mantener el control sobre sus sistemas y los hackers que quieren estas computadoras y sus datos para sus propios fines.
- ¡No sabemos exactamente el exito de los hackers en sus misiones! ¡Muchos no son reportados!

Asegurar a las computadoras (2)

- Las razones porque los hackers (piratas) quieren controlar los sistemas informáticos han variado con el tiempo.
- Hace 15-20 años era más por puro vandalismo. ¡Hoy se ha convertido en un gran negocio!
- Hoy se extorsiona , roba contraseñas e información financiera (números de tarjetas de crédito), para construir “botnets” que pueden ser utilizados para el envío de spam, cometer fraude, robar la identidad, realizar la ejecución de denegación de servicios en los sitios web específicos, etc.
- Algunas de estas técnicas también se están utilizando, pero en una forma mucho más sofisticada por parte de algunos gobiernos nacionales para el espionaje, la interceptación de las comunicaciones o servicios para otros fines.

Asegurar a las computadoras (3)

- Varias organizaciones están tratando de hacer frente a los retos:
- Las herramientas utilizadas para atacar computadoras incluyen: trojan horses, malware, botnets, phishing, ataques DDoS y man in the middle
  - Compañías de software (Eset, FSecure, Kaspersky , McAfee, Sophos, Symantec y Trend Micro)
  - Empresas enfocando en servidores de seguridad (Check Point Software, Cisco Systems, Juniper Networks , y SonicWALL)
  - Las compañías de hardware (AMD, Intel)
  - IETF

Protección de aplicaciones (1)

- Cualquier aplicación en un dispositivo, como una computadora personal o un teléfono inteligente, conectado y que se comunique a través de Internet es una “aplicación de Internet“.
- Correo electrónico.
- 90% del tráfico de correo electrónico es spam (es una carga para los recursos limitados).
- Protección contra spam realizado por proveedores de software commercial (Barracuda, Cisco / IronPort , McAfee , Proofpoint , Symantec , Trend Micro).
- Empresas como Spamhaus proporcionan listas negras y servicios de reputación.
- Buscadores en la web.

Protección de aplicaciones (2)

- El objetivo principal de los firewalls es proteger tanto a los usuarios de Internet como a los servidores web contra los fallos de seguridad que puedan estar ocultos en la aplicación. Por ejemplo: un tipo de ataque conocido como "inyección SQL" puede ser utilizado contra las aplicaciones web susceptibles de pasar por alto la aplicación y comunicarse directamente con la base de datos detrás de la aplicación.

- Ataques de inyección SQL: cuando tienen éxito, el atacante puede descargar la información de las bases de datos de las aplicaciones web (como nombres de usuarios, direcciones , contraseñas, e incluso números de tarjetas de crédito) o descargar contenido en un sitio web de un usuario desprevenido colocando por ejemplo malwares.

- El W3C está trabajando en la estandarización de aplicaciones

web.

Protección de datos

- Los usuarios de Internet esperan que los datos que envían y reciben sean seguros, por ejemplo: cuando se comunica con su banco, con el gobierno o con el profesional de la salud . En otras situaciones, por ejemplo: el contenido de las entradas en Wikipedia puede no ser seguro en el tránsito.

- La seguridad cibernética en este aspecto se debe dar en el momento de la obtención del dato, durante su tratamiento y almacenamiento.

Protección de identidad

- Desde el comienzo de Internet, se reconoció rápidamente que para muchas aplicaciones comerciales para tener éxito en los mecanismos construidos se necesitaban principios: confianza, gestión de identidades y seguridad para autorizar y autenticar usuarios de Internet.
- Un enlace seguro solo es bueno, siempre y cuando se consideren que los puntos finales sean entidades legítimas que estén autorizadas para llevar a cabo una transacción.
- Hay organizaciones que trabajan en esta área tal como, OASIS , W3C , IETF , etc.

Asegurar los servicios esenciales

- No hay una solución que sirva para todos ("servicios esenciales" deben ser definidos en cada caso).

- Estamos de acuerdo con que los servicios de energía son esenciales por ejemplo.

Cooperación y Colaboración

Tanto los problemas de seguridad cibernética en sí como otras actividades criminales, llevadas a cabo a través de Internet, no se van a resolver con la tecnología por sí sola !!

La estrecha cooperación y coordinación de todos los actores es clave. Seguridad de colaboración !

- Gobiernos,
- Empresas,
- Academia,
- Usuarios individuales y organizaciones,
- Fuerzas del orden,
- Responsables políticos de todo el mundo .


the Internet is for
everyone
Muchas Gracias!
Shernon Osepa
osepa@isoc.org
Internet Society
InternetSociety.org