Reunión de Representantes Técnicos de ARIU

Tendencia en ataques de seguridad en nuestra región

Graciela Martínez – Coordinadora WARP

lacnic

www.lacnic.net

Latin American and Caribbean Network Information Center

LACNIC, el Registro de Direcciones de Internet para América Latina y Caribe

- Es una organización no gubernamental internacional establecida en Uruguay en el año 2002
- Es esponsable de la asignación y administración de los recursos de numeración de Internet (IPv4, IPv6), Números Autónomos y Resolución Inversa, para la región de América Latina y el Caribe
- Coordina el desarrollo de las políticas
- Es uno de los 5 Registros Regionales de Internet en el mundo.

lacnic

¿ Porqué ?

- *"CaaS"* - Los criminales se han enfocado donde está el dinero y están organizados
  - Los estudios muestran que la economía de Internet genera anualmente > $3 Trillones, y se calcula que el cibercrimen se lleva entre 15% y 20%
- El espionaje robo de información confidencial a gobiernos, industrias, etc.
- Descontento con ideologías – *"hacktivismo"* – DDoS, Defacement
- Aprovechan el vacío legal

DDoS – Distributed Denial of Services – Denegación Distribuida de Servicios

Defacement – cambio intencional en página web

Estadísticas según el tipo de incidente

Reportados a WARP

https://warp.lacnic.net/estadisticas/

lacnic

Estadísticas según el tipo de incidente

Gestionados por WARP

https://warp.lacnic.net/estadisticas/

lacnic

Ransomware

Hancock Health pays $47,000 ransom to unlock patient data

Hackers logged into the hospital's remote access portal using a third-party vendor's username and password.

By **Jessica Davis** | January 16, 2018 | 04:01 PM

Fuente: https://www.healthcareitnews.com/news/hancock-health-pays-47000-ransom-unlock-patient-data

lacnic

Botnets más comunes que afectan a recursos de la región

https://warp.lacnic.net/estadisticas/#Tipos_de_Botnet_Regional

lacnic

Botnets más comunes que afectan a recursos de la región

Conficker – 79 %

- Malware de tipo gusano
- Afecta al sistema operativo Windows de Microsoft
- Puede ser utilizado para realizar muchas actividades delictivas – uso prinicipal robo de información y spam

Explota una vulnerabilidad de Windows Server – activo desde 2008 – varios sabores S.O.

Stealrat – 7 %

- Troyano
- Afecta S.O. Windows
- Envío de Spam

https://warp.lacnic.net/glosario/

lacnic

Otros tipos de incidentes

Advanced Persistent Threats

- Malware altamente sofisticado
- Requiere individuos muy calificados, con especialización en diferentes tecnologías
- Recursos financieros
- Utilizados en contra de organizaciones estatales, industriales y militares
- Las técnicas utilizadas para atacar por lo general son “Zero-Day exploit” para la comunidad de seguridad

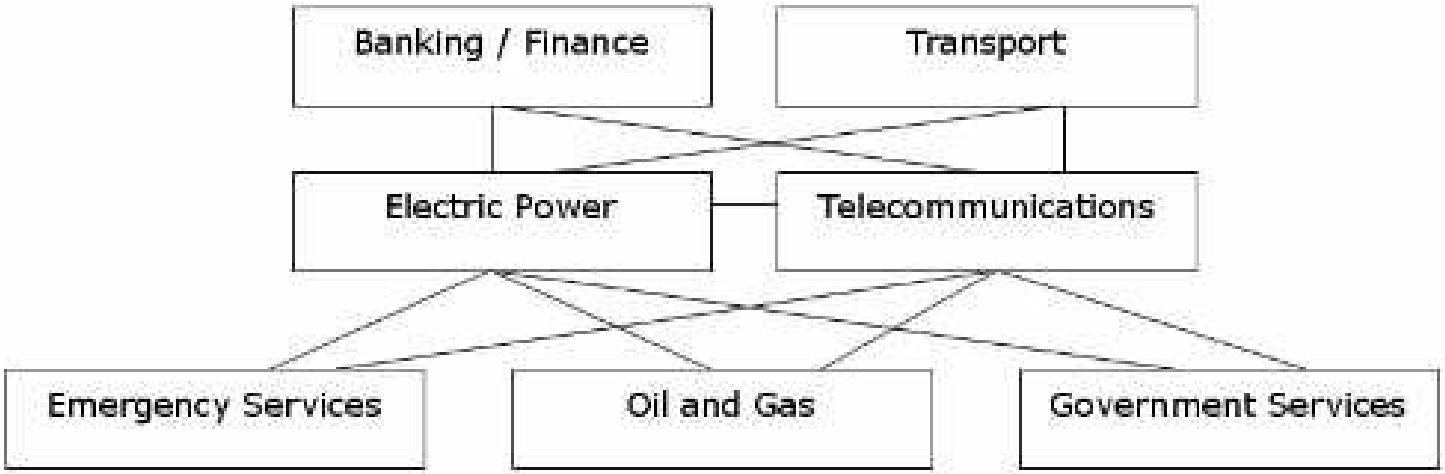
Otros tipos de incidentes

Algunos ejemplos:

- ✓ Red Octobrer - Activo desde Mayo 2007– Detectado en Octubre 2012
  - ✓ Objetivo: recolección de información de agencias diplomáticas, gubernamentales y científicas
- ✓ Stuxnet – Activo Junio 2009 (2005) – Detectado Junio 201
  - ✓ Objetivo: sabotaje (programa nuclear Iraní)
- ✓ Duqu – Activo desde Nov. 2010 – Detectado Set. 2011
  - ✓ Objetivo: espionaje

Ataques a infraestructuras críticas

Azar vs Ataques cruzados



Las fallas o los ataques pueden ser directos o indirectos, es decir resultado de ataques a otras IC.

Existen dependencias entre las IC por lo que deben analizarse todos los escenarios de riesgo

Fuente: Common Threats and Vulnerabilities of Critical Infrastructures -Rosslin John Robles

Algunos Problemas

- Comodidad vs. Seguridad
  - Protocolos inseguros, S.O. Obsoletos
- Medidas de seguridad no adecuadas
- Desarrolladores no toman en cuenta la seguridad desde el diseño
- Falta de implementación de buenas prácticas
  - Ejemplo: BCP 38 – Antispoofing, DNSSEC, RPKI

Algunos problemas

- Usuarios
  - Desconocen los riesgos
    - Exposición a través de terceros – se conoce a alguien que fue victima de hacking, fraude de tarjeta de crédito, etc.
    - Exposición a través de los medios – artículos on-line, series de TV, películas, etc.
  - Muchos no reportan los incidentes de seguridad
- Falta de cooperación entre organizaciones
- Mala legislación – Vacío legal – nacional e internacional
- Muchas veces las medidas se toman despues!
- Falta de percepción del riesgo - no somos conscientes de que tenemos un problema de seguridad

Recomendaciones

- Administración adecuada de patches
  - Sistemas Operativos
  - Aplicaciones
  - Efectos limitados ante Zero-Day exploits, pero previene que nuevos sistemas sean infectados
- Estaciones de trabajo – Hardening de Servidores
- Las redes no están segregadas adecuadamente
- Aplicar políticas de acceso a Internet, por ejemplo utilizando una white list de sitios
- Inspección de tráfico entrante y saliente
- Control del software a instalar y ejecutar en un sistema
- Control de cambios de configuraciones mediantes hashes
- Capacitación de usuarios

Ejes de trabajo

- Preparar a la organización para ser resiliente
  - Plan de continuidad del negocio
  - Capacidad de recuperación
- Mapa de riesgos (posibles, reales)
- Prevención
  - Buen diseño de la arquitectura de red – segregar redes
  - Tests
- Detección
  - Monitorear todo lo que pasa por la red
  - Correalacionar eventos para alertas tempranas
- Respuesta y recuperación
  - Análisis forense
  - Gestión de incidentes – línea estratégica – capacidad de respuesta
  - Gestión de crisis – hay que estar preparados
- ¿Personas? Tenemos que trabajar para generar cultura de seguridad en TI

Dónde reportar un incidente de seguridad informática

- Puntos de reporte: CERTs, CSIRTs

https://warp.lacnic.net/reportar-incidente/

- Comunicación adecuada puede evitar problemas mayores

¡Trabajemos siempre como si estuvieramos comprometidos!

lacnic

Muchas Gracias...

lacnic

www.lacnic.net

gmartinez@lacnic.net