lacnic23
18/22 mayo – lima, perú

LACNIC WARP
Respuesta a Incidentes de Seguridad

A.C. Graciela Martínez Giordano
Responsable WARP
gmartinez@lacnic.net

Iniciativa de respuesta a incidentes de Seguridad

- ¿Cómo surge?
  - Estado del arte de la Seguridad Informática en general
  - Reportes o consultas sin respuestas adecuadas, como por ejemplo:
    - Sospechas de secuestro de rutas
    - Uso de Sistemas Autónomos asignados por LACNIC a empresas que ya no existen
    - Listas de DNS recursivos abiertos
    - Casilla de abuse sin contemplar
  - Decisión de crear la función de respuesta a incidentes de seguridad

Características

A efectos de establecer el modelo para la implementación de la función de respuesta a incidentes de seguridad, se parte de la definición de que debe ser un *equipo coordinador y facilitador* del manejo de incidentes de seguridad informática para los miembros de la LACNIC.

Modelos evaluados

- Modelos :
  - CERT Computer Emergency Response Team (CERT CC – centro de coordinación mundial de problemas de seguridad, creado en 1998 por SEI Softw. Engineering Inst.)
  - WARP Warning, Advice and Reporting Point (Programa creado en 2002 que ahora depende de Centre for the Protection of National Infrastructure de U.K.)

LACNIC WARP

Para dar comienzo fue necesario definir:

- Misión
- Comunidad Objetivo
- Políticas
- Servicios
- Sitio web: www.lacnic.net/web/warp/inicio

Misión y Comunidad objetivo de LACNIC WARP

- Llevar a cabo las funciones de coordinación necesarias para el fortalecimiento de las capacidades de respuesta a incidentes vinculados a las direcciones de Internet de América Latina y el Caribe, en el marco de las metas específicas establecidas por la misión de LACNIC tendientes a lograr el fortalecimiento constante de una Internet segura, estable, abierta y en continuo crecimiento
- La comunidad objetivo está constituida por todas las organizaciones miembros de LACNIC

Autoridad

- LACNIC WARP no tiene autoridad para actuar sobre las operaciones de los sistemas de su comunidad, a excepción de los sistemas internos propios de LACNIC, por lo que no brindará asistencia directa remota ni in situ para la atención de incidentes de seguridad, aun cuando éstos involucren direcciones de Internet de Latinoamérica y el Caribe.

Servicios definidos de LACNIC WARP (I)

- Servicios a prestar por LACNIC WARP
  - Alertas de Seguridad a medida (Filtered Warnings): envío de advertencias de seguridad relevantes para la comunidad
  - Intermediación (Advice brokering): LACNIC WARP provee un ambiente seguro y anónimo de intermediación para la búsqueda, discusión e intercambio de información de incidentes de seguridad y buenas prácticas.

Servicios definidos de LACNIC WARP (II)

- Reporte de incidentes (Reporting Point)
  - LACNIC WARP provee a los miembros un punto de contacto de confianza para el reporte de incidentes de seguridad u otra información sensible.
  - Las organizaciones no miembros también podrán reportar incidentes, LACNIC WARP colaborará para redirigirlos según convenga.
  - El reporte de incidentes podrá realizarse a través de
    - Correo electrónico a la casilla: info@warp.lacnic.net
    - Formulario web: www.lacnic.net/web/warp/form

Camino recorrido

- Desde octubre llevamos considerados mas de 20.000 correos electrónicos - casilla abuse, reportes web y a la casilla de contacto
- Se han gestionado mas de 70 incidentes
- Se realizaron acuerdos de colaboración de intercambio de datos con diferentes organizaciones
- Identificaron trabajos en conjunto para fortalecer la cultura de seguridad en al región.

Tipos de incidentes reportados

Algunos de los tipos de incidentes gestionados:

- Ataques de DDOS utilizando varios tipos de protocolo
  - Open resolvers, Open SNMP, Servidor NTP
  - Causa principal: servidores MAL CONFIGURADOS!
- Phishing
- Ataques de fuerza bruta, Intentos de acceso no autorizado
- Intermediación – anuncios BGP

Otras Actividades

- Foro Lac-csirts
  - ¿Qué es?
  - Procedimiento de ingreso
  - Objetivos: Red de confianza, Compartir información y experiencias y Generar/producir trabajos en conjunto
- Amparo
  - Contribuye a fortalecer la capacidad regional en seguridad informática formando a nuestros miembros para que puedan crear la función de respuesta a incidentes de seguridad.

FIN

¡ Muchas gracias !