LACNIC WARP

Graciela Martinez (graciela @ lacnic.net)

Carlos Martinez (carlos @lacnic.net)

lacnic

LACNIC WARP

- Cómo surge?
  - 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

LACNIC WARP

- Equipo coordinador y facilitador del manejo de incidentes de seguridad **informá**tica para los miembros de la LACNIC
- Sitio web: www.lacnic.net/web/warp/inicio
- En línea con la misión de LACNIC tendiente 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

lacnic

LACNIC WARP - Modelos evaluados

- CERT Computer Emergency Response Team (CERT CC – centro de **coordinación** mundial de problemas de seguridad, creado en 1998 por SEI Software 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.)

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 a prestar por LACNIC WARP

- 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
  - Formularioweb:www.lacnic.net/web/warp/form

LACNIC WARP - 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.

WARP: Tipos de incidentes reportados

- 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.

Muchas gracias!