NACIONAL DE
INVESTIGACIÓN
Y EDUCACIÓN
DEL ECUADOR

e-mail: ernesto.perez@cedia.org.ec
Twitter: @CsirtCEDIA

redcedia
RED NACIONAL DE INVESTIGACIÓN Y EDUCACIÓN DEL ECUADOR

Agenda

¿Quiénes somos?

¿Qué hemos hecho este año?

¿Qué haremos el siguiente año?

¿Qué nos falta por hacer?

Conclusiones

¿Quiénes Somos?

Centro de respuesta a incidentes de seguridad informática (CSIRT)

Brinda servicio a IES miembro del CEDIA

Creado en 2012.

Comenzamos a operar Agosto/2013:

- Emisión de alertas
- Honeypots
- Entrenamiento en seguridad
- Colaboración con IES (y otros)

CSIRT

Prevención:
Auditoría de seguridad.
Entrenamiento y orientación a usuarios.
Diseminación de información relacionada a la seguridad.
Monitoreo de nuevas técnicas de ataque.
Respuesta:
Tratamiento de incidentes y vulnerabilidades.
Mejoramiento de la calidad de servicios de seguridad.
Consultoría en seguridad.
Análisis de Riesgos.
Planeamiento y recuperación de desastres.

Sistemas utilizados

Servidores para emisión de reportes: YARI
Honeypot
VPN para acceso
Sistema para capacitación mediante talleres
Suscripción a feeds para recibir información
- ShadowServer, HideMyAss, Xroxy, netcraft, zone-h, spamcop, teamcymru, cert-br, N6
Mirror SL (adicional)

Qué hemos hecho 2015?

Activado sitio web con información de interés
http://csirt.cedia.org.ec
Implementar feeds: netcraft, TeamCymru, n6
Emisión informes de revisión a universidades
Instalación honeypot smtp colaboración con CERT.br
Participación en conferencias exponiendo labor.
Infoday: UTA, ESPE, UIDE, UTC, UTN, UEB

Qué hemos hecho 2015?

Se emiten reportes de vulnerabilidades en SSL
Implementación de avisos por:
- portmapper/ssdp/snmp abiertos

Taller en evento de seguridad en UDA

Contacto con CERT-US para análisis de malware

Atención a mirror de SL

Qué hemos hecho 2015?

En CEDIA hemos logrado llegar a tener:

0 open resolvers

0 open ntp

0 open snmp

0 open proxies

¿Qué faltó?

Persisten los problemas con

- portmappers abiertos,
- ssl configurados con encriptación débil,
- ssdp
- botnets

¿Qué haremos el 2016?

DNS de cache para miembros del CEDIA con protecciones anti-botnets.

Acuerdo para implementar sensores creados por CAIS-RNP.

Almacenamiento de sitios web para análisis de evolución en el tiempo.

Qué nos falta por hacer

Adherirnos al FIRST

Implementar reportes de eventos ocurridos desde nuestras redes (sensores de CAIS)

Finalizar sistema YARI de manejo de eventos

Conclusiones

El CSIRT tiene una actividad interesante, creciendo con el tiempo.

En 2016 tengamos un conocimiento mayor de la red y aumenten los eventos reportados.

Con la creación de la ESR pueda comenzarse una nueva etapa trabajando la mayor falencia que que es el conocimiento apropiado del personal informático de las redes del país.

Conclusiones

CSIRT CEDIA
Ernesto Pérez Estévez
ernesto.perez@cedia.org.ec
+593 9 9924 6504