Creación de un CSIRT

- CSIRT: Computer Security Incident Response Team (Equipo de Respuesta a Incidentes de Seguridad Informática)
- Un ”CERT” es un CSIRT pero el término “CERT” es una marca registrada por Carnegie Mellon University.
- CMU autoriza el uso de “CERT” a los CSIRTs nacionales, usualmente.

Algo de terminología

- ***EVENTO***: Para la ciencia, un evento es un fenómeno (un hecho observable en un momento dado) o un acontecimiento que ocurre en una posición y momento determinados.(definicion.de)
- ***EVENTO DE SEGURIDAD INFORMATICA***: Es una ocurrencia identificada de un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información o la falla de medidas de seguridad (safeguards), o una situación previamente desconocida que pueda ser relevante para la seguridad. [ISO 18044]

Algo de terminología II

- *Ejemplos de evento*: Un usuario se conecta a un sistema, un intento fallido de un usuario para ingresar a una aplicación, el firewall que permite o bloquea un acceso, una notificación de un cambio de contraseña de un usuario privilegiado, etc.
- Un Evento de Seguridad Informática **no** es necesariamente una ocurrencia maliciosa o adversa. (agesic.gub.uy)

Algo de terminología III

- ***INCIDENTE***: Cosa que sobreviene en el curso de un asunto, negocio o juicio y tiene con él alguna relación.(wordreference.com)
- ***INCIDENTE*** (según ITIL): Cualquier evento que no forma parte del desarrollo habitual del servicio y que causa, o puede causar una interrupción del mismo o una reducción de la calidad de dicho servicio.(wikipedia.org)

Algo de terminología IV

- ***INCIDENTE DE SEGURIDAD INFORMÁTICA***: Es la violación o amenaza inminente a la violación de una política de seguridad de la información implícita o explícita. También es un incidente de seguridad un evento que compromete la seguridad de un sistema (confidencialidad, integridad y disponibilidad).
- Un incidente puede ser denunciado por los involucrados, o indicado por un único o una serie de eventos de seguridad informática. [NIST800-61, ISO 18044]. Ejemplos de Incidentes Informáticos: Acceso no autorizado, robo de contraseñas, robo de información, denegación de servicio, etc.

Algo de terminología V

- ***RESPUESTA A INCIDENTES***: Es una reacción acelerada a un problema. Con respecto a la seguridad de la información, un ejemplo sería las acciones del equipo de seguridad en contra de un hacker que ha penetrado un cortafuegos y está actualmente huzmeando el tráfico de la red. El incidente es la violación de la seguridad. La respuesta depende de cómo el equipo de seguridad reaccione, qué acciones toman para reducir los daños y cuándo reestablecen los recursos, todo esto mientras intentan garantizar la integridad de los datos. (mit.edu)

Algo de terminología VI

- ***Y "MANEJO DE INCIDENTES"***?

- ***RESPUESTA vs. MANEJO***: Respuesta a Incidentes es el conjunto de componentes técnicos requeridos para analizar y contener un incidente. Manejo de Incidentes son las funciones de logística, comunicaciones, coordinación y planificación necesarias para resolver un incidente en una manera calma y eficiente. (sans.edu)

Algo de terminología VII

- ***COMUNIDAD OBJETIVO*** (*Constituency*): Es aquel grupo de personas, sistemas u organizaciones para quienes se prestará el servicio de gestión de incidentes. (agesic.gub.uy)

- ***GESTION DE INCIDENTES***: Los servicios de gestión de incidentes de seguridad de la información, están destinados a prevenir, detectar y solucionar incidentes de seguridad que atenten contra la confidencialidad, disponibilidad, integridad ó autenticidad de la información, como es el caso de un incidente ocasionado por un código malicioso, un acceso no autorizado, una denegación de servicio o un uso inapropiado de los sistemas informáticos de la organización. (inteco.es)

Ahora sí, a nuestro tema!

Funcionamiento de un CSIRT

Francisco NEIRA BASSO fneira@defensoria.gob.pe
Encargado de Seguridad de la Información
Defensoría del Pueblo

Funcionamiento de un CSIRT

- Qué es un CSIRT?
- Qué es el PE-CERT?
- Marco legal y normativo
  - RM creando el PE-CERT
  - RM 129-2012-PCM de la 27001
- Cómo funciona un CSIRT?
- Cómo protege un CSIRT al Estado y al ciudadano?
- Quiénes tienen CSIRTs?

Funcionamiento de un CSIRT

- Funciona como una “estación de bomberos” de incidentes informáticos.
- Recibe llamados de instituciones atacadas por hacktivistas, analiza la modalidad del ataque y propaga la alerta a las demás instituciones
- Coordina con las fuerzas de la Ley, particularmente con la rama especializada: DIVINDAT o con FFAA
- Coordina con otros CSIRTs nacionales y extranjeros
- También puede realizar labor proactiva: Creando conciencia a la ciudadanía sobre ataques, estafas informáticas, privacidad de la información personal, etc.

El CSIRT en acción

1. **La institución es atacada**
2. **El ataque es detectado y reportado**
3. **Se notifica a los demás miembros y a las fuerzas del orden**

Funcionamiento de un CSIRT

PE-CERT es la *"Coordinadora de Respuestas a Emergencias en Redes Teleinformáticas"*

- A cargo de la ONGEI
- Creada con la RM 360-2009-PCM 19 Agosto 2009
- Por ser un CSIRT de alcance nacional, está autorizado por SEI-CMU a usar **"CERT"** en su nombre

Funcionamiento de un CSIRT

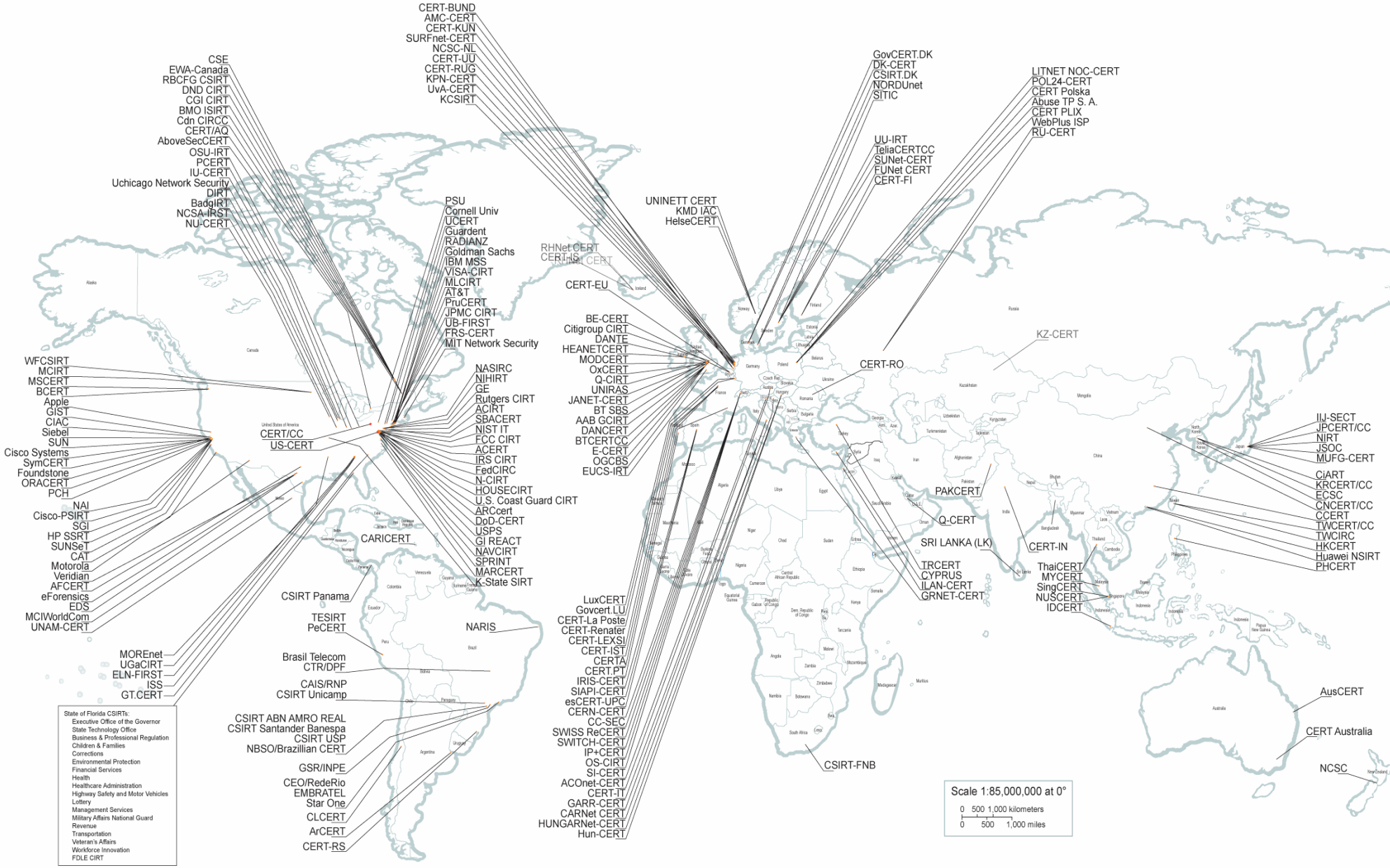
Un CSIRT tiene un “Catálogo de Servicios” según su madurez y sus recursos humanos y materiales

Servicios básicos son los de coordinación en su comunidad objetivo y con los proveedores de servicios Internet

Un CSIRT puede coordinar con otros CSIRTs para intercambiar información de ataques, análisis de “malware”, contramedidas, etc.

Incident Response Teams Around the World

International cooperation speeds response to Internet security breaches.



Guías para crear un CSIRT I

- Documento “Creación de Equipo de Respuesta a Incidentes de Seguridad Informática
- Grupo de alumnos entusiastas y con voluntad tanto de aprender como de hacer bien.
- Al menos un par de docentes con conocimientos de redes y de desarrollo (y también con mucho entusiasmo)

Guías para crear un CSIRT II

- Es mejor comenzar ofreciendo servicios sencillos hasta dominarlos y luego ampliarlos.
- La curiosidad y las ganas de aprender son fundamentales
- La confianza de la comunidad objetivo es clave. Si la perdemos, todo se vendrá abajo.

Guías para crear un CSIRT III

- Una vez que el equipo demuestre su solvencia técnica básica, podrá ampliar su cobertura y ofrecer sus servicios al resto de la Universidad, no solamente a la Escuela.
- Si se promueve la idea y el CSIRT demuestra con métricas que funciona bien, podrá crecer en número, en capacidades técnicas y ampliar su comunidad objetivo.
- Y por qué no al Parque Tecnológico?? ;-)