4a sesión – Vigilancia, precaución y respuesta a incidentes

Taller Regional sobre Marcos para la Ciberseguridad y la Protección de la Infraestructura básica de la Información

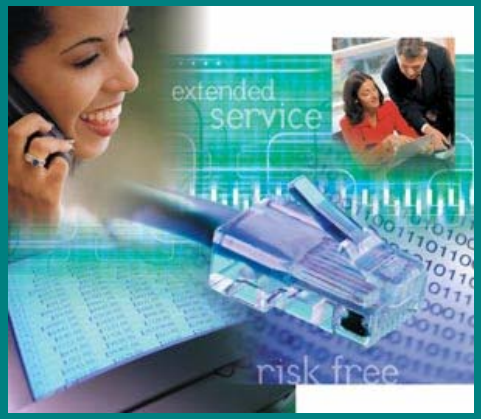
16 de octubre de 2007

Fred L. Clark, M. Sc. – Delegado de la Superintendencia de Telecomunicaciones ante el Comité Coordinador CSIRT-gt

CSIRT-gt

El Equipo de Respuesta a Incidentes de Seguridad Informática de Guatemala

16 de octubre de 2007



Antecedentes

- Las distintas instituciones de gobierno cuentan con redes telemáticas en las que se integran personas, equipo informático e información.
- Estas redes se encuentran conectadas a la Internet, una red pública en la cual existe un alto riesgo de ser víctima de ataque o de exponer alguna vulnerabilidad.
- Ante esta situación es importante desarrollar una estrategia que aumente los niveles de seguridad de las redes.

Antecedentes

- ¿Qué es un CSIRT?
- Necesidad de su creación (para que?);
- Historia;
- Equipo Coordinador y equipo nacional;
- Reuniones;
- Productos;
- Capacitaciones;

¿Qué es un CSIRT?

- El acrónimo responde a “Computer Security Incident Response Team”.
- Se refiere a una unidad de observación y alerta que está activa 24 horas al día, los 7 días de la semana, que responde a situaciones de crisis, incidentes y amenazas a la seguridad informática.
- Un componente clave de un CSIRT es el actuar como un “sistema de observación y alerta”.

¿ Para que un CSIRT?

- Es esencial para reducir la vulnerabilidad a un ataque, mitigar el daño y asegurar la integridad de las redes telemáticas en cada país.
- Amenazas:
  - DOS (negación de servicio);
  - Intrusión;
  - Ataque;
  - Virus y código malicioso;
  - Fraudes.

¿Cuál es su ámbito de trabajo?

- Un CSIRT provee servicios a comunidades de redes telemáticas bien definidas, pudiendo ser éstas de carácter gubernamental, nacional, regional o privadas, teniendo como valor agregado que éstas redes pueden integrarse dentro de un CSIRT nacional o regional; contribuyendo cada una de acuerdo a su especialización.
- i.e. entidades financieras, mercado de valores, operadores de telecomunicaciones

Objetivo

- Reducir la vulnerabilidad de las redes telemáticas de los países;
- Ser el punto de referencia de incidentes de seguridad;
- Tener el conocimiento para recuperar una red que ha sido o esta siendo atacada;
- Capacitar y formar personal de las distintas instancias para prevenir problemas y proteger los recursos.

Antecedentes en América

- *A principio de los años 1,990, con motivo de diversos actos terroristas ocurridos en el continente americano, se llevaron a cabo una serie de reuniones en el seno de la Organización de Estados Americanos (OEA), en las que las naciones americanas se comprometieron a "prevenir, combatir y eliminar el terrorismo", entre ellas la Primer Cumbre de las Américas, en 1994; la Primer Conferencia Especializada en Terrorismo, celebrada en Lima en 1996; y una Segunda Conferencia Especializada en Terrorismo, celebrada en Mar del Plata en 1998.*

Antecedentes en América

- *Esta última finalizó con la adopción del llamado Compromiso de Mar del Plata, en el cual se estableció, por parte de la OEA, el "Comité Interamericano contra el Terrorismo" (CICTE), AG/RES. 1,650 del 7 de junio de 1999; cuyo propósito es desarrollar la cooperación a fin de prevenir, combatir y eliminar los actos y actividades terroristas en los países del continente americano.*

Antecedentes en América

- *Posteriormente, en la cuarta sesión plenaria de Asamblea General de la OEA, celebrada el 8 de junio de 2004, AG/RES.2010 (XXIV-O/04), se adoptó el Estatuto del CICTE, el cual, en el Artículo 13 lista sus funciones; entre las cuales están:*
- *a) Promover el desarrollo de la cooperación entre los Estados Miembros para prevenir, combatir y eliminar el terrorismo;*

Información general

- Guatemala, nación de 108 mil km2, situada en la parte norte de Centroamérica.
- Su población estimada a diciembre 2006 era 13,074,862 habitantes. Pobreza: 54%;
- Teléfonos fijos: 1,354,926 td: 10/100 hab;
- Móviles: 7,178,745 td: 55/100 hab;
- Operadores de Red Local:18; OPI: 21
- Operadores de Móviles: 3;
- Operadores de Internet: más de 18.
- Conexiones de BA: 84,000; Dial Up 134,000

El caso guatemalteco, historia

- El CSIRT-gt nació a instancias de la convocatoria del Comité Interamericano de Lucha contra el Terrorismo, CICTE, quien invitó a los países que integran la OEA a conformar sus Equipos de Respuesta a Incidentes de Seguridad Cibernética (Computer Security Incident Response Team, CSIRT), para combatir amenazas a la seguridad cibernética.

historia

- El Ministerio de Relaciones Exteriores ha facilitado el proceso de conformación del Equipo Nacional, por lo que desde junio del 2006 comenzó a convocar a diversas instituciones públicas, privadas y académicas, para diseñar y cumplir con un plan de trabajo que permitiera seguir los pasos básicos de creación del CSIRT remitidos por el CICTE.
- Recomendación: Metodología de la Universidad Carnegie Mellon

El año pasado…

- Entre junio y noviembre del 2006 se realizaron alrededor de 12 reuniones las cuales al final permitieron que con el apoyo de la Superintendencia de Telecomunicaciones, el Clúster de Tecnologías de la Información, el Ministerio de la Defensa Nacional y el resto de entidades públicas y privadas se completara una primera etapa en la que se definió el contenido y ámbito de aplicación; así como la nominación oficial del Equipo Nacional ante el Comité Interamericano contra el Terrorismo.

Este año . . .

- Continuaron las reuniones, pero únicamente 4 personas, representando el MINEX, MINDEF, SIT y el CTI de Agexport.
- Se participaron en 2 seminarios taller:
  - Costa Rica, crímenes cibernéticos
  - Brasil, taller formación de CSIRT nacionales

Integración del CSIRT-gt

- Clasificación de las Organizaciones que integran al CSIRT-GT;
- Grupo Coordinador;
- Consejo Consultivo;
- Organización CSIRT-GT;

Clasificación de las organizaciones

- Instituciones gubernamentales del Organismo Ejecutivo y Judicial, entre ellas entidades autónomas y descentralizadas, secretarías; asociaciones civiles que agrupan diversos sectores de la iniciativa privada, organizaciones no gubernamentales sin fines de lucro, universidades y Operadores de Red de Servicio de Internet.
- Con el fin de ampliar la participación de este comité, próximamente se invitará a participar al Organismo Legislativo y a representantes del sector privado organizado.

Comité Coordinador

- Ministerio de Relaciones Exteriores;
- Superintendencia de Telecomunicaciones;
- Ministerio de Defensa Nacional;
- Clúster de Tecnologías de la Información y Comunicación, adscritas a Agexport (iniciativa privada).

Consejo Consultivo

- Ministerio de Defensa Nacional;
- Procuraduría General de la Nación (Sector Justicia);
- Universidad del Valle de Guatemala;
- Universidad Rafael Landívar;
- Clúster de Tecnologías de la Información y Comunicación de Guatemala de Agexport (Representante del sector privado)
- Secretaría General de Planificación y Programación de la Presidencia de la República (SEGEPLAN);
- Superintendencia de Telecomunicaciones;
- Superintendencia de Bancos;
- Consejo Nacional de Ciencia y Tecnología;
- Comisión Portuaria Nacional;
- COPRE para la modernización del estado;
- Ministerio de Gobernación (Policia, presidios, migración);
- OSI/INSTARED (Operador de Red de Internet);
- Superintendencia de Administración Tributaria (Impuestos y aduanas);
- Ministerio de Relaciones Exteriores.

Diagrama esquemático

Productos y logros

- Elaboración de la Misión y Visión del Comité;
- Organización del Comité;
- Elaboración de Reglamentos;
- Clasificación de Incidentes Informáticos;
- Estudio sobre la Ley Guatemalteca y los delitos de carácter informático.

Productos y logros

- Conformación de los integrantes del equipo nacional;
- Participación en foros internacionales;
- Reconocimiento del CICTE-OEA a los integrantes del CSIRT-gt como los participantes oficiales;
- Elaboración de 2 borradores de proyecto para obtener financiamiento para la puesta en marcha del CSIRT-gt.

Participación Internacional

- Costa Rica: Taller regional sobre Seguridad Informática y Delitos Informáticos.

- Brasil: Curso Básico para la Creación y Gerenciamiento de un Equipo de Respuesta a Incidentes de Seguridad Informática.
  - Participación en el acuerdo de colaboración entre los CSIRTS Interamericanos, llamado ***Carta de Brasilia***.

Comité Consultivo

- Participación del Equipo Consultivo: son los nombrados por su entidad para ser parte del CSIRT y reconocidos por el CICTE *(OEA).*
  - Colaboración con el Comité Coordinador;
  - Capacitación en Actividades CSIRT-gt;
  - Integrar Comisiones;
    - Legislativa, Divulgación, Técnica;
  - Presentar Mociones;
  - Ser un punto de Enlace;

Próximos pasos

- Finalización de propuestas de financiamiento para la puesta en marcha del CSIRT-gt;
- Presentación de propuestas a las agencias de cooperación;
- Preparación de agenda de trabajo para el próximo año;

Próximos pasos

- Invitar a otras organizaciones a formar parte del Comité Consultivo;
- Realizar gestiones para poder llevar a cabo talleres de capacitación al personal de las instituciones participantes;
- Desarrollo y fortalecimiento de destrezas técnicas y forenses;
- Elaborar propuestas de reformas a leyes del país.

Vulnerabilidades

October 3, 2007 -- Updated 1823 GMT (0223 HKT)

EMAIL SAVE PRINT

Lawmaker shows naked woman during school lecture

STORY HIGHLIGHTS

- Rep. Matthew Barrett giving civics lesson when computer shows topless woman
- Police confiscated memory stick, are investigating source of image
- Technology director says stick contained catalog of nude images, civics lesson
- Barrett: Memory stick was gift from legislative liaison for state library

Next Article in U.S. »

TEXT SIZE

NORWALK, Ohio (AP) -- A state legislator surprised a high school class when the computer he was using projected a photo of a nude woman during a lecture on how a bill becomes a law.

State Rep. Matthew Barrett was giving a civics lesson Tuesday when he inserted a data memory stick into the school computer and the projected image of a topless woman appeared instead of the graphics presentation he had downloaded.

Police interviewed Barrett and school officials and seized the data memory stick and the computer to determine where the image came from, a state highway patrol spokesman said.

Barrett said there were a few snickers from the approximately 20 students in the senior government class at Norwalk High School when the image appeared. He said he immediately pulled the memory stick out of the computer.

The legislator said he finished his lecture using printouts and then met with the school's principal and technology staff, who examined the stick. He said the school's technology director determined the stick had a directory of nude images in addition to Barrett's presentation on civics lessons.

"I have no idea where these came from," the Democrat said.

Barrett said the data memory stick was a gift he received about three weeks ago from a legislative liaison from the state Library of Ohio. E-mail to a friend

Vulnerabilidades

RECENT NOTABLE CYBER DEVELOPMENTS

Within the last 90-days there have not been any notable cyber events originating in Saudi Arabia. While it appears that there is some concern for Internet security in the Middle East,[13] the last incident reported that included Saudi Arabian hackers was in June 2003 when a group of Saudis hacked into cell phones and ran up significant long distance telephone usage charges.[14] Further research showed that this type of hack was not a difficult one, and the hack appears to have become sensational with mainstream media. This is apparently because some of the victims were Americans and the incident sparked a class-action lawsuit against AT&T, who maintained that its customers were responsible for the thousands of dollars that were charged to their accounts.

The US State Department has issued no warnings or travel inputs for the past 90 days for Saudi Arabia. Their last warning, however, issued in May 2005, remains in effect. *"Due to concerns about the possibility of additional terrorist activity directed against American citizens and interests, the Department of State continues to warn U.S. citizens to defer non-essential travel to Saudi Arabia…. the Department of State continues to warn American citizens to defer non-essential travel to Saudi Arabia due largely to targeted attacks against American citizens that have resulted in deaths and injuries. There have been a number of anti-Western attacks in Saudi Arabia since May 2003."*

ANALYSIS

Muchas gracias por su atención

fclark@sit.gob.gt

fclark@intelnett.com