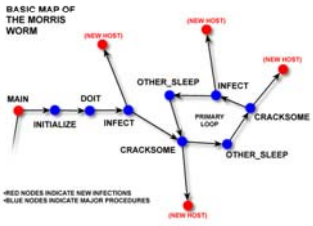
Respuesta a incidentes

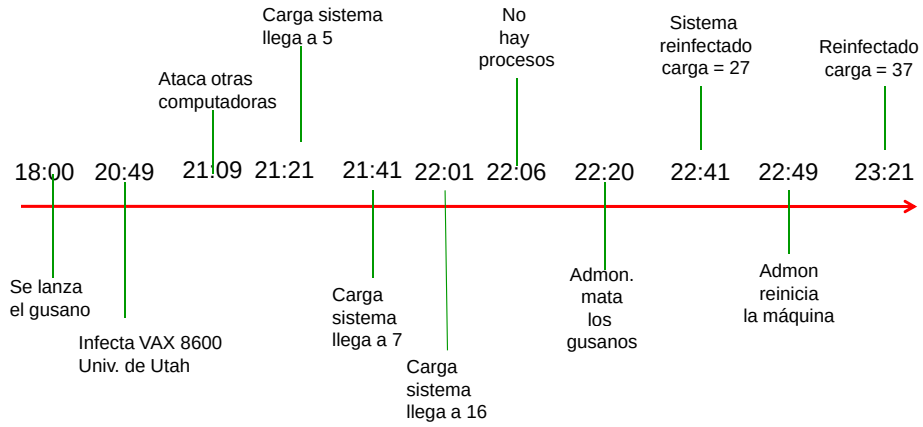
Roberto Gómez Cárdenas
ITESM-CEM
rogomez@itesm.mx
http://homepage.cem.itesm.mx/rogomez

Erase una vez…

- ¿Qué hacia en la tarde del 2 de noviembre de 1988?



¿Qué paso?



Carga: Medida de que tan duro esta trabajando la máquina. A las 21:30, la carga usualmente era de 1. Cualquier carga mayor de 5 provoca retrasos en el procesamiento de datos.

Lámina 3 Dr. Roberto Gómez Cárdenas

Consecuencias

- Lo mismo ocurre con 6,000 máquinas a través del país.
- Ningún daño físico.
- Perdidas entre 100,000 y 10,000, 000 debido a la perdida de acceso a internet.

Lámina 4 Dr. Roberto Gómez Cárdenas

¿Y qué se hizo?

Lámina 5 Dr. Roberto Gómez Cárdenas

¿Y en México?

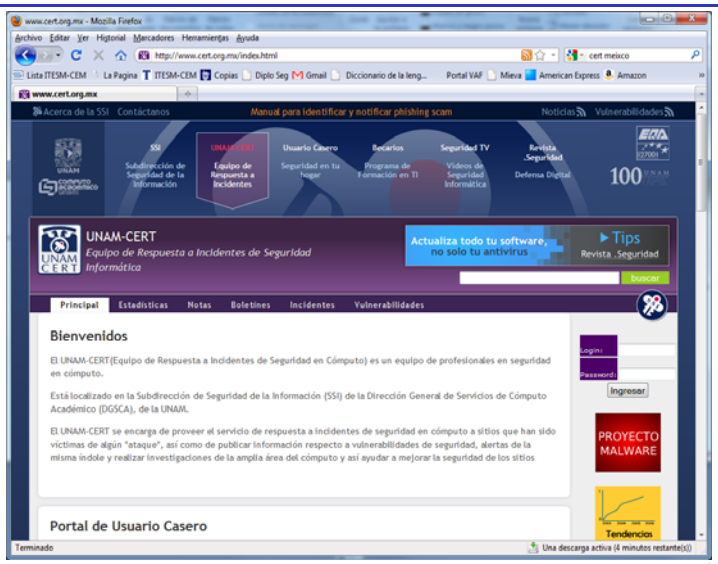


Lámina 6 Dr. Roberto Gómez Cárdenas

Incidente informático

- Incidente de seguridad computacional (o simplemente incidente) es cualquier evento que es una violación implícita o explícita de las políticas.
- Significa el intento, exitoso o no, de acceso no-autorizado, uso, divulgación, modificación o destrucción de información o interferencia con la operación de un sistema de información.

Lámina 7 Dr. Roberto Gómez Cárdenas

Tipos de incidentes

- Robo de propiedad intelectual.
- Pornografía infantil.
- Fraude
- Distribución de virus.
- Denegación de Servicios
- Extorsión.
- Estafa.
- Acceso no autorizado.
- Robo de servicios.
- Abuso de privilegios

Lámina 8 Dr. Roberto Gómez Cárdenas

Incidentes de Seguridad ocurridos en los últimos años

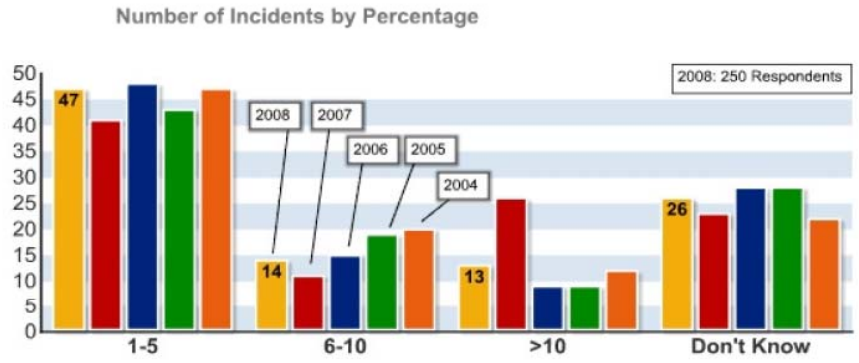


Lámina 9 Dr. Roberto Gómez Cárdenas

Incidentes de seguridad experimentados en los últimos 2 años

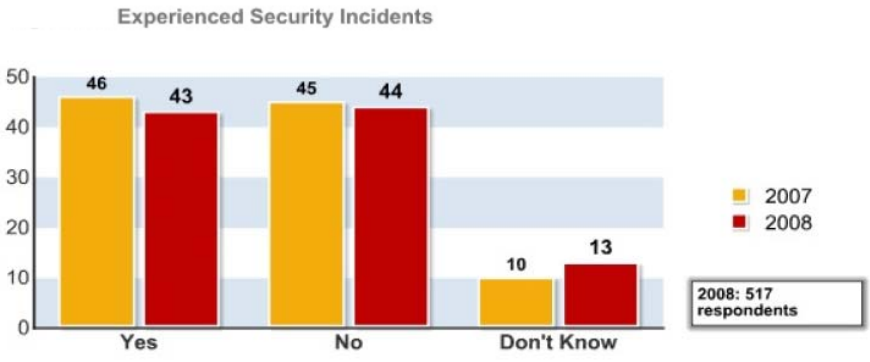
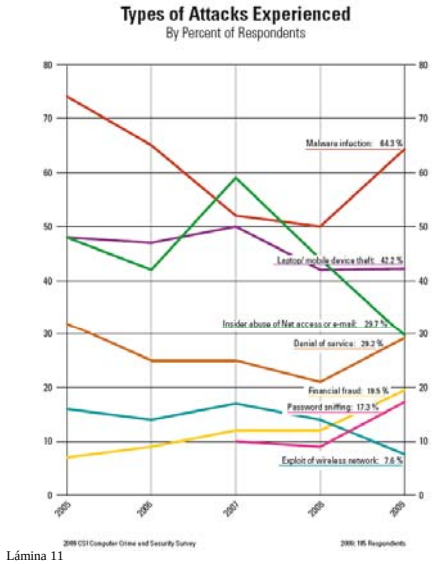


Lámina 10 Dr. Roberto Gómez Cárdenas

Porcentaje de tipos de ataque experimentados por las organizaciones



Types of Attacks Experienced
By Percent of Respondents

Type of Attack	2005	2006	2007	2008	2009
Malware infection	74%	65%	52%	50%	64%
Bots / zombies within the organization	added in 2007		21%	20%	23%
Being fraudulently represented as sender of phishing messages	added in 2007		28%	31%	34%
Password sniffing	added in 2007		10%	9%	17%
Financial fraud	7%	9%	12%	12%	20%
Denial of service	32%	25%	25%	21%	29%
Extortion or blackmail associated with threat of attack or release of stolen data	option added in 2009				3%
Web site defacement	6%	6%	10%	6%	14%
Other exploit of public-facing Web site	option altered in 2009				6%
Exploit of wireless network	16%	14%	17%	14%	8%
Exploit of DNS server	added in 2007		6%	8%	7%
Exploit of client Web browser	option added in 2009				11%
Exploit of user's social network profile	option added in 2009				7%
Instant messaging abuse	added in 2007		25%	21%	6%
Insider abuse of Internet access or e-mail (i.e. pornography, pirated software, etc.)	48%	42%	59%	44%	30%
Unauthorized access or privilege escalation by insider	option altered in 2009				15%
System penetration by outsider	option altered in 2009				14%
Laptop or mobile hardware theft or loss	48%	47%	50%	42%	42%
Theft of or unauthorized access to PII or PHI due to mobile device theft/loss	option added in 2008			8%	6%
Theft of or unauthorized access to intellectual property due to mobile device theft/loss	option added in 2008			4%	6%
Theft of or unauthorized access to PII or PHI due to all other causes	option added in 2008			8%	10%
Theft of or unauthorized access to intellectual property due to all other causes	option added in 2008			5%	6%
2009 CSI Computer Crime and Security Survey				2009: 185 Respondents	

Lámina 11 ez Cárdenas

Uso de pólizas de seguros para administrar riesgos de seguridad cibernéticos

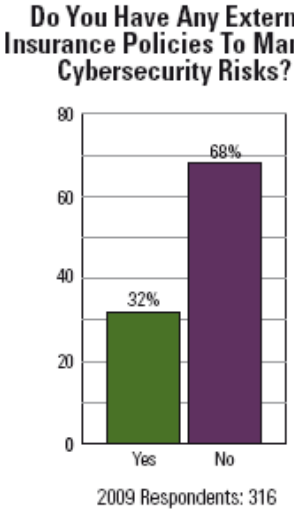
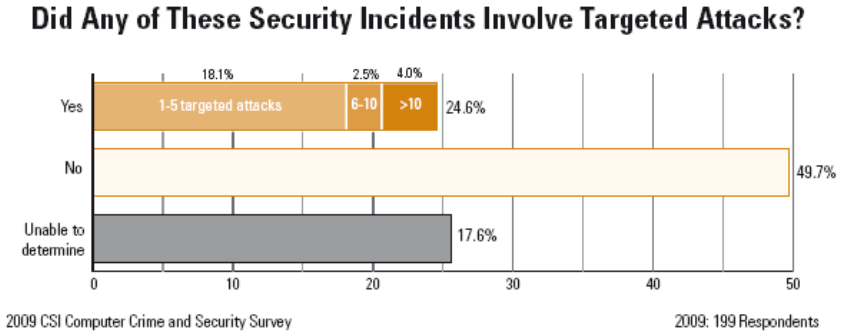


Lámina 12 Dr. Roberto Gómez Cárdenas

Porcentaje de incidentes de seguridad envueltos en blancos de ataques



"Only amateurs attack machines; professionals target people", B. Schneier

Lámina 13 Dr. Roberto Gómez Cárdenas

Porcentaje esperado de incidentes en sitios Web

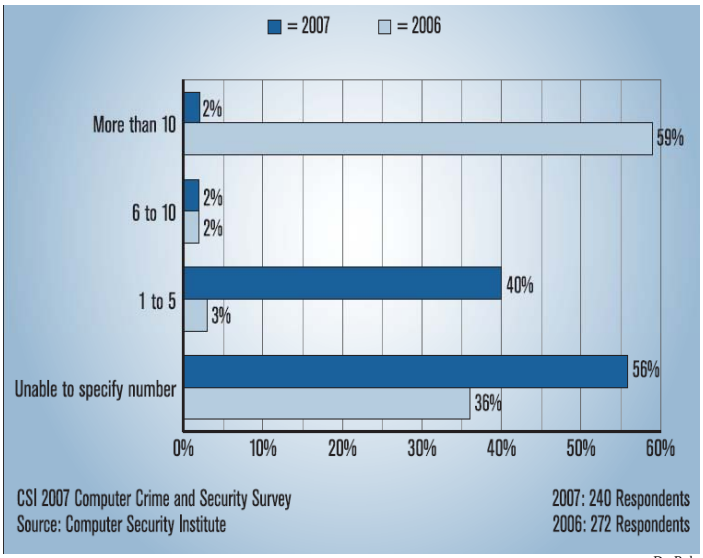


Lámina 14 Dr. Roberto Gómez Cárdenas

Cantidad estimada de pérdida por respuesta a incidentes

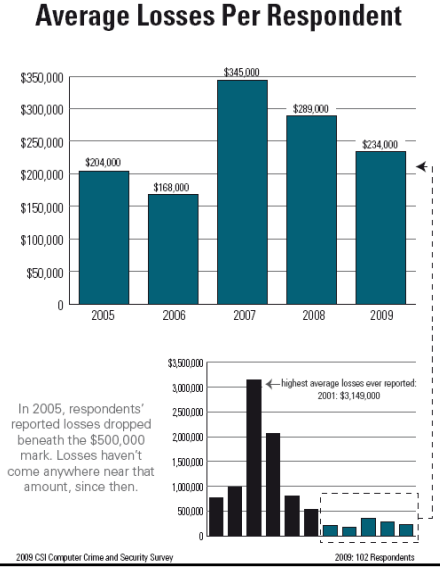


Lámina 15 Dr. Roberto Gómez Cárdenas

Cantidad estimada de pérdida por tipo de incidente

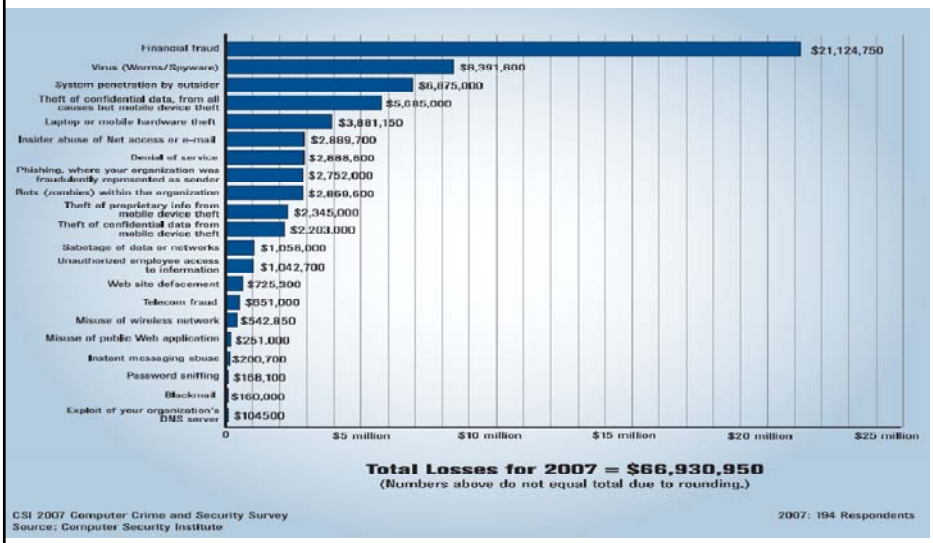


Lámina 16 Dr. Roberto Gómez Cárdenas

Porcentaje de pérdidas causadas directamente por incidentes de seguridad

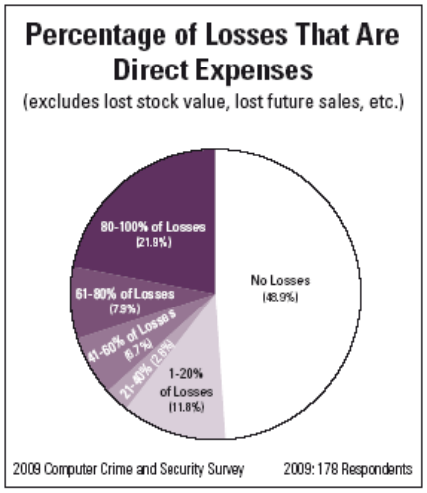


Lámina 17 Dr. Roberto Gómez Cárdenas

Porcentaje de perdidas debido a usuarios internos

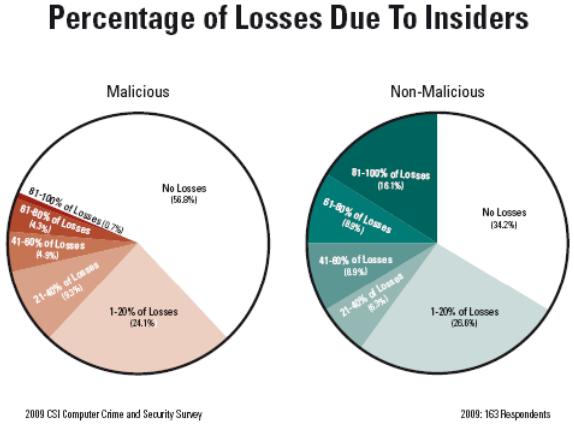


Lámina 18 Dr. Roberto Gómez Cárdenas

Acciones tomadas por las organizaciones después de un incidente de seguridad

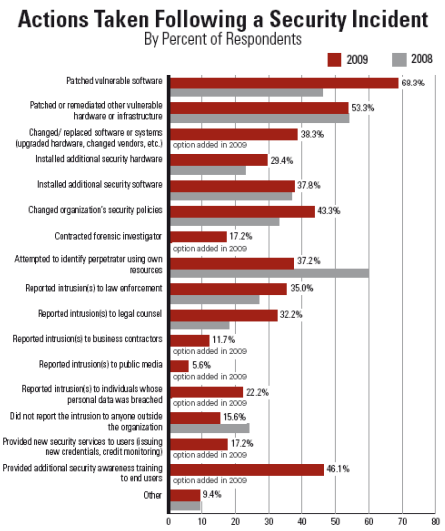


Lámina 19 2009 CSI Computer Crime and Security Survey 2009: 180 Respondents Dr. Roberto Gómez Cárdenas

A evitar

Lámina 20 Dr. Roberto Gómez Cárdenas

Respuesta a incidentes

- Un enfoque organizado para llevar a cabo las acciones necesarias después de que se detecto un incidente de seguridad.
- Objetivo
  - Manejar la situación de tal forma que se limiten los daños y se reduzca el tiempo de recuperación y costos.
- ¿Qué abarca?
  - Incluye una política que define, en términos específicos, lo que constituye un incidente y proporciona un proceso paso-a-paso de lo que debe hacerse cuando ocurre un incidente.

Lámina 21 Dr. Roberto Gómez Cárdenas

Respuesta incidentes y forencia digital

- Uno de los menos practicados, más estresante
- Cada incidente es único y puede involucrar diferentes áreas de la organización afectada.
- Analistas de incidentes deben ser capaces de pensar rápido, permanecer calmados y considerar todas las posibilidades.

Lámina 22 Dr. Roberto Gómez Cárdenas

Pasos manejo incidentes

- De acuerdo al SANS existen seis pasos dentro del manejo de incidentes
  - Preparación
  - Identificación
  - Contención
  - Erradicación
  - Recuperación
  - Lecciones aprendidas

Lámina 23 Dr. Roberto Gómez Cárdenas

Preparación

- La clave para una respuesta exitosa es la preparación
  - Formar una estrategia
  - Diseñar un procedimiento
  - Reunir recursos
  - Practicar, practicar, practicar

Lámina 24 Dr. Roberto Gómez Cárdenas

Preparación

- Identificar el equipo base
  - Personal técnico de TI
  - Administrativo
  - Legal
  - Forensia
  - Relaciones públicas
  - Seguridad física y mantenimiento
  - Telecomunicaciones

Lámina 25 Dr. Roberto Gómez Cárdenas

Preparación

- Organización del equipo
  - Todos los miembros del equipo de CSIRT deben conocer su rol y como interactuar con los otros miembros del equipo.
  - Miembros no pertenecientes a la organización (outsourcing) deben contar con contratos actualizados y firmados.
  - Deben conocerse los contactos con las autoridades legales y su involucración en el incidente debe ser discutida.

Lámina 26 Dr. Roberto Gómez Cárdenas

Preparación

- Desarrollar un procedimiento
  - La respuesta a incidente puede ser muy estresante.
    - Un procedimiento documentos, fácil de seguir, puede reducir la ansiedad del momento.
  - Desarrollar procedimientos de llamadas y procedimientos de notificación
  - Lluvia de ideas para posibles escenarios.
  - Identificar información general necesario en la mayor parte de los escenarios.
  - Definir checklists y formas tanto como sea posible.

Lámina 27 Dr. Roberto Gómez Cárdenas

Ejemplos checklist

Incident Response Checklist

The following steps will assist you to respond when a report of a special incident is received. The steps on the left are intended to guide you through the process. The strategies on the right are suggested guidelines for completing each step. Not all strategies will be applicable in every situation. Code Strategies as follows: **Y** = Yes, **N** = No, **NA** = Not Applicable.

Response Steps	Strategies
Insure the safety of the consumer	___ Is the consumer safe now? ___ Is medical treatment being provided? Needed? ___ Are further risks evident (fire or safety hazard, lack of adequate food or shelter, broken equipment, etc.)? ___ What interim measures have been taken to protect the consumer? Other consumers?
Notify legally required entities (as appropriate)	___ CCL ___ APS ___ CPS ___ Family/Guardian/Conservator ___ Police ___ LTC Ombudsman ___ DHS Licensing ___ Coroner
Check for completeness of information	___ Have the "who", "what", "when", and "where" questions been answered? ___ Is the type of incident reported consistent with the information and circumstances reported? ___ What may have contributed to the incident? ___ What aspects of the incident need to be further explored?
Inquire into inconsistencies	___ Are there unanswered questions about this incident? ___ When there are multiple reporters, are conflicts evident among reporters (e.g., family, consumer, direct service provider) from the various incident descriptions? ___ What additional information is needed to clarify these conflicts?
Document details (NOTE: If reportable incident, the SIR must be transmitted to DDS within 48 hours.)	___ Has the SIR been completed? ___ Has a preventative action plan been developed, if needed?
Explore causes of the incident	___ Have all "why" questions been answered? ___ Has the consumer had other incidents? ___ Should others be involved in analyzing this incident (e.g., nurse, PT, Behavior Analyst)? ___ Have significant changes in the person's life been explored? ___ Have some preventative actions already been implemented?

Sysadmin Incident Response Checklist

The checklist below is intended to outline some recommended actions system administrators should perform in the event of a system compromise or malicious activity.

1. Please contact IMSS Information Security at security@caltech.edu if you have not already performed this task.
2. Determine the nature and seriousness of the indcident by considering the following questions and discussing them with Information Security if necessary.

   A. Does the system contain sensitive or confidential information?
   B. Is there a chance outside law enforcement may need to get involved?
   C. Is there a requirement or desire to perform a forensics analysis of the system compromise?
3. If the answer is yes to any of the questions in item (2) then please disregard the instructions below and coordinate the actions to be taken with Information Security.
4. If the answer is no to all the questions in item (2) then continue to item (3) on the checklist.
5. Isolate the compromised system by disconnecting the network cable. If this is not feasible or desireable, Information Security can block access to the compromised system via the network.
6. Try to determine the cause of the malicious activity and the level of system privilege attained by the miscreants.
7. Disable any hacked accounts and kill all processes owned by them.
8. Compile a list of IP addresses involved in the incident, please include log entries if possible, and forward the data to Information Security.
9. Determine the user(s) that need to change their passwords due to the compromise as well as whether or not they have accounts on other systems. As you are aware, users often use the same credentials on numerous machines and if that proves to be the case, the administrators for those systems should be notified.
10. Make a backup copy of the local password file if appropriate, in case you need to compare who has and who has not changed their passwords after notification.
11. Please notify Information Security if your system uses Caltech LDAP authentication to authenticate users.

Lámina 28 Dr. Roberto Gómez Cárdenas

Preparación

- Comunicación
  - Muy importante durante un incidente.
    - No solo abarca a la gente involucrada, sino a la forma en que se lleva a cabo.
  - Actualizaciones deben ser frecuentes.
  - Comunicaciones no controladas son importantes
    - Faxes
    - Teléfonos celulares
    - Teléfonos inteligentes

Lámina 29 Dr. Roberto Gómez Cárdenas

Preparación

- Derechos de acceso
  - El equipo de respuesta a incidiente debe tener acceso a los sistemas sin necesidad de autorización por parte de los administradores.
  - Punto controversial.
  - Cuentas de usuario, contraseñas, y llaves de cifrados.
  - Disponibilidad de los métodos de almacenamiento de terceras partes.

Lámina 30 Dr. Roberto Gómez Cárdenas

Preparación

- Políticas
  - Política de búsqueda se encuentra detallada en el manual del empleado.
  - Mensajes, banners, de advertencia se despliegan fácilmente.
  - Proteger a la organización de demandas legales y permitir que los investigadores lleven a cabo su trabajo.
  - Recursos humanos y legales han firmado.
  - Empleados han confirmado que tienen conocimiento de sus espectativas en privacidad.
  - Estar conscientes de las leyes internacionales.

Lámina 31 Dr. Roberto Gómez Cárdenas

Preparación

- Obtención de recursos
  - Los analistas de incidentes deben contar con todas la información y deben estar listos para responder al incidente.
  - Procedimientos, checklist y formas se encuentran listos.
  - Credenciales de acceso se encuentran disponibles o se conoce a las personas que las tienen.
  - Información de los sistemas, diagramas de redes, software y propiedades intelectuales se encuentra documentados.

Lámina 32 Dr. Roberto Gómez Cárdenas

Preparación

- Capacitación
  - Instituto SANS y Certificaciones GIAC
    - Incident Response and Hacker Techniques
    - Digital Forensics
  - Capacitación vendedores
    - Guidance Software
    - Access Data

Lámina 33 Dr. Roberto Gómez Cárdenas

Identificación

- Objetivos
- Determinar alcance
  - Identificar que sistemas, gente y activos de información se encuentran involucrados en el evento.
- Preservar evidencia
  - Proteger los hechos del incidente mientras se determina el escenario

Lámina 34 Dr. Roberto Gómez Cárdenas

Identificación

- Eventos sospechosos
- Actividades no explicadas
  - Nuevas cuentas o archivos
  - Modificaciones archivos
  - Alertas de los IDS
  - Entradas en el Firewall
  - Desaparición de cuentas
  - Desempeño bajo / servicios no responden.
  - Inestabilidad del sistema

Lámina 35 Dr. Roberto Gómez Cárdenas

Identificación

- Identificación pasiva
  - Sniffers y análisis de tráfico
  - Sistemas de detección de intrusos
  - Verificadores de integridad de archivos
  - Honeypots y honeytokens
    - Sistemas específicos o cuentas con seguimiento y notificación adicional, para alertar en caso de actividad sospechosa.

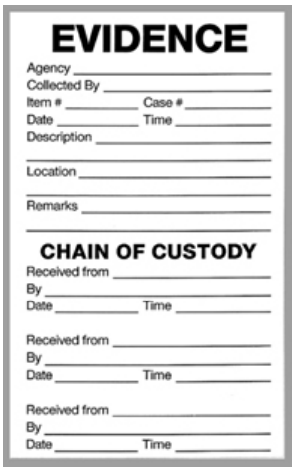
Lámina 36 Dr. Roberto Gómez Cárdenas

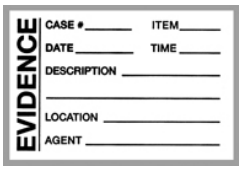
Identificación

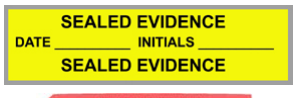
- Cadena de custodia
  - Evidencia debe ser “etiquetada” desde el tiempo en que es colectada hasta el tiempo en que es presentada.
  - Cada pieza de evidencia debe encontrarse bajo el control de una persona identificable todo el tiempo.
  - Un cambio en el control de la evidencia debe ser registrado.
  - La evidencia que resida en un medio de almacenamiento debe protegerse de posible contaminación (sellada y asegura).

Lámina 37 Dr. Roberto Gómez Cárdenas

Etiquetas







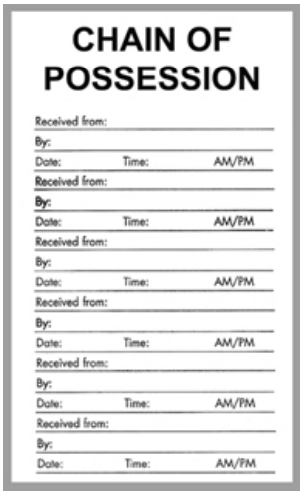


Lámina 38 Dr. Roberto Gómez Cárdenas

Contención

- Una vez que los eventos han sido identificados como un incidente y una cadena de custodia para la evidencia se ha establecido, se tomara el primer paso en la modificación del sistema para empezar con la contención.

Lámina 39 Dr. Roberto Gómez Cárdenas

Contención

- Coordinación con el vendedor.
- Identificar el Modelo de Confianza
  - Identificar no solo la tecnología sino la gente involucrada en el incidente.
- Estrategias de documentación
  - Documentación debe llevarse a cabo desde el más al menos volátil y desde el menos invasivo al más invasivo.
- ¿Se debe enviar a cuarentena?
  - Cambios al sistema puede ser fácilmente observados por el atacante.

Lámina 40 Dr. Roberto Gómez Cárdenas

Contención

- Análisis Inicial
  - Mantener un perfil bajo
  - Nunca analizar el original
  - Llevar a cabo frecuentes actualizaciones al CSIRT
  - Obtener los archivos de bitácoras
  - *Enfocarse en los hechos* y evitar culpas.
  - Considerar todas las posibilidades pero mantenerlo simple. (KISS)

Lámina 41 Dr. Roberto Gómez Cárdenas

I have not data yet. It is a capital mistake to theorize before one has data. Insensibly one begins to twist facts to suit theories, instead of theories to suit facts.

Lámina 42 Dr. Roberto Gómez Cárdenas

Contención

- Respaldos
  - Varios respaldos permiten investigación y preservación de la evidencia.
  - Diferentes estrategias existen y dependen de la situación.
  - El original se guarda como evidencia.
  - Respaldo 1: Para ponerlo de nuevo en producción.
  - Respaldo 2: Análisis forense
  - Respalado 3, 4, etc…. copias separadas para análisis.

Lámina 43 Dr. Roberto Gómez Cárdenas

Contención

- Forensia digital
  - Varios análisis separados llevan a los mismos resultados.
  - Necesidad de hardware especial, software y entrenamiento.
  - Copia bit a bit de los datos y análisis de estos.
  - Recuperación de datos borrados.
  - Identificación de sistemas de archivos alterados y binarios en un ambiente seguro.

Lámina 44 Dr. Roberto Gómez Cárdenas

Contención

- Bloqueadores hardware de escritura
- Software de forensia.
- ¿Qué se esta buscando?
- ¿Otros dispositivos?
  - Puede ayudar en la investigación.
  - USB, tarjetas SIM, celulares,
- Herramientas antiforensia
  - Windows: Eraser
  - Unix: Wipe

Lámina 45 Dr. Roberto Gómez Cárdenas

Contención

- Parar el avance del ataque
  - Cambiar contraseñas y derechos de acceso.
  - Cambiar nombres de hosts e Ips
  - Desviar tráfico sospechoso
  - Bloquear IPs o Redes
  - Aplicar parches a sistemas similares
  - Dar de baja servicios.

Lámina 46 Dr. Roberto Gómez Cárdenas

Erradicación

- Una vez que el incidente a sido contenido se intenta remover el total de aplicaciones maliciosas del sistema o la red.

Lámina 47 Dr. Roberto Gómez Cárdenas

Erradicación

- Remover o restaurar
  - Borrar archivos maliciosos o restablecer a partir de respaldos.
  - Rootkits demandan una reconstrucción
  - Es posible que los parches no se encuentren disponibles y se requiera un cambio total de la arquitectura.
  - Es necesario verificar los respaldos.

Lámina 48 Dr. Roberto Gómez Cárdenas

Erradicación

- Reforzar las defensas
  - Implementar métodos de protección adicionales y reforzar tecnologías y procesos existentes.
  - Aplicar filtros en reglas y firewalls.
  - Llevar a cabo “mini-assessments” usando las mismas herramientas y técnicas que los atacantes.
  - Buscar por exploits y backdoors similares en varias máquinas.

Lámina 49 Dr. Roberto Gómez Cárdenas

Recuperación

- Una vez que la amenaza ha sido eliminada la organización debe empezar el proceso de regresar el negocio a su operación normal.

Lámina 50 Dr. Roberto Gómez Cárdenas

Recuperación

- Regreso a la operación
  - Dueños de los sistemas deben tomar la decisión final para el regreso a producción.
  - Los dueños dependen en los sistemas y conocen su valor real.
  - Si existe desacuerdo en la decisión, este debe ser documentado por el analista y el propietario debe aceptar su responsabilidad.

Lámina 51 Dr. Roberto Gómez Cárdenas

Recuperación

- Monitoreo
  - En este punto dentro del proceso se cuenta con la información suficiente para identificar si el ataque ocurre de nuevo.
  - Crear firmas de IDS si es posible.
  - Verificar la operación normal en base a configuraciones.
  - Implementar la generación de bitácoras adicionales en la red, hosts y aplicaciones.

Lámina 52 Dr. Roberto Gómez Cárdenas

Lecciones aprendidas

- La junta de lecciones aprendidas proporciona un método a la organización para coordinar conocimiento de un incidente, sugerir cambios en procedimientos y políticas para el futura y justificar la implementación de nuevas medidas preventivas.

Lámina 53 Dr. Roberto Gómez Cárdenas

Lecciones aprendidas

- Junta de recapitulación
  - Debe tener lugar después de la erradicación de un incidente mientras los detalles se encuentran frescos en las cabezas de los miembros del equipo.
    - Crear una línea de tiempo de los eventos,
    - Proporcionar un consenso de notas y documentación.
    - Finalizar los hechos en un reporte final.

Lámina 54 Dr. Roberto Gómez Cárdenas

Ejemplo línea de tiempo

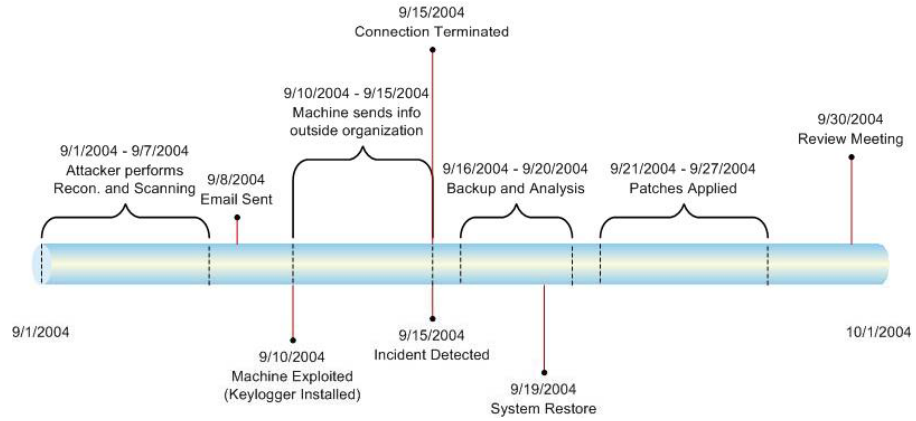
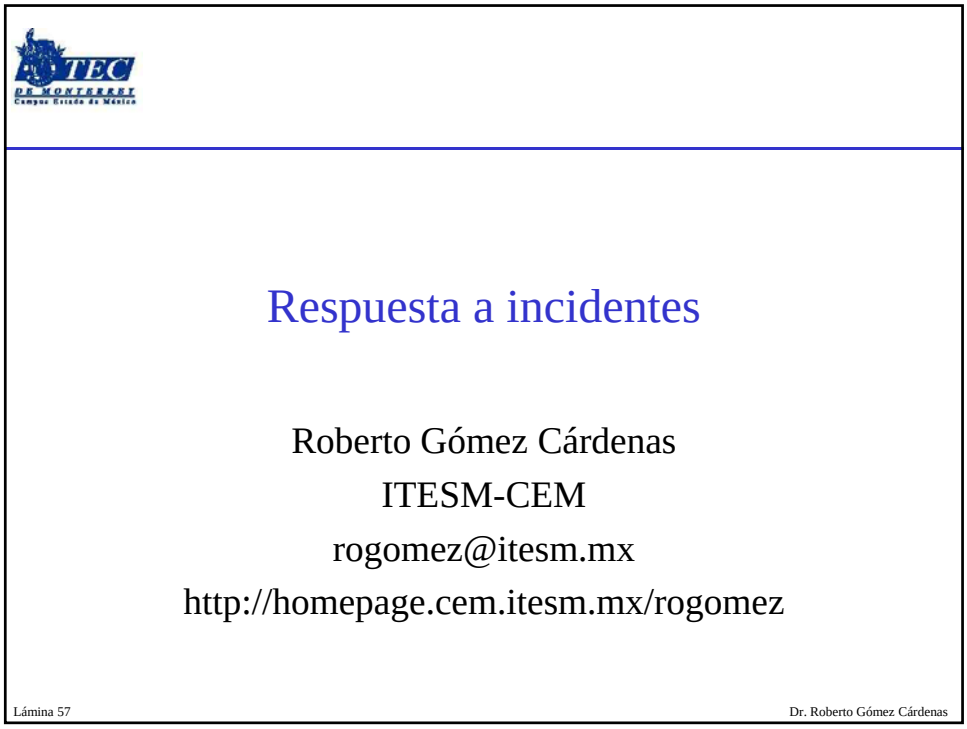


Lámina 55 Dr. Roberto Gómez Cárdenas

Siete pecados capitales

- Falla en reportar/pedir por ayuda.
- Notas no completas o inexistentes
- Mal manejo de la evidencia
- Fallas en la creación de respaldos.
- Fallas en la erradicación o en la contención.
- Fallas en la prevención de re-infencción.
- Fallas en aplicar las lecciones aprendidas.

Lámina 56 Dr. Roberto Gómez Cárdenas


Respuesta a incidentes
Roberto Gómez Cárdenas
ITESM-CEM
rogomez@itesm.mx
http://homepage.cem.itesm.mx/rogomez
Lámina 57
Dr. Roberto Gómez Cárdenas