Seguridad y Competencias Profesionales
Tema 4: Seguridad en el entorno
Curso 2012–2013

Ingeniería en Informática (2° ciclo)

Departamento de Ingeniería Informática
Universidad de Cádiz

Cádiz, 24 octubre 2012

Índice

Objetivos

Al finalizar este tema el alumno deberá ser capaz de:

Conocimiento

Enumerar los diferentes problemas de seguridad existentes en los aspectos de seguridad física y del personal.

Comprensión

Describir las medidas disponibles para reducir los riesgos asociados a los problemas de seguridad en los anteriores ámbitos.

Aplicación

Dada una empresa con unas características conocidas, diseñar una política de seguridad física y normas para el control del personal que puede tener acceso al sistema.

Seguridad física

Concepto

Se ocupa de los problemas de seguridad informática que no pueden ser previstos o evitados mediante mecanismos informáticos.

Ejemplos

- Robos del material,
- sabotaje o vandalismo,
- incendios,
- humedad, etc.

Amenazas por acceso físico a los equipos

Accidentes por personal autorizado

- Volcado de comida, bebida o tabaco sobre el equipo
- Tropiezos por la situación de los aparatos y cables
- Usos no habituales de las salas: conferencias, reuniones
- Mantenimiento: limpieza, pintado, aire acondicionado, etc.
- Caídas o vuelques durante transporte

Otras amenazas de tipo físico debidas a personas

- Robo del equipo completo o de sus módulos (RAM, p. ej.)
- Sabotajes, vandalismo
- Robo de la información almacenada (disco duro, soportes extraíbles)

Mecanismos contra accesos físicos no autorizados

Prevención

- Llaves (cuidado con el tipo de cerrojo)
- Tarjetas magnéticas o inteligentes
- Teclados con contraseña (ver artículo en el CV)
- Métodos biométricos
- Control de las vías de acceso alternativas

Detección

- Cámaras
- Sensores de presencia
- Concienciación del personal
- Personal de seguridad

Desastres del entorno

Condiciones ambientales

- Humo, polvo, sequedad y humedad
- Temperaturas extremas
- Insectos, ratas

Situaciones puntuales

- Sobrecargas de tensión, falta de fluido eléctrico
- Campos electromagnéticos fuertes
- Movimientos bruscos

Desastres naturales

Ejemplos

- Terremotos y vibraciones
- Tormentas eléctricas
- Incendios e inundaciones

Medidas

- Contratación de seguros
- Diseño del edificio a prueba de terremotos
- Equipamiento contra incendios (CO_2, espuma, halón)
- Situación de la sala de máquinas evitando zonas vulnerables a inundaciones

Normativa

A nivel de edificación

- Documento central: Código Técnico de la Edificación
- Exigencias para cumplir la ley 38/1999
- Compuesto de varios Documentos Básicos:
  - Seguridad Estructural
  - Seguridad Caso de Incendio
  - Ahorro de Energía, etc.

Incendios

- Se adopta la Norma Europea EN-3 (antes la BS EN 3)
- Se extiende con UNE-EN 3-7, 3-8, 3-9 (acceso por NORWEB)

Protección de los datos que residen en el sistema

Amenazas

- Robo de los datos
- Destrucción de los datos

Medidas contra el robo de los datos

- Cifrado de soportes extraíbles, cifrado de disco (no sirve si la máquina se roba encendida)
- Apagado de la máquina cuando no se necesita, para retirar información de RAM
- Contenidos de DRAM permanecen un tiempo (ataque *cold-boot*, `http://citp.princeton.edu/research/memory`)

Medidas contra la destrucción de los datos

Copias de seguridad, fundamentalmente.

Tareas

Ejercicio 4.1

Localice 4 ejemplos de software y hardware disponibles para conseguir cifrado de disco.

Ejercicio 4.2

- ¿Qué condiciones han de cumplirse para realizar el ataque *cold-boot*?
- ¿Le parece un ataque práctico?
- ¿En qué situaciones podría ser útil para los cuerpos de seguridad?

Protección de los datos que viajan por la red

En este tema sólo tratamos aspectos de tipo físico

Amenazas a nivel físico

- Cables de red "pinchados" o cortados
- Rosetas de red con equipamiento no autorizado

Medidas

- Cables fuera del acceso del público, en techos o suelos falsos o dentro de las paredes
- Cables a prueba de "pinchazos": fibra óptica, con cámara de vacío, etc.
- Desactivación de rosetas no utilizadas
- Uso de conmutadores de red en vez de concentradores

Protección de las copias de seguridad

Importancia

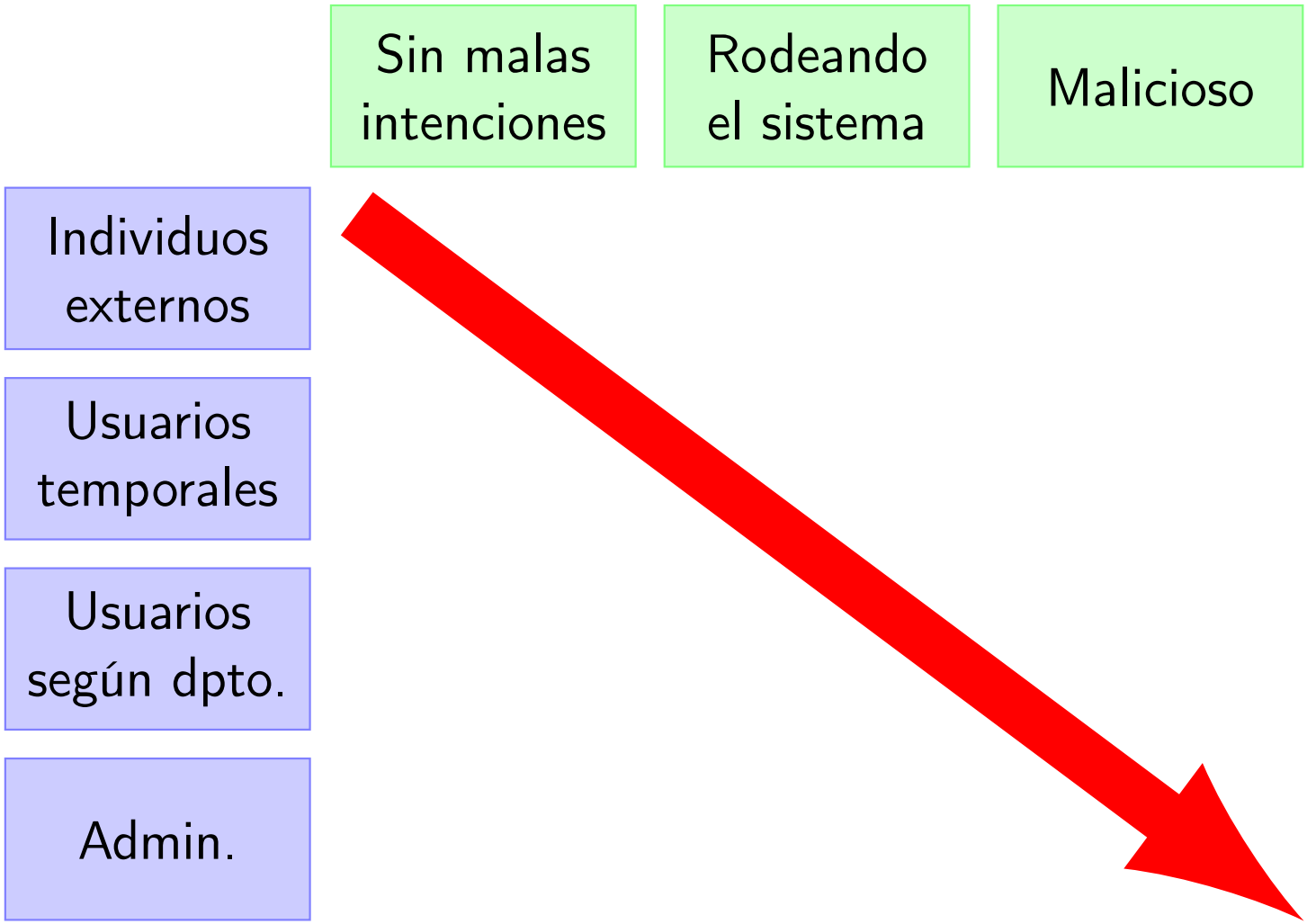
- Misma información que en producción: mismos problemas de confidencialidad y mismos costes
- Los armarios además contendrán información antigua, con entradas históricos y registros de auditoría

Medidas

- Etiquetar copias y organizar para evitar su pérdida
- Utilizar medios (cintas, CD/DVD de calidad) de almacenamiento apropiados y formatos abiertos
- Situar copias en otras instalaciones
- Protegerlas a nivel físico contra robos, sabotaje, incendios, etc.

Matriz de riesgo

Riesgo varía según la intencionalidad del usuario y sus privilegios



Matriz tomada de [SAMS].

Amenazas del exterior (I)

Ingeniería social

Pretextos	Construir historias "creíbles" tras investigar la organización, para ir sacando más información
Phishing	Enviar correos haciendo ver que somos una entidad con autoridad y que necesitamos la contraseña (Hacienda, Banco Santander, eBay, etc.)
Vishing	Equivalente de *phishing*, por teléfono
Uso de cebos	Pendrives USB y otros soportes "dejados", que instalan software malicioso al ser usados

Amenazas del exterior (II)

Otras amenazas

Shoulder surfing	Vemos la contraseña a la vez que es escrita
Mascarada	Aprovechamos que alguien está de vacaciones para suplantarle, o para "visitar" su despacho
Basureo	Rebuscamos en la basura documentación y soportes no limpiados debidamente
Uso de PBX	Utilizamos los teléfonos de la organización para hacer llamadas internacionales de larga duración, o a números de pago

Medidas para amenazas del exterior

Medidas fundamentales

- Concienciación del personal
- Formación en seguridad
- Ejecución y control de la política y los procedimientos necesarios

Amenazas del interior

Características del personal interno

Conocimiento	Saben cómo está dispuesto el sistema, qué se guarda y dónde se guarda
Experiencia	Conocen los fallos de seguridad y las incidencias anteriormente ocurridas
Ocasión	Tienen acceso al sistema, o saben cómo conseguirlo
Motivo	Pueden encontrarse descontentos con la organización, o deseando vengarse (tras un despido, p. ej.)

Medidas para amenazas del interior (I)

Controles previos a contratación

- Historial criminal
- Nacionalidad de origen y obtención de ciudadanía
- Registros de denuncias realizadas
- Comprobación de empleos anteriores
- Evaluaciones psicotécnicas
- Títulos académicos obtenidos

Medidas para amenazas del interior (II)

Control de privilegios

- Deben darse sólo los permisos estrictamente necesarios
- Evitar la aparición de "empleado clave"
- Realización de auditorías
- Ideal: administrador de sistemas, administrador de seguridad y gestor de auditorías separados

Mantener un buen ambiente de trabajo

- Seguridad en el trabajo: luz adecuada, entorno cómodo, higiene.
- Seguridad en el empleo
- Reconocimiento de la labor de los empleados, evitando horas extras

Otros tipos de personal "interno"

Ejemplos

Visitantes	Invitados a demostraciones, etc.
Op. externos	Mantenimiento, vendedores, instaladores, etc.

Algunas de las medidas más útiles

- Acordar una responsabilidad en caso de que se produzcan daños con la empresa relacionada
- Acompañar con personal propio
- Si necesitan contraseñas u otros credenciales, que sean de un solo uso

Tareas

Ejercicio 4.3

En grupos:

- Leer los siguientes ensayos de Bruce Schneier:
  - *The Importance of Security Engineering*
  - *Drawing the Wrong Lessons from Horrific Events*
  - *Detecting Cheaters*
  - *Thwarting an Internal Hacker*
- Discusión sobre cada uno de los ensayos
- Entrega de conclusiones sobre los aspectos discutidos

Referencias

Anónimo.
Maximum Security, capítulo 5.
SAMS, 4ª ed., 2003.

Bruce Schneier.
Essays and Op Eds, categorías "Physical Security" y "Psychology of Security".
http://www.schneier.com/essays.html.

José María López Hernández.
Seguridad Física COMO.
Disponible en el Campus Virtual.