Redes Abiertas y Cerradas
Experiencias

Antonio Ruiz Moya

Director del Centro de Informática y Redes de comunicaciones

Universidad de Granada

Universidad De Granada

CSIRC

Estadísticas CERT/CC *(http://www.cert.org/stats/cert_stats.html)*

Number of incidents reported

1988-1989

Year	1988	1989
Incidents	6	132

1990-1999

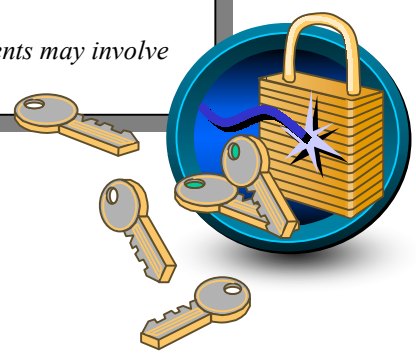
Year	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999*
Incidents	252	406	773	1,334	2,340	2,412	2,573	2,134	3,734	9,859

2000-2002

Year	2000	2001	2002+
Incidents	21,756	52,658	82,094

Total incidents reported (1988-2002): **182,463**

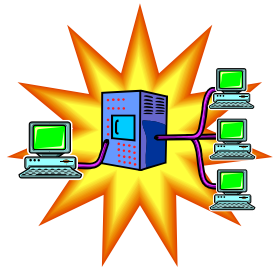
Please note that an incident may involve one site or hundreds (or even thousands) of sites. Also, some incidents may involve ongoing activity for long periods of time.

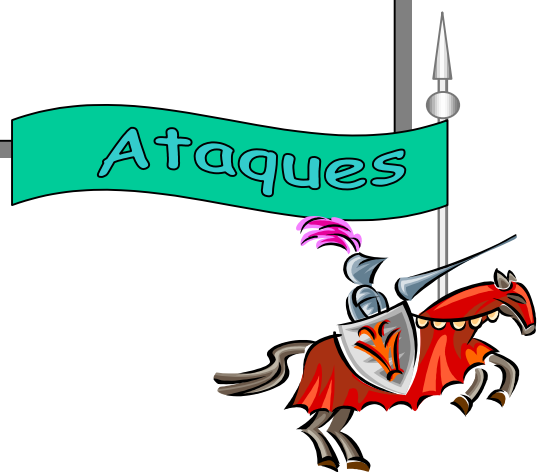


Universidad De Granada

Riesgos comunes en una Red Corporativa Universitaria

- Accesos no autorizados
- Tomar control del sistema
- Caballos de Troya
- Monitorización de las comunicaciones
- Simulación
- Denegar acceso al usuario legítimo y autorizado
- Repudio: Negar que se ha remitido un documento
- Denegación de Servicios
- Virus / Gusanos
- ...





CSIRC

Universidad De Granada

RedUGR en Cifras

- **85.000 usuarios**
  ***Alumnos**: 80.000, **PDI**: 3.250 **PAS**: 1.800*
- **7 Campus Universitarios**
  Cartuja & Fuentenueva & Centro & Ciencias de la Salud & Aynadamar & Ceuta & Melilla
- **28 Centros/edificios**
- **60 Aulas de docencia**
- **> 9.500 nodos en RedUGR**
  5.5k x Investigación - 1.5k x Gestión – 2.5k x Docencia
- ***Servicios de Acceso Remoto*** (RTB/RDSI/ADSL)
- **Acceso de Portátiles desde cualquier lugar**
- **Campus Virtual Inalámbrico**
- **…**

Universidad De Granada

Lo más importante a la hora de proteger a nuestra Institución es comenzar por la definición de una POLÍTICA DE SEGURIDAD

Implicados

- Equipo de Gobierno
- Responsables de Redes y Com.
- Responsables de Sistemas
- Responsables de Desarrollo
- Usuarios

Definición de Objetivos

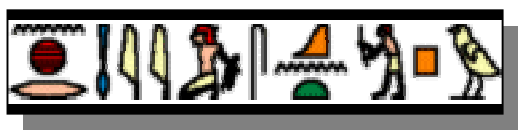
- Procedimientos A(Autenticación) A (Autorización) A (Accounting). AAA.
- Procedimientos de Detección y Actuación frente a ataques
- Conectividad Universidad
- Asegurar rendimientos en los Servicios
- Implicación de los usuarios
- Auditorías periódicas

Por qué, Qué, Cómo y Dónde protegemos ...

Universidad De Granada

ELEMENTOS DE SEGURIDAD

- ANTIVIRUS
- CORTAFUEGOS SOFT/HARD
- INSPECTOR DE CONTENIDOS
- SIST. GESTIÓN DE BW & TRAFICO
- ENCRIPTADORES
- ROUTER CON FIREWALL
- SISTEMAS DE ALMACENAMIENTO
- SERVIDOR DE VPN
- SISTEMAS DE DETECCION DE INTRUSOS
- SISTEMAS DE BACKUP
- FIREWALL / CORTAFUEGOS
- SISTEMAS DE AUTENTICACIÓN



Universidad De Granada

Definición de la Política de Seguridad de UGR

V6.5

- **Conectividad desde/hacia exterior.**
  - Correo electrónico controlado (filtrado puerto 25)
  - Control espacio direccionamiento de RedUGR
  - Servidores Gestión Corporativa filtrados
  - Conectividad de Aulas controlado
  - Acceso total de PAS & PDI
- **Conectividad en el interior de RedUGR.**
  - Acceso total a Servicios/Redes del PAS&PDI&Alumnos
  - Acceso total desde portátiles (registro temporal o definitivo) y CVI-UGR (VPN)
- **Servicios de Acceso Remoto UGR.**
  - Acceso RDSI/RTC……AAA
  - Acceso ADSL……VPN
  - Acceso desde Internet…..VPN
- **Servicios de Aulas informáticas de docencia.**
  - Redes Ocultas con acceso total en RedUGR
  - Acceso a Internet Proxy/Caché/Identificación usuario.
- **Servicio ADP** (**A**ulas de **D**ocencia **P**resencial).
  - Puntos activos / Acceso total (VLAN's no públicas + Direcc. oculto + Asignación de IP`s dinámicas + Filtros dinámicos)

Universidad De Granada

Definición de la Política de Seguridad de UGR

- **bdC: (User+Ether+IP…)/port**
  - Mantenimiento por parte del usuario a través de SV.
- **Secretaría Virtual** (AAA contra bdC)
- **Seguridad en Sistemas de Investigación/Gestión/Docencia/Red**
  - Acceso Controlado y Autentificado contra bdC
- **Definición de UGR-TF para detección/asesoría/análisis forense (recursos humanos).**
- **Protección ante virus: usuario / estafeta de correo electrónico.**
- **Sistemas de Auditorias periódicas. Red / Sistemas / Servicios**
- **Adaptación/cumplimiento de la LOPD/LSSI.**
- **…**

CSIRC

Universidad De Granada

Implementación de la Política de Seguridad de UGR

- **RedUGR <-> Internet :** **Routers IN/OUT / IDS**
  Seguridad proactiva: nessus / Formación usuario
  Seguridad reactiva: snort / ntop
- **Aulas :** **Red de Proxy/Cachés**
- **RAS/CVI-UGR/Portátiles :** **Servidor Radius/VPN** (LDAP)
- **Servicios AA contra :** **bdC** (LDAP)
- **Servicios de Auditoría :** **HP OpenView / MRTG / NTOP / SQUID**
- **Gestión Admin. RedUGR :** **Desarrollo propio (tomcat+jsp+Oracle)**
- **Sistemas IGDR :** **Services down, SSH, tcp-wrappers,…**
- **Antivirus/firewall personal : Panda & Trend Micro**

- **Objetivos en curso … :**
  - **Reducción de horas/técnico/día, automatizando las operaciones de filtrado / Control (FIREWALL+IDS)**
    Nokia+Checkpoint / Netscreen / Cisco / Open Source
  - **Idem Auditorías Red/Sistemas/Aplicaciones: Sistema de Alarmas**
  - **Gestión de tráfico para tunning de servicios (Automatricula/e-learning…)**
  - **Lanzamiento de servicios certificados a través de la autoridad de certificación de UGR.**

Universidad De Granada

Implicaciones de la implementación Política de Seguridad en UGR

- **>RRHH destinados al mantenimiento de la política de seguridad**
- **Formación**
- **Costes €:**
  - **Adquisición hard/soft:**
    - firewall
    - ids's
    - vpn servers
    - antivirus
    - Auditorías
    - …
  - **Mantenimientos anuales**
- **- colaboración del usuario final**
- **Nueva figura: 24x7**

CSIRC

I Jornadas de Arquitecturas de Red Seguras en las Universidades

Redes Abiertas y Cerradas

Experiencias

Antonio Ruiz Moya

Director del Centro de Informática y Redes de comunicaciones

Universidad de Granada