UNIVERSIDAD PARAGUAYO ALEMANA

Ingeniería en Tecnologías de la Información Empresarial TIE

Seguridad en TICs

Prof.: Chrystian Ruiz Diaz

DISCLAIMER

Todo el contenido de esta presentación se proporciona **exclusivamente con fines didácticos y educativos en el ámbito académico**.

El uso inapropiado de las técnicas y/o conocimientos expuestos en esta presentación puede violar leyes nacionales e internacionales.

El autor y la institución educativa no se hacen responsables del uso indebido de la información contenida en esta presentación.

Se enfatiza que la información debe ser empleada únicamente para propósitos éticos, legales y con la debida autorización de las autoridades competentes.

Contenido

1. Ciclo de Vida de la Seguridad
2. Mecanismos de Seguridad
3. Firewall
4. DMZ - *DeMilitarized Zone*
5. IDS - *Intrusion Detection System*
6. IPS - *Intrusion Prevention System*
7. PROXY
8. UTM - *Unified Threat Management*
9. SPAM
10. HONEYPOTS

Ciclo de Vida de la Seguridad

IDENTIFICAR: Desarrollo normativo, Plan Director y SGSI (Sistema de Gestión de la Seguridad de la Información)

- Definición de controles, indicadores y cuadros de mando
- Auditorías de cumplimiento
- Análisis y gestión de riesgos

PROTEGER: Implementar las contramedidas

- Asesoramiento en la incorporación de nuevas tecnologías
- Implantación de soluciones tecnológicas de Ciberseguridad
- Fabricación de soluciones y servicios propios

NIST - National Institute of Standards and Technology – U.S

Ciclo de Vida de la Seguridad

DETECTAR: Identificar la ocurrencia de un suceso a tiempo

- Diagnósticos especializados (hackings, código fuente, etc)
- Gestión de vulnerabilidades
- Red team (equipo para simular un ataque dirigido)
- Infraestructuras de monitorización continua
- SOC´s (*Security Operation Center*)

RESPONDER: Medidas de actuación ante un suceso para intentar contener

CERT (*Computer Emergency Response Team*)

- SERVICIOS PROACTIVOS

(Gestión de la configuración, Inteligencia)

- SERVICIOS REACTIVOS

(Gestión de incidencias, Análisis forense)

NIST - National Institute of Standards and Technology – U.S

Ciclo de Vida de la Seguridad

RECUPERAR: Enfocado a la recuperación y resiliencia en el menor tiempo posible

- BIA (*Business Impact Analysis*)
- Plan de Continuidad de Negocio
- Pruebas

NIST - National Institute of Standards and Technology – U.S

TAXONOMÍA DE ATAQUES CIBERNÉTICOS

Contenido abusivo
- SPAM
- Delito de odio: ej ciberacoso, racismo, amenazas
- Pornografía infantil, contenido sexual o violento inadecuado

Contenido dañino
- Sistema infectado
- Servidor C&C (Comando y Control)
- Distribución de malware
- Configuración de malware

Obtención de información
- Escaneo de redes (scanning)
- Análisis de paquetes (sniffing)
- Ingeniería social

Intento de intrusión
- Explotación de vulnerabilidades conocidas (CVE - *Common Vulnerabilities and Exposures*)
- Intento de acceso con vulneración de credenciales (Ej fuerza bruta)
- Ataque desconocido (exploit desconocidos - cero day)

Intrusión
- Compromiso de cuenta con y sin privilegios
- Compromiso de aplicaciones (inyección SQL)
- Robo

Disponibilidad
- DoS (Denial of Service)
- DDoS (Distributed Denial of Service)
- Sabotaje
- Interrupciones por cuestiones externas, desastres naturales

TAXONOMÍA DE ATAQUES CIBERNÉTICOS

Compromiso de la información

- Acceso no autorizado a información: robo credenciales snnifing
- Modificación no autorizada de información: ransomware

Fraude

- Uso no autorizado de recursos
- Derechos de autor: Warez – P2P
- Suplantación – Phishing

Vulnerable

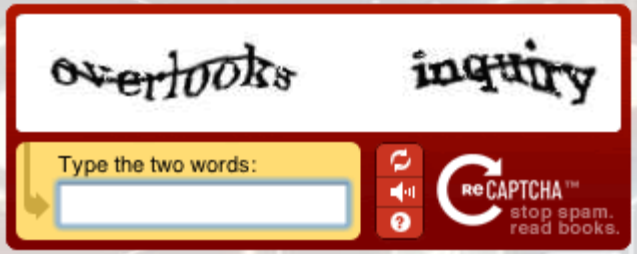
- Criptografía débil
- Amplificador DDoS
- Servicios con acceso potencial no deseado: Telnet
- Revelación de información

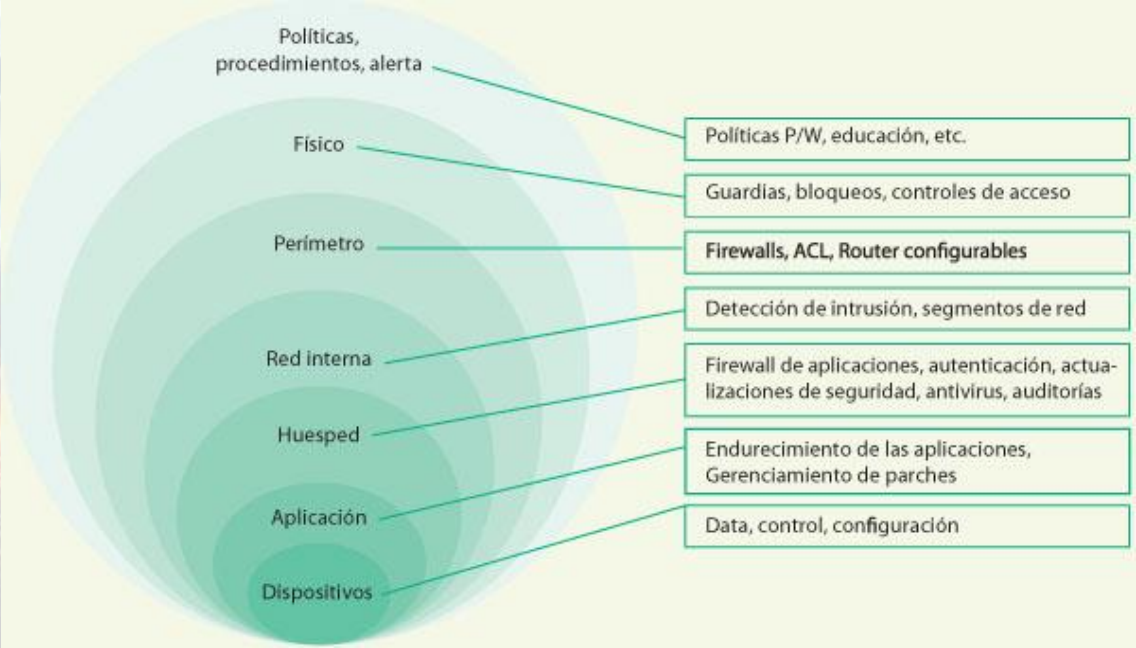
APT - *Advanced Persistent Threat*

Ciberterrorismo

MECANISMOS DE SEGURIDAD

CAPTCHAs (completely automated public turing tests to tell computers and humans apart)





MECANISMOS DE SEGURIDAD

Firewall: es un dispositivo software o hardware que forma parte de un equipo o dispositivo de una red y está diseñado para proteger dicho sistema bloqueando accesos no autorizados y permitiendo solo los que deban ser permitidos cumpliendo con las directrices definidas en la política de seguridad de la organización

Reglas: IP, Puerto, Origen - Destino, Protocolos, acción

Políticas permisivas
Políticas restrictivas

MECANISMOS DE SEGURIDAD

Firewall según se ubicación:

- De Host
- De red

Firewall según su funcionamiento

- De filtrado de paquetes (FWs antiguos, básicos)
- De aplicación
- De base de datos
- Web

Zonas desmilitarizadas

Es una red que suele albergar servidores que ofrecen algún servicio en Internet y que, generalmente, actúa como intermediaria entre la red interna de una empresa y la red externa, incrementando la seguridad de las redes internas

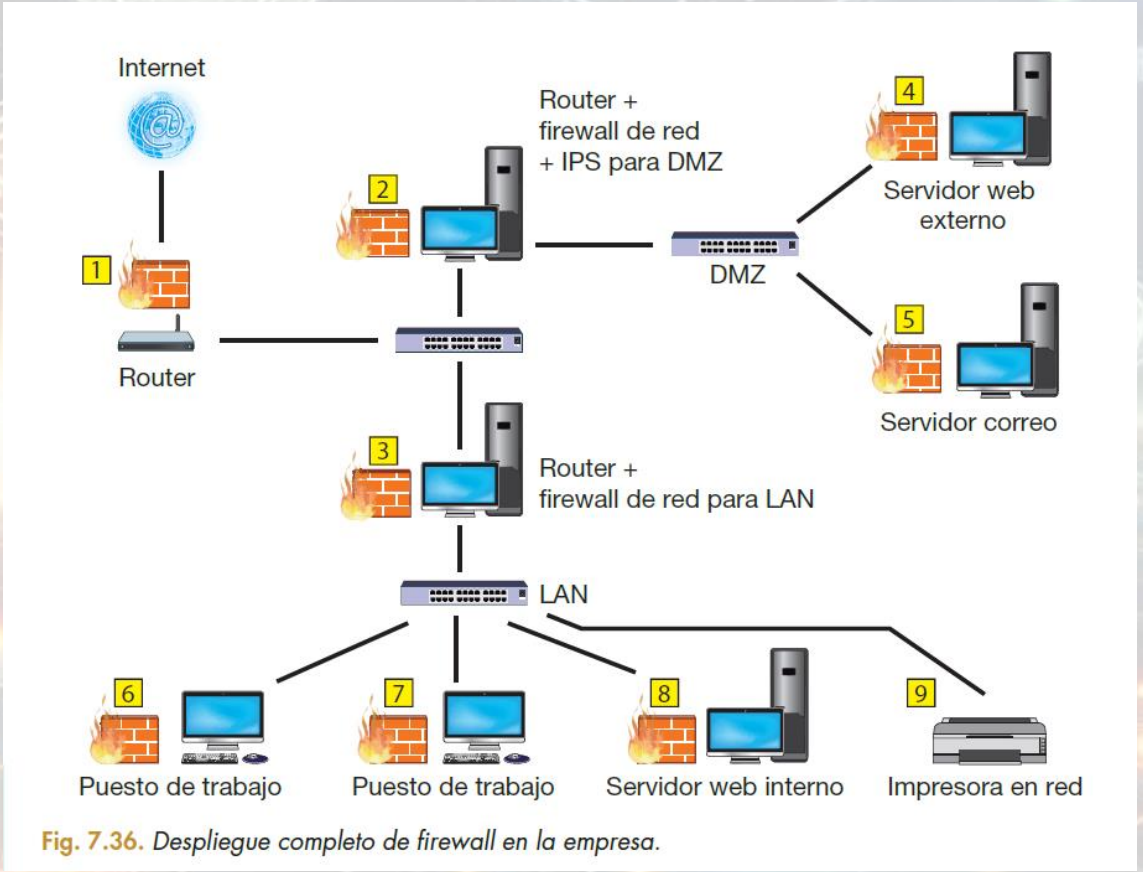


Fig. 7.36. *Despliegue completo de firewall en la empresa.*

IDS - *Intrusion Detection System*

Este tipo de sistemas está formado por un dispositivo o software que monitoriza, alerta ataques a la red o a los equipos informáticos

Tipos

- HIDS (Host IDS), que monitoriza y protege un equipo.
- NIDS (Network IDS), que monitoriza y protege una red.
- DIDS (Distributed IDS), donde se dispone de NIDS distribuidos y gestionados

Tarea Semanal

IPS - Intrusion Prevention System

son un elemento activo que trata de neutralizar el ataque, adaptándose a él. Suelen estar formados por un IDS y un cortafuegos que modifica sus reglas dinámicamente para evitar accesos no autorizados a la red

Proxies

Es un servicio, normalmente instalado en un servidor o dispositivo dedicado, que realiza la función de intermediario entre él y los clientes que solicitan un determinado servicio

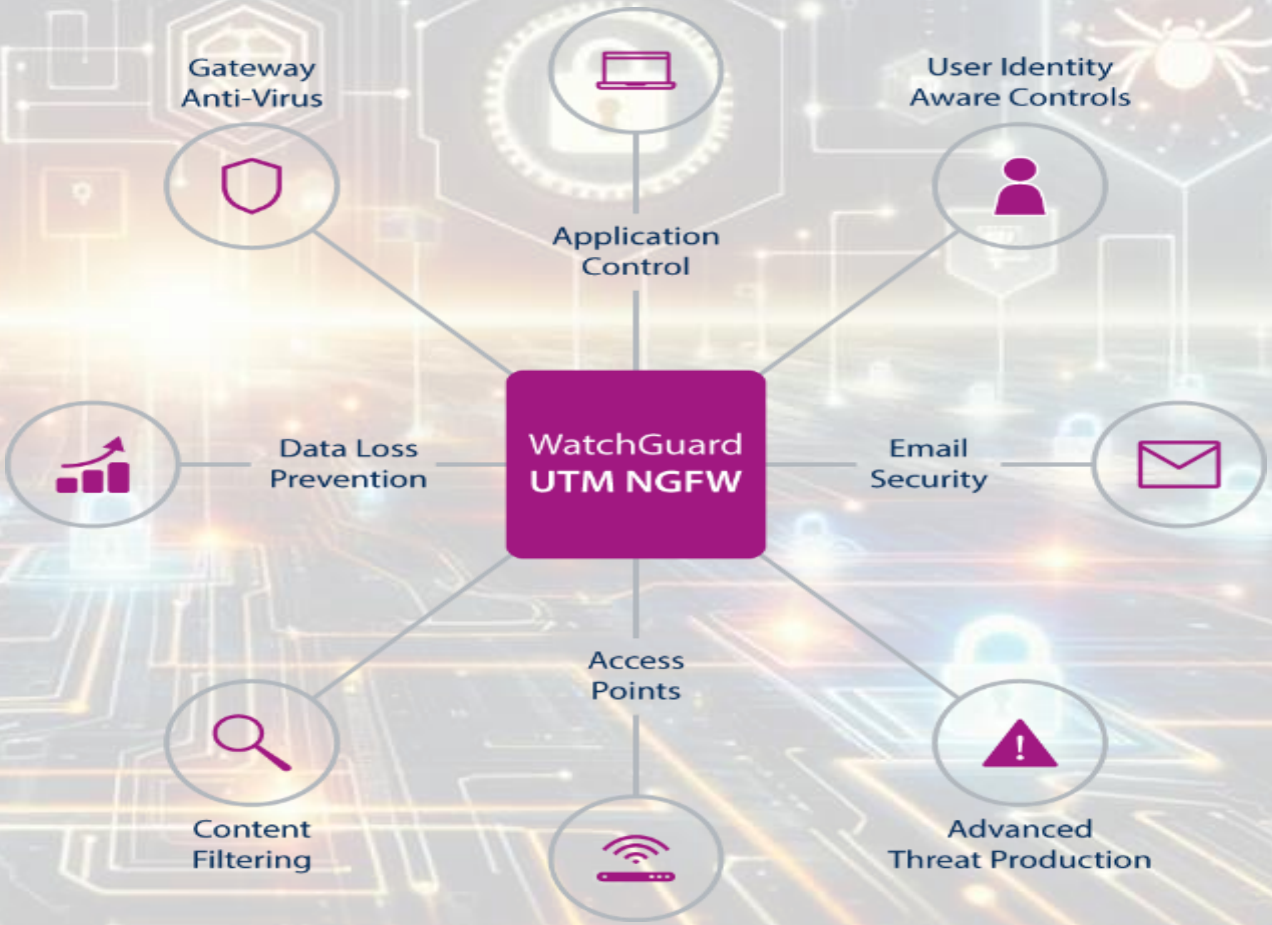
Ventajas

- Velocidad (cache)
- Seguridad frente a dispositivos externos (internet)
- Filtros de contenido y lista de control de acceso.

Seguridad Informática

UTM - Unified Threat Management

Combinan distintas técnicas de protección de redes como cortafuegos, antivirus, antispam, filtro de contenidos, detección y prevención de intrusos redes privadas virtuales y servidor proxy, todo ello en un único aparato.



Seguridad Informática

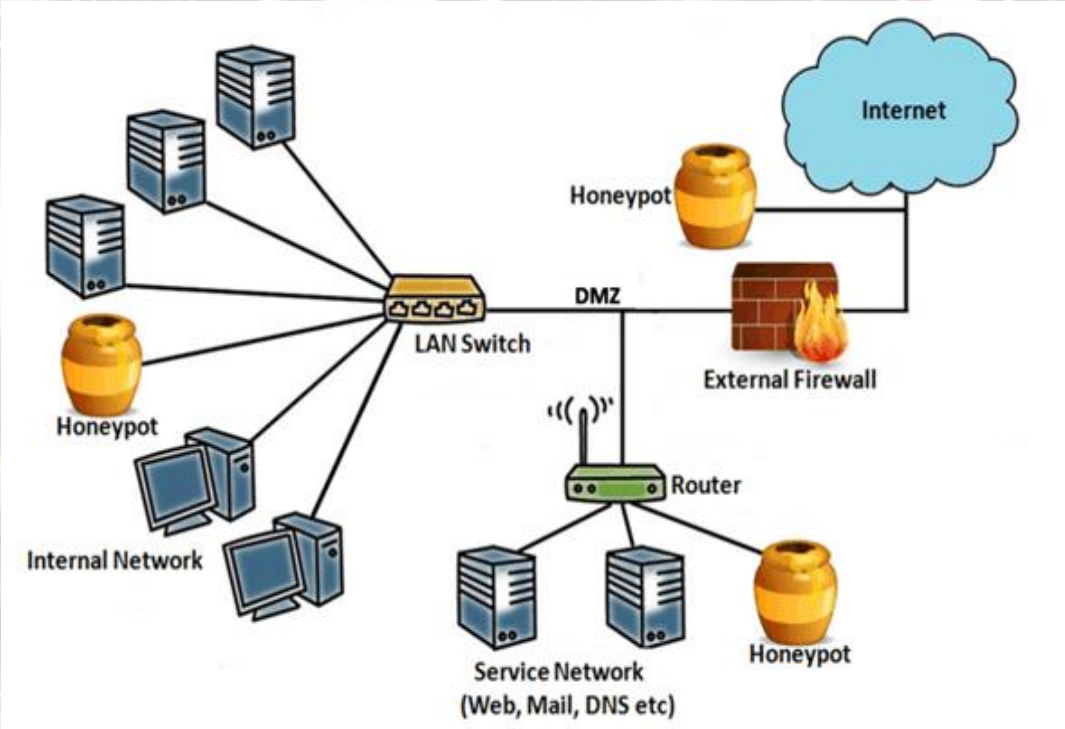
Spam

Hacen referencia a los mensajes de correo electrónico no solicitados, no deseados o con remitente no conocido (o incluso correo anónimo o de falso remitente

HONEYPOTS

Es un servidor configurado y conectado a una red para que pueda ser sondeado, atacado e incluso comprometido por intrusos.

Se trata, por lo tanto, de un equipo o sistema que actúa a modo de señuelo o trampa para los intrusos



Referencias

- BUENDIA, J. F. (2013). Seguridad informática. España: McGraw-Hill.
- ESCRIVA, G. R. (2013). Seguridad Informática. España: Macmillan Iberia SA .
- GMV SECTORES Ciberseguridad. (18 de 03 de 0221). Obtenido de GMV SECTORES Ciberseguridad
- INCIBE. (18 de 03 de 2021). INCIBE - Taxonomia. Obtenido de https://www.incibe-cert.es/taxonomia
- INCIBE-Riesgos. (18 de 03 de 2021). Obtenido de Analisis de Riesgos: https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo
- STEWART, J. M. (2013). Network Security, Firewalls and VPNs. Jones & Bartlett Publishers.
- VIEITES, Á. G. (2014). Gestión de Incidentes de Seguridad Informática. . RA-MA Editorial.

¿PREGUNTAS?

Actividad de Proceso

Elaborar la tarea C3 - Cuestionario de Ciberseguridad (10 puntos)

Completar la tarea y seguir las instrucciones indicadas en Google Classroom.

Referencias

ESCRIVA, G. R. (2013). *Seguridad informática*. España: Macmillan Iberia SA.

Muchas Gracias..!!