#gigatic16

gigaTIC X Congrés Iberoamericà de la Governança i la Gestió Avançada de les TIC

28 abril - Barcelona

Torre Telefónica - Diagonal 00

organitzen:

itSMF ESPAÑA Catalunya

ISACA Trust in, and value from, information systems Barcelona Chapter

Orednarbal sistemes internet seguretat TIC

El enemigo está dentro

Montserrat Labrandero

Factor Humano - Organización Empresarial

Orednarbal sistemes internet seguretat TIC

Sessió S3-2

#gigaTIC16

Tipos de amenazas

- Amenazas ruidosas:

Interfieren directamente en el desarrollo del trabajo

Spam, gusanos, virus

- Amenazas silenciosas:

Pueden pasar desapercibidas

robo de datos, perdidas economicas

El usuario

Amenazas voluntarias:

ocasionar daños

vanidad

Amenazas involuntarias:

negligencia

mal uso

falta de formación

La suplantación de identidad

Phising:

Ingenieria social para adquirir información confidencial o economica en nombre de un tercero

El usuario suplanta:

Una persona se hace pasar por otra

Caso práctico

- Cliente: empresa industrial (Barcelona)
- Sector: metalúrgico
- Empleados: 400
- Facturacion: superior a 25 millones de €
- Centros de trabajo en Catalunya: 2
- Mutinacional filial con mas de 10 plantas repartidas por el mundo

Toma de contacto

- Llamada del cliente
- Reunion inicial
- Propuesta y acciones a realizar
- Recogida de información

Punto de partida

- Correos procedentes de Gmail
- Dirigidos al director general
- Contenido amenazador
- Firmas en el correo
- Reenvios de correo

Nos encontramos ante

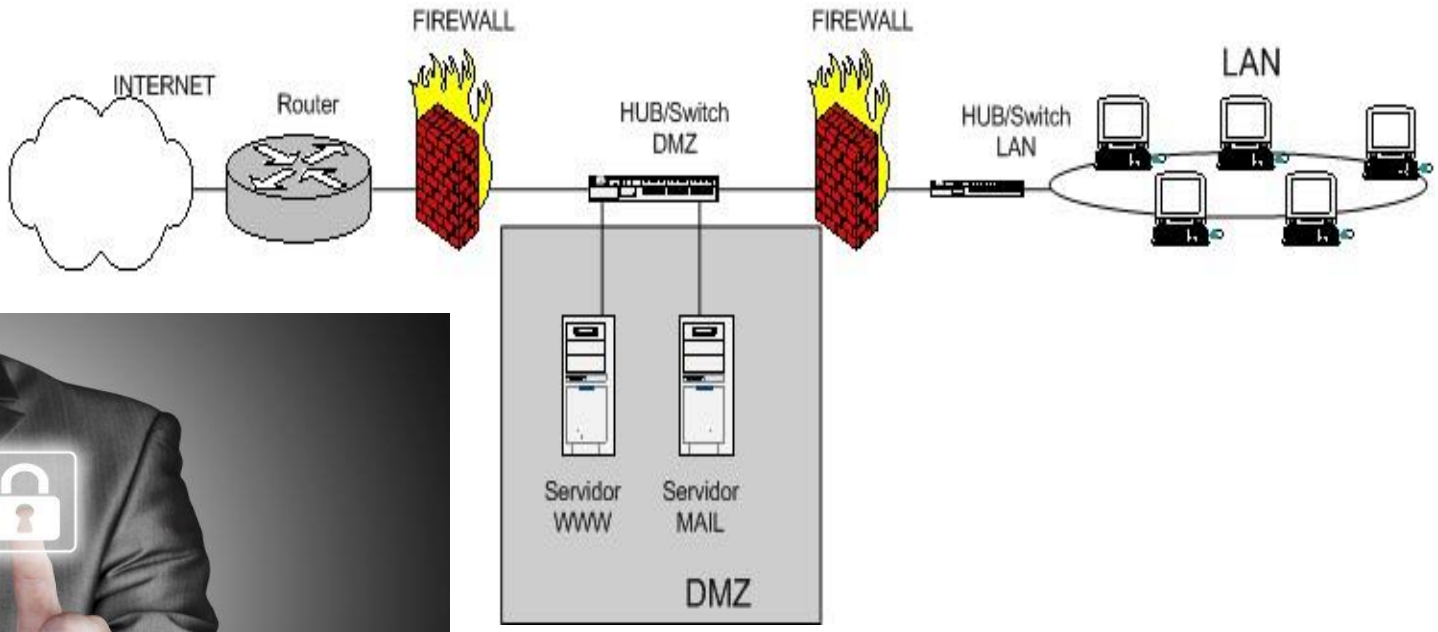
- Un anónimo actuando en nombre de un tercero (suplantación de identidad)

- Cumplimiento inexistente

Primera reunión

- Reunion analisis de la información
- Planificacion de los recursos
- Puesta en marcha
- Recogida de información
- Analisis de información

Esquema protección



Seguridad en internet

Acceso con puertas:

- Control de tiempo
- Control de acceso
- Control de contenido

Deficiencias:

Responsabilidad sin concreción

Normativas no comunicadas

Análisis recursos:

Personas y equipos implicados:

Comité de empresa

Dirección General

Equipo directivo

Total 30 personas (probables)

Fraude y Suplantación de identidad

Situaciones:

Robo de contraseñas o cuentas

Robo de imágenes

Acceso a cuentas y apropiación de datos

Revelacion de secretos

Actividades ilegales

Insultos y amenazas en nombre de terceros

Ips

1 semana de monitorización de logs de conexiones de los usuarios

Analisis de logs antispam y web filter

Conclusiones

La protección del usuario

- Medidas de seguridad organizativas

Recursos técnologicos: firewall, antivirus, antispam, filtrado de contenidos.

- Medias de seguridad normativas:

Redacción de documentos de seguridad, de uso de la información, de uso de la tecnología y formación.

Nuevo planteamiento

Grupos de usuarios

Encuesta

Documentación previa

- Acuerdo de confidencialidad
- Documento – compromiso de la dirección de que la información obtenida, no seria usada en contra de ninguna persona.
- IT – Director general


Conectamos con el mas alla

Gmail

Encuestas

Análisis de perfiles de usuarios

Acceso a Gmail

Contraseña

Información personal

Gmail

La cuenta remitente del correo era:

Holasoyunomismo@Gmail.com

Gmail acceso

Conclusión

La desconfianza es la madre de la seguridad

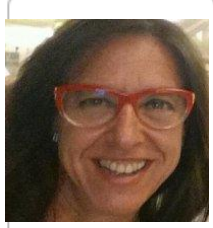
(Aristoteles)

Dime y lo olvido, enséñame y lo recuerdo, involúcrame y lo aprendo.

(Bejamin Franklin)

El enemigo está dentro

Detalls Contacte



Nom del ponent

Montserrat Labrandero

Adreça Correu

mlabrandero@orednarbal.com

Telèfon Contacte

637674438

Twitter

@orednarbal