Bastionado de Redes y Sistemas

Tarea 1

ESTHER CARRILLO GÁLVEZ

Contenido

1. Contexto de la organización

- Describe brevemente la empresa: sector, número de empleados y recursos tecnológicos disponibles.
- Identifica los **tres activos más críticos** y explica por qué lo son para el negocio.

La práctica de negocio de Digital Data está enfocada a la consultoría IT para empresas (servicios B2B). Ha dado su salto al sector con un capital social de 8 empleados que trabajan remotamente desde casa. Los recursos tecnológicos con los que cuentan incluyen software (aplicaciones, sistemas de gestión CRM y ERP) almacenado en la nube y hardware (portátiles, servidores).

Los tres activos más críticos para Digital Data según el riesgo de impacto al negocio y a la confidencialidad, son los siguientes:

· **Portátiles**: los ordenadores corporativos o *endpoints* suponen la puerta de acceso directa a la nube, por lo que el atacante puede vulnerar los dispositivos y comprometer las credenciales.

· **Sistemas de gestión empresarial (CRM y ERP) en la nube**: fuente de información valiosa que contiene datos financieros o facturación. Además de datos comprometidos, como ventas, datos de clientes o contratos. La integridad de estos sistemas es esencial, ya que el compromiso de los mismos podría paralizar la gestión interna y la información sensible de los clientes.

· **Portal del cliente (servidor web):** este servidor aloja la información a la que acceden los clientes para ver el estado de los proyectos. Es de gran criticidad, ya que cualquier caída podría ser percibida por el cliente. Asimismo, cualquier ataque puede poner en riesgo la continuidad del negocio y causar un daño reputacional irreversible.

2. Análisis básico de riesgos

- Elabora una **tabla sencilla** donde se reflejen las amenazas y vulnerabilidades más probables, indicando:
    - Impacto potencial
    - Probabilidad de ocurrencia
    - Nivel de riesgo (bajo, medio o alto)
- Señala cuál consideras el **riesgo más crítico** y justifica tu decisión.

Amenaza	Vulnerabilidad	Impacto potencial	Probabilidad de ocurrencia	Nivel de riesgo
Pérdida/robo de portátil	Falta de cifrado de disco	Información sensible	Baja	Bajo
Ingeniería social (phishing)	Ausencia de MFA	Acceso a ERP o CRM	Alta	Alto
Vulnerabilidad portal web	Inyección SQL	Compromiso de la base de datos subyacente al portal del cilente. Robo de datos o eliminación de información	Alta	Alto

El riesgo más crítico para Digital Data es el ataque de phishing. El nivel de criticidad es alto si se tiene en cuenta que es una empresa 100% remoto y que los empleados se conectan a redes no controladas. Además de tener una puerta de acceso directa a la víctima a través del correo, por lo que se puede comprometer la integridad de la información de ese *endpoint* y de la empresa entera. Es un ataque que está a la orden del día por su facilidad de explotación.

3. Medidas de bastionado

- Propón **al menos cinco medidas concretas** de bastionado adaptadas a la organización.
  Clasifícalas en:
    - **Medidas técnicas**: configuración segura, actualizaciones, redes, contraseñas, etc.
    - **Medidas organizativas**: políticas, formación, copias de seguridad, gestión de incidentes...

Medidas técnicas	
Medida	**Justificación**
Hardening de portátiles mediante Mobile Device Management (MDM) y cifrado de disco	Cifrar el disco para limitar la puerta de acceso a la nube y así mitigar el riesgo de pérdida/robo. La política de actualizaciones es esencial para mantener los dispositivos móviles seguros y protegidos.
Autenticación Multifactor (MFA)	Implantar el multifactor para evitar que un ataque de phishing vulnere las credenciales y reducir el compromiso de la barrera usuario/contraseña (2FA).
Instalación y configuración de Web Application Firewall (WAF)	Proteger las aplicaciones web al filtrar y monitorizar el tráfico HTTP entre una aplicación web e Internet, elevando la seguridad y logrando una capa DiD (Defense In Depth).
Medidas organizativas	
Formación y concienciación en ciberseguridad	Formar a la plantilla para reconocer correos fraudulentos, proteger contraseñas, gestionar datos sensibles y prevenir el phishing, ransomware y otros tipos de ataques.
Procedimiento de Gestión de Incidentes y Respuesta (PIR)	Herramientas que puedan necesitarse durante la gestión del incidente, como el *ticketing*. Disponer de diagramas para proporcionar una visión global y que sirva como ayuda para elaborar una estrategia para afrontar el problema.

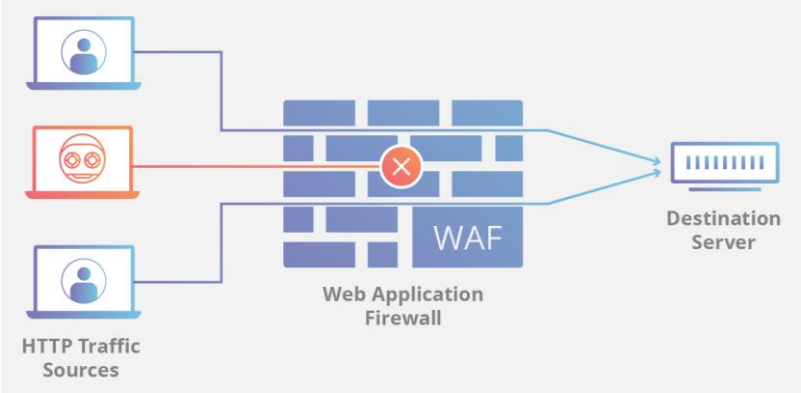

Figura 1. Fuente Cloudfare, *¿Qué es un Web Application Firewall (WAF)?*

4. Plan director de seguridad (visión general)

- Explica cómo estructurarías un **plan director de seguridad** en tu empresa.
- Incluye sus principales apartados: objetivos, alcance, responsables, seguimiento y mejora continua.

La estructura para la elaboración del Plan Director de Seguridad debe contener las siguientes fases:

1. Conocer la situación actual
2. Conocer la estrategia de la organización
3. Definir proyectos e iniciativas
4. Clasificación y priorización
5. Aprobación por la dirección
6. Implantación del PDS

Principales apartados	
Objetivos	· Reducir el compromiso de identidad en la nube mediante el MFA. · Instalación de un WAF para el hardening del servidor web que aloja el portal del cliente. · Prueba del Plan de Contingencia periódica.
Alcance	· Sistemas y equipos implicados, personal, aplicaciones, riesgos específicos, etc.
Responsables	· La CEO asume el rol de aprobar por la dirección y asegurar que la seguridad sea adecuada para el negocio. · Los consultores externos IT se encargan de la ejecución técnica.
Seguimiento y mejora continua	El PDS debe ser revisado una vez al año o antes en caso de un incidente.

Figura 2. Fuente: INCIBE, *Implantando un Plan Director de Seguridad*

5. Reflexión sobre Zero Trust

- Indica qué **principios del modelo Zero Trust** podrían aplicarse a tu empresa y cómo.
- Reflexiona sobre las **dificultades prácticas** que encontrarías para implantar este modelo en un entorno real de pequeña empresa.

Para una empresa que opera 100% en remoto como es Digital Data, el modelo Zero Trust es primordial para una robusta seguridad. Los principios que se deben de aplicar son los siguientes:

Mínimo privilegio: cada usuario debe tener unos permisos en función del grado de responsabilidad de la empresa, donde el privilegio se concede cuando es estrictamente necesario.

Autenticación Multifactor: cada acceso a los sistemas debe ser autenticado y autorizado mediante el MFA.

Microsegmentación: el portal del cliente podría ser comprometido por inyección SQL, lo que supone una posible alteración o eliminación de los datos por parte del atacante. Por ello, el servidor web no concede automáticamente acceso al CRM o ERP a través de la microsegmentación.

No obstante, la implantación de este modelo también se enfrenta a desafíos que dificultan su práctica en un entorno de empresa. Entre ellas se encuentran el elevado coste de las herramientas y licencias, además de una compleja configuración. Este hecho repercutiría paralelamente a la productividad, puesto que el uso del MFA ralentizaría la actividad de la plantilla, llevando a la resistencia del personal. Otro desafío sería la falta de personal dedicado a la gestión del modelo. No cualquier persona llevaría a cabo la labor de manera exhaustiva, por lo que habría un aumento de riesgo de errores de configuración.

6. Bibliografía

Anovo. (s.f.). *Gestión eficiente de recursos tecnológicos en grandes empresas*. Recuperado de https://www.anovo.es/gestion-eficiente-de-recursos-tecnologicos-en-grandes-empresas/

Check Point. (s.f.). *¿Qué es la seguridad de las aplicaciones (AppSec)? Vulnerabilidades OWASP Top 10*. Recuperado de https://www.checkpoint.com/es/cyber-hub/cloud-security/what-is-application-security-appsec/owasp-top-10-vulnerabilities/

Cloudflare. (s.f.). *¿Qué es la defensa en profundidad (Defense in Depth)?*. Recuperado de https://www.cloudflare.com/es-es/learning/security/glossary/what-is-defense-in-depth/

Cloudflare. (s.f.). *¿Qué es un Web Application Firewall (WAF)?*. Recuperado de https://www.cloudflare.com/es-es/learning/ddos/glossary/web-application-firewall-waf/

INCIBE. (s.f.). *Guía de Gestión de Ciberincidentes para el Sector Privado* [PDF]. Recuperado de https://www.incibe.es/sites/default/files/contenidos/guias/doc/incibe-cert_gestion_ciberincidentes_sector_privado.pdf

INCIBE. (s.f.). *Metodología para la elaboración de un Plan Director de Seguridad (PDS)* [Dosier]. Recuperado de https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan-director-seguridad.pdf

INCIBE. (2021). *Top 10 de vulnerabilidades web de 2021*. Recuperado de https://www.incibe.es/empresas/blog/top-10-vulnerabilidades-web-2021

Scribd. (s.f.). *7- Análisis de Riesgos y seguridad de sistema de información*. Recuperado de https://es.scribd.com/document/722976313/7-Analisis-de-Riesgos-y-seguridad-de-sistema-de-informacion

Splashtop. (s.f.). *Mobile Device Management (MDM)*. Recuperado de https://www.splashtop.com/es/blog/mobile-device-management

YouTube. (s.f.). *o33EgLwUl-A* [Video]. Recuperado de https://www.youtube.com/watch?v=o33EgLwUl-A