Pay
OK

CONTÁCTAME

ESCANÉAME

Resumen Ejecutivo
Cybersecurity for Managers Campus BBVA

Índice de Contenidos

6. Levantamiento As Is
7. Marco NIST: Funciones, Actividades y Ejemplos
8. ¿Qué es un proceso de referencia?
9. Workshop: Diseño Colaborativo del Proceso de Referencia
10. To Be
11. Definición y Reutilización de Controles
12. Definición y Reutilización de Controles
13. ¿Cómo incorporar controles en el proceso?
14. Identificación y gestión de gaps de control
15. Monitoreo de los controles

Módulo 7: Caso ficticio: Robo y filtración de datos en una entidad financiera

MÓDULO 1

Conceptos Fundamentales de Internet y Cibercrimen

1.1. Clear Web, Deep Web y Dark Web: diferencias y mitos

Explicación sencilla: Imagina que Internet es como una ciudad gigante.

- **La Clear Web** es la parte visible: calles, tiendas, parques. Es todo lo que puedes encontrar fácilmente con un mapa (Google, Bing, etc.). Aquí están las webs de periódicos, bancos, redes sociales...

- **La Deep Web** son los edificios y habitaciones privadas. Puedes entrar solo con llave (usuario y contraseña), como la intranet de una empresa o tu área privada en el banco. No es ilegal ni peligroso, simplemente es información que no está abierta a todo el público.

- **La Dark Web** sería como un club privado en un sótano al que solo entras con contraseña secreta y un acceso especial (como el navegador Tor). Aquí, por desgracia, se realizan muchas actividades ilegales, pero no todo es necesariamente malo: también hay foros de periodistas y activistas que necesitan anonimato.

Mitos y realidades:

- Mucha gente piensa que la Dark Web es la mayor parte de Internet, pero no es así: es mucho más pequeña que la Clear Web.

- La Deep Web no es peligrosa en sí misma: todos usamos la Deep Web cuando accedemos a nuestro correo privado o a Netflix.

Ejemplo práctico: Cuando accedes a tu cuenta de correo electrónico (Gmail, Outlook), estás en la Deep Web. Cuando navegas por el periódico El País sin iniciar sesión, estás en la Clear Web. Si quisieras entrar a una web oculta que solo funciona con Tor y no aparece en Google, estarías en la Dark Web.

Consejo profesional: No hace falta ser experto para navegar seguro: usa solo webs conocidas y no te aventures en la Dark Web a menos que sepas exactamente lo que haces y por qué.

1.2. Cibercrimen en la Dark Web: actores y modelos de negocio

¿Quiénes actúan en la Dark Web?

En la Dark Web operan grupos organizados de ciberdelincuentes que trabajan como si fueran una empresa:

- Hay "hackers" (algunos éticos, otros criminales)
- "crackers" (que rompen sistemas para hacer daño o robar)
- programadores de virus
- vendedores de datos robados
- y hasta "blanqueadores" que convierten el dinero robado en legal a través de criptomonedas.

¿Por qué es tan rentable el cibercrimen?

- Los ciberdelincuentes pueden atacar a miles de personas en todo el mundo desde su casa, sin moverse de la silla.
- Se estima que el cibercrimen mueve más dinero que el tráfico de drogas.
- Hoy existe el "Cibercrimen como Servicio": puedes comprar ataques informáticos, programas para robar datos o incluso alquilar "botnets" (redes de ordenadores infectados) por unos pocos euros.

Ejemplo sencillo: Un ciberdelincuente roba datos de tarjetas de crédito y los vende en foros de la Dark Web. Otro usuario los compra y los utiliza para hacer compras online. Si la tarjeta es tuya, tú eres la víctima.

Consejo práctico: No pongas nunca tus datos bancarios en webs dudosas y desconfía de "chollos" demasiado buenos para ser verdad.

1.3. Ciberataques APT: cómo y por qué suceden

¿Qué es una APT?

Una Amenaza Persistente Avanzada (APT) es un ataque muy sofisticado, dirigido a una empresa o institución concreta, donde los atacantes se cuelan en el sistema y permanecen ocultos durante semanas o meses.

Fases del ataque:

1. **Reconocimiento:** Los atacantes investigan todo sobre la empresa y sus empleados (redes sociales, webs públicas, prensa...).

2. **Diseño del ataque:** Preparan el ataque, incluso creando una copia del sistema para practicar.
3. **Intrusión:** Consiguen entrar (normalmente engañando a un empleado para que abra un archivo malicioso).

4. **Persistencia:** Se aseguran de poder seguir entrando y salir cuando quieran.

5. **Explotación:** Roban datos, dinero o controlan los sistemas.

Ejemplo real: Una pyme es atacada porque tiene menos seguridad. Desde ahí, los atacantes saltan a una gran empresa cliente, aprovechando la relación de confianza.

¿Quién está en riesgo?

Aunque suelan ser grandes empresas o gobiernos, las pymes son objetivos frecuentes porque suelen ser el "eslabón débil".

Consejo profesional: No bajes la guardia por ser pequeño: los atacantes buscan el camino más fácil.

MÓDULO 2

Amenazas Cotidianas y Fraudes Digitales

2.1. Monitorización y Egosurfing: cómo proteger tu identidad digital

¿Qué es el egosurfing?

Buscar tu propio nombre en Google (o cualquier buscador) para saber qué información hay sobre ti. ¿Por qué es importante? Porque si tú puedes verlo, los ciberdelincuentes también.

¿Qué puedes descubrir haciendo egosurfing?

- Fotos tuyas en redes sociales abiertas.

- Comentarios en foros antiguos.

- Datos personales en listados públicos.

Ejemplo sencillo: Buscas tu nombre y encuentras tu dirección y tu fecha de nacimiento en una web de antiguos alumnos. Un ciberdelincuente podría usar esa información para suplantarte.

¿Qué debes hacer si encuentras información sensible?

- Solicita su retirada al propietario del sitio web.
- Revisa la privacidad de tus redes sociales.
- Usa el "derecho al olvido" si vives en Europa.

Consejo profesional: Haz egosurfing al menos una vez al año y revisa qué datos tuyos están visibles. ¡La prevención empieza por saber qué saben de ti
¡Error! Nombre de archivo no especificado.

2.2. Business Email Compromise (BEC): el fraude por correo empresarial

¿Qué es el BEC?

Es un fraude donde el atacante se hace pasar por alguien de confianza (el jefe, un proveedor, un abogado) y pide una transferencia urgente de dinero.

¿Por qué funciona tan bien?

- El correo parece auténtico.
- El mensaje es urgente y personal.
- A menudo usan datos reales de la empresa (que han conseguido en la web o redes sociales).

Tipos comunes de BEC:

- Suplantación de proveedor (piden pagar una factura falsa).
- Fraude del CEO (el "jefe" pide una transferencia urgente).
- Cambios de cuenta bancaria para nóminas.

Ejemplo real: Recibes un correo del "director financiero" pidiendo cambiar la cuenta de un proveedor. Si no verificas, puedes transferir dinero a los delincuentes.

Consejo profesional: Ante cualquier solicitud de dinero o cambios bancarios, verifica siempre por teléfono o en persona, aunque el correo parezca real.

2.3. Pharming, Fake News y Malvertising: técnicas de engaño en la red

Pharming: Tiendas online falsas que parecen reales. Buscan robar tus datos bancarios o tu dinero.

Fake News: Noticias falsas que buscan manipularte, estafarte o instalarte un malware.

Malvertising: Anuncios maliciosos en webs reales: al hacer clic, te infectan con virus o te llevan a webs fraudulentas.

Ejemplo sencillo: Ves un anuncio en Instagram de zapatillas baratas, entras en la tienda, pagas y nunca recibes el producto. Además, tus datos de tarjeta quedan comprometidos.

Consejo profesional: Desconfía de tiendas desconocidas y nunca compres desde un anuncio sin comprobar la web. Usa siempre métodos de pago seguros.

2.4. Riesgos de las extensiones del navegador

¿Qué es una extensión?

Un pequeño programa que instalas en tu navegador (Chrome, Firefox, etc.) para añadir funciones (bloquear anuncios, traducir páginas, etc.).

¿Dónde está el peligro?

Algunas extensiones espían lo que haces, roban tus contraseñas o instalan virus.

Ejemplo sencillo: Instalas una extensión para cambiar el color de Facebook. Sin saberlo, roba tus credenciales y accede a tu correo.

Consejo profesional: Instala solo extensiones de tiendas oficiales y revisa los permisos que piden. Si una extensión pide acceso a tus datos en todas las webs, ¡desconfía
¡Error! Nombre de archivo no especificado..

2.5. Firewalls y Proxies: escudos digitales

Firewall: Es como un portero digital, solo deja pasar a quien tiene permiso.

Proxy: Es un intermediario entre tu ordenador e Internet, que filtra y oculta tu dirección real.

Ejemplo sencillo: El firewall de tu empresa bloquea accesos sospechosos. El proxy impide que accedas a webs peligrosas.

Consejo profesional: Asegúrate de tener un firewall activo en tu red y en tu ordenador. En empresas, usa proxies para controlar y registrar el tráfico de la red.

2.6. Antivirus: el guardián de tu información

¿Qué hace el antivirus?

Detecta y elimina software malicioso (virus, troyanos, etc.).

¿Es suficiente tener un antivirus?

No. Los virus evolucionan constantemente y el antivirus puede no detectar los más nuevos. Es fundamental mantenerlo actualizado y combinarlo con buenas prácticas (no abrir archivos sospechosos, no descargar de fuentes desconocidas, etc.).

Ejemplo sencillo: Recibes un archivo adjunto en un correo. El antivirus lo analiza y lo bloquea porque encuentra un virus.

Consejo profesional: Instala un antivirus de confianza, mantenlo actualizado y no bajes la guardia. La prevención es tu mejor defensa.

2.7. Ataque Man in the Middle (MitM): cómo proteger las comunicaciones

¿Qué es un MitM?

Un ciberdelincuente se coloca entre tú y el sitio web al que accedes (por ejemplo, tu banco), interceptando la información.

¿Cómo ocurre?

- Usando redes WiFi públicas y sin cifrar.
- Creando puntos WiFi falsos con nombres parecidos a los reales (por ejemplo, "WiFi_Aeropuerto_Gratis").

Ejemplo sencillo: Te conectas al WiFi de una cafetería y accedes a tu banca online. Si la red no es segura, un atacante puede robar tus credenciales.

Consejo profesional: No accedas a servicios sensibles desde redes públicas o abiertas. Si debes hacerlo, usa una VPN.

2.8. Seguridad del WiFi doméstico y amenazas

Principales riesgos:

- Usar contraseñas débiles o la de fábrica.
- No cifrar la red WiFi.
- Tener el WPS activado.

¿Qué puede pasar?

Un vecino o un ciberdelincuente puede colarse en tu red, espiar tu tráfico, robar contraseñas o infectar tus dispositivos.

Consejo profesional:

- Cambia la contraseña por defecto de tu router.
- Usa cifrado WPA2 o WPA3.
- Cambia el nombre de la red (SSID).

- Desactiva WPS.
- Actualiza el firmware del router.
- Restringe el acceso solo a dispositivos autorizados.

2.9. VPN personal: ventajas y usos

¿Qué es una VPN?

Una red privada virtual que cifra tu tráfico y oculta tu dirección IP.

¿Para qué sirve?

- Navegar anónimamente.
- Proteger tu información en redes públicas.
- Acceder a contenido restringido por ubicación.

Ejemplo sencillo: Trabajas desde una cafetería, con la VPN activa, tus datos viajan cifrados y seguros.

Consejo profesional: Elige una VPN de confianza, instálala en tus dispositivos y úsala especialmente cuando te conectes fuera de casa o la oficina.

MÓDULO 3

Seguridad de la Información y Gestión de Incidentes

3.1. Pilares de la Seguridad de la Información

La seguridad de la información se apoya en tres grandes pilares:

- **Confidencialidad:** Solo quienes tienen permiso pueden acceder a la información. Imagina que tus claves bancarias solo las conoces tú y tu banco, nadie más puede verlas.
- **Integridad:** La información debe mantenerse exacta y sin alteraciones no autorizadas. Es como asegurarte de que tu extracto bancario no haya sido modificado por terceros.
- **Disponibilidad:** Los datos y sistemas deben estar accesibles cuando los necesitas. Por ejemplo, que puedas consultar tus movimientos bancarios en cualquier momento.

Ejemplo práctico: Si eres emprendedor y tienes una tienda online, debes proteger la información de tus clientes (confidencialidad), garantizar que los pedidos no se manipulan (integridad) y que la web siempre esté operativa (disponibilidad).

3.2. Incidente de Seguridad vs Incidencia IT

No toda interrupción tecnológica es un ciberataque.

- **Incidente de seguridad:** Implica intencionalidad, un atacante y afecta la confidencialidad, integridad o disponibilidad. Ejemplo: Un hacker logra acceder a los datos de tus clientes.

- **Incidencia IT:** Es un problema técnico sin mala intención, como la caída del servidor por una avería.

Diferencia clave: Un incidente de seguridad siempre involucra a un atacante y puede ser recurrente y grave. Una incidencia IT es un fallo técnico accidental.

3.3. Tipos de Ciberamenazas

Las amenazas digitales evolucionan constantemente. Las más comunes son:

- **Malware:** Virus, troyanos y ransomware que buscan infectar y robar información.

- **Ataques web:** Páginas falsas o enlaces maliciosos.

- **Phishing:** Correos o mensajes que suplantan entidades legítimas para robar credenciales.

- **Ataques a aplicaciones web:** Aprovechan errores en las webs para robar datos.

- **Spam:** Correos no deseados que pueden incluir amenazas.

- **DDoS:** Ataques que saturan un servidor hasta dejarlo inaccesible.

- **Fugas de datos:** Cuando información confidencial sale de la empresa.

- **Amenaza de insider:** Empleados desleales o descuidados que ponen en riesgo la seguridad.

- **Botnets:** Redes de ordenadores infectados para lanzar ataques masivos.

Ejemplo sencillo: Un empleado recibe un correo sospechoso, hace clic y descarga un virus que cifra toda la información de la empresa (ransomware).

3.4. Metodología SANS: Recursos y Fases

La metodología SANS es una de las más reconocidas para gestionar incidentes de seguridad. Se basa en disponer de:

- **War Room:** Un espacio seguro y privado para trabajar en la resolución del incidente.

- **Jump Bag:** Un kit preparado con todo el material necesario (USBs, discos, herramientas) para actuar rápidamente.

Fases SANS:

1. Preparación
2. Identificación
3. Contención
4. Erradicación
5. Recuperación
6. Lecciones aprendidas

Ejemplo real: Si detectas un ataque en tu empresa, reúnes a tu equipo en una sala (war room), usas las herramientas del jump bag y sigues los pasos para controlar y solucionar el incidente.

MÓDULO 4

Defensa Personal

1. Las brechas y hackeos más grandes del mundo

Los ciberataques son como robos digitales en los que los delincuentes consiguen acceder a datos privados de empresas y personas. Cada año hay más ataques y los daños son mayores.

Ejemplo: Imagina que tu banco sufre un hackeo y los datos de todos los clientes se hacen públicos. Esto ocurrió con Yahoo!, donde miles de millones de cuentas fueron robadas. Las consecuencias son graves: robo de identidades, dinero y pérdida de confianza.

2. Internet desde la perspectiva de un cibercriminal

1. La estructura de Internet: Un entorno perfecto para el cibercrimen

Internet tiene varias capas.

- Clear Web: Es lo que ves al buscar en Google.
- Deep Web: Son partes privadas, como el área de clientes de tu banco.
- Dark Web: Es la zona oscura y anónima, donde se esconden los delincuentes.

Ejemplo: Comprar en Amazon es Clear Web. Entrar a tu cuenta bancaria es Deep Web. Comprar datos robados en foros secretos es Dark Web.

2. ¿Cómo ven internet los cibercriminales?

Los delincuentes ven internet como una gran oportunidad para ganar dinero robando datos o vendiendo servicios ilegales.

Ejemplo: Un hacker roba contraseñas y las vende a otros delincuentes, que luego las usan para sacar dinero de cuentas bancarias.

3. Servicios y precios en el mercado negro (2025)

Existe un mercado ilegal donde se venden ataques y datos robados a precios muy bajos.

Ejemplo:

- Piratear una red social: $230.
- Ataque para dejar fuera de servicio una web: $26 por hora.
- Rastrear a una persona: $195.

Esto significa que cualquier persona con malas intenciones y algo de dinero puede comprar estos servicios.

4. Conclusión y advertencia

El cibercrimen es un gran negocio, pero es ilegal y puede llevar a la cárcel.

Ejemplo: Si alguien usa datos robados para suplantar tu identidad y sacar un crédito a tu nombre, ambos pueden tener problemas legales si participan en este tipo de actividades.

3. Visual Hacking (Shoulder Surfing)

Es una técnica sencilla donde alguien mira tu pantalla por encima del hombro para robar información.

Ejemplo: Estás en un café y un desconocido observa cómo escribes tu contraseña. En un estudio, el 91% de los intentos de visual hacking tuvieron éxito.

Consejo: Siempre bloquea tu pantalla cuando te levantes y no dejes documentos confidenciales a la vista.

4. Ejemplos de Phishing y Smishing

Phishing: Recibes un correo falso que parece de tu banco, pidiéndote que ingreses tus datos en una web falsa. Al hacerlo, el delincuente se queda con tus claves.

Smishing: Un SMS urgente te pide hacer clic en un enlace o responder con tus datos personales.

Ejemplo sencillo: Un correo con errores ortográficos y enlaces raros es sospechoso. Si dudas, llama a tu banco antes de hacer nada.

Consejo: Nunca compartas información sensible por correo o SMS.

5. Tips de seguridad para conexiones y dispositivos

Redes WiFi: Evita conectarte a redes públicas o de hoteles. Si debes hacerlo, usa una VPN o tu conexión móvil.

Dispositivos: No uses USBs de origen desconocido ni cargadores públicos, ya que pueden instalar virus en tu equipo.

Ejemplo real: En una cumbre internacional, se entregaron USBs infectados para espiar a los asistentes.

6. ¿Por qué es tan importante la gestión de contraseñas?

Tus contraseñas protegen tus datos. Si usas contraseñas débiles o repetidas, es más fácil que los delincuentes las descubran.

Ejemplo práctico: Usar “123456” como clave es como dejar la puerta de tu casa abierta. Mejor usa frases largas y difíciles de adivinar y cambia tus claves si sospechas de un robo de datos.

Consejo: Utiliza un gestor de contraseñas y activa el doble factor de autenticación.

7. ¿Por qué el producto eres tú cuando una app es gratis?

Si una aplicación es gratis, normalmente recolecta y vende tus datos para ganar dinero.

Ejemplo: Una app para editar fotos te pide acceso a tus contactos, ubicación y galería: tus datos pueden ser vendidos a terceros o usados para publicidad.

Consejo: Revisa los permisos antes de instalar apps y elimina las que no uses.

MÓDULO 5

Herramientas y Procesos para la Gestión de Incidentes

5.1. Ciclo de Vida de la Respuesta ante Incidentes

El proceso estándar consta de cuatro fases:

1. **Preparación:** Formación del equipo y definición de protocolos.
2. **Detección y análisis:** Monitorización y análisis de alertas.
3. **Contención, erradicación y recuperación:** Limitar el daño, eliminar la amenaza y volver a la normalidad.
4. **Actividad post-incidente:** Aprender de lo ocurrido y mejorar.

Ejemplo: Tras resolver un ataque de phishing, el equipo revisa qué se hizo bien y qué se puede mejorar para la próxima vez.

5.2. SIEM: Definición, Arquitectura y Ventajas

¿Qué es un SIEM?

Es un sistema que recoge y analiza automáticamente todos los eventos de seguridad de la empresa (logs, alertas, accesos) para detectar amenazas.

Ventajas:

- Centraliza la información.
- Permite detectar ataques en tiempo real.
- Facilita el cumplimiento de normativas.

Ejemplo sencillo: El SIEM detecta que un empleado está intentando acceder a información confidencial fuera de su horario habitual y lanza una alerta.

5.3. Logs: Tipos, Estructura y Tratamiento

¿Qué es un log?

Es un registro de todo lo que ocurre en un sistema: accesos, errores, cambios y más.

Tipos de logs:

- Logs de sistemas (Windows, Linux)
- Logs de red (routers, firewalls)

- Logs de aplicaciones (web, correo, bases de datos)

Ejemplo práctico: Si hay una fuga de datos, los logs ayudan a saber quién accedió y cuándo, facilitando la investigación.

5.4. Automatización y Otras Funcionalidades Clave

Hoy existen herramientas que automatizan tareas repetitivas, como abrir tickets o enviar alertas, permitiendo que los expertos se concentren en lo importante. Además, los SIEM modernos pueden integrarse con otros sistemas y exponer información útil a través de API.

Ejemplo: El SIEM detecta un comportamiento sospechoso, automáticamente bloquea el acceso y notifica al equipo de seguridad.

MÓDULO 6

Gestión Segura de los Procesos Empresariales

1. Resumen: Fraude y Proceso Seguro

El fraude es cualquier engaño para obtener un beneficio propio. Para evitarlo, las empresas crean procesos seguros con controles que detectan y bloquean fraudes.

Ejemplo: Alguien usa una tarjeta robada para comprar online. Un control seguro puede detectar el patrón raro y bloquear la transacción.

2. Área de Gestión del Fraude

Es el departamento encargado de anticipar y combatir el fraude, usando datos y tecnología.

Ejemplo: Un equipo revisa los pagos sospechosos y forma a los empleados para detectar intentos de fraude.

3. Responsable del Proceso en la Gestión del Fraude

Es la persona que coordina y supervisa que los procesos sean seguros.

Ejemplo: No es quien hace todo, pero sí quien asegura que todos los controles funcionen y el equipo esté informado.

4. Escenarios que Requieren Gestión del Fraude

El área antifraude actúa cuando hay nuevas normativas, procesos, controles o ataques reales.

Ejemplo: Si un banco lanza un nuevo producto digital, el área de fraude revisa los riesgos antes de ponerlo en marcha.

5. ¿En qué consiste la fase de ideación?

Es el primer paso para analizar los procesos clave y anticipar riesgos usando mapas de calor.

Ejemplo: Antes de cambiar el proceso de apertura de cuentas, se revisan los posibles fraudes y problemas que pueden surgir.

6. Levantamiento As Is

Consiste en documentar cómo es el proceso actualmente, identificando puntos débiles y controles existentes.

Ejemplo: Se observa que muchos fraudes ocurren porque no se verifica bien la identidad del cliente al inicio.

7. Marco NIST: Funciones, Actividades y Ejemplos

El marco NIST es una guía internacional con 5 pasos para gestionar la seguridad:

1. Identificar riesgos
2. Proteger con controles
3. Detectar anomalías
4. Responder a incidentes
5. Recuperar datos y reputación

Ejemplo: Si hay un ataque, el equipo usa NIST para saber cómo actuar, desde identificar hasta recuperar.

8. ¿Qué es un proceso de referencia?

Es un modelo ideal de proceso seguro que sirve de ejemplo para toda la empresa.

Ejemplo: El proceso ideal para abrir una cuenta online incluye controles antifraude que luego se aplican a otros productos.

9. Workshop: Diseño Colaborativo del Proceso de Referencia

Es una reunión donde varios expertos y responsables proponen y acuerdan mejoras en los procesos para hacerlos más seguros.

Ejemplo: Durante el workshop, el equipo decide añadir una doble verificación de identidad en el registro de nuevos clientes.

10. To Be

Se define cómo debería funcionar el proceso idealmente, con todos los controles agrupados y documentados.

Ejemplo: El proceso “To Be” de onboarding digital incluye verificación biométrica, scoring antifraude y validación documental automática.

11. Definición y Reutilización de Controles

Si ya existe un control útil, se reutiliza. Si no, se crea uno nuevo y se añade al catálogo para compartirlo.

Ejemplo: Si hay un buen control para validar documentos, se reutiliza en todos los procesos similares.

12. Definición y Reutilización de Controles

El ciclo se repite: siempre que sea posible, reutilizar. Si no existe, definir y publicar para futuras ocasiones.

Ejemplo: Se detecta un nuevo tipo de fraude en un proceso y se crea un control específico, que luego podrán usar otros equipos.

13. ¿Cómo incorporar controles en el proceso?

Busca en el catálogo los controles existentes o diseña uno nuevo si es necesario. Así se garantiza que todos los riesgos estén cubiertos.

Ejemplo: Si tu proceso necesita verificación biométrica y no hay control en el catálogo, se crea uno y se añade para futuras aplicaciones.

14. Identificación y gestión de gaps de control

Se detectan debilidades en los controles y se definen planes de acción para cerrarlas.

Ejemplo: Una herramienta llamada Fraud Scoring Tool puntúa el proceso y ayuda a priorizar mejoras. Además, se hacen simulaciones (Crash Testing) para ver si los controles realmente funcionan ante ataques reales.

15. Monitoreo de los controles

Supervisar de forma continua si los controles funcionan, usando indicadores y aprendiendo de los errores.

Ejemplo: Si un control deja de funcionar, se detecta y se mejora. Si ocurre un fraude, se analiza para evitar que se repita.

MÓDULO 7

Caso ficticio: Robo y filtración de datos en una entidad financiera

1. Reconocimiento y selección del objetivo (Fase de reconocimiento)

Un grupo de ciberdelincuentes decide atacar a la entidad financiera "Banco Horizonte S.A. (nombre ficticio)". Primero, dedica varias semanas a recopilar información pública sobre el banco y sus empleados. Analizan:

- La página web corporativa (organigrama, contactos de prensa, notas de prensa).
- Perfiles de empleados en LinkedIn (especialmente de TI y finanzas).
- Noticias sobre proveedores tecnológicos del banco.
- Redes sociales, buscando información sobre procesos internos y campañas recientes.

Ejemplo realista: Descubren que uno de los proveedores de software del banco acaba de anunciar una integración tecnológica en la web corporativa del banco. Este detalle les da pistas sobre qué sistemas podrían estar expuestos y a qué personas dirigir su ataque.

2. Preparación y ataque de ingeniería social (Fase de acceso inicial)

Con la información recopilada, los atacantes diseñan un correo de phishing muy creíble dirigido a un empleado del área de pagos. El correo parece enviado por el proveedor tecnológico, tiene su logo y firma, y solicita al empleado que acceda a un portal "para validar unos cambios críticos en el sistema". El enlace lleva a una web falsa que simula el portal del proveedor.

El empleado, confiado por el tono profesional del mensaje y al reconocer el nombre del proveedor, introduce sus credenciales reales en la página falsa.

Error común: El empleado no verifica el dominio del remitente ni consulta con su responsable antes de introducir sus datos, lo que facilita el robo de credenciales.

3. Intrusión y movimiento lateral (Fase de escalada y persistencia)

Los atacantes usan las credenciales robadas para acceder al entorno corporativo. Una vez dentro, buscan aumentar sus privilegios. Aprovechan vulnerabilidades conocidas en un servidor (por ejemplo, una actualización de seguridad pendiente) para obtener permisos de administrador.

Instalan una puerta trasera (backdoor) y crean una cuenta de usuario oculta, de modo que pueden volver a entrar cuando lo deseen sin depender de las credenciales robadas inicialmente.

Ejemplo técnico: Utilizan herramientas automatizadas para buscar cuentas con permisos excesivos y servidores con software sin actualizar. Encuentran un servidor con una vulnerabilidad crítica y lo explotan para tomar el control total del sistema.

4. Exfiltración de datos (Fase de explotación)

Ya con acceso privilegiado, los atacantes localizan la base de datos de clientes y datos financieros. Para no levantar sospechas, extraen la información en pequeños paquetes cifrados y la envían fuera de la red durante las horas de menor actividad (madrugada).

Ejemplo realista: Copian listas de clientes, datos de cuentas, historiales de transacciones, emails, teléfonos y hasta contraseñas cifradas. Utilizan servicios de almacenamiento en la nube gratuitos o conexiones VPN para evadir los controles y dificultar el rastreo.

5. Fuga y venta de datos en la Dark Web (Fase de monetización)

Con los datos en su poder, los ciberdelincuentes publican un anuncio en un foro de la Dark Web, ofreciendo los datos a la venta. Incluyen “muestras” (listados parciales de clientes) para demostrar que la información es real y fresca.

Ejemplo: El anuncio ofrece “100.000 registros de clientes de banco español, con datos completos y credenciales de acceso”, solicitando pago en criptomonedas. Otros criminales pueden comprar esta información para fraudes, suplantaciones o más ataques.

6. Detección del incidente por el banco (Fase de detección y análisis)

El equipo de ciberseguridad del banco observa alertas inusuales en su sistema SIEM:

- Accesos desde direcciones IP extranjeras fuera del horario habitual.
- Descargas masivas de datos en intervalos cortos.
- Uso de cuentas administrativas en sistemas donde no deberían operar.

Se activa el protocolo de respuesta a incidentes y se convoca al equipo de gestión de crisis. El equipo revisa los logs, identifica la cuenta comprometida y detecta la puerta trasera instalada.

Buena práctica: El banco contaba con monitorización activa y alertas automáticas, lo que permite identificar el incidente antes de que se produzca un daño aún mayor.

7. Contención y erradicación (Fase de respuesta y remediación)

- Se bloquean de inmediato todas las cuentas sospechosas y se fuerza el cambio de contraseñas a todos los empleados.
- Se aísla el servidor afectado de la red y se realiza un análisis forense.
- Se elimina la puerta trasera y se revisan todos los sistemas en busca de otras posibles intrusiones.
- Se aplican los parches de seguridad pendientes y se revisan los privilegios de las cuentas administrativas.
- Se comunica el incidente a las autoridades y reguladores según la normativa vigente.

Ejemplo de error a evitar: No avisar inmediatamente a los responsables o tratar de tapar el incidente puede agravar la situación y acarrear sanciones legales.

8. Recuperación y comunicación (Fase de recuperación y post-incidente)

- Se restaura la base de datos desde copias de seguridad limpias y se verifica la integridad de los datos.
- Se refuerzan las medidas de seguridad: doble factor de autenticación, segmentación de redes, campañas de formación interna sobre phishing y protocolos de verificación para solicitudes sensibles.
- Se notifica individualmente a los clientes afectados, explicando el alcance de la fuga y las medidas de protección recomendadas.
- Se realiza un informe detallado para la dirección y aprendizaje de la experiencia, mejorando los procedimientos de prevención y respuesta.

9. Lecciones aprendidas y refuerzo de la seguridad

- Se revisan y actualizan los procedimientos internos de respuesta a incidentes y se realiza una simulación de ataque (tabletop exercise) para evaluar la preparación del equipo.
- Se implanta un programa de formación continua a empleados y se limita la información sensible publicada en la web y redes sociales.

- Se acuerda un protocolo de verificación adicional para todas las órdenes de pago o cambios críticos en sistemas.

Resumen y consejos clave

Este caso ficticio ejemplifica cómo un ataque puede comenzar con un pequeño descuido humano y, mediante movimientos sigilosos y técnicos, acabar en una fuga masiva de datos en la Dark Web. La detección temprana, los protocolos claros y la formación continua son esenciales para minimizar el daño y proteger la reputación de la entidad financiera.

Recomendaciones:

- Verifica siempre la legitimidad de correos y solicitudes sensibles.
- Mantén todos los sistemas actualizados.
- Limita los privilegios de las cuentas administrativas.
- Forma regularmente a los empleados en ciberseguridad.
- Ten protocolos claros de actuación y comunicación ante incidentes.

Para profundizar más:

- INCIBE - Guías y recursos para empresas
- ENISA - Guías de ciberseguridad
- ¿Estás preparado para hacer frente a una fuga de datos? - INCIBE.
- Recolección de pruebas digitales – INCIBE.

1 **Grupo de ayuda gratis PayOk:** Fintech, Adquirencia, Pagos Electrónicos, Gestión Riesgos, Medios de Pago, PBCFT y Compliance.

2 **Newsletter Radar Financiero Adquirencia PayOk**

3 **Sígueme con un click en LinkedIn**

4 **Tarjeta digital de contacto**