Brechas e Incidentes de Seguridad – Causas Raíz

Seolito Rodriguez, MBA

CISSP, CRISC, CISM, CISA, Security+, Pentest+, CySA+, MCT, MCSA 365, A+, Network+, CCNA, ITIL…..

¿Es posible prevenir la mayoría de los ataques cibernéticos?

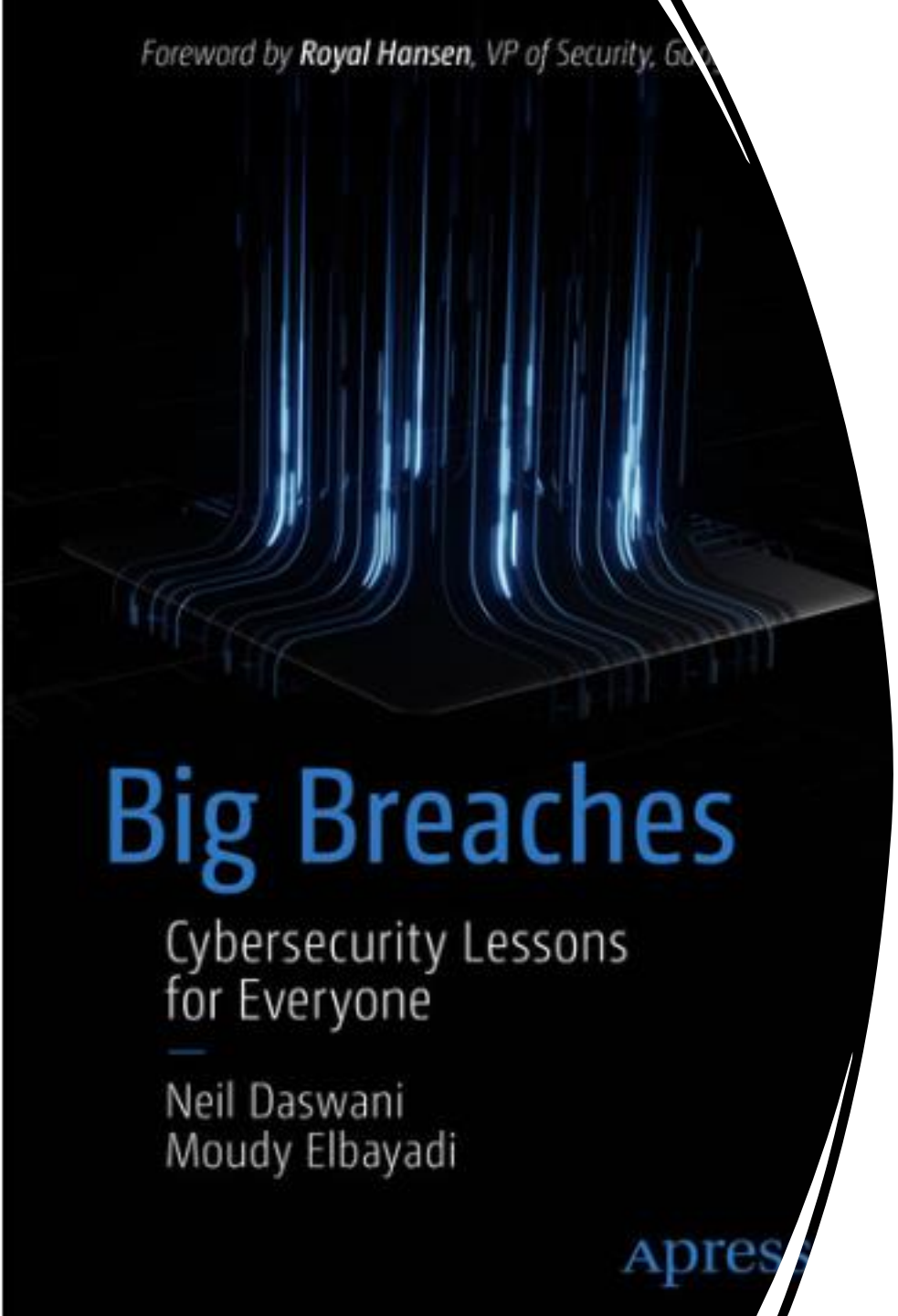
Agenda

BRECHAS E INCIDENTES

CAUSAS RAÍZ

ESTRATEGIAS Y CONTRAMEDIDAS

EN RESUMEN



Brechas Digitales Grandes – Viejas y Recientes

Un ataque de ingeniería social permitió al actor de amenazas introducirse en el entorno de MGM y establecer un punto de apoyo. Debido al error común de reutilizar contraseñas, CyberArk Labs. Con información adicional recopilada del perfil de LinkedIn de un usuario de alto valor, esperaban engañar al servicio de asistencia técnica para que restableciera la autenticación multifactor (MFA) del usuario. Tuvieron éxito.

MGM Resorts confirma que los piratas informáticos robaron datos personales de los clientes durante el ciberataque

Página de Carly @carlypage_ / 8:05 a. m.EDT • 6 de octubre de 2023

Comentario

Un miembro del grupo, denominado MemberX, logró acceder a la red del Ministerio de Hacienda y obtener permisos de administrador de dominio utilizando credenciales previamente comprometidas de una conexión VPN.

El robo de estas credenciales se logró a través de la instalación de una forma cifrada de la herramienta de pentesting legítima Cobalt Strike en una sub red del organismo.

Detalles de cómo se produjo el ataque del ransomware Conti a Costa Rica

Las investigaciones de Microsoft determinaron que Storm-0558 obtuvo acceso a cuentas de correo electrónico de clientes utilizando Outlook Web Access en Exchange Online (OWA) y Outlook.com falsificando tokens de autenticación para acceder al correo electrónico de los usuarios.

NOTICIAS

Cómo se violó el entorno altamente seguro de Microsoft

Lo que realmente sucedió en la violación de la OPM – Oficina de Administración de Personal

La OPM no priorizó el financiamiento para la seguridad cibernética. Su presupuesto de seguridad de 7 millones de dólares los colocó en el último lugar en comparación con todas las demás agencias.

Carecían de un liderazgo y una estructura de gestión eficaces para implementar políticas de seguridad informática fiables.

La OPM no implementó medidas de seguridad básicas críticas, como la autenticación de dos factores.

Su red tenía una "arquitectura insegura" y ejecutaba "una cantidad significativa de infraestructura obsoleta".

Finalmente, la agencia y su programa de seguridad de TI tuvieron dificultades para cumplir con muchos requisitos de cumplimiento de FISMA.

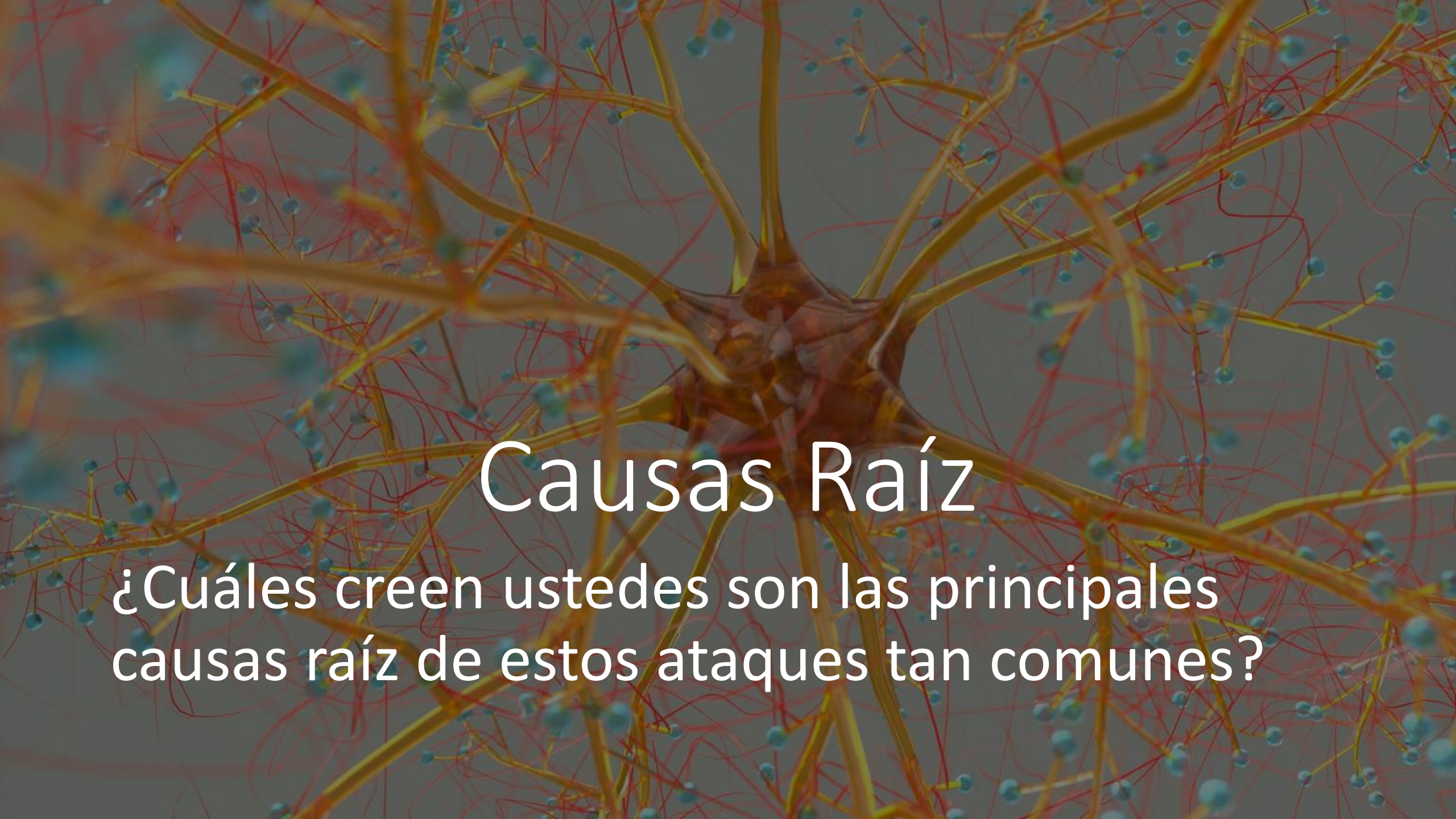
Preguntas frecuentes sobre la violación de datos de Equifax: ¿Qué sucedió, quiénes se vieron afectados, cuál fue el impacto?

La compañía fue hackeada inicialmente a través de un portal web de quejas de los consumidores, y los atacantes utilizaron una vulnerabilidad ampliamente conocida que debería haber sido parcheada, pero, debido a fallas en los procesos internos de Equifax, no lo fue.

Los atacantes pudieron pasar del portal web a otros servidores porque los sistemas no estaban adecuadamente segmentados entre sí, y pudieron encontrar nombres de usuario y contraseñas almacenados en texto sin cifrar que luego les permitieron acceder a otros sistemas.

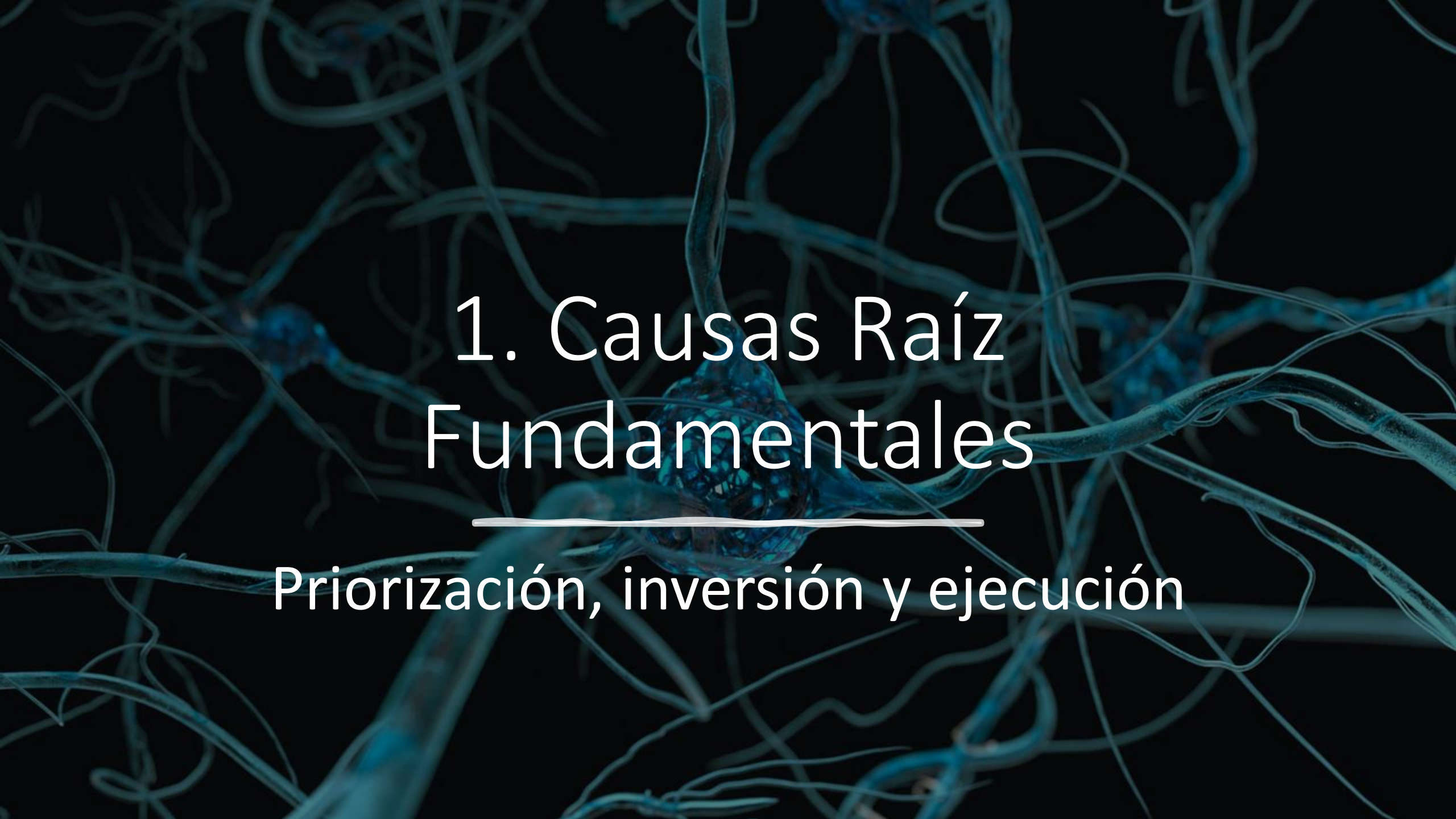
Los atacantes extrajeron datos de la red en forma cifrada sin ser detectados durante meses porque Equifax no había renovado un certificado de cifrado en una de sus herramientas de seguridad internas.

Crédito: rafapress / Shutterstock



Causas Raíz

¿Cuáles creen ustedes son las principales causas raíz de estos ataques tan comunes?



1. Causas Raíz Fundamentales

Priorización, inversión y ejecución

2. Causas Raíz Técnicas

- Falta de MFA
- Programa ineficiente de educación de ciberseguridad
- Mala higiene cibernética: email y DNS
- Malware
- Vulnerabilidades de software y procesos
- Mala configuración de sistemas
- Errores Involuntarios de los empleados
- Falta de cifrado

Estrategia de Ciberseguridad

Cuál es su estrategia de Ciberseguridad?

Zero Trust – Principios Básicos

1. Verificación Explícita
2. Usar el acceso de privilegios mínimos
3. Asumir que los incidentes son inevitables

En Resumen

- Causas Fundamentales de los ciberataques
- Causas Técnicas
- Se necesita una estrategia diferente
- Zero Trust es una estrategia diferente

Referencias

- The MGM Resorts Attack: Initial Analysis (cyberark.com)
- Detalles de cómo se produjo el ataque del ransomware Conti a Costa Rica (welivesecurity.com)
- How Microsoft's highly secure environment was breached (malwarebytes.com)
- Preguntas frecuentes sobre la violación de datos de Equifax: ¿Qué sucedió, quiénes se vieron afectados, cuál fue el impacto? | OSC en línea (csoonline.com)