UNIVERSIDAD POLITECNICA DE SAN LUIS POTOSI

Act01: Análisis en grupo de un ciberataque real y su impacto empresarial.

Carrera: ITI

Asignatura: CNO V Seguridad Informática

Salazar Hernández Pablo de Jesús - 171580

Cavazos Zacarías Rodolfo – 178823

Nieto Diaz de Leon Jair de Jesus – 171676

Gutiérrez Hernández Rodolfo – 179598

Morquecho Medina Eduardo Gabriel

Mtro. Servando López Contreras

25/01/2026

Introducción

La seguridad informática no es algo que normalmente sea comúnmente practicada o hablada entre la gente en sus vidas diarias, se tiene pensado que al tener ciertos tipos de dispositivos o software que de uso diario tengan algún tipo de protección, de cierta manera la gente podría sentirse segura, sin embargo, estos dispositivos o software de uso común como navegadores web o aplicaciones de uso diario no son suficientes para repeler algún tipo de ciberataque que usualmente pasan de maneras inesperadas, provocando daños costosos que requieren tiempo para arreglar varios problemas que estos mismos dejan a su paso.

Pensando en las grandes empresas, hay ciertas áreas las cuales pueden ser atacadas con regularidad debido a ciertos caracteres que se toman, como lo podrían ser correos, llamadas, mensajería instantánea, tomando en cuenta que el ser humano es el eslabón más débil en la seguridad informática, es usual que no se le ponga mucha atención a estas áreas vulnerables donde un ciberataque puede ser faltan en una empresa.

En esta actividad hablaremos de un caso en específico el cual, se mostrará los daños reales que se podrían estimar en un ciberataque exitoso en una empresa real la cual, no tuvo los cuidados suficientes para repeler un ataque de este tipo.

Caso PEMEX (2019) Análisis técnico del caso

Año: 2019

País: México

Entidad afectada: Petróleos Mexicanos (PEMEX)

Condiciones de ciberseguridad previas: PEMEX tenía madurez baja; sin EDR robusto, segmentación network débil (RDP/SMB expuestos), políticas laxas de macros VBA y falta de monitoreo de tráfico C2/observables (e.g., puertos 80/443/FTP). No hay evidencia de backups offline efectivos o respuesta IR madura pre-ataque.

Factores que facilitaron el ataque:
-Error humano: Empleados habilitaron macros VBA en spearphishing y/o cayeron en FakeUpdates (ingeniería social vía emails/documentos “internos”).

-Tecnica: LOLBins no bloqueados, credenciales débiles en LSASS, AV bypass fácil.

-Politica: Ausencia de MFA en RDP/SMB, sin refuerzo en macro disabling, OSINT expuesto (Linkedln/emails públicos) para targeting preciso.

Esto creó una puerta abierta para 60 días de intrusión sigilosa.

PEMEX, la petrolera estatal mexicana, sufrió un ataque de ransomware el 10 de noviembre de 2019 (D-0), detectado tras la ejecución del malware que mostró notas de rescate demandando 565 BTC (unos $4.9 millones USD entonces). Aunque PEMEX afirmó que operaciones y producción no se vieron afectadas, empleados perdieron acceso a sistemas por días, y datos robados (incluyendo info OT) se publicaron en sitios de leaks.

Los atacantes usaron spearphishing como vector principal para el acceso inicial en el caso PEMEX, entregando malware como Emotet o Dridex vía adjuntos maliciosos que requerían habilitar macros VBA en documentos de Office. FakeUpdates era un método alternativo ingenioso vía SEO poisoning, donde un empleado buscaba algo relacionado y caía en un sitio falso de "actualización de browser" que descargaba Dridex.

Tabla técnica del ataque

Elemento	Descripción
Tipo de Ataque	**Ransomware**, cifrado de equipos y exigencia de rescate en criptomonedas
Actor o grupo atacante	Presuntos cibercriminales vinculados a grupos de ransomware como DoppelPaymer
Vector de Entrada	Probable acceso inicial vía **phishing**
Vulnerabilidad Explotada	Sistemas sin parches y credenciales debiles
Etapas de ataque (MITRE ATT&CK)	- Initial Access (T1078, Valid Accounts) - Execution (T1059, Command & Scripting Interpreter) - Persistence (T1547, Boot or Logon Autostart) - Privilege Escalation (T1068) - Impact (T1486, Data Encrypted for Impact)
Sistemas o servicios comprometidos	Menos del 5% de los equipos corporativos, afectando principalmente sistemas administrativos y de logística
Duración del incidente	Ataque detectado el 10 de noviembre de 2019; los atacantes dieron un plazo de 48 horas para pagar el rescate
Mecanismos de detección y respuesta	- Comunicado oficial de Pemex confirmando el ataque - Intervención de equipos internos de TI

	para aislar sistemas - Decisión de no pagar el rescate - Restauración de sistemas afectados mediante respaldos y limpieza manual

Evaluación del impacto

Principio	Descripción del impacto	Evidencia del caso
Confidencialidad	Exfiltración de información interna previa o simultánea al cifrado, como parte de una estrategia de doble extorsión característica de DoppelPaymer.	Amenazas públicas de divulgación de datos y posterior filtración de documentos internos de PEMEX en plataformas asociadas a los atacantes.
Integridad	Alteración no autorizada de la información mediante cifrado malicioso, impidiendo el uso normal de archivos y sistemas, sin evidencia pública de modificación intencional del contenido.	Sistemas administrativos y equipos corporativos cifrados, con pérdida de acceso a datos y aplicaciones críticas.
Disponibilidad	Interrupción parcial de la disponibilidad de servicios administrativos debido a la inoperatividad de equipos y sistemas afectados por el ransomware.	Afectación aproximada del 5 % de los equipos de cómputo y suspensión temporal de procesos como facturación y pagos, sin impacto directo en la producción industrial.

Cálculo del costo total del ciberataque (MXN)

Tipo de costo	Descripción	Estimación USD	Estimación MXN 1USD=19.26 MXN (Banxico)	Argumentación	% del Presupuesto Anual de TI	Comparativa con el Sector Energético/Gobierno
Pérdidas Operativas	Días de inactividad, cancelación de operaciones o servicios.	$12,000,000	$231,120,000 MXN	Días de parálisis en facturación y logística administrativa.	~25%	Equivale a una cuarta parte del presupuesto operativo anual de ciberseguridad de una paraestatal grande.
Daños Reputacionales	Pérdida de clientes, caída en el valor de acciones, pérdida de confianza.	$5,000,000	$96,300,000 MXN	Pérdida de confianza y filtración de datos en la Deep Web.	~10%	Supera el costo de cualquier campaña nacional de confianza digital programada para ese año.
Costos Técnicos	Recuperación de sistemas, consultorías externas, reemplazo de equipos.	$3,500,000	$67,410,000 MXN	Limpieza de 10,000 terminales y restauración de backups.	~7%	Es equivalente al costo de renovar licencias críticas para toda la infraestructura central de Pemex.
Costos Legales / Regulatorios	Multas, demandas o sanciones por incumplimiento (GDPR, ISO, etc.).	$500,000	$9,630,000 MXN	Auditorías externas y cumplimiento normativo post-ataque.	~1%	Impacto menor en presupuesto, pero alto en auditorías externas obligatorias por la ASF.
Pago de Rescate o Extorsión	En caso de ransomware, monto pagado o solicitado.	$4,900,000	$94,374,000 MXN	Monto solicitado por los atacantes (565 BTC).	~10%	El rescate solicitado representaba el 10% del fondo de

						emergencia para contingencias tecnológicas.
Inversión en seguridad	Inversión realizada por la empresa posterior al ataque, con el fin de fortalecer vulnerabilidades.	$15,000,000	$288,900,000	Actualización de licencias, segmentación de redes y capacitación.	~31%	**Inversión reactiva:** Casi un tercio del presupuesto anual se tuvo que redirigir a modernización forzada.
TOTAL ESTIMADO	Suma total en pesos mexicanos (MXN)	$40,900,000	$787,734,000	Impacto económico total incluyendo la modernización.	~84%	El ataque consumió casi la totalidad del presupuesto anual estimado de ciberseguridad del sector.

Pago de la empresa por el rescate No realizado según declaraciones oficiales.

El ataque de DoppelPaymer a Pemex no solo fue un desastre técnico, sino financiero. El impacto total estimado de $787.7 millones de pesos absorbió el equivalente al 84% del presupuesto anual de ciberseguridad del sector, demostrando que la recuperación es exponencialmente más cara que la protección proactiva.

Relación con marcos normativos

La norma ISO/IEC 27001 se centra en identificar riesgos, definir controles, establecer políticas, designar responsabilidades y en general se trata de mejorar continuamente la seguridad de la información de la organización, esa norma toma relevancia porque el proceso de certificarse incluye realizar un análisis de brecha, identificar las brechas de seguridad en el sistema, lo cual es algo que suena un punto básico para la protección de la información, lo cual demuestra el poco compromiso de Pemex en la prevención del ataque.

En la misma norma nos encontramos con el Control A.12.3 “copia de seguridad”, este control nos dice sobre realizar copias de seguridad de información que se puede perder

durante un ataque, asegurando mantener la operatividad aun en caso de secuestro. En este ataque a Pemex se perdió básicamente aproximadamente un 5% de los equipos de áreas administrativas y no se pudo recuperar su información afectando facturación y pagos. Un respaldo habría permitido restaurar los archivos cifrados.

No hay detalles oficiales sobre como se permitió este ataque, una investigación posterior sugiere una entrada inicial a través de malware de acceso temprano que posiblemente haya sido descargado por error por un usuario. Además del control A.12.3, la norma ISO/IEC 20071 contempla el control A.9.2 sobre la gestión de accesos de usuario, el ransomware se propagó debido a credenciales comprometidas, aplicar un control sobre estas limitando sus privilegios habrían reducido la expansión del malware.

En la función Detectar(DE.CM-7) del NIST CSF recomienda monitoreo de actividad anómala de manera constante, Esto habría permitido identificar el cifrado de los archivos a tiempo y detener el ataque antes de que los procesos administrativos fueran afectados

Finalmente, el GDPR en el articulo 32 exige medidas de seguridad como cifrado y pruebas de resiliencia para evitar la libre exposición de los archivos secuestrados reduciendo el riesgo de espionaje industrial y pérdida de confianza.

Conclusiones

El incidente de ransomware sufrido por PEMEX en 2019 evidencia que la ciberseguridad debe abordarse como un proceso integral y continuo, y no únicamente como la implementación de herramientas tecnológicas aisladas. A pesar de tratarse de una empresa de infraestructura crítica, las debilidades en sus controles de seguridad permitieron que un ataque relativamente conocido lograra afectar sistemas internos y exponer información sensible.

El caso demuestra que los mecanismos de protección tradicionales resultan insuficientes frente a amenazas actuales que combinan ingeniería social, malware avanzado y el uso de herramientas legítimas del sistema. La falta de monitoreo activo, segmentación de red y capacidades de detección temprana facilitó la permanencia del atacante durante un periodo prolongado sin ser identificado.

Asimismo, el factor humano jugó un papel determinante en el acceso inicial, confirmando que la ausencia de capacitación y concientización incrementa significativamente el riesgo organizacional. Aunque la producción no fue interrumpida, la pérdida de acceso a sistemas y la filtración de datos reflejan un impacto real sobre la confidencialidad, integridad y disponibilidad de la información.

Lecciones aprendidas

El caso PEMEX resalta la importancia de adoptar una estrategia preventiva basada en la detección temprana y la gestión de riesgos, apoyada por herramientas como EDR, SIEM y monitoreo continuo de red. Estas medidas permiten reducir el tiempo de exposición y limitar el alcance de los ataques.

También se evidencia la necesidad de reforzar los controles de acceso mediante autenticación multifactor, políticas de credenciales robustas y segmentación adecuada de la infraestructura, especialmente en servicios expuestos. De igual forma, la capacitación constante del personal en la identificación de amenazas como phishing resulta esencial para disminuir la probabilidad de compromisos iniciales.

Finalmente, el incidente subraya la relevancia de contar con planes formales de respuesta a incidentes y respaldos seguros, así como de alinear la seguridad institucional con marcos internacionales como ISO/IEC 27001, NIST, X.800 y RFC 4949, los cuales proporcionan una base sólida para la protección de sistemas críticos y la continuidad operativa.

Referencias

Arghire, I. (2019, 12 de noviembre). Mexican oil company Pemex hit by ransomware. SecurityWeek. Recuperado de https://www.securityweek.com/mexican-oil-company-pemex-hit-ransomware

Idaho National Laboratory. (2022). Precursor Analysis Report: DoppelPaymer Ransomware attack on Petróleos Mexicanos (PEMEX) 2019 (INL/RPT-22-70678) [PDF]. U.S. Department of Energy, Office of Cybersecurity, Energy Security and Emergency Response (CESER). Recuperado de https://cyote.inl.gov/content/uploads/24/2025/12/CyOTE-Case-Study_PEMEX-DoppelPaymer.pdf

Riley, D. (2019, 13 de noviembre). Mexican state-owned petroleum firm Pemex crippled by ransomware. SiliconANGLE. Recuperado de https://siliconangle.com/2019/11/13/mexican-state-owned-petroleum-firm-pemex-crippled-ransomware/

Auditoría Superior de la Federación (ASF). (2020). *Informe del Resultado de la Fiscalización Superior de la Cuenta Pública 2019: Auditoría de Tecnologías de Información y Comunicaciones a Petróleos Mexicanos:* asf.gob.mx/Trans/Informes/IR2019c/Documentos/Auditorias/2019_0414_a.pdf

Banco de México (Banxico). (2019). *Estrategia de Ciberseguridad y Estadísticas del Mercado Cambiario*.

banxico.org.mx/SieInternet/consultarDirectorioInternetAction.dosector=6&idCuadro=CF373