“BRECHA DE SEGURIDAD EN LA UNIVERSIDAD DE CALIFORNIA (UCLA)” - 2023.

Explotación de vulnerabilidad de día cero de MOVEit Transfer.

OZONE

CIBER CASOS

Ruben Apablaza Muñoz

-OZonE-

- **Descripción breve**
  - El caso del ataque a UCLA en 2023.
  - Explotación de día cero a aplicación MOVEit. (CVE-2023-34362)

- **Qué falló**
  - Exploit de día cero

- **Impacto**
  - Los antecedentes ***SUGIEREN*** que el impacto del ataque afecto a alrededor de 16 millones de personas, mientras que otras fuentes hablan de 60 millones.
  - Impacto en la reputación sobre el manejo y seguridad de los datos de usuarios.

- **Lecciones aprendidas**
  - Revisar de forma periódica, automatizar la aplicación de actualizaciones y parches de seguridad.
  - La importancia de las pruebas de pentesting previo al lanzamiento de las aplicaciones.

"Brecha de Seguridad en la Universidad de California (UCLA)"

(Explotación de vulnerabilidad de día cero de app MOVEit.)

La Universidad de California, Los Ángeles (UCLA), una de las instituciones académicas más prestigiosas, fue víctima de ciberataques significativos en 2014 y 2021. El ataque comprometió datos sensibles, incluyendo información estudiantil, investigaciones y datos de empleados. A continuación, se presentan detalles clave del incidente:

Detalles del Incidente:

Origen del Ataque: Se sospecha que el ataque provino de un grupo de hackers (grupo CL0P[i] también conocidos como TA505) respaldado por un estado. La investigación sugiere que utilizaron técnicas avanzadas para evadir las defensas de seguridad de la universidad. En estricto rigor, el ataque del grupo CL0P fue a la aplicación MOVEit que tenía gran presencia en la universidad.[ii]

Método de Ataque: Los atacantes utilizaron una vulnerabilidad de DIA CERO (CVE-2023-34362) para infectar aplicaciones que interactúan con un sistema de transferencia de archivos conocidos como "MOVEit"[iii].

Impacto: La universidad experimentó la pérdida de datos confidenciales, interrupción de servicios esenciales y la publicación no autorizada de información sensible en la web oscura. La reputación de la institución se vio gravemente afectada, y se iniciaron investigaciones legales.

Los antecedentes del caso sugieren que la información de **16 millones de usuarios fue robada** en este ataque.[iv]

En enero de 2024, la UCLA's Life Sciences Division IT, sufrió un nuevo incidente de seguridad que afecto al 1.19% de la comunidad del campus de la UCLA.[v]

Para ser mas precisos, el caso no debiese vincularse exclusivamente a UCLA, fueron varias las organizaciones grandes afectadas por este ataque de dia cero a MOVEit Transfer.

1. RESPONSABILIDADES LEGALES Y ÉTICAS

Posibles responsabilidades legales y éticas de la UCLA en la gestión de la información sensible antes del ataque y después de este.

Cabe señalar que las responsabilidades legales incluyen principalmente la notificación del incidente a los afectados. [vi]

Antes

- Había antecedentes previos, en 2021 un ataque a la misma UCLA fue perpetrado con éxito, lo que podría constituirse como actitud negligente por parte de la organización en función de la triada CIA.

Después

- Tras el ataque UCLA tiene la responsabilidad de notificar a las personas afectadas.
    - *"Se ha notificado a quienes se vieron afectados —declaró un portavoz de la UCLA—. Este no es un incidente de ransomware. No hay evidencia de que se haya visto afectado ningún otro sistema del campus."* [vii]

¿Cómo podría la universidad haberse preparado mejor para proteger la información?

- Creo que lo primero es fomentar una cultura de ciberseguridad a partir de entender que se trata de una organización que por su tamaño y diversidad esta constantemente en la mira de los ciberatacantes.

- La cultura de seguridad no solo implica concientizar a los usuarios, existen aplicaciones practicas que incluyen la revisión periódica de la seguridad de la información.

- Exigir al proveedor del sistema de transferencia de archivos, en este caso MOVEit, el cumplimiento de las medidas de seguridad y actualizaciones que hubiesen prevenido la explotación de la vulnerabilidad, de aquí que son tan importantes las pruebas de pentesting cuando se desarrolla software y aplicaciones.

- A nivel técnico se puede hablar de:
  - Redundancia de servidores.
  - Segmentación de redes.
  - Copias de seguridad.
  - Cifrado de datos.

2. ESCENARIOS DE VULNERABILIDADES

Identifique posibles vulnerabilidades en la infraestructura de seguridad de la universidad que permitieron el éxito del ataque.

1. **Concientización de usuarios frente a correos phishing**

   En primera instancia, la falta de formación y concienciación de las medidas de seguridad por parte de los usuarios de la red de UCLA sobre que hacer frente a correos phishing es un ejemplo de vulnerabilidad en la infraestructura de seguridad.

2. **Redundancia de servidores y copias de respaldo de la información.**

   En segunda instancia se aprecia un problema en la redundancia de servidores que podría y debería haber mantenido el sistema funcionando pese al ataque.

3. **Cifrado de la información**

   La publicación de información confidencial da para asumir que parte sensible de los datos se encontraba sin clave de cifrado, una cosa es que te roben la información y otra distinta es que puedan leerla.

3. CONSECUENCIAS DE BRECHAS DE SEGURIDAD

Posibles consecuencias del ciberataque para la UCLA en términos de reputación y cumplimiento legal.

- **Reputación**
  - Pérdida de confianza
  - Afectación a la marca
  - Consecuencias económicas cuando usuarios e inversores perciben un entorno vulnerable

- **Cumplimiento legal**
  - Las instituciones son los responsables legales de los datos que almacenan y manejan, cuando esta información se ve expuesta sin autorización las responsabilidades legales deben ser respondidas.

Enumeración de medidas mitigatorias para abordar las brechas y restaurar la confianza de los estudiantes, empleados y la comunidad en general.

Si bien el ataque no fue responsabilidad exclusiva de una mala administración de la seguridad de la información por parte de UCLA, lo cierto es que a modo de recomendaciones generales siempre es bueno considerar las siguientes:

1. **Control de daños e información.**
   - Transparentar el daño recibido con el objetivo de establecer un plan de medidas mitigatorias y los puntos a reforzar.

2. **Comunicar el fortalecimiento de medidas.**
   - Es vital mostrar a la comunidad que se están redoblando los esfuerzos en materia de seguridad de la información, dando cuenta que no solo se está tomando una actitud reaccionaria sino que también proactiva.

3. **Involucrar a la comunidad.**
   - Bajo el lema, ***"La seguridad la construimos entre todos",*** es vital involucrar a ese eslabón más débil que es el usuario.

4. PRINCIPIOS DE CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD

¿Cómo los principios de confidencialidad, integridad y disponibilidad se vieron comprometidos durante el ciberataque?.

Confidencialidad.

Este principio asegura que solo aquellos autorizados tengan acceso a datos confidenciales. La investigación sugiere que la UCLA experimento la perdida de datos confidenciales por lo que se podría asumir que en el caso de que los datos no estaban cifrados, la información contenida fue vulnerada.

Integridad.

La integridad se enfoca en asegurar que los datos no sean alterados de manera no autorizada. La publicación no autorizada de información sensible en la web oscura me hace presumir que durante el ataque varios o muchos datos fueron alterados permitiendo la apertura de flancos que llevan a comprometer el siguiente principio.

Disponibilidad.

Garantiza que los recursos digitales estén disponibles cuando se necesiten. Debido a que el informe acusa de caída del sistema claramente este principio se ha visto comprometido.

¿Cómo la UCLA podría aplicar estos principios para mejorar su postura de ciberseguridad?

Confidencialidad.

- **Cifrado de datos**
  - Cifrar la información sensible de los usuarios de los servicios informáticos de la UCLA da una señal clara de confianza al saber que la información esta resguardada frente a un nuevo ataque.
- **Firewalls**
  - Establecer y revisar periódicamente que sitios se permite o no acceder a través del firewall.
- **IDS**
  - Cualquier actividad sospechosa el sistema debería de prevenirlo.
- **Capacitación de personas**
  - Capacitar a los usuarios de la red de UCLA en la identificación de posibles amenazas y en cómo manejar adecuadamente la información sensible puede ayudar a prevenir futuras violaciones de seguridad.

Integridad.

- **Firmas digitales**
  - Muy necesarias sobre todo con información sensible, asegurarse que la información no se ha alterado desde su creación.
- **Hashes criptográficos**
  - Su utilización en niveles de acceso restringidos al igual que las firmas digitales aseguran que los datos en el sistema no han sido modificados debido a que las cadenas cambian significativamente si los datos son modificados en lo más mínimo.
- **Registro de cambios**
  - Pueden incluir información como la fecha y hora de modificación, el usuario responsable y los detalles específicos de los cambios realizados. Se pueden identificar alteraciones no autorizadas y tomar medidas correctivas de manera oportuna.

Disponibilidad

- **Redundancia de servidores**
- **Copias de seguridad regulares**
- **Planificación de la continuidad del sistema.**

CONCLUSIÓN

El caso de la UCLA, deja varios aprendizajes, por una parte, entender que a mas grande la organización, mas se encuentra en el radar de los ciberatacantes por lo que la superficie de ataque es mayor y la seguridad debe ir de acuerdo a eso.

Si bien el caso es de un gigante como la UCLA en el contexto norteamericano, en Chile, el marco regulatorio se esta haciendo presente, la creación de la ANCI y leyes que se deben cumplir comienzan a colocar el rayado de cancha a los entornos digitales y hasta las empresas que no se consideran que prestan servicios esenciales, de alguna forma manejan datos de clientes que podrían ser expuestos. En este sentido, es importante entender que la ciberseguridad no es un "tema" que tiene solo que ver con las grandes empresas.

Es importante no perder de vista las amenazas de día cero, invita a considerar cuales son los proveedores de nuestras soluciones de TI. Estudiar un poco su historial de seguridad seria una buena practica para saber que tan confiable y que tanta seguridad nos puede brindar confiar en su solución tecnológica.

Siendo el primero de los casos de ciberseguridad que estoy estudiando, llama mi atención de lo poco que se habla del real **impacto financiero** que tienen los ciberataques, y es que los daños son realmente mayúsculos no solo en multas sino que también en términos reputacionales lo que aleja a los inversores. Un articulo muy interesante lo dejo aquí, del cual seguramente buscare más información en el futuro.[viii]

Si llegaste hasta acá te agradezco en primer lugar y si deseas complementar información de este caso o corregir algún dato, bienvenido sea.

BIBLIOGRAFÍA

[i] **UCLA entre las víctimas de ciberataque mundial**
https://www.telemundo52.com/noticias/local/ucla-victima-ciberataque-mundial/2443520/

[ii] **Los 39 hackeos más notorios de la historia que se incluyen en el Top 10 de OWASP**
https://www.indusface.com/blog/notorious-hacks-history/

[iii] **Sitio web de MOVEit**
https://www.progress.com/es/moveit/moveit-transfer

[iv] **UCLA confirms it was hit by cyberattack but offers few details by Nathan Solis**
https://techxplore.com/news/2023-07-ucla-cyberattack.html

[v] **UCLA Data Breach: What & How It Happened?**
https://www.twingate.com/blog/tips/UCLA-data-breach

[vi] **UCLA y CVS, dos de las últimas víctimas de ciberataques**
https://www.healthcarecompliancepros.com/blog/ucla-and-cvs-two-of-the-latest-victims-of-cyber-attacks#:~:text=UCLA%20Health%20is%20offering%20individuals,one%20of%20our%20professionals%20consultants

[vii] **UCLA confirms it was hit by cyberattack but offers few details by Nathan Solis**
https://techxplore.com/news/2023-07-ucla-cyberattack.html

[viii] **Vulnerabilidades de ciberseguridad y su impacto financiero**
https://cepr.org/voxeu/columns/cybersecurity-vulnerabilities-and-their-financial-impact