Universidad Autónoma de Baja California
Facultad de Ciencias Químicas e Ingeniería

Plan de Ingeniero en Software y Tecnologías Emergentes

Materia
Seguridad del Software(371)

Meta 4.1.3
Administración de vulnerabilidades

Docente
Carlos Francisco Alvarez Salgado

Participante:
Luis Eduardo Galindo Amaya (1274895)

Tijuana, 12. abril 2024

Ensayo

Historias de Terror de TI: Cómo el Software no Parcheado Daña a las Empresas

dentro de cada infraestructura existen múltiples entradas que los criminales pueden aprovechar para robar datos y perjudicar a los usuarios una de las principales amenazas en el área del software es definitivamente el software no parcheado, como desarrolladores mantener el software y darle mantenimiento constante es fundamental y previene futuros problemas de seguridad. Parchear software es de las tareas más importantes dentro del desarrollo de software.

En el artículo se narran algunos casos de hackeos a empresas en le ultimo año, los ejemplos dados son: T-mobile, MSI y Reddit y aunque todos los ataques tienen diferentes objetivos, tienen algo en común, todos fueron propiciados por software vulnerable.

- Vulnerabilidades de seguridad: Al no estar actualizado con los últimos parches, el software puede contener vulnerabilidades conocidas que los hackers pueden aprovechar para acceder a sistemas.

- Problemas de cumplimiento: Las organizaciones pueden violar regulaciones al no mantener su software actualizado, lo que resulta en multas y sanciones.

- Pérdida de datos: Las vulnerabilidades de seguridad pueden llevar a la pérdida de datos sensibles, como información de clientes o registros financieros.

- Daño a la reputación: Las brechas de datos pueden dañar la reputación de una empresa y dificultar la recuperación de la confianza de los clientes.

- Pérdida de productividad: Las interrupciones causadas por la explotación de vulnerabilidades pueden afectar la productividad de los empleados y las operaciones comerciales.

Conclusión

Después de leer el artículo, pude aprender a identificar las características que pueden propiciar un software que no recibe mantenimiento después de que su tiempo de desarrollo haya terminado. El mantenimiento, aunque es una tarea tediosa, es indispensable para el correcto funcionamiento del software una política de mantenimiento de software siempre puede mantener los focos de posibles ataques al minímo.