Riesgos PCI DSS

Como ya se ha comentado en el post anterior, existen empresas que han sufrido vulnerabilidades referentes al pago mediante tarjeta online. Según M.V. Kuzin[1] un estudio realizado por el equipo de riesgos de Verizon en conjunto con el Servicio Secreto de los Estados Unidos de América observaron que:

- Se habían comprometido 3,88 millones de elementos de datos
- El 96% de esos datos datos comprometidos se refiere a los datos de las tarjetas de pago
- En cuanto a los ataques descubrieron que el 43% no requirieron herramientas especiales para piratear, otro 49% se asoció con el uso de ciertos métodos y herramientas, y solo en el 8% de los casos se usaron conocimientos especiales y recursos de computación significativos
- El 89% de las organizaciones que procesaron y almacenaron datos de tarjetas de pago en el momento de la piratería no cumplían con los requisitos del estándar de la industria de datos de tarjetas PCI DSS (Norma de seguridad de datos de la industria de tarjetas de pago), y el 11% sí.

Además, el estudio reveló ciertos datos que pueden resultar curiosos como poco. En primer lugar, el haber pasado la auditoría de PCI DSS no quiere decir que se sigan cumpliendo las normativas del mismo, solo informa que en el momento sí que las cumplían.

Por otro lado mostró que las empresas ya no cumplían con los requisitos de PCI DSS, aunque sí que lo habían hecho en el momento de pasar la auditoría.

Finalmente, extrajo las siguientes dos conclusiones principales:

1. La norma o estándar no es suficiente para proteger los datos del titular de la tarjeta, y cumplir con sus requisitos no proporciona actualmente una seguridad adecuada;
2. La norma o estándar desplaza la carga de responsabilidad por fraude en lugar de evitar que los datos se vean comprometidos.

Una vez vistos datos reales creados por instituciones con credibilidad, te paras a pensar ¿cuáles son entonces los riesgos a los que te enfrentas al pagar con tarjeta?

Si bien la mayoría de los riesgos de la implementación de PCI DSS son generados en al implementación de código que las empresas realizan, según se puede leer en el artículo de Danial Clapper y William Richmond[2], existen varios otros riesgos relacionados con PCI DSS, muchos de ellos generados por el no cumplimiento del mismo. Uno de los riesgos que mencionan en el artículo es el riesgo al robo de la información del usuario que realiza una transacción. Para reducir este riesgo, proponen adherirse al *Payment Card Industry Data Security Standard* (PCI DSS). En general, las empresas pequeñas

no entienden la seguridad de la tecnología de la información y, por tanto, algunas de ellas suelen tener brechas de seguridad.

Además, no solo puede haber robos de datos, también podría darse el caso de acabar con pérdida de datos de los clientes, lo que no solo acabaría con una mala reputación de la empresa si no que acarrearía en compromisos legales por no haber contemplado esos casos con anterioridad.

Para poder tener una mayor control de los riesgos que puedan ser generados con PCI DSS, desde la página oficial de PCI [3] dentro de los requisitos que proponen, más concretamente en el punto 6.1, obliga a las organizaciones a establecer un proceso para identificar vulnerabilidades de seguridad, utilizando fuentes acreditadas e información actualizada sobre vulnerabilidades, es decir, organizaciones deben llevar a cabo una exploración de vulnerabilidades, al menos en los servidores que están en el ámbito de la regulación PCI. Para ello, habrá que hacer una gestión de riesgos siguiendo los siguientes puntos:

- Establecer un contexto. El equipo de riesgos tiene que comprender los parámetros internos y externos para poder hacer una evaluación de los riesgos.
- Identificación de activos. Los activos pueden ser algo de valor para la organización. En cuanto a PCI DSS, los activos incluyen las personas, procesos y tecnologías que participan el el procesamiento, almacenamiento transmisión y protección de los datos.
- Identificación de las amenazas. Las amenazas pueden incluir personas, los sistemas que utilizan y las condiciones en las que éstos se encuentran. La organización deberá ayudar al evaluador de riesgos a mostrarle dónde se encuentran potencialmente las amenazas.
- Identificación de las vulnerabilidades. Una vulnerabilidad es una debilidad que puede ser explotada por una amenaza y puede venir tanto de la tecnología, la organización, el medio ambiente o una empresa. En la evaluación de riesgos todas las vulnerabilidades deben de ser consideradas (p.ej. vulnerabilidades que pueden ocurrir como resultado del desarrollo, diseño y/o implementación software)

Este post lo voy a finalizar mostrando una imagen. En ésta se recoge un resumen más exhaustivo de las amenazas, vulnerabilidades, riesgos e impactos.

Threats	Vulnerabilities	Potential Outcome/Risk	Potential Impact to Business
External hackers, malicious individuals, cyber criminals	▪ Lack of network security—e.g., properly configured firewalls, lack of intrusion detection ▪ Weak password policy ▪ Transmission of unprotected CHD ▪ Lack of security awareness to social engineering, phishing ▪ Insufficient system hardening, malware protection	▪ Network intrusion ▪ Compromise of user credentials ▪ System compromise ▪ Introduction of malicious code ▪ System downtime ▪ Compromise of sensitive data	▪ Theft of CHD and/or SAD ▪ Reputational impact ▪ Loss of business due to decreased customer confidence ▪ Interruption to business processes ▪ Financial loss—cost of recovery, forensic investigation, lost revenue, possible fines/penalties
Internal malicious individuals, internal user mistakes, human error	▪ Lack of effective change control ▪ Lack of user knowledge/training ▪ Inappropriate assignment of access permissions (e.g., not based on need to know or least privilege) ▪ Lack of separation of duties ▪ Insufficient system hardening ▪ Weak encryption/poor key-management practices	▪ Introduction of malicious code through web browsing/email ▪ Untested system changes ▪ Privilege escalation of user accounts ▪ Unauthorized access to sensitive data	
Thief/intruder intending to cause physical damage or steal assets	▪ Lack of physical security/monitoring ▪ Insecure handling of payment terminals ▪ Lack of tamper-detection ▪ Disposal of storage media without deleting data ▪ Failure to properly supervise visitors/vendors	▪ Theft/replacement of payment terminals ▪ Undetected skimmers added to POS systems ▪ Unintended access to CHD ▪ Installation of rogue devices leading to network compromise	

Referencias:

[1] M. V. Kuzin. (2011). PCI DSS: Security Standard and Security in

Fact. *Bezopasnostʹ Informacionnyh Tehnologij, 18*(4), 120-125

[2] Clapper, Danial, and William Richmond. «Small Business Compliance with PCI DSS.» *Journal of Management Information and Decision Sciences* 19, no. 1 (2016): 54-67. [pdf carpeta ACCSI_Volumes]

[3] PCI Security Standard Council, Information Supplement: PCI DSS Risk Asessment Guidelines, noviembre 2012, acceso el 11 de noviembre de 2018, https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf