According to a group that focuses on loss of control over credit-card data, “In the last five years, approximately 500 million records containing personal identifying information of United States residents stored in government and corporate databases was either lost or stolen.”<http://www.insideidtheft.info/breaches09.aspx> The Web site InsideIDTheft.info, which is run by identity-protection expert Rob Douglas<http://www.insideidtheft.info/robdouglas.aspx>, has a wealth of historical information about data leakage and data theft as well as pages of helpful analysis and advice.

The prevalence of data theft has led to increased enforcement of compliance with standards to protect data – surely a Good Thing, right? Well, maybe not in the way compliance is sometimes being enforced. Long-time colleague Bob Gezelter contributes his thoughts today on the unreasoning application of security standards. Everything that follows is Bob’s work with minor edits.

* * *


Heartland is a large-scale third-party transaction processor. Processors of that size should comply with various security standards, including the Payment Card Industry’s Data Security Standard (PCI DSS).<https://www.pcisecuritystandards.org/saq/index.shtml> At the time of this writing (end of January) it is too early to find details, but the incident prompts me to ask whether compliance with standards is achieving the goal of protecting data.

Recently, my modest information security consulting firm was required to undergo compliance scanning under provisions of the same PCI DSS. The process had some requirements that were logical and appropriate but also some requirements that were illogical in our context. However, compliance with all of the requirements was mandatory, regardless of how irrelevant.

We deal mostly with corporations, which rarely use credit cards. Our few credit-card transactions are processed using a financial-grade, SSL/TLS-enciphered connection to a major payment processor from a conventional Web browser (e.g., Firefox, Internet Explorer) – just like any normal Web commerce. No electronic copy of credit card-related data is stored on any of our computer systems.

However, since the SSL/TLS-enciphered connection traverses our Internet connection, full compliance is obligatory. The requirements fit several categories:

- reasonable
- not reasonable for our configuration
not compliance related – idiosyncratic behavior of the programmed script verifying compliance: if the script does not see the precise response expected, non-compliance is reported, even if there is no actual non-compliance.

Several check-off items on the compliance review relate to problems which are deemed “Denial of Service” or “May lead to privilege escalation.” Indeed, this presumption may be so for many Windows and *IX (e.g., UNIX, Linux, AIX) systems running popular software packages such as sendmail. However, our WWW server does not run one of those systems, nor is our server in the path of PCI data processing. Our server runs Hewlett Packard’s OpenVMS <http://www.hp.com/go/openvms>. Our WWW site is served using the public domain WASD <http://wasd.vsm.com.au/> Web server. Indeed, one of the showstopper problems was nothing more than a testing script that presumed Windows/*IX file naming conventions.

Yet, despite several requirements that all transmissions involving PCI data to be encrypted, there is no requirement that the encryption be based upon a X.509 certificate issued by a generally recognized Certification Authority.< http://www.ietf.org/rfc/rfc4158.txt >

Once data are properly encrypted, they are opaque. If financial-grade SSL/TLS is not sufficiently opaque to block eavesdropping and prevent tampering, then there are serious problems with far more systems than just those involved in PCI processing.

A more likely scenario is that of a bouillabaisse: all the requirements related to security get tossed into the stew. For the requirements that make sense, this does no harm. For those which are not appropriate for a merchant’s configuration, there is a problem. For those hosting their own Web stores with payment processing, these requirements are reasonable. For those who do not fit the obvious model, the checklist can be like ill-fitting clothing: at best uncomfortable, at worst unwearable.

In some ways, this situation is reminiscent of what transpired when college programming instructors tried to standardize grading practices using metrics (see for example the discussion of metrics in Aivosto’s Project Analyzer™ software < http://www.aivosto.com/project/help/pm-loc.html >). Students were required to comment at least a stated percentage of the lines in their programs. Students quickly learned that even silly, nonsensical comments were accepted toward that benchmark metric. The result was predictable: students put in useless, uninformative comments to comply with the rule, and the instructors were obliged to accept that they had complied with the requirement to comment the stated percentage of their code.

The inappropriate PCI DSS requirements serve the interests of none of the parties involved: neither the consumer, the merchant, the processor, nor the compliance authority.

A more extensive discussion of this problem is online in “Securitization: A Risk to Compliance Integrity.”< http://www.rlgsc.com/blog/securitization-a-risk-to-compliance.html >

***


***

M. E. Kabay, PhD, CISSP-ISSMP <mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >
Copyright © 2009 Robert Gezelter & M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.