



# PCI newsletter

- January 2009

## 1. New version of the PCI Data Security Standard

The third version of the PCI Data Security Standard (PCI DSS) – version 1.2 – was released in October 2008. This standard must be complied with as of 1 January 2009.

A number of amendments have been made in version 1.2 of which you should be aware. The most important amendments are outlined below, but it is crucial that you read the new version in detail in order to identify any aspects of the standard which are relevant to your particular enterprise.

### **Broader definitions with regard to requirements**

The changes to the standard reflect the fact that in the majority of cases the requirements contained in the standard have been worded in broader terms. This applies in particular to the wording of actual technical specifications, which have been expressed in more general terms in order to ensure that PCI DSS can keep pace with ongoing technological developments such that the PCI Council need not issue a new revision every time a technological change takes place.

For example, PCI DSS no longer includes a specific list of the 10 most important vulnerabilities in web applications based on OWASP's prioritised list. Instead, the standard now simply refers to OWASP's list of the most important web vulnerabilities, and the PCI Council therefore has no need to update the standard every time a change or a reprioritisation of the vulnerabilities is carried out by OWASP.

The amendments mean that it is important that you remain up-to-date with respect to new technologies and security threats such that you can choose to take the necessary steps at the right time.

A number of examples of the amendments in PCI DSS version 1.2 are specified below.

### **Firewall review**

According to the new version, 1.2, there is no longer a requirement that a firewall review need be carried out every quarter. This has been amended to every six months.

### **Wireless**

Business enterprises that use wireless technology based on the old WEP protocol shall ensure that they replace their equipment by 30 June 2010. If you install new wireless units after 31 March 2009, you should be aware that these installations must not be based on the WEP protocol, but must comply with the newer WPA protocol instead.

This amendment is due to the fact that encryption in the WEP protocol is not implemented to a sufficiently secure degree. The WEP protocol has long been regarded as insecure, but the PCI Council has permitted its use on account of the large number of old WEP-based wireless terminals in circulation.

The amendment is particularly relevant to retail outlets with handheld terminals where some of the equipment is based on WEP.

### **Antivirus software**

In version 1.2 of PCI DSS the requirement with respect to antivirus software has been expressed in more general terms. This means, for example, that the previously specified exemption for UNIX systems no longer applies. The PCI Council is thereby future-proofing the standard so that it does not need to issue a revision in the event that hackers begin developing viruses aimed at UNIX systems.

Antivirus software shall now also be able to pick up malicious code. We therefore recommend that you examine whether the version of the antivirus software that you are using is able to discover such code. Generally speaking, you cannot expect all antivirus software to include functions that will pick up malicious code.

### **Patching**

Based on the new version of PCI DSS, you can now utilise an approach to patching that is based on the actual risks concerned. You now have to assess vulnerabilities and patches in relation to your own situation rather than having to update all high-risk vulnerabilities within 1 month – including those vulnerabilities that are not critical for your particular setup.

### **Backup solutions**

It has been stipulated that business enterprises that have backup solutions hosted offsite must visit their supplier at least once a year in future in order to ensure that the backup solution is secure.

### **Intrusion Detection System (IDS)**

In the previous version of PCI DSS, the IDS was responsible for monitoring all traffic. In the new version, the PCI DSS requirement has been defined in more detail such that the system only has to monitor the traffic within the IT environments that process card data.

The above examples are just some of the amendments that are described in the new PCI DSS version 1.2. FortConsult therefore recommends that you read the new version of the standard in full in order to discover what it means for your enterprise.

## **2. PA-DSS – new sibling to PCI DSS**

In May 2008 the PCI Council launched the new Payment Application Data Security Standard (PA-DSS), which is aimed at enterprises that develop or install payment systems. In Denmark, this includes developers and integrators of cash till solutions and terminal vendors of credit card terminals. These enterprises have already received a letter from PBS stating that they must comply with the security requirements in PA-DSS.

In Sweden, the business enterprises that have to comply with PA-DSS have been informed by Pannordic of the exact security requirements in a corresponding manner. We expect that other countries will follow suit due to the fact that VISA in the USA has clearly stated that all software must be PA-DSS validated.

#### **Easier to specify requirements**

PA-DSS has been developed in order to make it easier for those enterprises that purchase payment solutions – primarily shops – to communicate with their vendors and specify requirements with respect to security in their applications such that the shops are able to qualify for PCI certification. The new PA-DSS now provides software vendors with a tangible tool that they can use to see how to go about making their applications secure – and thereby meet the requirements from the shops.

#### **Get a good overall perspective as soon as possible**

If you develop software with credit card functionality, we advise you to get an overview of the standard and to identify which changes are required by your enterprise as soon as possible. This enables you to incorporate an action plan for PA-DSS validation into your development plans and to avoid wasting unnecessary development time on producing software that does not meet the requirements of PA-DSS and is thus not future-proof.

#### **Only Danish enterprise**

FortConsult is the only Danish enterprise certified by the credit card companies to check and audit security on their behalf in the debit card solutions that are subject to PA-DSS. Just 18 enterprises are certified to conduct PA-DSS audits on a global scale.

You can read a lot more about PA-DSS and what you can do to comply with the standard here: [http://www.fortconsult.net/pci/softwareudviklere\\_pa.php](http://www.fortconsult.net/pci/softwareudviklere_pa.php)

### **3. Internal PCI penetration tests**

The new PCI requirements with respect to internal penetration tests were issued in spring 2008 and came into immediate effect. The aim of internal PCI penetration tests is to test in practice whether all the provisions of PCI DSS are implemented correctly and whether it is possible for unauthorised parties to steal credit card data.

Internal penetration tests are carried out in the same way as when a hacker attacks a business enterprise in order to steal card data after he has physically penetrated the enterprise, or in the same way as it could be imagined that a normal employee without access to card data might attempt to break through the enterprise's defence mechanisms in order to steal credit card information.

#### **The test must be certified**

All enterprises that come within the scope of PCI DSS shall have an internal penetration test carried out in connection with a PCI audit. As part of the audit that FortConsult conducts, we check whether the test has been carried out and whether it meets the requirements specified by the PCI Council.

#### **Neutrality is a requirement**

Since PCI DSS specifies that it is not permissible to test your own work, the internal PCI penetration test must be carried out by an independent party. As an enterprise you can therefore either choose to carry out the tests yourself – with the proviso that this is done by a person who has not been involved in configuring the enterprise's security solutions – or get a security firm to carry out the tests. As a point of departure, there is nothing wrong with doing it yourself, but in such cases you should be aware that the PCI Council specifies exacting

requirements with regard to the test itself and to the level of competence of the person responsible for carrying out the test.

In order to have your own security test certified you need to be able to document what you have tested, as well as why and how in a manner which is sufficiently detailed for the documentation to be read by an outside party. When FortConsult conducts the audit, we must in other words be able to obtain a precise understanding of the test and be satisfied that it has been carried out in a sufficiently comprehensive manner such that we can vouch for it with respect to the PCI Council.

### **Targeted test**

It is essential that the test is put together based on the detailed documentation that is already available in order to ensure that the test covers the elements that are most critical for your enterprise. The existing documentation includes a risk assessment of your enterprise, the results of internal scans and an overview of the PCI scope.

When, for example, we carry out an internal PCI penetration test at FortConsult, we customise the content of the test with respect to the enterprise concerned by first of all acquainting ourselves with the existing documentation and looking at how a hacker might be able to attack the enterprise. This means that in practice the test ends up focusing on the enterprise's greatest risks for actually being hacked and having credit card data stolen, rather than covering the entire PCI standard in general terms and including areas which are irrelevant or difficult to exploit.

The enterprise that is tested thus benefits from a carefully targeted and practical test in which we examine what is actually possible, thus ensuring security in practice rather than "just" following the PCI standard.

### **New requirements concerning the external PCI penetration test**

New requirements have also come into effect for the external penetration test which have ensured a greater degree of clarity with regard to what to do. In practical terms, there are no changes for those enterprises that already have the penetration test carried out by FortConsult.

The revisions to the requirements with respect to both internal and external penetration tests are described in greater detail in the PCI Council's clarification letter:

[https://www.pcisecuritystandards.org/pdfs/infosupp\\_11\\_3\\_penetration\\_testing.pdf](https://www.pcisecuritystandards.org/pdfs/infosupp_11_3_penetration_testing.pdf)

If you have further questions concerning the new requirements regarding internal and external penetration tests, you are welcome to contact us.

## **4. New self-assessment questionnaire (SAQ)**

At the beginning of 2008 a new and improved version of the self-assessment questionnaire (SAQ) was issued. The questionnaire is relevant for enterprises that have to comply with PCI DSS, but which are not subject to an audit.

From the beginning of 2009, the change will have significance for many of our customers, who will have to use the new version of the questionnaire from the turn of the year.

### **More specific wording**

The original version of the SAQ – version 1.0 – was somewhat general, and many enterprises could answer yes to the majority of questions in the questionnaire with a clear conscience without having to read PCI DSS first. In the latest version – version 1.2 – however, the questions are worded in more specific terms, which will result in it being more immediately

apparent if there are aspects that are not complied with or areas which need to be looked at in more detail prior to answering the questions.

In practice, there have hitherto been many enterprises that have mistakenly stated that they comply with PCI DSS. When they begin using the new questionnaire, the areas where compliance is lacking will soon become apparent.

### **Security responsibility**

Even if your enterprise does not need to be checked, and you only need to complete the SAQ, you should be aware that you carry significant liability. In the event that you are hacked and you do not actually comply with the PCI standard in full, you will risk having to cover the amounts that have been lost due to fraud on the card numbers that have been stolen. Based on experience from previous fraud cases, claims for damages can be expected to amount to 1,000 Euro per card number, in addition to which you will have to pay a fine.

We are always happy to help you complete the SAQ if you wish to make sure that it is carried out correctly.

## **5. Clarification of typical misunderstandings**

When FortConsult's PCI security consultants conduct audits and tests for our customers, they typically come across two common misunderstandings, which we would like to help clarify in the following:

### **Misunderstanding 1:**

"If we do not store card data, then we don't have to comply with the PCI standard."

### **Clarification 1:**

Even if you do not store card data, PCI DSS must be complied with in full, although the practical aspects of complying with the standard will in many cases be more straightforward.

It goes without saying that it is easier for a hacker to hack into card databases containing large amounts of data gathered in one place. However, a hacker can also steal data by acquiring credit card data every time a card is processed; it just takes place over a longer period of time. In such cases, the hacker may install a program that copies every card number to a server on the Internet. The program is installed so close to the source that the card number can be acquired unencrypted.

Hackers have otherwise begun to use the latter method to a much greater extent, since many enterprises no longer store large amounts of card data for security reasons.

### **Be aware of the scope**

It is important that you are aware of the enterprise's scope – i.e. which systems PCI DSS applies to – both in terms of systems that store and/or process and/or transmit credit card data, and in terms of all other systems that are found on the same network segment. The designation "systems" covers everything from servers and workstations to firewalls, routers and other network units – and not least credit card terminals.

For many shops this means that all of their computers throughout the retail chain come within the scope of PCI DSS – not just a single cash till solution.

### **Misunderstanding 2:**

"Wireless network is not allowed on our premises, so we don't need to carry out a wireless test."

**Clarification 2:**

Even though you do not use wireless solutions, a wireless test still has to be carried out.

Requirement 11.1 of PCI DSS applies in all cases and stipulates that a wireless test must be carried out once every quarter. It also applies even if you do not have wireless equipment and even if the equipment is not connected to systems that store credit card data.

**Survey of wireless access points**

The purpose of the wireless test is to see whether there are any wireless access points that have been overlooked, for example as a result of an incorrectly configured laptop PC or a printer. In addition, the test is designed to reveal whether hackers or employees have set up wireless access points of which the enterprise has no knowledge.

In the latest version of PCI DSS – version 1.2 – an amendment has been made to 11.1, which concerns which test methods are acceptable. It is now also permissible to use wireless IDS rather than testing. However, since IDS is difficult to configure and typically requires many wireless access points in order to cover the enterprise's PCI scope in full, this will quickly become an expensive solution. In practice, it thus remains most sensible to carry out a wireless test in which all locations are manually checked with wireless test equipment.

If you have any questions or comments, you are more than welcome to contact us. We follow the development of PCI DSS and PA-DSS on an ongoing basis and will issue our next newsletter when there is new and relevant information available.

**FORTCONSULT***Straight talk on IT security*

FortConsult ApS    Tel +45 7020 7525  
Tranevej 16 - 18    Fax +45 7020 7526  
DK-2400 Copenhagen NV    [www.fortconsult.net](http://www.fortconsult.net)