



StayInTouch

– security news from FortConsult

Content in the newsletter for August 2010

1. Different approaches to security testing
2. FortConsult makes an international breakthrough
3. PCI news
4. FortConsult supports the Danish Council for Greater IT Security
5. New employees at FortConsult
6. New reference customers at FortConsult

You can subscribe to our electronic newsletter at
www.fortconsult.net

FORTCONSULT

Straight talk on IT security

1. Different approaches to security testing

- and what we can learn from each other

By Ulf Munkedal, Managing Director at FortConsult

For many businesses it has become a healthy and natural discipline to let their IT systems undergo security testing at regular intervals, as well as every time a new system is developed or major changes take place. The same applies to some extent to those companies that develop products or IT solutions intended for resale. How commonplace it has become to undergo security testing depends in many cases on the type of enterprise in question and the short-term benefits to be gained from testing.

Different categories of businesses with different test needs

In the following, I will review the various categories of businesses that have security tests carried out and compare these categories in order to discover which conclusions can be reached with regard to both differences and common factors, thus enabling knowledge to be gained of the different worlds in which these businesses operate.

Product manufacturers

In overall terms, manufacturers of products typically choose to have their products security tested before they are launched on the market, since this reduces costs by remedying security issues in the product. A golden rule of thumb says that the earlier in the process a security flaw is discovered, the cheaper it will be to remedy. Manufacturers are also aware that they minimise the risk of dissatisfied customers and bad publicity caused by the discovery of serious breaches of security in their products after release. However, it is the cost issue that is normally the overriding concern for product manufacturers.

IT solution providers

Providers of IT solutions typically choose to security test their IT solutions in order to ensure satisfied customers and avoid a loss of image and perhaps legal proceedings. In this case, once again the earlier this occurs in the development process the better, and must very definitely take place before the solution goes into production. The fear of dissatisfied customers and loss of image are the most important reasons why IT solution providers undergo security testing.

Other businesses (end customers)

Other businesses typically choose to have their IT systems security tested in order to find security issues to mitigate the risk of other parties exploiting any weaknesses, which can lead to loss of image, issues of confidentiality, corruption of data and/or inaccessibility. All the above situations can result in incalculable consequences to the business of the enterprise in question.

The majority of such businesses choose to have regular security tests conducted on the basis of a sort of subscription agreement in which all IT systems are tested at regular intervals and the test results compared in order to measure the general level of security in the systems. In addition, there is a growing tendency for businesses to choose to test their systems every time they reconfigure or patch their systems, or when new, serious vulnerabilities appear.

Conclusion

In FortConsult's experience, it is often the end customers that are most aware of the benefits of having security tests carried out. Although awareness amongst IT solution providers is increasing, this is only true of product manufacturers in a handful of cases. In actual fact, it ought to be the other way round, as this would enable vulnerabilities to be discovered before a situation occurs in which end customers risk losing data.

Different test methods

Whether testing a product or a solution, there are a number of common denominators for what denotes a good security test. However, in practice the three categories of businesses mentioned above that need

security testing actually undergo tests with completely different areas of focus and thus potential benefit with regard to the output of the test.

Here is a short description of the three types of test methods:

Product manufacturers' test method

Product manufacturers generally use a product tester to find flaws in components, which hopefully includes security flaws. This is often carried out by the manufacturers' own test department, external product testers or external penetration testers. They have to test to find manufacturer errors – i.e. development errors in each component – or compatibility errors – i.e. errors when the components are put together.

The strength of product testers is that they are traditionally used to working in accordance with a strong test methodology and structure. They are therefore usually very capable in terms of methodology and structure, and are often able to present documentation to back up the fact that they have carried out a comprehensive test assignment.

The weakness of product testers is that their focus is not directed at security tests and it is therefore not possible to be sure that they have the ability to discover all serious security weaknesses, or indeed that they are sufficiently comprehensive, despite the fact that they perform tests in accordance with a highly structured methodology.

IT solution providers' test method

Providers of IT solutions use solution testers to find flaws in the overall solution. It is also possible that they test for security flaws if it is part of the "acceptance test" which is agreed with the end customer. The security tests are performed by either a technician employed by the IT solution provider, technicians belonging to the end customer or external penetration testers. They have to test to find manufacturer errors, compatibility errors, design errors, IT solution provider errors and configuration errors. Manufacturer errors are development errors in each component, compatibility errors are errors that occur when the components are put together, design errors are errors in the way in which the design is put together, IT solution provider errors are errors in the solution provider's code, whilst configuration errors are errors in the setup/configuration.

The strength of solution testers is that they have a technical overview of the end customer's solution. They understand the solution and what it has to be able to do. Their weakness is that they do not have the required degree of competence or focus with respect to security testing and thereby cannot be relied upon to discover all serious security weaknesses, in addition to which there is a question mark as to whether they are sufficiently comprehensive.

Other businesses' test method

Other businesses – i.e. the end customers – use penetration testers to find vulnerabilities in their IT systems. They have focus on security and nothing else. The security tests are conducted by the businesses' internal security departments, test departments or external penetration testers.

Tests have to be carried out to find manufacturer errors, compatibility errors, design errors, IT solution provider errors, configuration errors and maintenance errors – i.e. errors in the enterprise's maintenance of the system.

The penetration testers have great security insight. They are highly specialised and cannot be used for much else other than different types of security tests and other tasks that require so-called vulnerability expertise – i.e. knowledge concerning different vulnerabilities, how they occur, how they can be exploited by hackers and worms and how an enterprise can protect itself against them.

What can the three business categories learn from each other?

Each of the three types of business has strengths which are important elements in any good security test, which must include:

- Performance of the test as early as possible in the development process

- Strong test methodology/structure
- Technical overview of the product or solution
- High level of security insight

It would be best if all the above points were fulfilled in every security test. In the following, I will look at the first two points, which I believe need a more detailed explanation in order to understand why they are so important.

Performance of the test as early as possible in the development process

For both product manufacturers and IT solution providers it is crucial to incorporate security as early as possible in the development process – not just at the end of the process either just before or just after the product has been released. In our experience, the elements that are most important when incorporating security into a development model are so-called secure coding checklists, which, for example, ensure that input validation of all input takes place, as well as so-called source code inspections – i.e. security tests which help to ensure that security is checked on an ongoing manner in the development process.

As stated earlier, it is a good idea to give the developers checklists which specify a number of principles according to which they have to work. These checklists do not have to be extensive – just a single page may be sufficient. The checklist must set out a framework from start to finish. Security code inspections should be included in the checklist, where the developers check each other in order to provide quality assurance. This ensures a good level of awareness.

Product manufacturers and IT solution providers are becoming increasingly aware of the benefits of testing as early as possible. For the end customers it is not an ingrained phenomenon, and only a handful of businesses that develop their own solutions or purchase IT solutions from solution providers ensure or demand that work takes place in accordance with secure coding checklists and that source code inspections are carried out. Of course it is possible for these businesses to have the source code examined for security flaws once they have purchased the IT solution and put it into production, but they should also consider specifying precise requirements to their IT solution provider, as this will save them a great deal of expense and inconvenience.

Strong test methodology/structure

In addition to carrying out security reviews and security tests as early as possible in the process, a disciplined structure is necessary when conducting tests. Quite simply, security tests require a detailed and structured test plan in order to make sure that the test is systematic and that nothing is forgotten. This is absolutely essential, as a security test carries the risk of giving a false sense of security if it does not cover every element, as there is then a risk that any weak links in the chain may not be checked. The test plan also enables a structured approach in which creativity and manual tests can be freely deployed within a structured framework, thus making sure that the tester does not have to worry about whether all the bases have been covered, but can concentrate on giving creativity free reign.

A good test plan must contain test scenarios, test cases and pass/fail criteria. We are familiar with test scenarios or “use-cases” in ordinary test plans. In a security test, this approach is turned on its head and is based on “misuse-cases” or “attack scenarios”. In order to be able to write good “misuse-cases”, it is, among other things, important to have a test background and a good understanding of common attack methodologies and vulnerabilities. Furthermore, testers must also have a good security background, which ensures an understanding and respect for a structured test.

A typical penetration tester is not necessarily particularly structured. It is therefore a good idea to introduce or demand a clear structure and test plan when using an external tester. Many tests on the market today are actually so-called “rent-a-hacker” tests, in which the security test depends only on the penetration tester’s own competence, and where the test is based on very limited – or indeed a complete absence of – test plans.

A solid test methodology is illustrated in figure 1, in which it can be seen that verification takes place on an ongoing basis throughout the various phases of development to ensure that what is being done is OK. It is a classical model that requires updating, but it illustrates the concepts of testing early in the process and following a structured approach.

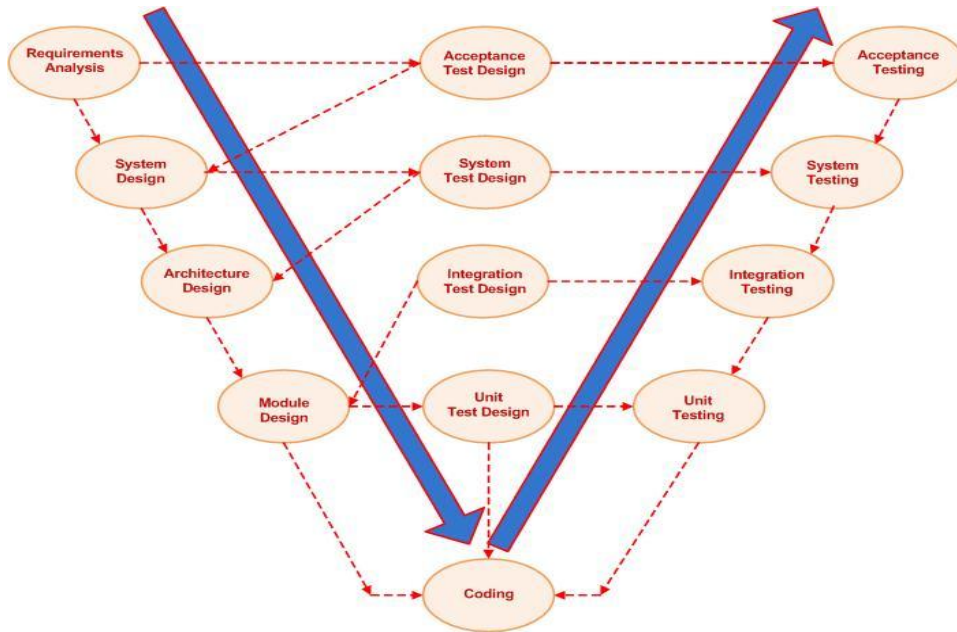


Figure 1: The classical V development model

It is also a really good idea to use a test management system to keep tabs on the information concerning the test. If you test with automatic tools, it is sometimes sufficient to use the management system integrated in the tools, but alternatives include systems such as Quality Center, which is a good test management tool, although not designed for security as such.

Which security level should you choose?

Last but not least, security also means being sure right from the start which level of security you wish to operate at, thus enabling you to relate to the test results and what they mean for your particular business.

The regular security tests are designed to verify the level of security that the business has decided is to be built into the product or the solution right from the start. Before embarking on the test, the following must therefore be decided:

- When is it secure enough?
- Which model will be used to agree on how great a level of security is required?

See, for example, FortConsult's model of threat levels in figure 2, where the desired security level is defined seen in relation to the threat scenario, i.e. the risks are weighed up and evaluated in relation to your level of ambition in terms of security.

Model used to determine the required level of security

- Level 1: Random/elementary attacks?
 - o Can withstand: Worms and amateur hackers
 - o Typical test methodology: Running of tools
- Level 2: Targeted attacks?
 - o Can withstand: Skilled and persistent hackers and politically-motivated hackers
 - o Typical test methodology: Manual tests performed according to test-cases supplemented by creative tests
- Level 3: Targeted attacks with insider knowledge?
 - o Can withstand: Former employees, customers, organised crime, business partners, industrial espionage and intelligence services
 - o Typical test methodology: Tailor-made "misuse-cases" and test plans supplemented by creative tests

Figure 2: FortConsult's model of threat levels

Level 1 concerns amateur hackers who “Google” the net and find tools. They are not particularly persistent or thorough in their approach, and hence it is not particularly difficult to protect yourself against them. This can be done by running a number of standard tools. If you wish to safeguard yourself at level 2, you also have to take targeted attacks into account. In this case, the hackers are more skilful and more persistent – they do not give up straight away. This may take place over a longer period and may also require manual test methodologies. Level 3 involves an extra dimension of insider knowledge in which the hacker may, for example, know the code. This requires the creation of tailor-made misuse-cases for the business concerned.

A level 1 test can be commenced relatively quickly and simply by anyone. At levels 2 and 3, organisational insight, a structured approach and a deep understanding of security are required. In these cases, it may be a good idea to ally yourself with capable penetration testers with considerable experience of vulnerabilities and a structured approach to testing. Only in this way is it possible to ensure comprehensive protection and to find all the serious security weaknesses that may enable your business to be hacked and data to be stolen, deleted or amended. I cannot emphasise strongly enough how important it is to have a structured approach to security testing, regardless of whether you are a product manufacturer, an IT solution provider or an end customer. Moreover, there is no doubt that penetration testers, who are typically capable, but unstructured, can improve their test results by learning from the product manufacturers’ advanced test methodologies.

2. FortConsult makes an international breakthrough

Danish tests of IT security are selling like hotcakes abroad. FortConsult’s international sales grew by 70 percent between 2008 and 2009, and the firm now has a foothold in Sweden, Norway, Iceland and Portugal. The first FortConsult office in Europe is expected to become a reality within the foreseeable future.

From a humble office on Nørrebro in Copenhagen, Denmark’s biggest firm in the field of security testing and credit card security sells its services to some of Europe’s most security-conscious business enterprises, including a number of leading financial enterprises. Portugal, Norway, Sweden and Iceland are currently the most successful markets outside Denmark, and FortConsult is aiming to realise sales to 17 different countries from its premises on Nørrebro.

- We are proud and happy to have received such a positive reception abroad. We see it as solid proof that our penetration tests and services to the financial sector are highly regarded internationally, says Managing Director Ulf Munkedal from FortConsult, which within a short space of time has achieved a position as one of the three biggest firms within the areas of penetration testing and credit card security in Europe.

FortConsult’s international sales grew by 70 percent between 2008 and 2009, and in the first five months of this year FortConsult has already sold as much abroad as it did throughout the whole of 2009.

FortConsult is already a market leader in Denmark with a clientele consisting of some of the country’s biggest businesses and the financial sector. Internationalisation is therefore a logical means of growth for FortConsult.

Although we have modest Danish roots, our goal is to become the preferred supplier of security tests throughout the whole of Europe, says Ulf Munkedal. We have drawn up a plan to test 17 markets over a period of 12 months, and so far we have far outstripped expectations. Ulf Munkedal predicts that FortConsult will open offices or enter into partnerships in several European countries during the course of the next 24 months.

Growth on the top and bottom line

FortConsult has generally not experienced any problems related to the economic recession, and the firm is able to present its best results ever. The security firm came out of 2009 with a turnover of DKK 26.9 million,

which represents a growth of 30 percent in relation to 2008. Pre-tax profits were DKK 4.0 million in spite of heavy investment in internationalisation, a result which Ulf Munkedal describes as “satisfactory”.

In April, FortConsult concluded a worldwide agreement with IKEA, which was looking for a security partner to audit credit card security on a global scale. In Germany Siemens chose FortConsult as its external provider of security tests on web applications at Siemens companies in a number of countries in Europe. This took place following a thorough review and approval of FortConsult’s test methods by Siemens’ own CERT organisation in Germany. In addition, Nordea and British American Tobacco are important international customers.

Hackers in the service of the greater good

FortConsult employs a number of consultants who act as hackers in the service of the greater good. Customers are typically major enterprises who hire the Danish firm to attempt to hack into their IT installations from outside. FortConsult’s consultants combine the hacker’s equibristic methods with a structured and proven approach, such that customers can be sure of an exhaustive and objective product when they employ security tests from FortConsult. FortConsult’s 30 employees include security test experts from Denmark, Sweden, the Netherlands, Belgium, South Africa and Greece.

FortConsult – in DKK mill.	2009	2008
Gross profits	22.5	17.1
Profit on main activities	3.8	1.8
Profit before tax	4.0	1.4
Profit for the year	2.9	1.0
No. of employees, start of year	27	24

3. PCI news

By Lars Syberg, PCI product manager at FortConsult

1. American PCI legislation heralds new era in Europe

Today, no specific legislation exists in the PCI area in Denmark. We only have the PCI standard, which is not a law, but a voluntary agreement between two parties subject to the rules of general contract law. This has hitherto also been the case in the USA, but here there are new legislative regulations on credit card security on the way, and this development will almost certainly spread to the EU and Denmark in the future. Among other things, new rules of law on data leakage are sure to be adopted in Europe.

The American rules

The new American rules of law mean that it has been decided to include rules on the protection of credit cards in legislation in Nevada, Minnesota and most recently Washington, and it is likely that more states will follow in due course.

The latest legislation in Washington came into force on 1 July 2010 and means that American businesses are now forced to comply with certain rules in terms of credit cards. The aim of the law is that an issuing bank will be able to receive compensation for costs incurred in issuing new cards if a shop with more than 6 million transactions or card processes loses card data because the data was not adequately protected. In the state of Nevada, a different approach has been taken, whereby new legislation requires that the business community must comply with the PCI standard.

What will it mean for the EU?

In the EU there is of course a great deal of interest as to whether, as in the USA, PCI-like requirements will be incorporated at national or European level. Credit card companies would rather not see legislation being introduced, but would prefer to be able to define and administrate the rules themselves. Currently, there is nothing to suggest that legislation on the protection of credit cards will be introduced in the foreseeable future. On the other hand, in Europe there has generally speaking been a tradition for incorporating consumer protection into legislation, and therefore in the not too distant future we can expect to see several new laws dealing with payment security in the EU.

In conjunction with the SEPA directive, which will primarily be implemented in the Euro member states, a requirement will be specified this year, for example, that payments must take place by means of a smart card. Unfortunately, the EU rules say nothing about the sanctions that will be imposed should the requirement concerning smart card payment not be complied with.

Rules on data leakage on the way in the EU

When it comes to consumer protection in connection with data leakage, rules of law already exist in the area in the USA. These rules mean that if you lose data, you are obliged to go public and account for this data loss.

Similar rules are also on the way to being incorporated into EU legislation, and the United Kingdom, for example, has already implemented sanctions in connection with data loss in its national legislation.

Since 6 April this year, the Information Commissioner's Office (ICO) has had the authority to issue fines and orders with respect to data loss. Fines today can be as high as £500,000, whereas prior to 6 April the maximum figure was £6,000. The rules were introduced following a scandal in which Customs & Excise lost information on 25 million British nationals because this information was stored on a CD which got lost in the post.

Marks & Spencer was also ordered to encrypt all its laptop computers after losing information about 26,000 employees because a computer was stolen from an employee.

Unlike the American rules, however, the British rules do not require that companies go public about all incidences of data loss.

At EU level, the so-called Digital Agenda is also on the way. It has seven main initiatives which mean that rules will soon be introduced specifying that Internet service providers will have to publicise incidences in which they lose personal data. The rules will probably subsequently be applied more widely, such that they will also end up applying to other types of business enterprise.

Rules will bolster credit card security in the EU and in Denmark

In terms of credit card security in the EU and Denmark, FortConsult believes that the new EU rules of law represent a definite improvement.

First of all, they will be of benefit to both businesses and consumers, because there will be greater transparency as we begin to get more information about the extent of data loss in Europe if businesses are forced to go public. It will also make it much clearer to businesses why it is so important to have credit card security under control.

At the same time, the rules will create a much more tangible incentive amongst businesses to protect the data as effectively as possible, since their reputations will suffer if an incidence of data loss forces them to go public, in addition to which they may end up facing economic sanctions.

2. Smart card on the way to amending the PCI standard

The smart card, or chip card, is on the cusp of replacing cards with magnetic stripes in the USA, and at the same time it is the PCI Council's intention that the PCI standard should be adapted to the smart card. This is good news for Denmark and the rest of Europe, where a wish to amend the PCI standard has long been on the agenda, because the smart card is much more widespread in Europe than cards with magnetic stripes.

PCI standard is based on cards with magnetic stripes

The PCI standard, which we use in Europe, and thus in Denmark, stems from the USA. The standard is therefore also based on protecting credit cards with magnetic stripes, since this is the type of card that is by far the most common in the USA.

The PCI standard is without doubt justified by the large volume of card numbers that are copied and misused all over the world. For several decades it has been possible to copy a magnetic stripe from a card and then transfer this content to another card. However, it is only within the last 5-10 years that criminals have focused to a major extent on fraud by means of technology and the Internet, since all payment systems are now either directly or indirectly connected to the Internet. Since 2004 the PCI Council has therefore focused on developing the PCI standard so that card numbers are protected during storage and when payment takes place.

The smart card is a step closer to secure technology

In Denmark and the rest of Europe, however, we have more or less replaced credit cards with magnetic stripes with the much more secure smart card (EMV). Since we use the same PCI standard as the USA, however, we still have to comply with the same 240 security provisions as American businesses, because the rules do not take into account the fact that European cards are a lot more secure.

This means that today's PCI standard does not actually reflect conditions in Europe, because it does not take into account the greater security inherent in a smart card.

While the PCI standard is actually designed to enhance security in what is basically an insecure technology – i.e. credit cards with magnetic stripes – in Europe we have chosen to focus on having technology which is fundamentally secure, in the form of the smart card.

As a consequence, many of the controls that are in the PCI standard today are of less importance in Europe seen from a security point of view. They are therefore reduced to a sort of compliance check.

As a result, there has long been a wish on many fronts for the USA to introduce EMV cards in order to boost security, at the same time as which the PCI standard can then be brought up to date and reflect the level of security in Europe.

The advantages of EMV

The advantage of EMV in overall terms is that it contains an integrated circuit which is involved in the actual transaction. The card contains a digital ID, which the card uses to prove its authenticity as part of the transaction. In newer cards, security is further enhanced through the use of Dynamic Data Authentication (DDA), which adds a "random challenge/response" to the authorisation process.

During the transaction process the terminal sends transaction information and a random number to the smart card. The chip uses an internal private key to generate a unique digital signature for the specific transaction. The chip's transaction signature is checked using a public key by the terminal and the network as part of the authorisation process. Only a genuine chip can provide a valid signature on the basis of the data it receives, and therefore the DDA process confirms that the card is both genuine and physically present. The chip in the card calculates the response internally, thus ensuring that the important information does not leave the chip, which means that information cannot be copied as in the case of a card with a magnetic stripe.

EMV has represented a robust safeguard against attack for many years, and the technology is still regarded as being relatively secure today. In a European perspective, however, the fact that our cards are still equipped with a magnetic stripe so that they can be used outside the EU represents a problem. The magnetic stripe can be copied and used to make copies of cards which can be used fraudulently abroad. This means, among other things, that the PCI rules impose a great expense on many businesses because of the risk of theft from insecure magnetic stripe systems (and through e-commerce).

FortConsult has conducted many audits throughout the past six years. The majority have taken place in Europe, but we have also conducted audits in the USA, China, Russia, Canada and several other countries outside Europe. Our experience clearly confirms that EMV significantly restricts the chance of stealing data.

We thus regard it as very positive that there are signs that there is a wish to use EMV in the USA and that it is the PCI Council's intention that the forthcoming version of the PCI standard will try to adapt the rules to the smart card – although we do not yet know how. This will be of benefit to both Danish and other

businesses that have implemented EMV, because the smart card deals with the root of the problem: that magnetic stripe technology is a fundamentally insecure system.

WalMart chooses the smart card

In the USA the supermarket chain WalMart has recently introduced payment by smart card and PIN in order to improve security. All WalMart's hardware is already primed to use EMV technology and the company is currently working on completing the software.

Ellen Richey, Chief Enterprise Risk Officer at Visa, USA, has commented on the problem in the USA. In this regard, she has remarked that it is not a question of whether the USA will begin to use chips or not, but rather a question of when and how. At the same time, Richey has said that Visa believes that chip technology increases security and makes it both easier and faster to effect transactions for customers and businesses, and that Visa is therefore in full support of this technology.

However, there is still a long way to go before the smart card becomes the dominant type of credit card in the USA, but as it becomes more common, it is hoped that the PCI standard will be adapted to the new and more secure reality in the USA and thereby also in Europe.

The smart card does not solve the problem of security with respect to online payment, however, where the card number, expiry date and card verification value or code are still used. Hence in this regard the same challenges will remain in terms of creating security with respect to the information on the card, although in this case work on new and more secure solutions is ongoing – but this lies somewhat further out in the future.

3. New standard for PCI scanning alters the process

Your ASV (Approved Scanning Vendor) will in future begin to put other questions to you and do a number of other things that you are not used to when carrying out PCI scanning. This is due to the fact that the PCI Council has amended the rules in the section of the PCI standard concerning scanning. New requirements will be specified with respect to the services of ASVs.

ASVs to become more involved in the process

The new rules do not make a huge difference to this type of scanning. It is still a scan which in overall terms is designed to reveal vulnerabilities with some focus on web applications, but the process concerning the scan has been fundamentally altered.

Although it has always been the intention in PCI scanning rules that the ASV is to help the customer with the scan, the rules hitherto have actually made it possible for an enterprise to take complete charge of the entire process involving an ASV scanning. This has meant that an ASV has in reality been able to make a web interface available for its customers, who have then been able to enter information and IP addresses themselves and carry out scanning on their own.

The problem with this method is that a number of PCI scans have been carried out erroneously because the ASV has not checked that the information that the customer enters in the web interface is the correct and necessary information. The previous solution has thus led to the risk of operating errors because in many cases ASVs have told their customers that a scan can be effected by means of just a few clicks in a web interface and nothing else. There is thus in principle no guarantee that the business is in fact secure, even though it may have passed the PCI scanning on paper, which can easily reduce the check to a sort of pseudo scanning. This means that there can be a great difference in the level of security that PCI scanning should provide – and which the PCI Council has intended – and the level of security which businesses actually achieve.

This type of self-service is a method that is typically seen practised by ASVs which primarily compete on price and is a method we at FortConsult have always been critical of, and which we have therefore never practised as an ASV.

We have always argued that the ASV should be an active part of the process. We are therefore also very satisfied to see that the new rules mean that the ASV is involved in the scanning process to a greater extent

than stipulated by the previous rules. This will help to verify that the actual security level follows the PCI standard, which is of course in the best interests of the customers.

Consequences of the new rules

As a purchaser of PCI scanning, one of the effects of the new procedures will be that your ASV will in future check that the information you enter is correct, that scanning takes place correctly and that the scanning report is accurate.

The new rules also specifically point out that the ASV must always double-check scanning results that are thought to contain false positives.

The enterprise must examine the supposed false positives itself and explain why they only represent an error in the scanning mechanism and not a real vulnerability. This also applies if a false positive is discovered in two consecutive quarters without the configuration having been altered. This will of course make the process more demanding than before, and many will find it a source of irritation. However, based on a principle of prudence, we believe that the tightening up of the rules makes good sense because something that looks like a false positive occasionally actually proves to be a vulnerability.

More focus on web applications

The new rules also mean that the web application test has received higher priority, a development that we particularly applaud. This area was almost completely overlooked in the previous rules, despite the fact that the majority of break-ins today take place via vulnerabilities in web applications. There is still a long way to go before a dedicated web application test is specified, but businesses should also carry out this type of test themselves in connection with chapter six of the PCI standard. In practice, however, there are many small businesses that do not carry out the checks in accordance with chapter six and therefore make do with PCI scanning (and this will of course make them noncompliant, since they do not carry out all the checks).

In addition, the rules also include help for situations in which IDS/IPS is used, when elements of the solutions are outsourced, as well as in many other situations that a customer might find itself in its day-to-day operations and which have not previously been clearly described.

New rules boost security levels

The new rules have been underway for a long time and have been subject to a lot of work by many different stakeholders. It has also been necessary to work on these rules, since they basically build on the MasterCard standard, which is almost 10 years old, and which was originally not coupled to the PCI standard (which is based on the Visa CISP standard).

In our opinion, previous PCI scanning has not provided appreciable security for those enterprises for which a scan was carried out. However, as mentioned earlier, it has resulted in an approval of security on paper, and in the case of many businesses PCI scanning has been the only process carried out by an external supplier in order to validate compliance with the PCI standard.

Therefore the new procedures are, in the opinion of FortConsult, a step in the right direction towards better security, because the previous rules were unable to ensure that the intention of the PCI Council's rules was backed up to a sufficient extent. We therefore also hope that the wording of the new rules will be clear enough to weed out a number of ASVs operating in the industry. Some ASVs have hitherto exploited the shortcomings of the former set of rules to offer discount scanning, which has unfortunately contributed to the dilution of the quality of PCI scanning. These ASVs have therefore undermined both the standard and, at the end of the day, also the security of their customers.

The new rules will therefore probably mean that low-price scanning will become more expensive – unless low-price ASVs are able to find a loophole in the PCI Council's rules and intentions. At FortConsult we do not expect to make any amendments to the price of ASV scanning, since we have always been involved in the scanning process in order to ensure that scanning for our customers is carried out on the basis of the correct procedures.

At present, ASVs can choose whether or not to follow the new or the former rules, but from 1 September all ASVs must comply with the new rules.

4. Simple PCI solutions are often the best and the cheapest

When we speak at PCI conferences around the world, we are often contacted afterwards by hardware and software vendors that want us to look at their PCI security solutions in more detail and recommend them to the customers for whom we are a QSA (Qualified Security Assessor). This is due to the fact that many of the hardware and software vendors have become aware of the opportunities available in the PCI area, and in many cases QSAs also operate a profitable business selling solutions alongside their core business of conducting audits. Mixing the role of QSA and vendor is not, however, without problems, because there is a tendency for customers to end up buying PCI solutions that are excessive and overly complex in relation to their actual needs.

In our opinion, it is most important for a QSA to retain its independence so that the customers always know that they can trust the advice given to them by the QSA about what they have to alter in their security system in order to comply with the PCI standard. If, like a car mechanic, you both point out the problem and sell the solution to the same problem, you risk losing credibility, and we therefore usually politely decline the opportunity to work with these vendors.

Many businesses overspend on PCI solutions

As a customer of a QSA the problem is often that you are not always aware of which solution is required to ensure compliance with the PCI standard. We therefore see a tendency for many businesses to buy over the odds in excessively advanced solutions in the PCI area. This is due to the fact that customers do not always know how to fulfil the concrete requirements of the PCI standard, but also that many customers have been overwhelmed by the many functions that typically make up comprehensive full-line solutions.

The problem with many of the advanced functions is that they are based on standard security products which are typically not designed to meet the requirements of the PCI standard, but instead are produced to cover many different types of security needs. Of course, many of the products can be adapted so that they cover a particular area of the PCI standard, such as the monitoring of log files or ID management. However, we often see that a business is often surprised that the advanced solution they have invested in does not in fact comply with all the PCI rules, but has to be supplemented by one or more other solutions. This often makes it difficult for businesses to assess and administrate their PCI solutions, and they can then easily end up in a situation in which their PCI solution is never properly implemented. In many cases we see very expensive and advanced solutions that are not properly implemented in the organisation and therefore do not function as they should.

Actually, however, it need not be so difficult.

Homemade solutions go a long way

Many of our customers have developed their own solutions which are simple and which function very well. They are certified by us as the QSA, and they are also typically very well integrated into the company's other processes and existing software.

In other words, the trick is to find a solution that fulfils the needs you actually have in terms of PCI, and then make sure that the solution is fully implemented into your day-to-day operations. This often results in both the most secure and cost-effective solution and a process that makes it possible to comply with the PCI standard in the most straightforward manner.

In the next newsletter you can read more about the new PCI standard, which is due to come into force on 1 January 2011.

4. FortConsult supports the Danish Council for Greater IT Security

FortConsult has chosen to support the Danish Council for Greater IT Security in their efforts to enhance IT security in Denmark and internationally. The council's primary aim is to ensure that the use of IT can take place in a secure manner. The council assesses IT security initiatives and strives to provide independent advice to political institutions and citizens, businesses and the public sector.

FortConsult has chosen to support the council and thereby hopes to be able to contribute to the enhancement of IT security in Denmark.

You can read more about the Danish Council for Greater IT Security at www.rfsits.dk

5. New employees at FortConsult

During the second quarter of 2010 FortConsult A/S has recruited three new employees. Security Consultant Anders Olsen, Business Development Manager Peter T. Hansen and Delivery Assistant Kristina Landsperg have all joined FortConsult to further boost the firm's continued growth.

Anders Olsen is a new Security Consultant at FortConsult. He has worked with IT security for more than 6 years and for the last 4 years has held a position as IT security manager at the Danish hosting firm EasySpeedy ApS. Prior to this, he was a self-employed operations and security consultant. Anders' primary area of responsibility at FortConsult will be carrying out penetration tests of our customers' IT systems.

Peter T. Hansen has a background in the IT industry and comes from a position as Country Sales Manager in Denmark for the German EPLAN group, where he was responsible for sales, marketing and customer support. Before this, Peter had a sales management job at Danmon Danmark A/S and Semco Danmark A/S. Peter will be looking after a fixed customer group at FortConsult, whilst also helping to further develop the sales organisation so that it provides the basis for FortConsult's future growth, both nationally and internationally.

Kristina Landsperg is employed at FortConsult as a Delivery Assistant and makes up part of our delivery planning team. You will therefore meet Kristina in the event that a delivery needs to be planned.

We are very happy that the three new employees have joined us and we hope that you will enjoy a good working relationship with them.

6. New reference customers at FortConsult

We would like to bid welcome to our new Danish reference customers: Chempilots, Cimber Air, Dansk Supermarked Gruppen, Region of Southern Denmark and SKAT.

We also bid welcome to our new international reference customers: Bank Petrocommerce (RU), Boss Media (SE), BS/2 (LT), DnB NOR (NO), EDB Business Partner (NO), EDB Card Services (SE), EMIS (AO), ErgoGroup (NO), HZMEDIA LIMITED (RU), IKEA (SE), INPAS (RU), Nurbank (RU), Russian Agricultural Bank (RU), Signicat (NO), Teris (IS), UniCredit Group (RU) and Valitor (IS).

EDB Card Services, Region of Southern Denmark, Dansk Supermarked Gruppen and Signicat have provided testimonials concerning our business relationship:

A professional and positive experience

"FortConsult's PCI auditor has been both positive and constructive, has operated at a high technical level and been ably qualified to advise us on technical issues. He was both detail-oriented and efficient, and

provided a very professional and thoroughly prepared PCI audit which both VISA and we ourselves were satisfied with. Throughout the entire process we have had the feeling that we were in good hands and we are pleased to have agreed a long 3-year contract with FortConsult. "

Tommy Johansson, EDB Card Services

Competent and flexible

"FortConsult has delivered a very good technical security report on the basis of our security test. The presentation of the report was aimed at both technicians and management and has provided good insight into our IT security. Top marks to the security consultant - he was very committed and was able to give a professional presentation of the test results and recommendations. We are very impressed. Furthermore, we have greatly appreciated the flexibility exhibited by FortConsult in terms of planning the test."

Carsten Frølich, Region of Southern Denmark

Good mix of technical competencies, business know-how and PCI knowledge

"I am very satisfied with the gap analysis which FortConsult carried out for us. FortConsult provides a good mix of technical competencies, business know-how and PCI knowledge when conducting such a project. Throughout the entire process we have felt comfortable and have been engaged in excellent dialogue with all the involved parties at FortConsult. This has enabled us to retain our focus on relevant matters concerning compliance. I can warmly recommend working with FortConsult to others."

Allan Fabricius, Dansk Supermarked Gruppen

9.5 for a good process and a high level of professionalism

"Throughout our entire collaboration with FortConsult we have had the feeling that we were in safe hands - we have received good feedback and good information about subsequent steps. FortConsult has had full control of the process and exhibited great flexibility in adapting the time of delivery to meet our needs. We are also fully satisfied with the security report, which is well framed and with a very high level of technical content. We are extremely positive and therefore happy to award FortConsult a score of 9.5 on a scale of 1-10, where 10 is highest."

Harald Stendal, Signicat

FORTCONSULT

Straight talk on IT security

FortConsult Tel +45 7020 7525
Tranevej 16 - 18 Fax +45 7020 7526
DK-2400 Copenhagen NV www.fortconsult.net