solarwinds msp

PCI and PAN Scan

Assessment completed on: 2017-01-30T01:37:43Z

IP: 192.168.2.16 Hostname: bernini.communica.local OS: Windows Server 2008 R2

Unprotected Data Summary

FAIL

Unprotected Data Count by Type

Visa13	3

Elapsed Time	0 hours, 6 minutes, 16 seconds
Files Scanned	57,645
Files with Violation	3
Total Violations	3

Scan Results Summary

FAIL

PCI DSS Requirements

In Place	Not In Place	Not Evaluated
7	8	0

PASS

Vulnerability and Patch Policies

Policy	High	Medium	Low
Windows Server 2008 R2 Patch Policy	0	0	0
Windows Server 2008 R2 Vulnerability Policy	0	0	0

PCI DSS Requirements Details

Requirement 1: **Install and maintain a firewall configuration to protect cardholder data**

Firewalls are devices that control computer traffic allowed between an entity's networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity's internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity's trusted network.A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.Other system components may provide firewall functionality, provided they meet the minimum requirements for firewalls as provided in Requirement 1. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment of Requirement 1.

1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.

1.4.b Inspect a sample of mobile and/or employee-owned devices to verify that: Personal firewall software is installed and configured per the organization's specific configuration settings; Personal firewall software is actively running; Personal firewall software is not alterable by users of mobile and/or employee-owned devices.

5022:	Verify that host has any personal firewall software installed and active	**Compliant**

Firewalls and routers are key components of the architecture that controls entry to and exit from the network. These are software or hardware devices that block unwanted access and manage authorized access into and out of the network.If a computer does not have a personal firewall or anti-virus program installed, malware may be downloaded and/or installed unknowingly and may introduce weaknesses to your network perimeter and provide opportunities that malicious individuals can exploit. The computer is even more vulnerable when directly connected to the Internet and not behind the corporate firewall. Malware loaded on a computer which is not behind the corporate firewall, can maliciously target information within the network when the computer is reconnected to the corporate network.Please ensure a personal firewall is installed on each device connected to your business' corporate network.If you need assistance, your local IT administrator will be able to provide you with guidance on implementing personal firewalls on your devices. Once implemented, repeat this scan and if the personal firewall is correctly implemented on the device being scanned, this clause will be marked compliant for this device.

Requirement 3: **Protect stored cardholder data**

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.
Please refer to the PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms for definitions of —strong cryptography and other PCI DSS terms.

3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:
One-way hashes based on strong cryptography, (hash must be of the entire PAN)
Truncation (hashing cannot be used to replace the truncated segment of PAN)
Index tokens and pads (pads must be securely stored)
Strong cryptography with associated key-management processes and procedures.

3.4.b Examine several tables or files from a sample of data repositories to verify the PAN is rendered unreadable (that is, not stored in plain-text).

214276:	PAN Detection Windows	**Not Compliant**

The PAN is the Primary Account Number and is the long number on the front of the payment card (normally 16 numbers for VISA/MasterCard).You must ensure that the PAN is rendered unreadable when stored. This includes and is not limited to storage in flat files such as spread sheets, electronic scans/faxes, databases, hard drives, stored call recordings and computer logs such as audit or system logs.To help you locate where PAN may be present on your network, please launch the PAN scanning tool from your merchant dashboard within the compliance portal. You should scan any device connected within your network. If the scan finds any payment card data you must either secure the data using secure encryption tools or securely erase it in accordance with PCI DSS. Once you complete this step, re-run the scan and if you have securely stored or erased the data, it will not be found by the scan.

Requirement 6: Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor- provided security patches, which must be installed by the entities that manage the systems. All critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software.
Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.

6.1 Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release.
Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.

6.1.a For a sample of system components and related software, compare the list of security patches installed on each system to the most recent vendor security patch list, to verify that current vendor patches are installed.

Patches:	Patch & Vulnerabilty Scan	**Compliant**

Many attacks use widely published exploits. Without implementing the most recent patches on critical systems as soon as possible, a malicious individual can use these exploits to attack vulnerable systems and disable the network.You must perform regular reviews and install the latest vendor security patches for all software and devices connected to your cardholder data environment, thereby ensuring you are protected against new exploits.Your security policy must include the requirement to install all critical new security patches within one month. Critical security patches are those that, for example, address vulnerabilities risk rated as 'high' (critical) in accordance with your process per Requirement 6.1(c) or which affect your more exposed Internet-facing systems or a database storing cardholder data.If you need assistance, your local IT administrator will be able to provide you with guidance on implementing this. Once implemented repeat this scan and if the latest security patches are installed on the device being scanned, this clause will be marked compliant for this device.

Requirement 8: Assign a unique ID to each person with computer access

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.
Note: These requirements are applicable for all accounts, including point-of-sale accounts, with administrative capabilities and all accounts used to view or access cardholder data or to access systems with cardholder data. However, Requirements 8.1, 8.2 and 8.5.8 through 8.5.15 are not intended to apply to user accounts within a point-of-sale payment application that only have access to one card number at a time in order to facilitate a single transaction (such as cashier accounts).

8.1.4 Remove/disable inactive user accounts at least every 90 days.

8.1.4 Verify that inactive accounts over 90 days old are either removed or disabled.

5066:	Verify inactive accounts	**Compliant**

Inactive accounts may occur due to removal of software, ex-employees or contractors/suppliers who no longer provide services to you. These forgotten about accounts which may include those with extensive privileges or access rights, could be used by malicious persons to gain unauthorised access to your systems.You must have a process in place to identify and review inactive accounts that have not been used in 90 days and either remove or disable them, thereby preventing account compromise which could lead to malicious use. You can set up rules on your system components to complete these checks.If you need assistance, your local IT administrator will be able to provide you with guidance on implementing this policy. Once implemented repeat this scan and if the policy is implemented correctly on the device being scanned, this clause will be marked compliant for this device.

8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.

8.1.6.a For a sample of system components, obtain and inspect system configuration settings to verify that authentication parameters are set to require that a user's account be locked out after not more than six invalid logon attempts.

5018:	Account lockout check	**Not Compliant**

Locking accounts after multiple failed logon attempts ensures that an attacker cannot continually attempt to guess or "brute force attack" a password until they achieve success.You must ensure that failed logon attempts are limited to six failed attempts after which the account is locked for at least 30 minutes. This should be enforced using a policy or setting on the system components that cannot be bypassed by the user.If you need assistance, your local IT administrator will be able to provide you with guidance on implementing this policy. Once implemented repeat this scan and if the policy is implemented correctly on the device being scanned, this clause will be marked compliant for this device.

8.1.7 Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.

8.1.7 For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account.

5019:	Account Lockout Duration Check	**Not Compliant**

Locking accounts after multiple failed logon attempts ensures that an attacker cannot continually attempt to guess or 'brute force attack' a password until they achieve success.You must ensure that failed logon attempts are limited to six failed attempts after which the account is locked for at least 30 minutes. This should be enforced using a policy or setting on the system components that cannot be bypassed by the user.If you need assistance, your local IT administrator will be able to provide you with guidance on implementing this policy. Once implemented repeat this scan and if the policy is implemented correctly on the device being scanned, this clause will be marked compliant for this device.

8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.

8.1.8 For a sample of system components, obtain and inspect system configuration settings to verify that system/session idle time out features have been set to 15 minutes or less.

5002:	Check screen saver grace period	**Not Compliant**
5003:	Check time limit for active but idle Terminal Services sessions	**Not Compliant**
5000:	Check Password On Battery Wake	**Compliant**
5001:	Check Password On Power Wake	**Compliant**

When users walk away from an open, unlocked machine with access to critical systems, that machine and any other sessions the user has open (e.g. to your payment application or POS system) may be used by others in the user's absence, resulting in unauthorised access and/or system misuse. An idle session may indicate that the user's machine is unattended, you must ensure that if a user's session/computer has been idle for more than 15 minutes their session/computer is locked and they are required to re-enter their logon details. This should be enforced using a policy or setting on the system components that is not able to be bypassed by the user.If you need assistance, your local IT administrator will be able to provide you with guidance on implementing this policy. Once implemented repeat this scan and if the policy is implemented on the device being scanned, this clause will be marked compliant for this device.

8.2.3 Require a minimum password length of at least seven characters.

8.2.3a For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require passwords to be at least seven characters long.

5007:	Minimum Password Length Check	**Not Compliant**
5008:	Password Complexity	**Not Compliant**

Strong passwords are the first line of defence into a network since a malicious individual will often first try to find accounts with weak or non-existent passwords.You must ensure that user passwords are a minimum of at least 7 characters long. This should be enforced using a policy or setting on the system components that is not able to be bypassed by the user.Your local IT administrator will be able to provide you with guidance on implementing this policy. Once implemented repeat this scan and if the policy is correctly implemented on the device being scanned, this clause will be marked compliant for this device.

8.2.4 Change user passwords at least every 90 days.

8.2.4a For a sample of system components, obtain and inspect system configuration settings to verify that user password parameters are set to require users to change passwords at least every 90 days.

5006:	Maximum Password Age	**Compliant**

Strong passwords are the first line of defence into a network since a malicious individual will often first try to find accounts with weak or non-existent passwords.You must ensure that user passwords are changed at a minimum every 90 days. Passwords used for a long time without change increase opportunity for a malicious person to compromise the associated account. Periodic password change should be enforced using a policy or setting on the system components that is not able to be bypassed by the user.If you need assistance, your local IT administrator will be able to provide you with guidance on implementing this policy. Once implemented repeat this scan and if the policy is correctly implemented on the device being scanned, this clause will be marked compliant for this device.

8.2.5 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.

8.2.5.a For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that new passwords cannot be the same as the four previously used passwords.

5005:	Password History Check	**Not Compliant**

Strong passwords are the first line of defence into a network since a malicious individual will often first try to find accounts with weak or non-existent passwords.You must ensure that user passwords are not repeated within the last four password changes. This should be enforced using a policy or setting on the system components that is not able to be bypassed by the user.If you need assistance, your local IT administrator will be able to provide you with guidance on implementing this policy. Once implemented repeat this scan and if the policy is correctly implemented on the device being scanned, this clause will be marked compliant for this device.

Requirement 11: Regularly test security systems and processes.

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

11.2.1 Perform quarterly internal vulnerability scans.

11.2.1.b Review the scan reports and verify that the scan process includes rescans until passing results are obtained, or all High vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved.

Patches:	Patch & Vulnerabilty Scan	**Compliant**

Vulnerability scans are used as a means of detecting and identifying actual and potential vulnerabilities within your system components. Vulnerabilities are system weaknesses that could be used to compromise a system's integrity, thereby allowing an attacker access to the system and potentially cardholder data.Once vulnerabilities are detected and have been documented, you are required to take action to resolve these vulnerabilities. Your process must include a requirement to re-scan until you have achieved a passing scan (i.e. all vulnerabilities resolved) or at a minimum all "High" Vulnerabilities (i.e. those vulnerabilities posing the highest risk which have been ranked "High" per Requirement 6.2) are resolved. You can repeat this scan on a quarterly basis on all of your business' devices to ensure you are identifying potential vulnerabilities within your system components.

Vulnerability Summary

PASS

No Vulnerabilities Detected

Total number of security checks executed: 8,614

Unprotected Data Details

Currently showing a maximum of 500 suspected instances.
Each instance type is limited to 50 findings.

File Name	Findings Count
D:\DATA\Styrelse\Complete\WO99D\ob\1\Arkiv\2010.zip	1

SHA256	b1415f015a487c9ed22eb9e0f4ce02ba4c2869b44e1490ddebcff11678bc8d91
SHA1	b3576f5278860b062338527aace816ef89850a71
MD5	56271beafef5b992f85a60a623299e6d

93980up.HTM

Visa13

4209XXXXXXXX5262

D:\DATA\Styrelse\Complete\WO99D\shipped\Arkiv\2009.zip	1

SHA256	68bd0f662d804811093be5a7dc9340b167431dee0b027462b52687ab53d27cdb
SHA1	899501e4e9214d18ed25b20f0a5d08172c588b68
MD5	7316dd83bba89bac035048fd52066608

89711.htm

Visa13

4026XXXXXXXX0567

D:\DATA\Styrelse\Complete\WO99D\TEMP\bak\flrad.txt	1

SHA256	73108a2bd8f926342740b11c4871aa8be941b124959e920645dd0bcd0bfa22f3

SHA1	eeb1e786dbb485fca29138a85b0cf8abf53f2847
MD5	2d309c1412b9b35f58d76a6e73eb5167

Visa13

4971XXXXXXXX2608

Unprotected Data Scan Statistics

Elapsed Time	0 hours, 6 minutes, 16 seconds
Files Scanned	57,645
Files with Suspect Data	3
Bytes Scanned	3,893,222,938
Suspected Instances Found	3

Volumes Scanned

Drive Root	Drive Capacity	Used Space	Free Space
D:\	73,369,907,200	22,712,729,600	50,657,177,600
E:\	146,776,518,656	74,068,197,376	72,708,321,280
C:\	73,265,049,600	48,948,252,672	24,316,796,928

Network Port Details

This section displays the open and listening TCP/IP ports on this system. Open ports indicate that a service is listening for external communication from a remote computer. Review the list of open ports to determine if they are absolutely necessary. Disable any unnecessary services to reduce the risk of compromise from malware or attackers. We recommend that you back up your system before making any changes. Your local IT administrator will be able to provide you with guidance on managing your network ports.

Result

```
TCP    0.0.0.0:25             0.0.0.0:0              LISTENING
TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
TCP    0.0.0.0:88             0.0.0.0:0              LISTENING
TCP    0.0.0.0:110            0.0.0.0:0              LISTENING
TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
TCP    0.0.0.0:143            0.0.0.0:0              LISTENING
TCP    0.0.0.0:389            0.0.0.0:0              LISTENING
TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
TCP    0.0.0.0:464            0.0.0.0:0              LISTENING
TCP    0.0.0.0:587            0.0.0.0:0              LISTENING
TCP    0.0.0.0:593            0.0.0.0:0              LISTENING
TCP    0.0.0.0:636            0.0.0.0:0              LISTENING
TCP    0.0.0.0:808            0.0.0.0:0              LISTENING
TCP    0.0.0.0:993            0.0.0.0:0              LISTENING
TCP    0.0.0.0:995            0.0.0.0:0              LISTENING
TCP    0.0.0.0:2301           0.0.0.0:0              LISTENING
TCP    0.0.0.0:2381           0.0.0.0:0              LISTENING
TCP    0.0.0.0:2814           0.0.0.0:0              LISTENING
TCP    0.0.0.0:3268           0.0.0.0:0              LISTENING
TCP    0.0.0.0:3269           0.0.0.0:0              LISTENING
TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
TCP    0.0.0.0:5000           0.0.0.0:0              LISTENING
TCP    0.0.0.0:5314           0.0.0.0:0              LISTENING
TCP    0.0.0.0:5432           0.0.0.0:0              LISTENING
TCP    0.0.0.0:5948           0.0.0.0:0              LISTENING
TCP    0.0.0.0:6001           0.0.0.0:0              LISTENING
TCP    0.0.0.0:6002           0.0.0.0:0              LISTENING
TCP    0.0.0.0:6003           0.0.0.0:0              LISTENING
TCP    0.0.0.0:6004           0.0.0.0:0              LISTENING
TCP    0.0.0.0:6005           0.0.0.0:0              LISTENING
TCP    0.0.0.0:6006           0.0.0.0:0              LISTENING
TCP    0.0.0.0:6007           0.0.0.0:0              LISTENING
TCP    0.0.0.0:6008           0.0.0.0:0              LISTENING
TCP    0.0.0.0:6010           0.0.0.0:0              LISTENING
TCP    0.0.0.0:6011           0.0.0.0:0              LISTENING
TCP    0.0.0.0:9389           0.0.0.0:0              LISTENING
TCP    0.0.0.0:21300          0.0.0.0:0              LISTENING
TCP    0.0.0.0:29367          0.0.0.0:0              LISTENING
TCP    0.0.0.0:29382          0.0.0.0:0              LISTENING
TCP    0.0.0.0:29387          0.0.0.0:0              LISTENING
TCP    0.0.0.0:29419          0.0.0.0:0              LISTENING
TCP    0.0.0.0:29445          0.0.0.0:0              LISTENING
TCP    0.0.0.0:29455          0.0.0.0:0              LISTENING
TCP    0.0.0.0:29479          0.0.0.0:0              LISTENING
TCP    0.0.0.0:29483          0.0.0.0:0              LISTENING
TCP    0.0.0.0:29485          0.0.0.0:0              LISTENING
TCP    0.0.0.0:29488          0.0.0.0:0              LISTENING
TCP    0.0.0.0:29494          0.0.0.0:0              LISTENING
TCP    0.0.0.0:29500          0.0.0.0:0              LISTENING
TCP    0.0.0.0:29518          0.0.0.0:0              LISTENING
TCP    0.0.0.0:29642          0.0.0.0:0              LISTENING
TCP    0.0.0.0:29664          0.0.0.0:0              LISTENING
TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING
TCP    0.0.0.0:64327          0.0.0.0:0              LISTENING
TCP    0.0.0.0:64337          0.0.0.0:0              LISTENING
TCP    127.0.0.1:53           0.0.0.0:0              LISTENING
```