PCI DSS 3.2.1 and what it means for the NonStop

by Greg Swedosh *Knightcraft Technology*

The latest version of PCI DSS, version 3.2.1, came into effect earlier this year and with it there are some new considerations for organizations that are running HPE NonStop servers. Version 3.2.1 was essentially an update to change the new requirements for version 3.2 from recommendations to edicts as the cut-off dates have already rolled around. This article describes what needs to be done now to be compliant with PCI DSS for these changes. It will also have a look at the other great change that has occurred recently with PCI DSS, that of compliance vs security. Finally, a list will be provided of what minimum functionality you need on your systems to truly be secure as well as compliant.

SSL/TLS on the HPE NonStop

"Entities using SSL and early TLS must work toward upgrading to a strong cryptographic protocol as soon as possible. Additionally, SSL and/or early TLS must not be introduced into environments where those protocols don't already exist", PCI DSS v3.2.1, Appendix A2.

As of June 2018, SSL and early version TLS are not acceptable solutions for encrypting data in transit. That means that all SSL/TLS connections need to be upgraded to a minimum accepted version of at least TLS 1.1, though TLS 1.2 is the recommended minimum. When we think of SSL/TLS connections in the NonStop world, the ones that often come to mind are those related to terminal emulation and TACL or FTP sessions. These of course need to be considered but there are a number of other places where this type of transport method may also need to be upgraded. The following is not an exhaustive list but will hopefully get you thinking about possible areas where SSL/TLS is used within your organization:

1. Terminal emulator sessions (TACL, OSH) via NonStop SSL or software vendor products.
2. Secure FTP sessions via NonStop SSL or software vendor products.
3. iTP secure Webserver.
4. Connections to virtual tape devices such as VTS or BackBox VTC.
5. File transfer links to mainframe or other systems within the organization.
6. Communication to external organizations (interchange links, file transfer links).
7. Between the HPE NonStop and ATMs or POS devices.
8. Expand links.

Multi-Factor Authentication and PCI DSS 3.2

"Incorporate multi-factor authentication for all non-console access into the CDE (Cardholder Data Environment) for personnel with administrative access", PCI DSS v3.2.1, Requirement 8.3.1.

Previously, multi-factor authentication (MFA) was only required when connecting to systems from outside of the corporate network. The change for PCI DSS 3.2.1 is that now all administrative access to the system requires MFA. The first thing to be considered is what actually constitutes administrative access? Typically in the NonStop world we think of SUPER.SUPER and of course this powerful userid is right at the top of the list. But a number of other userids need to be considered also. This may be due to the inherent privileges that they possess or because their use may facilitate a user being able to elevate their privileges to those of SUPER.SUPER or to gain access to cardholder data:

1. SUPER.SUPER (of course).
2. All SUPER group userids.
3. Security administrator userid(s).
4. Application/Data owner userids.
5. Application builder userids.
6. Data replication owner ID.
7. Netbatch administrators.
8. Userids with the ability to modify system/subsystem/application startup or config files or objects.
9. Any userids or aliases that manage configurations for security utilities such as XYGATE Access Control (XAC), SECOM, CSP Passport etc.

All of the above userids should be considered userids with "administrative access" due to the various powers they possess. And if you are going to be enforcing these userids to authenticate with MFA, why not enforce all users? It will likely be simpler to manage than trying to implement one solution for certain IDs and another for others.

The other aspect of this requirement that needs considering is how you will implement multi-factor authentication. There are a number of possible alternatives for this as the MFA does not need to occur specifically on the HPE NonStop server itself, although that is of course one possibility. The following example methods of MFA are all considered acceptable:

1. MFA at the time of logging on to the NonStop.
2. At the network level if the segment in which the system resides is appropriately isolated e.g. authentication as part of setting up a VPN prior to accessing the NonStop.

3. Authentication to a jump server (jump host) from where the NonStop is accessed e.g. via a Citrix server.
4. Single Sign-On (SSO) using a mechanism such as Kerberos, as long as the initial sign-on has been authenticated using MFA.
5. SSH private/public keys with a passphrase. Note that while this method is likely to be accepted by a QSA (PCI Qualified Security Assessors) as MFA, at least currently, it is potentially flawed due to the ability to store the passphrase within a terminal emulator.

One other aspect of this requirement is in regards to the specification of "non-console access". PCI DSS states that administrative access may be obtained to the system without MFA if the user is logging in directly from the system console. This applies to console sessions where the user is physically sitting at the console in an access controlled and monitored environment. It DOES NOT apply to sessions where a user has remotely connected in to the console using Remote Desktop or other similar mechanism. For that kind of access, users should certainly be using an accepted method of MFA.

Defining the Cardholder Data Environment

"At least annually and prior to the annual assessment, the assessed entity should confirm the accuracy of their PCI DSS scope by identifying all locations and flows of cardholder data", PCI DSS v3.2 Template for Report on Compliance, Section 3.1.

The template for Report On Compliance (ROC) section 3.1 is used by QSAs when performing a PCI DSS assessment. In reference to defining the cardholder data environment (CDE), it says that organizations must:

- *"Describe the methods or processes used to identify and document all existences of cardholder data."*
- *"Describe the methods or processes used to verify that no cardholder data exists outside of the defined CDE."*

QSAs must:

- *"Describe why the methods used for scope verification are considered by the assessor to be effective and accurate."*

This will likely result in a greater push by QSAs for organizations to use automated tools, to prove that cardholder data exists only where they have specified and that no cardholder data exists outside of the area defined.

The other major change in PCI DSS... Perceptions of compliance vs security

Many organizations seem to believe that if they are passed by a QSA as compliant with PCI DSS, then that means that their systems are secure. This is not necessarily the case, as the many high profile data breaches tell us. A number of these breaches resulting in the loss of millions of credit card and/or PII records have occurred within organizations that believed that they were PCI DSS compliant at the time. In fact in many cases they had been ticked off by QSAs as being compliant. This has led to a lot of discussion over the merits of PCI DSS and whether it was truly a standard of worth, as following it didn't seem to guarantee security from credit card fraud. The truth is that at the time of these breaches, none of the organizations in question was truly compliant. And clearly they weren't secure.

- PCI DSS is a minimum standard for security and auditing settings, procedures and documentation.
- QSAs are typically not experts in HPE NonStop security. Many in fact know very little about the NonStop environment.
- PCI DSS assessments are typically based on a checklist, documentation and on responses from the customer. They are not an in-depth system security review.
- Staff may be tempted to withhold unasked-for information from QSAs so that the company is marked as compliant.

Given the above points, how can compliance necessarily imply security?

While PCI DSS compliance is essential for organizations to ensure that they have appropriate procedures, documentation and security fundamentals in place, and of course to avoid any fines or increased transaction charges associated with non-compliance, organizations should take measures to also have a regular review (at least annually) of their security by somebody with an appropriate level of NonStop security expertise.

What is required to achieve both PCI DSS compliance and security?

The following is a list that should be considered as a minimum set of controls that HPE NonStop customers should have in place to ensure that they are both PCI DSS compliant and that they have secure systems.

- Safeguard optimally configured with "deny all by default" to prevent unauthorized access and to also provide appropriate auditing of file access.
- OSS security configured for appropriate directory and file access levels.
- Security aspects of all subsystems configured to prevent users gaining unauthorized elevated privileged access (Safeguard, Pathway, Netbatch, TACL, SCF, Expand etc.).
- XYGATE Merged Audit (XMA) installed and configured to deliver security events in real-time to a SIEM device.
- NonStop SSL/SSH implemented to provide encrypted TACL/OSH/FTPS sessions.
- Mechanism to provide individual accountability to all user logons (e.g. force users to logon to personal userid before logon to super.super or other shared privileged userid). XUA now ships with the operating system and can be used for this purpose.
- HPE optional or software vendor product to provide keystroke logging of user sessions (e.g. XAC, Safepoint/KSL, SECOM, Passport).
- File Integrity Monitoring (FIM) software to detect any changes to critical files (application objects, system configuration files, startup/shutdown files etc.). A number of solutions exist from software vendors.
- Encryption or tokenization of cardholder data. This can now be achieved without changes to the application or database using tokenization and intercept library based products such as comForte DPS, XYGATE Data Protection (XDP) or TANDSoft products.
- Automated tool to verify that there is no unprotected cardholder data in unauthorized locations. Currently only PANfinder (4tech Software) provides this capability on the NonStop.
- Appropriate Multi-Factor Authentication.

Greg Swedosh is the director and senior security consultant of Knightcraft Technology. He is a regular presenter on NonStop security at the NonStop advanced technical boot camp and has provided PCI compliance reviews of NonStop systems on behalf of a QSA. Knightcraft security services for the HPE NonStop can be procured directly (www.knightcraft.com), through your HPE account team or from comForte. A free copy of the PCI DSS for HPE NonStop Servers technical white paper can be downloaded from http://www.knightcraft.com/hpe-nonstop-pci-dss-3-2-compliance.