PCI DSS V4.0 ADDS NEW PAN DATA DISCOVERY REQUIREMENT

With the introduction of the new Requirement 12.5.2, PCI has effectively mandated the use of PAN data discovery – necessary for defining and verifying your PCI DSS Scope and Cardholder Data Environment.

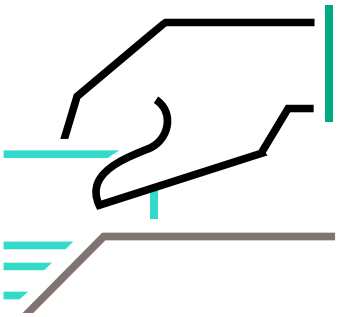
Dan Lewis, Director and co-founder at 4tech Software Ltd., takes a look at one of the key updates in PCI DSS V4.0

One of the most significant updates to V4.0 of the Payment Card Industry Data Security Standard (PCI DSS) compared to the out-going V3.2.1 is the new emphasis being placed on the importance of Scoping – or defining and confirming your Cardholder Data Environment (CDE). It's your CDE which needs to meet PCI's increasingly stringent requirements, as that's where your customer card data lives and is processed.

PCI DSS V3.2.1 devoted three pages of the introduction to information on the Scope of PCI DSS Requirements and defined the CDE as "...people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication data."

PCI DSS V4 goes *much* further, providing a far more detailed introduction on the subject of Scoping (now running to ten pages) and now also includes a brand-new specific requirement within the Standard: '12.5 - PCI DSS scope is documented and validated'. That validation requirement will be covered later in this article.

V4.0 is also far more broad when it comes to defining the CDE, which is now described as "System components, people, and processes that store, process, and transmit cardholder data and/or sensitive authentication data, ***and, System components that may not store, process, or transmit CHD/SAD* but have unrestricted connectivity to system components that store, process, or transmit CHD/SAD. And system components, people, and processes that could impact the security of the CDE***."



*CHD is Card Holder Data
SAD is Sensitive Authentication Data

Why has the Payment Card Industry done this?

Because it's been demonstrated in countless data breaches, that stolen payment card data was lifted from locations which were deemed to have been outside of companies' defined scope! In other words, companies *thought* they knew where all their card data was, they *thought* it was adequately protected, they *thought* their documented CDE was accurate and they *thought* they were PCI DSS compliant. But time and time again, they were wrong! Often with huge financial cost and reputational damage. These companies were putting all their efforts into protecting data where it *should* have been, but failed to consider where their valuable customer card data *could* have been. This over-reliance on the accuracy of their initial PCI DSS Scoping left them oblivious to the payment card data residing outside their CDE and the exposure they faced. With the publication of DSS V4.0, PCI aims to put an end to the breaches caused by loss of data from areas deemed to be outside of PCI DSS scope, by mandating far more rigorous checking and throwing the 'in scope' net far wider than was previously acceptable.

By introducing Requirement 12.5.1 and the far more extensive 12.5.2, PCI is no longer simply highlighting the importance of an accurate CDE inventory, like it was in all previous editions. It's now making **validation** of your CDE a specific requirement, shining a light on the fact that PCI DSS compliance now applies to your entire network, not just the area/s on individual systems where you believed payments data is being stored and processed.

Requirement 12.5.2 in detail

Below is a cut-and-paste of the new requirement 12.5.2 contained in PCI DSS V4.0:
12.5.2 PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes:
• Identifying all data flows for the various payment stages (for example, authorization, capture settlement, chargebacks, and refunds) and acceptance channels (for example, card-present, card-not-present, and e-commerce).
• Updating all data-flow diagrams per Requirement 1.2.4.
• Identifying all locations where account data is stored, processed, and transmitted, including but not limited to:
1) any locations outside of the currently defined CDE
2) applications that process CHD
3) transmissions between systems and networks, and
4) file backups.
• Identifying all system components in the CDE, connected to the CDE, or that could impact security of the CDE.
• Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope.
• Identifying all connections from third-party entities with access to the CDE.
• Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope.

All those bullets listed above are important, but the third one, with its four separate sub-points is especially key. **You now need to confirm/validate there is no account data (aka customer payment card data) being stored outside your CDE.**

As with all DSS requirements, PCI spells out what you need to achieve, but doesn't tell you how you need to achieve it, because there is often more than one way you can meet a standard. In the case of requirement 12.5.2, the Guidance provided includes the sentence "A data discovery tool or methodology can be used to facilitate identifying all sources and locations of PAN, and to look for PAN that resides on systems and networks outside the currently defined CDE or in unexpected places within the defined CDE—for example, in an error log or memory dump file. This approach can help ensure that previously unknown locations of PAN are detected and that the PAN is either eliminated or properly secured."

Can I be PCI DSS compliant without using a data discovery tool?

Technically, yes you can - but don't get too excited. The alternative to using a PAN data discovery tool to validate the accuracy of your defined CDE and confirm you don't have readable card data in unknown locations would be: to read every byte of data in every single file on your network manually! If you can knock down say 100kB of data in one minute, you should be able to check a full 1TB disk in *only 19 years*. With PCI DSS Requirements 12.5.2 and 12.5.2a stating that you must confirm and validate your PCI DSS Scope at least once every 12 months and upon significant change to the in-scope environment, you'd need an army of 1,900 people reading 24h a day to read 100TB of data in a year! So as I said, technically it is possible to be PCI compliant without PAN data discovery, but practically and realistically: no, it's not.

Is PCI DSS Compliance the Gold Standard?

As with all PCI DSS requirements, they are the minimum standards you should be achieving. In reality, checking and validating your PCI DSS Scope once per year is clearly inadequate. Validating your defined CDE and checking your systems once per years is certainly a lot better than never, but in reality PAN data discovery (aka CDE validation) should be an on-going, 24x7x365 process. Any company which truly wants to protect its customer payment data to the best of its abilities would want to be PCI DSS compliant every second of every day, not once per year when the annual compliance audit comes around again. While PCI don't mandate 24x7 PAN monitoring, they do emphasise the importance of ongoing compliance and ongoing monitoring in their Good Practice notes: "*Scoping activities, including careful analysis and ongoing monitoring, help to ensure that in-scope systems are appropriately secured.*"

Payment Card Data Discovery on HPE NonStop

If only there was a commercially available tool, created exclusively for the NonStop server, with the sole purpose of searching every corner of your NonStop and identifying readable payment card data…?

Well, as I'm sure you've gathered by now, that tool already exists, and it has since 2010. It's being used in production by companies all over the globe who genuinely take data security seriously and are pro-active in taking steps to reduce the risk of a data breach. That tool is called PANfinder - PAN is the acronym for Primary Account Number, which is the long number on any credit or debit card. It's worth noting that PANfinder also searches for full track data, not just the PAN part

Quiz Time

Whenever a company installs PANfinder, they usually hope it will just confirm what they already knew. That being: they know where all their PAN data is/was, their manually created CDE is accurate, their customer data is being adequately protected and there is no rogue readable payment data hiding in unknown locations, outside of their defined CDE. If that was the case, PANfinder would run its scan and come back with a squeaky clean set of reports containing zero PANs. Have a guess how many PANfinder customers ran their first scan and came back with a clean report? The answer is zero - none of them. Every single PANfinder user has identified unknown readable payment data on their system. And that includes companies who had tokenized their databases and were convinced they were 100% PCI DSS compliant.

Where does PAN data hide?

Sometimes PANfinder users found mountains of live card data copied over to a test system for a project and then left behind by contractors after the project has finished (live data being copied to a test system is a separate issue!). Sometimes it's transaction data being inadvertently copied to trace files. Sometimes it's in the log files of third party session-tracking applications installed to improve data security, but were actually creating data security problems of their own! And there are many other examples of readable payment data residing in all manner of places where it shouldn't be and that data being identified by PANfinder.

While it might be a little embarrassing for companies to admit (internally at least) that PANfinder had identified holes in what they thought was a water-tight data security ship, every time PANfinder highlights an issue is actually a fantastic result. It means rogue data can be deleted or encrypted and it means systems, procedures or software causing the problems can be patched to prevent further data creation. By taking those steps to remove readable card data from their systems, PANfinder customers are reducing their risk, reducing easy opportunities for hackers/rogue insiders to steal data and reducing the chances of huge financial and reputational damage to their organizations which result from a breach.

Additional Reading

.

The full version of PCI DSS V4.0 is available via the PCI website at:
www.pcisecuritystandards.org/document_library

PCI has also published a useful 25-page Information Supplement relating to PCI DSS scoping called: Guidance for PCI DSS Scoping and Network Segmentation.
www.pcisecuritystandards.org/search_result/documents/pci_scoping_guidance

The PANfinder Data Sheet is available via the HPE website at:
www.hpe.com/psnow/doc/a50005007enw