Protecting Cardholder Data

Meeting PCI Software Security Standards

Meet the experts:

Martin Callinan has over 20 years of experience in the software industry specializing in software licensing, IT Governance and risk avoidance. He is a member of The Linux Foundation's OpenChain project and Software Freedom Conservancy.

Michael Christodoulides is a cyber security, risk and assurance professional with extensive experience managing and delivering risk and assurance assessments across the payment card industry. He has previously represented payment card industry stakeholders as a representative to the Board of Advisors of the PCI SSC.

Kendra Morton is the Senior Product Marketing Manager at Revenera focused on Software Composition Analysis and open source scanning solutions. Kendra has experience leading all areas of technology marketing including software, data and analytics, cloud offerings, and customer management solutions.

With the regulatory changes by the Payment Card Industry Security Standards Council (PCI SSC) related to the development and management of payment application software, Revenera conducted an interview with several experts to address frequently asked questions.

QUESTION: Who should care about PCI standards and more specifically the most recent security standard updates?

Martin: The PCI Secure Software Standard and fundamental Secure Software Lifecycle Standard applies to payment software that is sold, distributed, or licensed to others that support payment transactions. Software companies developing applications for payment processing and selling those applications should particularly take notice of the security standards and any updates to regulations.

QUESTION: There's been some buzz since early 2019 about newer standards related to open source governance. Can you explain the changes that were introduced?

Kendra: The goal is to make electronic payments more secure by ensuring that the security of payment software is addressed throughout the entire software development lifecycle.

The new standard requires software companies developing payment solutions to continuously identify and assess weaknesses within software applications, including the entire software supply chain. This includes accounting for the entire codebase. The key word here is "continuously."

QUESTION: For software development companies delivering payment application software to customers, what does it mean to be PCI compliant?

Michael: PCI compliance means that controls are in place to protect cardholder data as described by one of the 15 security standards published by the PCI SSC. A PCI certified security assessor will be able to provide guidance regarding all responsibilities and relevant PCI standards. For a list of regional assessors, go to https://www.pcisecuritystandards.org/ and search the Assessor and Solutions tab.

QUESTION: How difficult is it to discover open source vulnerabilities and compliance issues?

Martin: First of all, open source is definitely in your codebase. No question, so you need to track it. Manual tracking and discovery of open source risk is difficult and impractical. Engaging in ad hoc audit services can be a step in the right direction but serves more of a point-in-time approach and doesn't create an ongoing, continuous and repeatable scenario for payment software companies. To really get a handle on vulnerabilities and other risks, and to meet the standards set forth by the PCI SSC, it requires an automated scanning tool used throughout the SDLC. We recommend implementing a Software Composition Analysis solution.

Revenera research shows that companies are only aware of **2% of the risk issues** hiding in their open source and third-party components.

QUESTION: What does a Software Composition Analysis solution do exactly?

Kendra: Open source today is at the heart of software development. It's a mainstay, and for good reason. However, it's important for organizations and their engineering teams to know what's in their code and to proactively manage the security vulnerabilities and license compliance issues that come with the territory. The way to do that is by using Software Composition Analysis (SCA).

Look for an end-to-end platform that integrates seamlessly with your build environment while providing automated detection and remediation of issues. It's important to find a solution that enables flexible analysis and scanning of source code, binaries, and subcomponents that you can dial up or down—stay high level or go deep—depending on changing business requirements.

QUESTION: What was the main driver behind the PCI's updates to open source security requirements?

Michael: Compared to only a few years ago we now transact payments using a variety of form factors. The number of stakeholders that comprises the payments ecosystem has also grown significantly. The traditional physical payment card is also being digitized. Our shopping habits have changed, moving from bricks and mortar to online. The PCI SSC responded to these changes by publishing relevant security standards so that stakeholders can understand and deploy appropriate security methods to protect cardholder data.

QUESTION: Who ultimately is responsible for what's in our software and how we're meeting PCI standards?

Martin: Inside payment solution organizations, legal, security and development teams play a primary role in making sure that the software being developed meets all security standards.

NEXT STEPS

To learn more on PCI standards and the role of SCA, read *Software Composition Analysis in the Payment Card Industry.*

READ NOW >