Eva Dukerschein

DevOps

7/27/2024

Module 12

Compliance

There are a number of regulations that revolve around the movement and storage of sensitive information that information technologies must comply with. Most of these have been set forth by various governments with significant consequences for breaking them. Others are set by governing bodies and offer assurances to users and stakeholders that their information is secure. However, many of these regulations were developed when the technology industry was at a much less mature state. Many companies at this point were utilizing Waterfall development methods with highly separated development and operations teams. As the industry has grown and changed over the years we have learned that there is much to be gained from adopting Agile and DevOps practices. Learning how to balance compliance with these regulations while still maintaining a fast and stable momentum is critical to success.

There are a number of regulations with regard to payment information, especially when non-physical payment such as credit or debit cards are involved. The Payment Card Industry (PCI) Data Security Standards (DSS) Cardholder Data Environment (CDE) defines the services and tools that are overseen by this standard as “the people, processes, and technology that store, process, or transmit cardholder data or sensitive authentication data.” This definition covers a large range of services and in this case Etsy’s payment application “I Can Haz Tokens” (ICHT). ICHT is an internal application that takes customer entered cardholder data, tokenizes it, communicates those tokens to the payment processor, and executes the transaction.

In order to comply with PCI DSS, the ICHT application and application team are entirely separated from the rest of the Etsy codebase and teams. In addition, the ICHT hardware is configured differently from the rest of the organization and the components are kept under lock and key for security. This has several disadvantages. Because ICHT is configured differently, it means that the environment lacks the same set of controls and settings that the rest of the company uses. This means that tools, techniques, and systems of management need to be different in order to be effective. In addition, the ICHT team is kept separate from the rest of the organization which leads to siloing and a lack of communication. For the purposes of security this can be seen as a good thing, but in practice it does mean that the ICHT team is essentially isolated from the rest of the organization and will have difficulty sharing information and knowledge that could apply to all systems. Finally, because of the separation based on the PCI DSS requirements, there is a significant divide between the operations team and the development team which can slow down development significantly and cause unintentional service errors or even interruptions.

There are a number of ways that Etsy has used to try to mitigate the negative impacts of this however. There is a high level of telemetry in place so that possible errors can be caught and security issues can be found before deployment. Even though there are several steps involved for change approval through a single person, which would normally slow down production and release significantly, the use of JIRA in particular to flag deployments in an automated way allowed the approver to review, approve, and deploy the code in a relatively timely manner.

What this case study shows us is that compliance to regulations can create friction within a DevOps setup. However, it is still important to follow these regulations for security and compliance. What companies must do is be innovative about how to follow those guidelines not only to the letter of the law, but also to the spirit of the law in order to keep that data secure.

In another case, a financial services company that develops, maintains, and deploys the software for Automatic Teller Machines (ATMs) has found that many pieces of the security puzzle tend to rely too much on code control to detect possible problems. They found that Information Security, auditors, and regulators tend to look toward code development in order to try and detect fraud. This is a short-sighted and incomplete understanding of software production however as it fails to recognize the power and advantages of monitoring and simultaneously underestimates the skill and cunning of bad actors. In a notable instance, a developer had created a backdoor to the code that was deployed to their ATMs. It was set up in such a way as to be incredibly difficult to detect, and did in fact go to production despite the many safeguards put in place by information security in accordance to regulations. The reason why the fraud was detected was due to a robust telemetry and reporting system. The backdoor was set up to allow the individual to withdraw cash from an ATM when in maintenance mode. Thanks to the reporting systems in place, it was noted that the ATMs were going into maintenance mode when they were not supposed to. Code reviews, separation of duties, and change approval processes failed to catch the exploit while active production reporting did. This example shows us that regulations require a much more comprehensive understanding of the process used to create, deploy, and maintain code in a modernized setting.

The concept of regulation and of product development are not inherently at odds. However, the time it takes to understand and change regulations can create problems when techniques for development progress faster than the regulations themselves. It is imperative that companies still adhere not only to the regulations as they exist, but also adhere to the idea behind those regulations which is to create safe and secure applications for users. This may seem difficult in a DevOps environment where much of the development is done tightly coupled with operations, but as can be seen with the recent inclusion of security services to the process, sometimes called DevSecOps, it is not impossible to attain. New ways of approaching this evergreen topic must be considered as the industry continues to grow and change.

Sources

Kim, G., Debois, P., Willis, J., Jez Humble, & Allspaw, J. (2021). *The DevOps handbook : how to create world-class agility, reliability, & security in technology organizations*. It Revolution Press, Llc.

‌