Providing Compliance in Regulated Environments 2015

This case study highlights the work of Bill Shin, a principal service solutions architect at Amazon Web Services, or AWS. One of the challenges and main points Bill Shin identifies is the disconnect between the traditional ways AWS audits in comparison to more modern DevOps practices. Shin explains that auditors have “been traditionally trained to ask for a sample of one thousand servers” and to rely on manual reviews, such as “screenshot evidence of asset management, access control settings, and server logs.” While this method might have worked well in terms of physical servers, it falls short in cloud-based environments where “infrastructure is code” and servers are dynamically created. Due to this disconnect in dated auditing, Shin proposes the solution and main point of integrating systems such as Splunk or Kibana in the auditing process. Utilizing these tools would help auditors access real-time data. Shin notes, “Auditors can get what they need, completely self-serviced.” The auditors can simply “log into Kibana, and then search for audit evidence they need for a given time range. This would help the dated auditing process not only more efficient but also help increase transparency. Another key point in the case study is AWS’s adoption of an iterative process by closely collaborating with auditors during the control design phase. This approach ensures that compliance requirements are met while preserving the flexibility and speed of DevOps practices. The collaboration between security, DevOps, and compliance teams ensures that controls are properly implemented and audit evidence is always available.

Relying on Product Telemetry for ATM Systems 2013

This second case study focuses on Mary Smith, a DevOps leader in a major US financial services organization. Smith observes that regulators and auditors often place "too much reliance on code reviews" as a primary method to detect fraud, whereas production monitoring controls should play a more significant role. She tells of an incident in which a developer planted a backdoor in the ATM software, which allowed for unauthorized access to the machines. Despite having a separation of duties between Development and Operations and a change approval process in place, the fraud was not detected through code review. Instead, it was uncovered through production telemetry when someone noticed that "ATMs in a city were being put into maintenance mode at unscheduled times." This example highlights the limitations of traditional security measures like code reviews and approvals, particularly when dealing with sophisticated attacks. Smith notes that these methods often fail to catch certain risks, especially when attackers have "sufficient means, motive, and opportunity." She stresses the importance of continuous monitoring through telemetry, which offers the necessary visibility to detect and respond to fraud in real-time. By proactively monitoring production environments, organizations can identify issues early, allowing them to react swiftly and mitigate potential damage. This case study also makes the broader point that relying on production telemetry can reduce the need for rigid processes like separation of duties or extensive change review boards. Continuous monitoring not only enhances security but also offers a more dynamic and effective approach to detecting fraud and errors.

Lessons Learned

Both case studies emphasize the need for more modern security and compliance practices that align with DevOps principles. Shinn at AWS shows the importance of automating audit processes and providing auditors with real-time data. This approach helps ensure compliance is maintained in any environment. Smith’s experience with ATM systems shows the limitations of traditional security measures like code reviews, and separation of duties and emphasizes the value of production telemetry in detecting fraud. Both cases show that effective security in regulated environments requires more than simply adhering to outdated methods. Organizations need to start embracing automation, real-time monitoring, and cross-team collaboration to ensure that both compliance and security goals are being met.