Sonatype's Derek Weeks on Eliminating Silos and Infusing Security Early in DevOps

Partner Content
How integrating security into the development life cycle can enhance the value created by a team.
Tue, 01/01/2019 - 10:04

Sonatype Vice President Derek Weeks joined GovernmentCIO Media & Research President Michael Hoffman to discuss the value of DevSecOps, security breaches and Sonatype's All Day DevOps conference.

Question: What is the difference between DevOps and DevSecOps?
**Weeks:** DevOps really started as a way to eliminate waste within software development basically helping software developers move business value to market a lot faster and it basically eliminated the 18-month release cycle. With DevSecOps it's really about bringing security into the software development lifecycle, not only as just a bolt on thing at the end of the lifecycle, but really at the beginning of the development process itself and then throughout development.

**Question:** What impediments do government agencies face when implementing a DevSecOps approach?

**Weeks:** I think in both large enterprises as well as government organizations the biggest impediment that I've seen is that people generally like their silos. They've operated in silos of development security and operations for years and they haven't integrated those workflows in order to help bring value to market faster. I think in this new age of higher velocity releases to market or to constituents, what we have to consider is that security is baked into the beginning of the lifecycle. It's actually integrated in for the developer to make decisions faster where they can actually make decisions with intelligence presented to them inside their tools within seconds versus sending it off to a security organization for reviews that might take anywhere from a number of hours to months for response time. So I think that organizations need to understand that there are tools and solutions that can be instrumented in their workflows to help them achieve security much earlier in the lifecycle development with less friction.

**Question:** Where are supply chains most susceptible to attack?

**Weeks:** The super micro hack was very interesting because it really focused on an attack that was within a technology supply chain. Technology supply chains are very sophisticated and they're multifaceted. And to pull off a hack of this scale had to take a lot of coordinated effort. There are some that say it was a hoax. There are some that say that this particular hack was real. But when we look at our technology supply chains, while the hardware hack that was documented by Bloomberg was sophisticated, there are less sophisticated attacks that are happening already within our software supply chains and software supply chains have much more attack surface available to them to our adversaries than what we see in the technology or hardware supply chain.
Question: Are software supply chain attacks even more dangerous than hardware supply chain attacks?

Weeks: I think when it comes to software. Our organizations are a lot more exposed than most people imagine. Today an average application is composed of open source software components. In fact, about 80 percent of the typical application is composed of these components. These components are brought into the organization by software development teams that bring in hundreds of thousands of components from unknown sources of unknown origin and unknown quality.

When these software components are downloaded and used in applications we're seeing download vulnerability rates in the range of 12 percent for Java components, in the range of 50 percent or JavaScript components that are used by developers.

When these vulnerable components are built into the applications, it increases the attack surface available to adversaries and hackers out there, which leaves a lot of great exposure within software supply chains that are feeding development practices in these organizations. We've seen that it's very easy for hackers to pull off injecting malicious code into these software components that have been downloaded by millions of people a week in some cases. By comparison hardware supply chain attacks are very sophisticated. They're multifaceted. There are a lot of high touch points and you have a lot more physical controls in place for those attacks to be harder to pull off. So I think just because of the ease of software supply chain attacks they are more dangerous.

Question: Are government agencies with mature DevOps practices integrating automated security more often?
**Weeks:** Matured DevOps practices are instrumenting their automated security much more in the software development lifecycle. In fact, we saw 335 percent more automated security implementations in mature DevOps practices versus organizations that had no dev ops practices. The other really interesting thing about the results from the survey was we saw empirical information that said where automated security was being applied compliant to the security rules was more effective. In fact, it was twice as effective in those environments where we asked people do you have security controls in place and are you following them in the places where security was automated most throughout the development lifecycle we saw a 2X higher compliance ratio to those security policies.

**Question:** Why do web applications receive the most attacks?

**Weeks:** Web applications or not only the most targeted by hackers, they are the most breached by hackers. The primary reason for this is they're connected to where all the data sets. Whether that's personal information or financial information that's available to the consumers using those web applications. The hackers know that that's the entry point or the front door to that data for the organization.

Now, the exploit patterns have actually changed over the last few years and I don't think most organizations are aware of this. If it was 10 years ago the time between a vulnerability being announced and it being exploited in the wild was about 45 days. In 2017, in the case of Equifax as the most notable breach of that year, we saw the exploit pattern reduced to three days between the vulnerability announcement and the exploit. While a lot of people focus on Equifax as the breached organization, they don't realize that during that same week within those same few days after the vulnerability was announced we saw nation states scanning the DoD networks. We saw the Canadian Revenue Office, Canada Statistics, the Japanese Post, Okinawa Power and India Post were all breached through the same vulnerability within the same week.
I think we need to be much more aware that not only have our development and security practices gotten faster through automation but our adversaries are using similar technology to speed up their attack patterns. More recently, in 2018, we're seeing the time between vulnerability exposure and exploit reduce down to zero. That hackers are basically injecting malicious code into the software supply chain where they can attack as soon as those open source components or open source software are deployed into production.

**Question: What stood out to you most from Sonatype's DevSecOps Community Survey this year?**

**Weeks: I think one of the results that stood out to me this year was that automated security is being introduced in more places in the software development life cycle and I think that's good for all the organizations that are experiencing breaches or know that they have adversaries or hackers approaching their infrastructure or their IT environments. That investment is good. At the same time we saw the number of known or suspected breaches increasing 50 percent year-over-year from our previous year's survey.**

So while the investments in automated security have gone up we're still seeing that the adversaries or hacker community have the upper hand. So I think we need to figure out ways to make sure that the things that we're investing in from a security standpoint are actually the things that are making the most difference in terms of protecting the data and the information that we have within our applications.

**Question: How did Sonatype's All Day DevOps conference start?**

**Weeks: What we really tried to do with All Day DevOps was bring DevOps education to the world and to do this we did it by eliminating all the barriers that people would normally applying to this kind of education. First, we made it online making it accessible to anyone with an internet connection. Secondly, we made it free. The third thing that we did was we invited a large community of DevOps professionals and thought leaders to the conference.**
So this year we had 125 speakers. We had many speakers from large enterprises as well as government organizations from the Department of Homeland Security to HHS to GSA to the Department of Defense, all were able to participate with speakers and with their employees to learn about DevOps and exchange information on a global scale and to do so in a very free environment.

I think the thing that stood out to me most was this year we had about 30,000 people participate in All Day DevOps making it the largest DevOps conference in the world. But we saw many organizations setting up viewing parties inside their own organizations where they could watch as a team, share information as a team, and be able to get more value out of the experience than just showing up and feeling like they were watching a webinar. They were also able to exchange information on our slack channel with DevOps professionals around the world which made the experience a lot more useful to them in terms of a learning platform. So it's exciting to see what we've built in the last two years -- from something that started as nothing and no attendees, to something that has 30,000 attendees.