Entrust Datacard™

IDG
STRATEGIC
MARKETING SERVICES

DEVOPS AND SECURITY: **TOO LITTLE, TOO LATE?**

NEW SURVEY FROM IDG FINDS THAT DEVOPS SECURITY SHOULD BE A SHARED RESPONSIBILITY BETWEEN DEVELOPMENT, SECURITY, AND IT OPERATIONS TEAMS—BUT IT'S NOT.

SECURITY RISKS AND BREACHES HAVE BECOME PART OF THE DAILY LANDSCAPE as companies and organizations of every size and in every vertical and industry announce that they have been compromised. In 2016 reported security breaches were up 40%, and this year is on pace to surpass that steep rise. Over the past year alone, there have been high-profile breaches in the gaming, financial services, hospitality, food service, consumer packaged goods, and retail sectors. Many of those breaches occurred due to vulnerabilities in applications and on websites. For example, this past April, the IRS announced a breach attributable to a tool designed to fetch data for the Free Application for Federal Student Aid (FAFSA) form.

These breaches have shined a spotlight on the DevOps environment, which bears the brunt of these attacks when they come to light. After all, as history has shown time and again, applications that are not secured correctly can mean the difference between getting hacked and keeping company and customer data safe and secure.

By 2020 fully 60% of digital businesses will suffer major service failures due to the inability of teams to manage digital risk. SOURCE: Gartner

Even with these high-profile breaches, there is still much work to be done to get the industry—and the applications it produces—up to speed, according to a new survey from IDG Research.[1] The risk becomes even more significant when you consider that by 2020 fully 60% of digital businesses will suffer major service failures due to the inability of teams to manage digital risk, according to research firm Gartner.[2]

STARTING FROM SCRATCH

Unlike other IT functions, security is built in to the DevOps journey from the start by only a few development teams. For example, nearly four in 10 (38%) build in security and compliance policies and controls only *after* an application has been completely developed, meaning that these crucial elements are an afterthought, putting companies and customer data at risk. Less than one-third (30%) consider security from the start before development begins.

There are significant reasons that the journey to DevSecOps—the integration and embedding of security and compliance policy and control into every aspect of the development process—has been slow, according to the survey. In the past, developers worried that building in security would stanch the development process. Today, however, the biggest challenge, according to more than half of the respondents, is the increased pace of change and evolving threats. The number of new malware and viruses is skyrocketing, with one security vendor reporting that it found 176 new threats per minute over a single quarter.[3]

At the same time, there's a serious skills and knowledge gap, a problem cited by 35% of the respondents, with about the same percentage also citing a lack of tools and technology for adopting a DevSecOps approach. For example, only a few organizations besides large enterprises are automating security testing. The IDG study found that only 28% of companies completely automate the DevSecOps process today.

DEVOPS, SECURITY, AND FINANCE: WHERE WE STAND

The 2017 Edelman Trust Barometer—Financial Services delivered some sobering news. Only 54% of the respondents to the Barometer survey reported that they trust companies in the financial sector. Although this may not be surprising, given high-profile breaches such as that at Equifax, the fact is that many finance organizations are extremely behind—and out of touch.

For example, 17% of financial companies represented in the IDG survey said that IT security policies are integrated with application and corporate policies "to little extent," as compared to 2% of all the respondents. In addition, half of all the finance organizations represented in the survey reported that "lack of organizational alignment" is a major impediment to adopting a DevSecOps program.

There are some glimmers of hope, however. About one-third of the respondents surveyed said they are piloting DevSecOps programs in their organization, with another 28% saying they have plans to start within the next 12 months. This is good news, since organizations that use pervasive, early DevSecOps practices can help thwart attacks that take advantage of vulnerabilities.

Most of the organizations looking to implement DevSecOps are doing so by leveraging Public Key Infrastructure (PKI), using strong cryptography and digital certificates as part of the development tool chain, with 70% of the respondents saying they are using PKI to secure authentication and 68% looking to the technology to protect digital signatures. About two-thirds (67%) will tap PKI for encryption. Nearly half (48%) of large organizations with more than 5,000 employees are already using PKI for container management. Although organizations may have balked at using PKI due to slowed development schedules and the time it takes to acquire keys and certificates, the landscape is changing, making it easier to implement. Using PKI in conjunction with security processes and strategies that start from the beginning of the development process creates better, more secure applications and less chance of future security breaches. This strategy, along with building security into the development process from the start, can have far-reaching, beneficial results for everyone involved.

Most important: Applications are developed with fewer vulnerabilities, which translates into shorter application response times, increased customer and user satisfaction, and the ability to provide continuous application delivery and updates. In addition, fewer security holes and issues—in theory—mean fewer costly security breaches that not only require capital for reactive remediation but also damage public sentiment and the trust and confidence of the user base. Customers are simply less likely to stick with a company that puts their personally identifiable information and assets at risk.

PKI enables developers to solidify device, user, and app identity by using authentication, digital signatures, and encryption. Issuing trusted identities to developers as well as applications and the devices they run on means that hackers have fewer ways in and users, systems, and networks are protected now and in the future.

TO LEARN MORE ABOUT PKI AND HOW ENTRUST CAN HELP YOUR DEVELOPMENT TEAM GET TO THE NEXT LEVEL, GO TO **www.entrustdatacard.com/pki.**

[1] Including 60 IT decision-makers surveyed September 14–20, 2017, by IDG Research

[2] https://www.gartner.com/newsroom/id/3337617

[3] https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2017.pdf