DZone

THE DZONE GUIDE TO

APPLICATION AND DATA SECURITY

VOLUME II

BROUGHT TO YOU IN PARTNERSHIP WITH

bmc NGINX SYNOPSYS® WhiteHat SECURITY®

Executive Insights on Application and Data Security

BY **TOM SMITH**
RESEARCH ANALYST AT **DZONE**

QUICK VIEW

01 5 keys to security: know the fundamentals, execute best practices, integrate security into the SDLC, practice data-centricity, and test and monitor continuously.

02 The security landscape has changed to involve more threat access points, and the number of threats and hacks expanding daily.

03 The most effective security techniques combine different approaches and tools throughout the SDLC process, of which testing is integral.

To gather insights on the state of application and data security, we spoke with 18 executives who are involved in application and data security for their clients. Here's who we talked to:

SAM REHMAN, CTO, Arxan
BRIAN HANRAHAN, Product Manager, Avecto
PHILIPP SCHÖNE, Product Manager IAM & API, Axway
BILL LEDINGHAM, CTO, Black Duck
AMIT ASHBEL, Marketing, Checkmarx
JEFF WILLIAMS, CTO and Co-Founder, Contrast Security
TZACH KAUFMAN, CTO and Founder, Covertix
JONATHAN LACOUR, V.P. of Cloud, Dreamhost
ANDERS WALLGREN, CTO, Electric Cloud
ALEXANDER POLYKOV, CTO and Co-Founder, ERPScan
DAN DINNAR, CEO, HexaTier
ALEXEY GRUBAUER, CIO, Jumio
JOHN RIGNEY, CTO, Point3 Security
BOB BRODIE, Partner, SUMOHeavy
JIM HIETALA, V.P. Business Development Security, The Open Group
CHRIS GERVAIS, V.P. Engineering, Threat Stack
PETER SALAMANCA, V.P. of Infrastructure, TriCore Solutions
JAMES E. LEE, EVP and CMO, Waratek

KEY FINDINGS

01 The most important elements of application and data security are: **1) focusing on the fundamentals; 2) identifying best practices, frameworks, and architectures; 3) embedding security in the entire software development lifecycle (SDLC); 4) being data-centric; and 5) testing and monitoring continuously.** The four pillars of security are 1) securing the database to prevent SQL injection; 2) scanning software for sensitive data discovery; 3) actively monitoring the app and the database; and 4) providing dynamic data masking as needed. There is a huge variance in best practices from one manufacturer and operating system to another. 99% of application developers will benefit from application frameworks. Moving security to the left of the SDLC inherently provides visibility across the entire process, providing much-needed insight for developers, engineers, and security professionals.

02 The programming languages and frameworks most frequently mentioned by respondents were **JavaScript, Java, and C++**; however, there were mentions of 28 others along with a couple of companies using 20 and 70 additional languages respectively and two companies using whatever their clients are using.

03 The cybersecurity landscape continues to evolve with **more threats and more access points** thanks to IoT and connections to the cloud. With all of these access points and connections, vulnerabilities and hacks will continue to grow. The focus of the attacks has changed from users, credit cards, and malware to industry specific vectors like oil and gas and retail. Hackers are going after personal identifiable information (PII) for identity theft like passports and social security numbers. The old threats have been automated. Countries and businesses are providing root kits and services to other hackers because there is so much money to be made by the hackers and the companies providing the tools.

04 The most effective security techniques and tools are: **1) a combination of different approaches; 2) a secure SDLC process**

with which testing is integral; and, 3) security baked into the architecture. Companies are identifying security issues by layering static, dynamic, and interactive tests. Fundamental security elements include encryption when data is in transit, at rest, and flowing between data centers. Platforms can serve as the foundational element for authentication, authorization, and other techniques to ensure a strong foundation.

05 **Most real-world problems are being solved in financial services and healthcare** since these are the most highly regulated industries. Solutions revolve around following the best practices like PCI implementation and the OWASP 10. However, there are a lot of companies who are not in highly regulated industries who are putting themselves, and their customers' PII, at risk. Stay current with patches and updates. Reduce mean-time-to-failure with recovery, remediation, and application of the process all taken into consideration.

06 The most common issue our respondents see affecting application and data security is **not taking a holistic view of security as a strategic necessity** as evidenced by lack of knowledge of fundamentals and best practices. Also, companies continue to spend 95% of their security budget on infrastructure and web security versus application security where 90% of attacks are aimed. In addition, companies do not have the security personnel necessary to monitor security and address vulnerabilities and concerns.

07 Virtually all of the respondents have concerns regarding the current state of application and data security. **It's bad and it's going to get worse before it gets better for a number of reasons.** According to Verizon, there are an average of 22.4 serious vulnerabilities in each application they tested. The development of IoT devices are way ahead of processes and best practices needed to create even more secure devices and applications. Too many organizations are not looking at the research and strategies as a first step before buying a tactical solution. The bad guys continue to find vulnerabilities faster than the good guys can fix the problems with nothing meaningful to disrupt the cycle. Government agencies have become quite sophisticated, but so have the bad guys. It's an ongoing "cat and mouse" game with very real implications.

08 The future of application and data security is **automation and algorithms driving artificial intelligence and machine learning**. However, we still need organizations to start looking at security as part of their SDLC and IT strategy and funding it at a sufficient level so the vision can be realized. We will use instrumentation to improve security by orders of magnitude. In the future all software will be instrumented for security all of the time. We will have insight into how an app is operating and automatically take action as a result—automated remediation.

09 Developers need to **think security first and learn and follow best practices for greater career success and longevity**. Get application security training so you know how to build resilient applications. Be aware of threat and design principles, as well as the OWASP 10 and vulnerability databases. Have a good knowledge of frameworks and the security strengths and weaknesses of the frameworks you are using. Monitor the performance of your applications and be aware of unusual or unintended use. There are greater career opportunities for developers and architects with secure coding skills. More skills equate to greater career growth. There are a lot of advantages to being a secure developer and a lot of tools available to understand and learn secure coding.

10 Additional considerations regarding application and data security include:

- **Software security is invisible**. In the marketplace, you get the same price for software regardless of how secure it is. There's no incentive to build secure software. This has to change if we hope to address the problem.
- **Applications are currently working in silos**. Ultimately we'll connect all applications in a safe and secure way just by using a browser. Apps will communicate using agreed upon security protocols.
- There's not a lot of emphasis on protecting data. **How do we secure the data, encrypt access, and scan to know what data resides where?**
- We need to **be aware of how changes to applications threaten the service** and what new vectors of attack will become popular.
- **Privacy is huge**. Credit card data is one thing; however, heart rate monitors, knowing when you're at home or not, and where your car is parked, and for how long, have massive privacy implications that affect peace of mind.
- As we become more agile and cloud based, there are more challenges with changed in cybersecurity, as well as security and development in the cloud. **How does compliance, security, and operations address these challenges?**
- **How is DevOps affecting the security process?** Does it help or hurt? What does it take to make the transition to Dev/Sec/Ops that enables continuous integration and secure integration? Communications between developers, security, and operations becomes critical.
- **How realistic is it to expect developers to write more secure code?** Is over-reliance on the status quo delaying the development and implementation of new security technologies and techniques?
- **Use smaller chunks of data** because it's worth less to hackers.
- **Blockchain is not fine, it's chaos**.
- **How do we go faster securely?** Make security and accelerator to increase speed to market.

TOM SMITH is a Research Analyst at DZone who excels at gathering insights from analytics—both quantitative and qualitative—to drive business results. His passion is sharing information of value to help people succeed. In his spare time, you can find him either eating at Chipotle or working out at the gym.