3 security risks that architecture analysis can resolve

Synopsys Editorial Team
Posted by (https://www.synopsys.com/blogs/software-security/author/synedt/) on Monday, January 25, 2016

Only 50% of application security issues are code-related defects. The other 50% are design-level problems. How to resolve them: with architecture analysis.

Verizon performs an annual assessment of a large sample of breaches and attacks that take place all over the world and analyzes the most common problems and key areas that lead to major attacks. In this article, we discuss three specific security incident patterns from Verizon's report and how architecture analysis assessments (https://www.synopsys.com/software-integrity/software-security-services/software-architecture-design.html) can help organizations detect and prevent these issues earlier in the software development life cycle (SDLC) (https://www.synopsys.com/glossary/what-is-sdlc.html).

Point-of-sale (POS) intrusions

A point-of-sale (POS) intrusion is when an attacker tries to capture payment data by compromising the computers/servers running the POS applications. Such attacks can originate from a social engineering attack (https://www.synopsys.com/glossary/what-is-social-engineering.html) (like a phone call to gain credentials) to a more sophisticated mechanism involving multiple steps. Trends from the past three

years show a constant growth in POS attacks (2013 had 173 (http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf), 2014 had 196, and 2015 had 396 (http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf)).

Commonly, POS intrusions are due to use of weak authentication controls for remote access to systems where sensitive information, like user passwords or credit card details, are stored. For smaller organizations, attackers often conduct direct attacks on the POS system by guessing or brute-forcing the password, possibly because of weak password complexity policies. Attacks on larger organizations often include multiple steps where attackers compromise other systems before targeting the POS.

A major factor in past compromises was use of default credentials, but the recent shift has been toward stolen credentials. Other factors that contribute to the success of these breaches are a general lack of security controls and audit logs in POS systems, insufficient network segmentation, and vulnerabilities in the POS device software.

Architecture analysis assessments can help detect these weaknesses and provide remediation guidance to prevent them from being exploited in a breach. Architecture analysis helps identify weak or missing security controls and is therefore an effective approach to analyze access to POS systems from various perspectives. For example, it can assess the password complexity policy, credential storage, and multifactor authentication controls to determine if they are adequate to prevent these types of attacks on POS systems. The analysis can also identify dependencies on other components and systems to highlight weaknesses that can be exploited if other internal systems have been compromised. This was a common attack vector for large-scale POS breaches, according to the Verizon report.

Architecture analysis identifies not only technical failures but also process-oriented loopholes. As an example, it can analyze if the process for adding or modifying user access must follow a sequence of approvals and verification checks, and whether these are audited to avoid abuse.

Insider threats and privilege misuse

One of the most prominent, and common, security incident patterns is insider threats (https://www.synopsys.com/blogs/software-security/insider-threats-cloud/). Insiders usually have a high degree of trust within their organization and thereby easier access to critical information such as credit card numbers, SSNs, and bank account information. Thus, lack of a centralized data classification and PII inventory, together with inappropriate access control, can easily lead to a disaster.

To perform their duties, some users need elevated privileges from time to time to access the sensitive data stored by the application. However, persistent and unaudited privileged access can lead to an increased risk of abuse by these insiders.

Another risk is that unintended changes or misconfiguration by privileged users of a database could provide sensitive-data access to a malicious end user. The Verizon breach report points out that a majority of insider breaches are carried out by end users, rather than developers or system administrators. Reasons for a deliberate internal attack range from personal financial gain to frustrated employees venting their dissatisfaction by divulging sensitive internal information.

Architecture analysis assessments can help identify the data residing in an application, appropriately classify the data, and assess if the controls in place are sufficient to protect the data. It can further assess the actors (insiders and outsiders) and their privileges to ensure they follow the principle of least privilege and segregation of duties, which helps prevent privilege misuse. Finally, architecture analysis can also help to identify deficiencies in application logging and audit trails, which are important both as a deterrent and as a valuable source of information for a forensic investigation if an insider breach occurs.

Web app attacks

The 2015 Data Breach Investigations Report (DBIR) from Verizon shows that 9.4% of attacks were related to web applications. The causes of these attacks range from lack of two-factor authentication to configuration errors, brute-force attacks, and lack of egress filter on traffic leading to data breaches.

Penetration testing and code review are the primary tools organizations use to identify web app attacks. But you can supplement these assessments with architecture analysis. Architecture analysis reviews assess crucial security controls to prevent applications from being compromised by potential web-related attacks. Some examples of these controls are authentication, authorization, cryptography, input validation, output encoding, auditing/logging, monitoring/alerting, session management, runtime environment verification, and password storage.

The review doesn't have to be limited to the validation of security controls. It can also include configuration issues. A good architecture analysis can point out issues related to security misconfiguration and lack of environment segregation.

Architecture analysis can also play a crucial role in identifying many web app-related vulnerabilities. For instance, two major issues usually identified in applications are SQL injection (SQLi) (https://www.synopsys.com/glossary/what-is-sql-injection.html) and cross-site scripting (XSS)

(https://www.synopsys.com/glossary/what-is-cross-site-scripting.html). A well-defined architecture analysis review can evaluate whether the application employs effective security controls and follows best practices to defend against these and other common attack patterns.

Beyond these standard attack patterns, more advanced architecture analysis reviews can evaluate system-specific attacks and perform dependency analysis to discover vulnerabilities related to the frameworks and components that the application relies on. Keeping an inventory of these and deploying a process that ensures they are kept up to date and regularly patched for security issues goes a long way to counter the opportunistic web attacks that account for three-quarters of all web app compromises analyzed in Verizon's report.

Securing applications earlier in the SDLC

Statistics show that while 50% of security issues are code-related defects, the remaining 50% are design-level problems, which can't be found effectively by code reviews or penetration testing alone. Architecture analysis (https://www.synopsys.com/software-integrity/software-security-services/software-architecture-design.html) can help you detect flaws early in the SDLC by analyzing underlying design principles, architecture, security controls, and processes used to implement the application.

Architecture analysis requires an in-depth understanding of the application architecture. The assessments involve interview sessions with technical team members such as architects, lead developers, and design engineers to gain an understanding of the application design and architecture. This is usually followed by brainstorming exercises to uncover the potential weak points. In addition to identifying the flaws, these assessments can also categorize risks based on the business impact and help organizations prioritize them accordingly.

By deploying architecture analysis, you can find and prevent design-level flaws in your applications and systems before they are exploited by criminal hackers or insiders. We hope you won't be part of the statistics in next year's edition of Verizon's Data Breach Investigations Report.

Find architecture and design defects in your software (https://www.synopsys.com

This post is filed under Security news and research (https://www.synopsys.com/blogs/software-security/category/security-research/).

Synopsys Editorial Team

Posted by
Synopsys Editorial Team

SEE AUTHOR ARCHIVE (https://www.synopsys.com/blogs/software-security/author/synedt)

More from Security news and research

Podcast: The current state of DevOps (https://www.synopsys.com/blogs/software-security/podcast-ep1-current-state-of-devops/)

Synopsys Editorial Team
Posted by (https://www.synopsys.com/blogs/software-security/author/synedt/) on June 26, 2023

Application security best practices (https://www.synopsys.com/blogs/software-security/tag/application-security-best-practices/)

Application security program strategy and planning (https://www.synopsys.com/blogs/software-security/tag/application-security-program/)

DevSecOps (https://www.synopsys.com/blogs/software-security/tag/devsecops/)

Forrester recognizes Synopsys as a Leader in software composition analysis (https://www.synopsys.com/blogs/software-security/forrester-wave-sca/)

Posted by Mike McGuire (https://www.synopsys.com/blogs/software-security/author/mmcguire/) on June 13, 2023

Software composition analysis (https://www.synopsys.com/blogs/software-security/tag/software-composition-analysis/)

Software Integrity Group's products and services (https://www.synopsys.com/blogs/software-security/tag/appsec-product-offering/)

CyRC Vulnerability Advisory: CVE-2023-32353, Apple iTunes local privilege escalation on Windows (https://www.synopsys.com/blogs/software-security/cyrc-vulnerability-

advisory-cve-2023-32353/)

Zeeshan Shaikh
Posted by (https://www.synopsys.com/blogs/software-security/author/zeeshans/) on June 1, 2023

Cybersecurity Research Center (https://www.synopsys.com/blogs/software-security/tag/cybersecurity-research-center/)

Synopsys named in 2023 Fortress Cyber Security Awards (https://www.synopsys.com/blogs/software-security/2023-fortress-cyber-security-award/)

Synopsys Editorial Team
Posted by (https://www.synopsys.com/blogs/software-security/author/synedt/) on May 31, 2023

RELATED TAGS

Software composition analysis (https://www.synopsys.com/blogs/software-security/tag/software-composition-analysis/)

SEE ALL TAGS

(https://twitter.com/synopsys) (https://www.facebook.com/synopsys) (https://www.linkedin.com/company/synopsys) (https://www.youtube.com/user/synopsys) (https://www.instagram.com/synopsys/) (https://www.slideshare.net/synopsys) (https://www.flickr.com/photos/synopsys/) (https://www.synopsys.com/blogs/feed)