One of a CISO's primary responsibilities is to protect their company's important digital assets, which can include corporate intellectual property such as proprietary source code and other patented technology or confidential information. However, because of emerging privacy and regulatory laws and standards, CISOs and data protection officers now also need to protect user data—personally identifiable information (PII), personal health information (PHI), and payment card industry (PCI) data.

These new privacy laws are increasing the restrictions on the use, retention, and geographic residency of user data. This requires many organizations to protect this data and its use both internally as well as with third-party vendors that handle this data. CISOs need to work with their colleagues in data protection, privacy protection, IT infrastructure, compliance, and software development to ensure compliance with these data protection and privacy laws, standards, and guidelines. In addition, the emergence and adoption of hybrid clouds and multicloud services creates new challenges for data security. Other factors—the geographic origin of data, storage location, and user access location points—further complicate what services providers and major cloud infrastructure providers need to do to secure their data.

Consumers are becoming more wary about their personal information and how it is used. The National Conference of State Legislators, citing a report by the Pew Research Center, writes, "More than 80% of Americans say they go online on a daily basis." It adds, " Of those, 28% go online almost constantly and 45% go online several times a day. Consumers are now more aware that businesses, social media sites, and other websites may collect and share their personal information with third parties. They also hear more about security breaches, cyber attacks, and unauthorized sharing of personal information."

Similarly, a survey of 1,000 consumers from the U.S. and the U.K. conducted by Entrust on data privacy showed that "79% of consumers said they're concerned about data privacy, and 64% said that concern has increased in the past 12 months. The top reasons for consumers' heightened concerns were news stories about data breaches and seeing an increase in targeted ads on social media."

The recent surge in remote work has also resulted in increased worker data privacy concerns. "What we found was that roughly two years ago most companies barely had a privacy team; it was tucked away in a legal office," says Robert Waitman, director of data privacy at Cisco. "But with the shift to remote work because of the pandemic, privacy has become more important, mainly because employees were uncomfortable with the privacy of the tools available and the need for companies to provide a safe workplace."

Understanding how application security ties into data and privacy protection is essential. With the digital transformation happening in many industries, organizations

Web applications can serve as a conduit for hackers to gain access to sensitive data. The OWASP Top 10 outlines the 10 most-critical security risk categories for web applications. For example, in a SQL injection attack, hackers try to get access to sensitive data in a database without proper authorization by executing unintended commands through a web input form. Another danger to web applications is sensitive-data exposure. According to Open Web Application Security Project (OWASP), "Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser." Similarly, the OWASP Mobile Top 10 outlines the top risk categories for mobile applications.

The CWE Top 25 is a community-developed list spearheaded by MITRE. This list catalogs the most dangerous software and hardware weaknesses that are often easy to find and exploit, and that can allow cyber attackers to completely take over a system, steal data, or prevent an application from working. The CWE team created the 2020 list by leveraging the common vulnerabilities and exposures (CVE) data in the National Vulnerability Database (NVD), as well as the common vulnerability scoring system (CVSS) scores associated with each CVE. Some of the top 10 weaknesses include both quality issues (e.g., out-of-bounds memory buffer, use after free, out-of-bounds read or write) and security issues (e.g., cross-site scripting, improper input validation, SQLI, cross-site request forgery, and exposure of sensitive information to an unauthorized actor).

The Consortium for Information & Software Quality (CISQ) has coordinated a new OMB standard, the Automated Source Code Data Protection Measure. According to CISQ, the measure is "based on a collection of relevant CWEs that can be used to support enterprise and supply chain needs in protecting data, confidential information, intellectual property, and privacy. These CWEs are currently available for use. This new standard is highly relevant to GDPR, CCPA, and Cybersecurity Maturity Model Certification (CMMC) for controlled unclassified information protection."

The standard seeks to spotlight CWEs that can enable data leakage—those that have CWSS technical impacts that allow unauthorized access to read/modify data. CISQ notes that "Scanning code that will run or is running in enterprises (on systems and devices that process or transmit data) would determine if the systems or devices enable data leakage. If so, then such a scan would reveal if the data protection/privacy controls associated with the process assessment were inadequately implemented."

Static application security testing (SAST) tools along with other AppSec tools (e.g., interactive application security testing [IAST], software composition analysis [SCA], and dynamic application security testing [DAST]) can help development teams automate the identification and remediation of security vulnerabilities and weaknesses in the top categories listed by standards, such as the OWASP Top 10 and CWE Top 25.

Business logic, or application logic, refers to the set of rules that define how an application operates and functions according to a specification. SAST tools can find issues by examining static code, but they often can't easily identify business logic weaknesses—flaws in the design or implementation of an application that allow an attacker to elicit unintended behavior by

S S

0 0)

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle.

For more information, go to www.synopsys.com/software.

Synopsys, Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

Contact us:
U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com