Build Secure Apps in Seven Steps

With over 80%[1] of security breaches involving application vulnerabilities and 46%[2] of security professionals reporting incidents due to insecure applications, Application Security is essential for risk reduction. By integrating security into the Software Development Life Cycle (SDLC) from the start, vulnerabilities decrease, making the process more secure and manageable.

1 Cultivate a Security-Conscious Culture

- Promote a no-blame environment to encourage reporting of security concerns.
- Appoint executive sponsors and security champions to share knowledge and best practices.
- Make security a shared responsibility across all departments.

2 Exercise and Empower Teams

- Provide security exercises and labs to empower development teams.
- Adopt a people-centric approach, focusing on end-users' needs for better security outcomes.
- Align applications with user expectations for higher satisfaction and trust.

3 Balance Innovation and Security

- Conduct cost/benefit analyses to make informed decisions that prioritize both innovation and security.
- Foster a culture of collaboration between innovation and security teams to ensure that new initiatives are developed with security considerations in mind.
- Establish clear guidelines and frameworks for assessing the security implications of new technologies and innovations before implementation.

4 Address Legacy Systems and Tech Debt

- Modernize or replace legacy systems to avoid security gaps.
- Proactively allocate resources to address technical debt.
- Ensure a strong security foundation for new developments.

5 Implement Proactive Security Measures

- Integrate security into the SDLC from the beginning.
- Adopt proactive security measures to prevent breaches and fines.
- Position your organization to effectively adapt to the cyber threat landscape.

6 Avoid Outsourcing Pitfalls

- Prioritize security expertise in vendor selection.
- Conduct thorough due diligence on third-party vendors.
- Stay informed about industry trends and regulatory requirements related to outsourcing security practices to ensure compliance and alignment with best practices.

7 Change Culture Around Security

- Recognize security as a shared obligation across the organization.
- Integrate security from the outset of the development process.
- Invest in security education and foster a security-conscious culture.

Creating secure applications is a continuous journey requiring technical expertise, cultural transformation, and proactive planning. By fostering a security-conscious culture and integrating security measures throughout the development process, organizations can safeguard against cyber threats, ensuring their applications are resilient and trustworthy.

To learn more about strategic development approaches, read our comprehensive guide to application security.

[1] The Continued Threat to Personal Data: Key Factors Behind the 2023 Increase, Professor Stuart E. Madnick, Ph.D., Dec. 2023
[2] Security Outcomes Report, Cisco, 2023

IMMERSIVELABS