axway
business. in motion.

api:first

API SECURITY CHECKLIST

11 ways to guard your enterprise entry points

☐ ONE

Use design patterns. Design patterns that allow for scalability and manageability (like Model-Approach-Controller) separate concerns based on the system's ability to evaluate a request against access-control policy.

☐ TWO

Know and contain your assets. Define and enforce security policy to achieve the same granular control for your APIs as you have for your users.

☐ THREE

Design for malice. Don't naively extend trust. Enforce non-bypassable defensive services (including input validation, content filtering, output encoding and data-sanitization routines) on all data handled by your APIs.

FOUR ☐

Monitor for server-side flaws. Servers hold the keys to the kingdom. Log access requests to all APIs, monitor all access attempts for brute-force and lateral attacks, and employ risk-based access control that adapts to how the application is used.

FIVE ☐

Think mobile and beyond. Centralize security enforcement with an API gateway for authentication and authorization, including enforcement of OAuth protocols and token management.

SIX ☐

Think of sessions, not just APIs. How will you coordinate session timeouts? How will you synchronize identifiers? Three or more full-session lifecycles (generation, propagation, usage, timeout and reinstantiation) must all work together cohesively and in accordance with security policy.

SEVEN ☐

Make security a "no-brainer" for users. Ensure the default mode (or only mode) is the highest level of security the system can achieve, and don't ask users to toggle or upgrade security configurations on their own.

EIGHT ☐

Simplify the developer experience. Prevent performance degradation and DoS, Privilege Escalation and other security issues by setting a default API mode that complies with your enterprise security policy.

NINE ☐

Appoint an API curator. It's a soft-skill — more process than tech — but it can position you to take a strategic role in making the change necessary to ensure a more secure API deployment for your enterprise.

TEN ☐

Be bi-directional. APIs will increasingly have to speak a wide spectrum of different protocols and step into non-traditional roles where servers initiate communications, including notifications, Websockets and SMS.

ELEVEN ☐

Focus on the data. Data: attackers want it, individuals and businesses need it. Focusing on data must be a central tenet of any security architecture program whether the technology is FTP or web or mobile API.

For more information, visit www.axway.com/api-first