Payroll Integrations’ API Security Checklist

PAYROLL INTEGRATIONS
www.payrollintegrations.com

Ensure you have a team that knows what it is doing.

Whether in-house or via a partnership that provides enterprise-grade protection, every organization of any size today utilizing APIs and handling sensitive data (so, virtually every organization that isn’t still using punch cards) needs a cybersecurity professional or team of professionals who are well-qualified and attentive. Period.

Ensure your team has a ‘seat at the table.’

Once you invest in a team, let them have a say in major leadership and management decisions with implications for the systems they manage; a lack of communication and coordination between leadership and security teams is a major complicating factor in costly breaches.

Set proactive security measures and policies.

With the right security team and right executive posture toward security prioritization and feedback, your organization should be well-positioned to put in place policies and procedures that take a proactive stance that anticipates threats rather than merely reacts to them (by which point, it’s too late).

Engage in regular and extensive API Security Testing.

One of major API security concepts not delved into above is all of the time, energy, effort, and data science poured each year into testing. Simulated penetration scenarios and regular, automated scanning helps to identify those potential vulnerabilities before they become actual nightmares.

Engage in regular and (very) extensive cybersecurity training for regular personnel.

It is worth repeating: human error is the number one threat vector. It is only with the right tools to help anticipate and prevent human errors as well as extensive training within an organizational culture of trust and individual accountability that you can mitigate this risk factor.

Always use an API Gateway.

An API Gateway is the first roadblock in ensuring that not just any individual or entity online can send and receive data from your APIs. This, together with the next item on our checklist, is how you ensure you are authenticating and authorizing.

Always use tokens for access, and centralize authorization.

Tokens should be issued from an internal server central to your API infrastructure. Processes such as OAuth can ensure this complex procedure is centralized and done properly. You don’t want each of your API Gateways to do this themselves, because differing levels of data access (and from differing sources) can be involved; centralization streamlines, focusing your most vulnerable areas.

Ensure proper logging, monitoring, validation & encoding.

Failure to engage thoroughly and correctly in any one of these processes creates vulnerabilities across your threat surface that smart threat actors rely on you to neglect to access your sensitive data.

Secure all your APIs thoroughly, even if internal.

No API should go unsecured (which is to say, without due diligence to the items in this checklist), not even when it seems like no threat actor could access it externally.

Set intelligent quotas ready to throttle traffic

TO PREVENT VULNERABILITIES

Beyond even the need for proper log integrity at the encoding and validation level, throttling is a precautionary safeguard designed to help prevent attacks meant to overwhelm your system, compromise your gateway, or altogether deny functionality for critical API systems.

The latter is found in Denial-of-Service attacks, which can be financially devastating.