5 FIRST STEPS

CISOs CAN TAKE TO IMPROVE API SECURITY

By a Special Committee of Ping Identity's CISO Advisory Council, including Chris Gullett, VP of Information Security for Allegiant Air; Diane Ball, CISO for BCBS Tennessee; Karl Mattson, CISO for City National Bank; and Michael Strong, CISO for GCI.

To say that API security is an increasing concern for security leaders is an understatement. Influenced by broad-reaching factors (like mobile initiatives) and industry-specific ones (like open banking), the API footprints of organizations across the spectrum are expanding at a rapid rate with no signs of slowing down.

Not only are today's CISOs managing a growing number of internal APIs, but they must also navigate the complexities of exposing external-facing APIs and consuming third-party ones. Certainly, there are a lot of moving parts to keep track of. But there are also steps CISOs can take now to improve the governance and cybersecurity of APIs.

#1

KNOW WHAT APIs ARE IN USE. As APIs proliferate, it's increasingly difficult to know about all of the APIs in an organization. In many cases, various groups have been developing APIs in silos with little central control or input from security teams. Exacerbating this, APIs aren't always included in the release workflows designed to build security into software application releases. Nor do they have their own established processes, leaving them documented only within the purview of each API management tool, of which there may be several.

The first step is to know exactly what APIs are in use in your organization today. Gain access to your API catalog, and talk with development teams throughout your organization to understand what they've developed and what's in the pipeline. You can also investigate the use of scanning tools to identify the internal and third-party/vendor APIs present in your environment.

#2

GAIN VISIBILITY INTO API ACTIVITY. Given the challenges with identifying what APIs are in use, it stands to reason that there's a lack of visibility into API traffic. While picking up anomalous traffic for web activities—like an FTP transfer, for example—is straightforward, identifying anomalies in API traffic and activity isn't as cut and dried. Without the ability to distinguish good traffic from bad, you face a classic you-don't-know-what-you-don't-know conundrum.

But you don't need to settle for the status quo. There are new tools entering the market that provide deep and unified API traffic visibility—even in multi-vendor, hybrid and API gateway environments. They will also sort out good and abnormal behaviors on API infrastructures. When you gain the ability to identify abnormal use, you gain the ability to defend yourself by blocking and reporting attacks.

#3

ASSEMBLE THE RIGHT RESOURCES. Because API security is relatively new, most organizations don't have clearly defined job roles to manage it. The functional roles typically involved are tasked with either security or development, but not both. The security concerns of APIs are not in the wheelhouse of traditional security professionals who are accustomed to defending the network, not exposing it. On the flip side, security also isn't the primary responsibility of developers, who are incentivized to quickly release new features and functionality, not to ensure security.

Some organizations are hunting for those rare security professionals with development backgrounds, while others are looking for greenhorn developers that they can shape into security professionals. There is no one-size-fits-all answer, so we suggest that you choose one and refine as needed until you find and identify the right solution for your organization.

#4

ASSIGN OWNERSHIP OF API SECURITY. Because security and development are typically discrete roles, the question of who owns API security doesn't always produce a clear answer. The challenges around resources and ownership are inextricably intertwined and without a clear path forward, many security leaders are left searching for what feels like unicorns.

Similar to the challenges of assembling the right team, there is no one right answer. The key is that both security and development need to play a role, and both will need the support of the other group. As long as both teams are working jointly on the problem, you're on the right track.

#5

ADDRESS API SECURITY BY DESIGN. API security today is more often an afterthought than an intentional design consideration. And our CISO Council agrees that this is the crux of the problem. While security measures such as authentication, authorization and detection of anomalous behavior are clearly needed, they're not enough on their own.

Security must be addressed during the development process. Similar to the software development life cycle, API development needs to be a continuous cycle and include thorough testing requirements. Growing API security threats alone are worthy of prioritizing security by design, but what's really needed is a fundamental shift from DevOps to DevSecOps, where security is incorporated at every step of the development process.

A good rule of thumb is to treat all internal APIs as if they were externally facing. And considering the threat models for APIs during the development process will help eliminate the re-work caused by discovering vulnerabilities only at the end of development, or worse yet after the API has gone out into production.

YOU HAVE TO START SOMEWHERE

Most organizations are still finding their way in this new environment, and API security is arguably a moving target. Most agree that the desired end state is Zero Trust, where transactions are always authenticated, authorized and tracked, and there's a high level of assurance about the identities of those making requests. For starters, though, security leaders can begin implementing these five recommendations to realize immediate improvements in their API security.

ABOUT PING'S CISO ADVISORY COUNCIL: Made up of CISOs from industry leaders across a range of industries, this group provides insight to Ping Identity on security, privacy and compliance challenges facing the global enterprises we serve. It helps inform Ping's strategic vision, product roadmap and go-to-market strategies. Interested in getting involved? Please reach out to your account executive to learn more.

#3445 | 09.05.2019 | v01