RSA® Conference 2019

BETTER.

Peer2Peer

What’s Your Externally Facing API and Service Attack Surface?

P2P3-W15: What’s Your Externally Facing API and Service Attack Surface?

Mark Willis Director, Software Security, Aetna

What's Your Externally Facing API and Service Attack Surface?

In discussions with security professionals over the past few years, not one person has ever disagreed that the threat of unknown externally facing APIs and Services poses a major security risk to their organization – a blind spot that needs to be addressed and solved. This P2P dove into this topic feet first and challenged our participants to share their opinions about the subject, as well as tools and techniques that might help all of us get just a bit closer to solving this problem.

Understanding the Blind Spot of Externally Facing APIs and Services

Right out of the gate, we all agreed that the blind spot related to not fully knowing our externally facing attack surface related to our APIs and Services presented a huge problem - and how we all came to this conclusion was very interesting.

While each idea was well received by the larger group, many different answers as to why we believed this issue to be so important emerged. One participant noted that lack of standardization and overall governance for API and Service development was the reason this issue existed in the first place and should have been in place years ago.

Another participant talked about the overall lack of best practices, as well as how the lack of security controls helps exacerbate this problem.

On the flip side, some participant talked about how developers and architects are rewarded in their organizations for doing the right thing by properly documenting and inventorying their APIs and Services. Methods such as a report card with good grades or conversely, “public flogging” of those who drop the ball were presented as ways to drive awareness to senior leaders as to the importance of this issue.

How to Identify and Secure our APIs and Services

Perhaps the most interesting takeaway of the session was that everyone agreed that somehow, someway, each organization needed to get serious about their inventory of APIs and Services to begin the journey of implementing tools and techniques to identify what should be known and what will be. We also agreed that there isn't a silver bullet to solve this issue – be it in the cloud or on prem and that an approach of security, business, IT, and architecture working together to appreciate and address this issue is long overdue.

Some attendees suggested that you needed to have an API Gateway to inventory the “known” or “what is being used” APIs and Services. Such a gateway would allow application security testers to test the full attack surface as part of a secure software development lifecycle.

Additionally, the group agreed that an inventory would help the organization avoid legal liability as the organization would ultimately be held liable for any data breach attributed to unknown APIs or Services – a strong case that could be made to senior executives as to why this is an urgent matter.

The topic of inventorying and ensuring our third party APIs and Services are secure came up as part of our discussion. The discussion around involvement of third party risk management to hold our vendors accountable for secure APIs and Services was very popular as well.

Exploring Tools and Techniques to help us solve this problem

While we all agreed that an inventory is a must, the session then turned to, what types of tools and techniques are we using within our organizations that can be shared with the larger session audience.

One attendee was taking a very hard line, or what we ended up calling an, “Old School Use or Lose It” approach when it came to APIs and Services – whereby he was on a mission to block access and push to remove anything that wasn’t being used within a given time frame. Those in his organization who needed such APIs and Services would eventually speak up and he would know that the APIs or Services were legitimate.

Without getting into names of actual tools, a few attendees in the session talked about periodic external scanning of their environment to identify any “New” APIs or Services that might pop up. However, the issue of “old” or “unknown” APIs and Services still presented a challenge that no one really felt as if they had a solid tool or technique to solve.

Other attendees discussed how they use large databases or repositories to tell them what is out there, while others were grepping for “old names” within source code and systems and studying web proxy logs, both inbound and outbound for clues as to better understanding their architecture.

Lastly, the idea of working closely with our network teams to perform a “DNS Dumpster Dive” was well received as a way to study our externally facing environment for clues as to APIs and Services being called.