Your Attack Surface is not just a Buzzword

June 23, 2023

Sr. Security Solutions Architect

Wil has focused much of his career working with CISOs and their organizations to solve complex problems and manage risk. He is passionate about innovation, and believes cyber risk is a business conversation. A cybersecurity strategist with 24+ years experience having worked across most business lines from security operations, architecture, product management, R&D, go-to-market, and C-Level leadership.

Submitted by Wil Klusovsky on 23, Jun 2023
Your Attack Surface is not just a Buzzword

Our industry is swimming in a sea of acronyms and "marketing speak." Some firm, product company, or industry expert will come up with a new (ish) idea. Then everyone else takes that idea and spins it to fit their story. It’s like viral videos on social media; there’s a lot to keep up with, and eventually you get tired of hearing about it and dismiss it. Your attack surface is not a buzzword. It’s real, and you want to pay attention to it. But how?

Why is attack surface management a new idea? Cybersecurity has been like watching a tennis match. We focus on endpoint security, then network, then back and forth. Over time, what falls into those two categories evolves, but one thing is constant; we focus on our own house. Vendors build products to protect our internal systems. We assess our internal processes. More recently, we have come to realize that we need to pay attention to the outside. There are things we can’t see or don’t know about. Threat actors are coming from the outside after all. We want to keep an eye on what we can, so we are best prepared to defend. New tech, services, and this

viewpoint are what created attack surface management.

The attack surface is about looking at that external exposure as a hacker would. This goes beyond giving a "white hat" your external IPs as scope for a penetration test. There are complex tools and intelligence available today to find your company beyond the web servers and access you have set up. The reconnaissance phase can find misconfigurations in your cloud presence allowing access you don’t want. Decommissioned systems that are not so decommissioned. Rogue systems or the remains of a breach that wasn’t cleaned up so well. These all become viable attack vectors that you don’t know about. You believed that your house was secure. You locked the doors and barred the windows, but you didn’t know there was a hole in the roof or that someone had your key.

Good management of this goes beyond identifying your external view. An attacker is also going to look for useful data. This could be on the dark web, Google Drives, or GitHub. As security professionals, we know one can piece bits of information together to solve a puzzle. A file with log-on credentials makes it super easy. A data set with personal information (PII) will increase the success rate of spear phishing. Finding code your business uses gives insider information on how you operate. This data is already exposed. Implementing controls to stop it from happening again is not going to undo this. Cleanup is one part. More importantly, it’s looking at that data and understanding what an attacker can do with it. Now you have that external view. You know what information could be used. So how do you leverage this knowledge?

Context and threat modeling help in validating where the real risk is. Are those rogue systems we discovered able to access other systems? Can that misconfiguration be exploited to an attacker’s benefit? When the testing shows there is real risk, you can do something to fix it. If there is no risk, it’s not a priority to deal with it. Good cyber hygiene will take place, but you want your limited resources working on real impacts to the business first. You need validation.

A good attack surface management program will not only identify your attack surface but also test and confirm the risk areas within it. Discovery is an important part, but the optimal value comes from it being a continuous process. Having the attacker's view continually, provides real risk management.

It's not only about seeing the map. You want to know what routes to take, where the short cuts are, where construction is, and where the bad parts of town are. Attack

surface management is a continual road trip. You want real-time traffic and construction information. You want to know your arrival time and where the gas stations are. Simply having a static paper map isn’t enough.