Cyber-risks & Liabilities

Courtesy of The Risk Hub Ltd

Attack Surface Management Explained

Attack surfaces refer to the total possible entry points (also known as attack vectors) for unauthorised access into any system. The recent increase in remote and hybrid work combined with the shift to the cloud and widespread implementation of software-as-a-service (SaaS) applications have made attack surfaces increasingly large, complex and difficult to defend against cyber-attacks.

As a result, organisations face the challenge of continuously monitoring their attack surfaces to identify, block and respond to threats as quickly as possible. That's where attack surface management (ASM) can help. This article provides more information on ASM and explains how it works.

What Is ASM?

ASM involves continuously discovering and monitoring potential attack vectors, including any pathway or method a hacker may use to gain access to a company's data or network to facilitate a cyber-attack.

A company's attack surface is constantly changing and generally includes four main surfaces:

1. On-premises assets, such as hardware and servers
2. Cloud assets, such as workloads, cloud-hosted databases or SaaS applications
3. External assets, such as an online service provided by an external vendor that may be integrated with the company's network or is used to store its data
4. Subsidiary networks shared by more than one organisation

How ASM Works

ASM aims to provide a company's security team with a current and complete inventory of exposed assets to accelerate responses to threats and vulnerabilities that put the company at risk.

ASM includes four automated core processes that must be carried out continuously as the size of the digital attack surface is constantly in flux. These processes include the following:

1. **Asset discovery—**Asset discovery is a continuous process that scans for potential entry points for a cyber-attack. These assets may include subsidiary assets, third-party or vendor assets, unknown or non-inventoried assets, known assets, or malicious or rogue assets.
2. **Classification and prioritisation—**Assets are analysed and prioritised by the likelihood that hackers could use them as a target. They're inventoried by their connections to other assets in the IT infrastructure, IP address, identity

riskhub
the business resilience people

and ownership. Assets are also analysed for exposures such as missing patches, coding errors and potential attacks, including spreading ransomware or malware. Each vulnerable asset is assigned a risk score or security rating.

3. **Remediation—**Potential vulnerabilities are remediated in order of priority. It may be necessary to apply software or operating system patches, debug application codes or use stronger data encryption. Previously unknown assets may need new security standards, or it may be necessary to integrate subsidiary assets in the company's cyber-security strategy.
4. **Monitoring—**Security risks change whenever a new asset is deployed or existing assets are used in new ways. The network and its inventoried assets are continuously monitored for potential vulnerabilities to allow ASM to find attack vectors in real time. Security teams can then act quickly to neutralise the threat.

Conclusion

A well-designed ASM strategy not only helps protect an organisation from cyber-attacks—it is also a practice frequently required by underwriters to obtain cyber-insurance. For additional cyber-risk management information and insurance solutions to help protect your company from the financial effects of a cyber-attack, contact us today.

This Cyber Risks & Liabilities document is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact a legal or insurance professional for appropriate advice. Design © 2023 Zywave, Inc. All rights reserved.