**Attack Surface Management In Cyber Security**

The onset of the digital era has initiated a lot of opportunities including for businesses and enterprises. From reading books to using mobile phones, everything is just a click away. But the more we connect to digital assets, the more is the chance of vulnerabilities of our confidential data. This data is protected by Cyber security. In technical terms, Cyber security is the body of technology, processes, and practices designed to prevent unauthorized use of data, tampering of data, and protection of data from hackers.

Attack surface refers to some of the different points in the network environment where the unauthorized user, the attacker can extract or tamper with the data. It is the sum of all the vulnerabilities that the data can face. Attack surfaces can be of various types like software attack surfaces, physical attack surfaces, etc. It is necessary to have a minimal attack surface as the smaller the attack surface, the better for the organization in terms of risk and exploitation. For this, attack surface management is used.

**Need for Attack Surface Management**

Today’s attackers have grown extra cautious and take tons of effort to understand where the attack should be most promising. Thus, it is very important to manage this issue effectively.

Attack surface management is a procedure of finding out the organization’s assets that are under threat, thereby classifying their security. With the digital revolution worldwide, the organization’s assets have become a strengthened base for cyber-attacks which are difficult to trace. This management is done in two ways, one where the internal assets of the organization are taken into consideration, and the other one is the external asset that is revealed to the internet.

**How the Attack surface Management platform meets the needs**

The management platforms are used to identify unknown assets and investigate threats. This platform enables many use cases to be conducted. By discovering unknown assets, the vulnerability risk program is extended, threats are found and eliminated, and allow cloud and IoT expansion. By investigating threats, we can scale out threat hunting, automate security operations, and have a faster incident response.

Some other key points that are associated with attack surface management are:

* Surface must be checked regularly as with the increase of paired devices, not only does the risk of cyber attack increase but also the chances of misconfigurations and exposed data is a matter of concern.
* Context is very important as without proper information like IP address, device name, the status of usage, etc, it becomes very difficult to give attention to the asset’s well-being from attackers.
* The risks needing immediate lookout should be prioritized. For that, apart from a business context, points like attacker priority, and exploitation ease must be taken care of.
* After setting the priorities, the management work can be initiated as per the priority. Giving the business context and the information builds trust and lets the work happen smoothly.

**References**

1. <https://www.techtarget.com/searchsecurity/tip/What-is-attack-surface-management-and-why-is-it-necessary#:~:text=Attack%20surface%20management%20is%20the,tasks%20from%20an%20attacker's%20perspective>.
2. <https://www.kaspersky.co.in/resource-center/definitions/what-is-cyber-security>
3. <https://www.techtarget.com/whatis/definition/attack-surface>
4. <https://www.fortinet.com/resources/cyberglossary/attack-surface>
5. <https://www.upguard.com/blog/attack-surface-management>
6. <https://informer.io/resources/what-is-attack-surface-management>
7. <https://www.firecompass.com/attack-surface-management/>
8. <https://www.techtarget.com/searchsecurity/definition/cybersecurity>