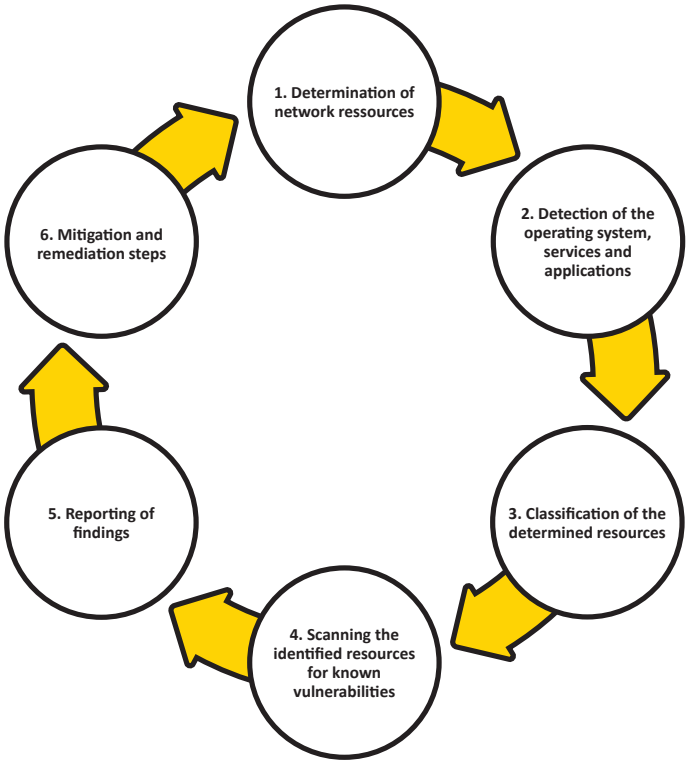
Targeted vulnerability elimination with Vulnerability Management as a Service.

On their own, the results from a vulnerability scan are usually not very meaningful. That‘s why UMB‘s comprehensive reporting engine compares your results with information from countless other scans. This allows UMB to alert you to and respond to serious vulnerabilities at an early stage.

Another benefit is that you can define the frequency of the scans (weekly, monthly) yourself and optimally adjust them to your needs. In the event of a suspected vulnerability, you can, of course, order additional scans on short notice. Our approach to vulnerability management:



Recommendations for action:

Vulnerability detection becomes vulnerability management when a specific action, such as mitigation or remediation, follows the detection of a vulnerability. Specific recommended actions from an expert help to reduce vulnerability mitigation time and to ensure the correct and most effective assignment of your remediation resources to reduce risk.

Different scan options

External Scan: An attacker‘s perspective
With the external scanning service, you gain an attacker‘s perspective. The predefined network resources (assets) accessible from the Internet will be scanned.

Agent-based Scan: Scan devices everywhere
By deploying an agent on your devices, you can keep informed about their vulnerability situation, apps deployed, and overall risks independently of their location.

Onsite Scan: Security across the network
To ensure that security does not end at the perimeter, Onsite Scan focuses on your local area network (LAN). Depending on the desired depth of the scan, single or multiple sensors are placed on your network. This allows the system to detect vulnerabilities that attackers could use to move laterally across the network. Scan results are combined with the central reporting engine and remote scan results.

Discovery Scan: Find assets on your network
The focus of the discovery scan is to find network resources. You define the network areas, UMB will scan them systematically. As a result, you receive a determination of the operating system and the network services: As part of the operating system detection, UMB shows you which ports are accessible per service, for which applications a corresponding port is accessible or open, and which operating systems are used.

Option: Automated patch-management - seamless defense
UMB's automated patch-management module facilitates the timely distribution of security patches across your systems. This minimizes the risk of attacks exploiting known vulnerabilities and ensures that your systems are consistently up to date with the latest security measures.

Service components:

- External Scan
- Agent-based Scan
- Onsite Scan
- Discovery Scan
- Recommendation for action
- Remediation coordination
- Monthly reporting

Your advantages:

- You will learn about the vulnerabilities of your systems and always have the threat situation of your infrastructure under control.
- You will be informed about configuration errors as well as newly installed or unauthorized systems, also known as shadow IT.
- You will receive vulnerability classifications and recommendations for action from experienced specialists.
- You will be informed at an early stage about new vulnerabilities that pose high risks.
- You can simplify and accelerate vulnerability remediation for all your IT assets.

Sounds interesting? Contact us!

We are happy to answer you questions about Vulnerability Management as a Service und more.

Contact

Markus Kaegi
Team Leader Strategic Sales Consulting
markus.kaegi@umb.ch
+41 58 510 16 98
www.umb.ch