Vulnerability Management

Identify and remediate vulnerabilities in a timely and controlled manner.

more security. usd
Cyber Defense
Approved Security

As IT infrastructures grow more complex, threats grow increasingly critical, making it all the more important to be able to identify system vulnerabilities as quickly as possible and remediate them in a controlled manner. We assist you in designing and implementing a professional vulnerability management process, including applicable tools, for your company.

Our Phase Model

Prepare

During the preparation phase, together with you we determine what requirements have to be met by your vulnerability management (VM) process, taking your security policies, compliance requirements, contracts and service level agreements into account. We then determine what types of vulnerabilities can be found. We differentiate between internal and external scans. External scans mimic the perspective of a malicious individual carrying out an attack from the internet. Therefore, they reveal vulnerabilities that are visible from outside the network. Internal scans, however, mimic the perspective of an attacker from inside the network and therefore reveal vulnerabilities that are visible within the network.

Discover

During this phase, we conduct a comprehensive analysis of your current setup. We identify your IT assets and determine network perimeters.

Organize

We perform risk assessments of your IT assets and networks and classify them. The results from this phase will impact the designated scan intervals.

Assess

During this phase, scan properties and testing parameters are configured and the intervals in which vulnerability scans will be performed are determined. We then configure your scans accordingly.

Report

We define your vulnerability scan reports' templates according to your specifications, allowing you to work as efficiently as possible with the results.

Remediate

The remediation phase is intended for establishing processes and measures for rectifying identified vulnerabilities. Our experts are happy to assist you with the remediation process. We analyse vulnerabilities and verify, for example, whether patches or workarounds are available, or whether the configuration can be hardened. Additionally, we identify threats and offer to perform code reviews for you. We furthermore establish and/or implement policy management processes (Ticketing).

Verify

In this phase, we verify whether measures for remediating vulnerabilities have been implemented. We conduct rescans and validate the results accordingly.

We offer an all-round service.

Do you also require assistance with operational tasks? We do not only implement the process. If you wish, we also provide operational support, either on site or via remote access. We furthermore train your employees in how to handle the tools.

This product sheet will be valid until a new version is released. *Product sheet creation date: 28/11/2018*

usd AG
Frankfurter Straße 233, Haus C1
63263 Neu-Isenburg, Germany | www.usd.de

Phone: +49 6102 8631-190 | E-mail: sales@usd.de
PGP or S/MIME for secure communication