Incident and Vulnerability Handling II

Vulnerability Handling

Vulnerability

Nach ISO 27005 ist eine **Schwachstelle** eine Schwäche eines Vermögenswerts oder einer Gruppe von Vermögenswerten, die von einer oder mehreren Cyber-Bedrohungen ausgenutzt werden kann.

Hierbei ist ein Vermögenswert (auch Asset) alles, was für die Organisation, ihren Geschäftsbetrieb und dessen Kontinuität von Wert ist, einschließlich Informationsressourcen, die den Auftrag der Organisation unterstützen.

Was verursacht Vulnerabilities?

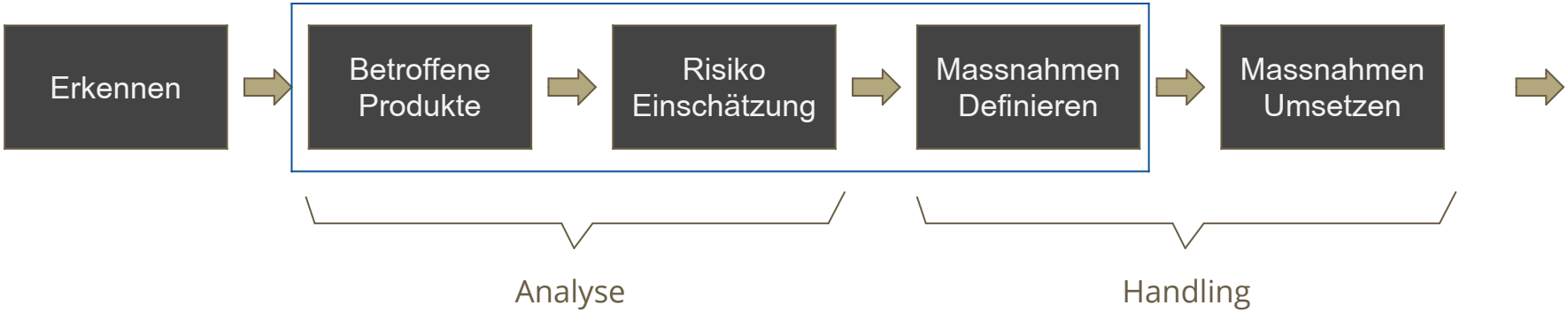
Es gibt viele Ursachen für Schwachstellen, darunter::

- Komplexität
- Connectivity
- Schwaches Password Management
- Betriebssystemmängel
- Unkontrollierten Internetzugang
- Software Bugs
- Unkontrollierter (User) Input
- etc

CWE

Was ist Vulnerability Management?

Vulnerability Management ist eine regelmäßige Praxis der Identifizierung, Klassifizierung, Behebung und Entschärfung von Sicherheitsschwachstellen. Zu den wesentlichen Elementen des Schwachstellenmanagements gehören die **Erkennung** von Schwachstellen, die **Bewertung** von Schwachstellen und die **Behebung** der Risiken aus Schwachstellen.



Ziel

Eine Schwachstelle durchläuft einen “vulnerability assessment process”

Aufgaben

Identify/detect vulnerabilities: Analyse von Netzwerk-Scans, Pen-Test-Ergebnissen, Firewall-Protokollen und Ergebnissen von Schwachstellen-Scans, um Anomalien zu finden, die darauf hindeuten, dass ein Cyber-Angriff eine Schwachstelle ausnutzen könnte. (https://vuldb.com/?recent.202105)
Verify vulnerabilities to affected components and existing controls : Entscheiden, ob die ermittelte Schwachstelle ausgenutzt werden könnte, und Einstufung des Schweregrades der Schwachstelle, um den Grad des Risikos zu verstehen (Configuration Repositories/Databases)
Mitigate Vulnerabilities: Nehmen Sie einen potentiellen Angriff auf Basis der Schwachstelle die Wirksamkeit.
Remediate Vulnerabilities: Aktualisieren Sie nach Möglichkeit die betroffene Software oder Hardware bzw. entfernen Sie die Schwachstelle.

Methods of vulnerability detection include:

- Vulnerability Scanning (tool basierend)
- **Vulnerability Monitoring (feed basierend)**
- Penetration Testing
- “Reports by Security Researcher” oder ähnlich

Deliverables

Regelmäßiger Vulnerability Report

Ziel

Vorbeugende Information der Kunden über alle bekannten Bedrohungen und Schwachstellen

Sie müssen die gesetzlichen Anforderungen erfüllen.

Inhalt

Beschreibung der Bedrohung/Schwachstelle

Betroffene Produkte und Komponenten

Ausnutzungs-Bedingungen (exploit conditions) als CVSS-Attribut

Entschärfungs- und Kontrollmaßnahmen

Risikoabschätzung

https://www.first.org/cvss/calculator/3.0

CVE-2021-22114 NVD MITRE CIRCL	VMware	Spring-integration-zip	1.0.0, 1.0.1, 1.0.2, 1.0.3	Incomplete Fix CVE-2018-1263	Privilege Escalation	4.6	Rated	—	2021-03-03 01:23:43	2021-03-03 10:28:55	2021-03-01
CVE-2021-21320 NVD MITRE CIRCL	—	matrix-react-sdk	3.0, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, 3.8, 3.9, 3.10, 3.11, 3.12, 3.13, 3.14	—	Weak Authentication	2.6	Rated	—	2021-03-03 01:23:42	2021-03-03 09:53:34	2021-03-02
CVE-2021-27803 NVD MITRE CIRCL	—	wpa_supplicant	2.0, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9	P2P Provision Discovery Request Handler	Denial of Service	4.0	Rated	—	2021-02-28 01:23:02	2021-03-03 10:23:11	2021-02-26
CVE-2020-27618 NVD MITRE CIRCL	GNU	C Library	2.0, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11, 2.12, 2.13, 2.14, 2.15, 2.16, 2.17, 2.18, 2.19, 2.20, 2.21, 2.22, 2.23, 2.24, 2.25, 2.26, 2.27, 2.28, 2.29, 2.30, 2.31, 2.32	Mutlibyte Handler	Denial of Service	4.3	Rated	—	2021-02-28 01:22:57	2021-03-03 10:19:13	2021-02-26
CVE-2021-24113 NVD MITRE CIRCL	Microsoft	Edge	—	—	Security Bypass	5.4	Rated	—	2021-02-27 01:23:43	2021-03-03 09:52:13	2021-02-25
CVE-2021-23979 NVD MITRE CIRCL	Mozilla	Firefox	85.x	—	Remote Code Execution	6.3	Rated	—	2021-02-27 01:23:29	2021-03-03 09:58:28	2021-02-26
CVE-2021-23978 NVD MITRE CIRCL	Mozilla	Firefox, Firefox ESR, Thunderbird	—	—	Remote Code Execution	6.3	Rated	—	2021-02-27 01:23:29	2021-03-03 09:58:11	2021-02-26
CVE-2021-23977 NVD MITRE CIRCL	Mozilla	Firefox	85.x	—	Information Disclosure	2.5	Rated	—	2021-02-27 01:23:29	2021-03-03 09:51:20	2021-02-26
CVE-2021-23976 NVD MITRE CIRCL	Mozilla	Firefox	85.x	Fullscreen Handler	Privilege Escalation	6.3	Rated	—	2021-02-27 01:23:28	2021-03-03 09:56:36	2021-02-26
CVE-2021-23975 NVD MITRE CIRCL	Mozilla	Firefox	85.x	Developer Page	Denial of Service	3.3	Rated	—	2021-02-27 01:23:28	2021-03-03 09:46:21	2021-02-26
CVE-2021-23974 NVD MITRE CIRCL	Mozilla	Firefox	85.x	DOMParser API	Cross Site Scripting	4.3	Rated	—	2021-02-27 01:23:28	2021-03-03 09:46:33	2021-02-26
CVE-2021-23973 NVD MITRE CIRCL	Mozilla	Firefox, Firefox ESR, Thunderbird	—	Decoding Handler	Privilege Escalation	4.3	Rated	—	2021-02-27 01:23:27	2021-03-03 09:56:34	2021-02-26

(Vulnerability) Responsible Disclosure*

Ziel

Informieren Sie Kunden präventiv über kritische oder öffentlichkeitsbezogene Angriffsflächen und vermeiden Sie Aufwand durch die Beantwortung individueller Fragen/Beschwerden.
Sie müssen die gesetzlichen Anforderungen erfüllen.

Inhalt

Threat/Vulnerability Beschreibung
Betroffene Produkte und Komponenten
Exploit Bedingungen
“Mitigating and controlling measures”
Risiko Einschätzung
Technische Details
Nächste Schritte

*Verantwortliche Offenlegung

Vulnerability-& Threat Advisory

Ziel

Information der Kunden zur Vorbeugung bekannter kritischer oder öffentlichkeits relevanter Bedrohungen und Schwachstellen

Sie müssen die gesetzlichen Anforderungen erfüllen.

Inhalt

Threat/Vulnerability Beschreibung

Betroffene Produkte und Komponenten

Exploit Bedingungen

“Mitigating and controlling measures”

Risiko Einschätzung

Technische Details

Nächste Schritte

Hands On

Liste der relevanten Schwachstellen/Bedrohungen

CVE-2023-23415 (ICMP)
CVE-2019-12262 VxWorks
ESXiArgs (CVE-2021-21974)
Log4Shell
Ripple20 (Set of CVEs 2020)
Bluekeep [CVE-2019-0708]
Sweyntooth (Set of CVEs 2019)
NAME:WRECK (Set of CVEs 2021)
SMBGhost [CVE-2020-0796]
WannaCry [MS17-010]
(Solarwinds 2020-12-09)
Pulse Connect Secure Vulnerabilities [CVE-2021-22893]
Microsoft IoT Warning (Set of CVEs 2021)
OpenSSL [CVE-2021-3450]
FragAttacks (short for FRagmentation and AGgregation Attacks)

Übung: Erstellen eines “Vulnerability-& Threat Advisory”

Log4Shell Vulnerabilities*

Axeda Vulnerabilities**

*https://nvd.nist.gov/vuln/detail/CVE-2021-44228

**https://www.ptc.com/en/support/article/CS363561

References

ISO/IEC 27035-2
Information technology — Security techniques — Information security incident management — Part 2:Guidelines to plan and prepare for incident response

ISO/IEC 30111
Information technology — Security techniques — Vulnerability handling processes

CVE
Common Vulnerability Enumeration
https://www.cve.org/

CWE
Common Weakness Enumeration
https://cwe.mitre.org/

CVSSv3
https://www.first.org/cvss/specification-document

The DFIR Report
https://thedfirreport.com/

Mentimeter

https://www.menti.com/alnd7zx3tzzn