Checkliste

SYSTEM-HÄRTUNG

Jedes IT-System, ob Software, Netzwerk oder Server/Client Gerät kann gehärtet werden.

Härtung ist weit mehr als das Entziehen von „Admin Rechten“ oder die Sperrung eines USB-Slots auf einem Laptop.

Eher bezieht sich dies auf die richtige Konfiguration des jeweiligen Systems (Betriebssystem, Datenbank, Netzwerkgeräte, Applikation). Große Applikationen wie SAP oder Oracle haben mehr als 1.000 Systemparameter, die das Verhalten der Instanz beim Start bestimmen und von denen – geschätzt – etwa 10 % sicherheitsrelevant sind.

Also setzt Härtung die genaue Kenntnis jedes einzelnen Parameters voraus. Da dies unmöglich ist, empfehlen wir den Fokus auf die bekannten Schwachstellen zu legen – gemeldet von den Herstellern oder unabhängigen Organisationen. Wie man diese einsehen kann, ist im Folgenden beschrieben.

Härtung ist oft wichtiger als die Kenntnis von Schwachstellen, da es darum geht, die Ausbreitung von Schadsoftware einzudämmen und nicht darum, ein Eindringen unmöglich zu machen.

Die Wahrscheinlichkeit eines Eindringens ist selbst bei den besten Schutzmaßnahmen hoch, daher geht es vielmehr darum, den Schaden zu begrenzen und einzudämmen.

STIG

Die von der DoD Cyber Exchange herausgegebenen Normen - veröffentlicht in Cyber Exchange Public - sind die einzige wirkliche Norm bzw. Dokumentation zur „**Härtung**“ von Systemen.

„Härtung“ ist z.B. in **MDS-2 SAHD** (vor)geschrieben.

Jedes einzelne System/Hersteller (Nutanix, Redhat, vmware, …) kommt in der „DISA-Norm Library“, mit einer Reihe von Empfehlungen wie man ihr System härten kann (häufig über Konfigurationsparameter), vor.

Diese sind pro System/Technologie in **STIGs** beschrieben.

STIGs steht für: Security **T**echnical **I**mplementation **G**uides

Dort sind die Maßnahmen nach Priorität in **High/Medium/Low** kategorisiert.

+49 (0)621 867510 info@cairo.ag www.cairo.ag Hermsheimer Straße 3 68163 Mannheim

Die STIGS sind pro Hersteller, Modell und Release für sehr viele Hard- und Softwarekomponenten hier im Detail beschrieben: https://stigviewer.com/

oder hier direkt vom Hersteller am Beispiel VMware: Suche nach „Security Configuration“:

https://www.vmware.com/docs/vmware-vsphere-security-configuration-guide-archive

Natürlich halten sich die Hersteller mit Ihren Aussagen hier bedeckt, aber die Durchsicht des STIG-Viewer ist ein erster wichtige Schritt.

Maßnahme: Durchsicht und Prüfung alle Parameter der Priorität „High“ für alle genutzten Systeme.

ÜBERBLICK HÄRTUNGSMAßNAHMEN

Die wichtigsten Härtungsmaßnahmen sind:

Härtungsbereich	Härtungsmaßnahme
Systeme	STIG pro System umsetzen, weitere wie M365 Tenant-Härtung durchführen
Netzwerk	VLAN einführen, Management Netz, Backup-Netz, usw…
Netzwerk (sehr kritische Systeme)	Mikrosegmentierung durchführen
Netzwerk: Zweite Firewall	Gem. der BSI „P-A-P“ Regel mit unterschiedlicher FW von versch. Herstellern
Zugriff auf Daten	Benutzer und Rechte auf das Minimum reduzieren (Least Privilege), GPO analysieren
Zugriff auf Dateien	File Server Berechtigungen prüfen
Zugriff auf Dateien	Microsoft Teams Rechte analysieren
Benutzer	Auto-LogOff am Client einstellen, Kein Admin Account
Benutzer	Auto-LogOff am Mobile einstellen
Benutzer	Zentralen Kennwort Manager einführen
Harte Datensicherungen	3-2-1 Backup etablieren

Achtung: Härtungsmaßnahmen können auf die Nutzung und den Betrieb einen deutlich negativen Effekt haben und sollten daher mit viel Erfahrung durchgeführt werden.

+49 (0)621 867510 info@cairo.ag www.cairo.ag Hermsheimer Straße 3 68163 Mannheim