medbo | 93042 Regensburg

Geschäftsbereich
Wirtschaft und Finanzen
Direktor Konrad Kastner

Jürgen Schmalzbauer
Fon +49 (0) 941/941-1783

juergen.schmalzbauer@medbo.de
Az.: 505-3.41
Datum 04.10.2023

medbo Netzwerk Grundlagen

Inhalt

Allgemein

Jeder Standort der medbo ist mittel eigenem Core Switch versorgt. Diese sind in einem homogenen Netzwerkplan medbo-weit eindeutig erkennbar.

Das Netzwerk erstreckt sich über sieben Standorte, die durch eigene Subnetze voneinander getrennt erreichbar sind.

Standort	Kurzname	IP Netzsegment
Regensburg	BKR	10.0.0.0 /16
Parsberg	BKP	10.20.0.0/16
Wöllershof	BKW	10.30.0.0/16
Weiden	WEN	10.40.0.0/16
Cham	CHA	10.50.0.0/16
MVZ Rgsb	MVR	10.60.0.0/16
Parsberg II	PAR	10.70.0.0/16
Amberg	AMB	10.80.0.0/16
MVZ Cham	MVC	10.90.0.0/16
MVZ Roding	ROD	10.95.0.0/16

Netzsegmente

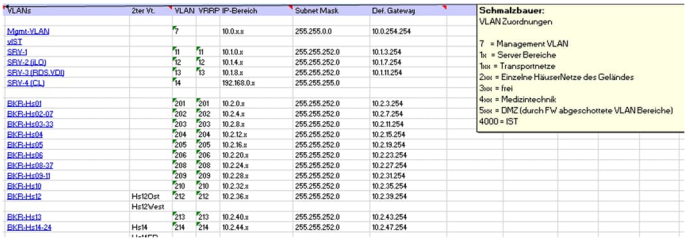
An jedem Standort gibt es verschiedenste Virtuelle Netzwerke (VLAN) je nach deren Notwendigkeit und Anforderungen der Nutzer/Funktionsstell. Eine Aufteilung in VLANs ist aus Gründen der Performance und der Sicherheit notwendig. Es soll keine IP Netze geben, in denen mehr als 500 Rechner eingetragen sind.

Auf Grund deren darin enthaltenen Endgeräten, werden manche VLAN von den Anderen durch eine externe Firewall abgeschottet. Die Regelwerke werden auf Grund der Notwendigkeit der Netze dementsprechend restriktiv vergeben um:

1. Die Endgeräte in dem VLAN vom medbo Netz getrennt zu halten

2. Den Zugriff auf andere Netze zu unterbinden.

Dennoch müssen diese Systeme zur Überwachung und Kontrolle erreichbar von den Managementsystemen erreichbar sein.



VLANs	2ter Vl.	VLAN	VRRP	IP-Bereich	Subnet Mask	Def. Gateway
Mgmt-VLAN		7		10.0.x.x	255.255.0.0	10.0.254.254
vIST						
SRV-1		11	11	10.1.0.x	255.255.252.0	10.1.3.254
SRV-2 (ILO)		12	12	10.1.4.x	255.255.252.0	10.1.7.254
SRV-3 (RDS,VDI)		13	13	10.1.8.x	255.255.252.0	10.1.11.254
SRV-4 (CL)		14		192.168.0.x	255.255.255.0	
BKP-Hs01		201	201	10.2.0.x	255.255.252.0	10.2.3.254
BKP-Hs02-07		202	202	10.2.4.x	255.255.252.0	10.2.7.254
BKP-Hs03-10		203	203	10.2.8.x	255.255.252.0	10.2.11.254
BKP-Hs04		204	204	10.2.12.x	255.255.252.0	10.2.15.254
BKP-Hs05		205	205	10.2.16.x	255.255.252.0	10.2.19.254
BKP-Hs06		206	206	10.2.20.x	255.255.252.0	10.2.23.254
BKP-Hs06-37		208	208	10.2.24.x	255.255.252.0	10.2.27.254
BKP-Hs09-11		209	209	10.2.28.x	255.255.252.0	10.2.31.254
BKP-Hs10		210	210	10.2.32.x	255.255.252.0	10.2.35.254
BKP-Hs12	Hs12Ost Hs12West	212	212	10.2.36.x	255.255.252.0	10.2.39.254
BKP-Hs13		213	213	10.2.40.x	255.255.252.0	10.2.43.254
BKP-Hs14-24	Hs14	214	214	10.2.44.x	255.255.252.0	10.2.47.254

Schmalzbauer:
VLAN Zuordnungen

7 = Management VLAN
1xx = Server Bereiche
1xxx = Transportnetze
2xxx = Einzelne HäuserNetze des Geländes
3xxx = frei
4xxx = Medizintechnik
5xxx = DMZ (durch FW abgeschottete VLAN Bereiche)
4000 = IST

Netzmanagement

Alle Aktiven Netzwerkkomponenten und Server werden mittels Simple Network Management Protokoll (SNMP) zentral gemonitored und überwacht. Dabei werden die Aktivitäten jeglicher Switche periodisch abgefragt um in einem Performance Chart gelistet zu werden.

Alle kritischen Ereignisse werden zu dem Monitoring Tool mittels SNMP Trap gesendet, welches diese auswertet und je nach SLA per E-Mail oder SMS die entsprechenden Teams informiert. Als Beispiel sei hier ein Netzwerk Loop, oder Broadcaststürme genannt.

Des Weiteren werden auch die Server und Medizin Systeme in die Überwachung aufgenommen, um hier auch deren Gesundheitszustand zu protokollieren und im Warnfall die dementsprechenden Teams über ein ggf. anstehendes Ereignis (z.B. Füllstände von HDD, Speicherüberlauf, …) zu informieren.

Switch Konfigurationen

Die Switche werden auf Grund einer zentralen Vorlage konfiguriert. Neben den bei der medbo üblichen „Shortest Path Bridging“ (SPB) Technologie sind des weiteren „Loop Prevention“, „Storm Control“ neben der zentralen RADIUS Server Anbindung über NAC zu nennen.

Das Switch Sample File wird zentral vorgehalten und fortwährend nach den Neuerungen angepasst.

Firewall

Jeder Standort wird von einer eigenen Firewall (je nach Standort auch Cluster) abgesichert gegenüber dem Internet. Das bedeutet das jeder Standort für den Zugriff auf das Internet über einen „Local Brackout“ verfügt. Generell werden aus dem medbo Netzwerk hin zum Internet nur die Port 80 (http) und 443 (https) freigeschaltet. DNS, NTP Dienste werden zentral von einem Domänencontroller, der in der Firewall das Regelwerk besitzt dies mit dem Internet abzugleichen.

Der über die Firewall geleitet Verkehr wird mittels „Deep Packet Inspection“ durch ein IDS / IPS geleitet und dort analysiert, womöglich bei Einbruchserkennung geblockt.

Alle Firewallsysteme werden von einem Zentralen Controll Center verwaltet. Dieses sammelt auch die Log Files der einzelnen Systeme zusammen.

Auf Grund der Sicherheitsthematik werden die Firewallsystem von einem externen Partner gemonitored, der auch ein zus. Alerting betreibt. Neben den aktuellen Vorkommnissen werden durch die Fa. Monats Reports generiert, die den Sicherheitszustand des kompletten Systems wiederspiegelt.

VPN

Mit ausgewählten Partnern und anderen Einrichtungen gibt es VPN Verbindungen. Diese terminieren immer auf der Firewall um die Verbindungpunkte zu fixieren.

Einige wenige Mitarbeiten haben einen Telearbeitsantrag, der es ermöglich, das nur diese Mitarbeiter, über einen durch Zertifikate und Benutzeridentifizierung abgesicherten Zugriff auf das LAN zu erhalten. Dieser Zugriff unterliegt der permanenten Kontrolle durch die

Network Access Controll

Auf Grund der Absicherung des Netzes wird ein NAC System aufgebaut. Dies stellt sicher, dass die Endgeräte, die sich am Netzwerk anstecken, auch Endgeräte der medbo sind.

Medizingeräte, Technische Überwachungssystem, werden automatisch in ihr VLAN verschoben, so dass diese Geräte immer in der gewünschten Umgebung eingebunden sind! Eine Integration in den Virenschutz ist angedacht, befindet sich derzeit noch in der Planungsphase. Damit soll sichergestellt werden, das ungepatchte System in ein Quarantäne VLAN zur Aktualisierung verschoben werden.

E-Mail

Das Zentrale System zur E-Mailspeicherung ist ein Exchange System. Dieses speichert alle E-Mails, Adressen, Kalender und Notizen der Nutzer. Von extern ist das System mittel VPN Tunnel zum retarus Dienstleister angebunden. Das heißt wir haben kein System, das direkt am Internet hängt. Jegliche E-Mails werden über retarus angenommen bzw. versendet.
Eingehende E-Mails werden durch verschiedenste SPAM Techniken und Virenkiller geprüft.

Ausgehender E-Mailverkehr, kann nur über den Exchange Server stattfinden, der ebenfalls nur Zugriff via MAPI und bei Druckern explizit deren IP Adresse und einer Benutzer Authentifizierung vorsieht. Es muss gewährleistet sein, das jeglicher Verkehr nachvollzogen und nachgewiesen werden kann.

Virenschutz

Jeder Server und Client, der am medbo Netz teilnimmt, ist mit einem aktuellen Virenschutz, der am zentralen System verwaltet und überwacht wird, versehen. Somit gibt es einen Zweifachschutz von Server und Firewall System.

Über den Virenschutz gibt es ein eigenes Dokument, da von Herrn Storm bearbeitet wurde.

Personal Firewall System

Jeder Client PC, als auch Systeme von medizinischen Verfahren werden mit einer „Personal Firewall“ versehen, um den Grundschutz zu erhöhen. Die Verkehrsverbindungen der einzelnen Endgeräte, werden in Verfahren zusammengefasst, um hier alle unnötigen Verbindungen einzuschränken.

Medizinische Verfahren

Diese werden, sofern es sich anbietet in einzelnen VLAN getrennt, oder durch dezentrale Sicherung mittels Personal Firewall vom restlichen Netzwerk „getrennt“.
Dabei wird das Verfahren an sich nicht beeinträchtigt, sondern in der Sicherheit gestärkt.

Windows Dateiausführungsverhinderung

Windows Domänenmitglieder, werden mittels Gruppenrichtlinien zentral gesteuert, um die „Data Execution Prevention“ aktiv zu schalten.
Somit wird verhindert, das ggf. durch den Virenschutz nicht erkannte Programme nicht auf Speicherbereiche zugreifen, auf die sie keine Berechtigung haben. Diese Regeln gelten sowohl für den Client, als auch für die Server.

PKI

Um Rechner und Server eindeutig identifizieren zu können werden Rechner Zertifikate ausgestellt. Diese werden zentral verwaltet. Diese werden auch genutzt um die Verbindung zwischen den Client und Server zu verschlüsseln.

Neben den Zertifikaten, die für die Rechner ausgestellt werden, gibt es auch Benutzerzertifikate, mit denen wir Software signieren um diese gesichert ausführen zu können. Somit wird ein einschleusen von Fremdsoftware auf Server erheblich erschwert.

Alle über das Intern in der DMZ erreichbaren Server werden mittel offiziellen Zertifikaten ausgerollt.

Reporting

Alle Subsysteme liefern ausgewählte Reports, die deren Zustand und Tätigkeiten wiederspiegeln. Die Wöchentlich / Monatlich generierten Reports werden durch die jeweilige Teamleitung abgearbeitet. Im Problemfall wird daraus ein Ticket generiert und dem Fachbereich zur Nachkontrolle übergeben.

Jürgen Schmalzbauer

cn=Schmalzbauer Jürgen,
email=Juergen.Schmalzbauer@medbo.de
2023.10.04 12:04:25 +02'00'