Netzplan-Steckbrief

„Zeigen Sie mir Ihren Netzplan“ ist Standardfrage Nummer zwei jedes IR-Teams – davon hängt ab, wie sich ein Angreifer bewegen konnte und wo sich Isolationsgrenzen ziehen lassen. In der Realität existiert oft nur ein veralteter Visio-Plan auf dem (verschlüsselten) Fileserver. Diese Vorlage erzwingt die handhabbare Minimal-Version: Segmente, Übergänge, Internet-Breakouts, Standortkopplungen.

Warum dieses Dokument?

Ohne Segmentübersicht keine Isolationsentscheidung: Was kann getrennt werden, und was fällt dann aus? Der Steckbrief beantwortet das, bevor das IR-Team stundenlang Switches nachverfolgen muss.

Wann brauchen Sie es?

In Stunde 1 bei der Eindämmung (zusammen mit der Isolations-Matrix IR-15) und danach bei der Rekonstruktion der Angriffswege.

Wo aufbewahren?

VERTRAULICH: Ein Netzplan ist für Angreifer eine Schatzkarte. Nie unverschlüsselt digital im normalen Netz – nur Ausdruck im Tresor + zweiter Brandabschnitt.

In vier Schritten zum Notfall-Netzplan

1. **Segmente listen** – VLAN, IP-Bereich, Zweck, Inhalt
2. **Übergänge markieren** – welche Firewall verbindet welche Segmente
3. **Außenverbindungen** – Breakouts, VPN, Standleitungen, Fernwartung Dritter
4. **Skizze zeichnen** – Handzeichnung genügt – Raster-Blatt am Ende

Beispiel Muster Maschinenbau: 6 Segmente (Clients, Server, OT Halle 1+2, DMZ, Gäste-WLAN, Azure via S2S-VPN), zwei Internet-Breakouts (Augsburg + Werk Leipzig) – und rot markiert: die Fernwartungs-VPNs zweier Maschinenbauer in die OT.

So sieht ein ausgefüllter Eintrag aus

BEISPIEL – Muster Maschinenbau GmbH, Augsburg (fiktiv)

Segment	VLAN / IP	Zweck	Übergänge	Isolierbar? Wie?	Folgen der Isolation
Clients	VLAN 10 · 10.10.0.0/16	Arbeitsplätze beide Standorte	→ Server via FW-01	ja: Regelgruppe „Clients-Out“ deaktivieren	kein Zugriff auf ERP/Mail, Produktion läuft
OT Halle 1+2	192.168.50.0/24	CNC-Steuerungen, Leitstand	→ Server via FW-01	ja: FW-Regel #240 ODER Patchfeld B, Ports 12–16 ziehen	keine Auftragsübertragung an CNC; Produktion läuft lokal ca. 4 h weiter

⚠ **Fernwartungszugänge Dritter sind der häufigste Initial-Access-Pfad.** Tragen Sie jede Außenverbindung vollständig ein – besonders Dienstleister-VPNs in Server- und OT-Segmente. Wer sie trennen kann und wie, muss hier stehen, nicht im Kopf eines einzelnen Admins.

Halbjährliche Prüfung: ☐ Segmente aktuell ☐ Außenverbindungen vollständig ☐ Skizze erneuert
Geprüft am: _____ von: _____

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

UNTERNEHMEN	STAND / VERSION	VERANTWORTLICH	ORT DER OFFLINE-KOPIE	NÄCHSTE PRÜFUNG

NETZSEGMENTE – EINE ZEILE PRO SEGMENT

Segment-Name	VLAN-ID / IP-Bereich (CIDR)	Zweck / was steht drin	Übergänge zu welchen Segmenten (über welche Firewall?)	Isolierbar?	Wie? (Regel, Port, Stecker)	Folgen der Isolation (was fällt aus?)
Clients				☐ ja ☐ nein		
Server				☐ ja ☐ nein		
OT / Produktion				☐ ja ☐ nein		
DMZ				☐ ja ☐ nein		
Gäste-WLAN				☐ ja ☐ nein		
				☐ ja ☐ nein		
				☐ ja ☐ nein		
				☐ ja ☐ nein		

Vorbelegte Segment-Namen bei Bedarf durchstreichen und anpassen – wichtig ist, dass kein Segment fehlt (auch Gäste, Kameras, Telefonie, Gebäudetechnik).

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112

AUSSENVERBINDUNGEN – ALLES, WAS DAS NETZ MIT DER WELT VERBINDET

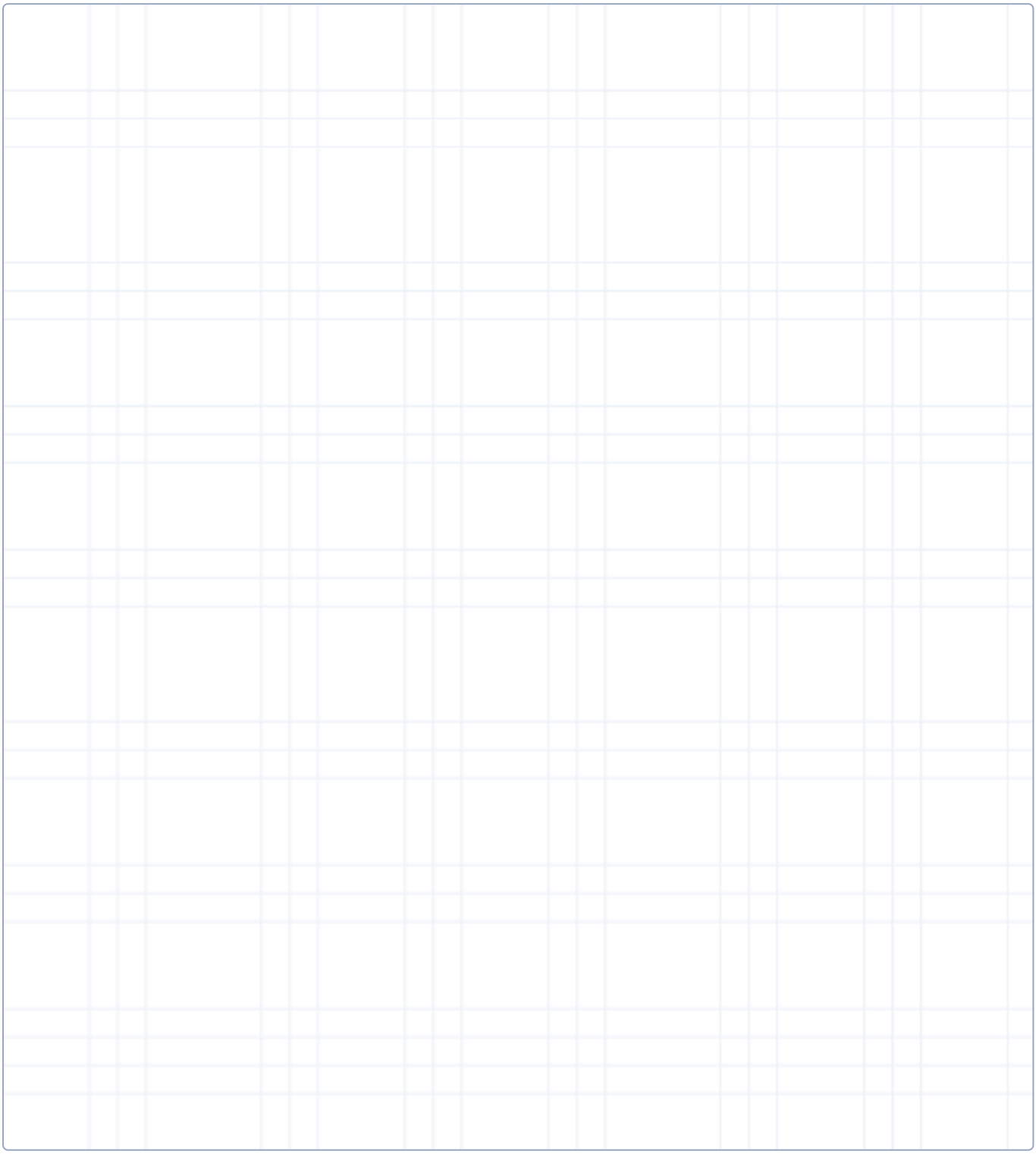
Verbindung	Endpunkt / Gegenstelle	Gerät (Firewall/Router, Modell, Standort)	Wer kann sie trennen – und wie?	Fernwartungszugänge Dritter darüber?
Internet-Breakout 1				☐ nein ☐ ja:
Internet-Breakout 2				☐ nein ☐ ja:
S2S-VPN (Cloud/Werk)				☐ nein ☐ ja:
Client-VPN				☐ nein ☐ ja:
MPLS / Standortkopplung				☐ nein ☐ ja:
Standleitung Partner				☐ nein ☐ ja:
				☐ nein ☐ ja:
				☐ nein ☐ ja:
				☐ nein ☐ ja:

Tipp aus der Einsatzpraxis: Für jede Verbindung muss die Antwort auf „Wer kann sie trennen – und wie?“ ohne Rückfrage funktionieren: Name, Gerät, Regel oder Stecker. „Der Dienstleister macht das“ zählt nur mit 24/7-Nummer in IR-01.

NOTIZEN

NETZSKIZZE – HANDZEICHNUNG GENÜGT

Segment · Firewall / Übergang · Internet / extern · VPN / Fernwartung Dritter (Dienstleister-Name dazuschreiben!)



Skizzieren Sie: alle Segmente als Kästen, dazwischen die Firewalls/Übergänge, oben die Internet-Breakouts und Cloud-Anbindungen, gestrichelt jede Fernwartung von extern. Datum an die Skizze – ein alter Plan ist gefährlicher als keiner.

Im Ernstfall – Argos IR-Hotline 24/7
+49 89 45 24 24-112