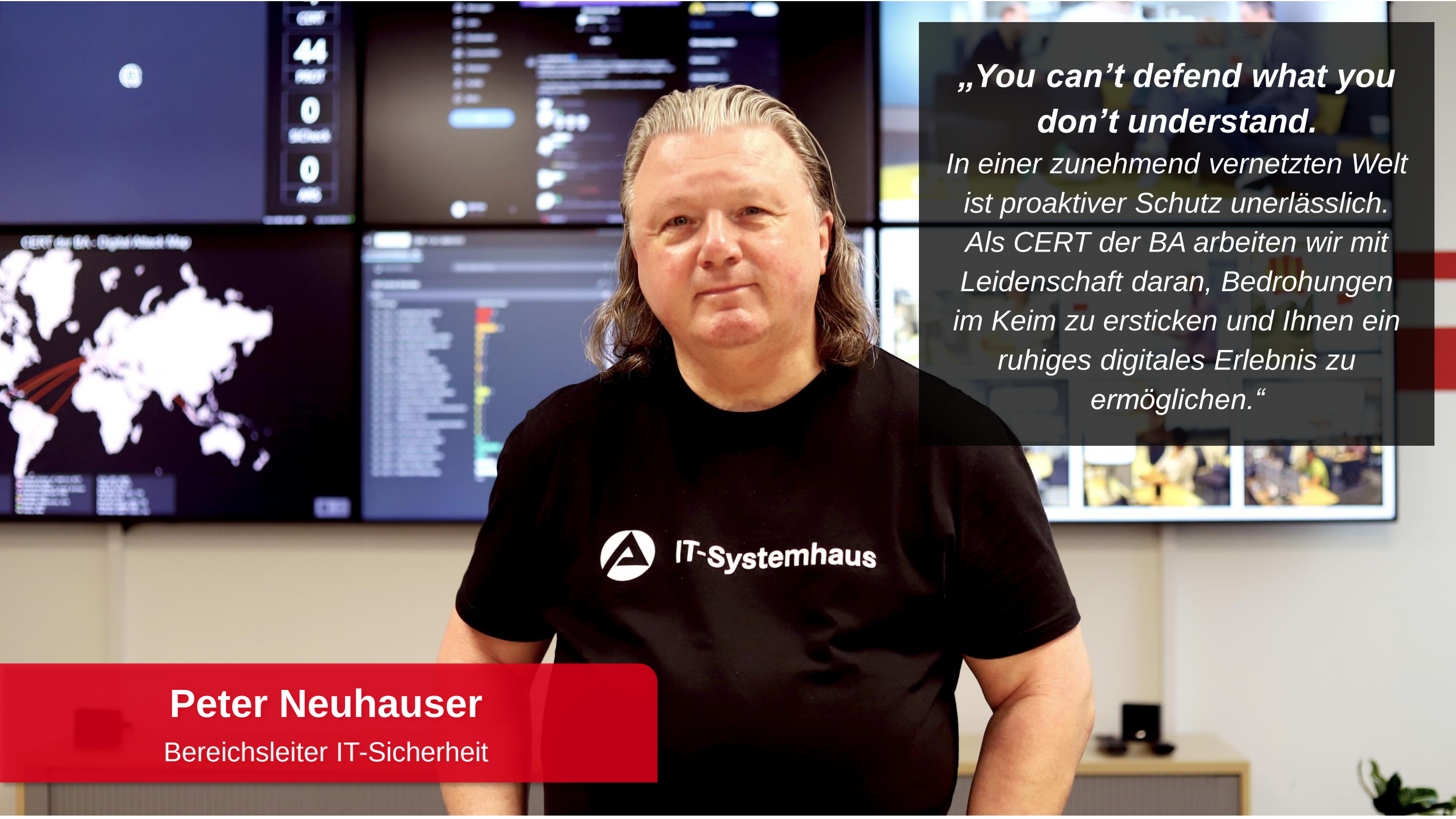
Von der Festung in die Wolke

IT-Security im Wandel



„You can’t defend what you don’t understand.

In einer zunehmend vernetzten Welt ist proaktiver Schutz unerlässlich. Als CERT der BA arbeiten wir mit Leidenschaft daran, Bedrohungen im Keim zu ersticken und Ihnen ein ruhiges digitales Erlebnis zu ermöglichen.“

Peter Neuhauser

Bereichsleiter IT-Sicherheit

Die Präsidentin des Bundesamts für Sicherheit in der Informationstechnik bewertet die Cybersicherheitslage in Deutschland als besorgniserregend

> Wir haben Angriffe rund um die Uhr. Und das nicht nur auf deutsche Behörden, sondern auch auf Industrieunternehmen. [...] Wir haben ein großes Rauschen. Ganz viele Angriffe, die täglich stattfinden. Viele können wir abwehren. Aber die, die mir Sorgen machen, sind natürlich die, die durchkommen.

Claudia Plattner
Präsidentin des Bundesamts für Sicherheit in der Informationstechnik (BSI)
am 12. Dezember 2024 in „Neugier genügt“ des WDRs

Als größte Bundesbehörde Europas verarbeitet die BA unzählige Daten von Bürgerinnen und Bürgern und ist daher ein attraktives Ziel für Cyberkriminelle

> 57 Milliarden Euro
jährliche Gesamtausgaben

5,25 Millionen
Leistungsempfänger*innen

10 Millionen
Kindergeldempfänger*innen

Leistungserbringung

3,23 Mrd. Euro
für konjunkturelles Kurzarbeitergeld

16,53 Mrd. Euro
für Arbeitslosengeldzahlungen

47,92 Mrd. Euro
für Kindergeldzahlungen

Online-Serviceangebot

4,5 Mio.
tägliche Blockungen durch Firewalls

344 Tsd. Downloads
der Kunden-App „BA-mobil“

Alle 67 Services
sind OZG-konform digitalisiert

Die BA ist **Betreiberin Kritischer Infrastrukturen** in den **Rechtskreisen SGB II und SGB III** und unterliegt daher den gesetzlichen Anforderungen des **§ 8a des BSI-Gesetzes**.
Dieser definiert Vorgaben für die Sicherheit in der IT Kritischer Infrastrukturen.

Welche Daten werden bei uns gespeichert und welchen Impact hat ein Ausfall (durch einen Cyberangriff)

Sozialdaten

Personenbeziehbare Daten von Kunden und Geschäftspartnern (Namen, Anschrift, Telefon, E-Mail, Bankverbindung, Lebensläufe ...)

Gesundheitsdaten

Ärztliche Gutachten, Betriebspsychologische Gutachten, ...

Zeugenschutzfälle

Im Einzelfall

Mitarbeiterdaten

Personenbeziehbare Daten aller Mitarbeitenden

Ausschreibungsunterlagen

Verdingungsunterlagen, Bewertung von Angeboten, Verträge ...

Imageverlust

Verlust der Reputation bei Bekanntwerden von Ausfällen der IT durch erfolgreiche Cyberangriffe

Datenschutzvorfall

Meldepflicht bei Datenschutzvorfällen bei der zuständigen Datenschutzstelle (BfDI)

Sicherheitsvorfall

Als Kritische Infrastruktur sind Sicherheitsvorfälle je nach Kategorie meldepflichtig und gefährden die Zertifizierung

Verlust von Intellectual Property

Insbesondere beim Verlust von Mitarbeiterdaten bzw. Ausschreibungsunterlagen geraten ggf. Firmengeheimnisse in fremde Hände

Sozialer Frieden

Bei Ausfall der Zahlungsverkehrsplattform (KRITIS-relevant) ist der soziale Friede im Land nachhaltig gefährdet

Wir müssen uns vor den größten Bedrohungen schützen und unsere Widerstandsfähigkeit stärken

DDoS

Durch Überlastungsangriffe droht ein Ausfall des Online-Angebots und der dazugehörigen IT-Infrastruktur.

Phishing und Identitätsdiebstahl

Opfer sollen zur Herausgabe sensibler Informationen bewegt werden. In Folge droht eine Infektion mit Mal- oder Ransomware.

Malware (Ransomware)

Schadprogramme die schädliche Operationen ausführen oder andere Programme dazu befähigen.

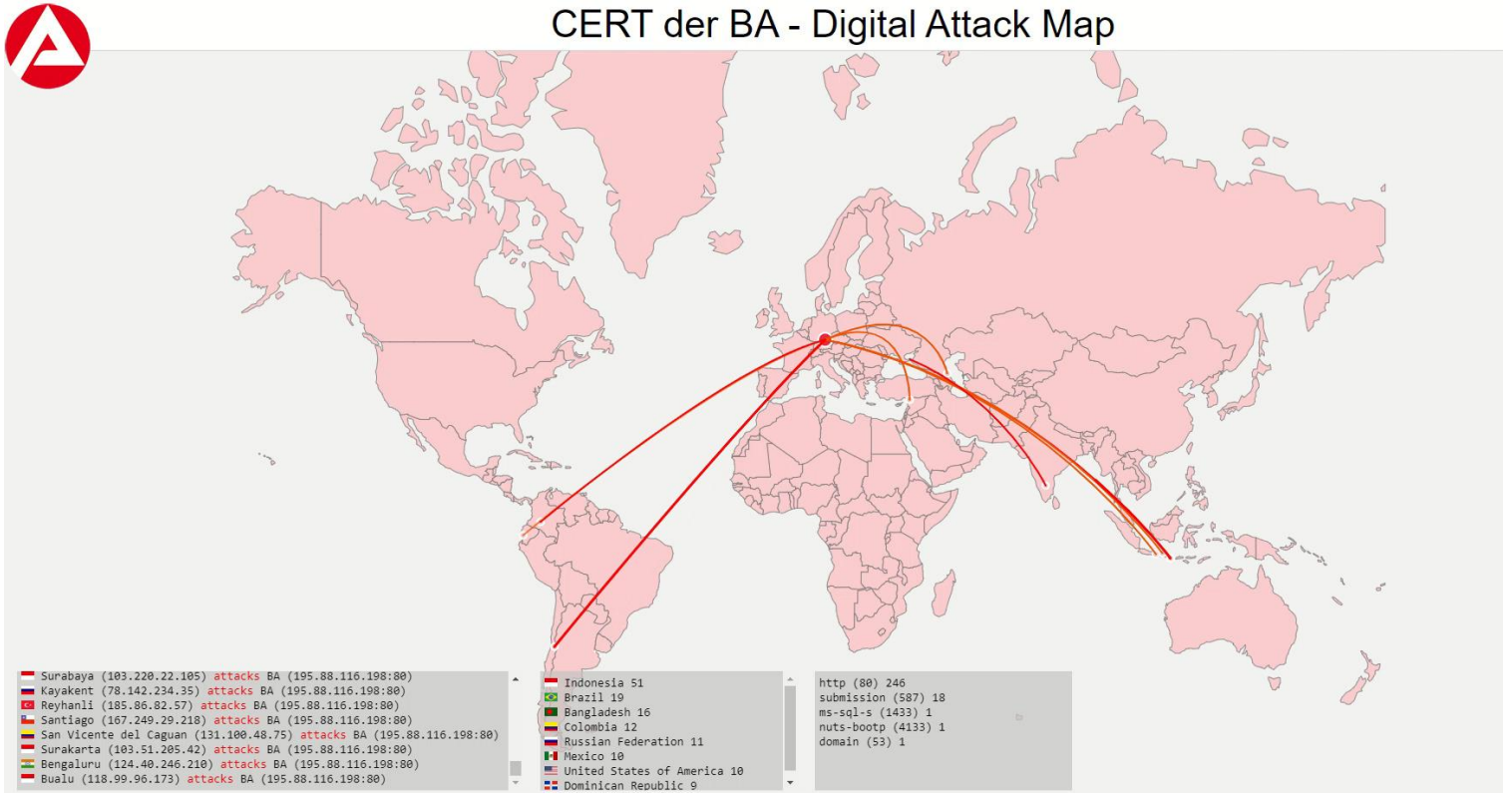
Supply Chain Angriffe

Schwachstellen in der Lieferkette werden gezielt ausgenutzt, um bösartige oder kompromittierte Komponenten einzuschleusen.

Schwachstellen

Schwachstellen in Kaufsoftware und zunehmend in Open Source Bibliotheken werden von Angreifern ausgenutzt

Digital Attack Map



In Zahlen: Ein „normaler“ Arbeitstag des Computer Emergency Response Teams (CERT) der BA

1.000.000 SPAM-Mails werden geblockt

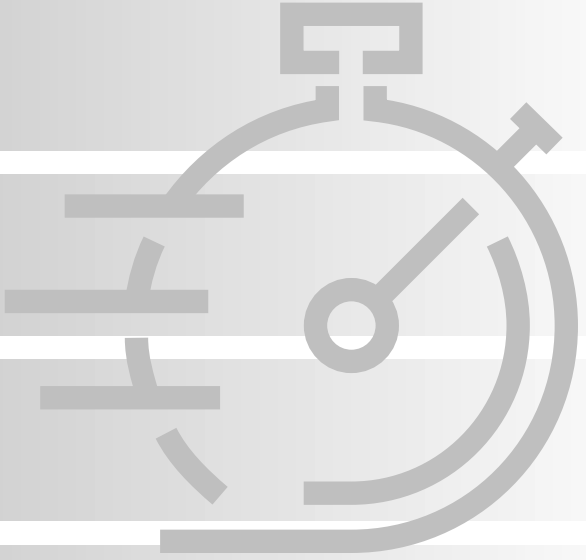
4,8 Millionen Blockungen durch Firewall-Systeme

11 Millionen geblockte Seitenaufrufe

600 abgewehrte Virenangriffe

550 geblockte Einschleusungen von Schadcode

20 verhinderte gezielte Angriffe



24 Stunden

Seit jeher hat man seine Kronjuwelen in einer Festung geschützt

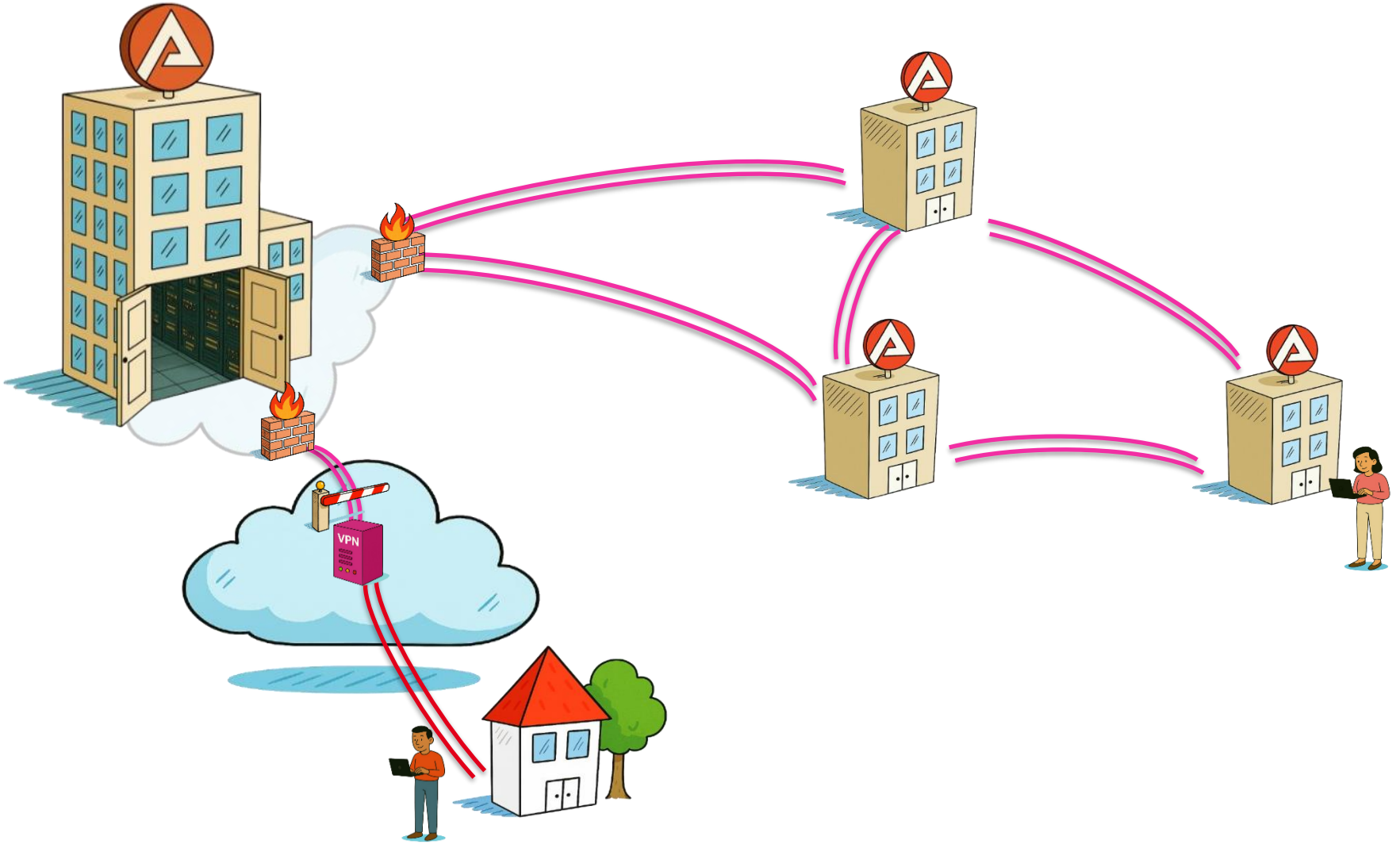
Paradigmen

- Eigene Data Center im Eigenbetrieb
- Weitgehend abgeschottetes Kommunikationsnetz
- Ein zentraler Outbreak-Point
- Mehrstufige Sicherheitsarchitektur
- Kontrolle in einer Hand
- Compliant zu IT-Grundschutz und KRITIS

Kommunikation Heute

Netzwerkzentriert

- Basis für die Kommunikation in der BA sind **dedizierte Leitungen** die unsere Liegenschaften verbinden
- Über dieses Netz (Wide Area Network - WAN) wird auf die zentralen Verfahren zugegriffen
- **„Sicherheitsinfrastruktur“ schützt das Netzwerk**
- Wer einmal in unser Netzwerk hereingelassen wurde **bewegt sich** darin **weitgehend ungehindert**



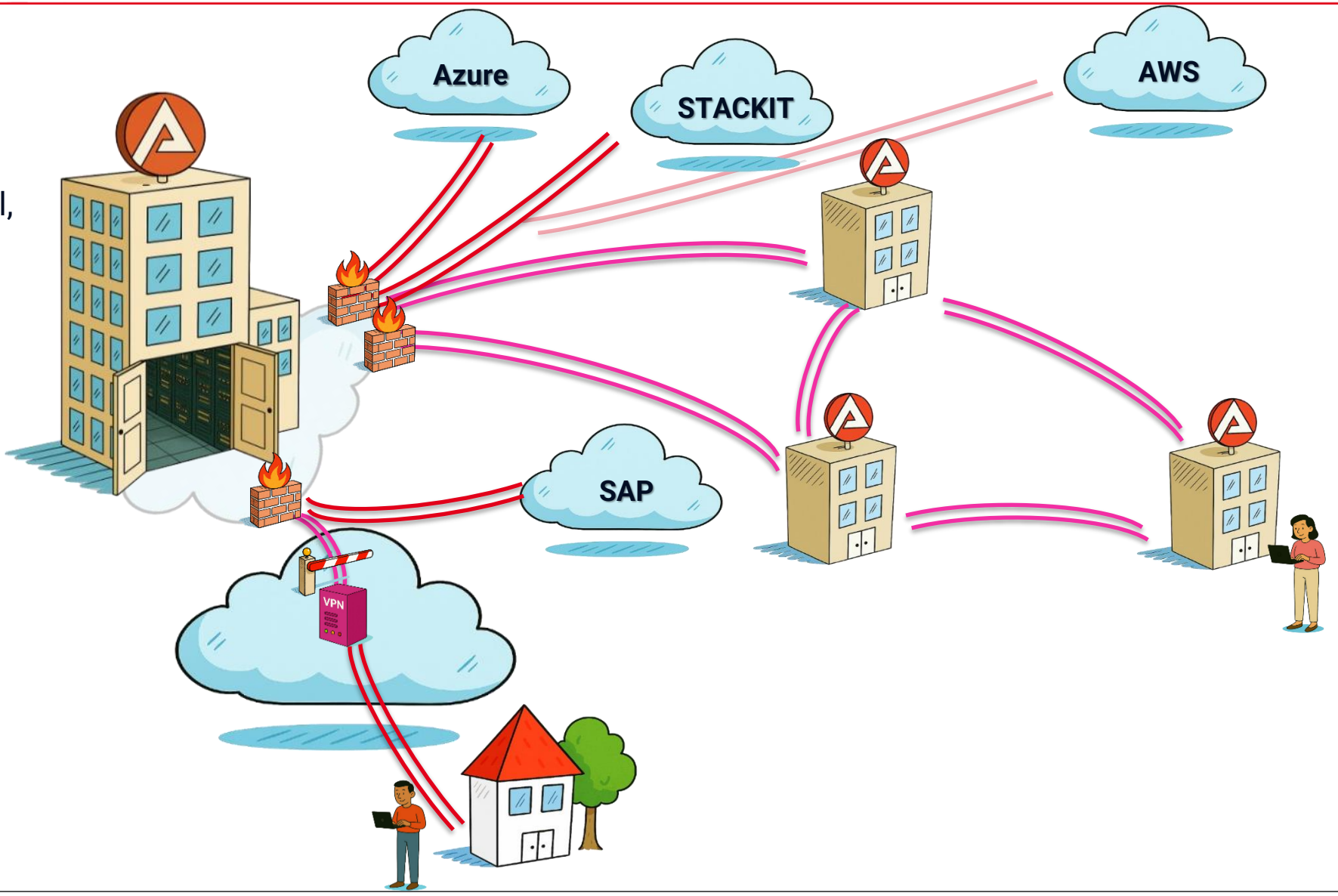
Neue Entwicklungen rütteln an den Paradigmen ... Die Festung bröckelt

- Zunehmende Nutzung von Cloud Diensten
- Colocation ersetzt sukzessive das eigene Data Center
- MPLS ist nicht mehr State-of-the-art
- Der Grad mobiler Nutzung nimmt rapide zu

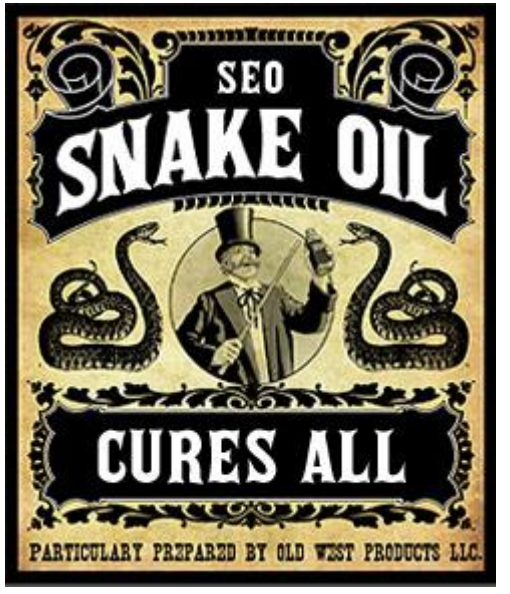
Kommunikation Morgen

IT ist nicht mehr überwiegend im BA-Netz („Cloudifizierung“)

- **IT ist nicht mehr „überwiegend“ im BA-Netz**
- Cloud Angebote sollen flexibel, sicher und direkt erreichbar sein
- Im heutigen Modell wird die **Kommunikation** (abgesehen von Sonderkonfigurationen) **immer über Nürnberg geführt**
- **Nachteile:** Das erhöht Zugriffszeiten, Komplexität und das Potential für Instabilitäten



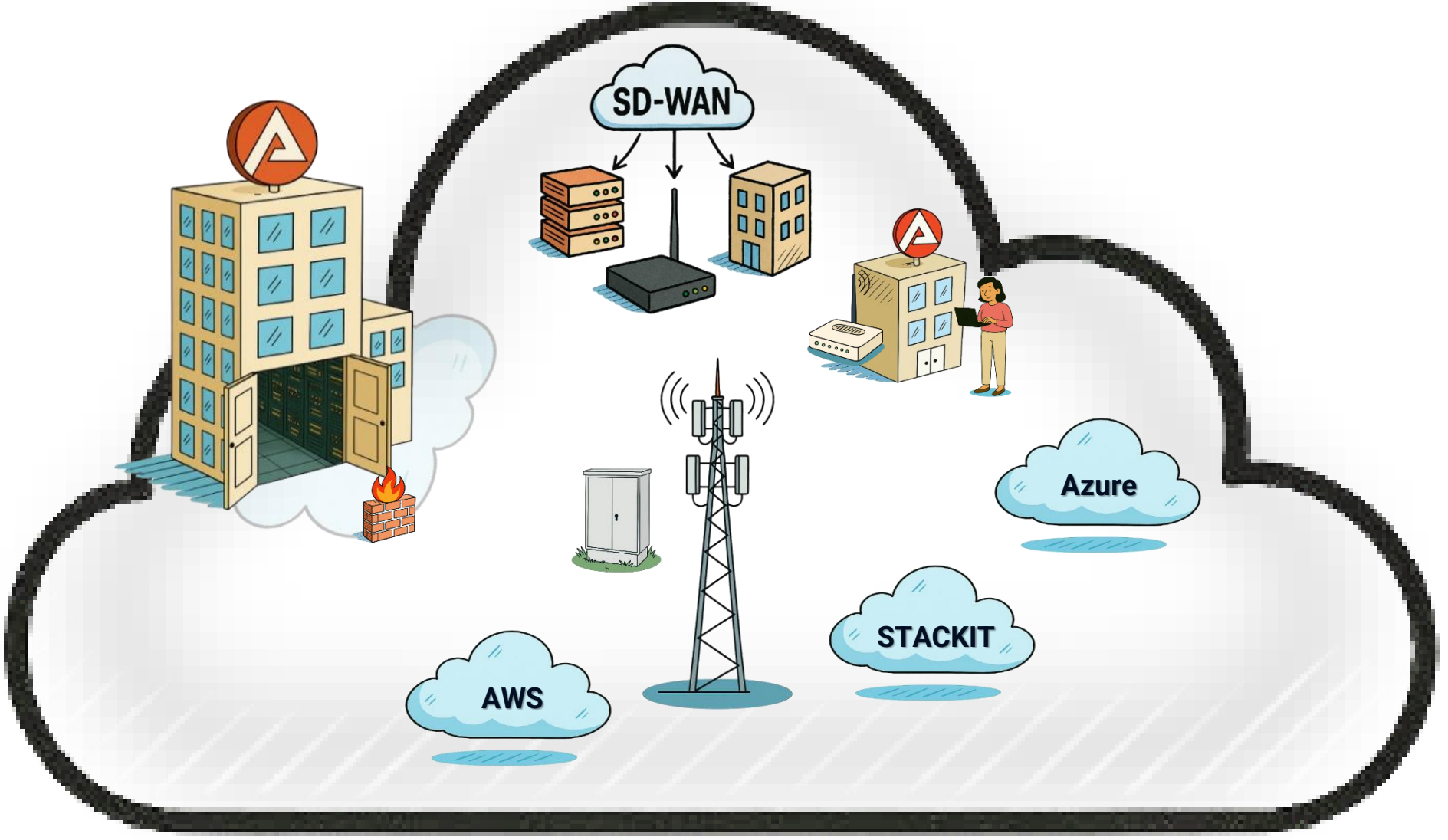
Neue Buzzwords – Zaubertrank oder Schlangenöl



Neue Technologien – SD-WAN

Software Defined Wide Areas Network

- SD-WAN erlaubt virtuelle Netze auf Basis beliebiger Verbindungen
- **Die BA kann damit beliebige Internetverbindungen** (5G, DSL, Glasfaser) **für die Kommunikation nutzen**
- **Sicher, flexibler und souveräner**
- SD-WAN erlaubt eine einfache und direkte Anbindung an und zwischen beliebigen Clouds (Zukunftssicher)



Zero Trust – die neue Zauberformel

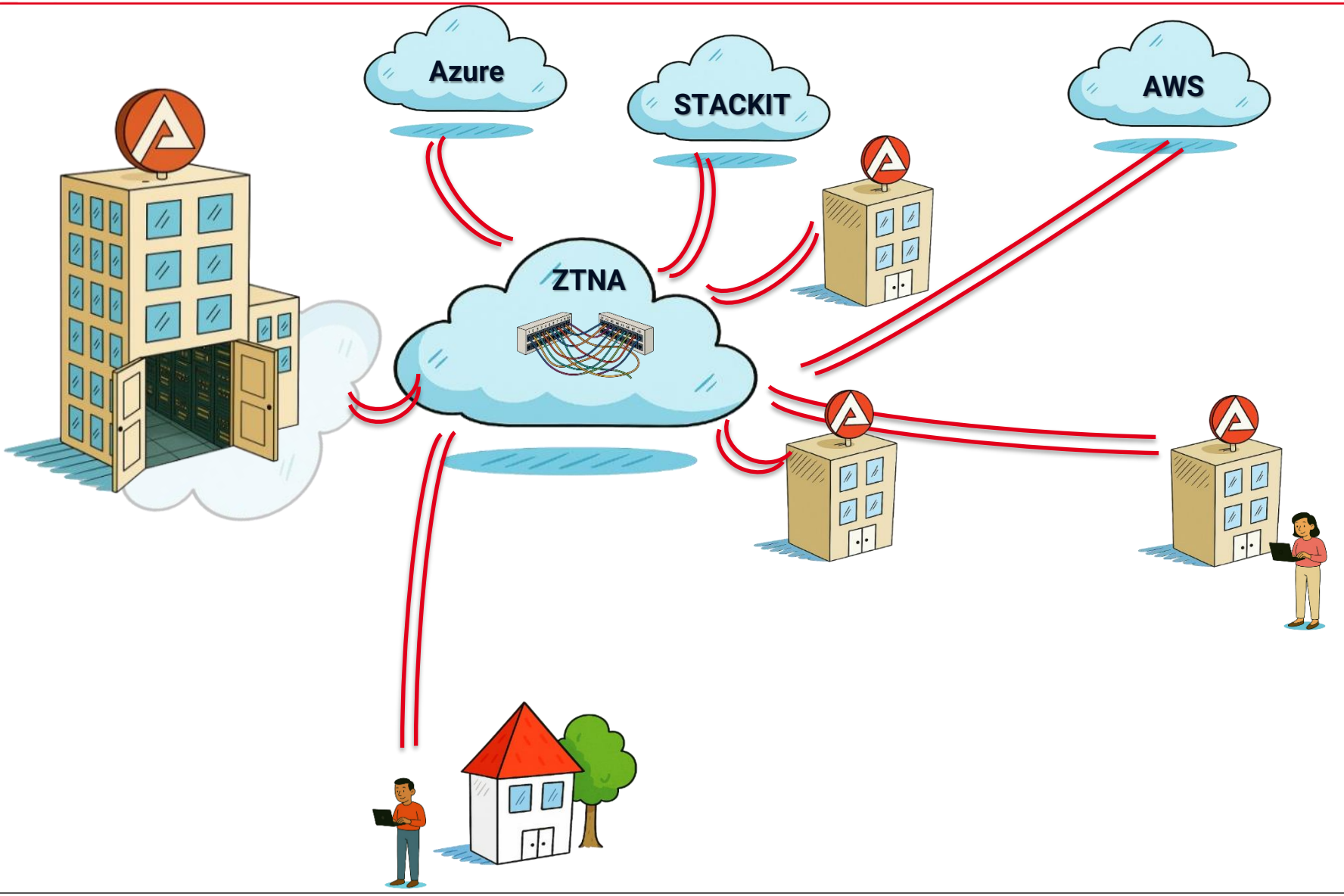
Zero Trust ist ein Sicherheitskonzept, das auf dem Prinzip „Vertraue niemandem, überprüfe alles“ basiert.

Im Gegensatz zu traditionellen Ansätzen wird nicht mehr davon ausgegangen, dass alles, was sich innerhalb eines Firmennetzwerks befindet, automatisch vertrauenswürdig ist. Stattdessen wird jeder Zugriffsversuch – egal ob von intern oder extern – kontinuierlich überprüft.

Neue Technologien – ZTNA

Zero Trust Network Access

- **BA Geräte** (Laptop, PC) können über einen **beliebigen Internetzugang** einen ZTNA Anbieter für die Verbindung zu unseren Daten und Diensten nutzen
- Der ZTNA Anbieter stellt sicher, dass nur **zugangsberechtigte Identitäten die notwendigen Verbindungen** auf dem **kürzesten Weg** erhalten



IT-Strategie 2030 / Programm Netzwerk 3.0

Ausgestaltung des Umbaus der Kommunikationsinfrastruktur als Programm

Die strategischen Zielbilder der IT-Strategie 2030

- Cloud Strategie
- RZ Strategie
- Arbeitsplatz der Zukunft
- Zero Trust Strategie

erfordern eine

sichere, flexible, stabile und zukunftsfähige Kommunikationsinfrastruktur

Gestaltet wird dies durch Umsetzung von Initiativen

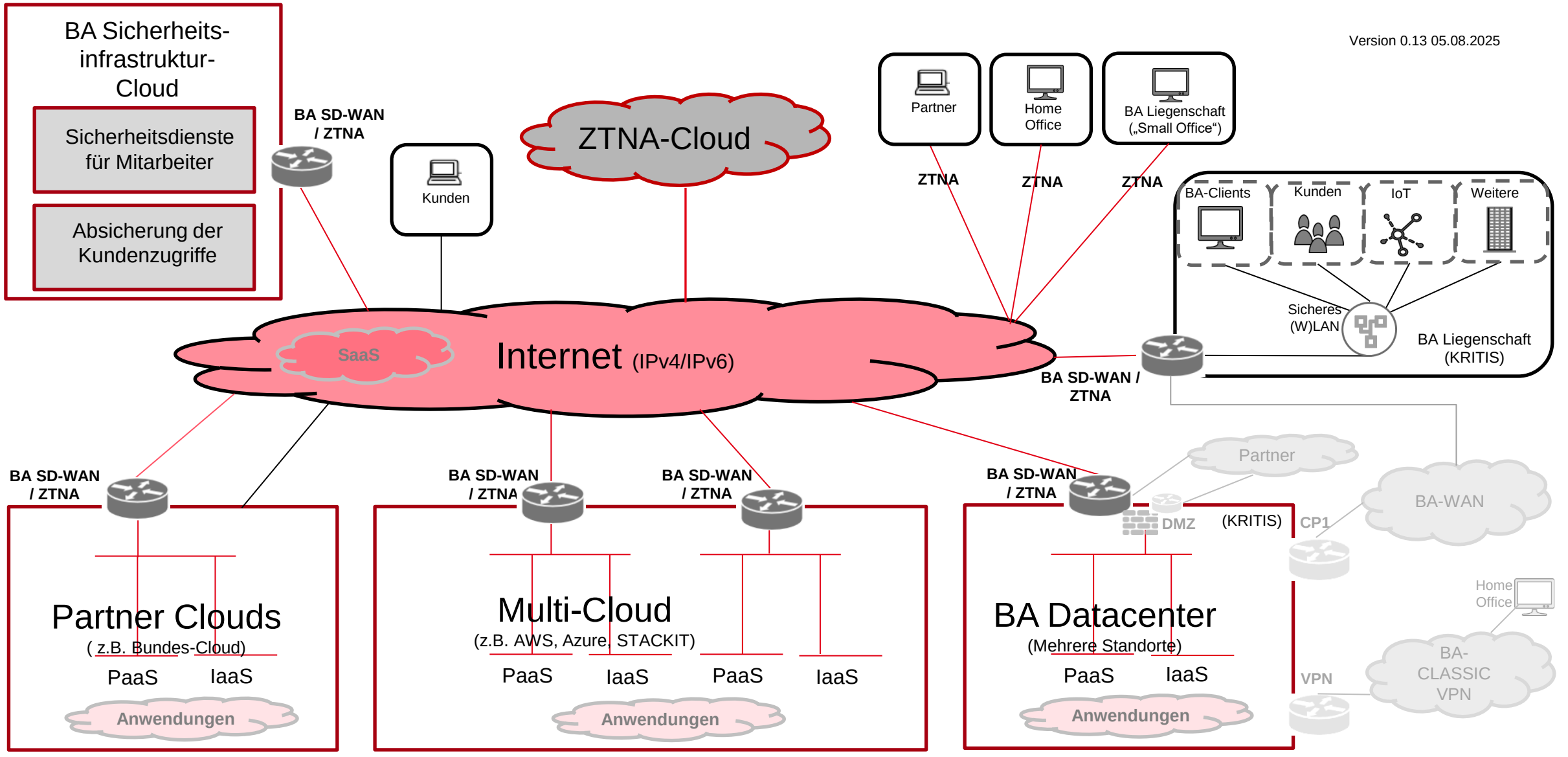
- SD-WAN / Segmentierung
- ZTNA Einführung
- IPv6 Einführung
- Umfassende Netzanalyse
- Weitere...

im Rahmen des Programmes

NETZWERK 3.0

Zielbild der zukünftigen Kommunikationsinfrastruktur (Netzwerk 3.0)

Kommunikation primär direkt über das Internet auf Basis einer Zero Trust Architektur



Die digitale Identität – Schlüssel der IT-Sicherheit

Modern attackers don't hack in, they log in!

Digitales Identitätsmanagement für
- 150.000 verwaltete Identitäten
- 120 Fachverfahren

Cloud-Identität
- Identity-Provider (IdP) für Mitarbeiter:innen in der Cloud
- Z.B. für Unterstützung der ZTNA-Lösung

Identity Threat Detection and Response (ITDR)
- Proof of Value (PoV) einer Identity Governance Lösung zu ganzheitlichen Schutz von Identitäten

Multi-Faktor-Authentifizierung (MFA)
- Bereitstellung einer integrierten MFA-Lösung
- Z.B. Einhaltung der NIS2-Vorgaben

Moderne Authentifizierung
- Bereitstellung moderner Mechanismen zur Authentifizierung interner Fachapplikationen

Cloud-Anbindung
- Anbindung verschiedener Cloud-Anbieter direkt oder indirekt an das Enterprise IAM

Tier-Trennung
- Trennung der Infrastruktur in drei Tier
- Administrative Zugriffe auf Tier-0 über Privileged Access Workstation (PAW)

Vertrauensdiensteanbieter der BA
Das Trustcenter der Bundesagentur für Arbeit

Qualifizierter VDA nach eIDAS

Qualifizierte elektronische Signaturkarten für digitale Prozesse (z. B. DiBAS) und qualifizierte Zeitstempel als digitaler Posteingangsstempel.

X.509 Client- und Serverzertifikiate

Zertifikate für Client- und Serversysteme als integraler Bestandteil einer Zero-Trust-Architektur.

E-Mail-Verschlüsselung

Übermittlung von Informationen bis Schutzstufe Sehr-Hoch per S/MIME-verschlüsselter E-Mail.

Trustcenter

Betrieb des Trustcenters der BA inkl. aller Infrastruktur. Bereitstellen der nötigen Softwarekomponenten für die Nutzung der PKI in der BA.

Beratung und Support

Kompetente Beratung von technischen und Fach-Bereichen in Bezug auf kryptographische Verfahren (auch Post-Quanten-Kryptographie) und den Einsatz von Signaturen.

VORTEILE - ZTNA und SD-WAN

ZTNA

SD-WAN

Zero Trust Network Access

- Zero Trust Network Access basiert auf der anerkannten Sicherheitsphilosophie Zero Trust und dem Need-to-know Prinzip
- **ZTNA ist mehr als nur ein technologisches Upgrade; es ist ein grundlegender Wandel hin zu einer anpassungsfähigeren, identitätsgesteuerten Sicherheitsarchitektur**
- Ständige Überprüfung der Zugangsberechtigung
- **Zugriff** auf eine Anwendung **wird** einer Identität **nur gewährt, wenn notwendig** (Rollenmodell)
- Angriffsfläche wird deutlich reduziert

Software Defined Wide Area Network

- Nutzbarkeit beliebiger Internetanschlüsse möglich
- **Sicher, Flexibler, kosteneffizienter und souveräner**
- Einfachere Anbindung an Cloud-Dienste

Hinweis: Beide Technologien sind unabhängig voneinander einsetzbar

Herausforderungen - ZTNA und SD-WAN

ZTNA

Zero Trust Network Access

- BSI Einschätzung ZTNA: „Aktuell (noch) nicht Stand der Technik“
  Formale Bewertung auf Basis fehlender „Standards und Normen“ und zu „geringer Erprobung in der Praxis im jeweiligen Bereich“ (öffentliche Sozialversicherungen).
  Jedoch in der Wirtschaft seit mehreren Jahren erfolgreich auch bei Großkonzernen im Einsatz
- Starke Anbieterabhängigkeit, diese entsteht durch die zentrale Nutzung für die Kommunikation (bei Ausfall des ZTNA Dienstes ist aus Anwendersicht die komplette IT nicht mehr nutzbar)
- BCM muss diese Änderung konzeptionell begleiten

SD-WAN

Software Defined Wide Area Network

- **Netze des Bundes (NdB)** Anbindung der BA sind mit „Bestandsschutz“ geduldet, Klärung ob Einführung von SD-WAN die Anbindung gefährdet, muss bei BDBOS adressiert werden.
- **Ersatz bzw. Anpassung** einiger Technologien und Verfahren notwendig.
  Manche klassische Netzwerkkommunikation z.B. **Druckerserver**, dezentrale **Fileserver**, dezentrale **Primion** Zutrittssysteme, **Amok bzw. ARE** (Alarmruf EDV) und ggf. weitere sind teilweise nicht ohne Anpassungen mit ZTNA vereinbar. Analyse und Umsetzung ist noch vorzunehmen.

FAZIT

Eine moderne Architektur erfordert flexible, performante Lösungen unter Beachtung von Souveränität und Kosteneffizienz

SD-WAN und ZTNA sind unabhängig voneinander einsetzbar, beide ergänzen sich jedoch ideal

- **SD-WAN schafft Sicherheit, Flexibilität, mögliche Kostenreduktion,** Abhängigkeitsreduktion und einfache technische Anbindbarkeit von Cloud-Diensten
- **ZTNA sichert den Zugriff auf Unternehmensressourcen** (Anwendungen, Server, Daten) nach Zero Trust Prinzip ab, jedoch entsteht eine hohe Abhängigkeit zum Dienst bzw. Anbieter
- ZTNA bietet einen identitätsbasierten Zugriff unabhängig vom Standort des Nutzers und auf dem schnellsten Weg
- ZTNA ist aus regulatorischer Sicht (BSI) noch nicht „Stand der Technik §8a BSIG),
  jedoch erfolgreich im praktischen Einsatz in Industrie- und Wirtschaftsunternehmen

- Bedingung für den Einsatz dieser Technologien ist eine Erarbeitung der Konzepte und Schaffung der Voraussetzungen.
  Hierfür soll das Projekt (NETSEC.UP2) gestartet werden.