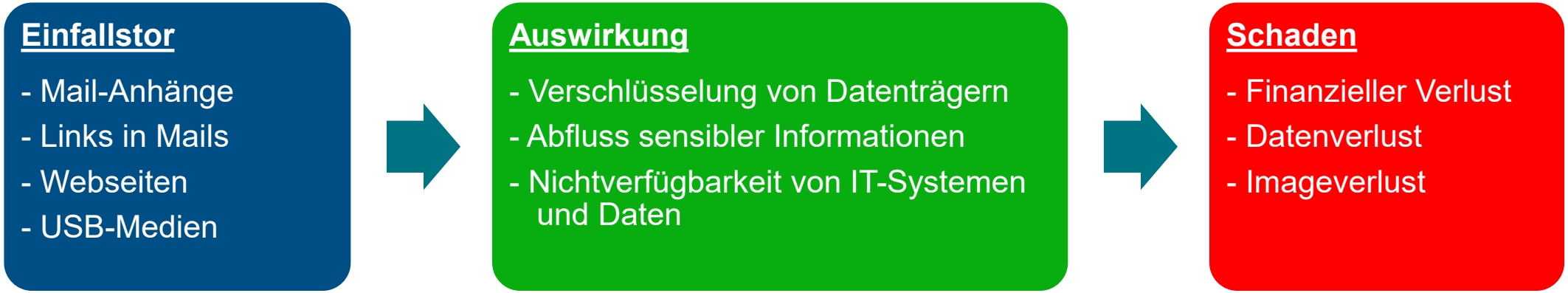
SEGMENTIERUNG IM WDR-NETZWERK

2025 / Infrastruktur / CC IP-Netze / Köln

Gefährdungslage im WDR



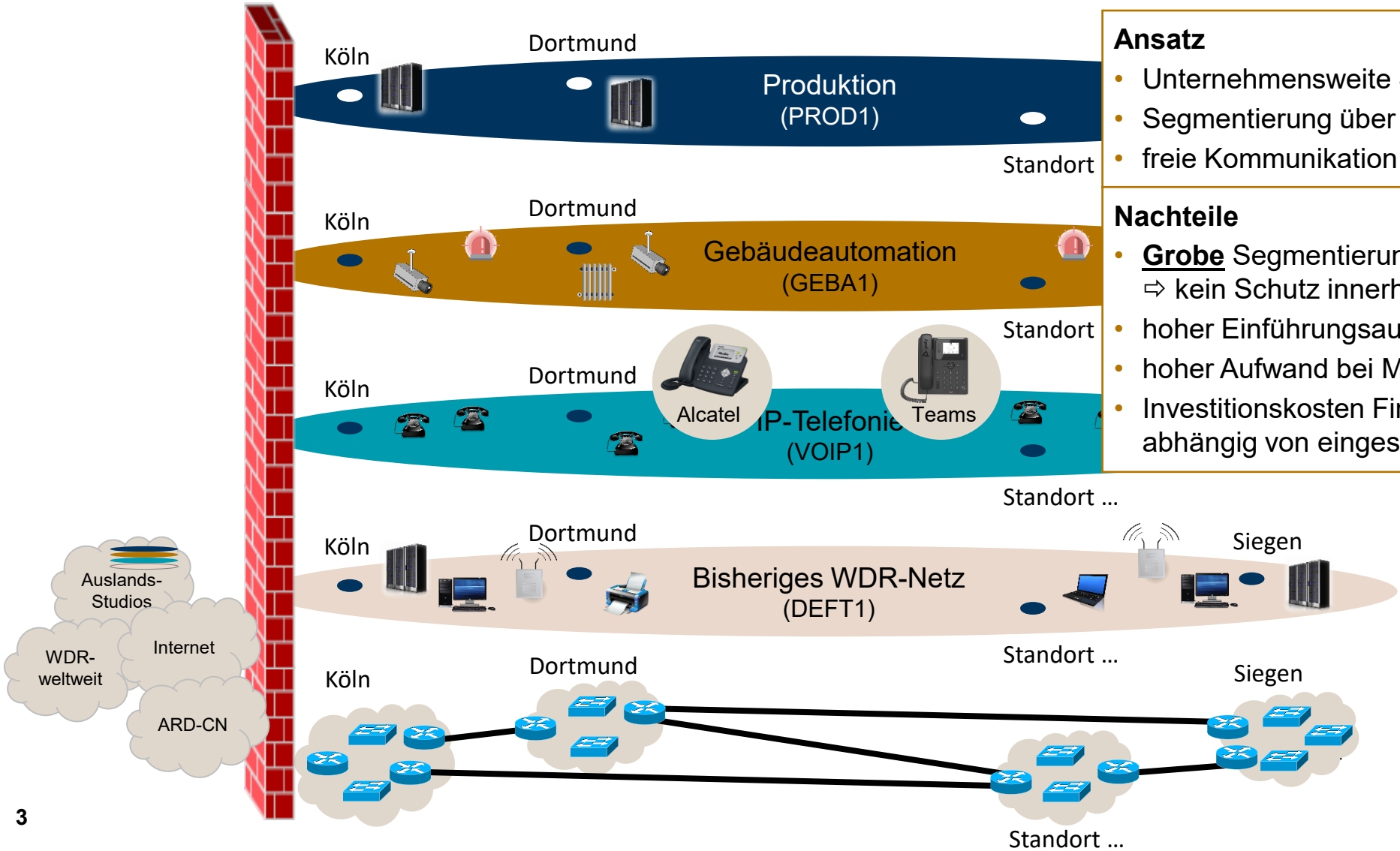
Welchen Nutzen bringt hier eine Segmentierung des Netzwerkes?

- **Reduzierung** von nicht autorisierten Zugriffen, Angriffen, Verteilung von Schadsoftware
- **Begrenzung der Ausbreitung** im Falle von Infektionen oder Angriffen

Präsenz dieses Themas

- **Allgemeine Empfehlung** des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und zahlreicher weiterer Organisationen, Gremien, Arbeitsgruppen
- **Explizite Empfehlung an den WDR** nach externem IT-Sicherheits-Audit in 2015

Netzwerkebenen (Makrosegmentierung)



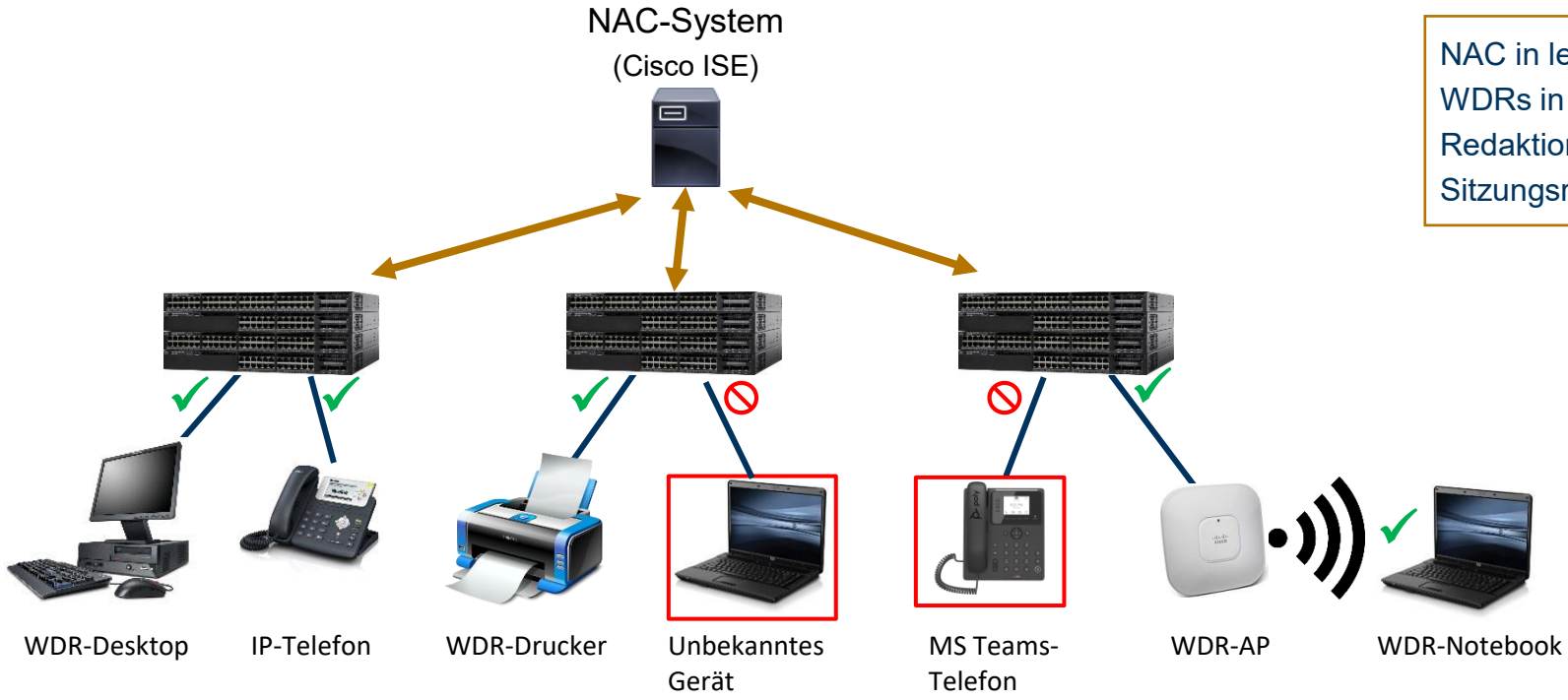
Ansatz

- Unternehmensweite Schutzzonen (Ebenen)
- Segmentierung über Core-Firewall
- freie Kommunikation innerhalb einer Ebene

Nachteile

- **Grobe** Segmentierung
  ⇨ kein Schutz innerhalb einer Ebene
- hoher Einführungsaufwand (mehrere Jahre)
- hoher Aufwand bei Migrationen
- Investitionskosten Firewall (Performance abhängig von eingesetzter FW-Hardware)

Network Access Control - HEUTE



NAC in leicht zugänglichen Bereichen des WDRs in Köln und der Region (Büro- & Redaktionsbereiche, Empfangsbereiche, Sitzungsräume & Flure)

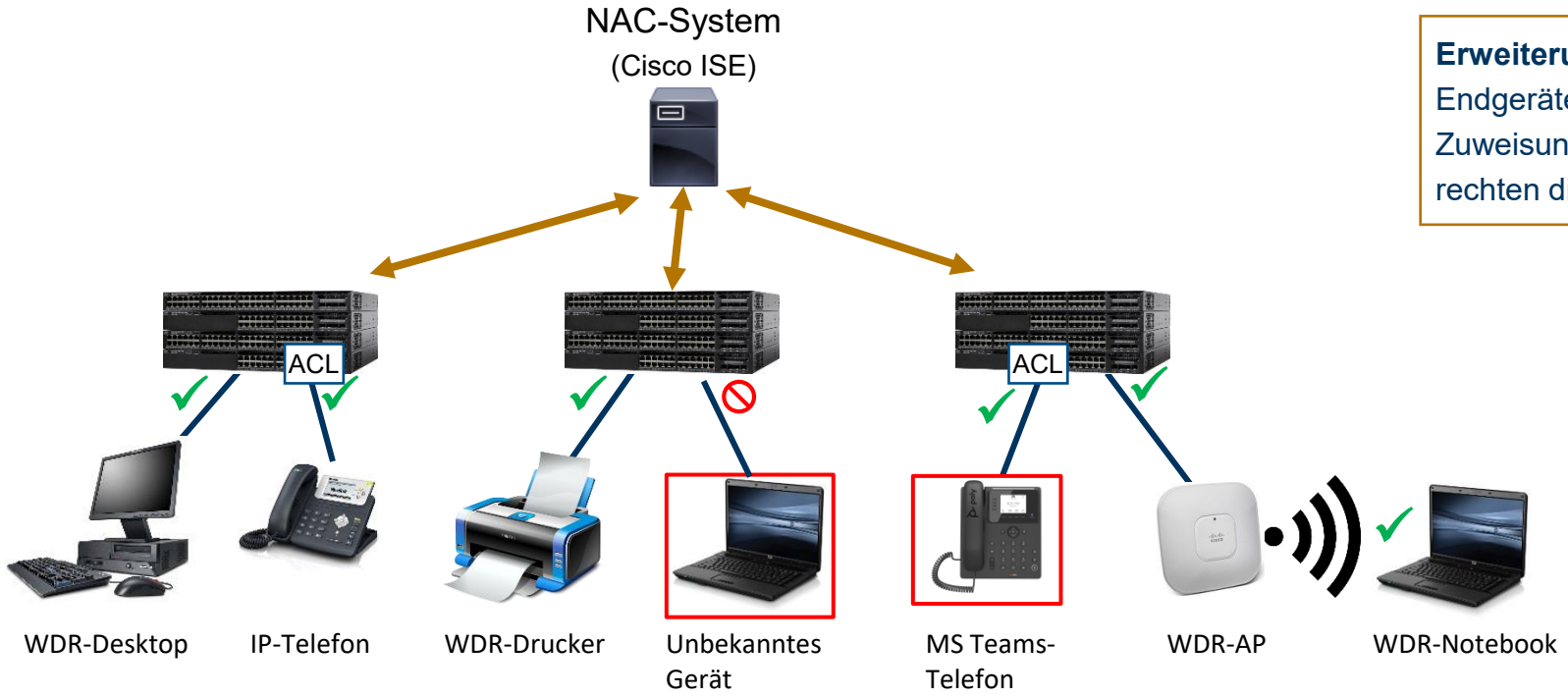
Basisaufgaben

1. Identifizierung von Endgeräten ⇨ Welche Geräte möchten sich mit dem Netzwerk verbinden?
2. Authentifizierung von Endgeräten ⇨ Welche Geräte erhalten Zugang?

Weitergehende Funktionen (Auszug)

3. Autorisierung von Endgeräten ⇨ Welche Zugriffe (Applikationen) werden gewährt?
4. Konformitätsprüfung von Endgeräten ⇨ Werden die Sicherheitsrichtlinien eingehalten (OS, AV)?

Network Access Control - ERWEITERUNG



Erweiterung: Autorisierung ausgewählter Endgerätegruppen durch automatische Zuweisung von gruppenbasierten Zugriffs-rechten direkt am Netzwerkzugangspunkt

Basisaufgaben

1. Identifizierung von Endgeräten ⇨ Welche Geräte möchten sich mit dem Netzwerk verbinden?
2. Authentifizierung von Endgeräten ⇨ Welche Geräte erhalten Zugang?

Weitergehende Funktionen (Auszug)

3. Autorisierung von Endgeräten ⇨ Welche Zugriffe (Applikationen) werden gewährt? ⇨ **Mikrosegmentierung**
4. Konformitätsprüfung von Endgeräten ⇨ Werden die Sicherheitsrichtlinien eingehalten (OS, AV)?

Makrosegmentierung vs. Mikrosegmentierung

Makrosegmentierung (Netzwerkebenen)	Mikrosegmentierung (NAC Autorisierung)
Unternehmensweite Schutzzonen (Ebenen), freie Kommunikation innerhalb einer Ebene	Verfügbarkeit in Bereichen in denen NAC eingesetzt wird
Grobe Segmentierung (Basisschutz)	Feine Segmentierung (Erweiterter Schutz)
Basiert auf IP-Netzen	Basiert auf Endgerätegruppen (unabhängig von IP-Netzen/-Adressen)
Segmentierung über Core-Firewall - Datenrate begrenzt - Betrieb der Regelwerke komfortabel	Segmentierung direkt auf den Switchports - Datenrate unbegrenzt bis zur Nenn-Datenrate des Switchports - Betrieb der Regelwerke aufwendiger (ACL)

- Beide Technologien werden parallel eingesetzt
- Mikrosegmentierung betrifft nur ausgewählte Endgerätegruppen, die übrigen Endgeräte bleiben unberührt
- Netzwerkebenen können neu bewertet werden ⇨ Ebenen können ggf. größer gefasst, Gewerke innerhalb einer Ebene per Mikrosegmentierung getrennt werden

Konkrete Einsatzbeispiele Mikrosegmentierung

Gerätetyp	Mikrosegmentierung	Umsetzungsstatus
Alcatel IP-Telefone	Verbot Kommunikation zum Proxy. Zusätzlich Unterbindung jeglicher IPv6-Kommunikation	Umgesetzt
MS Teams-Telefone (im Test)	Beschränkung auf Kommunikation zu Proxy und MS-Teams-Range im Internet. Zusätzlich Unterbindung jeglicher IPv6-Kommunikation	In Umsetzung
NTP-Uhren	Beschränkung auf Kommunikation zu NTP-Servern und wenigen weiteren Systemen	Umgesetzt
Command Labeldrucker	Beschränkung auf Kommunikation zu Command und wenigen weiteren Systemen	Umgesetzt
Infizierte Endgeräte	Automatisierte Erkennung der Virusinfektion (durch zentrale IT-Security-Systeme), hieraufhin dynamische Beschränkung (per NAC) auf Kommunikation zu Update-Servern (Virenscanner, Win-Updates) und IT-Security-Systemen. Zusätzlich Unterbindung jeglicher IPv6-Kommunikation	In Entwicklung
Diverse GBW Geräteklassen	Webcams, Kartenleser, Überwachungsanlagen etc., jeweils Beschränkung auf benötigte zentrale Systeme	In Entwicklung
Drucker/MFP	Beschränkung auf Kommunikation zu Druckserver und zu administrativen Zwecken (u.a. Mailversand)	Idee
Standardclients	Beschränkung der Kommunikation untereinander (z.B. nur RDP)	Idee

Auswirkungen Mikrosegmentierung auf den Betrieb der WDR IT-Infrastruktur

- Überwiegend bleibt Alles, wie es ist
- Spezielle Endgerätetypen werden bedarfsgerecht mit Mikrosegmentierung ausgestattet
- Vor Einführung neuer Endgerätetypen wird zukünftig geprüft inwiefern der Einsatz von Mikrosegmentierung sinnvoll und möglich ist
- Im Betrieb ist bei Kommunikationsproblemen von Endgeräten zusätzlich zu Firewall-Systemen auch die Mikrosegmentierung zu berücksichtigen

Vielen Dank.