

# Zukunftsorientierte & sichere IT-Konzepte für Ihre Zahnarztpraxis

## Aktuelle Herausforderungen und Lösungen

**ARCONDA**.systems  
Aktiengesellschaft

**SCHIEBLER**  
Zahntechnik GmbH



11. Februar 2020 EAST Hotel Hamburg



Frank Espenhain

CEO

Security und Cloudprojekte

f.espenhain@arconda.ag

Tel.: 040 823158 15

Seit 1995 bei der Arconda Systems AG

Dr. Bernd Lühr

Leiter Datenschutz

b.luehr@arconda.ag

Tel.: 040 823158 13

Seit 1998 bei der Arconda Systems AG

- 1 Zukunftsorientierte und sichere IT-Konzepte für Ihre Zahnarztpraxis
  - 1.1 Herausforderungen
  - 1.2 Maßnahmenkatalog für Datenschutz und Datensicherheit
  - 1.3 Telematik Infrastruktur
  - 1.4 Best Practice Ansatz
  - 1.5 Cyber Resilience
- 2 Sicherer E-Mail-Empfang
  - 2.1 Hintergrund
  - 2.2 Firewall: E-Mail Virens Scanner
  - 2.3 Firewall: Sandboxing Technologie
  - 2.4 URL-Filter gegen Stealth-Angriffe
  - 2.5 Mailarchivierung
  - 2.6 Human Factors
  - 2.7 Fallbeispiel CEO Fraud
- 3 Sichere E-Mail-Versendung
  - 3.1 Hintergrund
  - 3.2 TLS-Verschlüsselung
  - 3.3 E-Mail-Signaturen / Zertifikate
  - 3.4 Versendung verschlüsselter E-Mails
  - 3.5 Links statt Dateien versenden

- 4 Arbeitsplatzrechner
  - 4.1 Endpoint Security
  - 4.2 Lokale Firewall
  - 4.3 Next Generation Firewall
  - 4.4 Zugriffskontrolle
  - 4.5 Human Factors
- 5 Netzwerkinfrastruktur
  - 5.1 LAN-Sicherheit
  - 5.2 WLAN-Sicherheit
- 6 Sicherer Umgang mit Mobile Devices
  - 6.1 Verhaltensgrundsätze
- 7 Server
  - 7.1 Betriebsbedingungen
  - 7.2 Betriebskonzept
  - 7.3 Ausfallsicherheit
  - 7.4 Datensicherung und  
-wiederherstellung
  - 7.5 Offside-Sicherung
- 8 Fazit
- 9 IT-Assessment

## 1.1 Herausforderungen

### 1.1.1 Produktionsfaktor EDV-Ausstattung ist kritisch

Warum? Durchdringt alle Prozesse von der Terminvereinbarung bis bildgebenden Verfahren

### 1.1.2 Steigende Gefährdungen

Organisierte Kriminalität hat nach Kreditkartenbetrug und Phishing Trojaner und Viren (Malware, Ransomware) als zukunftssträchtiges Geschäftsfeld entdeckt

„Der Traditions-Juwelier Wempe wurde nach eigenen Angaben am 24.06.2019 Opfer eines Ransomware Angriffes auf die hauseigenen Server. Im Zuge des Angriffes wurden Firmendaten verschlüsselt und von den Angreifern eine Nachricht sowie eine E-Mail Adresse zur Kontaktaufnahme hinterlegt. Die Erpresser forderten ein Lösegeld und boten als Gegenleistung die Herausgabe des Passworts zur Entschlüsselung an.“ Weitere Einzelheiten wurden nicht veröffentlicht.

## 1.1.3 Bedrohungslage

- Fahrlässige Missachtung von Sicherheitsvorkehrungen kann zu erheblichen Betriebsstörungen bis zu einer Gefährdung der Unternehmensbestandes führen
- Üblicherweise geringe Bedrohungslage und gezielte Angriffe eher unwahrscheinlich
- „Nicht mit Kanonen auf Spatzen schießen“

## 1.1.4 DSGVO

Gesetzlicher Rahmen: *Art. 32 DSGVO Sicherheit der Verarbeitung*

fordert Technische und Organisatorische Maßnahmen (TOM) „um ein dem Risiko angemessenes Schutzniveau zu gewährleisten [...] und die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme sicherzustellen [...]“

## 1.1.5 Betreuungsniveau

- Schwierige Betreuungslage für Kleinunternehmen
- Keine eigene kompetente IT aufgrund der Betriebsgröße
- IT-Lieferanten oftmals sehr klein und mit dem technologischen Fortschritt überfordert
- IT als Bundlingprodukt Software oder Verbrauchsmaterial mit Hardware

## 1.2 Maßnahmenkatalog für Datenschutz und Datensicherheit

### 1.2.1 Höchste Anforderungen an die Datenverarbeitung

- Besonderer Schutz sensibler Daten wie medizinische Diagnose, Befunde und Therapien
- Persönlichkeitsrechte des Einzelnen erfordern den sorgsamsten Umgang mit diesen Daten
- Grundlagen der ärztlichen Schweigepflicht folgen sowohl aus dem Strafgesetzbuch (Paragraf 203 StGB) als auch der Berufsordnung der Zahnärzte (Paragraf 7 MBO)
- DSGVO Art. 9: Verarbeitung besonderer Kategorien personenbezogener Daten

## 1.2.2 Praktische Umsetzung

- Konkrete technische Beschreibung der Maßnahmenumsetzung

## 1.2.3 Maßnahmenbewertung

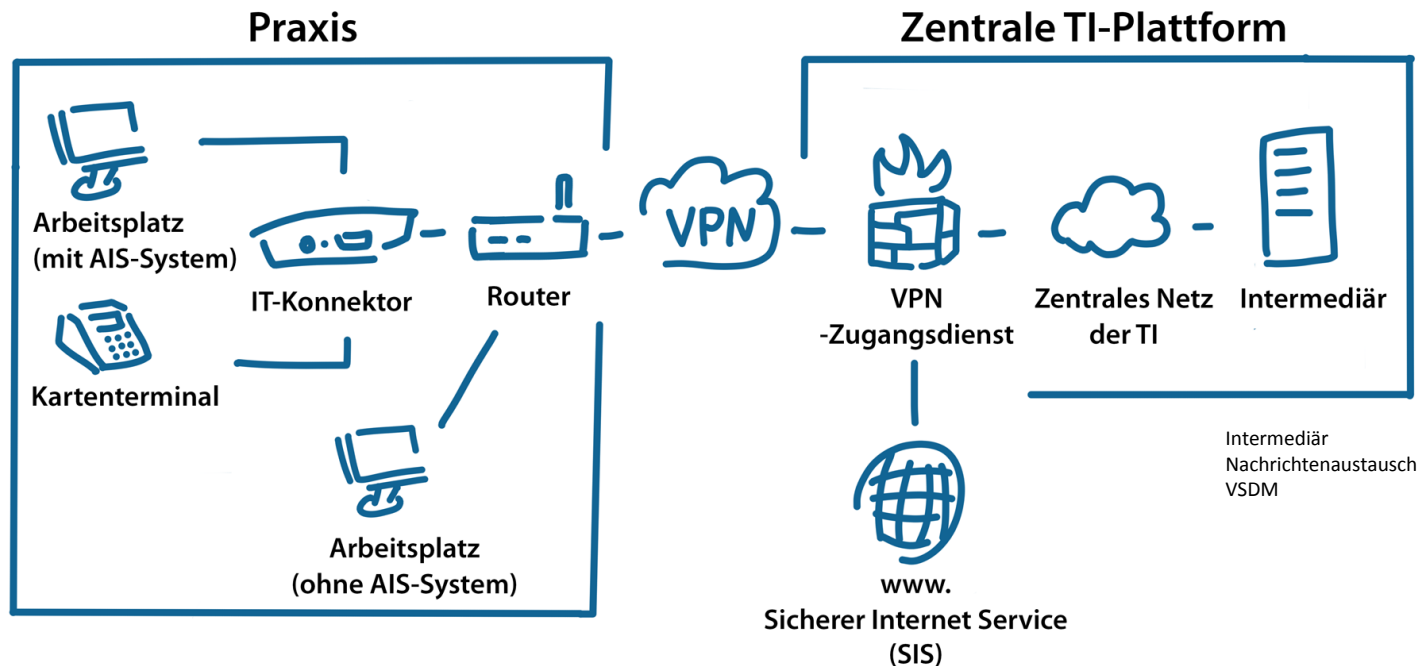
- Klassifizierung der Maßnahmen in
  - Mindestanforderungen
  - Empfohlene Maßnahmen
  - Erhöhter Schutzbedarf

## 1.3 Aus gegebenem Anlass: Telematik Infrastruktur

### 1.3.1 VDSL-Router inkl. VPN-Tunnel für > 2.000 €



### 1.3.2 Vision der Gematik



## 1.3 Aus gegebenem Anlass: Telematik Infrastruktur

### 1.3.3 Konzeptionelle Schwächen

Internetzugang in dieser Form unpraktikabel weil

- limitiert
- teuer
- starr
- zentral kompromittierbar (angreifbar)

## 1.3.4 Streiflicht: Chaos Computer Clubs in Leipzig, 27.12.2019

Aktueller Bericht vom 36C3, Kongress des Chaos Computer Clubs in Leipzig, 27.12.2019  
(<https://www.ccc.de/de/updates/2019/neue-schwachstellen-gesundheitsnetzwerk>):

"Hackern des Chaos Computer Club ist es gelungen, sich Zugangsberechtigungen für das sogenannte Telematik-Netzwerk zu verschaffen. [...] CCC-Sicherheitsforschern ist es gelungen, sich gültige Heilberufsausweise, Praxisausweise, Konnektorkarten und Gesundheitskarten auf die Identitäten Dritter zu verschaffen. Mit diesen Identitäten konnten sie anschließend auf Anwendungen der Telematik-Infrastruktur und Gesundheitsdaten von Versicherten zugreifen."

## 1.4 Best Practice Ansatz in Zeiten der TI-Infrastruktur

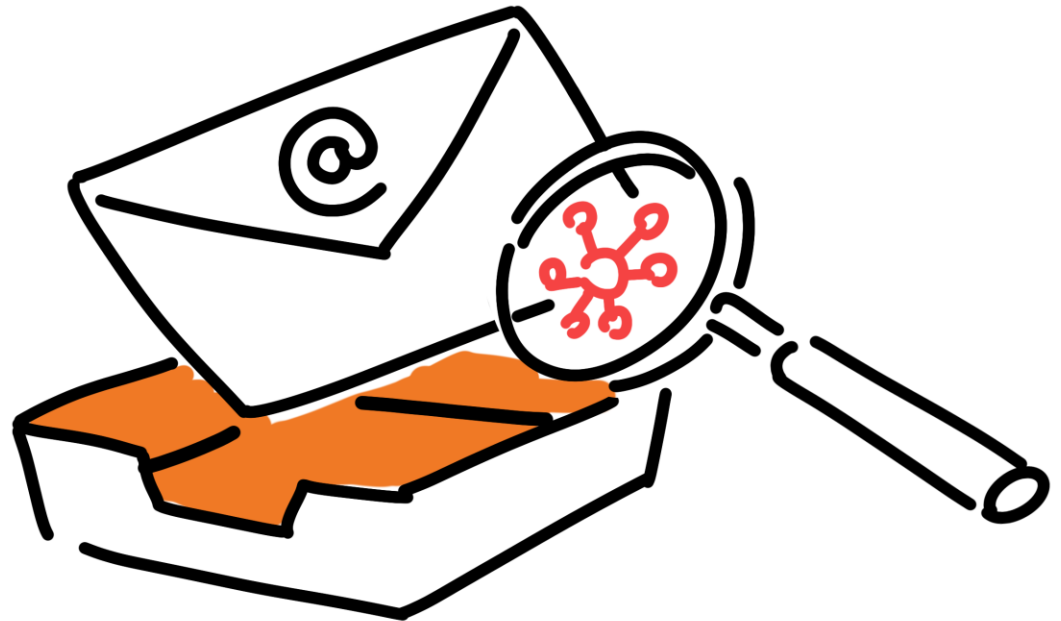
- Bedrohungssituation erkennen
- Einfallstore für Schadcode schließen
- Ökonomisches Prinzip
  - Wie erreiche ich das gewünschte Schutzniveau mit geringsten Investitionen oder
  - Wie kann ich bei einem vorgegebenen Budget das Schutzniveau maximieren

## 1.5 Cyber Resilience

bzw. die „Widerstandsfähigkeit gegen webbasierte Bedrohungen“ ist die Fähigkeit eines Unternehmens, sich anzupassen und auf unerwünschte Cyber-Ereignisse zu reagieren – unabhängig davon, ob es sich um interne oder externe, böswillige oder unbeabsichtigte Ereignisse handelt – auf eine Weise, die die Vertraulichkeit, Integrität und Verfügbarkeit der für das Unternehmen wichtigen Daten und Dienste gewährleistet



# 2. Sicherer E-Mail Empfang



## 2.1 Hintergrund

- E-Mails als Einfallstor für Schadcode
- Prädiktive = Vorausschauende E-Mail-Sicherheit
- Geeignete Firewall (⚠ Mindestanforderung) für prädiktive E-Mail-Sicherheit – vorausschauende Erkennung von Payloads = Gefährdungspotentialen anhand verschiedenster Indikatoren
- Praxisbeispiel:

### **Experten warnen vor Mails zu Coronavirus**

Kriminelle nutzen derzeit Ängste vor dem Coronavirus, um mit Hilfe von Mails Schadsoftware zu verbreiten. Dabei handelt es sich um Computerwürmer oder Trojaner. Das berichtet das Sicherheitsunternehmen Kaspersky in einer Pressemitteilung. Die Dokumente enthalten Trojaner oder Würmer, die Daten vernichten, verschlüsseln, ändern oder kopieren, sowie den Betrieb von Computern oder Computernetzwerke stören. (Quelle: [www.t-online.de](http://www.t-online.de))

- Neueste Masche: Erpressung durch Androhung der Veröffentlichung personenbezogener Daten


## 2.2 Firewall: E-Mail Virens scanner ( Mindestanforderung)

- Durchsuchen des eingehenden Datenstromes nach Schadcode
- Geeignete Hard- und Software erforderlich: Fritzbox kann das nicht

### 2.3 Firewall: Sandboxing-Technologie (👍 Empfohlene Maßnahme)

- Ausführen der verdächtigen Dateien auf einem virtuellen System im Rechenzentrum des Firewall-Anbieters
- Verwerfen von E-Mails bei bösaartigen Verhalten

### 2.4 Firewall: URL-Filter gegen Stealth-Angriffe

 Empfohlene Maßnahme)

- Verhindern, dass Schadcode über das Anklicken potentiell gefährlicher Links in den eMails später nach dem Empfang eingeschleppt wird
- Validierung zum Zeitpunkt des Anklicken der eMail und nicht zum Empfangszeitpunkt der eMail verhindert verschleppte Angriffe
- Liveabfrage der URL durch Firewall bei Zugriff

### 2.5 Mailarchivierung ( Mindestanforderung)

- Archivierung von eMails gesetzeskonform
- Rechtlicher Hintergrund GoBD (Grundsätzen zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff )
- Archivierung erforderlich: Geschäfts- bzw. Handelsbrief, oder steuerlicher Bezug
- Inhalte von Handelsbüchern, Inventaren, Jahresabschlüssen oder auch Buchungsbelegen

Optional:

**Externer Rechenzentrumsdienstleister** (  Empfohlene Maßnahme)

### 2.6 Human Factors (⚠ Mindestanforderung)

- Wichtige Ergänzung zu den technischen Maßnahmen
- Ihre Mitarbeiter sind der wichtigste Teil Ihrer Firewall
- Sensibilisierung der Mitarbeiter für eMails mit fragwürdigen Anforderungen - Social Engineering Scams
- Bei kleinsten Verdachtsmomenten über anderen Kommunikationskanal verifizieren
- Klare Abläufe definieren

### 2.7 Fallbeispiel „CEO Fraud“

Betrugsmasche, bei der Firmen unter Verwendung falscher Identitäten zur Überweisung von Geld manipuliert werden:

Sehr geehrte Frau M., ich kann doch in einer streng vertraulichen Finanzangelegenheit auf Ihre Unterstützung zählen. Unser Unternehmen plant eine Expansion in den asiatischen Geschäftsraum und wird hierzu eine existierende Firma übernehmen. Wie Sie sicher verstehen können, ist diese Transaktion streng geheim. Aus diesem Grunde und zu Dokumentationszwecken für die Bafin darf die gesamte Kommunikation mit mir ausschließlich per Mail erfolgen. Mit der Abwicklung wurde das Schweizer Notariat E. betraut. Der Rechtsanwalt und Notar Dr. E. wird sich morgen telefonisch bei Ihnen bezüglich der Details melden. Bitte bereiten Sie alles für eine entsprechende Auslandsüberweisung vor. Ich weiß, dass ich mich auf Sie verlassen kann. Mit freundlichen Grüßen Dr. W., CEO

# 3. Sichere E-Mail Versendung



## 3.1 Hintergrund

- Privacy und Datenschutz für das Kommunikationsmedium E-Mail

## 3.2 TLS-Verschlüsselung ( Mindestanforderung)

- Standard
- Transport Layer Security (TLS) , alte Bezeichnung Secure Sockets Layer (SSL)
- Mailserver/Mailclient
- Abhängig vom Mail-Provider
- TLS-Einrichtung auf eigenem Mailserver oder dem bei dem Provider nicht erfolgt => Mails können ggf. in den involvierten Netzwerken mitgelesen werden

## 3.3 E-Mail Signaturen / Zertifikate (👍 Empfohlene Maßnahme)

- Nachweis Identität des Absenders
- Einbau in den Mailserver –soweit vorhanden- oder in den Mailclient oder die Firewall

## 3.4 Versendung verschlüsselter E-Mails



Firewall Erhöhter Schutzbedarf

- Sporadische / einmalige E-Mail Empfänger
- E-Mail kann nur mit Passwort geöffnet werden

## 3.5 Links statt Dateien versenden

- Zeitlich steuer- und widerrufbarer Zugriff auf Dateien in der Cloud
- Z.B. Nextcloud bei Rechenzentrumsdienstleister
- Ersatz für USB-Sticks
- Möglicher Ablageort für Backups

Externer Rechenzentrumsdienst (  Erhöhter Schutzbedarf)

# 4. Arbeitsplatzrechner



## 4.1 Endpoint Security ( Mindestanforderung)

- Virens Scanner & Malwareschutz
- Nicht unerhebliche Kosten
- Zentrales Updatemanagement
- Verhindern des Abschaltens bei restriktivem Verhalten des Scanners

## 4.2 Lokale Firewall ( Mindestanforderung)

Bremsen der netzwerkinternen Verbreitung von Schadcode

## 4.3 Next Generation Firewall ( Empfohlene Maßnahme)

Zumeist in den Virens Scanner integriert

Deaktivierung externer Datenträger = Einfallstore für Schadcode

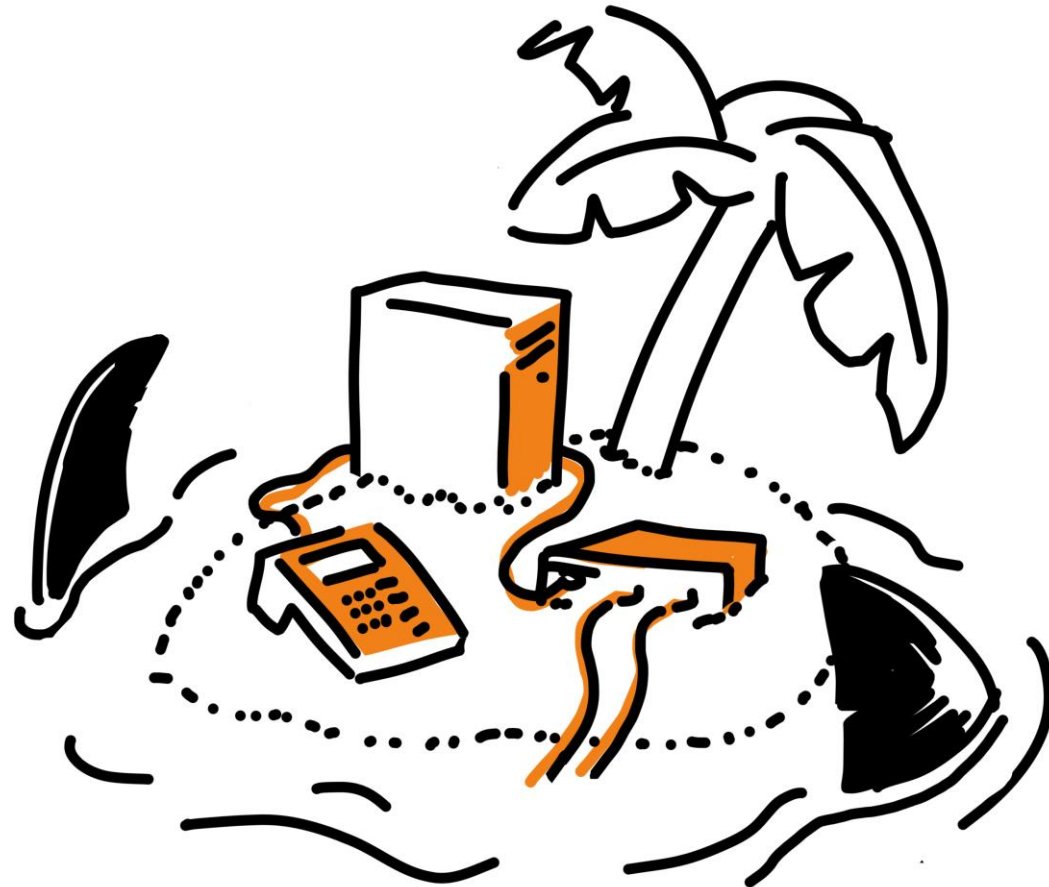
## 4.4 Zugriffskontrolle ( Mindestanforderung)

- Benutzerauthentifizierung
- Passwortsicherheit (Anmeldung2/Anmeldung2 besser ganz ohne Passwort?)
- Restriktive Rechtevergabe
- Rollen- und Berechtigungskonzepte
- Bildschirmschoner mit Kennwort (automatisch)

## 4.5 Human Factors (⚠ Mindestanforderung)

- Passworthandling
- Bildschirm sperren bei Verlassen des Arbeitsplatzes
- Einsichtnahme von Dritten auf Bildschirm reduzieren, ggf. Schutzfolien

# 5. Netzwerkinfrastruktur



## 5.1 LAN-Sicherheit (⚠ Mindestanforderung)

- Abwehr von unerwünschten kabelgebundenen Netzwerkzugriffen
- Netzwerksteckdosen
- Wo, welcher Zugriff bzw. wie gepatched
- Im öffentlichen Bereich vermeiden

## 5.2 WLAN-Sicherheit ( Mindestanforderung)

- Authentifizierung Standard WLAN-Name und Passwort
  - Nicht benutzerspezifisch
- Besser: Radius-Server
  - benutzerspezifisch
  - WLAN + AD-Kennung und PW ggf. Token
- Verschlüsselung WPA2 (Wi-Fi Protected Access 2)
- VLAN für Patienten
  - Portisolierung: Gast zu Gast Verbindung nicht möglich

# 6. Sicherer Umgang mit mobile Devices



## 6.1 Verhaltensgrundsätze

( Mindestanforderung)

- „Bring your own device“
- Umgang mit Passwörtern – z. B. von ausgeschiedenen Mitarbeitern
- Zugriff von Apps auf Telefonbuch/Kontakte unterbinden (WhatsApp)
- Passwortschutz
- Sperrbildschirm
- Remote Löschung
- Verschlüsselung der Datenträger (Standard IOS und Android)


# 7. Server



## 7.1 Betriebsbedingungen ( Mindestanforderung)

- Aufstellort
- Wo steht der Server, wer hat physikalischen Zugriff
- Vandalismus, Diebstahl, versehentliche Beschädigungen
- Elementarschäden (Feuer, Wasser)
- Klima / Betriebstemperatur ( $\leq 25^\circ \text{C}$ )
- Staub

### Alternative:



Zentraler Rechenzentrumsdienstleister (  Empfohlene Maßnahme)

## 7.2 Betriebskonzept (⚠ Mindestanforderung)

- Routinekontrollprogramm auf Hard- und Softwareebene
- Vorbeugende Maßnahmen zur Vermeidung von unerwünschten Betriebszuständen
- Regelmäßige Update / Softwareaktualisierungen

Zentraler Rechenzentrumsdienstleister (👍 Empfohlene Maßnahme)

## 7.3 Ausfallsicherheit

- Ausfallsichere Festplattenspeicher RAID (  Mindestanforderung)
- Redundante Komponenten für den Server
- Virtualisierung und Storage (  Empfohlene Maßnahmen)
- Rechenzentrum

Externer Rechenzentrumsdienstleister (  Empfohlene Maßnahme)

## 7.4 Datensicherung und –wiederherstellung (⚠ Mindestanforderung)

- Vollautomatisch, zuverlässig und schnell wiederherstellbar
- Benachrichtigungsemail
- Imagebasierte Datensicherung
- 3-2-1-0 Regel (3 Kopien mit mindestens 2 verschiedenen Technologien speichern. Davon mindestens 1 Kopie außer Haus lagern. 0 Fehler)
- Backup-Konzept
  - Wie häufig?
  - Wie lange?
  - Aufbewahrungszeit (wie weit kann ich zurückspringen)
  - Validiertes Wiederherstellungskonzept

## 7.5 Offside-Sicherung ( Mindestanforderung)

- Wechselfestplatten (schwieriges Betriebskonzept)
- oder
- Cloud-Backup durch spezialisierte Dienstleister

Externer Rechenzentrumsdienstleister (  Empfohlene Maßnahme)





	Mindestanforderung	Empfohlen	Erhöhter Schutzbedarf
<b>1. Sicherer E-Mail Empfang</b>	<ul style="list-style-type: none"> <li>• Firewall</li> <li>• E-Mail Virens scanner (Firewall)</li> <li>• Mailarchivierung</li> <li>• Human Factors</li> </ul>	<ul style="list-style-type: none"> <li>• Sandboxing (Firewall)</li> <li>• URL-Filter (Firewall)</li> <li>• Externer Rechenzentrumsdienstleister</li> </ul>	-
<b>2. Sichere E-Mail Versendung</b>	<ul style="list-style-type: none"> <li>• TLS-Verschlüsselung (Mailserver, Mailclient)</li> </ul>	<ul style="list-style-type: none"> <li>• E-Mail Signaturen /Zertifikate</li> <li>• (Mailserver, Mailclient)</li> </ul>	<ul style="list-style-type: none"> <li>• Verschlüsselte E-Mails versenden (Firewall)</li> <li>• Links statt Dateien versenden</li> </ul>
<b>3. Arbeitsplatzrechner</b>	<ul style="list-style-type: none"> <li>• Virens scanner und Malwareschutz</li> <li>• Lokale Firewall</li> <li>• Zugriffskontrolle</li> <li>• Human Factors</li> </ul>	<ul style="list-style-type: none"> <li>• Endpoint Security</li> </ul>	-
<b>4. Netzinfrastruktur</b>	<ul style="list-style-type: none"> <li>• LAN-Sicherheit</li> <li>• WLAN-Sicherheit</li> </ul>	-	-



	<b>Mindestanforderung</b>	<b>Empfohlen</b>	<b>Erhöhter Schutzbedarf</b>
<b>5. Sicherer Umgang mit mobile Devices</b>	<ul style="list-style-type: none"> <li>• Verhaltensgrundsätze</li> </ul>	-	-
<b>6. Server</b>	<ul style="list-style-type: none"> <li>• Betriebsbedingungen</li> <li>• Betriebskonzept</li> <li>• Ausfallsicherer Festplattenspeicher RAID</li> <li>• Datensicherung und -wiederherstellung</li> </ul>	<ul style="list-style-type: none"> <li>• Virtualisierung und Storage</li> <li>• Rechenzentrumsdienstleister</li> </ul>	

Anhand der Checkliste kann Ihr EDV-Dienstleister ein IT-Assessment durchführen und Lösungsvorschläge für verbesserungsbedürftige Prozesse erarbeiten

Der Vortrag ist online verfügbar:

- [www.arconda.ag](http://www.arconda.ag) - Dokumente – Präsentationen – Zukunftsorientierte IT-Konzepte

# Vielen Dank für Ihre Aufmerksamkeit

**ARCONDA**.systems  
Aktiengesellschaft

**SCHIEBLER**  
Zahntechnik GmbH



11. Februar 2020 EAST Hotel Hamburg