



# 5 aktuelle Risiken

## für die IT-Sicherheit von Unternehmen

Christine Deger, IT-Sicherheitsexpertin

**1****Häufigkeit, Schnelligkeit und Wandelbarkeit:**

Gewisse Bedrohungen gibt es schon lange, darunter Ransomware, Trojaner, Phishing usw. Was sich verändert, ist die Intensität dieser Bedrohungen. Attacken passieren häufiger, sie verbreiten sich in immer schnellerer Geschwindigkeit, und vor allem Schadsoftware und Ransomware sind extrem wandelbar.

**2****Mehr Angriffe von “innen”:**

Neu hinzukommt, dass es häufiger zu Attacken durch ehemalige oder unzufriedene Mitarbeitende gibt. Besonders schützen sollten man seine Daten vor externen Berater und Wettbewerbsunternehmen. Auch Hobby-„Hacker“ greifen Unternehmen an, nicht aus finanziellen Motiven aber um zu zeigen, dass man es einfach kann.

**3****Mehr “versteckte Angriffe”:**

Schadsoftware verhält sich heutzutage unauffällig und passt sich langsam und Schritt für Schritt den Gegebenheiten des Unternehmens an. IT-Kriminelle bieten Malware „as a service“ an, das heißt Malware kann gezielt hergestellt und eingekauft werden und ist dadurch noch mal um einiges wirkungsvoller.

**4****Mehr Schnittstellen:**

Mit IOT (Internet Of Things) vervielfachen sich sowohl privat als auch im beruflichen Bereich die Angriffspunkte. So sind Industrie- und Produktionsanlagen ebenso wie Alltagsgegenstände (Stichwort Smart Home) beliebte Ziele. Häufig fehlt Unternehmen die Übersicht über all diese Schnittstellen und es fehlt die Kapazität, all diese externen Dienstleister zu prüfen.

**5****Veraltete Software, Hardware und Geräte**

Veraltete Software und Hardware, die nicht mehr auf dem aktuellen Stand sind, werden zum Sicherheitsrisiko, weil es keine Patches und Updates mehr gibt. Unternehmen fürchten ein Upgrade – never touch a running system – denn dies erfordert Aufwand, Planung und Konzeption.

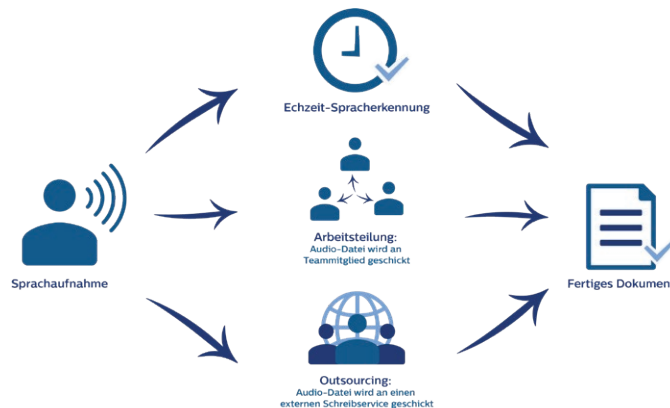
# Sichere Zusammenarbeit im virtuellen Team mit Sprachtechnologie

## 1

### Sprachaufnahme erstellen, zu jeder Zeit und an jedem Ort

Sprachtechnologie, wie zum Beispiel Philips SpeechLive, ist im Aufwind, da es die Effizienz und virtuelle Zusammenarbeit verbessert.

**Warum ist das sicher?** Professionelle Aufnahmegeräte weisen einen ausgeklügelten Geräteschutz auf. Beim "remoten" Arbeiten ist das ein Muss. Philips SpeechLive verschlüsselt die Aufnahme dreistufig, das heißt von der Aufnahme bis zur Übertragung und Speicherung ist höchste Sicherheit gewährleistet.



## 2

### Sprachumwandlung über eine webbasierte Plattform

Mit Philips SpeechLive wandelt Sprache in Text um durch:

- Spracherkennung in Echtzeit
- die automatische Weiterleitung an ein Teammitglied
- Outsourcing an einen Schreibservice

**Warum ist das sicher?** Philips SpeechLive speichert die Aufnahmen auf redundanten Servern, in der Europäischen Union. Dadurch ist die Lösung DSGVO-konform und Sie haben immer Zugriff auf Ihre Daten. Zudem trennen wir Diktatdaten von Benutzerdaten, diese werden in einem Hochsicherheitsserverzentrum in Österreich gespeichert.

## 3

### Fertiges Dokument zur weiteren Verarbeitung

**Warum ist das sicher?** Philips SpeechLive als Cloud-Lösung ist immer up to date, das heißt der Benutzer muss sich um die Sicherheitsstandards nicht kümmern. Dennoch gibt es maximale Entscheidungsfreiheit. So können Diktate und Aufnahmen jederzeit heruntergeladen oder gelöscht werden und keine Daten verbleiben in der Cloud.

## Unser Angebot

Testen Sie Philips SpeechLive 30 Tage kostenlos!

- + Keine komplexen Installationsprozesse
- + Zugriff auf alle Ihre Dateien überall
- + Sofort und standortunabhängig arbeiten
- + Mit dem Mobiltelefon nutzbar
- + MAC-kompatibel
- + On-Screen Spracherkennung inklusive

Schreiben Sie uns eine E-Mail an [info.isr@speech.com](mailto:info.isr@speech.com) mit dem Kennwort „IT Sicherheit ist Chefsache: 30 Tage Philips SpeechLive“!