PHILIPS

Diktieren

Schwerpunkt Sicherheit:
So schützen Sie sensible Daten

Die Digitalisierung schreitet in vielen Unternehmen voran und das hat zahlreiche Vorteile; verbesserter und schneller Service, Flexibilität und unternehmerische Agilität sind nur einige davon. Diese Vorteile sind jedoch mit Risiken verbunden. Je digitaler das Unternehmen, desto wahrscheinlicher werden Sicherheitsprobleme, sei es durch eigene Nachlässigkeit oder Angriffe von Cyberkriminellen. Abgesehen von einem finanziellen Schaden führt dies langfristig zur Rufschädigung und einem Vertrauensverlust. Um sensible Informationen zu schützen und gleichzeitig mit den Anforderungen der Kunden Schritt zu halten, ist es entscheidend, die Datensicherheit Ihres Unternehmens speziell in diesen sechs Bereichen zu prüfen:

1

Verschlüsselung

Dies ist grundlegend für den Schutz persönlicher Informationen vor Cyberkriminellen. Durch die Kombination von Geräten und Anwendungen mit mehreren Verschlüsselungsebenen wird ein sicherer End-to-End-Pfad zwischen Hardware und Software für die sichere Übertragung und gemeinsame Nutzung von Daten geschaffen.

2

Überlegungen zur Mobilität

Mobilität ist Trend unter Mitarbeitern, die regelmäßig firmeneigene oder „BYOD“ (Bring Your Own Device)-Smartphones und Tablets benutzen. Verhindern Sie, dass mobile Geräte zum Einfallstor werden, indem Sie Sicherheitsmerkmale wie Echtzeit-Verschlüsselung und die Nutzung virtueller privater Netzwerke (VPN) für WiFi-Verbindungen einsetzen.

Cyberkriminalität steigt

PWC stellte in der Fraud Survey 2020 unter über 5.000 Teilnehmern fest, dass 34% der befragten Unternehmen in den letzten 24 Monaten Opfer von Cyberkriminalität wurden. Die Tendenz steigt. Besonders betroffen sind Technologie-Unternehmen, Finanzdienstleister wie zum Beispiel Banken, die öffentliche Verwaltung und Regierungen aber auch zunehmend das Gesundheitswesen.

Vorsicht vor Cybercrime in Zeiten von COVID-19

In Zeiten der globalen Pandemie COVID-19, in der viele Menschen weltweit um Ihre Gesundheit besorgt sind, ist auch ein Anstieg von Cybercrime zu beobachten. Einerseits, weil viele Mitarbeiter zu Hause arbeiten und andererseits, weil die Unsicherheit von Menschen ausgenutzt werden kann. Im Umlauf sind z.B. Fake-Websites zum Medikamentenkauf, Fake-E-Mails, dass man für Homeoffice Software downloaden sollte oder dergleichen. Vorsicht ist geboten!

3

Zugriffsverwaltung

Sie sollten mittels PIN oder biometrischen Daten geschützte Geräte, rollenbasierte Berechtigungen für verschiedene Anwendungen und Anforderungen an die Komplexität von Passwörtern beachten. Wenn Sie neue Technologien in Ihrem Unternehmen einführen, ist es wichtig, nach Lösungen zu suchen, die mit dieser Art von Funktionalitäten integriert oder kompatibel sind.

4

Cloud ermöglicht Sicherheit

Höhere Sicherheit ist einer der Hauptgründe, warum immer mehr Daten in der Cloud gespeichert werden. Da Cloud-Dienste in der Regel komplexere Sicherheitsmechanismen als lokale Server verwenden, bieten sie ein zusätzliches Maß an Schutz.

5

Sicherheitsstandardisierung

Konsistenz in den Sicherheitsverfahren und -anforderungen verbessert die Sicherheitslage eines jeden Unternehmens. Es braucht formalisierte Standards und die konsequente Einhaltung dieser. Agiert man in Sicherheitsfragen ad-hoc, sind diese Praktiken oft nicht robust genug, um sich gegen Cyber-Angriffe zu schützen.

6

Befähigung der Mitarbeiter

Schließlich sind die Mitarbeiter, unabhängig davon, wie sicher Technologien sind, immer noch der Schlüssel zur Wahrung des Datenschutzes und der Vertraulichkeit. Durch die Ausstattung der Teams mit regelmäßig aktualisierten Schulungs- und Ausbildungstools sowie durch die Einhaltung von Compliance-Anforderungen wird die Eigenverantwortung für den Schutz sensibler Informationen gestärkt.

Benötigen Sie weitere Informationen darüber, wie Sie Ihre Kunden und die Daten Ihrer Firma schützen können?

Besuchen Sie die Website von Philips Dictation oder senden Sie uns eine E-Mail an info.isr@speech.com, um mehr über sichere, hochmoderne Sprache-zu-Text-Lösungen zu erfahren.