PHILIPS

Dictation

Sicherheit: So wird Ihr Team exzellent beim Schutz sensibler Daten

Die Digitalisierung schreitet voran. Besserer Kundenservice, unternehmerische Agilität, flexiblere Arbeitsweisen, die die Motivation und Produktivität von Teams steigern – das sind nur einige der vielen Vorteile. Doch die neue Arbeitswelt birgt Risiken, speziell was die Datensicherheit betrifft. Je digitaler das Unternehmen, desto wahrscheinlicher werden Sicherheitsprobleme, sei es durch Nachlässigkeit von Mitarbeitern oder den gezielten Angriff durch Cyberkriminelle. Für das Unternehmen ist der Schaden groß: finanziell aber auch was Reputation und Vertrauen betrifft. Um sensible Daten zu schützen, sind auch Führungskräfte gefordert.

Dieser Quick-Guide hilft, den Status Quo in Sachen Datensicherheit Ihrer Teams in 5 Bereichen unter die Lupe zu nehmen:

1

Mobilität

Schon vor COVID-19 gab es einen Trend zum mobilen Arbeiten. Dieser wird nun verstärkt. Mobile Geräte können zum Einfallstor für Cyberkriminelle werden. Arbeitet Ihr Team oft mobil, sollten Sie über Tools für Dokumentation und Datentransfer nachdenken, die Sicherheitsmerkmale wie Echtzeit-Verschlüsselung und die Nutzung virtueller privater Netzwerke (VPN) für WiFi-Verbindungen einsetzen. Mittels PIN oder biometrischen Daten geschützte Geräte, rollenbasierte Berechtigungen für verschiedene Anwendungen und Anforderungen an die Komplexität von Passwörtern sind schlagkräftige Möglichkeiten, die Datensicherheit zu erhöhen.

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, die öffentliche Verwaltung 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!

2

Cloud ermöglicht Sicherheit

Da Cloud-Dienste in der Regel komplexere Sicherheitsmechanismen als lokale Server verwenden, bieten sie ein zusätzliches Maß an Schutz. Unabhängig davon, wo Ihr Team arbeitet, erhalten sensible Kundendaten auch immer denselben hohen Schutz.

3

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. Für Führungskräfte gilt: Im gesamten Team müssen dieselben Regeln und Anweisungen gelten und eingehalten werden.

4

Befähigung der Mitarbeiter

Mitarbeiter sind 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. Stellen Sie sicher, dass Ihr Team immer auf dem neuesten Stand ist und kommunizieren Sie interne Guidelines klar und verständlich.

5

Selbst Vorbild sein

Vergessen Sie als Führungskraft nicht Ihre Vorbildfunktion. Jeder kennt das Sprichwort, Wasser predigen und Wein trinken. Ihr Team muss mitbekommen, dass Sie Datensicherheit selbst wichtig nehmen und die Regeln befolgen.

Benötigen Sie weitere Informationen darüber, wie Sie und Ihr Team Daten Ihrer Kunden 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.