Initiative Bundesverband Deutscher Rechenzentren
Bienengarten 4
D-56295 Kerben
www.german-cloud.de

Finger weg von unseren Firmendaten!

Patientendaten verkauft – wie kann sich der Mittelstand vor derartigen Gefahren schützen?

Immer öfter kommen Datenklau-Skandale ans Tageslicht. Diese Vorgänge übertreffen sich an Dreistigkeit. Die Verantwortlichen gehen in mit sensiblen Daten um, als wären es die eigenen. Auf der anderen Seite helfen Skandale dem Mittelstand dabei, vorbeugende Maßnahmen zu treffen. Im aktuellen Fall wurden 42 Millionen Patientendaten in kaum verschlüsselten Zustand verkauft. Wie kann der Mittelstand verhindern, dass dies mit seinen Clouddaten passiert?

Wer ist Herr der Schlüssel?

Erstens sollten Firmendaten natürlich in Deutschland gespeichert werden, um schon einmal die Grundsicherung in Sachen Datenschutz und Datensicherheit zu haben. Sie geben also ihre Daten in die Cloud. Der Cloudanbieter versichert Ihnen, dass er eine gute Verschlüsselung verwendet, die selbst bei illegalem Datenklau die Sicht auf die Rohdaten verhindert. Doch was nützt es, wenn der Cloudanbieter Ihre Firmendaten verschlüsselt ablegt? Der Kunde muss der Herr der Schlüssel sein. Der Cloudanbieter soll gar nicht wissen, was sich in seinen Speichern befindet.

Deutsche Schlüssel sind die besten

Die Prism-Affäre hat uns gezeigt, dass die führenden amerikanischen Anbieter von Verschlüsselungs-Lösungen mit den Schnüffelbehörden zusammenarbeiten. Also ist es empfehlenswert, auch hierfür deutsche Anbieter zu suchen. Die Kryptierung muss also nicht nur End-to-End erfolgen. Das bedeutet, nicht nur, dass alle Daten die PCs und Server über ein Verschlüsselungs-Gateway verlassen und autorisierte Empfänger diese empfangen, sondern auch, dass man besser ein deutsches Produkt zum Einsatz bringt.

Standard PC-Wissen bei Mitarbeitern erweitern

So wie die Beschäftigten heute sicher mit den ERP- und Office Anwendungen umgehen können müssen, so selbstverständlich muss der sichere Umgang mit Daten in Fleisch und Blut übergehen. Wenn man schon Weiterbildungsmaßnahmen dazu einleitet, sollte man das Verhalten grundsätzlich für Informationssicherheit trainieren. Denn was nützt es, wenn die Firmengeräte sicher genutzt werden und gleichzeitig der Umgang mit dem privaten Smartphone (ein Computer, der so tut, als wäre er ein Telefon) Tür und Tor zum Datenmissbrauch bietet?

Informationssicherheit und Compliance gehören zusammen

Compliance und Informationssicherheit sind im Mittelstand noch kein Breitenthema (Informationssicherheit ist nicht IT-Sicherheit!). Doch ein geschulter Firmen-Codex tut Not. Denn wenn erst Image oder Reputation aufgrund von Datenproblemen gelitten haben, ist es zu spät. Deshalb empfiehlt Götz Piwinger, Gründer der Initiative GERMAN CLOUD für sichere Firmendaten folgenden Projektplan für den Weg in die Cloud:

1. Unternehmensziele analysieren
2. Ggf. Wertesystem in Sachen Informationssicherheit ergänzen
3. Alle IT-Anwendungen auf Cloudfähigkeit und möglichen Performancegewinn prüfen
4. Potentielle Gefahrenquellen identifizieren
5. Investitions- und Liquiditätsverbesserung prüfen
6. Geeignete Cloud- und Verschlüsselungsanbieter als Partner identifizieren
7. Prozesse, Leistungskataloge und Servicevereinbarungen in Firmenprozesse aufnehmen
8. Kampagne zur Informationssicherheit und Compliance (Infopliance) im Unternehmen starten
9. Umsetzung starten

Gemeinsam geht's besser!

Die sichere Umsetzung von Cloudstrategien gehört nicht zum Kerngeschäft des Mittelstandes. Deshalb ist es sinnvoll, sich fernab von Standardseminaren und Angstmachern in eine Gemeinschaft von Gleichgesinnten zu begeben und eine neutrale Stelle, wie die Experten GERMAN CLOUD für die Begleitung einzuplanen.

Kontakt:

GERMAN CLOUD
info@german-cloud.de
Universitätsstraße 3
56070 Koblenz