



Götz Pwinger
Geschäftsführer GERMAN CLOUD



meine Firmendaten bleiben in Deutschland!

Großangriff auf die Daten des Deutschen Mittelstands

Welche Auswirkungen hat die „PRISM-Affäre“ auf Deutsche Unternehmen?

PRISM ist ein seit dem Jahr 2007 existierendes, als streng geheim eingestuftes und von der US-amerikanischen National Security Agency (NSA) geführtes Programm zur Überwachung und Auswertung von elektronischen Medien und elektronisch gespeicherten Daten. Daran wirken folgende Internetunternehmen mit: Microsoft (incl. Skype), Google, Facebook, Yahoo, Paltalk, AOL und Apple. Dabei kann auf Kommunikationsdaten und gespeicherte Informationen von Privatpersonen und Unternehmen ohne Zustimmung der Beteiligten zugegriffen werden. Dies betrifft E-Mails, Webkonferenzen, Daten in der Cloud, Videos. Über die Funktionsweise von PRISM ist nicht bekannt. Deshalb leiben Fragen offen, ob PC-Mikrofone oder –Kameras ebenfalls betroffen sind. Wir müssen davon ausgehen, dass asiatische Anbieter ähnliche Verfahren eingerichtet haben.

Was kann meinem Unternehmen passieren?

Deutschland ist das Land der Ideen, Patente und guter Prozesse. Der Mittelstand lebt von seinem Spezialwissen. Wenn in der Kommunikation mit Geschäftspartnern Daten in Form von Grafiken, Bildern oder technischen Daten über einen der genannten Anbieter ausgetauscht werden, besteht Gefahr. Rund 70% aller deutschen Unternehmen wurden bereits Opfer von Internetangriffen. Wichtig: Technischer Schutz reicht nicht aus! Ergänzend müssen Unternehmen auf ihre Prozesse, Lieferanten und Mitarbeiter achten. Denn künftig werden die Angreifer in der Lage sein, die vielen legal und illegal gespeicherten Daten zu vernetzen (Big Data Mashup). So können eindeutige Profile über Produkte, Know-How, Passwörter und Personen erstellt werden. Wo die geklauten Erkenntnisse landen weiß niemand. Aber eines ist klar: Sobald sich ein ausländisches Unternehmen für Ihre Branche interessiert, sich beispielsweise mit der Produktion ähnlicher Erzeugnisse beschäftigt und dafür Know-How und Kundenadressen sucht können sie sicher sein, das in diesem Fall sehr genau „recherchiert“ wird. Daraus sind heute entsprechende Maßnahmen abzuleiten.

Trau, schau, wem! Wie kann ich meine Daten vor Fremdzugriffen schützen?

Sich für einen vertrauenswürdigen Anbieter entscheiden

Das Deutsche Bundesdatenschutzgesetz verbietet Internetfirmen die Weitergabe persönlicher Daten an Dritte. Darüber hinaus ist auf die ergänzende Datensicherheit zu achten. Darin sind extern gespeicherte und extern verarbeitete Daten zu schützen. Das bedeutet: Wenn sein Anbieter sich dem Deutsche Datenschutz verpflichtet, ist dies ein wichtiger Schritt, doch für Unternehmen nicht ausreichend. German Cloud hat es sich zur Aufgabe gemacht, Unternehmensdaten zu schützen. Sichere Anbieter zertifizieren sich mit dem Qualitätssiegel „German Cloud“. Daran können Unternehmen erkennen, ob sein Cloud-Anbieter die entsprechenden Standards für Datenschutz und Datensicherheit gewährleisten kann. Damit ist der Punkt „Vertrauensvoller Cloud-Lieferant“ gesichert.



Götz Pwinger
Geschäftsführer GERMAN CLOUD



meine Firmendaten bleiben in Deutschland!

Mitarbeiter sensibilisieren

Eine weitere Maßnahme ist die Sensibilisierung der Mitarbeiter im Umgang mit Firmendaten (Nach dem Motto: „Ich schicke ihnen das Diagramm grad mal von meinem Iphone zu..“). Es ist erstaunlich, welche Informationen unsere Spezialisten erhalten, wenn sie Daten einzelner Personen aus sozialen Netzwerken, App-Datenabruf und einen beauftragten Hack herausfinden! Im aktuellen Fall ging es um eine Gruppe von Softwareentwickler in einem Unternehmen. Es dauerte nur eine Stunde, um herauszufinden, an welchen Produkten mit welcher Technologie und welchem Ziel gearbeitet wurde. Je nach Wert einer Information gehen Profis noch weiter. Sie gelangen über die Vorlieben einer Person in persönlichen Kontakt (social engineering). Angreifer nutzen dafür natürliche menschliche Reaktionen aus, positive Eigenschaften wie Hilfsbereitschaft, Kundenfreundlichkeit, Dankbarkeit, Stolz auf die Arbeit und das Unternehmen oder weniger positive Aspekte wie Gutgläubigkeit, Respekt vor Autoritäten oder gar Bestechlichkeit, ein Blick in die Schufadatenbank genügt. Um dem zu begegnen, bieten sich entsprechenden Weiterbildungsmaßnahmen an.

Verfahren und Prozesse wasserdicht machen

Der Unternehmen beziehungsweise Geschäftsführer haftet persönlich für Vergehen gegen das Bundesdatenschutzgesetz. Datenpannen sind zu veröffentlichen. Am 12. Oktober 2012 musste das Klinikum Mittelbaden bekanntgeben (Frankfurter Rundschau), dass Datensicherungsbänder mit Patientendaten, Befunden etc. verschwunden sind. Deshalb ist es wichtig, die internen Prozesse regelmäßig zu überprüfen und eindeutige (interne) Services zu definieren. Denn das Bundesdatenschutzgesetz gilt für Unternehmen jeder Größe und Branche. Wenn keine internen Profis verfügbar sind, helfen hierbei zertifizierte Datenschützer.

Kontakt:

German Cloud
Universitätsstrasse 3
D-56070 Koblenz
info@german-cloud.de