

## Beispiel-Unternehmen: Example CreditCard Service GmbH aus Berlin

### Geschäftsfeld

- Tokenization  
(Speicherung von Karteninhaberdaten als externe Dienstleistung für Unternehmen)

### Abteilungen

- Geschäftsführung inklusive Vertrieb (2 Personen)
- Buchhaltung und Sachbearbeitung (3 Vollzeit- und eine Teilzeitkraft)
- Software-Entwicklung (6 interne und 2 externe Software-Entwickler)
- IT-Administration (3 Admins, 1 Werkstudent)

### Externe Dienstleister

- Reinigungsunternehmen für das Büro
- Steuerberater (Buchhaltung, Lohnabrechnung)
- Externer Datenschutzbeauftragter (mehr formal als real)

### Personalführung

- 2 Geschäftsführer und aus jeder Abteilung ein Teamleiter

### Weiterbildungsmaßnahmen

- On-the-job training

### Security Management

- IT-Sicherheitsbeauftragter ist der Teamleiter Softwareentwicklung
- Dokumentation (Richtlinien, Standards, usw.) besteht primär aus einem Wiki mit allgemeineren Security Best Practices

### IT-Infrastruktur

- Alles innerhalb der Büroräume. Keine Videoüberwachung oder elektronisches Schließsystem.
- Standleitung nach außen; Firewall/Router vorhanden; von innen alles erlaubt, von außen auf notwendige Verbindungen eingeschränkt
- Unterteilung in zwei interne Netze: Office-Clients und Server (nur Webserver mit Apache und Datenbanken mit MySQL für den Tokenization-Service und diverse Server für die Büroinfrastruktur)
- Karteninhaberdaten werden base64 kodiert/verschlüsselt in einer SQL Datenbank hinterlegt
- Tokenization-Service ist extern über TLS erreichbar
- Auf den Clients laufen einzelne Viren-Scanner

### Prozesse

- IT-Administratoren verwalten Server
- Interne Softwareentwickler deployen Software nach Rücksprache mit dem Softwareentwickler-Teamleiter; die externen Entwickler haben keinen Zugriff
- Change-Management wird mündlich realisiert

### PCI Zertifizierung

- **nicht vorhanden, aber angestrebt**