Zentrum für Informations- und Medientechnik
Internet: www.its-stuttgart.de
E-Mail: IT-Schule@stuttgart.de
Tel: 0711-216 89 234
Fax: 0711-216 89 279

Sie haben Ihre Ausbildung bei der IT Sol GmbH begonnen.

Für die IT Sol GmbH ist die Informationssicherheit aus verschiedenen Gründen von besonderer Bedeutung.

Zunächst einmal kann jedes kleinste Sicherheitsleck das gute Unternehmensimage schädigen. Es kommt immer wieder vor, dass Sicherheitsvorfälle ein Unternehmen ruinieren.

Ein Beispiel hierfür ist der Cyberangriff in den USA. Hierbei wurde nach einem Hackerangriff bei Kunden des US Dienstleisters Kaseya eine Erpressungssoftware in mindestens 17 Ländern entdeckt. Eine schwedische Lebensmittelkette musste deshalb hunderte Filialen schließen, weil deren Kassen nicht mehr funktionierten. Die Opfer wurden aufgefordert, Lösegeld zu zahlen, damit ihre gesperrten Computer wieder freigegeben werden. (vgl. Tagesschau vom 04.07.21: https://www.tagesschau.de/wirtschaft/unternehmen/cyberangriff-unternehmen-weltweit-101.html)

Außerdem bietet die IT Sol GmbH ihren Kunden eine Reihe von Sicherheitslösungen an. Der Sicherheitsmarkt wächst stetig, liegt derzeit um über 10% jährlich, und die IT Sol GmbH möchte die Wachstumschancen nutzen und sich wichtige Marktanteile sichern.

In diesem Bereich hat die IT Sol GmbH mit vielen eigenen und fremden Datenbanken und Vernetzungen ihrer Kunden zu tun. Täglich werden Hunderttausende Malwareangriffe auf Unternehmen gerichtet, die meisten dauern nur wenige Sekunden. Schon ein Angriff kann aber verheerende Folgen habe, wie das Beispiel des Software-Dienstleisters Kaseya zeigt.

Das Sicherheitsmanagementsystem ist demnach besonders wichtig. Jeder Mitarbeiter muss sensibilisiert und über mögliche Gefährdungen informiert sein. Angriffsmöglichkeiten müssen sofort erkannt werden, um schnell Maßnahmen einleiten zu können und Notfallmaßnahmen parat zu haben.

Der Staat hat strenge Gesetze erlassen und nimmt Unternehmen in die Pflicht, die IT-Sicherheit für diese und deren Kunden zu gewährleisten.

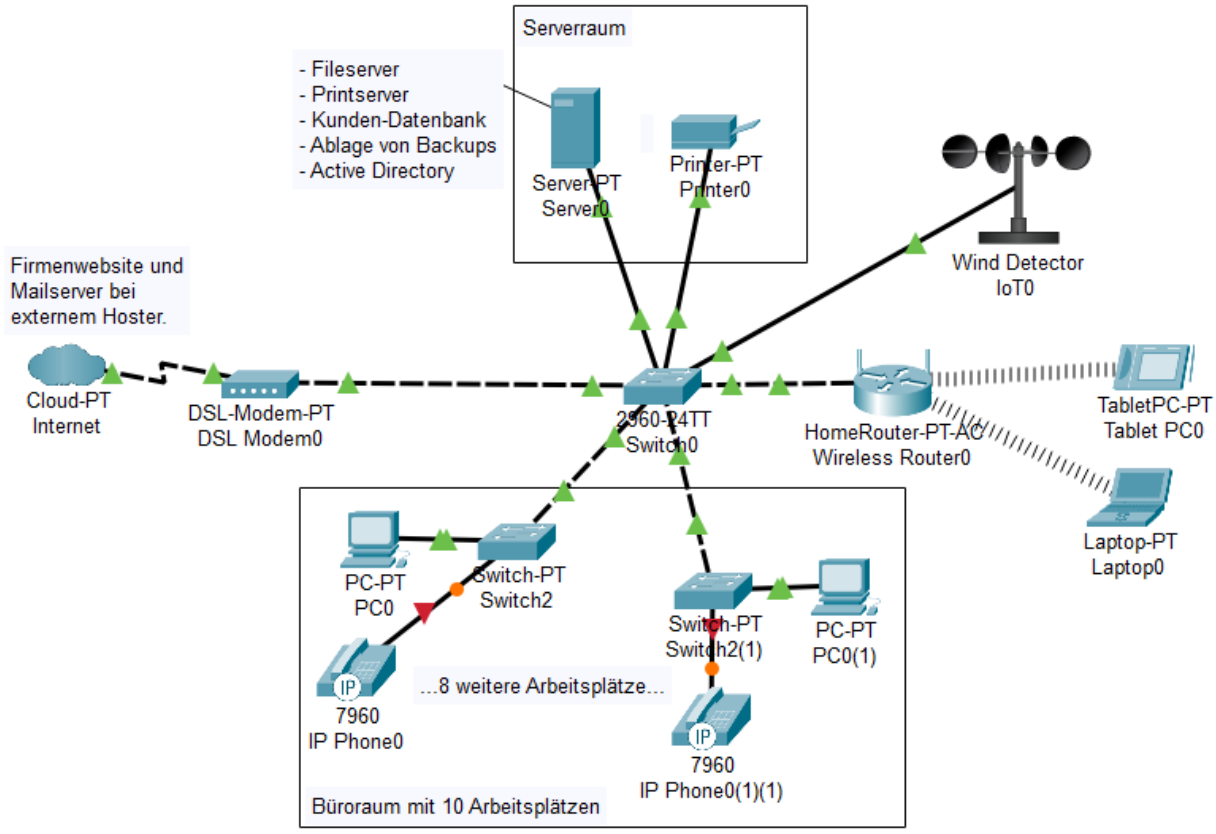
Daher hat sich die IT Sol GmbH als Ziel gesetzt, das sicherste Systemhaus für seine Kunden und Mitarbeiter zu sein. Um dieses Ziel zu erreichen strebt das Unternehmen eine Grundschutz Zertifizierung ISO 27001 nach BSI an. Hierfür sind sowohl technische als auch organisatorische Maßnahmen, kurz TOM genannt, zu ergreifen und in einer vorgeschriebenen Weise zu dokumentieren.

Sie erhalten nun den Auftrag, den IT-Sicherheitsbeauftragten zu unterstützen und die Zertifizierung vorzubereiten.

Da die Unternehmen hinsichtlich Organisation, Geschäftsprozessen und IT-Systemen doch sehr unterschiedlich aufgestellt sein können, bietet sich das BSI als mögliche Informationsquelle an. Das BSI sieht eine systematische Erarbeitung eines Sicherheitskonzepts auf Basis einer Sicherheitsleitlinie vor. Im ersten Schritt sollen nun die wichtigsten technisch-organisatorischen Maßnahmen auf Grundlage des BSI zusammengestellt und unterschieden werden.

Zentrum für Informations- und Medientechnik
Internet: www.its-stuttgart.de
E-Mail: IT-Schule@stuttgart.de
Tel: 0711-216 89 234
Fax: 0711-216 89 279

Das Bild unten zeigt den Aufbau des Netzwerks der IT Sol.



Um sich über das Thema und das Vorgehen zu informieren, stehen ihnen die Datei „BSI-Standard_1002.pdf“ und weiteres Material im Infopool zur Verfügung. Bearbeiten sie (nach Wunsch auch im Team) die untenstehenden Arbeitsaufträge.

Aufträge

1.1 Erklären Sie die Begriffe Vertraulichkeit, Integrität und Verfügbarkeit und deren Zusammenhang im CIA-Modell.

1.2 Erstellen Sie eine Übersicht über die Objekte (Geräte, Daten, Zugänge). Welchen Schutz benötigen diese bzgl. Vertraulichkeit, Integrität und Verfügbarkeit?

1.3 Erstellen Sie eine Präsentation Ihrer Zusammenstellung

2. Definieren Sie die folgenden Schutzbedarfskategorien. Was bedeutet Schutzkategorie…
   …“normal“,
   …“hoch“,
   …“sehr hoch“ für ihren Betrieb.

Zentrum für Informations- und Medientechnik
Internet: www.its-stuttgart.de
E-Mail: IT-Schule@stuttgart.de
Tel: 0711-216 89 234
Fax: 0711-216 89 279

3. Schutzbedarfsfeststellung für Anwendungen
   „Was wäre wenn…?“ Schätzen Sie für die aufgelisteten Geräte ein: Welche Anwendungen laufen darauf und welche Schadensszenarien können auftreten? Dokumentieren Sie Ihre Ergebnisse

4. Schutzbedarfsfeststellung für IT-Dienste / IT-Services im Unternehmen
   Gehen Sie wie bei Aufgabe 3 vor und erstellen Sie eine entsprechende Feststellung für die IT-Systeme und Dienste in dem Unternehmen.

5. Schutzbedarfsfeststellung für Räume
   Nehmen Sie sich nun die einzelnen Räume vor und bearbeiten Sie folgende Unterpunkte:
   - Physische Zugangssicherung Serverraum / Vereinzelungsschleusen
   - Zugriff auf ein Terminal
   - Zugriff auf Schrank mit Backups
   - Aktenschrank (Papierform)

6. Welche weiteren Aspekte müssen Sie bei der Schutzbedarfsfeststellung beachten, die nicht in den vergangenen Aufgaben vorkamen? Legen Sie ein besonderes Augenmerk auf die Kommunikationsverbindungen.

7. Ermitteln Sie die Bausteine, die das BSI passend für die hier geschilderte Problemstellung vorgesehen hat. Füllen Sie die vorgesehene Checklisten entsprechend des Bedarfs aus.