

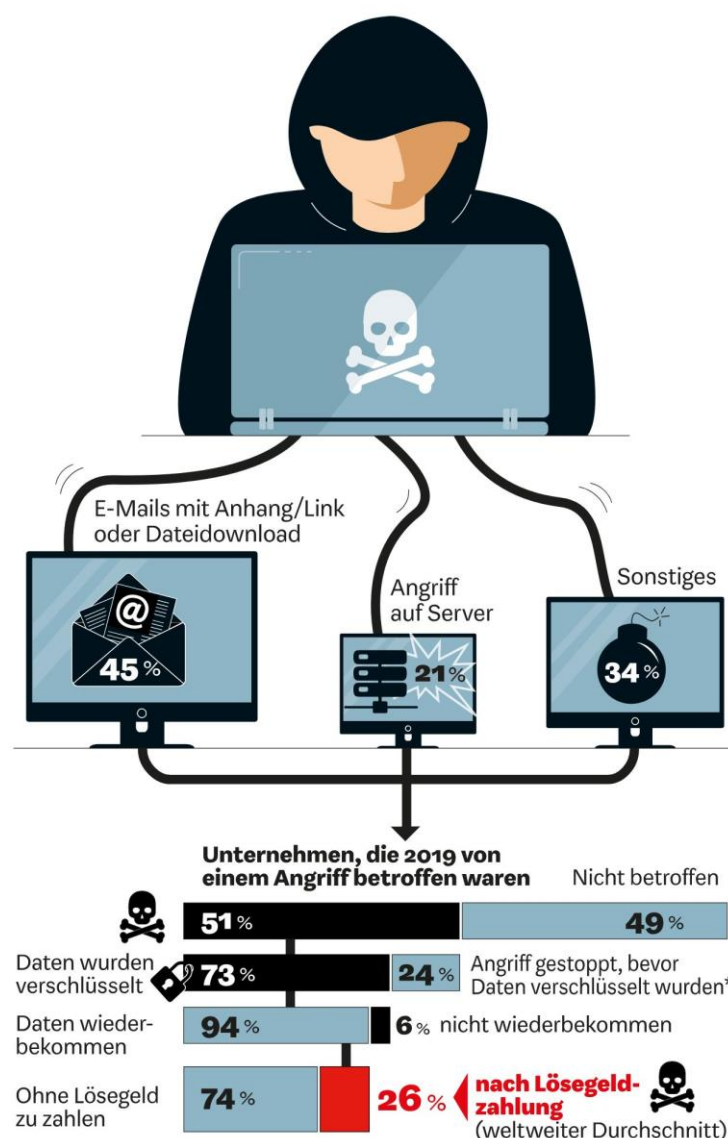
Sie haben Ihre Ausbildung bei der IT Sol GmbH begonnen. Für die IT Sol GmbH ist die Informationssicherheit aus verschiedenen Gründen von besonderer Bedeutung.



Zunächst einmal kann jedes kleine Sicherheitsleck das gute Unternehmensimage schädigen. Es kommt zudem immer häufiger vor, dass Sicherheitsvorfälle ein Unternehmen ruinieren, da sie zum Angriffsziel fremder Geheimdienste oder anderer Unternehmen werden, die ihre Konkurrenz illegal ausspionieren, um sich einen Wettbewerbsvorteil zu verschaffen.

Ein Beispiel ist der Cyberangriff in den USA. Hierbei wurde nach einem Hackerangriff bei Kunden des US Dienstleisters Kaseya eine Erpressungssoftware (Ransomware) 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>)




Sicherheitsbehörden warnen immer wieder davor, auf Lösegeldforderungen der Hacker einzugehen. Doch ein Viertel der Unternehmen weltweit zahlt das Geld, zeigt die nebenstehende Infografik (Wirtschaftswoche 16.06.2020).

Die Vorfälle zeigt, wie angreifbar eine vernetzte IT-Infrastruktur mit einer Sicherheitslücke sein kann und welche mitunter weltweiten Auswirkungen dies haben kann.

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.

Sie erhalten nun den Auftrag, sowohl technische als auch organisatorische Maßnahmen zu ergreifen und in einer vorgeschriebenen Weise zu dokumentieren.

	BfK-B	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
	Datensicherheit - Schutzbedarfsanalyse	

Arbeitsaufträge:

- 1) Geben Sie einfache Maßnahmen zur Gewährleistung der Datensicherheit an, die Privatpersonen zu Hause bzw. Mitarbeiter eines Unternehmens durchführen sollten.

- 2) Welche Maßnahmen sollte ein Unternehmen selbst zusätzlich realisieren?

Primäre Schutzziele:

1. Vertraulichkeit „Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.“

2. Integrität „Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen.“

3. Verfügbarkeit „Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT- Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.“

Erweiterte Schutzziele:

1. Authentizität „Mit dem Begriff Authentizität wird die Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden. Der Begriff wird nicht nur verwendet, wenn die Identität von Personen geprüft wird, sondern auch bei IT-Komponenten oder Anwendungen.“

2. Nichtabstreitbarkeit „Bei der Nichtabstreitbarkeit liegt der Schwerpunkt auf der Nachweisbarkeit gegenüber Dritten. Ziel ist es zu gewährleisten, dass der Versand und Empfang von Daten und Informationen nicht in Abrede gestellt werden kann.“

3. Verbindlichkeit „Unter Verbindlichkeit werden die Sicherheitsziele Authentizität und Nichtabstreitbarkeit zusammengefasst. Bei der Übertragung von Informationen bedeutet dies, dass die Informationsquelle ihre Identität bewiesen hat und der Empfang der Nachricht nicht in Abrede gestellt werden kann.“

4. Zuverlässigkeit Das Schutzziel der Zuverlässigkeit bezieht sich auf die technische Funktionsfähigkeit von IT-Systemen und Komponenten und kann daher in Szenarien hoher Abhängigkeit von IT-Systemen zusätzlich zum Schutzziel der Verfügbarkeit betrachtet werden.