Sachverhalt:

Nachdem Sie sich über die gesetzlichen Grundlagen zum Datenschutz informiert haben und die Aufgabenbereiche des Datenschutzbeauftragen und des IT-Sicherheitsbeauftragten gegeneinander abgegrenzt wurden, widmen Sie sich nun dem Thema “Security Threats and Vulnerabilities“.

Aufgabe: Informieren Sie sich über Sicherheitsbedrohungen und Schwachstellen in der Informationstechnologie. Ergänzen Sie die Tabelle in der die Sicherheitsbedrohungen und Schwachstellen auflisten sind, indem Sie diese kurz erklären und dazu jeweils geeignete Schutzmaßnahmen nennen.

Sicherheitsbedrohungen	**Erklärung**	**Schutzmaßnahme**
Informationsdiebstahl	Informationsdiebstahl ist Einbruch in einen Computer, um an vertrauliche Informationen zu gelangen (z.B. Forschungs- und Entwicklungsdaten).	- Gesicherte Verbindungen (SSL, SSH) - Zugriffsberechtigungen (AAA, auf das Dateisystem)
Datenverlust und –manipulation	Datenverlust und -manipulation tritt auf, wenn jemand in einen Computer einbricht, um Datensätze zu zerstören oder zu verändern.	- Datensicherung - Zugriffsberechtigungen (AAA, auf das Dateisystem) - Virenscanner
Identitätsdiebstahl	Identity theft ist eine Form des Informationsdiebstahls, bei der persönliche Informationen gestohlen werden, um die Identität einer Person zu übernehmen (z.B. Kreditkarteninformationen).	- Verschlüsselung
Dienstunterbrechung	Die Unterbrechung des Dienstes hindert rechtmäßige Nutzer daran, auf die ihnen zustehenden Dienste zugreifen zu können (z.B. DoS).	- Firewalls - IDS/IPS - End-Point-Security

Schwachstellen	**Erklärung**	**Schutzmaßnahme**
Technologische Schwachstellen	- Schwachstellen in der Funktionsweise von Protokollen - Schwachstellen in Betriebssystemen - Schwachstellen in Netzwerkgeräten	- Auswahl der verwendeten Techniken und Protokolle nach „Stand der Technik“ - Regelmäßige Updates, (Patche und Upgrades - Getestete und zertifizierte Hardware
Schwachstellen in der Konfiguration	- Unsicher gespeicherte oder übertragende Benutzerkonten - Einfache Kennwörter - Fehler in der Konfiguration von Internetdiensten - Unsichere Standardeinstellungen - Falsch oder schlecht konfigurierte Netzwerkgeräte	- Schulungen für alle Mitarbeiter - Kennwortrichtlinien - Qualifiziertes Personal (gut Schulen) - Nicht unter Zeitdruck konfigurieren - Konfigurationen ausführlich testen - Änderungen protokollieren und dokumentieren
Schwachstellen in den Richtlinien	- Fehlende schriftliche Sicherheitsrichtlinien - Unbedarfte oder nachlässige Firmenpolitik - Fehlende Kontrollen und Überprüfungen - Missachtung von Vorgaben - Fehlende Backup-Strategie	- Vorgaben erstellen und regelmäßig aktualisieren - Die Einhaltung der Vorgaben überprüfen und durchsetzen - Gute Backup-Strategien erstellen und Worst-Case-Szenarien simulieren