Name des/der Auszubildenden:	Mustermann, Max
Datum:	01.08.2021
Thema des Fachberichts	Softwarearten

Softwarearten

Software steht in der Computertechnik für Programme und Betriebssysteme, die in einem digitalen Speicher abgelegt werden können. Es befinden sich verschiedene Softwarearten im Umlauf, die nicht immer klar voneinander abzugrenzen sind. Im Folgenden wird eine Übersicht über die verschiedenen Begrifflichkeiten gegeben.

Paketierte Software (usw. Standardsoftware)

Das Besondere bei dieser Form von Programmen ist, dass sie bereits fertig gebaut und nicht mehr für den Kunden spezifisch angepasst werden. Die Herausforderung bei der Programmierung ist hier, dass diese Computer Programme auf unterschiedlichsten Rechnern mit unterschiedlichsten Konfigurationen installiert werden.

Unternehmens- / Beratungs-Software fällt zum Teil auch in den Bereich paketierter IT Systeme. Hierbei werden bereits paketierte Programme an Unternehmen angepasst.

Bei paketierter Software handelt es sich in der Regel um proprietäre Software. Die Weiterverbreitung oder Veränderung dieser Software ist verboten oder es wird eine Erlaubnis benötigt.

Open Source und Freie Software

Bei Open Source und Freier Software handelt es sich um Software, die mit der Erlaubnis für jeden verbunden ist, sie zu benutzen, zu kopieren und zu verbreiten, entweder unverändert oder verändert, entweder gratis oder gegen ein Entgelt. Im Besonderen bedeutet das, dass der Quellcode verfügbar sein muss. Freie Software ist eine Frage der Freiheit, nicht des Preises.

Embedded Software

Bei Embedded Software handelt es sich um Technik, welche in einer speziellen Hardware eingespielt und später nicht mehr verändert wird. Ein Beispiel hierfür wäre eine Software welche in ein Auto implementiert wird.

Desktop und Cloud Software

Desktop Software ist eine Software zur Anwendung und Datenspeicherung auf lokalen Rechnern ohne erforderliche Webanbindung. Cloudbasierte Anwendungen laufen hingegen über einen Browser und speichern die Daten auf externen Servern. Eine beliebte Form des Cloud Computings ist Saas (Software as a service).

Cloud Software wird zunehmend beliebter und spielt bereits bei jedem zweiten Unternehmen eine Rolle. Ein klarer Vorteil liegt in der kostengünstigen Nutzung, weshalb auch kleinere Unternehmen von dieser Lösung profitieren. Die Nutzung einer Cloud Software setzt jedoch einen hohen Vertrauensfaktor voraus, da die Daten auf externen Servern liegen.

Name des/der Auszubildenden:	Mustermann, Max
Datum:	01.08.2021
Thema des Fachberichts	Sicherheitsrisiken in der Netzwerktechnik

Sicherheitsrisiken in der Netzwerktechnik

Alle im Einsatz befindlichen Sicherheitssysteme, -verfahren und -methoden weisen zwangsläufig Risiken auf. Sicherheitslücken entstehen immer dort, wo Sicherheitskonzepte oder Implementierungen fehlerhaft sind.

Nachfolgend werden einige Sicherheitslücken aufgelistet, die Sicherheitsrisiken verursachen können. Eine vollständige Auflistung ist aufgrund der Masse an Möglichkeiten sowie der sich ständig neu entwickelnden Methoden nicht möglich. Dementsprechend gibt es auch keinen absoluten Schutz vor Sicherheitslücken.

Mögliche Sicherheitslücken sind:

- Zero-Day-Exploit (Fehler in der Software)
- Geheime Hintertüren in Hardware und Software (Backdoor)
- Unzureichende Zugangskontrolle zur Infrastruktur (temporär geöffnete Türen von EDV-Räumen)
- Konfigurationsoberflächen sind über das Internet erreichbar
- Ungesicherte System- und Konfigurationsdateien
- Fest einprogrammierte Administrationspasswörtern
- Möglichkeit zum Einschleusen von Befehlen oder Programmen
- Unzureichende Begrenzung der Berechtigung (großzügig ausgelegte Berechtigungen)
- Veraltete Hardware und Software mit unzureichenden Sicherheitsstandards
- Offene Ports in der Firewall

So vielfältig wie Netze sind, so vielfältig sind auch die Angriffsmöglichkeiten auf ein Netz. In vielen Fällen werden mehrere Angriffe kombiniert, um ein Ziel zu erreichen. Beispiele für Angriffsszenarien sind:

- DoS - Denial of Service
- Man-in-the-Middle
- IP-Spoofing
- Drive-by
- Brute-Force-Attacke auf Konten und Logins
- SQL-Injection

Sicherheitsrisiken können zudem von verschiedenen Quellen ausgehen. Der Anwender gilt als größtes Sicherheitsrisiko. Vor allem unbedarfte Anwender gehen oft naiv ans Werk, was EDV und IT angeht. Deshalb ist es notwendig, den Anwender für Sicherheitsrisiken zu sensibilisieren. Ein typisches Beispiel ist das Öffnen von E-Mail-Anhängen, die Viren, Würmer oder Trojaner enthalten. Weitere weit verbreitete Anwenderfehler stellen die Verwendung von Standard-Passwörtern oder unsicheren Passwörtern sowie versehentlich aktivierte Datenfreigabe dar.

Name des/der Auszubildenden:	Mustermann, Max
Datum:	01.08.2021
Thema des Fachberichts	Sicherheitsrisiken in der Netzwerktechnik

Ein weiteres Sicherheitsrisiko stellt “Bring your own Device”, kurz BYOD, dar. BYOD bezeichnet den Trend, dass Arbeitnehmer in Unternehmen ihre eigenen privaten elektronischen Geräte und die darauf befindliche Software innerhalb der Unternehmens-IT nutzen wollen. In der Regel handelt es sich um persönliche Geräte, wie Smartphones, Tablets und Notebooks, die der Anwender für seine privaten Zwecke individuell eingerichtet hat. Ohne eine klare Trennung von dienstlichen und privaten Geräten sind die oftmals strengen Regeln für den Datenschutz nicht einzuhalten.

In der Netzwerktechnik sind Zertifikate eine Möglichkeit, um den Kommunikationspartner zu identifizieren. Dazu wird eine Zertifizierungsstelle befragt, die das jeweilige Zertifikat ausgestellt hat. Eine Zertifizierungsstelle ist demnach eine zentrale Instanz, der vertraut werden kann. Ein Risiko entsteht, wenn es einem Angreifer gelingt, Zugriff auf eine Zertifizierungsstelle zu bekommen und beliebige Zertifikate zu erstellen.

Ebenfalls risikobehaftet ist der Schritt der Authentisierung. Verschlüsselung wie zum Beispiel mit SSL ist nur sicher, wenn ein Programm die Identität der Gegenstelle, also deren Zertifikat, zuverlässig überprüft. Angriffe funktionieren häufig nur deshalb, weil die Identität bei der Authentifizierung nur sehr nachlässig geprüft wird oder sogar fehlerhaft ist. Wenn zum Beispiel die Zertifizierungsstelle bei der Validierung eines Zertifikats nicht erreichbar ist, kann ein fehlerhaftes Programm das Zertifikat trotzdem als gültig anerkennen, obwohl es dies möglicherweise nicht ist.

Ein Schwachpunkt bei der Verschlüsselung ist zudem der Schlüssel an sich, der von Zufallszahlengeneratoren (Kombination aus Hardware und Software) erzeugt wird. Wenn der Schlüssel nicht zufällig erzeugt wird, dann kann er durch einfaches Ausprobieren berechnet werden. Wenn die Anzahl der Zufallszahlen zu gering ist, wird jedes kryptografische Verfahren geschwächt. Eine konkrete Sicherheitslücke bei der Verschlüsselung kann auch eine schlechte Initialisierung des Pseudozufallszahlen-Generators (Pseudo Random Number Generator, PRNG) sein.

Ein weiteres Sicherheitsrisiko geht von Fernwartungsfunktionen aus. Fernwartung oder Remote Control bezeichnet meist Fernzugriffsmöglichkeiten auf Netzwerke oder Rechner. Meistens werden dafür entsprechende Zugänge eingerichtet, mit begrenzenden Berechtigungen versehen und die Verbindungen verschlüsselt. Dennoch stellen Fernwartungsfunktionen eine Angriffsstelle in ein sicheres System dar.

Datum, Unterschrift Auszubildender

Datum, Unterschrift Ausbildender oder Ausbilderin

Name des/der Auszubildenden:	Mustermann, Max
Datum:	01.08.2021
Thema des Fachberichts	Service Level Agreement

Service Level Agreement

Ein Service Level Agreement (SLA) ist die Vereinbarung oder der Vertrag zwischen Kunde (Servicenehmer) und Dienstleister (Servicegeber, Service Provider oder IT-Dienstleister). Im Service Level Agreement werden die zu erbringenden Dienstleistungen (IT-Services oder IT-Teilleistungen) einschließlich Qualitätsanforderungen und Messgrößen (Kennzahlen) sowie die Rechte und Pflichten beider Parteien beschrieben. Dabei spielt es keine Rolle, ob sich der Servicegeber im eigenen Unternehmen befindet oder eine externe Organisation ist.

Merkmale von SLAs

Folgende Merkmale sind charakteristisch für ein Service Level Agreement. Ein Service Level Agreement

- ist eine formell ausgehandelte und schriftlich dokumentierte Vereinbarung,
- wird zwischen zwei untereinander unabhängigen Partnern abgeschlossen,
- bezieht sich inhaltlich auf Dienstleistungen,
- beinhaltet die Verpflichtung des einen Partners (Servicegeber), bestimmte Leistungen zu erbringen, sowie die Verpflichtung des anderen Partners (Servicenehmer bzw. Provider) im Gegenzug dafür bestimmte Gegenleistungen zu erbringen,
- bezieht sich stets auf einen bestimmten Zeitraum,
- beinhaltet eine inhaltliche Beschreibung der zu erbringenden Dienstleistungen und regelt für beide Partner relevante Prozesse der Dienstleistungserbringung (einschließlich der Rechte und Pflichten der beteiligen Parteien bei der Dienstleistungserbringung),
- beschreibt die Qualität der zu erbringenden Dienstleistungen durch die Definition von Kennzahlen, die relevante Merkmale der zu erbringenden Dienstleistungen quantifizieren, als Service Levels,
- nennt die Verrechnungspreise für die Dienstleistung (Kompensationszahlung, Gegenleistung des Kunden) in Abhängigkeit von den vereinbarten Service Levels und
- enthält Regelungen für den Fall der Abweichung von vereinbarten Service Levels.

Kennzahlen von SLAs

Die Definition von Kennzahlen wird im Service Level Agreement gefordert, um die relevanten Eigenschaften der zu erbringenden Dienstleistungen zu quantifizieren und zu messen. Kennzahlen, die zur Vereinbarung von Service Levels verwendet werden sollen, haben folgende Anforderungen zu erfüllen:

- Vollständigkeit
  Eine Kennzahl gilt als vollständig, wenn sowohl Dienstleister als auch Kunde aufgrund dieser Definition ein klares und einheitliches Verständnis von der Ermittlung und Aussage dieser Kennzahl haben und sich diesbezüglich keine

Datum, Unterschrift Auszubildender

Datum, Unterschrift Ausbildender oder Ausbilderin

Interpretationsprobleme ergeben. Diese Anforderung beinhaltet insbesondere, dass Informationen zur Beschreibung einer Kennzahl (Bezeichnung, Bezugsobjekt, Bezugszeit, Basisdaten und Berechnungsformel) angegeben werden. Es reicht zum Beispiel nicht aus, von telefonischer Erreichbarkeit zu sprechen, wenn nicht definiert wird, wie diese ermittelt und gemessen wird.

- Relevanz:
Als relevant für eine Dienstleistung ist eine Kennzahl dann, wenn diese ein Merkmal der Dienstleistung beschreibt, das den Nutzen dieser Dienstleistung für deren Kunden beeinflusst. Der Nutzen einer IT-Dienstleistung kann dabei anhand des Beitrags dieser Dienstleistung zur Unterstützung von betrieblichen Prozessen des Kunden gemessen werden. Uninteressant für den Kunden ist zum Beispiel eine Kennzahl, die angibt, wie hoch der Anteil der Anrufer ist, die diese Nummer versehentlich gewählt haben.

- Proportionalität:
Eine weitere Anforderung an eine Kennzahl ist, dass deren Ausprägung sich proportional zum Sachverhalt verhält, den sie ausdrücken soll. Sollten diese Anforderung nicht erfüllt ist, ist es nicht möglich, aus dem Grad der Veränderung des Wertes der Kennzahl direkt Rückschlüsse auf den Grad der Veränderung des zu bewertenden Sachverhalts zu ziehen. Die telefonische Erreichbarkeit im Beispiel ist proportional und die Levels sind jeweils in 5-Prozent-Schritten angegeben.

- Aussagekraft für den Kunden:
Eine Kennzahl muss für den Kunden aussagekräftig sein. Grund dafür, dass eine Kennzahl für einen Kunden nicht aussagekräftig ist, kann zum einen sein, dass die Kennzahl für ihn nicht verständlich ist, da dieser nicht über das hierzu erforderliche technische Fachwissen verfügt. Zum anderen kann eine Kennzahl für Kunden wenig aussagekräftig sein, wenn sie nicht die Sichtweise des Kunden berücksichtigt. Kennzahlen, die sich primär an technischen oder organisatorischen Gegebenheiten des IT-Dienstleisters orientierten, sind somit meist nicht für SLAs geeignet. Um für Kunden aussagekräftige Kennzahlen zu erhalten, ist bei der Festlegung der Kennzahlen stets die Perspektive des Kunden einzunehmen.

- Vollständige Beeinflussung durch den Dienstleister:
Als vollständig beeinflussbar durch einen Dienstleister gilt eine Kennzahl dann, wenn sich deren Ausprägung ausschließlich aufgrund von Aspekten bestimmt, die im Zuständigkeits- und Verantwortungsbereich des Dienstleisters liegen. Wird dem Anbieter des Call-Centers von seinem Telefonnetzanbieter nur eine Verfügbarkeit des Telefonnetzes von 97 Prozent angeboten, wird er selbst seinen Kunden keine Verfügbarkeit anbieten, die „mindestens 97 Prozent" beträgt.

- Wirtschaftlichkeit:
  Die Ermittlung einer Kennzahl ist stets mit Kosten verbunden. Diesen Kosten steht der aus der Kenntnis der Kennzahl erzielbare Nutzen gegenüber. Eine Kennzahl soll hier als wirtschaftlich bezeichnet werden, sofern der Nutzen, der aus der Kenntnis der Kennzahl gewonnenen werden kann, die Kosten für die Ermittlung der Kennzahl mindestens ausgleicht.

Beispiele von SLAs

Service-Level-Agreements können individuell vereinbart werden. Besonders die Festlegung von Kennzahlen zur Qualitätsbewertung bietet eine Möglichkeit zur Differenzierung. Im Kundenservice sind beispielsweise die folgenden SLA Arten verbreitet:

- Reaktionszeit-SLAs:
  Eingehenden Nachrichten von Kunden wird eine Antwortzeit zugeordnet, innerhalb derer ein Agent am Service Desk dem Kunden antworten muss. Die Antwortzeit ist hier die Service-Level-Kennzahl und diese stellt sicher, dass Kunden nicht länger als nötig auf eine Antwort oder ein Update warten müssen. Die Zeit bis zur ersten Antwort (Reaktionszeit) ist ein besonders wichtiges SLA, da sie auch als Bestätigung der Kundenanfrage fungiert.

- Lösungs-SLAs:
  Jedem Anliegen beziehungsweise jedem SLA-Report wird auch ein Lösungs-SLA zugeordnet. Dieses setzt eine Frist, bis zu der das Ticket geschlossen oder gelöst sein muss. Lösungs-SLAs stellen sicher, dass die Kundenanfrage mit zufriedenstellenden Antworten und Maßnahmen gelöst wird und nicht nur mit schnellen Rückmeldungen.

- Anliegen-basierte SLAs:
  Spezifische Anliegen, wie zum Beispiel Server-Ausfälle oder Service-Probleme, erfordern schnelle Antworten und Lösungen. Problembasierte Service Level Agreements weisen daher bestimmten Arten von Support-Tickets eine spezielle Frist zu.

Name des/der Auszubildenden:	Mustermann, Max
Datum:	01.08.2021
Thema des Fachberichts	Schutzziele der Informationssicherheit

Schutzziele der Informationssicherheit

Informationssicherheit hat das Ziel, Informationen jeglicher Art und Herkunft zu schützen. Dies umfasst Informationen, die sich in den Köpfen der Beteiligten befinden, genauso wie Informationen in Papierform und Informationen, die elektronisch in Systemen und Netzwerken verarbeitet werden. Informationssicherheit verfolgt somit einen breiteren Ansatz als die IT-Sicherheit, die sich vorrangig auf elektronisch gespeicherte Informationen und die verarbeitenden IT-Systeme bezieht.

Aufgrund der hohen Bedeutung von Informationen als Unternehmenswerte sollte die Informationssicherheit als notwendige Managementaufgabe verstanden werden, um Datenverlust und Datenmissbrauch zu verhindern. Zusätzlich eröffnet die Informationssicherheit viele Möglichkeiten zum Schutz von personenbezogenen Daten, wodurch auch Synergieeffekte zum Datenschutz erzielt werden können. Ziel der Informationssicherheit ist es, Risiken auf ein für die Organisation akzeptables Niveau zu minimieren.

Die Informationssicherheit setzt sich aus drei primären Schutzzielen zusammen. Die Vertraulichkeit, die Integrität und die Verfügbarkeit von Informationen.

Vertraulichkeit

Das erste Schutzziel der Informationssicherheit ist die Vertraulichkeit. In der Informationssicherheit bedeutet der Begriff „Vertraulichkeit", dass Daten nur von solchen Personen eingesehen, bearbeitet und verwaltet werden dürfen, die auch dazu befugt sind. Durch die Vertraulichkeit wird somit der Zugang zu Informationen geschützt. Um die Vertraulichkeit von Daten gewährleisten zu können und den Zugriff von nicht berechtigten Personen zu verhindern, muss eine organisierte Struktur im Unternehmen bestehen. Es muss festgelegt werden, welche Personen des Unternehmens Zugriff auf bestimmte Daten haben und inwiefern dieser Zugriff besteht.

Ein alltägliches Beispiel hierfür ist der E-Mail Verkehr eines Unternehmens. Heutzutage arbeitet so gut wie jedes Unternehmen mit E-Mails. Die meisten dieser E-Mails beinhalten vertrauliche Informationen. Der E-Mail Verkehr eines Unternehmens muss deshalb unbedingt geeignet verschlüsselt werden. Eine Verschlüsselung sorgt dafür, dass bei Übertragung der E-Mails unbefugte Personen keinen Zugriff auf diese erhalten. Somit kann durch eine Verschlüsselung die Vertraulichkeit der Informationen gewährleistet werden.

Integrität

Das zweite Schutzziel der Informationssicherheit ist die Integrität. Der Begriff „Integrität" bedeutet, dass die unerkannte Veränderung von Daten nicht möglich sein soll. Im Gegensatz zu der Vertraulichkeit, die sich mit der Berechtigung der Datenänderung beschäftigt, soll bei der Integrität die Korrektheit der Daten sowie

Datum, Unterschrift Auszubildender

Datum, Unterschrift Ausbildender oder Ausbilderin

eine korrekte Funktionsweise des Systems gesichert werden. Somit liegt der Fokus der Integrität auf der Nachvollziehbarkeit von Datenänderungen.

Die Integrität setzt sich aus Datenintegrität und Systemintegrität zusammen. Dabei wird in der Praxis zwischen einer starken Integrität und einer schwachen Integrität unterschieden. Von einer starken Integrität ist die Rede, wenn das System und die Funktionen keine Möglichkeit zur unbemerkten oder unerkannten Datenveränderung bieten. Eine schwache Integrität liegt vor, wenn eine generelle Möglichkeit der Datenveränderung besteht, diese Datenveränderung jedoch keinesfalls unerkannt erfolgen kann. Dieser Fall ist in der Praxis leider kaum zu vermeiden. In vielen Unternehmen ist eine Manipulation der Daten nicht zu verhindern. Für diese Fälle soll jedoch die Möglichkeit bestehen, dass eine Datenveränderung zumindest nicht unerkannt bleibt. Eine Manipulation der Daten kann durch das Abändern, Löschen oder Einfügen von Daten erfolgen.

Verfügbarkeit

Als letztes Schutzziel der Informationssicherheit gilt die Verfügbarkeit. Der Begriff „Verfügbarkeit" steht für die Zeit, in der das System funktioniert. Das bedeutet, dass das System jederzeit verfügbar sein muss und für befugte Personen zugänglich sein sollte. Um das Schutzziel zu erfüllen, sollte die Verfügbarkeit möglichst hoch gehalten werden. Als klassisches Beispiel gilt der berühmte Systemausfall im Unternehmen. Durch einen Systemausfall werden nicht nur die Abläufe eines Unternehmens beeinträchtigt, sondern auch der Zugriff auf bestehende Datenbestände. Ein Unternehmen sollte sich deshalb vor Systemausfällen und Angriffen schützen. Die Durchführung einer Risikoanalyse kann hier von Vorteil sein, um Schäden abzuwiegen und Gegenmaßnahmen zu etablieren.

Erweiterte Schutzziele

In bestimmten Kontexten können noch zusätzliche Schutzziele definiert werden. Diese sind oft die Authentizität, Nichtabstreitbarkeit, Verbindlichkeit und Zuverlässigkeit.

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.

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. Es wird unterschieden zwischen

- Nichtabstreitbarkeit der Herkunft. Es soll einem Absender einer Nachricht unmöglich sein, das Absenden einer bestimmten Nachricht nachträglich zu bestreiten.

- Nichtabstreitbarkeit des Erhalts: Es soll einem Empfänger einer Nachricht unmöglich sein, den Erhalt einer gesendeten Nachricht nachträglich zu bestreiten

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.

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.

Name des/der Auszubildenden:	Mustermann, Max
Datum:	01.08.2021
Thema des Fachberichts	Schutzbedarfsfeststellung

Schutzbedarfsfeststellung

Ziel der Schutzbedarfsfeststellung ist es, für die erfassten Objekte im Informationsverbund zu entscheiden, welchen Schutzbedarf sie bezüglich Vertraulichkeit, Integrität und Verfügbarkeit besitzen. Dieser Schutzbedarf orientiert sich an den möglichen Schäden, die mit einer Beeinträchtigung der betroffenen Anwendungen und damit der jeweiligen Geschäftsprozesse verbunden sind.

Die Schutzbedarfsfeststellung für den Informationsverbund gliedert sich in mehrere Schritte:

1. Definition der Schutzbedarfskategorien
2. Schutzbedarfsfeststellung für Anwendungen
3. Schutzbedarfsfeststellung für IT-Systeme
4. Schutzbedarfsfeststellung für Räume
5. Schutzbedarfsfeststellung für Kommunikationsverbindungen
6. Schlussfolgerungen aus den Ergebnissen der Schutzbedarfsfeststellung

Die Definition der Schutzbedarfskategorien muss auf die eigenen Bedürfnisse erfolgen. Begrifflichkeiten wie „normal", „hoch" und „sehr hoch" werden zwar universell eingesetzt, die Bedeutung, was unter „normal" und den anderen allgemeinen Begrifflichkeiten im Einzelfall zu verstehen ist, kann aber nur im jeweiligen Einzelfall definiert werden.

Die Schäden, die bei dem Verlust der Vertraulichkeit, Integrität oder Verfügbarkeit für einen Geschäftsprozess beziehungsweise eine Anwendung einschließlich ihrer Daten entstehen können, lassen sich typischerweise folgenden Schadensszenarien zuordnen:

- Verstoß gegen Gesetze, Vorschriften oder Verträge,
- Beeinträchtigung des informationellen Selbstbestimmungsrechts,
- Beeinträchtigung der persönlichen Unversehrtheit,
- Beeinträchtigung der Aufgabenerfüllung,
- negative Innen- oder Außenwirkung und
- finanzielle Auswirkungen.

Sind Schutzbedarfskategorien definiert und potenzielle Schadensszenarien identifiziert, erfolgt die Schutzbedarfsfeststellung für die jeweils potenziell bedrohten Ressourcen. Ist der Schutzbedarf festgestellt, so resultiert daraus als Ergebnis, welche Ressource gegen welche Bedrohung zu schützen ist. Idealerweise lassen sich aus der Identifikation des Risikos auch direkt Maßnahmen zum Schutz der Ressource ableiten.

Name des/der Auszubildenden:	Mustermann, Max
Datum:	01.08.2021
Thema des Fachberichts	Programmbibliothek

Programmbibliothek

Eine Programmbibliothek bezeichnet in der Programmierung eine Sammlung von Unterprogrammen/-Routinen, die Lösungswege für thematisch zusammengehörende Problemstellungen anbieten.

Bibliotheken sind im Unterschied zu Programmen keine eigenständig lauffähigen Einheiten, sondern sie enthalten Hilfsmodule, die von Programmen angefordert werden. In erweitertem Sinn gelten als Programmbibliotheken alle Arten von Bibliotheken, die Programmcode enthalten. Insofern unterscheidet man Programmbibliotheken unter anderem nach dem Typ des Programmcodes (z. B. Quelltexte, Makros, Objekt- oder Bytecode, Maschinencode).

Bibliotheken werden zu unterschiedlichen Zeitpunkten benutzt, manche nur im Rahmen der Softwareentwicklung, andere nur zur Ausführung von Programmen, wieder andere als Mischform von beiden. Solche Bibliotheken enthalten häufig nicht nur Unterprogramme, sondern Programmcodeteile aller Programm-Typen.

Mögliche Zugriffe auf Funktionen einer Programmbibliothek sind durch die Programmierschnittstelle (API) definiert. Dabei handelt es sich um die Gesamtheit der öffentlich verfügbaren Funktionen und Klassen, in Abgrenzung zu den privaten Einheiten der Bibliothek, die nicht zugänglich sind. Manche proprietären Programmbibliotheken werden nicht im Quelltext veröffentlicht, da sie Firmengeheimnisse darstellen.

Statische und dynamische Bibliotheken

Eine Unterscheidung kann zwischen statischen und dynamischen Bibliotheken getroffen werden.

Als „Statische Bibliothek" wird eine Programmbibliothek bezeichnet, die Module oder Unterprogramme enthält, die durch einen so genannten Linker mit dem Compiler eines anderen Programms verbunden werden. Dabei erzeugt der Linker, in der Regel für ein Hauptprogramm, eine ausführbare Datei oder (je nach Betriebssystem) ein Ladermodul in einer Ladebibliothek, in der die von diesem aufgerufenen Module fest (statisch) eingebunden beziehungsweise angehängt sind.

Aus dynamischen Bibliotheken werden Komponenten hingegen erst während der Laufzeit eines Programms über einen sogenannten Lader in den Arbeitsspeicher geladen. Das geschieht entweder durch eine explizite Anweisung durch das Programm oder implizit durch einen so genannten Laufzeit-Lader, wenn das Programm dynamisch gebunden wurde.

Name des/der Auszubildenden:	Mustermann, Max
Datum:	01.08.2021
Thema des Fachberichts	Programmbibliothek

Speicherungsformen

Programmbibliotheken und ihre Inhalte können, abhängig vom Betriebssystem und der Entwicklungsumgebung, in unterschiedlichen Formen und Strukturen gespeichert werden. Folgend sind einige Beispiele aufgelistet:

- Die Bibliothek ist ein Dateiverzeichnis, ihre Elemente/Komponenten sind einzelne Dateien.
- Die Bibliothek ist eine Datei, die darin enthaltenen Komponenten werden von den Programmen der Entwicklungsumgebung oder einer speziellen Bibliotheksverwaltungssoftware identifiziert und verarbeitet.
- Unterschiedliche Arten von Bibliotheken werden in einer gemeinsamen Datei verwaltet, die Entwicklungsumgebung kann dies unterscheiden/verarbeiten.
- Es existiert keine „Bibliothek", die Komponenten werden als einzelne Dateien gespeichert und ausgeführt, z. B. als „EXE-Dateien".

Name des/der Auszubildenden:	Mustermann, Max
Datum:	01.08.2021
Thema des Fachberichts	OSI-Modell

OSI-Modell

Das OSI-Schichtenmodell ist ein Referenzmodell für herstellerunabhängige Kommunikationssysteme beziehungsweise eine Design-Grundlage für Kommunikationsprotokolle und Computernetze.

Die Abkürzung OSI steht für Open System Interconnection (Offenes System für Kommunikationsverbindungen). Es wurde von der ISO (International Organization for Standardization), der Internationalen Organisation für Normung, als Grundlage für die Bildung von offenen Kommunikationsstandards entworfen. Das OSI-Modell wird daher auch als ISO/OSI-Schichtenmodell bezeichnet.

Zielsetzung bei der Definition des ISO/OSI-Standards war es, ein Referenzmodell zu schaffen, das die Kommunikation verschiedener technischer Systeme über unterschiedliche Medien und Technologien ermöglicht und Kompatibilitäten herstellbar. Um dieses Ziel zu erreichen, verwendet das OSI-Modell insgesamt sieben verschiedene Schichten (Layer), die hierarchisch aufeinander aufbauen.

In jeder einzelnen Schicht werden genau definierte Aufgaben ausgeführt. Die Schnittstellen zur jeweils darüber- und darunterliegenden Schicht sind exakt beschrieben. Dadurch lassen sich Zwischenschichten austauschen, ohne dass die anderen Layer davon betroffen sind. Netzwerkprotokolle, Anwendungsprotokolle oder Übertragungsmedien werden dank des Schichtenmodells prinzipiell beliebig erweiterbar. Jede Schicht bietet der direkt über ihr liegenden Schicht Dienste zur Nutzung an. Um diese Dienste zur Verfügung zu stellen, verwendet die Schicht die Dienste des unter ihr liegenden Layers und führt die Aufgaben des eigenen Layers aus.

In den einzelnen Schichten müssen eine Vielzahl verschiedener Aufgaben bewältigt werden, die für die Sicherheit, die Zuverlässigkeit und die Performance der Kommunikationsverbindung sorgen. Kommunizieren zwei Systeme miteinander, werden alle sieben Schichten des OSI-Modells mindestens zweimal durchlaufen, da sowohl der Sender als auch der Empfänger das Schichtenmodell zu berücksichtigen hat.

Kurz zusammengefasst sind die wesentlichen Merkmale und Aufgaben des Modells:

- das Referenzmodell setzt sich aus sieben einzelnen Schichten zusammen
- in jeder Schicht werden bestimmte Aufgaben ausgeführt
- einzelne Schichten sind austauschbar
- die Kommunikation zwischen den Schichten erfolgt immer hierarchisch mit der direkt darunter oder darüber befindlichen Schicht
- Schnittstellen definieren den Austausch zwischen den Schichten
- die ersten vier Schichten sind transportorientiert
- die Schichten 5 bis 7 sind anwendungsorientiert

Datum, Unterschrift Ausbildender

Datum, Unterschrift Auszubildender oder Ausbildung

Name des/der Auszubildenden:	Mustermann, Max
Datum:	01.08.2021
Thema des Fachberichts	OSI-Modell

Im Folgenden werden die sieben Schichten des OSI- Modells kurz beschrieben.

Schicht 1: Bitübertragungsschicht / Physical Layer

Die unterste Schicht des OSI-Modells kümmert sich um die Bereitstellung elektrischer und mechanischer Funktionen zur Übertragung von Bits. Als

Übertragungstechnische Verfahren kommen beispielsweise elektrische Signale, optische Signale oder elektromagnetische Wellen zum Einsatz. Mittels Schicht 1 erfolgt die Übertragung auf leitungsgebundenen oder leitungslosen Übertragungsstrecken. Typische Geräte, die auf dem Physical Layer arbeiten, sind Repeater, Kabel, Stecker, Antennen, Hubs oder Verstärker. Standards und Normen der Schicht 1 sind beispielsweise V.24, X.21 oder RS 232.

Schicht 2: Sicherungsschicht / Data Link Layer

Zentrale Aufgabe der Schicht 2 ist es, zuverlässige und möglichst fehlerfreie Übertragungen auf dem jeweiligen Medium zu ermöglichen. Zu diesem Zweck werden die Bitströme aus der Schicht 1 in Blöcke oder Frames unterteilt. Durch das Hinzufügen von zusätzlichen Prüfsummen kann der Empfänger fehlerhafte Frames eindeutig erkennen und diese korrigieren oder verwerfen. Ebenfalls auf dem Data Link Layer kann die abschnittsweise Datenflusskontrolle gesteuert werden. Dem Empfänger ist es dadurch möglich, die Geschwindigkeit dynamisch zu regeln, mit der ein Sender Frames abschickt. Typische Hardwaregeräte der Schicht 2 sind Switches oder Bridges. Protokolle und Normen des Data Link Layers sind zum Beispiel HDLC, ARP oder IEEE 802.11 (WLAN).

Schicht 3: Vermittlungsschicht / Network Layer

Auf dem Networking Layer werden Verbindungen in leitungsvermittelten Netzen hergestellt und Datenpakete in paketvermittelten Netzen weitergeleitet. Die Übertragung der Daten erfolgt über das komplette Netzwerk vom Sender bis zum Empfänger. Auf dem Weg dorthin werden Adressen ausgewertet und die Daten durch das Netz von Zwischenknoten zu Zwischenknoten gerouted. In den Zwischenknoten erfolgt in der Regel keine Verarbeitung der Daten in den Schichten über dem Networking Layer. Eine der zentralen Aufgaben des Network Layers ist die Bereitstellung von Adressen für die Kommunikation über das Netzwerk. Auf Basis der Adressen erfolgt das Routing und der Aufbau von Routingtabellen. Weitere Dienste der Schicht 3 sind die Fragmentierung von Datenpaketen und die Bereitstellung von bestimmten Dienstgüten. Router sind die typischen Geräte der Schicht 3. Protokolle des Network Layers sind zum Beispiel IP oder X.25.

Schicht 4: Transportschicht / Transport Layer

In der Schicht 4 erfolgt die Ende-zu-Ende-Kontrolle der übertragenen Daten. Der Transport Layer kann Stausituationen erkennen und vermeiden sowie Datenströme segmentieren. Das Datensegment erhält eine eigene Adresse in der Schicht 4, über die es einer bestimmten Anwendung zugeordnet werden kann. Bei den Protokollen UDP oder TCP wird diese Adresse als Port bezeichnet. Den darüber liegenden

anwendungsorientierten Schichten stellt der Transport Layer den transparenten Zugriff auf die Daten zur Verfügung. Den Schichten 5 bis 7 müssen daher die darunterliegenden Kommunikationsnetze und deren Eigenschaften nicht bekannt sein. Der Transport Layer stellt eine Art Bindeglied zwischen den transportorientierten und den anwendungsorientierten Schichten dar. Die bekanntesten Protokolle aus der Schicht 4 sind TCP und UDP.

Schicht 5: Kommunikationsschicht / Session Layer

Der Session Layer steuert die logische Verbindung zwischen zwei Systemen und verhindert beispielsweise Zusammenbrüche der Verbindung oder andere Probleme. Über die bereitgestellten Dienste der Schicht 5 ist es möglich, abgebrochene Sitzungen wieder neu aufzusetzen und zu synchronisieren, nachdem die eigentliche Transportverbindung ausgefallen ist. Dadurch lässt sich verhindern, dass Sitzungen oder Übertragungen erneut von vorne beginnen müssen. Betrachtet man die TCP/IP-Protokollfamilie stellen Protokolle wie Telnet, FTP, TFTP, mTFTP oder SMTP und NetBios die typischen Services und Steuerungs- oder Kontrollmechanismen der Schicht 5 zur Verfügung.

Schicht 6: Darstellungsschicht / Presentation Layer

Aufgabe der Darstellungsschicht ist es, die systemabhängige Darstellung von Daten in eine für die Anwendung unabhängige Form zu übertragen. In der Schicht 6 sind auch Aufgaben wie die Verschlüsselung von Daten oder die Datenkompression angesiedelt. Um die Daten in eine unabhängige Form zu bringen, kann der Presentation Layer als Übersetzer zwischen verschiedenen Datenformaten auftreten. Er wandelt die Daten in verschiedene Formate und Codecs. Bei Protokollen aus dem TCP/IP-Referenzmodell wie Telnet, mTFTP, NetBios oder FTP sind neben den Services der Schicht 5 auch die typischen Aufgaben der Darstellungsschicht implementiert.

Schicht 7: Anwendungsschicht / Application Layer

Den Abschluss des Schichtenmodells in Richtung Anwendung bildet die Schicht 7, der Application Layer. Diese Schicht regelt unter anderem die Ein- und Ausgabe von Daten und stellt Funktionen für die Anwendung zur Verfügung. Die eigentliche Anwendung ist allerdings nicht Bestandteil des Application Levels. Protokolle wie Telnet, FTP, NNTP, mTFTP oder SMTP erfüllen Funktionen der Schicht 7.

Name des/der Auszubildenden:	Mustermann, Max
Datum:	01.08.2021
Thema des Fachberichts	Netzwerkprotokolle

Netzwerkprotokolle

Netzwerkprotokolle regeln den Datenaustausch in Computernetzen. Sie definieren die erforderlichen Regeln für Aufgaben wie das Adressieren von Datenpaketen, die Vermittlung von Datenpaketen, den Transport von Datenpaketen, den Verbindungsaufbau oder die Fehlerüberprüfung.

Je nach Protokoll kann die Datenübertragung in verschiedenen Formen wie verbindungsorientiert, verbindungslos, gesichert oder ungesichert erfolgen. Damit der Datenaustausch gelingt, müssen die beteiligten Stationen die gleichen Netzwerk-Protokolle verstehen und verwenden. Für die Kommunikation ist in der Regel ein Zusammenspiel mehrerer Netzwerk-Protokolle erforderlich, die jeweils unterschiedliche Aufgaben erfüllen.

Aufbau eines Protokolls

Um für eine Struktur der verschiedenen Protokolle zu sorgen, sind sie gemäß ihren Aufgaben in verschiedenen Schichten (Layer) organisiert. Jedes Protokoll gehört einer bestimmten Schicht an und übernimmt spezifische Aufgaben dieser Schicht.

Die Funktionen der Protokolle bauen aufeinander auf. Die Protokolle der höheren Schichten greifen dabei auf die Protokolle der tieferen Schichten zu. Transportprotokolle sind für den Austausch der Daten auf der Hardware-Ebene zuständig und bereiten den Übertragungsweg für von ihnen prinzipiell unabhängigen Anwendungsprotokollen. Das stellt sicher, dass Anwendungsprogramme auf unterschiedlichen Systemen untereinander kommunizieren können, sobald diese Systeme in der Lage sind, auf irgendeine Art eine Verbindung herzustellen. So regelt beispielsweise das Internet Protocol die weltweit eindeutige Adressierung von Rechnern. Diese Adressierung nutzen dann beispielsweise das Transmission Control Protocol zur Datenübertragung und das Simple Mail Transfer Protocol zum Übermitteln von E-Mails. Dieses schichtweise Aufeinanderaufbauen der Protokolle wird mit Hilfe des OSI-Modells dargestellt.

Aufgaben eines Netzwerkprotokolls

Zu den typischen Aufgaben eines Netzwerkprotokolls zählen:

- Ein sicherer und zuverlässiger Verbindungsaufbau zwischen den an der Kommunikation beteiligten Computern
- Das verlässliche Zustellen von Paketen
- Wiederholtes Senden nicht angekommener Pakete
- Zustellen der Datenpakete an denjenigen gewünschten Empfänger
- Das Sicherstellen einer fehlerfreien Übertragung
- Das Zusammenfügen ankommender Datenpakete in der richtigen Reihenfolge
- Das Verhindern des Auslesens durch unbefugte Dritte (durch Verschlüsselung)

- Das Verhindern der Manipulation durch unbefugte Dritte (durch MACs oder elektronische Signaturen)

Arten von Netzwerkprotokollen

Je nach Art des Netzwerkes und der angeschlossenen Endgeräte oder Systeme existiert eine Vielzahl an verschiedenen Netzwerkprotokollen. Für die unterschiedlichen Netze und Kommunikationsformen sind unterschiedliche Protokolle definiert. Es gibt Protokolle, die Daten an einzelne Empfänger (Unicast-Protokolle), mehrere Empfänger (Multicast-Protokolle) oder alle Stationen (Broadcast-Protokolle) übermitteln. Auch der Weg des Datenstroms ist ein wichtiges Merkmal, um Netzwerk-Protokolle voneinander zu unterscheiden.

Bei Simplex-Protokollen ist eine Station nur Sender und die andere Station nur Empfänger. Vollduplex-Protokolle ermöglichen den gleichzeitigen Datenaustausch der beteiligten Stationen in beide Richtungen. Ein weiteres Unterscheidungsmerkmal der Netzwerk-Protokolle ist die Hierarchie der verbundenen Rechner. Unterschiedliche Protokolle übernehmen die Aufgaben der Datenübermittlung in Client-Server- oder Peer-to-Peer-Strukturen.

Sender und Empfänger von Daten können über die Protokolle synchronisiert oder asynchron Daten übertragen. Weitere Arten von Netzwerk-Protokollen sind verbindungslose und verbindungsorientierte Protokolle. Verbindungsorientierte Protokolle sorgen für den definierten Auf- und Abbau einer Verbindung für den Zeitraum der Kommunikation. Verbindungslose Protokolle verzichten auf Verbindungen und müssen weitere Mechanismen zur Sicherung der Datenübertragung implementieren oder in höheren Schichten übertragen.

Name des/der Auszubildenden:	Mustermann, Max
Datum:	01.08.2021
Thema des Fachberichts	Netzwerkplan

Netzwerkplan

Ein Netzwerkplan ist die Aufzeichnung des technischen Ist-Zustands eines Netzwerks. Diese IT-Dokumentation enthält in Tabellen, Dokumenten und Grafiken alle wichtigen Informationen über die gesamte Netzwerkinfrastruktur.

Im Einzelnen sollte der Plan mindestens die folgenden Objekte enthalten:

- die in das Netz eingebundenen IT-Systeme,
  dazu zählen Computer (Clients und Server), Netzdrucker sowie aktive Netzkomponenten (Switches, Router, WLAN-Access Points), usw.;
- die Verbindungen zwischen diesen IT-Systemen,
  LAN-Verbindungen (Ethernet), Backbone-Technik (z. B. ATM), usw.
- die Außenverbindungen der IT-Systeme,
  bei diesen sollte zusätzlich die Art der Verbindung gekennzeichnet sein (z. B. Internet-Anbindung, DSL).

Die Dokumentation jedes Netzwerks ist eine essentielle Hilfe bei der Netzwerkadministration, -wartung und -pflege, bei allen Stör- und Notfällen sowie auch bei Neubeschaffungen. Vorteile einer IT-Dokumentation aus technischer Sicht sind insbesondere:

- schnelle Fehlersuche bei Störungen, um Ausfallzeiten zu minimieren
- zügiger Neuaufbau von IT-ish-Systemen bei Upgrade oder Verlust
- strukturiertes und effizientes Anlernen neuer Mitarbeiter
- gezielte Ermittlung möglicher Risiken bei geplanten Änderungen oder Erweiterungen der Netzwerkinfrastruktur
- rechtzeitiges Erkennen von Schwachstellen und potenziellen Engpässen, um die Stabilität und Sicherheit des Firmennetzwerks zu erhöhen.

Im laufenden Betrieb zieht der wirtschaftliche Wert und Nutzen von einem Netzwerkplan generell darauf ab Kosten und Zeit zu sparen, sowie den gesetzlichen Anforderungen zu entsprechen. Eine IT-Dokumentation unterstützt dabei, den Überblick für eine effiziente, strategische Planung zu behalten. Zudem ist eine vollständige Dokumentation des Netzwerks Pflicht wenn eine ISO-Zertifizierung angestrebt wird.

Bei einem System-Ausfall kann die IT-Dokumentation darüber hinaus helfen, den Verlust von finanziellen und anderen Ressourcen zu reduzieren. Das System kann im besten Fall auf Grundlage des Netzwerkplans schnell und ohne großen betriebswirtschaftlichen Schaden wieder zum Laufen gebracht werden. Ist der Schaden größer, ist ultimativ die vollständige Netzwerkdokumentation eine grundsätzliche Voraussetzung um einen Versicherungsfall zu aktivieren.

Name des/der Auszubildenden:	Mustermann, Max
Datum:	01.08.2021
Thema des Fachberichts	Netzwerkkomponenten

Netzwerkkomponenten

Netzwerkkomponenten, auch bekannt als Netzwerkgeräte oder Computernetzwerkgeräte, sind physische Geräte, die für die Kommunikation und Interaktion zwischen Geräten in einem Computernetzwerk erforderlich sind. Insbesondere vermitteln sie Daten in einem Computernetzwerk.

Bei Netzwerkkomponenten wird zwischen aktiven und passiven Netzwerkkomponenten unterschieden. Als passive Netzwerkkomponenten wird das Material bezeichnet, das ohne jegliche Stromversorgung auskommt. Dazu zählen insbesondere Leitungen, Kabel und Patchkabel, Anschlussdosen, Stecker und Buchsen, Baugruppen, die lediglich passive Bauelemente enthalten (also Widerstände, Kondensatoren usw.) wie zum Beispiel die DSL-Splitter, werden meistens auch dieser Gruppe hinzugerechnet.

Aktive Netzwerkkomponenten sind alle Geräte, die aktiv Signale verarbeiten beziehungsweise verstärken können (Netzwerkgeräte). Sie benötigen dazu eine Stromversorgung. Zu dieser Gruppe gehören Hubs und Switches, Router, Bridges, Firewalls und Session Border Controller. Ein Bestandteil eines Computers kann ebenfalls eine Netzwerkkomponente sein, zum Beispiel Netzwerkkarte und ISDN-Karte.

Im Folgenden werden ausgewählte Netzwerkkomponenten kurz vorgestellt.

Switch
Ein Switch ist ein Kopplungselement, das mehrere Stationen in einem Netzwerk miteinander verbindet. In einem Ethernet-Netzwerk, das auf der Stern-Topologie basiert dient ein Switch als Verteiler für die Datenübertragung.

Router
Router verbinden Netzwerke mit unterschiedlichen Protokollen und Architekturen. Router finden sich häufig an den Außengrenzen eines Netzwerkes. Hier wird die Verbindung zu anderen Netzen und dem Internet geschaffen.

Gateway
Ein Gateway ist eine Hardware oder Software oder eine Kombination daraus, die eine Schnittstelle zwischen zwei inkompatiblen Netzwerken darstellt. Das Gateway sorgt dafür, dass die Form und Adressierung der Daten in das jeweilige andere Format und die Protokolle eines anderen Netzes konvertiert werden.

Firewall
Eine Firewall ist eine Schutzmaßnahme gegen fremde und unberechtigte Verbindungsversuche aus dem öffentlichen (Internet) ins lokale Netzwerk. Mit einer Firewall lässt sich der kommende und gehende Datenverkehr kontrollieren.

Datum, Unterschrift Ausbildender

Datum, Unterschrift Auszubildender oder Ausbildende

protokollieren, sperren und freigeben. Dabei ist die Firewall genau zwischen dem öffentlichen und dem lokalen Netzwerk platziert. Meist ist die Firewall Teil eines Routers. Sie kann aber auch als externe Komponente einem Router vor- oder nachgeschaltet sein.

Server
Ein Server ist ein Computer, der Rechenleistung, Speicher, Daten und Dienste in einem Netzwerk bereitstellt und die Zugriffsrechte darauf verwaltet. In den Regel handelt es sich um ein jeweils angepasstes System, der Rechenleistung, Speicherplatz und I/O-Leistung auf kleinstem Raum bereitstellt, und je nach Anwendungsfall mit spezieller Hardware und Software ausgestattet ist.

Der Begriff "Server" ist mehrdeutig. Zu unterscheiden ist zwischen Hardware und Software. Wenn Hardware gemeint ist, wird häufig die Bezeichnung "Server" verwendet. Wenn von Software die Rede ist, verwendet man die Begriffe "Service", "Dienst", "Anwendung" und "Applikation" oder benennt die eingesetzte Software.

Name des/der Auszubildenden:	Mustermann, Max
Datum:	01.08.2021
Thema des Fachberichts	Hardwarekomponenten

Hardwarekomponenten

Hardware ist der Oberbegriff für die physischen Komponenten (die elektronischen und mechanischen Bestandteile) eines datenverarbeitenden Systems. Die einzelnen Komponenten eines Computers sind klassischerweise Festplatte, Mainboard, Prozessor, Laufwerke, Arbeitsspeicher, Maus, Tastatur, Gehäuse, Lüfter und Netzteil. Hinzu kommt optionale Hardware, zum Beispiel in Form eines Scanners oder einer Webcam.

Mainboard

Das Mainboard ist die Hauptplatine eines PCs. Sie verbindet die Hardwarekomponenten des Systems. Auf ihr befinden sich Steckplätze für CPU (Central Processing Unit), RAM (Random Access Memory) und Schnittstellen für Laufwerke. Jedes Mainboard hat einen Chipsatz, der die Leistungsfähigkeit des Mainboards wiederspiegelt.

CPU (Central Processing Unit)

Die CPU (auch Hauptprozessor genannt) ist die zentrale Recheneinheit des Computers. Sie führt Rechenoperationen durch und steuert andere Hardwarekomponenten. Die CPU wird über einen Prozessorsockel mit dem Mainboard verbunden.

Laufwerke

Laufwerke unterscheide ich in magnetische Laufwerke (Festplatten) und in optische Laufwerke. Die Festplatte (auch HDD – Hard Disc Drive genannt) besteht meist aus mehreren drehbaren Platten, Schreib- und Leseköpfen, einem Motor zum Antreiben der Schreib- und Leseköpfe und der Elektronik (für die Fehlerkorrektur).

Optische Laufwerke verwenden verschiedene Medien zum Beispiel CDs, DVDs, HDs, Blu-Ray Discs. Zur Speicherung und Archivierung von Datenbeständen sind diese ideal geeignet.

RAM (Random Access Memory)

Der RAM (auch Arbeitsspeicher genannt) eines Computers ist die Bezeichnung für den Speicher, der die gerade auszuführenden Programme oder Programmteile und die dabei benötigten Daten enthält. Der Hauptspeicher ist eine Komponente der Zentraleinheit. Da der Prozessor unmittelbar auf den Hauptspeicher zugreift, beeinflussen dessen Leistungsfähigkeit und Größe in wesentlichem Maße die Leistungsfähigkeit der gesamten Rechenanlage.

Grafikkarte

Die Aufgabe der Grafikkarte ist es Signale in Bildschirmanzeigen umzuwandeln und damit dem Benutzer eine bequeme Schnittstelle zu bieten, die die Kommunikation

mit der Hardware ermöglicht. Eine Grafikkarte besteht meistens aus einer GPU (Graphics Processing Unit), dem Video-RAM, RAMDAC (Random Access Memory Digital/Analog Converter) und einem Anschluss für den Monitor.

[illegible]

Name des/der Auszubildenden:	Mustermann, Max
Datum:	01.08.2021
Thema des Fachberichts	Grundlagen der Netzwerksicherheit

Grundlagen der Netzwerksicherheit

Jede Organisation, die von Kunden und Mitarbeitern geforderte Services bereitstellen möchte, muss ihr Netzwerk schützen. Netzwerksicherheit umfasst jede beliebige Aktivität, welche die Funktionsfähigkeit und Integrität eines Netzwerks schützt. Netzwerksicherheit kombiniert dabei mehrere Verteidigungsebenen am Netzwerk-Edge und im Netzwerk. Jede Netzwerksicherheitsebene implementiert Richtlinien und Kontrollen. Autorisierte Benutzer erhalten Zugriff auf Netzwerkressourcen, Angreifer werden jedoch davon abgehalten, Bedrohungen in Umlauf zu bringen.

Eine Verbindung kann immer dann als sicher angenommen werden, wenn die Gegenstellen einer Verbindung sich gegenseitig authentifiziert haben und die Übertragung der Daten verschlüsselt ist. Die Netzwerksicherheit umfasst dabei meist folgende drei Pfeiler, Authentizität, Vertraulichkeit und Integrität.

- Bei der Authentizität der Kommunikationspartner geht es darum festzustellen, ob der Kommunikationspartner auch tatsächlich der ist, für den er sich ausgibt.
- Bei der Vertraulichkeit einer Kommunikation geht es darum dafür zu sorgen, dass niemand Einblick in die Daten und Kommunikation erhält.
- Zur Integrität zählen Mechanismen und Verfahren, die die Echtheit von Daten prüfen und sicherstellen können und somit auch vor Manipulation schützen.

Ein Netzwerk auf Basis von TCP/IP teilt sich grob gesehen in die Anwendungsschicht, die Netzwerkschicht und die Übertragungsschicht. Auf allen Schichten lassen sich Maßnahmen zur Verbesserung der Sicherheit einsetzen. Fast aller dieser Maßnahmen und Verfahren sind optional.

In der Übertragungsschicht kommen meist Tunneling-Protokolle zum Einsatz, die beliebige Netzwerk-Protokolle übertragen können. Auch für die Anwendung, die eine solche Verbindung nutzt, spielt das Protokoll auf der Übertragungsschicht keine Rolle. Die hohe Flexibilität wird mit einem großen Verarbeitungsaufwand wegen mehrfacher Header erkauft.

Auf der Netzwerkschicht werden häufig Paketfilter (Firewall) und Masquerading (NAT) verwendet. Paketfilter dienen zur Einschränkung oder Verhinderung von Datenverkehr während Masquerading HSTS (HTTP Strict Transport Security) gezielt versteckt. Diese Sicherheitsverfahren sind eng mit der Netzwerkschicht verwoben und funktionieren in diesem Fall nur mit TCP/IP. Auf der Netzwerkschicht wird auch oft mit einer Firewall gearbeitet.

Sicherheitsmechanismen auf der Anwendungsschicht sind direkt mit dem Dienst, einer Anwendung oder einer Sitzung gekoppelt. Sie können nicht einfach anderweitig genutzt werden. Das ist jedoch kein Nachteil, sondern mit einer hohen Sicherheit

Datum, Unterschrift Auszubildender

Datum, Unterschrift Ausbildender oder Ausbilderin

verbunden. Sofern Anwendungen Sicherheitsprotokolle unterstützen, sind sie bei kurzzeitigen Verbindungen das sicherste Verfahren.

Darüber hinaus soll Sicherheitssoftware vor unberechtigten Zugriffen durch Schadsoftware schützen. Die meisten Angriffe und Zugriffe erfolgen über den Versuch, Schadsoftware durch Unachtsamkeit des Nutzers einzuschleusen, zu installieren und zu aktivieren und somit Zugriff auf das System zu bekommen. Beispiele hierfür sind Viren, Würmer, Trojaner, Malware, Rootkit und Fakeware.

Virenscanner sind Bestandteil einer Sicherheitssoftware, die einen Computer im laufenden Betrieb auf Viren, Würmer und Trojaner untersucht. Dabei wird neben dem Arbeitsspeicher auch die Festplatte nach verdächtigen Dateiinhalten durchsucht. Zusätzlich klinken sich Virenscanner dort im Betriebssystem ein, wo Daten zwischen Massenspeicher und Arbeitsspeicher übertragen werden, um zu verhindern, dass Schadsoftware zur Ausführung kommt. Weil sich Schadsoftware im Laufe der Zeit weiterentwickelt und von einem normalen Programm teilweise nicht zu unterscheiden ist, eignen sich herkömmliche Mittel, wie der klassische Virenscanner nicht mehr, um einen Großteil der Schadsoftware zu erkennen. Aus diesem Grund baut moderne Sicherheitssoftware immer öfter auf Verhaltenserkennung.

Name des/der Auszubildenden:	Mustermann, Max
Datum:	01.08.2021
Thema des Fachberichts	Cyber-physisches System

Cyber-physisches System

Cyber-physische Systeme, oft mit CPS abgekürzt, bestehen aus mechanischen Komponenten, Software und moderner Informationstechnik. Durch die Vernetzung der einzelnen Komponenten über Netzwerke wie das Internet lassen sich komplexe Infrastrukturen steuern, regeln und kontrollieren. Der Austausch von Informationen der miteinander vernetzten Gegenstände und Systeme kann in Echtzeit drahtlos oder kabelgebunden erfolgen.

Wesentliche Bestandteile sind mobile und bewegliche Einrichtungen, Geräte und Maschinen (darunter auch Roboter), eingebettete Systeme und vernetzte Gegenstände.

Das Funktionsprinzip basiert auf Sensoren, Aktoren und vernetzter Software. Sensoren liefern Messdaten aus der physischen Welt und melden sie über Netzwerke an eine Software weiter, die sie verarbeitet. Daraus ergeben sich die Steuerdaten, die die Software über das Netz an Aktoren weitergibt. Häufig sind die einzelnen Komponenten in eine Cloud-Architektur eingebunden. Menschen können auf die Cyber-physischen Systeme einwirken, indem sie über Benutzeroberflächen Abläufe konfigurieren, steuern, kontrollieren oder Informationen abrufen. Die Cyber-physischen Systeme lösen die herkömmlichen lokal geschlossenen Systeme ab, die keine übergreifende Kommunikationsfähigkeit besitzen.

Cyber-physische Systeme kommen in vielen verschiedenen Anwendungsbereichen zum Einsatz und decken ein großes Spektrum möglicher Funktionen ab. Anwendungsgebiete ergeben sich in der Logistik, in der Industrieproduktion, in der Umwelttechnik, der Medizintechnik, in der Verteidigungstechnik oder in der Verkehrstechnik. Ziel der Systeme ist es, für eine höhere Effizienz, niedrigere Kosten und schnellere Bearbeitung von komplexen Vorgängen zu sorgen. Beispiele für Cyber-physische Systeme sind Smart Grid (intelligente Stromnetze), Tsunami- oder Erdbeben-Warnsysteme, militärische Drohnen oder Flugabwehrsysteme sowie Fahrer-Assistenzsysteme und autonome Fahrzeuge.

Cyber-physische Systeme sorgen für zahlreiche Vorteile bei der Steuerung und im Betrieb komplexer Systeme. Sie sind extrem anpassungs- und wandlungsfähig und tragen zur Effizienzsteigerung bei. Prozesse laufen weitgehend autonom und automatisiert ohne den Bedarf des menschlichen Eingriffs ab. Dir erfüllen Menschen nur noch Kontroll- und Steuerungsfunktionen. Auch die Arbeitssicherheit und die Geschwindigkeit von Abläufen lässt sich mit den Cyber-physischen Systemen steigern.

Dem gegenüber stehen einige Nachteile, die sich aus der Komplexität der Technik ergeben. So können die Strukturen und Abläufe sehr anfällig sein. Zudem entstehen Abhängigkeiten, die beim Ausfall einzelner Komponenten oder Infrastrukturteile Gesamtprozesse lahmlegen können. Arbeiten die Systeme überwiegen autonom,

kann es dazu kommen, dass falsche Entscheidungen getroffen werden oder auf unvorhergesehene Ereignisse nicht passend reagiert wird. Schäden an Maschinen oder Menschen sind unter Umständen die Folge.

Eine weitere Gefahr besteht durch die bewusste Manipulation von Cyber-physischen Systemen durch Hacker oder Angreifer. Aufgrund der vernetzten Strukturen sind die Systeme gegen Angriffe oder feindliche Übernahmen besonders zu schützen.

Name des/der Auszubildenden:	Mustermann, Max
Datum:	01.08.2021
Thema des Fachberichts	Anforderungsanalyse

Anforderungsanalyse

Die Anforderungsanalyse ist in der Informatik ein Teil des Systementwicklungsprozesses sowie der Business-Analyse. Das Ziel einer Anforderungsanalyse ist es, die Anforderungen an ein durchzuführendes Projekt zu ermitteln, zu konkretisieren, zu strukturieren und zu prüfen. Das Ergebnis einer Anforderungsanalyse wird meistens in einem Lastenheft dokumentiert oder bei einer agilen Softwareentwicklung resultiert daraus ein Product Backlog.

In einer Anforderungsanalyse wird häufig zwischen funktionalen und nichtfunktionalen Anforderungen differenziert. Bei den funktionalen Anforderungen handelt es sich um Anforderungen, welche direkt dem Projekt dienen. Es handelt sich um für das Projekt spezifische Anforderungen. Bei nichtfunktionalen Anforderungen handelt es sich um Anforderungen, die auch an andere Projekte oder Vorhaben gestellt werden können, wie beispielsweise Zeitverhalten oder Ressourcenverbrauch.

Die Anforderungsanalyse hat zwei grundlegende Aufgaben:

- Informationssammlung: Informationen werden nicht nur gesammelt, sondern die daraus entstehenden Anforderungen auch auf Machbarkeit und Risiko geprüft. Das gesammelte Wissen wird zudem mit Expertenwissen kombiniert und angepasst.
- Konsensbildung: Die Anforderungsanalyse soll ein unternehmensweites gemeinsames Verständnis über alle betroffenen Personengruppen schaffen und zu einer Konsensbildung führen. Da jede Gruppe die Anforderungen an das Vorhaben definiert, können diese aufeinander abgestimmt und angepasst werden. Sie dient dabei auch als Basis für weitere Schritte wie Kommunikation, Ausschreibungen, Vertragsgestaltungen, Systemarchitektur und weiteres.

Die Anforderungsanalyse umfasst im Wesentlichen vier Schritte, die in verschiedenen Modellen abgebildet werden (zum Beispiel IEEE, CMMI, Volere, IIBA, PRINCE).

In einem ersten Schritt werden Anforderungen gesammelt. Hierbei kann beispielsweise auf ein bestehendes Lastenheft zurückgegriffen, Anwendergespräche geführt oder andere Methoden genutzt werden, um einer erste Informationsrecherche durchzuführen. Alle Anforderungen, die mit dem Projekt oder Vorhaben in Verbindung stehen, sollten zunächst gesammelt und dokumentiert werden.

Die im ersten Schritt gesammelten Anforderungen werden in einem nächsten Schritt ausgewertet. Dabei werden die Informationen klassifiziert und beispielsweise unter einem Kosten-Nutzen-Aspekt bewertet. Die Anforderungen werden zudem auf

Name des/der Auszubildenden:	Mustermann, Max
Datum:	01.08.2021
Thema des Fachberichts	Anforderungsanalyse

Vollständigkeit und Konsistenz geprüft und mit anderen Anforderungen verglichen, um ähnliche zusammenfassen zu können.

Sobald alle Anforderungen gesammelt und analysiert wurden, können diese in einer einheitlichen Form detailliert beschrieben und in einem Dokument zusammengefasst werden. Damit die Anforderungen auch für andere leicht verständlich sind, empfiehlt es sich, diese in einzelnen Anwendungsfällen zu beschreiben.

Der letzte Schritt stellt die Anforderungsrevision dar. Im Hinblick auf einen kontinuierlichen Verbesserungsprozess ist es ratsam, festgeschriebene Anforderungen zu einem späteren Zeitpunkt neu zu überprüfen und gegebenenfalls anzupassen.

Die konkreten Bestandteile einer Anforderungsanalyse hängen nicht nur von dem Projekt, sondern auch von der Zielsetzung ab. Ganz allgemein lassen sich die folgenden Inhalte als elementare Bestandteile der Anforderungsanalyse herauskristallisieren:

- Definition der Zielsetzung
- Allgemeine Beschreibung des Vorhabens
- Festlegung von Definitionen und Abkürzungen
- Definition der funktionalen und nichtfunktionalen Anforderungen
- Beschreibung des Ist-Zustands
- Beschreibung des Soll-Zustands

Name des/der Auszubildenden:	Mustermann, Max
Datum:	01.08.2021
Thema des Fachberichts	Agile Softwareentwicklung

Agile Softwareentwicklung

Agile Softwareentwicklung bezeichnet Ansätze im Softwareentwicklungsprozess, die dafür sorgen sollen, dass Entwicklungsprojekte einfach, unbürokratisch und iterativ ablaufen. Dazu wird versucht, die Entwurfsphase auf ein Mindestmaß zu reduzieren und im Entwicklungsprozess so früh wie möglich zu ausführbarer Software zu gelangen. Diese wird in regelmäßigen, kurzen Abständen mit dem Kunden abgestimmt. So soll es möglich sein, flexibel auf Kundenwünsche einzugehen, um so die Kundenzufriedenheit insgesamt zu erhöhen. Agile Softwareentwicklung zeichnet sich durch selbstorganisierende Teams sowie eine iterative und inkrementelle Vorgehensweise aus.

Agile Prinzipien dienen als Leitsätze für agile Arbeit. Manchmal werden agile Prinzipien auch als Methoden bezeichnet. Die zwölf Prinzipien agiler Softwareentwicklung lauten:

- Kundenzufriedenheit durch frühe und kontinuierliche Auslieferung wertvoller Software.
- Anforderungsänderungen sind auch spät in der Entwicklung willkommen.
- Funktionierende Software (regelmäßig und möglichst zügig) innerhalb weniger Monate oder Wochen liefern.
- Tägliche Zusammenarbeit zwischen Fachexperten und Entwicklern.
- Ein Projekt erfordert motivierte Individuen, die das richtige Umfeld sowie Unterstützung und Vertrauen benötigen.
- Informationen für das Entwicklungsteam sollten im direkten Gespräch vermittelt werden.
- Der Projektfortschritt bemisst sich an funktionierender Software.
- Agile Prozesse fördern nachhaltige Entwicklung (Auftraggeber, Entwickler und Benutzer sollten auf unbegrenzte Zeit ein gleichmäßiges Tempo halten können.)
- Agilität erfordert einen steten Blick auf technische Raffinesse und gutes Design.
- Einfachheit ist ausschlaggebend und definiert sich dadurch, die Menge nicht getaner Arbeit zu maximieren (doppelte Arbeit vermeiden).
- Selbstorganisierte Teams entwickeln die besten Architekturen, Anforderungen und Entwürfe.
- Das Team reflektiert regelmäßig selbst, wie es effektiver werden kann und passt sein Verhalten an.

Um diese Prinzipien umzusetzen, setzt man bei einem Softwareprojekt verschiedene agile Prozesse ein. Zu den beliebtesten agilen Prozessen zählen Scrum und das Kanban-Prinzip.

Datum, Unterschrift Auszubildender

Datum, Unterschrift Ausbildender oder Ausbilderin

Name des/der Auszubildenden:	Mustermann, Max
Datum:	01.08.2021
Thema des Fachberichts	Agile Softwareentwicklung

Scrum

Zu den wichtigsten Methoden der agilen Softwareentwicklung zählt das Scrum-Prinzip. Scrum wird nicht nur in der Softwareentwicklung eingesetzt, sondern ist inzwischen eine weit verbreitete Projektmanagement-Methode, bei der das Projekt in Form von sogenannten Sprints entwickelt wird.

Sprints laufen nach dem immer gleichen Schema ab. Zunächst werden dem Sprint im Rahmen eines Planungsmeetings Ziele und Dauer vorgegeben. Begleitet wird der Sprint mit täglichen Kurzmeetings, um das Team abzustimmen. Nach Abschluss des Sprints gibt es eine Sprint-Demo mit der Präsentation der Ergebnisse. Zu guter Letzt wird im Rahmen einer Sprint-Retrospektive ein Rückblick erstellt, der Verbesserungen des kommenden Sprints ermöglicht.

Auf diese Weise gibt es einen kleinteiligen, aber konstanten und sich ständig selbst verbessernden Entwicklungsprozess, der die Teammitglieder permanent motiviert. Zudem können Änderungen schnell umgesetzt werden.

Es werden drei Projektrollen definiert:

- Der Project Owner hält das Gesamtziel vor Augen und verbindet die Scrum-Teams mit dem Unternehmen oder Kunden.
- Der Scrum-Master agiert als Teamleiter, der für die Fortschritte und Koordination eines Teams verantwortlich ist. Gleichzeitig muss er in Absprache mit dem Project Owner dafür sorgen, dass optimale Bedingungen für sein Team bei gleichzeitig maximaler Effizienz des Teams gewährleistet sind.
- Das Scrum-Team wiederum ist ein Team aus maximal sieben Mitarbeitern, das sich um die Umsetzung der Vorgaben kümmert. Das Team sollte nicht größer sein, um die für Sprints notwendigen Absprachen innerhalb des Teams effektiv zu halten und ein „Wir-Gefühl" zu schaffen, das die Teamdynamik unterstützt.

Kanban

Anders als Scrum setzt Kanban vor allem auf die Fokussierung auf bestimmte Tätigkeiten. Mit anderen Worten geht es darum, möglichst wenige Aufgaben möglichst effektiv abzuhandeln. Dazu ist allerdings, anders als bei Scrum, deutlich mehr Planung notwendig.

Der Arbeitsfluss sollte vorab festgelegt werden, das Ziel eines jeden Teilnehmers muss sein, ein Ziel abzuschließen anstatt viele offene Aufgaben mit sich zu führen. Dadurch werden lähmende und konzentrationshemmende Ablenkungen möglichst eliminiert. Anders als bei Scrum gibt es vom Start weg eine durchaus zielgerichtete Vorstellung des Gesamtergebnisses.