ALLE PROTOKOLLE DES SCHULJAHRS 2018/19

MIS Hoheiser

5AHBGM

Inhaltsverzeichnis

Mitschrift am 10.09.2018

CIA-Triade

Von einer Ecke was weg, dass Niveau aufrecht zu erhalten, muss man bei den anderen 3 Ecken, was dazu stecken.

Jede Maßnahme, die man durchführt, kostet Geld.

Vertraulichkeit:

Nur bestimmte dürfen nur die Daten einsehen

Integrität:

Wer darf die Daten verändert. Nur berechtige Personen dürfen daten verändern. Muss nachweisbar sein.

Verfügbarkeit:

Leistungen der Maschinen müssen funktionieren. Dürfen nicht ausfallen, durch Störung. Kann ein Notfall sein

Gewisse rechtliche Aspekte die man betrachten muss, für jedes Element der Triade.

Die drei Elemente sind entstanden, weil es rechtliche Rahmenbedingungen gibt.

Integrität der Daten muss vorhanden sein.

DSGVO

Österreich hat früh erkannt, dass das DSGVO für Gesundheitsdaten ist zu wenig.

Neue Datenbank für jede Frau und Mann zugreifbar

https://www.ris.bka.gv.at

Wird immer von Elga und Gesundheitstelematikgesetz wird gesprochen

Datenschutz muss eine höhere Priorität bei Gesundheitsdaten haben als bei anderen.

Wenn zwei GDAs Gesundheitsdaten austauschen haben sie diese von Zugriff anderer zu schützen.

Ich muss verhindern das Unbekannte nicht Zugriff darauf haben. Integrität überlegen.

Jeder hat Technische und organisatorische Angaben zu treffen.

Das Objekt gehört der Stadt Wien. Also das AKH. Die Infrastruktur.

Wenn du es nachweisen kannst das die Infrastruktur von anderen nicht nutzbar ist, also physisch und technisch. Musst du es nicht verschlüsseln. So sagt es der Gesetzgeber.

Problem der Sicherheit im Deutschen. Wieso?

Auf einer Seite die Datenmanipulation und wir wollen sicher nicht, dass ein Patient stirbt.

Im englischen spricht man von Safety und Security.

Safety auf Person. Und Security auf Hard und Software.

Die zwei Daten, die zwischen den GDAs weitergeleitet werden, müssen verschlüsselt werden.

Weil wir nicht wollen das jemand tut was er will, haben wir ein eigenes Gesetz getroffen.

ELGA ist dafür da das alle GDAs sicher die Gesundheitsdaten untereinander austauschen können.

Verfügbarkeit:

Verschiedene Abhängigkeiten. Staatliche und kriminelle Organisation mit Cybersicherheitsbedrohungen, unsere Verfügbarkeit in Mitleidenschaft gezogen wird. Gesetzgeber sagt das wir eine Sicherheit brauchen.

Kritische Infrastruktur: wenn nicht mehr funktionieren, haben wir als Gemeinschaft ein Problem.

Es kann für uns gefährlich werden. Es könnte zu einer Plünderung kommen.

Wenn es jemanden gelingt anzugreifen, hat der Staat sehr schnell ein Problem.

Richtlinie wurde erlassen. Ist mit der Datenschutzordnung in Kraft gezogen ist.

Richtlinie: ist eine Vorgabe für alle Mitgliedstaaten ein Nationales recht zu erlassen. Mai 2018

Grundverordnung:

NIS = Network Information Security

Wenn wir wollen, dass wir nicht entsprechend Probleme haben bezüglich Cybercrime, dann müssen wir uns überlegen wie wir den Cyberschutz aufrechterhalten. Etwas wo wir als Gemeinschaft erkennen muss alle unsere Prozesse zu steuern.

Norm:

ist geregelt. Organisationen kümmern sich darum, dass sich Staaten daranhalten. Ist immer einstimmig zu beschließen

Standard:

was sich verschiedene Organisation wo sich Firmen zusammentun und sich auf ein gemeinsames Regelwerk abzustimmen aber kein Recht für ein Staat umzusetzen. Firmen können sich daranhalten müssen aber nicht. Standards können als Normen übernommen werden. Ist immer mehrstimmig zu beschließen.

Auf der IHE Norm basiert die Elga. Iso-Norm ist international. ISO-OSI-Modell

ICE 80001 gilt entsprechend und ist zu beachten.

Ethernet basiert auf CSMA/CD. Standard hat sich durchgesetzt.

IEEE ist der Standard.

ISO(8) 821.3

Ein Standard kann nicht vom Gesetz referenziert werden.

Eine Norm kann vom Gesetz referenziert werden.

Je breiter die Möglichkeit des Ankaufs ist, dann nur eine andere Rechnung bekommen.

IHE kommt aus dem Amerikanischen Bereich danach international.

Einheitliche Verbindungen und Modelle werden versucht zu ermöglichen.

Mitschrift am 24.09.2018

Risiko

- Abweichung vom Ziel

Wenn wir unseren Erfolg als Graph darstellen, dann weichen wir beim Eintreten einer als Risiko eingestuften Situation in die negative Richtung ab. Bei Erfolgen im Projekt, sogenannten Chancen bewegt man sich in die positive Richtung.

Mit Schutzmechanismen versuchen wir Faktoren, die unseren Erfolg in die negative Richtung abweichen lassen können einzuschränken und zu minimieren.
Dazu kommen technische und organisatorische Maßnahmen in Frage, für diese werden Regeln, sogenannte Policies benötigt. (Auch Dokumentenlenkung fällt in diese Kategorie)

In der Projektentwicklung bedeuten Risiken meist zusätzliche Kosten und Chancen sind meist mit Ersparnissen gleichzustellen.

Privacy by Design:

Schon in den ersten Atemzügen eines Projektes muss überlegt werden wie Sicherheit realisiert werden soll. Dies soll dazu führen, dass Sicherheit von Anfang an einen wichtigen Teil des Projektes einnimmt und später keine kostspieligen Maßnahmen getroffen werden müssen.

Privacy by Default:

Eingeplante Sicherheitsmaßnahmen müssen immer und ausnahmslos standardmäßig aktiviert sein. Als Beispiel kann der Airbag im Auto genannt werden, der eine Opt-out Möglichkeit für Sicherheit bietet aber im Normalfall immer aktiviert ist.

Security by Design:

- Schutz für das tatsächliche Produkt

  Im Gegensatz zum Begriff Safety geht es bei Security um die Sicherheit des Produktes (sei es Software oder Hardware) und nicht um die Sicherheit des Benutzers. Bei dem Erzeugen eines Produktes muss darauf geachtet werden technische und/oder organisatorische Maßnahmen zu treffen, die das Produkt bei Normalverwendung vor Einflüssen von außen zu schützen. Sollte das Produkt zum Erzielen einer höheren Security verändert werden, ist die Person, welche diese Veränderung durchgeführt hat per Definition der neue Verantwortungsträger.

GRC: Governance, Risks and Compliance

Der Nachweis, Sicherheitsmaßnahmen gesetzt zu haben, dies bringt einen Aufwand mit sich.

Mit der heutigen Informationsgesellschaft hat sich an Risiken ein grundlegender Faktor verändert: Die Geschwindigkeit, mit der sich beim Eintreten eines Risikos Informationen auf dem Globus verteilen. Wenn vor einigen Jahren eine als Risiko einzustufende Situation eingetreten ist hatten Firmen, die um ihre Sicherheit gebangt haben, noch Zeit gehabt Maßnahmen zu treffen. Diese Möglichkeit gibt es heutzutage nicht mehr, vielmehr kann die Situation mit einem Schädlingsausbruch auf eine Monokultur verglichen werden.

PDCA Zyklus: Plan, Do, Check, Act

Typische Vorgehensweise in der Projektentwicklung.

- Plan: Vorgehen planen
- Do: Geplantes Vorgehen durchführen
- Check: Fortschritt überprüfen
- Act: Dementsprechend handeln

Mitschrift am 01.10.2018

Tier – Inhalt

Tier 4:

- T1 (Client)
- T2 (Webserver)
- T3 (Business/Logical Server)
- T4 (Datenbank Server)

Tier 1, 2, ,3 und 4 sind Klassifikationen für Netze, um eine hohe Verfügbarkeit erreichen zu können.

Bei Tier 4 sind komplette Redundanzen vorhanden und dadurch ist die Verfügbarkeit sehr hoch.

Falls man eine Vielzahl an Clients hat und man nicht will das alle auf den Webserver zugreifen können benötigt man einen Proxy. (es darf nicht jeder auf den Proxy zugreifen und der Proxy greift dann auf den Webserver zu). Dafür muss jedoch ein Proxy-fähiges Protokoll verwendet werden.

Es gibt auch die Möglichkeit nach einem Proxy ein Reverse Proxy hinzuzufügen. Diese täuscht vor der Webserver zu sein aber greift eigentlich im Endeffekt nur auf den Webserver zu.

Ticketgranting:

Bei Ticketgranting werden Zertifikate zu einem gewissen Zeitpunkt dem Client mitgegeben, da wenn es nur ein Passwort geben würde ein Hacker, sobald er dieses besitzt, auf alles zugreifen könnte. Es gibt sowohl Software als auch Hardware Zertifikate und bei Hochsicherheit Zertifikaten wird eine dritte Instanz benötigt.

Internet:

offen Für alle

Intranet:

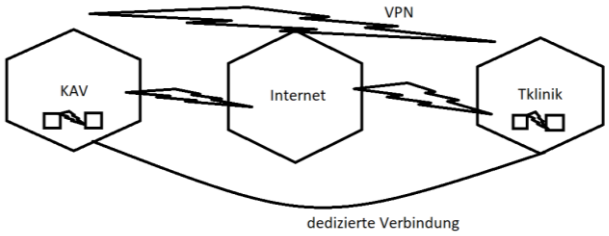
Internes Netz (sorgt für mehr Sicherheit)

Extranet:

Zwei dedizierte Netze die verbunden aber nicht durchs Internet erreichbar sind

Datenaustausch (nicht über das Internet:

Man kann entweder ein VPN (virtual private Network) oder eine dedizierte Verbindung einrichten, um Daten nicht über das Internet auszutauschen. Dies sorgt für mehr Vertraulichkeit.



Zeitfestlegung:

- Local Time: Es wird einmal eine Uhrzeit eingestellt und es wird immer weiter hinauf gezählt.
- UTC: Ein Client holt sich die Uhrzeit von einem Time-Server

Wofür einheitliche Zeit?

Da Transaktionsnummern dann leichter zu handhaben sind und z.B. die Fehlersuche dadurch erleichtert wird.

Authentifizierung:

- 1 Faktor Authentifizierung (Wissen):
  - Es wird nur ein Passwort benötigt
- 2 Faktor Authentifizierung (Wissen + Besitz):
  - Es wird ein Passwort benötigt und zusätzlich muss man noch etwas besitzen (z.B. Smartphone)
- 3 Faktor Authentifizierung (Wissen + Besitz + Biometrisches Merkmal):
  - Es wird ein Passwort, ein Gegenstand sowie ein Biometrisches Merkmal (z.B. Fingerabdruck) verlangt

Handysignatur:

Die Handysignatur ist „eineindeutig“ da für die Freischaltung ein Ausweis sowie die Meldestelle benötigt wird und für die Verwendung das Handy sowie das Passwort gebraucht wird.

Ergänzende Informationen:

Ein Netz ist immer nur so sicher wie sein schwächstes Element.

Mitschrift am 22.10.2018 (1)

E-Card in Spitälern

Österreichs Spitäler hätten einen zu großen, komplexen Aufwand, wenn alle Ambulanzen O-Cards verwenden würden. Deswegen gibt es eine Softwarelösung für diese Spitäler. Eine Ausnahme gibt es in Österreich, die die O-Card verwenden – die Barmherzigen Brüder. Den Vorteil, den Spitäler haben, damit sie diese IT-Lösung verwenden dürfen ist der, dass sie eine eigene IT-Abteilung im (Spital) Haus haben.

Arten der Zertifizierung

- Die Hardware wird zertifiziert
    - Das bedeutet, dass nur passende Hardware antworten von dem Server bekommt. Dadurch ist es nicht möglich eine „Man-in-the-Middle Attacke“ durchzuführen

Warteschlangenproblem

Das sogenannte Warteschlangenproblem besagt, dass die Personen in der Ambulanz nicht wissen, zu welcher Abteilung der Patient muss. Das hat das Problem zur Vorlage, dass es pro Abteilung eine eigene O-Card geben müsste, die jedes Mal neu gesteckt werden müsste. Ebenfalls würden Patienten, die später als andere Patienten da waren, jedoch ihre Schlange schneller ging, früher drankommen, als die Patienten, die vor ihnen da waren, jedoch noch in der Schlange stehen. Um bei diesem Problem entgegen zu wirken, gibt es die Softwarelösung.

Medienbruch

Die Darstellung von Medien bricht. Das bedeutet, dass Daten erst bestätigt werden sollten, bevor sie angezeigt werden, damit die Korrektheit der Daten garantiert werden kann.

E-Card – allgemein

Die E-Card ist ein Krankenscheinersatz und keine Identifizierung oder Registrierung.

Nicht jeder Krankenversicherter muss eine E-Card berechtigt. Grundsätzlich bekommen bzw. besitzen alle Personen, die eine Arbeitsberechtigung oder eine Aufenthaltsberechtigung in Österreich haben eine E-Card.

Versionen

- O-Card
  steht für Ordinationskarte. Diese Karte wird von dem Arzt bzw. Ordinationsgehilfin bei niedergelassen Ärzten verwendet.
- A-Card
  steht für Apothekerkarte. Wird bei den Apotheken genutzt.

- E-Card
  ist die reguläre Karte für jeden, der Krankenversichert ist.

Problematik

In der Ordination kann man alleine mit der E-Card nicht bestätigen, ob der Träger der E-Card auch der Besitzer der E-Card ist.

Zertifikatshirarchie

- Public Key
- Private Key

Wenn man beide Keys miteinander verbindet nennt man es Public Key Infrastructure (Wenn es verwendet wird, ist es eigentlich eine Closed Key Infrastructure) Dadurch ist es ohne Infrastruktur der E-Card nicht möglich Zertifikate zu überprüfen. Man stellt dem Server eine Anfrage, ob das Zertifikat möglich (verwendbar) ist, und antwortet nur dann. In Österreich können nur bestimmte Rechner diese Anfragen stellen (z.B. GINA-Box, …).

Problematik

Bürgerkarte: Man kann unterschreiben, weil das Zertifikat auf der E-Card sitzt. Das Zertifikat liegt in einem hohen Sicherheitsbereich. Die E-Card hat 4 Teile: 4. Teil: Netcard Projekt: Europäische Sozialversicherungskarte für den europäischen Bereich. Manche Länder können dies sogar schon lesen.

Methoden Identifizierung

Es gibt unterschiedliche Identifizierungsmethoden. Ein Beispiel für eine Mehrfaktorauthentifizierung ist die Handysignatur. Der Benutzer hat ein Passwort und einen dazugehörigen Code vom Handy. (2-Faktor)

1-Faktor

- Mit Hilfe eines Passworts

2-Faktor

- Mit Hilfe eines persönlichen Merkmals und einem Passwort

3-Faktor

- Mit Hilfe eines biometrischen Merkmals, einem persönlichen Merkmal und einem Passwort

Problematik beim Ausrollen

Die SVC hatte beim Ausrollen der E-Card ein unerwartetes, nicht bedachtes Problem. Jeder Arzt eine unterschiedliche Infrastruktur. Deswegen suchten sie mit einem Experten nach einer Lösung. Die damalige Telekom (heute A1) half ihnen eine Infrastruktur aufzubauen. Ebenfalls erstellten sie einheitliche Architektur schnellstmöglich.

Grundwissen – TCP/IP

Steht für Transmission Control Protocol/Internet Protocol (TCP/IP).

Ist eine Familie von Netzwerkprotkollen und wird aufgrund ihrer großen Bedeutung im Internet auch als Internetprotkollfamilie bezeichnet.

TCP/IP merkt sich die Verbindung bzw. hält sich auch aufrecht. Sie funktioniert nach dem Prinzip des 3-Wege Handschlags. Der besagt, dass der Client bei dem Server was anfragt, der Server fragt den Client an, und wenn beide sich einig sind ist der Prozess abgeschlossen. Der Nachteil von diesem Aufbau ist der lange Verbindungsaufbauvorgang bei kleinen zu übermittelten Dateien.

UDP/IP

Steht für User Datagram Protocol.

Diese Verbindung wird im Gegensatz zu TCP/IP nicht gehalten. Es wird nur in eine Richtung kommuniziert. Der Server nimmt nur Anfragen von gewissen Konfigurationen an. (z.B. passende Hardware oder Software)

RFC

Steht für resources in common. (?)

Dies ist ein Standard. Wesentlich dafür ist die Nr.1918. Diese besagt, wie private IP-Adressen auszusehen haben. Ebenfalls besagt dieses Regelwerk, dass diese IP Adressen private IP-Adressen verwendet werden.

Private IP-Adressen

Private IP-Adressen sind jene IP-Adressen, die das private Netzwerk nicht verlassen (z.B. das Home-WLAN bzw. Netzwerk). Auch werden sie „Hidden IP-Adressen“. Diese sollten von Servern abgelehnt werden.

IPv4

IPv4 ist eine Version der IP-Adressen. Sie setzt das Limit und wird derzeit verwendet. IPv6 ist der Nachfolger.

Man-in-the-Middle-Attacke

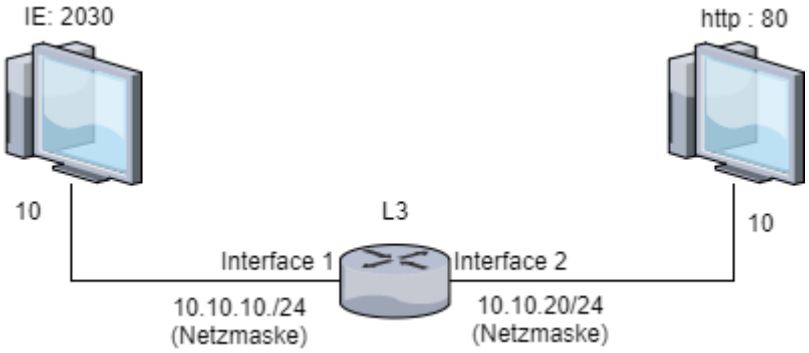
Diese Form von Attacke ist eine weitverbreitete Methode in Systeme einzudringen. Diese Form von Attacke wird wie folgt ausgeübt: Eine Verbindung zwischen Server und Client steht. In dieser dringt der Angreifer unbemerkt als Dritter ein und steht genau zwischen Client und Server. Dadurch kann er Daten abfangen und/oder verändern. So können Angreifer an Daten herankommen, oder Befehle an den Server, sowie an den Client senden. Bei TCP/IP ist in manchen Fällen diese Art von Angriff sehr einfach möglich.

Zusammensetzung einer IP-Adresse

- Subnetzmaske
  setzt eine Grenze in welchen Bereich sich die Computer (Clients) befinden
- Webbrowser senden im Normalfall einen generierten Code und erstellen einen eigenen Port am PC zum Öffnen, die Socket ID. Diese stellt den Endpunkt der Kommunikation da.
- Well-Known-Port
  sind normalisierte bzw. standardisierte Ports, wie z.B. die von http(s): 80 (bzw. für https: 443)
- Host Adresse
  ist jene Adresse, die zum Server/Client gehört
- TCP/IP Adresse
  ist jene Adresse, die auf die Netzwerkkarte gebunden ist.

Socket ID

Der Socket ID Punkt ist der Endpunkt einer Kommunikation. Stellt in bestimmten Fällen einen Port am PC bzw. in der Software dar. Das Default-Gateway schaut nach, welches Interface verwendet werden soll.



Kommunikationsmatrix

Eine Kommunikation zwischen zwei Kommunikationspartner ist immer, wie folgt, aufgebaut:
Aus einer IP-Adresse, eine Netzmaske, einem Port, einer Host ID, und einer Netz ID. Für jede gestartete Software, die eine Netzwerkanbindung nutzt, wird ein Port erstellt. Auch ein Beginn, und ein Ende. Das ist die sogenannte Kommunikationsmatrix.

Mitschrift am 22.10.2018 (2)

Proxy und reverse Proxy

Ein Proxy steht immer zwischen einem Server und einem Client. Die Anfrage kommt immer vom Client an dem Webserver.

Proxys besitzen ein Schützenden Funktionalität (Firewall). Der Firewall wird benötigt, wenn man zwei unterschiedliche Sicherheitsklasse eine Verbindung aufbauen wollen.

Beispiel: Internet und Intranet sind zwei unterschiedliche sicherheitsklasse.

Welche Sicherheitsklasse man benötigt hängt vom den jeweiligen Policy (Regelwerk) ab.

Proxys sind transparent, das bedeutet, dass für die Rufenden oder die Aufrufenden es sichtbar ist. Der Vorteil dabei ist, dass in den beiden Programmwelten keine Veränderungen bzw. Konfiguration benötigt werden. Die beide Kommunikationspartner werden in eine Zentrale punkt (demilitarisierte Zone) verwaltet.

Ein Proxy überwacht den Aufrufenden und überprüft welche Protokolle in Verkehr gebracht werden. In der OSI-Modell befindet sich der Proxy in der Applikation Layer.

Unterschied Proxy und reverse Proxy

Proxy:

- Stellvertreter für den Client
- Zugriff eines vom Client auf einem Server
- Clients verstecken, die auf einen Server zugreifen wollen
- Benötigt eine Konfiguration

Reverse Proxy:

- Stellvertreter für den Server
- Versteckt dem Webserver vor dem Client
    - Client greift nicht direkt auf dem Webserver zu
    - Reverse Proxy leitet die Anfrage des Clients weiter an dem Webserver
- Koordiniert den Traffic auf einer Webserver
- Überprüft ob die Seite erreichbar ist und ob Zugriff gewährt wird

Warum verwenden wir Proxy

Zur Überwachung der Kommunikation und Traffic des Clients mittels einer Überwachungskanal. Die Konsequenzen müssen die Verantwortliche tragen, spricht in Falle einer Anomalie soll jeder Zeit die Möglichkeit bestehen dieses System auszuschalten.

Clientvarianten

Auf dem entsprechenden Client wird die Traffic auf Viren überprüft (Antivirensystem), falls welche erkannt werden, werden diese eliminiert. Die Voraussetzungen hierfür ist das man auf dem Client entsprechende Konfigurationen durchführen darf, um entsprechenden Software zu installieren.

In der Medizinbereich ist dies aufgrund der Medizinproduktgesetz nicht möglich zu realisieren.
Beispiel:
Wenn der in Verkehr bringender eines Medizinprodukts keine Antivirensystem in sein Produkt vorsieht, so stellt dies eine Sicherheitslücke im System dar. Wenn man nun etwas am Medizinprodukt verändert oder anders als vorgesehen verwendet, so verfällt die Haftpflicht des Händlers und man Haftet selbst für jegliche Schaden.

Servervarianten

Der Proxy ist aus der Serverseitige aktiv und überprüft die Traffic. Bei einem gemeinsamen Punkt kann der Proxy oder Reverse Proxy, alles überprüfen.

Datenschutzverordnung (DSGVO)

- Security and Privacy by Design: Datenschutz durch Technikgestaltung
- Security and Privacy by Default: datenschutzfreundliche Voreinstellungen
    - disabled: Verantwortliche müssen bewusst sein, dass Sie über die Sicherheitsschwelle (Risiko) durchschreiten

ergänzende Informationen

Durch die Entwicklung und Produktionsüberwachung oder DEVOP verschwinden die Grenzen durch die Cloudentwicklung. ➔ Kapseln … Security Container

Mitschrift am 05.11.2018

DNS – Domain Name System:

Namensauflösung → Hinter jeder URL versteckt sich eine IP-Adresse

Port 53:

für DNS

UDP – User Datagram Protocol:

Kein 3Wege Handshake

Wie findet die Adresse seinen DNS-Server.
In den Konfigurationseinstellungen wird definiert wer dein DNS-Server ist.

Wenn wir z.B:. www.spengergasse.at abfragen, was läuft ab?

Der Client schickt eine Anfrage an DNS-Server

TCP/IP - Transmission Control Protocol/Internet Protocol:

Hierarchie DNS

Oberste Rechner im DNS „.“ → Root. 15 Rechner weltweit

Resolver Auflösung für DNS über Konfiguration

Resolver → Hat auch eine IP-Adresse

TOP-Level-Domain: .at .de ….

Root-Server haben Top-Level-Domains.

Second Level Domain: spengergasse

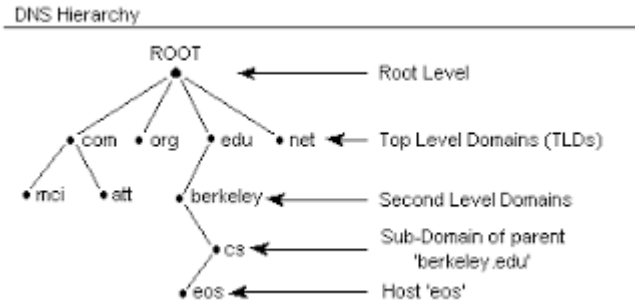
Spengergasse hat auch einen DNS-Server → Verwaltet die entsprechenden Rechnernamen

DNS-Server (2)

DNS-Server hat das Recht die Second Level Domain zu verwalten in dem Fall „spengergasse“ und gibt eine Antwort

Die erste Antwort vom DNS-Server: zählt am meisten

Wenn der DNS-Server das Recht hat die Domain zu verwalten (wird konfiguriert) wenn der Server nicht antworten kann dann leitet er die Anfrage an den Forwarder weiter.

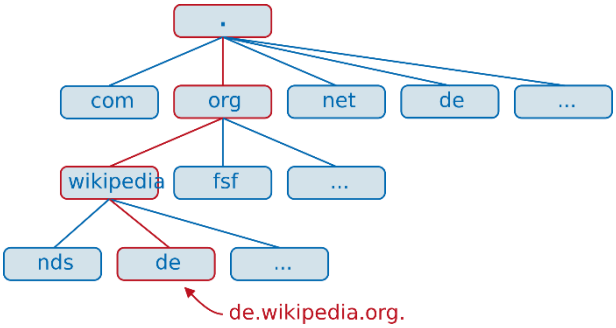


Forwarder → Der Dns-server hat einen eingetragenen DNS-Server, der übergeordnet ist. Wenn er keinen Forwarder hat dann geht er in die Root Logik.

Abhängigkeit von den Root-Servern. → Verträge zwischen Ländern (Von der UNO gelöst)

Risiko: Wirtschaftskriege (Absturz der Kommunikation)

DNS-SERVER von der Spengergasse: hat keinen Eintrag z.B über orf.at und geht zum Forwarder und wenn der keinen Eintrag hat dann schickt er ihn weiter bis er die IP-Adresse bekommt.



DFD:

Risikoanalyse → Wenn ein Angriff passiert dann betrifft es eine Person → Restrisiko1

DNS → Hierarchisches Protokoll → Es gibt immer einen Client und einen Server
Server kann auch zum Client werden → Wenn er die Anfrage nicht auflösen kann, bzw. es nicht im Cache hat, dann geht er zum übergeordneten DNS-Server und fragt nach der IP-Adresse

Instanzen: Forwarder oder die Rootlogik

Forwarder split: Interne DNS-Server kommunizieren mittels einen Forwarder split das heisst sie gehen nicht über den externen DNS-Server

Hidden-DNS: Versteckte DNS → bei meisten Organisationen → Man versteckt die Infrastruktur

Auflösung der DNS-Records kann nur im Intranet erfolgen
Im internet ist die Auflösung nicht möglich

DNSextern Rechner eingetragen die von außen erreichbar sein dürfen z.B mein Webserver

Hierarchie:

Root	.

Top-Level-Domain(TLD)	at
Sub-Level-Domain(SLD)	orf
Host	www

Wir wissen nicht ob der Host ein Rechner ist oder ein C-Name ist.

Deny of Service Attacke

Wenn ich einen Rechner mit zu vielen PACKETEN beglücke dann bricht der Rechner seinen Service ab.

Multihomed: Rechner mit mehreren Netzwerkkarten
Darf nicht Routing eingeschalten haben → Weil er sonst alle Routingprotokolle in seine Liste einträgt und die Router Funktion ersetzt

Intermediate System:

Physical Layer → Repeater (Signalverstärker)
DLL → Switch oder Bridge
Network Layer → Router

Mitschrift am 26.11.2018

Transmit-Receive/Firewall

Kurzzusammenfassung:

Zum Senden und Empfangen werden immer 2 Kanäle an beide Clients und Server benötigt.

Noch kurz beschrieben werden:

- Bits
- Ports
- Applikation-Firewall/ Reine Firewall

Inhalt Transmit-Receive/Firewall

Ports:

- http: 80
- https: 443

Skizze Client -> Server mit Request & Response mit einer Firewall.

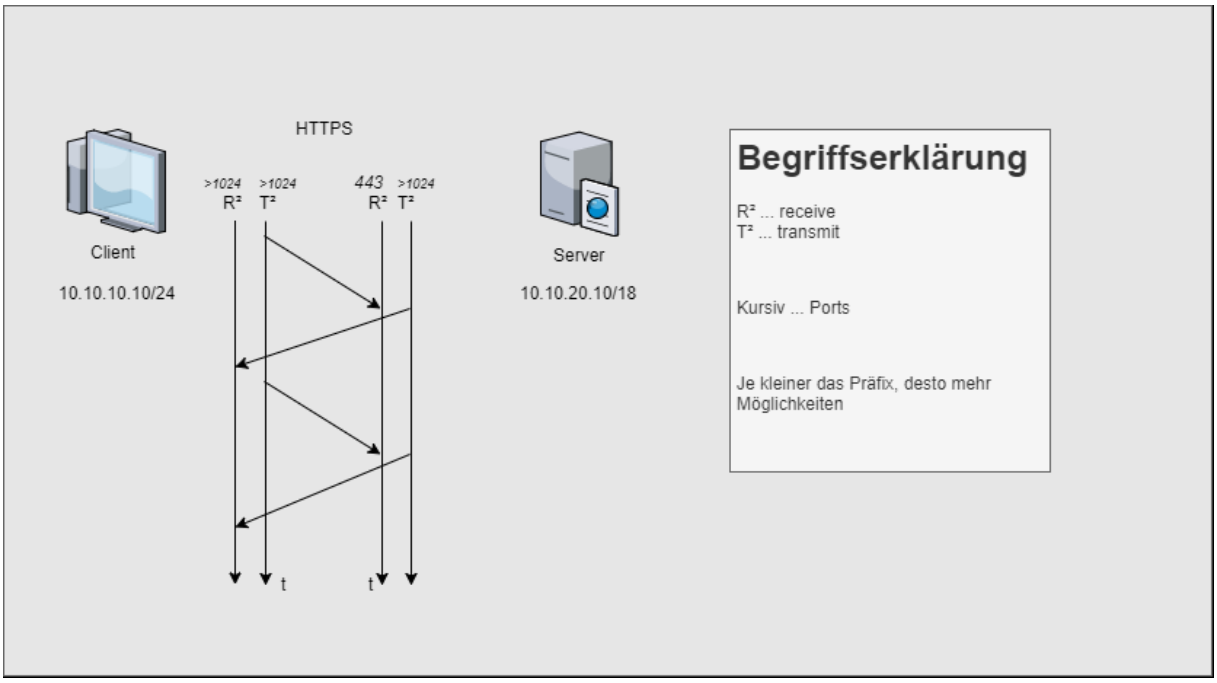
Die Pfeile nach untern sind die zeitlichen Abläufe des Kommunikationsprotokolls. (t steht für die Zeit)

Die erste Zeitachse zeigt

Damit sie kommunizieren können, brauchen sie ein Absende und ein Empfangsboard (commit…)

Sende und Empfangskanal brauchen wir bei Client und Server:

- Transmit und Receive vom Client
- Transmit und Receive vom Server



T → Transmit

R → Receive

Die Portnummer stehen über den Pfeilen

- Server Receive – 443 Port
- Server Transmit– größer als 1024
- Client Receive – größer als 1024
- Client Transmit– größer als 1024

Client: 10.10.10.10/18

Server: 10.10.20.10/ 18

Präfix: wird mit / getrennt

Networkmaske

0 →2 → 4→ 8→ 16 → 32 → 64→ 128 → 255

10.10.20.10/.18 = 255.255.192.0 Netzmaske
192 weil 64 und 128
Ersten 24 Bit fix → Präfix
Intermedia System; Indem Fall fehlt ein Router bei diesem BSP daher wird es anstatt /24 zu 18
Im dritten Oktett steht 20

Wie viele Rechner können adressiert werden: über 9 tausend ?-2 weil 0 und 1 nicht verwendet werden dürfen. (Null zählen 0→2→4→..)

Applikation-Firewall	**Reine Firewall**
Simuliert den Server	Alle Ports größer als 1024 werden durchgelassen
Und hört nur auf die Applikation	Client weiß ja nicht, was von wem benötigt wird
So steuerbar mit Ports und IP-Adresse	

ENISA → Sicherheitsbehörde der EU

Wenn der Server nicht mit https geschützt wird, kann er simuliert werden und dies kann dazu führen, dass der Server von jemand anderen übernommen wird.

Vor allem wenn es um Personenbezogene Daten geht darf muss die Sicherheit des Patienten garantiert sein.

Safety: es darf zu keiner Fehlfunktion beim Patienten kommen.

Mitschrift am 03.12.2018

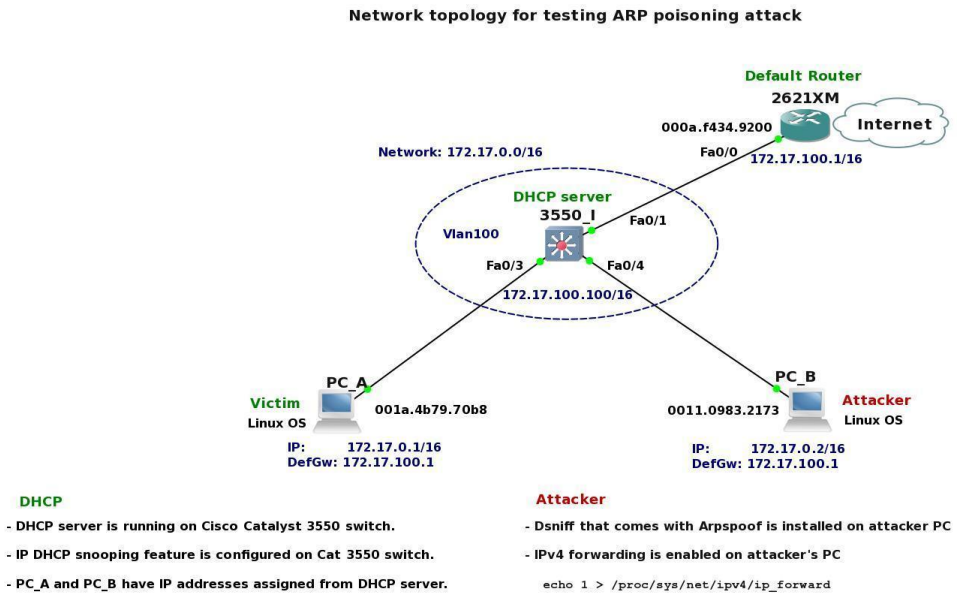
MAC Address Poisoning (Lange Beschreibung)

Definition:

ARP-Spoofing, oder auch ARP Request Poisoning bezeichnet das Senden von gefälschten ARP-Paketen. Es wird benutzt, um die ARP-Tabellen in einem Netzwerk so zu verändern, dass anschließend der Datenverkehr zwischen zwei (oder mehr) Systemen in einem Computernetz abgehört oder manipuliert werden kann. Es ist eine Möglichkeit, einen Man-In-The-Middle-Angriff im lokalen Netz durchzuführen.

Ziel eines derartigen Angriffes kann auch IP-Telefonie sein, um Telefonate abzuhören.

Trotz der Bekanntheit und des Alters des Angriffes bieten gängige Betriebssysteme keinen Schutz vor ARP-Spoofing an. Dieser muss in der Regel nachgerüstet werden.



Dieses Bild zeigt einen ARP-Vergiftungsangriff auf ungesicherte Netzwerkinfrastruktur.

Konsequenzen:

Damit hat ein Angreifer bei ungeschützten Verbindungen, wie sie beim Senden von E-Mails oder Betrachten von Webseiten verwendet werden, fast freie Hand zum Mitlesen und Manipulieren. Verschlüsselte und authentifizierte Verbindungen sind tendenziell sicher; sie verwenden oft sichere kryptografische Algorithmen und digitale Zertifikate zur Authentifizierung der Gegenstelle.

Klinkt ein Angreifer sich zum Beispiel in eine HTTPS-Verbindung ein, um das Homebanking zu manipulieren, so erkennt der Anwender dies an einer Warnmeldung des Browsers über ein ungültiges Zertifikat. Ein Angreifer kann allerdings in praktischen Szenarien Benutzer daran hindern, TLS-Verbindungen aufzubauen und kann die angeforderten HTTPS-Verbindungen durch solche über HTTP ersetzen. So ist es möglich, Daten, die sonst verschlüsselt versendet würden, trotzdem abzufangen.

SSH-Verbindungen sind dann als sicher einzustufen (SSH Version 1 nicht), wenn ein veränderter Fingerprint zum Abbruch des Verbindungsaufbaus führt. Oft wird der Benutzer nach Anzeige der Fingerprints aufgefordert, zu entscheiden, ob er mit dem Verbindungsaufbau fortfahren möchte.

Funktionsweise:

Um den Datenverkehr zwischen Host A und Host B abzuhören, sendet der Angreifer an Host A eine manipulierte ARP-Nachricht zur Zuordnung einer bestimmten IP-Adresse. In dieser Nachricht ist seine eigene MAC-Adresse anstelle der von Host B enthalten, so dass Host A zukünftig die Pakete, die eigentlich für Host B bestimmt sind, an den Angreifer sendet. Dasselbe geschieht mit Host B, so dass dieser Pakete statt direkt an A nun ungewollt zum Angreifer sendet. Der Angreifer muss nun die von A und B erhaltenen Pakete an den eigentlichen Empfänger weiterleiten, damit eine abhörbare Verbindung zustande kommen kann. Ist dies geschehen, so arbeitet der Angreifer unbemerkt als Proxy. Man spricht dabei von einem Man-In-The-Middle-Angriff. Der Angreifer kann selbstverständlich auch den Netzwerkverkehr verwerfen, um eine Kommunikation zwischen bestimmten Hosts unmöglich zu machen oder aber den Datenverkehr verändern.

Während ein reines Abhören des Netzwerkverkehrs mit Hilfe eines Sniffers nur in ungeswitchten Netzwerken funktioniert, ist dieser Angriff auch in geswitchten Netzwerken erfolgreich. Software, die diese Proxy-Funktion implementiert, ist für alle gängigen Betriebssysteme kostenlos im Internet zu erhalten und relativ leicht zu bedienen.

Erkennung, Prävention und Schutz:

Die folgenden Methoden sind empfohlene Maßnahmen zum Erkennen, Verhindern und Schützen von ARP-Spoofing-Angriffen:

- Paketfilterung: Paketfilter prüfen Pakete, wenn sie über ein Netzwerk übertragen werden. Paketfilter sind bei der Verhinderung von ARP-Spoofing nützlich, da sie Pakete mit widersprüchlichen Quelladressinformationen (Pakete von außerhalb des Netzwerks, die Quelladressen von innerhalb des Netzwerks und umgekehrt anzeigen) herausfiltern und blockieren können.
- Vermeiden Sie Vertrauensbeziehungen: Organisationen sollten Protokolle entwickeln, die auf Vertrauensbeziehungen so wenig wie möglich angewiesen sind. Vertrauensbeziehungen verlassen sich bei der Authentifizierung nur auf IP-Adressen, sodass Angreifer ARP-Spoofing-Angriffe wesentlich einfacher ausführen können, wenn sie vorhanden sind.
- Verwenden Sie ARP-Spoofing-Erkennungssoftware: Es gibt zahlreiche Programme, mit denen Organisationen ARP-Spoofing-Angriffe erkennen können. Diese Programme arbeiten, indem sie Daten prüfen und zertifizieren, bevor sie übertragen werden, und das Blockieren von Daten, die scheinbar gefälscht sind.
- Verwenden Sie kryptografische Netzwerkprotokolle: Transport Layer Security (TLS), Secure Shell (SSH), HTTP Secure (HTTPS) und andere sichere Kommunikationsprotokolle unterstützen den ARP-Spoofing-Angriff, indem Sie Daten vor der Übertragung verschlüsseln und Daten authentifizieren, wenn sie empfangen werden.

MAC Address Poisoning (Kurze Beschreibung)

Vortäuschen einer **gefälschten MAC Adresse**

Funktioniert nur in einem **LAN** (=Local Area Network) = lokales Netzwerk

Technische Eingrenzung: **Topologie** (=Ausprägung)

Intermediate System = IS

Layer 1 = Repeater (=REP) “wiederholen“, „verstärken“

Layer 2 = Switch

Bekommt physikalische Flanke (weiß nicht ob eine Collision vorliegt)

Lernt in welchem Segment sich welches Element befindet (A, B, C, und für D gibt es ein Router Interface R_1)

Wenn Topologie nicht bekannt, Abwehr von Angriffen schwer

wenn keine Switch Logik → fällt in Repeater Logik zurück?

90% der Pakete fallen in Repeater Modus zurück, wenn Switch mit Paketen belastet ist (Funktion gefährdet)

Folge: keine Switch-Funktion mehr

Layer 3 = Router

Angreifer muss die MAC Adresse kennen

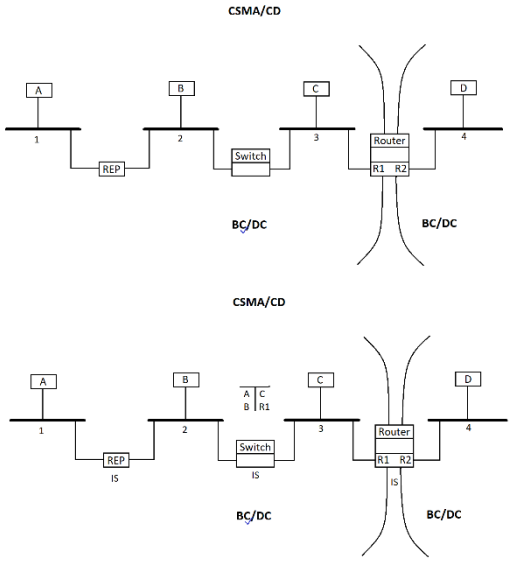
Verhindert Collisions und Broadcasts! → trennendes Element

Grenze der Broadcast Domain: Router

Bsp.

4 kennt die IP-Adresse vom Router, der Router kennt die IP-Adresse vom PC

3 schickt an 4 → Pakete gehen über den Router an 4

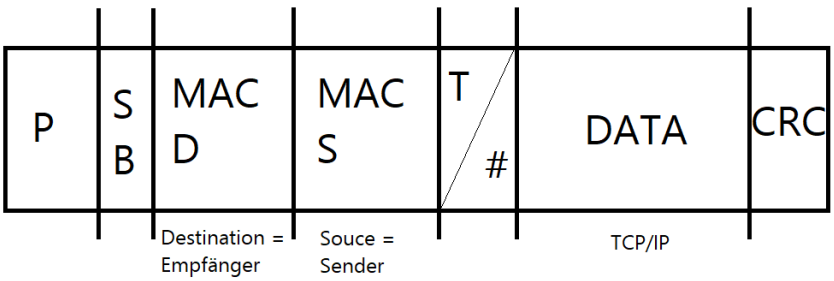


MERKSATZ

In einem LAN ist jeder Rechner Nachbar des anderen Rechners, wenn dieser direkt erreichbar ist

Ist D Nachbar von C, B oder A? – Nein

Blockierung durch Broadcastdomäne (für verbreiten von Paketen)



Mitschrift am 10.12.2018

Eldar wischt die Tafel ab
Basti geht zu der Tafel

Wiederholung der letzten Stunde (jeder kann das natürlich, wie immer)
Basti zeichnet die Grafik auf die Tafel

OSI-Referenzmodell

Was ist die 1. Schicht?
Die Bitübertragungsschicht (englisch: Physical Layer) ist die erste Schicht des OSI-Referenzmodells und des hybriden Referenzmodells. Die Übertragungsmedien und alle Geräte, die direkt mit den Medien verbunden sind, das schließt auch Antennen, Stecker und Repeater ein, sind Teil der Bitübertragungsschicht. Die Art und Weise, wie die Daten (Bitfolgen) auf den Übertragungsmedien gesendet werden, legen Leitungscodes fest, deren Definition auch Teil dieser Schicht ist.

Was macht der WLAN – Repeater?

Je nach Modell können Sie die Reichweite des kabellosen Internets bis zu 100 Meter vergrößern. Dabei funktioniert der Repeater wie eine Funkstation, die das Router-Signal aufnimmt und dann weiterleitet.

Unterschied zwischen Switch und Repeater:

- Als Verteiler kommt ein Switch im Netzwerk zum Einsatz, wenn die Anschlüsse für Ethernet-Kabel am vorhandenen Router nicht ausreichen, um alle kabelgebundenen Geräte ins Netzwerk zu bringen.
- Repeaters sind dann nützlich, wenn ein WLAN auch in entlegene, abgeschirmte Winkel von Wohnung und Büro dringen soll und ein Netzwerkkabel mit Access Point dafür nicht in Frage kommt. Ein Repeater wird dagegen nicht die Bandbreite oder den Datendurchsatz erhöhen – im Gegenteil.

Was ist IEEE 802.3?

Ethernet ist eine Familie von Netzwerktechniken, die vorwiegend in lokalen Netzwerken (LAN), aber auch zum Verbinden großer Netzwerke zum Einsatz kommt (WAN).
Für Ethernet gibt es eine Vielzahl an Standards, für die das Institute of Electrical and Electronics Engineers (IEEE) verantwortlich ist. Seit der Einrichtung einer Arbeitsgruppe für den Standard eines lokalen Netzwerks ist der Name "Ethernet" das Synonym für alle unter der Arbeitsgruppe 802.3 vorgeschlagenen und standardisierten Spezifikationen.

Bei Ethernet spricht man von einer paketvermittelnden Netzwerktechnik, deren Standards auf den Schichten 1 und 2 des OSI-Schichtenmodells die Adressierung und die Zugriffskontrolle auf unterschiedliche Übertragungsmedien definieren. Die Nutzdaten kommen bereits in Datenpaketen von den darüberliegenden Protokollen. Zum Beispiel von TCP/IP. Diese Datenpakete werden mit einem Header versehen und anschließen im Ethernet-Netzwerk übertragen. Ich würde

Quelle: https://www.elektronik-kompendium.de/sites/net/0603201.htm

Das IP-Adressierungsschema beinhaltet die Informationen, die benötigt werden, eine Nachricht irgendwo auf der Welt zuzustellen, es ist für das Internet konzipiert. Das Internet-Protokoll beinhaltet zum einen das IP-Adressierungsschema, zum anderen die Protokollinformationen für einen ungesicherten Datentransport. IP ist ein Protokoll der Schicht 3, der Vermittlungsschicht (Network Layer). IP gehört zu den routebaren Protokollen.

Mitschrift am 14.01.2019

Inhalt:

Kein Überblock über Topologie → kann man keine Informationen schützen

Verschiedene Prozesse die digital unterstützt werden, diese liegen vor z.B in einem Spital: Röntgen, Labor, Apotheke u.a. auch Zugriffsberechtigungen

Verwaltungsprozesse, ob das Haus seine Leistungen erbringen kann, ob das Personal Schulungen, Dienstplan, Zahlungen bekommt, sofern sie nicht in die Technik fallen.

Ohne Prozesse und ohne Topologie, können wir nicht die digitalen Prozesse schützen, man zielt dabei auf CIA

Bei der Verfügbarkeit geht es um eine messbare Qualität. Zu einer bestimmten Zeit eine bestimmte Leistung, man muss nicht unbedingt verfügbar sein →Effizienzmessung

ISO/OSI:

7 Schichten, verschiedene Aufgaben und Protokolle →Frage: Wenn wir die Schichten betrachten und die TCPIP v4 (Version 4) vergleichen. Wo liegt der Unterschied? ISO/OSI hat 7 Schichten und IPv4 hat 4 Schichten. (Warum ist das so, TCPIP älteres Protokoll, in der Überlegung keine 7 Schichten eingesetzt, weil keinen Netzwerkprogramme abgebildet werden sollten. ISO/OSI Modell ist ein generisches Modell, heißt man kann es zwischen mehreren Protokollen verwenden, nicht nur bei einem, wie beim TCPIP v4.)

Wir referenzieren heutzutage auf ISO/OSI arbeiten aber mit dem TCPIP Modell.

Wichtiges was wir haben in diesem Bereich: Warum heißt das Netzwerk local area network und warum hat es die Definition, dass die Nachbarn……//

Intermediate System:

Vermittlungssysteme, 3 unteren Schichten vom ISO/OSI.

Sonderfunktion:

Broughter (Brücke), Layer 3 Switch (Network Router) → auf der Komponente werden verschiedene logische Netze zusammengeführt, aber an verschiedenen Enden raus, ab 3 Han weg routet er nicht mehr, sondern switched und wird zu switch

Local Area Network

Wenn jeder Rechner ein direkter Nachbar ist.

Jede logische Adresse hat eine physische Adresse.

ARP Table:

ist die Tabelle, die logische IP-Adresse zu einer physischen mapped (MAC Adresse: Media Access Number, wir sprechen physikalisches Protokoll an, ISA Net Adresse, Adress Resulution Protokoll) gibt es nur bei End Systemen und bei Intermediate Systemen (Layer 3 Router)

Endsysteme kommunizieren immer miteinander

Mitschrift am 21.01.2019

Inhalt

Gesetzliche Rahmenbedingungen im Medizinischen Informationsbereich, eines davon: primaryheltcare center. Ziel ist eine größere Auswahl der Ordinationszeiten zu ermöglichen. Alle Umsetzungen müssen nach dem IHE Modell umgesetzt werden, dieses ermöglicht Austausch zwischen GDAs, daher soll ELGA verwendet werden. ELGA basiert auf einem Gesetz mit Verordnungen, Minister kann Verordnungen verfeinern. Der Patient soll in der Elga nur, laut Verordnungen ELGA-Anwendungen ansehen können, daher soll der Patient auch alle Gesetze anwenden können. Das wichtigste dabei ist den, in ELGA gespeicherten, Zugriff auf Dokumente zu steuern. Alle Dokumente, die nicht in LEGA gespeichert werden, sind daher nicht betroffen

Dokumente haben Zugriffsberechtigungen, diese erfolgen in der ELGA nach dem Prinzip: der Arzt kann in einer gewissen Zeitspanne darauf zugreifen, der Patient kann sich abmelden (Opt-Out; permanent, situativ)

- situativ -> Patient kann sagen dieser Bericht soll nicht auf ELGA gespeichert werden (oder ausgeblendet)
  Bei Damen: bei Chromosom Defekt kann eine Schwangerschaft abgebrochen werden aber nur während der Behandlung nicht mehr im Nachhinein

Der Patient kann kein Löschen der Daten in der ELGA löschen lassen. Wenn man innerhalb elektronischer Prozesse agiert sind Regeln. Hierfür benötigt man eine Identifikation. Eine Identifikation ist kein technischer Prozess, es ist ein rein organisatorischer Prozess, d.h. in einem organisatorischen Prozess muss einen Nachweis erbringen, um die Person korrekt zuordnen zu können, man benötigt einen Ausweis. Das Anlegen eines User oder einer Berechtigung entspricht dem Anlegen eines Avatars. Man kann eine Authentifizierung mit Kriterien erstellen, um diesen Avatar beschreiben zu können. Die gesamte ELGA referenziert sehr stark auf das e-govenrment. Eine Anwendung hierbei ist die Identifikation und die anschließende Authentifikation. Wenn der Anmeldende mit der Bürgerkarte seine Informationen weitergibt, sind die Prüfer nicht verpflichtet dies zu melden. Wenn die trotzdem erfolgt kann man eine Anzeige erhalten da man selbst für die Sicherheit seiner Dokumente zuständig ist.

Es gibt eine **A**potheke Card, **O**rdination Card, E-Card, bei keinem dieser Vorgänge gibt es eine Prüfung daher gibt es hier keine Identifikation, daher muss man bei der Aufnahme einen Ausweis dabeihaben. Es wird nur geprüft, dass eine A-, O-Card gesteckt wird nicht wer. Bei z.B. einer Bankomatkarte muss man einen PIN angeben.

Es gibt 3 Varianten der Authentifizierung:

1) User, Passwort
2) Physischer beweis (Karte)
3) Biometrisch (Fingerabdruck, Iris Scan, …)

Ohne 2 Faktor Authentifizierung kann kein valider Beweis gestellt werden. Der Prüfer muss schauen ob alle Faktoren (Karte, Passwort) übereinstimmen.

Dies gilt auch für die EU → ist im e-government Gesetz der EU definiert, daher kann jemand aus Deutschland einfach in Österreich sich authentifizieren. Durch die Authentifizierung bekommt man eine Rolle, durch diese bekommt man Berechtigungen, das ist das System der ELGA. Dort wird nur validiert ob eine E-Card, bei einer bestimmten Organisation, gesteckt wurde.

Mitschrift am 18.02.2019

Inhalt

Viele Rechtssysteme -> Gesetze

Das wichtigste sind dabei die stillen Teilhaber.

Ein Arzt darf kein Arzt einstellen
-> Arzt öffnet eine Praxis und stellt

Gruppenpraxis
-> Mehrere Ärzte in einer Praxis (aber gleiche Ausrichtung)

Primary Healthcare Center
-> Eine virtuelle Ordination mehrerer Ärzte und Praxen. Um differenzieren zu können, wer auf welche Daten Zugriff haben darf.

Deshalb benötigen wir dafür ein Berechtigungs- und Protokollierungssystem. **Geschlossene Umgebung** (zentralesVerwaltungssystem -> AktiveDirectory mit einem oder mehreren Domain Controllern) besser als **Föderierte** (jeder Rechner in der Workgroup verwaltet seine eigenen Berechtigungen).

Geschlossene Umgebung – zentrale Architektur:
Der Lokale Rechner gibt die gesamte Verwaltung an den Domain Controller. → Der Administrator hat dadurch Zugriff auf mein Account, da mein Account von dem Domain Controller verwaltet wird.
- haben wir in Österreich nicht!

Normalerweise in Österreich: mehrere Lokale Rechner und wenige zentrale Rechner → Föderiertes System → man muss Rechte vergeben (applicatorisch), mit gewissen **Vorgaben**. Wir benutzen das IHE konforme System **ELGA**. Das Gesetzt verlangt, dass ein GDA nur dann auf Patientendaten zugreifen darf, wenn dieser mit dieser Person ein Behandlungsverhältnis hat. → nicht möglich, dass ein GDA auf meine Daten zugreifen kann, bevor ich nicht dort war → Patient muss zuerst aufgenommen werden, er war schon mal da, war in der Ambulanz, hat seine e-card gesteckt, wurde in einem Spital aufgenommen (→ Rechtliche erlaubnis diesen Patienten zu behandeln und die Daten einzulesen). Um sich international ausweisen zu können gibt es einen National Contactpoint (Nationaler Server um Patienten über Organisations oder Landesgrenzen hinaus zu Identifizieren → Föderiertes Identitymanagement (An verschiedenen Stellen wird die Identität geprüft und durch bestimme Protokolle von der Source zur Destiny weitergegeben))

Voraussetzungen, um Daten einzulesen und Patient behandeln zu dürfen:

1. Der Mediziner, der behandelt muss ein Behandlungsverhältnis aufweisen (Bestätigung durch die Sozialversicherung, dass die e-card gesteckt wurde, wenn keine vorhanden ist muss der Patient sich anders ausweisen. **International → National Contactpoint: Nationaler Server**)
    - **Niedergelassener Bereich**: Validierung durch stecken der e-card
    - **Größere Organisationen:** stecken der e-card ist keine Voraussetzung. Es raucht aus, wenn eine Aufnahme durchgeführt wird (e-card wird auch verwendet muss aber nicht)

Ergänzende Informationen

epSOS: European Summary ….

BKI: Anzahl von Rechnern die Zertifikate ausstellen (Elektronischer prüfbarer Ausweis) → dazu braucht man verschiedene Protokolle

Föderiertes Identitymanagement: Es gibt verteilte Instanzen, an verschiedenen Stellen wird die Identität geprüft und durch bestimme Protokolle von der Source zur Destiny weitergegeben. → in der **ELGA** heißt das **Lapita**.

Grundvorrausetzung beim Entwickeln von medizinischer Software: Safety by design → der Developer muss sich mit der richtigen Implementierung, gemäß der Voraussetzungen beschäftigen.

SSL: v2 und v3, man sollte v3 einsetzen. Verschlüsselter Transport von Daten
TLS: neuerer besserer verschlüsselter Transport von Daten

DOKA Container: sind abgespeckte virtuelle Maschinen, wo sehr viele auf einem Server laufen können und in einem DOKA Container läuft ein Service. Sind miteinander verbunden → man braucht http**s**, damit die Daten nicht abgefangen werden können!

Mitschrift am 18.03.2019

Verschlüsselungsverfahren

2 Formen: symmetrisch, asymmetrisch

Warum heißt das eine sy und das andere asy? → Symmetrie: gleichmäßig, asymmetrisch: ungleichmäßig

Sy Aszicode:

eindeutige Zahl die in den entsprechenden 8 Bit verwendet wird. Ein Einfaches Schlüsselverfahren wäre symmetrisch

Cäsarschifre:

ist ein einfaches symmetrisches Verschlüsselungsverfahren, das auf der monographischen und monoalphabetischen Substitution basiert. Als eines der einfachsten und unsichersten Verfahren dient es heute hauptsächlich dazu, Grundprinzipien der Kryptologie anschaulich darzustellen. Der Einfachheit halber werden oftmals nur die 26 Buchstaben des lateinischen Alphabets ohne Unterscheidung von Groß- und Kleinbuchstaben als Alphabet für Klartext und Geheimtext verwendet und Sonderzeichen, Satzzeichen usw. nicht beachtet.

Stabtverschlüsselung

Papyrus gehabt und über stab gewickelt und man hat seine Nachricht auf Zeile geschrieben wo man das gedreht hat. Der Schlüssel war der Durchmesser des Stabs

Deschifrieren

Ein Schlüssel, der entschlüsselt und verschlüsselt.

Franzose hat sowas ähnliches gemacht wie Cäsarschifre- er hat bei jeder Zeile, die er geschrieben hat Verschiebungsmechanismus geändert – hat versucht das erraten der Texte schwieriger zu machen, man wusste nicht nach welchem Mechanismus er vorgegangen ist

Enigma - ist eine Rotor-Schlüsselmaschine, die im Zweiten Weltkrieg zur Verschlüsselung des Nachrichtenverkehrs der Wehrmacht verwendet wurde. Auch Polizei, Geheimdienste, diplomatische Dienste, SD, SS, Reichspost und Reichsbahn setzten sie zur geheimen Kommunikation ein. Trotz mannigfaltiger vor und während des Krieges eingeführter Verbesserungen der Verschlüsselungsqualität gelang es den Alliierten mit hohem personellem und maschinellem Aufwand, die deutschen Funksprüche nahezu kontinuierlich zu entziffern.

Passwörter

Hacker verwenden Wörterbuchattacke: man sammelt Wörter die Leute gerne verwenden (Passwörter) und versucht diese als erste auszurechnen.

Passwörter müssen bestimmte länge haben, aus verschiedenen Zeichen bestehen usw.

Je länger Passwörter werden, desto schwieriger berechnet man diese.

Verschlüsseln

Verschlüssen ist die erste Aktion – wichtig das man weiß welchen Schlüssel man als 2tes verwendet – verschränkt

damit Menschen diese Dinge einfacher verstehen, hat man für das eine das wording verschlüsseln und für das andere das wording signieren

wenn wir verschlüsseln haben wir das Ziel, das wir eine Nachricht nur für den Empfänger lesbar machen wollen

Pretty Good Privacy

(PGP; engl. „ziemlich gute Privatsphäre“) ist ein von Phil Zimmermann entwickeltes Programm zur Verschlüsselung und zum Unterschreiben von Daten.

PGP

benutzt ein sogenanntes Public-Key-Verfahren, in dem es ein eindeutig zugeordnetes Schlüsselpaar gibt:

Genutzt wird ein öffentlicher Schlüssel, mit dem jeder Daten für den Empfänger verschlüsseln und dessen Signaturen prüfen kann, und ein privater geheimer Schlüssel, den nur der Empfänger besitzt und der normalerweise durch ein Passwort geschützt ist. Nachrichten an einen Empfänger werden mit dessen öffentlichem Schlüssel verschlüsselt und können dann ausschließlich mittels seines privaten Schlüssels entschlüsselt werden. Diese Verfahren werden auch asymmetrische Verfahren genannt, da Sender und Empfänger zwei unterschiedliche Schlüssel verwenden.

Die erste Version wurde 1991 geschrieben und verwendete einen RSA-Algorithmus zur Verschlüsselung der Daten. Spätere Versionen benutzten den Elgamal-Algorithmus.

Bei PGP wird aber nicht die ganze Nachricht asymmetrisch verschlüsselt, denn dies wäre viel zu rechenintensiv und es wäre nicht praktikabel, dieselbe Nachricht an mehrere Empfänger zu schicken. Stattdessen wird die eigentliche Nachricht symmetrisch und nur der verwendete Schlüssel asymmetrisch verschlüsselt (Hybride Verschlüsselung). Dazu wird jedes Mal ein symmetrischer Schlüssel (session key) zufällig erzeugt.

Dieser symmetrische Schlüssel wird dann z. B. per RSA- oder Elgamal-Kryptosystem mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und der Nachricht hinzugefügt. Dadurch ist es möglich, eine Nachricht für mehrere Empfänger gleichzeitig zu verschlüsseln. Eine für mehrere Empfänger verschlüsselte Nachricht sieht dann folgendermaßen aus:

PGP basiert dabei auf dem sogenannten Web of Trust, bei dem es keine zentrale Zertifizierungsinstanz gibt, sondern Vertrauen von den Benutzern selbst verwaltet wird.

Da PGP darauf ausgelegt ist, Nachrichten dauerhaft entschlüsseln zu können, wird, falls es einem Angreifer gelingt, einen privaten Schlüssel zu erlangen, die gesamte Kommunikationshistorie dieses Schlüssels kompromittiert. Für Instant Messaging wurde als Alternative zu PGP Off-the-Record Messaging (OTR) entwickelt; dabei bleibt auch bei späterer Kompromittierung des privaten Schlüssels die verschlüsselte Kommunikation unlesbar für den Angreifer (allerdings auch für den legitimen Schlüsselbesitzer)

Mitschrift am 29.04.2019

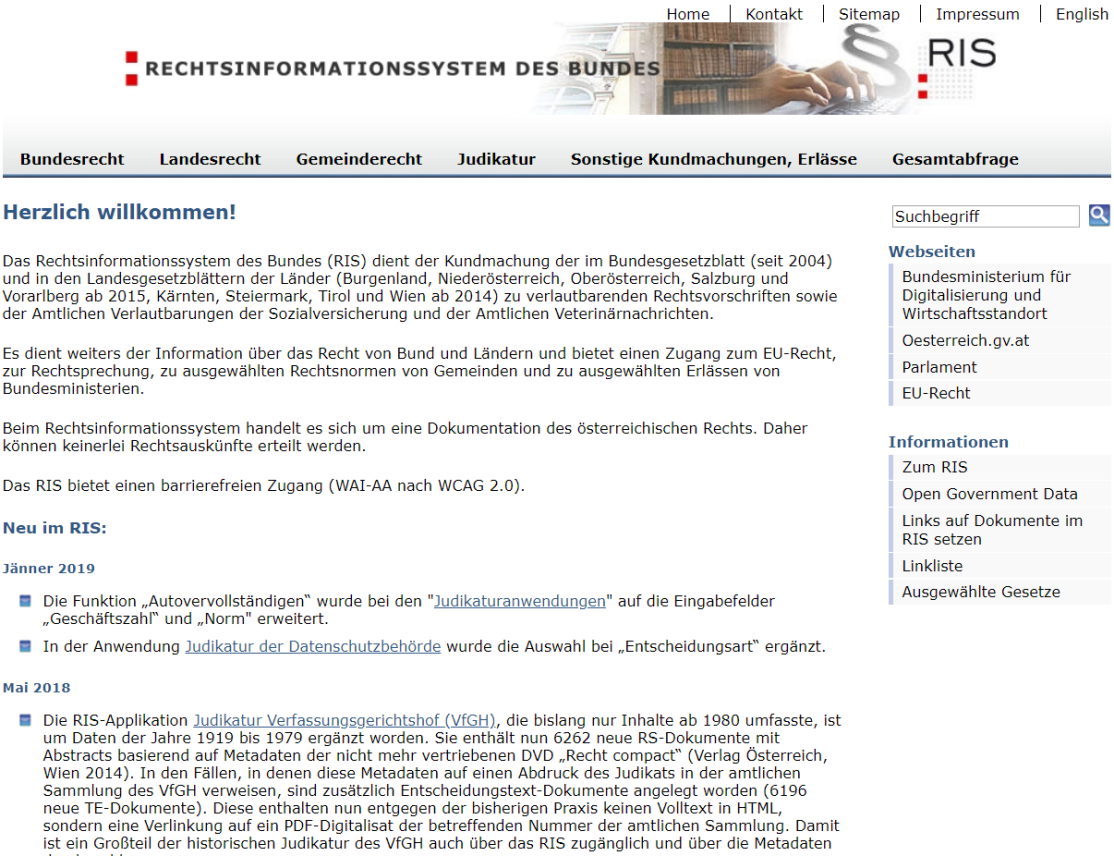
Verordnungen

sind unmittelbar geltendes Recht, verbindliches Recht für die Mitgliedsstaaten und die Bürger. Es bedarf keines legislativen Umsetzungsaktes durch die Staaten. Die Staatsorgane müssen die Verordnung vollziehen.

Richtlinien

sind dagegen nur für die Staaten verbindlich und geben diesen ein zu erreichendes Ziel vor, das sie dann durch nationale Gesetze umsetzen müssen.

Gesetze können im RIS nachgelesen werden:



https://www.ris.bka.gv.at/

Österreich → Verordnung → der Minister hat das Recht eine Verordnung zu erlassen

Ministerium:

- Bundeskanzler
- Bundesminister für Inneres

Das Innenministerium ist für die Umsetzung für die Verordnungen der Sektoren (z.B Gesundheitswesen) zuständig

Medizinische Prozesse können von dem polizeilichen Wesen beeinflusst werden

Ausfälle oder Beeinträchtigungen (z.B Cyberagriff), die länger als 3 Stunden andauern sind zu melden! → **Meldepflicht**

Informationssicherheit auf dem Computer sicherstellen:

- Virtuelle Maschinen für die Entwicklung verwenden
- Infortmationssicherheitsmanagementsystem
- Security by Design und Security by Default

EPU → Ein-Personen-Unternehmen

Infortmationssicherheitsmanagementsystem (ISMS)

definiert Regeln und Methoden, um die Informationssicherheit in einem Unternehmen oder in einer Organisation zu gewährleisten.

Risikoanalyse → Welche Risiken können auf mein Entwicklumgsenviroment einwirken?

Control → Steuerungselement, eines Entwicklungsrechners

Governance

ist die Unternehmensführung durch definierte Richtlinien. Dazu zählt die Festlegung von Unternehmenszielen, die darauf angewandte Methodik zur Umsetzung und die Planung der notwendigen Ressourcen für das Erreichen der Ziele.

Risk

steht für das Risikomanagement mit bekannten und unbekannten Risiken durch definierte Risikoanalysen. Ein wichtiger Faktor dabei ist das frühzeitige Auseinandersetzen mit Risiken, der Bereitstellung von Strategien zur Risikominimierung und dem Vorbereiten von Schadensfallpuffern bei Risikoeintritt.

Compliance

ist das Einhalten interner wie externer Normen für die Bereitstellung und die Verarbeitung von Informationen. Diese beinhaltet unter anderem Vorgaben aus Normierungsbestrebungen und die Zugriffsreglementierung für die Daten sowie die gesetzlichen Rahmenbedingungen für deren Verwendung.

Regelmäßig kontrollieren, ob die Konfigurationen dem letzten Stand entsprechen!

DevOps → saubere Entwicklungsumgebung und Operations

Risiko → Risiken sind die aus der Unvorhersehbarkeit der Zukunft resultierenden, durch "zufällige" Störungen verursachten Möglichkeiten, von geplanten Zielwerten abzuweichen. → beeinflussen den Erfolg

Mitschrift am 13.05.2019

Verschiedene Varianten von Entwicklungsumgebungen: eine davon Docker.

Logik der IP-Architektur

Localhost:

- IP-Adresse: 127.0.0.1
    - Logische Instanz
    - Connection als Instanz innerhalb des Netzwerkes gesehen

3 Modi, wenn Container / virtuelle Maschine startet:

- Isoliert
    - Docker läuft nicht auf 127er Netz -> nicht erreichbar -> isoliert

3 Möglichkeiten bei Start:

- Instanzen möchten miteinander kommunizieren -> gebridget
    - Bleibt in virtuellen Kommunikation -> geht nicht nach außen

Bridge-Funktion:

Mehrere Varianten:

- Versteckt
    - Für alle anderen nur über offizielle Adresse des Interfaces erreichbar
- Publiziert

Mehrere virtuelle Maschinen / Container:

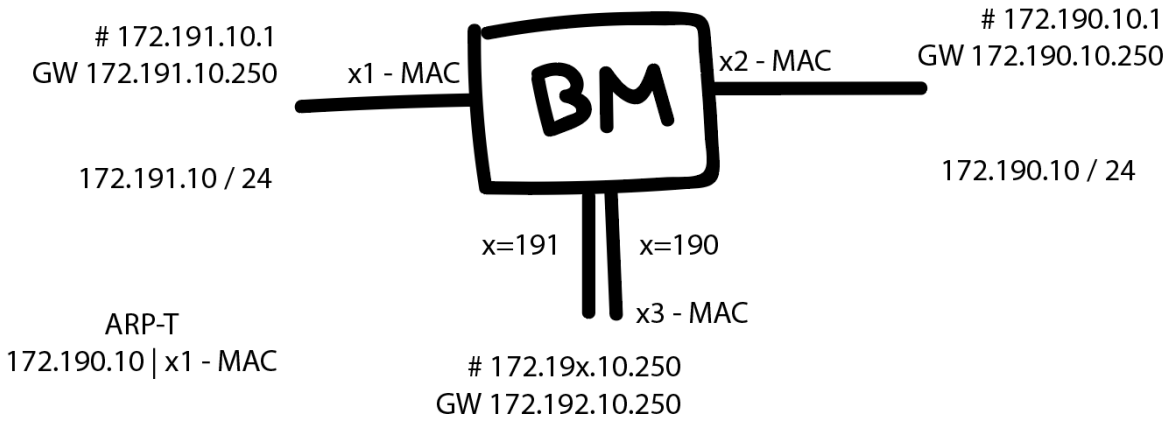
- Stern
- Über Router erreichbar (wie im echten Netz)
- Wenn nicht im selben Subnetz benötigt man Routinginstanz

Wie ist Topologie der Entwicklungsmaschinen?

Mehrere Interfaces -> mehrere Subnetzmasken -> mehrere IPs

Ethernet: Jeder Container bekommt hinter der logischen Adresse eine physische Adresse (willkürlich).

Bei Entwicklung auf virtuellen Instanzen überlegen welche Instanzen miteinander kommunizieren sollen. Diese müssen auf ein virtuelles Netz abgebildet werden, wie bei einem echten Netz.
-> gewährleisten das das Entwickelte auch im echten Netz funktioniert



Mitschrift am 20.05.2019

Netzwerk Topologie anpassen für die CIA Triade

Bedienen wir uns eines kleinen oder großen Rechenzentrums?

Bei externen RZ muss man die Anforderungen definieren

Bei einer internen wird ein IT- Personal gebraucht.

Interne RZ – Eigentum Hardware und Software

Datenschutz für Eigentum: sind verantwortlich für die Daten

Wer darf auf die Daten zugreifen?

Externe RZ benötigt einen Vertrag → Rechtsgrundstand

CIA Triade

Vertraulichkeit, Integrität und Ausfallsicherheit

Interne RZ

- Vorteil: Eigentum gehört mir, kann machen was ich will
- Nachteil: Man muss Ausfallsicherheit selbst garantieren
  – mittels Funkverbindung, über Redundanz (A & B Weg, unabhängig voneinander)

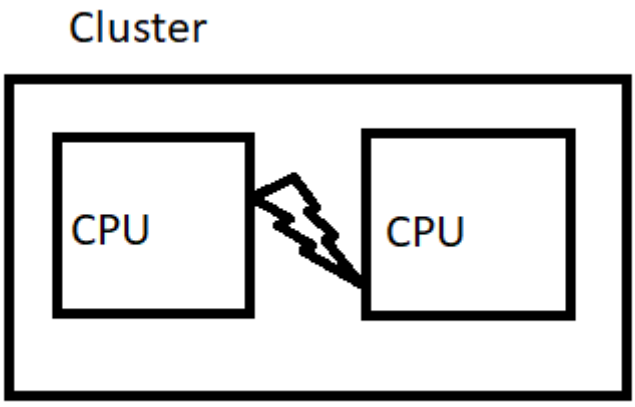
Externes RZ

- Vorteil: Ausfallsicherheit wird außerhalb garantiert

RAID System zum Daten sichern während dem Programmieren (Entwickler PC mit DB außerhalb)

Multiprozessor: Platine mit mehreren Prozessoren (virtuellen Multi Prozessoren)

Hardware von Software trennen



Stand-by-Cluster

2 Router stehen nebeneinander. Die 2. Maschine wartet nur dass die 1. Defekt ist und wird dann einspringen

Load- Balancer: Arbeit wird aufgeteilt auf die 2 Maschinen

Primär – Tertiär Struktur

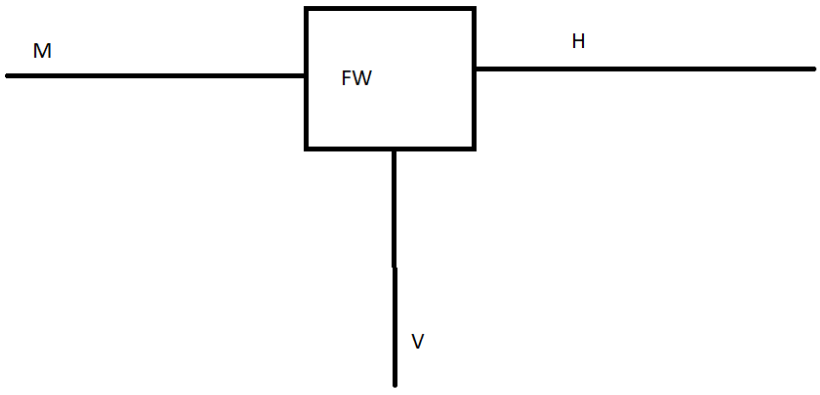
Transfermative Logik: Frontend und Backend (Server)

4er Logik: Client (Frontend) Backend teilt sich auf (DB – Server, Applikation logik und Darstellung)

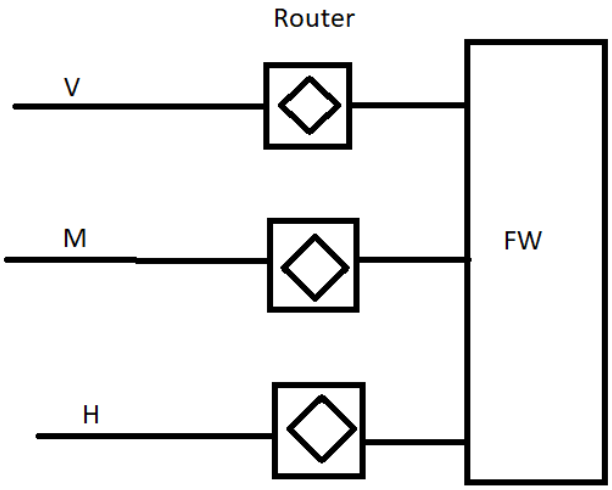
➔ Flexibilität wird ermöglicht: falls eine Maschine ausfällt

Dafür benötigt man mehr Netzwerk Komponenten

Mehr Router um die Abteilung (oder Verwaltung) im Krankenhaus voneinander abzutrennen
→ Separation



V = Verwaltungsnetz H= Hausnetz M = Medizin FW= Fireware



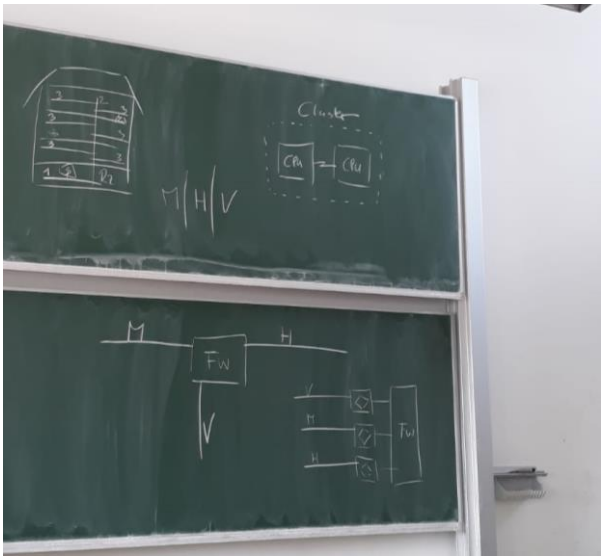
V-LAN: 2 Komponenten ausfallsicher verbunden

Überlegung: Wie baue ich meine Redundanz auf? – Ausfallsicherheit (auch physisch) garantieren

Möglichkeit: eigenes Personal für Netzwerkverwaltung

Katastrophenschutz → kann mit eigenem Personal besser behandelt werden

USV = unterbrechungsfreie Stromversorgung – Batterien die im Stromausfall eingesetzt werden



Nicht berechtigte Personen sollen nicht auf die sensiblen Daten zugreifen können

Wird umgesetzt mithilfe von Benutzerrollen – organisatorische und technische Rahmenbedingungen dokumentieren

2 Kriterien:

- Rollen und Berechitgungsystem
- Bestimmte Administratoren für bestimmte Bereiche (Netzwerksystem und Applikation)

Admin und Nutzer muss man unterweisen für System und Ordnung. Rahmenbedingungen zum Gesetze einhalten. Wie kann man nachweisen, dass alle Mitarbeiter nach den Richtlinien mit den Medizindaten umgehen?

→Datenschutzunterweisung

Nachweislich zu Kenntnis bringen – mithilfe eines Vertrags (Unterschrift)

Control:
werden alle Regeln befolgt? Mithilfe Schulungen oder Penetrationstests

Penetration Test:
hält das Programm einen gewissen „Druck" aus? SQL insection OWAS

Social Engineering:
Benutzername und Passwort per mail anfordern- alle Mitarbeiter dieser Methode aufklären.

LDAP
Active Directory fällt aus – Work Around: man muss sich vorher schon überlegen was gemacht werden soll falls es ausfällt →Jede Maschine im Haus hat einen berechtigten User

2 Techniker die den Benutzer konfiguriert haben am Rechner, schreiben 1 Hälfte des Passworts auf und geben es in ein Kuvert→ Passwort im Kuvert wird beim Abteilungsleiter aufbewahrt

Jeder PC hat einen Admin. Dadurch wird mehr Sicherheit gewährleistet. Der Hacker braucht nicht nur 1 Passwort für den admin sondern muss auch wissen was das Passwort spezifisch für den Rechner ist.

ISO2025 – Norm: Informationssicherheitsmanagement System

Kein Rechner, sondern Organisatorische technische und rechtliche Regelungen in der entsprechenden Gemeinschaft.

Datenschutzgrundverodnung:
Datenschutzmanagement System DMS

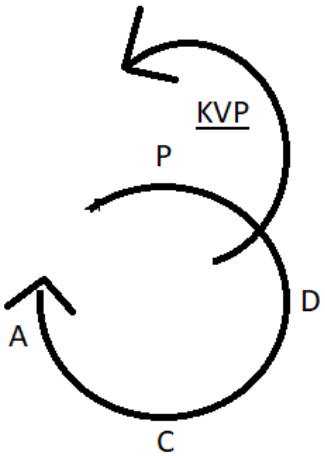
Regeln und Verordnung wie mit den Daten umgegangen werden soll

Daten werden verwendet, um auf Informationen zu zugreifen.

PDCA: Plan Do Check Act
Definiere einen Prozess (Plan) – Durchführen – Conrolliert – Act (Reaktion)

Welche Schritte muss der Administrator durchgehen

KVP: kontinuierlicher Verbesserungsprozess, (Hat sich die Technik oder Regel verändert?)



Gesetzliche Grundlage: man darf die Daten nur im gesetzlichen Rahmen zu verwenden

Grundrecht: alle personenspezifischen Daten werden geschützt

Anonymisierung: Ein- Weg Funktion, nicht möglich aus dem Datenbestand zurückzuführen Rückführbarkeit nicht möglich

Pseudonymisierung: Mehr- Weg Funktion, berechtigte Personen haben einen Schlüssel

Mitschrift am 27.05.2019

Verkabelung – Inhalt

Mikro-Switch: brauchen entsprechende Stromlieferung→Verkabelung

Ein Mikroschalter ist ein elektrischer Schalter, dessen Kontakte im geöffneten Zustand weniger als 3 mm Abstand voneinander haben. Das Gehäuse ist mit dem Symbol µ gekennzeichnet.

LWL: Lichtwellenleiter

Lichtwellenleiter (LWL) sind aus Lichtleitern bestehende und teilweise mit Steckverbindern konfektionierte Kabel und Leitungen zur Übertragung von Licht. Das Licht wird dabei in Fasern aus Quarzglas oder Kunststoff geführt. Sie werden häufig auch als Glasfaserkabel bezeichnet, wobei in diesen typischerweise mehrere Lichtwellenleiter gebündelt werden, die zudem zum Schutz und zur Stabilisierung der einzelnen Fasern noch mechanisch verstärkt sind.

Glasfasernetz: bestimmte Meter, Kilometer, leiten kann

Ein Glasfasernetz ist ein Übertragungsmedium zur Datenkommunikation in Form einer Verbindung mehrerer Glasfaserkabel-Systeme einem Netzwerk.

Kupferverkabelung ist nur für eine kurze Strecke.

SDPK7-Verkabelung: ?

UTP-STP:

UDP (Unshielded Twisted Pair) : Nicht geschirmt. Vorteil: keine magnetische Strahlung durch den Kupferkabel

STP: shielded twisted pair

Eine Gebäudeverteiler reicht für gesamtes Gebäude aus. Vorteil: wenige Angriffspunkte.

Wärme und Stromversorgung sollte redundant gehalten werden und sie sollten geschützt vor unbefugten Personen sein. Eine regelmäßige Kontrolle und Risikomanagement sollten gehalten werden. Die Stromversorgung sollte ein eigenes Kabel haben, gemeinsame Erdung und ein Schutz.

Potential Ausgleich im elektrischen Bereich spielt einen wichtigen Faktor.

Zugriff, Administrator, Verschlüsselung und Benutzerverwaltung… Wer darf was?

Die Kritikalität ist die, welche Prozesse geschützt werden sollen. Eine Risikoanalyse wird gemacht, um Probleme zu minimieren.

IT-Prozess: alle Tätigkeiten, die wichtig sind: Aufnahme, Entlassung usw.

Mediziner sollten Wissen darüber haben, was sie machen.

Verhinderung der Probleme: Redundanz, weniger Geräte/ Systeme/ Programme→ nur die nötigsten (Härten des Betriebssystems)

Ziel: was will man schützen? DEN PATIENTEN und dann die Verwaltung und all die Prozesse, die dafür sorgen, Patienten gesund zu halten.

Verfügbarkeit, Vertraulichkeit, Integrität der Information und Datenschutz sind wichtig.

Immer dokumentieren und berichten an verschiedenen Fachleuten.