SYSINT AUSARBEITUNG

Philipp Adler

***Abstract*—Die Technologie breitet sich in unserer modernen Welt aus. Digitale Devices sind Gegenstände, die uns im Alltag begleiten und unser Leben einfacher gestalten. Wir benutzen täglich unser Smartphone, schauen Videos über dem Laptop oder betreiben fortgeschrittenen Sport mit Sensoren. All diese Geräte waren vor Jahren kaum vorstellbar und auch noch ziemlich teuer. In den letzten Jahren ist der Preis für diese sogenannten Gadgets rapide gefallen. In Zukunft sollen uns elektronische Geräte nicht nur in unserer Freizeit, sondern auch zuhause, in einem "Smart Home, helfen. Wie der Name schon sagt, sind "Smart Homes" automatisierte Häuser, die Routineaufgaben des Menschen erledigen sollen. Doch neue Techniken müssen auch vor Angriffen geschützt werden. In dieser Ausarbeitung gehen wir einige Möglichkeiten durch, wie hardwaretechnische Systeme, das IoT das Smart Home, schützen, sowie dafür sorgen, dass kein unauthorisierter Zugriff zustande kommt. Außerdem sehen wir uns ein paar Szenarien an, die unser Umfeld gefährden könnten und welche Lösungsvarianten es dafür gibt.**

I. CLOUD COMPUTING AND INTERNET OF THINGS

Das Thema Cloud Computing hat in den letzten Jahren stark an Bedeutung gewonnen. Es erlaubt Endanwendern ihre Daten überall abzurufen. Die Daten werden in eine Wolke, für den User in ein nicht einsehbares Netzwerk, gespeichert. Es bietet Firmen die Möglichkeit, flexibler und billiger Daten zu speichern und Services an den Endkunden anzubieten. Bei einem Server ist es schwierig, in wenigen Sekunden Rechenleistung hinzuzufügen, bei einer Cloud ist das Standard.
In diesem Kapitel gehen wir auf die Vorteile des Cloud Computing ein, wie das Remote Monitoring, die automatische Skalierung und die Lastenaufteilung.

A. LB System-Ebene

Cloud Load Balancing ist der Prozess der Verteilung von Workloads und Ressourcen in einer Cloud-Umgebung. Load Balancing ermöglicht es Anforderungen zu verwalten, indem Ressourcen mehreren Servern zugewiesen werden. Dieses System erzielt eine hohe Leistung für wenig Geld. Man zahlt nur das was man verbraucht. Cloud Load Balancing nutzt den Vorteil der Cloud-Skalierbarkeit und Agilität um den Anforderungen gerecht zu werden. Es verbessert dadurch die Gesamtverfügbarkeit der Cloud. Um *noisy neighbors* zu vermeiden, verwendet der LB VLANs. Viele Anbieter wie Amazon Web Service (AWS), Google oder Microsoft bieten LB als Service in der Cloud an. [1]

B. Layer & Frameworks

Cloud Computing bietet zahlreiche Layer, wie Infrastructure, Platform oder Software Layer. Für das deployen gibt es auch einige Möglichkeiten, wie die Public, Community, Private und Hybrid Cloud.

1) SaaS: Software as a service ist eine Softwarelizenzierung, bei dem Software auf Abonnementbasis lizenziert und zentral vom Anbieter gehostet werden. Mögliche Anbieter wären Google Apps, Microsoft Office. Es hat den Vorteil, dass die Software zentral gemanaget wird und Anwender sich nicht um Updates kümmern müssen.[2]

2) PaaS: Platform as a Service bietet den Anwendern ein vordefinierte Umgebung, wo schnell und einfach eine Web-Applikation deployt werden kann. Die Umgebung beinhaltet ein OS, Datenbanken, Webserver und installierte Programmiersprachen. Anbieter in diesem Model sind Windows Azure und Google App Engine. Diese Plattform bietet Tools für das Designen von Webformularen und erlaubt die einfache Integration von anderen Plattformen.[2]

3) IaaS: Infrastructure as a Service erlaubt dem Anwender seine eigene Infrastruktur individuell zu erstellen. Der Vorteil, die Infrastruktur in die Cloud zu verlagern, könnte die dynamische Skalierung und die variablen Kosten sein. Das heißt ich zahle nur was ich verbrauche. Mögliche Anbieter sind Amazon Web Services und Google Compute Engine.[2]

4) Public Cloud: In einer public Cloud werden Ressourcen, wie Applikationen und Speicher, öffentlich über das Internet zur Verfügung gestellt. Public Cloud Services können entweder kostenlos oder Bezahlung

nach Verbrauch angeboten werden. [2]

5) Community Cloud: Die Cloud Infrastruktur wird mit mehreren Organisationen geteilt und unterstützt eine spezifische Community, die gemeinsame Anliegen haben. Universitäten und Banken finden meistens gefallen an diesem Modell.[2]

6) Private Cloud: Wenn man Sofware und Services nicht teilen möchte, verwendet man eine private Cloud. Dabei ist man für die Sicherheit der Daten selbst verantwortlich.[2]

7) Hybrid Cloud: Die hybride Cloud ist eine Zusammensetzung von der public und private Cloud. Mithilfe der Hybrid Cloud können unternehmensinterne Lösungen den Kunden mittels einer Middleware zur Verfügung gestellt werden.[2]

C. Monitoring

Cloud Monitoring ist der Prozess von der Überprüfung, Überwachung und Verwaltung von Prozessen und Abläufen in einem Cloud-System. Sozusagen überwacht es alle Vorgänge, um die Performance optimieren. Es sorgt für die Gesundheit des Systems, zu Gunsten des Providers und des Anbieters. Es erlaubt den Anwender Zugriff und Kontrolle auf die Geräte. So hat man immer alles im Überblick, kann in Notfällen reagieren und sieht, welche Daten die Geräte liefern.
Unter *Resource Monitoring* versteht man, das Erkennen des laufenden Gerätes und das Sammeln von Informationen. Bei der Feststellung eines unnormalen Systemverhaltens, probiert das System zuerst das Problem selbst zu lösen und falls das Vorhaben nicht funktioniert, wird der Anwender alermiert z.B. mittels einer SMS. Dabei muss es sich nicht unbedingt immer um Hardware handeln, sondern es kann auch um Software gehen.
Es gibt zwei Arten von Monitoring: High-Level und Low-Level. Die High-Level-Überwachung bezieht sich den Status der Virtuellen Plattform, während Low-Level Informationen auf der physikalischen Ebene sammelt. Da man beim IoT nicht nur ein Gerät überwachen muss, ist das Monitoring Multithreading basierend.[3]
Netzwerkmonitoring kann entweder durch eine zentrale- oder einer dezentralen-Architektur realisiert werden.
Zentralisiert senden die PaaS und IaaS Ressourcen, die Informationen an den zentral liegenden Server.

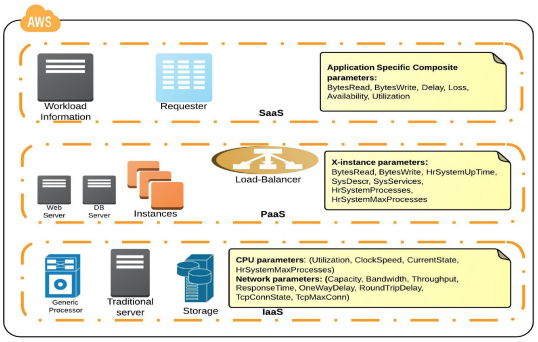

Fig. 1. Monitoring von verschiedenen Applikationen und Layers [3]

Bei dieser Technik werden die Informationen in einer periodischen Zeitspanne von den Geräten gepullt, was ein besseres Management für die Cloud-Applikation erlaubt. Aber es gibt auch einige negative Dinge, wie single point of failure, mangel an Skalierbarkeit und fehlende Rechenleistung, je größer die Anzahl der zu überwachenden Geräte wird.
Die **Dezentralisierte**-Architektur kann die Fehler der Zentralisierten-Architektur überwinden. In einem dezentralen System sind alle Komponenten gleich wichtig. Wenn eines der Komponenten ausfällt, hat das keine Auswirkungen auf das andere. Bei einem strukturierten Peer-to-Peer Netzwerk wird der Ausfall des zentralen Punkts entschärft. Bei einem unstrukturierten Peer-to-Peer Netzwerk ist das Suchverzeichnis, nicht wie beim strukturierten Peer-to-Peer Netzwerk, zentral.
Eine kommerzielle Monitoringlösung wäre Nagios, das in der Lage ist, Ressourcen verschieder Cloud Infrastrukturen zu überwachen. Zur Überwachung verwendet Nagios SNMP. Es baut auf einer zentralen-Architektur auf, deren Nachteile durch die Vielfältigkeit an Konfigurationsmöglichkeiten reduziert werden kann.[3]

D. Skalierung

Unter Skalierung versteht man die Leistungsteigerung, durch das Hinzufügen von Ressourcen, in ein bestehendes System. In der Cloud können Anwendungen nach Bedarf, sei es Datenspeicher oder der Ausbau des Netzwerks, angepasst werden. Es gibt drei Arten von Cloudskalierung, Horizontale, Vertikale und die Automatische.[4]

1) Horizontale Skalierung: Durch hinzufügen von mehreren Servern, die als eine Einheit fungieren, wird die Geschwindigkeit und die Verfügbarkeit erhöht.

Sozusagen erledigen alle Server, gleichen Aufbaus, den selben Job.[4]

2) Vertikale Skalierung: Die Kapazität von bereits eingesetzter Hardware wird durch hinzufügen von Ressourcen erhöht. Die vertikale Skalierung erreicht bessere Leistung, mit mehr Hardware.[4]

3) Automatische Skalierung: Je nach Gegebenheiten skaliert sich das System von selbst. Bei vielen Anfragen wird die Kapazität skaliert, um die Leistung zu erhöhen. Um Kosten zu sparen, wird bei weniger Anfragen die Ressourcen gesenkt. Falls eine Instanz ausfällt oder nicht mehr erreichbar ist, wird sie durch eine Neue ersetzt.[4]

II. AUTOMATISIERUNG, REGELUNG UND STEUERUNG

III. SECURITY, SAFETY, AVAILABILITY

In einem Smart Home spielen Faktoren wie Sicherheit und Hochverfügbarkeit eine wichtige Rolle. Wie kann ich sicherstellen, dass mein Zuhause von Hackern nicht angegriffen wird und ein Zugriff von außen nicht möglich ist. Nicht nur Zertifikate und Firewalls, sondern auch Load Balancing sorgen, dass meine Geräte jederzeit zur Verfügung stehen und geschützt sind.

A. Network-based Application Firewall

Die Web Application Firewall (WAF), überwacht, filtert und blockt eingehende und ausgehende HTTP Nachrichten von der Web-Applikation. Es schützt sozusagen die Applikation, indem es die HTML, HTTPS, SOAP und XML-RPC Packete überprüft. Das Cloud-Service verhindert z.B. Angriffe wie XSS, SQL Injection, Session Hijacking und Buffer Overlows. Außerdem ist es auch in der Lage neue Attacken zu identifizieren, indem es den Netzwerkverkehr nach unbekannten Mustern absucht. WAF kann entweder network-based oder Host-based sein und wird typischerweise über einen Proxy bereitgestellt. Es befindet sich im Netzwerk immer vor der Webapplikation. Es analysiert Anfragen nach vordefinierten Regeln und filtert potenzielle Gefahren aus.[5]

B. VPN

Ein Virtual Private Network ist eine Gruppe von Computern, die über ein öffentliches Netzwerk vernetzt sind. Man verwendet VPNs um auf Ressourcen zuzugreifen, die nicht im gleichen physikalischen Netzwerk liegen oder als Verfahren zur sicheren Kommunikation verwenden. Um sich in ein VPN zu verbinden, braucht es einen VPN-Client am Rechner, bei diesem man die Zugangsdaten eingibt, sowie einen Schlüsselaustausch mit dem Server vollführt. Dann kann die sichere, verschlüsselte Kommunikation über das Internet stattfinden. Wichtig ist, dass die Anbieter SSL/TLS, PPTP, IPSec und L2TP unterstützen. Es gibt folgende Anbieter: proXPN, TorVPN, TorGuard und WiTopia.
Für die Erstellung eines VPN-Tunnels gibt es mehrer Benutzerauthentifizierungsmethoden. Bei PPTP muss vorher mittels PPP eine erfolgreiche Benuterauthentifizierung stattgefunden haben, bevor PPTP die Daten verschlüsselt. Hingegen wird bei SSTP eine sichere Verbindung mit einem Zertifikat am Gateway, wo sich der Client authentifizieren, hergestellt. Zusätzlich bei L2TP/IPSec besitzt auch der Client ein Zertifikat, damit sich auch die VPN-Clients gegenüber dem Server authentifizieren müssen. [6]

C. Load Balancing

Für die Hochverfügbarkeit im Internet braucht es zum Einen Cluster mit Failover(Active/Passive Mode) und einen Load Balancer. Es wird empfohlen den Load Balancer außerhalb des Clusters zu stationieren, um die horizontale Skalierbarkeit zu erhöhen.[7]

1) Active-Active: Bei der Active-Active Variante verteilen beide Load Balancer die Anfragen und agieren als Backup für den anderen Load Balancer. Damit man die Active-Active Variante verwenden kann, gibt es mehrere Möglichkeiten. Eine davon ist die Verwendung von mehreren VIPs. Falls einer der Load Balancer ausfällt, übernimmt die noch funktionierende Einheit auch die VIP des Ausgefallenen. Jetzt muss nur ein Weg gefunden, wie die Anfragen auf die beiden LB verteilt werden. Dafür kann man DNS verwenden, dass die Web Domain zu einer IP-Adresse entschlüsselt und ein Round-Robin zwischen den beiden VIPs durchgeführt, damit beide LB Anfragen erhalten.[7]

2) Active-Standby: Die aktive Einheit verteilt den Netzwerkverkehr auf die vorhandenen Server, der Passive reagiert auf keine Anfragen. Die zwei Load Balancer sind über einen private Link miteinander verbunden und kontrollieren mittels eines speziellen Protokolls den Zustand des jeweils anderen Load Balancers. Wenn der aktive Load Balancer ausfällt, springt die passive Einheit sofort ein.[7]

3) Healthchecks: Health Checks sind notwendig, damit der LB Anfragen nicht an fehlerhafte Server versendet. Das kann bedeuten, dass der Server zwar verfügbar ist, jedoch aber die Applikation fehlerhaft oder der Content korrupt ist. Durch Healthchecks erkennt der LB solche Fehler. Es gibt zwei Arten von Tests, nämlich die in-band- und out-of-band checks.
Bei in-band-checks kontrolliert der LB einfach den normalen Netzwerkverkehr, ob der Server intakt ist. Out-of-band Health Checks jedoch werden explizit vom LB durchgeführt.
Mit ARP(L2) schaut man, ob der Server darauf reagiert und noch funktioniert. Mittels Ping(L3) findet man heraus, ob der Server und die Applikation mit TCP/UDP(L4) läuft. Auch Health Checks auf Layer 7 mittels GET Anfrage an die URL, kann je nach Statuscode, Fehler entdecken.

IV. Authentication, Authorization, Accounting

In einer komplexen, viel vernetzen Umgebung dürfen nur bestimme Geräte auf Ressourcen zugreifen. Authentifizierungssysteme sorgen, dass diese Richtlinien eingehalten werden. Durch die Identität kann festgestellt werden, ob man sich beim Dienst anmelden kann und die Rechte auf die Ressourcen zuzugreifen, hat.

A. SSO

Single Sign-On ist ein Authentifizierungsprozess. Der Anwender muss nur einmal seine Benutzerdaten angeben und erhält daraufhin Zugriff auf alle Applikationen, die für ihn freigegeben wurden. Der Teilnehmer erhält seine Zugriffsrechte über Transaktionen im Hintergrund.
Bei dem Ablauf werden drei Parteien, Service Provider, Identity Provider und das Client-Programm konfrontiert.[8]

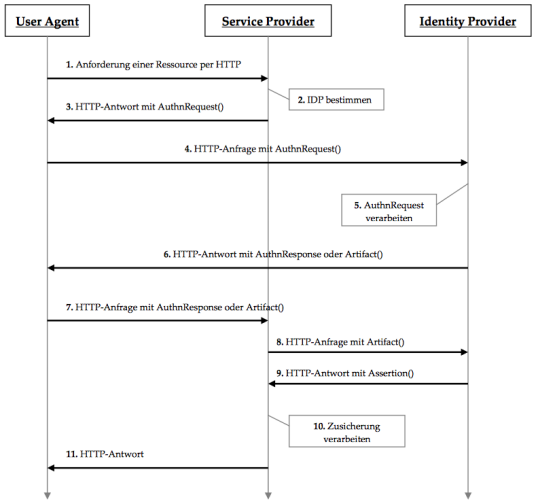

Fig. 2. Ablaufschema beim Single Sign-On [8]

B. OpenID

OpenID ist ein dezentrales Authentifizierungssystem, wo durch die Angabe einer einzigen Identität, einer URL, man sich bei mehreren Diensten anmelden kann. Es ist ein Vertreter im Bereich SSO. Die URL entspricht immer den selben Schema: *https:name.anbieter*. Durch diese Angabe kann man sich dann bei allen Webseiten anmelden die OpenID. Wie beim SSO gibt es hier auch drei Komponenten, den Benutzer, dem Konsumenten und dem Anbieter.
End-User der Anwender der eine Seite aufruft bzw. auf eine Ressource zugreifen möchte.
Relying-Party ist ein Webdienst der Ressourcen beinhaltet, die nur von bestimmten Leuten einsehbar sind.
OpenID-Provider stellt den Dienst der Anmeldung mittels einer URL zur Verfügung, der einem erlaubt mehrere Seiten zu benutzen.
Der Anwender wird vom Benutzer-Login zum Anbieter weitergeleitet, um sich dort zu authentifizieren. Nach Eingabe der OpenID-URL, extrahiert der Konsument die URL und baut eine Verbindung in Form eines Geheimschlüsselt mit dem Provider auf. Dieser Schlüssel dient dazu, dass bei späterer Kommunikation kein direkter Informationsaustausch stattfinden muss. Als nächstes muss der Client seine Anmeldedaten angeben. Nach Verifizierung der Authentifikation, hat der Client Zugriff auf seine Ressourcen.
Hat Client beim Anbieter und beim Provider schon einen Account, werden diese beiden Konten miteinander verknüpft und der Client muss sich nur mehr mit seinem OpenID-Account anmelden. Wenn noch kein Account beim Konsumenten besteht, kann der Client die Accountdaten vom Provider übertragen und erhält dasselbe Ergebnis wie vorher.
Um Phising zu vermeiden, wurde OpenID auf Version 2.0 erweitert, wo nicht mehr die Daten über einer gefälschten WWW-Adresse angegeben werden, sondern nur mehr der Providername genannt wird. So kann sich der User direkt beim Anbieter anmelden und wird nicht von der Website zu diesem weitergeleitet.[9]

C. OAuth

Im Gegensatz zu OpenID, gewährt OAuth eingeschränkten Zugriff auf eigene Ressourcen,

ohne die eigene Identität zu verraten. OAuth dient der Autorisierung und leitet auch an einen dezentralen OpenID-Anbieter weiter. OAuth erlaubt es, die Anmeldeinformationen eines Endanwenders zu verwenden, ohne das Passwort des Benutzers anzugeben, indem es die Eingaben durch einen Authorisationsprozess ersetzt. Es macht Sinn, wenn man einer Anwendung Zugriff auf bestimmte Daten geben möchte. Dieser Prozess basiert auf Tokens. Wenn man einer Anwendung erlaubt auf die Ressourcen zuzugreifen, bekommt diese eine Access Token. Dieser erlaubt der Anwendung ohne Zugangsdaten zuzugreifen.[10]

D. Radius

RADIUS steht fur Remote Authentication Dial-In User Service und ist ein Client-Server- Protokoll, welches zur Authentifizierung, Autorisierung und zum Accounting (AAA-System) von Benutzern bei Einwahlverbindungen in ein Computernetzwerk dient. RADIUS ist Defacto-Standard bei der zentralen Authentifizierung von Einwahlverbindungen über Modem, ISDN, VPN, WLAN und DSL.
Anmeldungen vom Supplicant (Client) werden vom Authenticator zuerst an den Authentication Server weitergeleitet. Der entscheidet, ob der Supplicant Zugang bekommt. In Abhängigkeit einer erfolgreichen Authentifizierung, wird der Zugang zum Netzwerk über einen bestimmten Port freigeschaltet. Für IEEE 802.1x kann ein Port eine Buchse an einem Switch oder eine logische Assoziation sein. Denkbar ist hier die Zugangsmöglichkeit zum Netzwerk für einen WLAN-Client an einem WLAN-Access-Point. Mit IEEE 802.1x/EAP wird dem WLAN-Client zu Beginn einer Sitzung, die dafur gültigen WPA2-Schlussel mitgeteilt.
Beim Zugriff auf ein lokales Netzwerk eines Unternehmens über WLAN, reicht die einfache Authentifizierung über ein gemeinsames Passwort (WPA2-PSK) nicht aus. Wenn das Passwort die Runde macht, dann ist das WLAN praktisch offen. Mit RADIUS werden serverseitig Passwörter zugeteilt, was dem Administrator Arbeit erspart und fur die Nutzer vergleichsweise einfach ist.[11]

1) Ablauf: Der Client meldet sich beim WLAN-Access-Point an. Gibt für die Authentifizierung Benutzername und Passwort an, die vom Access-Point(Supplicant) an den Radius-Server(Authentication Server) weitergeleitet. Passt alles, gibt Radius ein Master Secret zurück. Der Acces-Point generiert den Sitzungsschlüssel, teilt diesen dem Client mit. Nun hat der Client Zugriff auf das Netzwerk. Um den dauernden Zugriff zu ermöglichen, bekommt der Anwender in regelmäßigen Abständen einen neuen Sitzungsschlüssel.[11]

E. Zertifikate bei VPN

Bei einer VPN-Verbindung haben Client und Server ein öffentliches/privates Zertifikat. Der Server lässt nur Verbindungen durch, die von bekannten Zertifizierungsstellen signiert wurden. Bei einer Clientanfrage schickt der Server sein Zertifikat zurück. Daraufhin schickt der Client sein Zertifikat an den VPN-Server. Wie es bei SSL üblich, erstellt der Client ein sogenanntes *pre-master secret*, welches er mit dem öffentlichen Schlüssel des Servers verschlüsselt. Der Server entschlüsselt die Nachricht, erstellt aus diesem Secret, dass *master-secret*, also den Sitzungsschlüssel für die Kommunikation.

V. DESASTER RECOVERY

Disaster Recovery (dt. auch Katastrophenwiederherstellung), im Folgenden auch DR genannt, beschreibt die Vorbereitung und Reaktion auf sogenannte Katastrophen, die abgespeicherte Daten und Lauffähigkeit eines IT-Systems betreffen. In diesem Bereich der Sicherheitsplanung ist mit negativen Ereignissen all das gemeint, was den Betrieb eines Unternehmens gefährdet.

A. Disaster Recovery Plan

Ein DRP dokumentiert konkrete Richtlinien, Verfahren und Maßnahmen, um die Störung eines Unternehmens im Falle eines Desasters zu begrenzen, und möglichst innerhalb eines bestimmten Zeitrahmens wieder zurück in den Normalzustand zu gehen.

1) Szenarien: Mögliche Katastrophen könnten sein:

- Hardwareausfälle
- Überlastung
- Stromausfall, Brand oder Wasserschaden
- Sicherheitsprobleme

2) Vorbeugemaßnahmen: Hardwareausfälle können immer wieder vorkommen. Um sich dagegen vorzubeugen empfehle ich eine Active-Active Strategie. Das bedeutet wenn ein System ausfällt, kann das wartende Ersatzsystem den Part übernehmen. Überlastungen können dafür sorgen, dass unsere Applikation bzw. das System nicht mehr verfügbar ist. Dank Load Balancing kann Last auf die Server

gleichmäßig aufgeteilt werden. Auch die Cloud kann je nach Mehrbedarf die Ressourcen skalieren und erweitern.
Um sich am Besten gegen Stromausfälle, Brand oder einen Wasserschaden zu schützen, schlage ich mal vor alle Daten auszulagen, sei es in die Cloud oder ein Rechenzentrum. Dort sind die Daten vor Naturkatastropen geschützt. Durch regelmäßige Backups, Replikationen und Hot Swap sind die Daten sicher und immer Verfügbar, sodass unser System keine Downzeit hat.
Sicherheitsprobleme können nur dann stattfinden, wenn unsere Umgebung zu wenig geschützt ist. Es ist immer wichtig die Daten verschlüsselt zu übertragen und mit Zertifikaten zu sichern. Um unauthorisierten den Zugang zu verwähren sind Authentisierungssysteme unumgänglich. Eine Firewall in unserem Netzwerk, kann gefährliche Packete filtern und so eine Angriff verhindern.

3) Reaktion: Sollten die Vorbeugemaßnahmen nicht ihren Zweck erfüllen, was sehr unwahrscheinlicht ist, müssen wir uns ernsthaft Gedanken machen.

VI. Algorithmen und Protokolle

Unter dem Kapitel Algorithmen und Protokoll werfen wir einen Blick, wie Protokolle für eine sichere VPN-Kommunikation und für das Monitoring funktionieren. Wir betrachten die Prtokolle SNMP für das Monitoring und PPTP/SSTP/L2TP für das sichere Tunneling.

A. Monitoring SNMP

Das Simple Network Management Protocol, abgekürzt SNMP, ist für die Verwaltung, Steuerung und Monitoring von Netzwerkkomponenten zuständig. Es gehört zum TCP/IP Protokoll und erlaubt remote Einstellungen zu tätigen. Um die Geräte zu überwachen, brauchen diese eine TCP/IP-Anbindung und einem SNMP-Server. SNMPv1 eignet sich für private LANs, die sich hinter einer Firewall verstecken, da diese Version keine Verschlüsselung beinhaltet. Bei der zweiten Version, konnte das Thema Sicherheit noch immer nicht gelöst werden, aber das Protokoll wurde um ein paar Features erweitert. Die dritte und derzeit letzte Version hat die Sicherheit von SNMP gesteigert, aber aufgrund der Komplexität, findet es kaum Verwendung.[12]

1) Funktionsweise: **SNMP Manager** ist eine eigenständige Einheit, kann ein Host sein, der mit dem SNMP-Agent kommuniziert, welches in einem Gerät implementiert ist. Informationen von den Agents werden von ihm zusammengeführt und analysiert.
SNMP Agent ist ein Programm, welches in den Geräten steckt. Es verwaltet Ressourcen und macht sie für den Manager erreichbar bzw. aufrufbar. Es speichert und ruft Management-Informationen als MIB. Nimmt Anfragen vom Manager entgegen und sendet die entsprechende Antwort.
Managed Devices ist das Gerät, von dem die Informationen geliefert werden.
MIB, Management Information database oder Management Information Base, befindet sich zwischen Agent und Manager. Hierbei handelt es sich um eine Datenbank, die Geräteparameter verwaltet. Der Manager verwendet diese Datenbank um Anfragen an den Agent zu schicken, um bestimmte Informationen zu fordern, die das NMS benötigt. Das MIB beinhaltet standardgemäß nur Statistiken und Regelwerte über das zu verwaltende Objekt. Sozusagen sind MIB-Dateien, eine Menge von Fragen, die der SNMP Manager an den Agent stellen kann.
Zusätzlich zur normalen Kommunikation, wie GET, können ”Traps” verwendet werden. Es handelt sich hierbei um ein Datenpaket, welches nicht vom SNMP Manager geforderd wird, sondern der Agent schickt ijm ein Signal, aufgrund eines auftretenden Ereignisses. Bei ”Inform” ähnlich wie bei ”Trap” sendet der Agent ein Signal, aber diesmal schickt der Manager auch eine Nachricht zurück. [12]

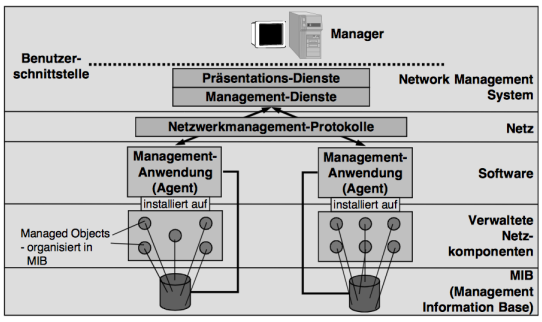

Fig. 3. Arbeitsmodell [12]

B. PPTP/SSTP/L2TP

Das folgende Kapitel zeigt einen Überblick und die Unterschiede der bekanntesten VPN-Protokolle. Welche Vorteile und Nachteile bieten mir PPTP, SSTP und L2TP.

1) PPTP: Das Point-to-Point Tunneling Protokoll baut auf eine Remote-Access-Verbindung auf. Da der Anmeldevorgang mit MS-CHAPv2 umgesetzt wird, gilt die PPTP Verschlüsselung als unsicher. Mit dieser Authentifizierung handeln die Komponenten einen Schlüssel aus, mit dem die Pakete verschlüsselt werden. Die Architektur teilt sich in zwei logische Systeme auf, dem PPTP Access Concentrator und den PPTP Network Server. Das PAC ist im Client integriert und verwaltet die Verbindungen zum PNS, welcher für das Routing zuständig ist.
Der Client baut über den Port 1723, wo die Kontrolldaten übermittel werden, eine Verbindung mit dem Server auf. Unter dem GRE(Generic Routing Encapsulation) werden die Pakete getunnelt.
Wenn sich der Client in einem NAT-Netzwerk befindet, ist dank dem GRE, nicht möglich die Nachrichten jemanden zuzuordnen. Das ist deshalb so, weil das GRE keine Portnummern speichert.[13]

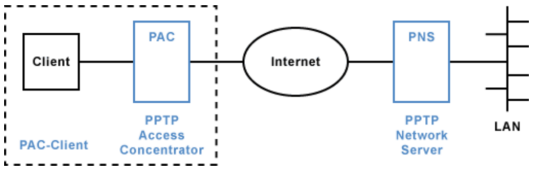

Fig. 4. PPTP Architektur [13]

2) L2TP: Layer-2-Tunneling-Protokoll, ist die Weiterentwicklung von PPTP und L2F und baut eine Verbindung zwischen zwei Netzwerken auf. Es bietet den Vorteil, dass im Gegensatz zu PPTP jedes beliebige Netzwerkprotokoll versenden kann. L2TP selbst bietet keine Verschlüsselung. Es arbeitet aber mit Preshared-Keys und Benutzerkonten, auf die sich verschiedene Verschlüsselungsverfahren anwenden lassen. Um die Kommunikation zu schützen ist der Einsatz von IPSec erforderlich.
Wie beim PPTP gibt es einen LAC und LNS. Es existieren zwei Kanäle, in Einem werden die Kontrollnachrichten sicher und im Anderen die eigentliche Nachricht ungesichert übertragen.
Um nun eine sichere Übertragung zu gewährleisten, muss zuerst eine IPsec-Verbindung aufgebaut werden und erst danach kann die sichere L2TP-Kommunikation stattfinden.[14]

3) SSTP: Secure Socket Tunneling Protokoll verwendet SSL für die sichere Kommunikation. Es hat den Vorteil, dass nicht durch eine Firewall oder einen Router blockiert wird.
Beim Ablauf baut der Client eine TCP-Verbindung mit dem Server auf. Der Client sendet dann die SSTP-

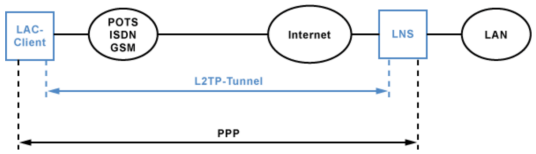

Fig. 5. L2TP Architektur [14]

Kontrollpakete über die HTTPS-Sitzung. Wenn der SSTP-Status auf beiden Seiten bereit ist, erfolgt eine link-up Signalisierung an die PPP Sicherungsschicht auf beiden Seiten. Über SSL erfolgt dann der PPP-Verbindungsaufbau. Wenn alles erfolgreich war, werden auf beiden Seiten IP-Interfaces mit privaten IP-Adressen erstellt, also ein neues zusätzliches Interface, mit den die Geräte kommunizieren.

VII. KONSISTENZ UND DATENHALTUNG

Im Internet of Things werden so viele Daten gesammelt, dass es schwierig ist, diese konsistent zu halten. Durch Replikation und dem CAP-Theorem versucht man diese Daten zu sichern und eventuelle konsistent zu halten. Die Replikation sollte bei Ausfällen, den aktiven Server so gut wie möglich ersetzen und als Master agieren, um die Performance und Verfügbarkeit so hoch wie möglich zu halten.

A. LDAP Replikation

Unter der Technik Replikation versteht man, dass duplizieren von Daten zwischen verschiedenen Verzeichnissen. Das hat den Vorteil, das die Performance, Skalierung und Redundanz verbessert wird. Bei der Replikation gibt es mehrere Master(Supplier) auf denen geschrieben wird und mehrere Replica(Consumers), die vom Master lesen. Der **Master** beinhaltet directory mit Informationen. Jede Veränderung oder Aktuallisierung auf der Master-Ebene werden von den Replica übernommen. Die Replica agieren als Backup und kopieren die Daten von den Masters. Sollte es zu einem Ausfall kommen, springt der Supplier ein und übernimmt die Rolle als Master. Für eine bessere Performance können die Client-Anfragen an die Consumers weitergeleitet werden. Auch bei mehrere Mastern kann der Workload auf verschiedene Geräte aufgeteilt werden.[15]

B. Master-replica topology

Das ist die einfachste Topology, welche nur einen Master beinhaltet. Die Änderungen vom Master werden von den Replica-Server übernommen. Im Falle, dass es zwei Masters und nur einen Replica gibt, sollte jeder Subtree ein Update, von nur einem Master, erhalten.[15]

C. Master-forwarder-replica topology(Cascading Replication)

Hier sendet der Server die Änderungen nicht direkt zum Replica, sondern diese Rolle übernimmt ein anderer Server, der Forwarder. Der Forwarder befindet sich zwischen den beiden Komponenten. Jede Änderung vom Master geht an den Replica, welcher das Update weiterleitet. Der Forwarder kopiert die empfangenen Daten und verteilt die Informationen an die Replicas. Diese Topologie bietet den Vorteil, dass sich nicht der Master darum kümmern muss, die Änderungen an alle Replica zu senden. So kann sich der Master um wichtigere Dinge kümmmern. Im Falle das alle Daten vom Master verloren gehen, kann der Forwarder, der früher ein Replica war, als Master agieren.[15]

D. Peer replication

Peer-to-Peer vermeidet den Verlust von Updates und den Ausfall eines Masters. Die Server akzeptiern, dabei nicht nur Änderungen von einem Peer-Server, sondern von mehreren.

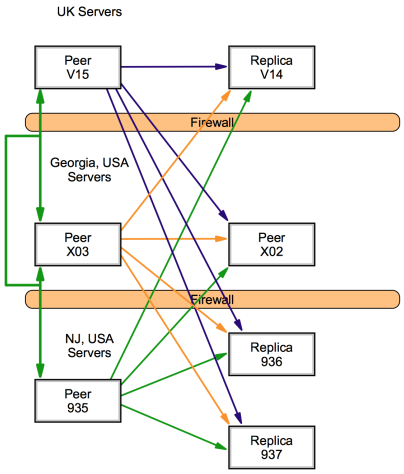

Fig. 6. Multiple peer LDAP flow [15]

E. Delegation

Meistens ist es sinnvoll als Administrator nicht jede Aufgabe selbst zu machen, sondern delegiert diese Recht auf andere Personen. Wenn man im Bereich LDAP über Delegation redet, meint man Objektverwaltung zuweisen. Unter diesem Unterpunkt kann der Administrator eine Gruppe oder eine einzelne Person, die mit Mehraufwand verbunden ist, auswählen. Gruppen lassen sich flexibler verwalten. Diesen ausgewählten Personen können nun bestimmte Rechte zugeteilt werden, wie z.B. das speeren von Konten.

LIST OF FIGURES

1 Monitoring von verschiedenen Applikationen und Layers [3] II
2 Ablaufschema beim Single Sign-On [8] . IV
3 Arbeitsmodell [12] VI
4 PPTP Architektur [13] VII
5 L2TP Architektur [14] VII
6 Multiple peer LDAP flow [15] VIII

REFERENCES

[1] N. Rando, "cloud load balancing." http://searchcloudcomputing.techtarget.com/definition/cloud-load-balancing, 2015.
[2] priyathevaishnavite, "Cloud computing." https://priyathevaishnavite.wordpress.com/2014/05/28/cloud-computing/, 2014.
[3] K. Alhamazani, "An overview of the commercial cloud monitoring tools: Research dimensions, design issues, and state-of-the-art." http://arxiv.org/pdf/1312.6170.pdf, 2013.
[4] M.Kriushanth, "Auto scaling in cloud computing." http://www.ijarcce.com/upload/2013/july/67-o-kriushanth2013.
[5] M. Bacon, "Web application firewall (waf)." http://searchsecurity.techtarget.com/definition/Web-application-firewall-WAF, 2015.
[6] A. Henry, "Why you should start using a vpn (and how to choose the best one for your needs)." http://lifehacker.com/5940565/why-you-should-start-using-a-vpn-and-how-to-choose-the-best-one-for-your-needs, 2012.
[7] D. Quaid, "Understanding active-passive, active/active load balancing." http://loadbalancerblog.com/blog/2013/01/understanding-active-passive-activeactive-load-balancing, 2013.
[8] M. Schönberg, "Single sign-on-technologien für das world wide web." https://vsis-www.informatik.uni-hamburg.de/getDoc.php/thesis/179/Single_Sign-On-Technologien_für_das_World_Wide_Web.pdf, 2007.
[9] M. Russer, "Web-authentifizierung mit openid." https://www4.cs.fau.de/Lehre/SS10/PS_KVBK/papers/10.v2.martin.russer.ausarbeitung.pdf, 2010.
[10] Zend, "Einführung zu oauth." http://framework.zend.com/manual/1.12/de/zend.oauth.introduction.html, 2016.
[11] Elektronik-Kompendium, "Ieee 802.1x / radius." http://www.elektronik-kompendium.de/sites/net/1409281.htm, 2016.
[12] M. Vogel, "Snmp (simple network management protocol) aufbau, funktion, sicherheit." http://www.ruhr-uni-bochum.de/dv/lehre/seminar/snmp/snmp-slides.pdf, 2000.
[13] Elektronik-Kompendium, "Pptp - point-to-point tunneling protocol." http://www.elektronik-kompendium.de/sites/net/0906141.htm, 2016.
[14] Elektronik-Kompendium, "L2tp - layer-2-tunneling-protocol." http://www.elektronik-kompendium.de/sites/net/0906131.htm, 2016.
[15] S. Tuttle, "Understanding ldap design and implementation." http://www.redbooks.ibm.com/redbooks/pdfs/sg244986.pdf, 2004.