ComConsult Research

Der Netzwerk Insider

Mai 2017

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

„UCaaS Lite“: Können die Cloud-Anbieter mit ihren On-Premises Kollegen konkurrieren?

von Timo Schmitz, B.Sc. und Dipl.-Ing. Dominik Zöller

Cloud-Dienstleistungen der unterschiedlichsten Art sind mittlerweile sowohl im Alltag als auch im beruflichen Umfeld als Alternative zu On-Premises Lösungen angekommen. Die Nutzung von Everything as a Service (XaaS) ist heute kein Wunschdenken mehr, sondern in vielen Fällen bereits gelebte Realität. Warum sollte ein Unternehmen also im Bereich der Kommunikation und Kollaboration, zwei der essentiellen Grundsteine im Businessalltag, auf den Luxus, den ein Full-Managed-Cloud-Service mit sich bringt, verzichten? Dieser Frage folgend, etablierten sich bereits einige der großen Anbieter mit „Unified Communications as a Service“ (UCaaS) Leistungen am Markt (z.B. Microsoft, Cisco, Avaya).

Mit *Amazon Chime* möchte nun auch Amazon einen Teil vom UCaaS-Kuchen abhaben und startete vor kurzem seine eigene Cloud-Kommunikationsplattform. Mit Features wie „crystal clear audio and high definition video [conferencing]“ , gestützt durch die geballte AWS Rechenleistung, versucht der Anbieter seine potentielle Kundschaft zu umgarnen. Wir stellen uns dabei jedoch die Frage: Kann eine solche Lösung aus der Cloud effektiv mit einer On-Premises UC Plattform der Enterprise-Klasse mithalten? Ist der Funktionsumfang vergleichbar, lohnen sich die Kostenunterschiede und welche Vor- oder Nachteile bieten die Varianten?

weiter auf Seite 6

Zweitthema

Abwehr zielgerichteter Angriffe - die Paradedisziplin der Informationssicherheit

von Dr. Simon Hoff und Dipl.-Math. Simon Oberem

Zielgerichtete Angriffe, im Englischen Advanced Persistent Threats (APTs), zur Spionage und Sabotage der IT von Unternehmen, Behörden, politischen Institutionen und insbesondere auch kritischer Infrastrukturen (KRITIS) haben seit mehreren Jahren eine kontinuierliche Präsenz in den Statistiken zu Informationssicherheitsvorfällen.

Von APTs geht ein erhebliches Gefährdungspotential aus, und es ist sogar schon vorgekommen, dass am Ende einer Abwehrschlacht eine Komplettsanierung der IT anstand, wie der Angriff auf den Deutschen Bundestag vom Juni 2015 eindrucksvoll gezeigt hat.

weiter auf Seite 17

Geleit

Verdrängt BGP OSPF? Stehen wir vor einem signifikanten Design-Wandel in unseren Netzwerken?

auf Seite 2

Standpunkt

Ist Windows für Produktionsumgebungen geeignet?

auf Seite 14

Sonderveranstaltung

Das PSTN stirbt: Die neue Kommunikation mit SIP/IP

auf Seite 15

Aktuelle Seminare

Betriebsvereinbarungen und Mitarbeiterdatenschutz bei IT- und TK-Systemen

Sommerschule 2017 – Intensiv-Update auf den neuesten Stand der Netzwerktechnik

auf Seite 13 und Seite 4

Geleit

Verdrängt BGP OSPF? Stehen wir vor einem signifikanten Design-Wandel in unseren Netzwerken?

Diese Frage hat explosiven Charakter. Sie beinhaltet nicht weniger als eine Abkehr von einem Netzwerk-Design, das nun seit mehr als 15 Jahren unsere Unternehmen und Behörden prägt. Und nicht nur das. Die Frage ist gleichzeitig verbunden mit einer komplett anderen Produktauswahl: es geht also nicht um den Austausch von Software. OSPF kommt noch aus der Zeit der großen (und teuren) Modularen Switches im Kern unserer Netzwerke. BGP kommt einher mit einem Parallel-Design aus Nicht-Modularen, relativ einfachen und preiswerten Switches, dafür dann aber in größerer Zahl. Dies geht automatisch einher mit einem deutlich höheren Verkabelungs-Aufwand. BGP liegt voll auf der Linie eines Trends hin zu Switches, die mehr Hersteller-neutral sind, auf Third-Party ASICs basieren (Broadcom und Mellanox dominieren diesen Mark) und die gleichzeitig eine Basis für ein komplett offenes Netzwerk legen könnten (keine Sorge, davon sind wir noch weit entfernt, und natürlich sind Cisco und Konkurrenten fleißig dabei mit Analytics und ähnlichen Anwendungen wieder Hersteller-spezifische Elemente im Markt zu platzieren). Und dies ist keine Hersteller-abhängige Diskussion, auch Cisco ist dabei.

Wir haben die offene Diskussion dieser Frage vor dem ComConsult Netzwerk Forum 2017 begonnen und seitdem hat sie weiter an Fahrt aufgenommen. Tatsächlich hat sie gerade in den letzten Wochen einen neuen Höhepunkt erreicht. Und natürlich ist die Frage auf den ersten Blick absurd. BGP wurde nie für den Einsatz im Rechenzentrum oder im Campus geschaffen (wenn man einmal von den Hyperscalern absieht, deren Design fast immer auf BGP basiert. Dies betrifft nicht nur Facebook und Co., auch Betreiber sehr großer Rechenzentren wie Microsoft sind den Weg nach BGP gegangen). Was bedeutet das, wenn ein Protokoll nicht für einen bestimmten Einsatzzweck geschaffen wurde? Nun, ganz einfach, es erfüllt nicht alle Anforderungen dieses Bereiches. Im Falle von BGP sind das mindestens einmal die notwendigen Umschaltzeiten im Fehlerfall. Hinzu kommt, dass es mehrere Varianten von BGP gibt. So gibt es im Markt ein verwirrendes Produktangebot. Nicht alle Hersteller unterstützen alle Varianten und dies wird ergänzt um Hersteller-spezifische Erweiterungen, um die Mängel an BGP auszugleichen. Ein ak-

zeptierter offener Standard sieht definitiv anders aus. Aber man arbeitet daran. Microsoft hat eine Liste von BGP-Erweiterungen in die Normierung eingebracht, die im Prinzip alle Mängel des Verfahrens beseitigen würden.

Wieso haben wir diese Diskussion überhaupt? Und mit welchen anderen Annahmen oder Fragen geht sie einher?

Der Hauptauslöser dieser Diskussion ist die Unterstützung von Tunnelverfahren im Layer 3-Bereich von Netzwerken. Tunnelverfahren wie VXlan oder Geneve sind für virtuelle Umgebungen unverzichtbar. Der Handlungsdruck ist dabei direkt abhängig von der Größe des virtuellen Bereiches, sprich der Anzahl der virtuellen Maschinen oder Container, und der Anzahl der physikalisch durch Layer 3 getrennten Layer-2-Bereiche. In der reinen Theorie können solche Tunnel-Verfahren in jedem IP-basierten Layer-3-Netzwerk ablaufen ohne dort irgend eine Änderung zu erfordern. In der Praxis gilt dies nur für kleinere und sehr lokale Umgebungen. Für diese ist ein Design mit OSPF und eventuell MC-LAG in der Regel die beste Wahl. Dabei ist die Lokalität wichtiger als die Größe.

Gleichzeitig ist die Prognose von ComConsult Research, die wir exklusiv zu den Technologietagen 2016 im November vorgestellt haben, dass wir eine deutlich Zunahme der Anzahl von virtuellen Maschinen in den nächsten Jahren bekommen werden, die untereinander auf Layer 2 kommunizieren wollen.

Warum ist das so und wieso beeinflusst das das Netzwerk?

Analysiert man die Megatrends in den IT- und Anwendungs-Architekturen so gibt es einen Trend, der sich wie ein roter Faden durch alle Diskussionen zieht: der Zwang zur Agilität. Unter Agilität verstehen wir die Fähigkeit eines Unternehmens innerhalb von Stunden (Minuten oder Tagen, je nach Situation) seine Kapazitäten an Servern, Speicher und Netzwerk um mehrere Hundert Prozent erweitern zu können.

Wo kommt diese scheinbar absurde Forderung her? Wir haben eine ganze Reihe von Industrie-Bereichen, die vor großen Umbrüchen stehen. Beispiele wären Medien, Banken, Versicherungen, Produktionsunternehmen. Ein populäres Beispiel ist der Trend zum autonomen Auto, auch wenn dies eher im Sinne dieser Diskussion ein Randgebiet ist. Auch innerhalb der IT erleben wir große Verschiebungen: angefangen von der Ablösung der traditionellen TK-Anlagen durch UC und nun zum Beispiel im Speicher-Bereich. Generell geht es innerhalb der IT um die Ablösung von Spezial-Hardware durch Standard-Hardware und Software. Auch im Netzwerk-Bereich drohen solche Tendenzen zum Beispiel im Access-Bereich.

Was bedeutet das Wort Umbrüche und mit welchen Forderungen geht es einher?

Nehmen wir als Beispiel den Bankenbereich. Änderungen der Software im Internet-Banking erforderten in der Vergangenheit nicht selten Laufzeiten von 2 Jahren. Die neue Forderung ist: 2 Wochen. Von 2 Jahren auf 2 Wochen: dies ist der rote Faden, der sich durch unsere Untersuchung zieht, ich erspare Ihnen die anderen mehr oder weniger gleich lautenden Beispiele. Wenn es in Ihrer Branche zu einem Umbruch kommt, muss Ihr Unternehmen reagieren können. Und zwar sofort.

Na und, werden Sie denken. Was hat das mit meinem Netzwerk zu tun? Unternehmen können nur agil sein, wenn dies die Anwendungen sind. Agile Anwendungen sind grundsätzlich anders von ihrer Architektur her. Dies ist erforderlich, um zum Beispiel schnelle Änderungen in 2 Wochen in einer Banking-Applikation durchsetzen zu können ohne dabei den Super-Gau zu riskieren. Das Schlüsselwort heißt hier Mikroservice-Architekturen. Große monolithische Anwendungen werden zerlegt in viele kleine Einzel-Services. Diese skalieren besser, zum Beispiel kann ich dann von einem

Schwerpunktthema

„UCaaS Lite“: Können die Cloud-Anbieter mit ihren On-Premises Kollegen konkurrieren?

Fortsetzung von Seite 1

Timo Schmitz, B.Sc. ist bei der ComConsult Beratung und Planung GmbH in den Bereichen „Kommunikationslösungen“ und „IT-Sicherheit“ tätig. Im Projektgeschäft befasst er sich u.a. mit der Erstellung von Konzepten und der Erarbeitung von Seminarinhalten.“

Dipl.-Ing. Dominik Zöller ist seit 2006 Berater bei der ComConsult Beratung und Planung GmbH und fungiert hier als Leiter des Competence-Center „Kommunikationslösungen“. Gemeinsam mit seinem Team berät er eine Vielzahl von Kunden in Privatwirtschaft und öffentlichem Sektor. Die thematische Spannbreite umfasst insbesondere die Themenfelder Unified Communications, Sprachkommunikation, Kollaborationswerkzeuge, integrierte Geschäftsprozesse und sichere Kommunikationslösungen. Herr Zöller ist regelmäßig als Referent für die ComConsult Akademie tätig und als Autor und Co-Autor an einer Vielzahl von Veröffentlichungen beteiligt. Unter anderem ist er Co-Autor der „Technischen Leitlinie für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf“ (TLSTK II) des BSI.

Um diesen Fragen nachzugehen schauen wir uns zwei Anbieter einer solchen Cloud-Dienstleistung einmal genauer an: Zum einen Amazon Chime, als Neuankömmling in der Branche, sowie *Zoom*, einem erfolgreichen und mittlerweile etablierten Anbieter, mit über die Jahre aufgebauter Expertise im Bereich der Multi-Tenancy Unified Communications.

Amazon Chime

Mit den Amazon Web Services (AWS) entwickelte sich Amazon zu einem der populärsten und erfolgreichsten Anbieter im Segment des Cloud Computings. Die Angebote entwickelten sich im Laufe der Jahre kontinuierlich hin zu einem breit aufgestellten Leistungsportfolio. Im Februar 2017 entschied sich Amazon nun dazu, einige der Kapazitäten für eine eigene Kommunikationsplattform zur Verfügung zu stellen: *Amazon Chime* (siehe Abbildung 1).

Amazons Versuch in den Cloud-basierten UC Markt einzudringen, kann als Angriff gegen Mitbewerber wie Microsoft mit *Office 365* oder Google mit seinen als *G Suite* vermarkteten Unternehmensapplikationen gewertet werden. Bern Elliot, ein Analyst von Gartner, schätzt den Umsatz im entsprechenden Marktsektor auf 12 Milliarden Dollar im Jahr 2016 ein. Dieser soll seinen Einschätzungen zufolge, um 15 % wachsen und damit ein Umsatzhoch von 22 Milliarden Dollar im Jahr 2020 erreichen [2] (Anm. d. Autors: ein Wachstum von 12 auf 22 Mrd. Dollar binnen vier Jahren entspricht einem CAGR von durchschnittlich 16,3%). Im Unterschied zu Microsoft oder Google kann Amazon jedoch wenig Erfahrung im UC Bereich vorweisen. Um diese Wissenslücke zu schließen, erwarb Amazon im Jahr 2015 das Unternehmen *Elemental*, welches sich laut eigenen Angaben mit „Software-Defined Video Processing Solutions“ auseinandersetzt. Im darauffolgenden Jahr eignete das Unternehmen sich zusätzlich *Biba* an – ein Anbieter für Chat, Video und Audio Conferencing. Die dadurch gewonnen technologischen Erkenntnisse stellen die Basis für die nun erschienene Amazon Chime Dienstleistung dar.

Chime bietet seinen Nutzern, laut Produktkatalog [3], die gängigen UC Funktionalitäten, wie beispielsweise Online Meetings, Videokonferenzen, Chaträume, Smart Presence sowie Datenaustausch. Gegenüber seinen Konkurrenten möchte sich Chime u.a. durch herausragende Audio- sowie Videoqualität hervorheben. Eine zentrale Applikation soll als Einstiegshub für die verschiedenen Kommunikationsdienste dienen, die von stationären und mobilen Geräten angesteuert werden können. Hierbei verspricht Amazon einen „nahtlosen Übergang“ (auch während Meetings) zwischen den verschiedenen Gerätetypen, inklusive automatischer Synchronisation zwischen diesen.

Für die Nutzung von Amazon Chime werden Applikationen für die Plattformen iOS, Android, Windows sowie Mac bereitgestellt. Raumsysteme, die H.323 mit G.711/G.722 unterstützen, können eben-

„UCaaS Lite“: Können die Cloud-Anbieter mit ihren On-Premises Kollegen konkurrieren?

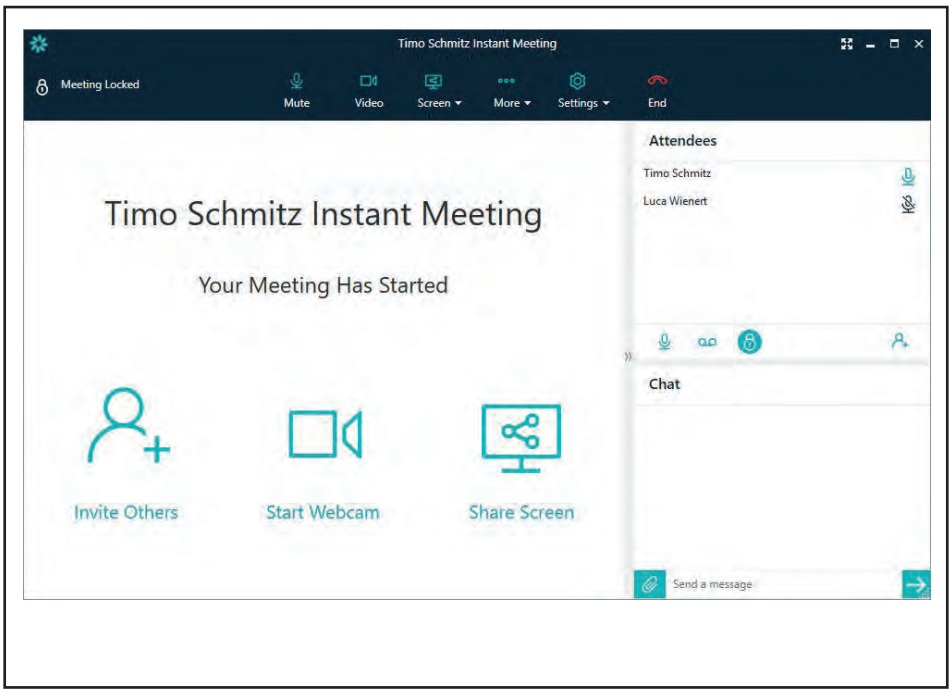

Abbildung 1: Amazon Chime Meeting User Interface

falls (ohne zusätzliche Kosten) in Meetings eingebunden werden. Damit werden die gängigsten Systeme im Enterprise-Umfeld unterstützt; einem nicht zu unterschätzenden Teil des Marktes (Linux, Windows Phones, …) wird jedoch – wie marktüblich – zunächst der Zugang verwehrt.

Dies wäre verschmerzbar, wenn die UC Plattform einen Zugriff über den Browser ermöglichen würde. Leider scheitert der Dienst in diesem Bereich jedoch kläglich: In Zeiten von HTML5 und WebRTC mit einem Produkt an den Markt heranzutreten, welches lediglich massiv eingeschränkte Funktionalitäten im Browser bietet (einzige Browser-Funktionalität: Beobachtung der Bildschirmfreigabe – ohne Audiofeed; siehe Abbildung 2), ist nicht mehr zeitgemäß. Gerade bei Cloud-Dienstleistungen sollte eine vollständige Plugin-lose Browser Lösung, auf Basis moderner, mittlerweile weit verbreiteter Protokolle, eine Selbstverständlichkeit darstellen. Interessant ist dabei, dass die Amazon Chime Software laut ersten Meldungen wohl WebRTC als technologische Basis einsetzt [4] – ohne die Möglichkeit zur Nutzung im Browser, geht der größte Mehrwert dieser Technologie für den Kunden jedoch verloren.

Insbesondere externe Teilnehmer sind dadurch gezwungen, eine proprietäre Software herunterzuladen, sofern sie am Videochat teilhaben wollen. Immerhin: Ein externer Teilnehmer muss hierfür keinen Account anlegen (anonyme Teilnahme). Für interne Teilnehmer ist außerdem eine SAML-basierte SSO Anmeldung möglich – sofern ein Chime Plus Account vorliegt.

Um externen Teilnehmern die Installation der Applikation zu ersparen, bietet Chime jedoch die Möglichkeit des Dial-In auf Kostenbasis einer Per-Minute-Rate. Auf sämtliche weitere UC Features fernab der Audiokommunikation muss der Teilnehmer dann natürlich verzichten. Die Kosten belaufen sich bei Anrufen aus Deutschland derzeit auf $0,004/Min. bzw. ca. 0,4 Euro-Cent/Min. [5]

In Punkto Sicherheit kann Amazon Chime eine AES 256-Bit Verschlüsselung vorweisen. Grundsätzlich gibt sich Amazon etwas wortkarg in der Beschreibung der Sicherheitsumstände, unter denen die (ggf. streng vertraulichen) Gesprächsdaten gesichert werden: „Amazon Chime is an AWS service, which means you benefit from a data center and network architecture built to meet the requirements of the most security-sensitive organizations“. [3]

Wie der Titel bereits andeutet: Man sollte Amazon Chime nicht ohne weiteres als vollwertige UCaaS Lösung bezeichnen. Die Telefonie über SIP-Nebenstellen kann nicht durch die Applikation übernommen bzw. aufgefangen werden. Eine Ergänzung der Lösung im Sinne einer Hybrid Cloud oder einer Kombination von Cloud-Lösungen wird daher vonnöten sein, wodurch die ursprünglich eingesparten Investitionskosten u.U. wieder hinfällig sein werden.

Beim Zahlungsmodell setzt Amazon auf ein gestaffeltes Abonnement-Modell und die „Pay-As-You-Go“ Zahlungsvariante. Basisfunktionalitäten, wie die 1:1 Kommunikation, stehen Nutzern dabei kostenlos zur Verfügung. Für $2,50/User/Monat stehen Funktionalitäten zur Bildschirmfreigabe sowie Anbindung an das Active Directory zur Verfügung. Um Meetings selbst leiten und erstellen zu können, wird jedoch eine Pro Lizenz notwendig, welche mit $15/User/Monat zu Buche schlägt. Diese ermöglicht die Erstellung von Video Meetings für bis zu 100 Teilnehmer. Abbildung 3 stellt die Funktionalitäten, die durch die jeweilige Lizenz freigeschaltet werden können, noch einmal explizit vor. Zunächst erscheint das Zahlungsmodell mit der Basic und Plus Variante preislich sehr fair gestaltet. Der drastische Preisunterschied zwischen der Plus und Pro Lizenz stößt dabei jedoch sauer auf. Bei

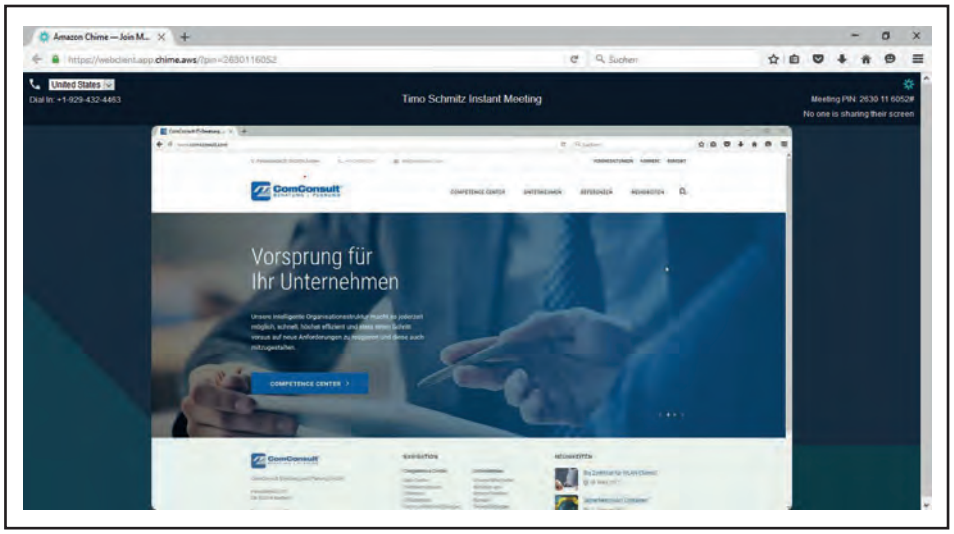

Abbildung 2: Amazon Chime Ansicht einer Bildschirmfreigabe im Browser

Zweitthema

Abwehr zielgerichteter Angriffe - die Paradedisziplin der Informationssicherheit

Fortsetzung von Seite 1

Dr. Hoff ist technischer Direktor der ComConsult Beratung und Planung GmbH und blickt auf jahrelange Projekterfahrung in Forschung, Standardisierung, Entwicklung, Planung und Betrieb in den Bereichen IT-Sicherheit, lokale Netze und mobile Kommunikationssysteme zurück.

Dipl.-Math. Simon Oberem ist als Berater bei der ComConsult Beratung und Planung GmbH in dem Bereich IT-Sicherheit tätig. Im Projektgeschäft befasst er sich maßgeblich mit den Aspekten von ISMS nach ISO 27001, auch auf Basis BSI-Grundschutz sowie deren praxistauglicher Umsetzung.

Es wäre nun fatal zu denken, man selber könnte nie Ziel eines solchen Angriffs werden. Eine typische Frage ist hier: „Was könnte ein Angreifer bei mir schon holen?“. Eine Antwort kann z.B. einfach sein: Identitäten. Es hat schon APTs gegeben, die zunächst eine Institution angegriffen und kompromittiert haben, um das eigentliche Angriffsziel durch E-Mails, die nachvollziehbar von einer vertrauenswürdigen Quelle (nämlich der zunächst angegriffenen Institution) stammen, leichter angreifen zu können. Als Beispiel kann hier ein Angriff auf das Weiße Haus in den USA im Jahr 2015 [1] genannt werden. Hier hatte der Angreifer zunächst das Außenministerium gehackt, um dann von dort aus am Weißen Haus mit bösartigen Phishing Mails anzugreifen [2].

Außerdem gibt es einen weiteren gefährlichen Trend. Wie dem Lagebericht des BSI 2016 zu entnehmen ist, „findet ein Technologietransfer aus dem Bereich der Advanced Persistent Threats (APT) hin zu den allgemeinen Schadprogrammen statt“ [3]. Dieser Technologietransfer hat sich z.B. im Bereich der Kryptotrojaner schon deutlich gezeigt.

Um Abwehrstrategien gegen APTs entwickeln zu können, ist es entscheidend die Vorgehensweise und den Werkzeugkasten der Angreifer zu verstehen („Know your enemy!“) und die eigene IT mit den Augen eines potentiellen Angreifers zu sehen.

.1. Was genau ist ein zielgerichteter Angriff?

Ein zielgerichteter Angriff hat ein fest umrissenes Angriffsziel, läuft typischerweise in mehreren Phasen ab und kombiniert unterschiedliche, aufeinander aufbauende Angriffstechniken. Der englische Begriff APT beschreibt die Charakteristiken sehr treffend:

- **Advanced:** Der Angreifer hat Know-how und nutzt fortgeschrittene Techniken. Das heißt natürlich nicht, dass der Angreifer nicht auch auf frei verfügbare Werkzeuge zurückgreift.

- **Persistent:** Ein APT kann sich über einen längeren Zeitraum hinziehen und der Angreifer arbeitet sich ausdauernd zum Angriffsziel vor und wartet auch geduldig auf sich bietende Angriffsgelegenheiten. Je nach Angriffsziel kann der Angreifer zum Dauergast in der angegriffenen Infrastruktur werden.

- **Threat:** Der Angreifer nutzt systematisch Schwachstellen aus, die er in der angegriffenen Infrastruktur vorfindet. Im Extremfall werden auch sogenannte Day Zero Exploits eingesetzt, d.h. bisher unbekannte Ausnutzungen von (ggf. bis dato unbekannten) Schwachstellen, die die Organisation des Angreifers selbst entwickelt oder in der dunklen Seite des Internets eingekauft hat.

Typischerweise läuft ein APT in fünf Phasen ab (siehe Abbildung 1).

Phase 1: Auskundschaften / Zielerfassung

In der ersten Phase werden Spear Phishing, Watering-Hole-Angriffe und andere Varianten des Social Engineering eingesetzt. Beim Spear Phishing enthält eine als seriös getarnte E-Mail ein Attachment mit Schadsoftware oder einen Link auf eine schadenstiftende Web-Seite. Watering-Hole-Angriffe infizieren zielgerichtet Web-Seiten, die das Ziel potentiell besucht, z. B. eine spezielle Community, wie ein Developer-Forum.

Phase 2: Eindringen und Erstinfektion

In Phase 2 wird der in Phase 1 eingebrachte schadenstiftende Code dann ausgeführt und lädt typischerweise den eigentlichen Schädling auf das angegriffene System. Hierzu muss lediglich ein Internet-Zugang für das infizierte System erlaubt sein, das dann beispielsweise ein sogenanntes Remote Administration Tool (RAT) herunterlädt und ausführt. Das RAT unterhält dann eine Verbindung zur zentralen Infrastruktur des Angreifers, dem Command and Control Server (C&C). Diese Kommunikation ist natürlich nach den Regeln der Kunst verschleiert, d.h. die Kommunikation erfolgt verschlüsselt über mehrere Stufen (z.B. Systeme in einem Bot-Netz), die eine Nachverfolgung ausgesprochen schwer macht.

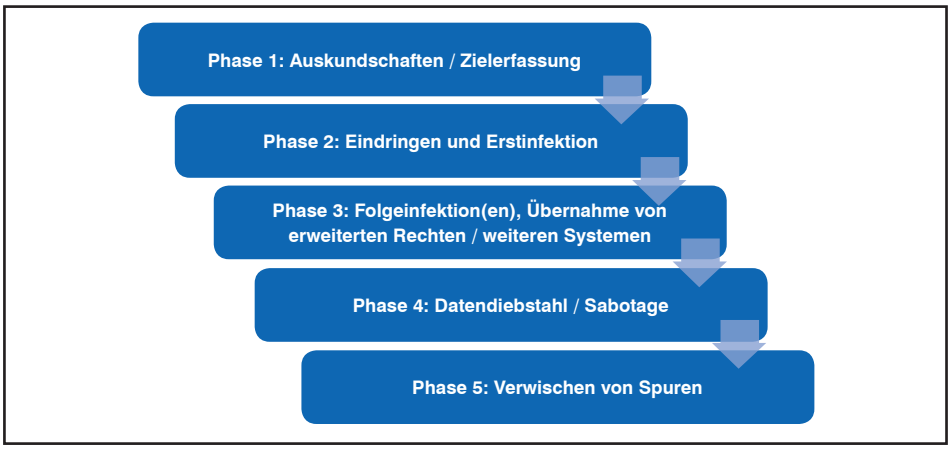

Abbildung 1: Typische Phasen eines zielgerichteten Angriffs

Phase 3: Folgeinfektion(en), Übernahme von erweiterten Rechten / weiteren Systemen

Nicht selten ist das zunächst angegriffene System nicht das eigentliche Ziel bzw. nicht das einzige Ziel. In der dritten Phase erfolgt dann die Ausbreitung des Angriffs im Netzwerk, indem Server, PCs von Administratoren und sonstige Systeme angegriffen werden. Ggf. wird hierfür zusätzliche Schadsoftware vom C&C geladen. Alternativ können auch auf dem kompromittierten Rechner vorgefundene Tools wie Shells, Windows Terminal Services, NetBIOS-Befehle oder Virtual Network Computing verwendet werden.

Phase 4: Datendiebstahl / Sabotage

In Phase 4 verrichtet der Angreifer über die Schadsoftware in der angegriffenen Infrastruktur seinen Dienst, indem er z. B. Systeme sabotiert oder Passworte, Dokumente, etc. überträgt. Bei einem Datendiebstahl befindet sich der eigentliche Ziel-Server wie eben skizziert über mehrere Stufen versteckt im Internet.

Phase 5: Verwischen von Spuren

Zuletzt vernichtet sich der Schädling selbst, mutiert, indem er neuen Schadcode nachlädt, oder löscht lediglich einen Teil seiner Komponenten bzw. Daten und legt sich zur Ruhe.

2. Warum sind zielgerichtete Angriffe so oft erfolgreich?

Der Erfolg zielgerichteter Angriffe hat zwei grundlegende Ursachen:

- **Das Ganze ist mehr als die Summe seiner Einzelteile**
  Es werden system- und anwendungsübergreifende Angriffe ausgeführt. Hierdurch entsteht ein Kumulationseffekt hinsichtlich der ausgenutzten Schwachstellenlage. Hinzu kommen das mangelnde Bewusstsein bei Nutzern und Administratoren, die oft unzureichende Umsetzung von Sicherheitsmaßnahmen und zugehörigen Prozessen sowie auch eine Überschätzung der eigenen Security.

- **Ausnutzung längst bekannter Schwachstellen in der IT**
  Oft müssen gar keine High-End-Angriffswerkzeuge eingesetzt werden, sondern es reichen allgemein verfügbare Freeware Tools. Beim oben genannten Bundestags-Hack 2015 haben die Angreifer unter anderem auch auf das in der Praxis bewährte Tool mimikatz [4] urückgegriffen, um über Schwachstellen in Windows-PCs an Credentials für die Anmeldung an Admin-Konten heranzukommen [5].

3. Gibt es Symptome eines zielgerichteten Angriffs?

In den Phasen 1 und 2 des Angriffs finden sich z. B Malware in E-Mail-Anhängen oder auf Web-Seiten und in Folge Backdoor-Trojaner auf Endgeräten. Hier ist zwar eigentlich der Virenschutz gefordert, nur gelingt es den Angreifern immer wieder sich erfolgreich am Virenschutz vorbei zu schmuggeln.

In den weiteren Phasen eines APT gibt es gewisse Symptome, die auf den Angriff hindeuten können.

In der dritten Phase des Angriffs kann beispielsweise die Zahl der Anmeldungen an Konten mit erweiterten Rechten zunehmen. Dies ist oft auch häufig außerhalb der regulären Arbeitszeit zu verzeichnen. Auch Log-Einträge, die auf gehäufte Fehlanmeldungen an einem System / Konto hindeuten, oder solche, die auf den Stopp / Neustart sicherheitsrelevanter Dienste wie Virenschutz oder Firewall hindeuten, können ein Indiz für einen zielgerichteten Angriff in der Phase 3 sein. An dieser Stelle wird oft die Rolle einer (zentralen) Protokollierung unterschätzt. Die typische Maßnahme, fehlerhafte Anmeldeversuche an Systemen und Anwendungen zentral zu protokollieren und ggf. eine Alarmierung auszulösen, kann solche Angriffe nämlich durchaus aufdecken. Wie die WirtschaftsWoche im Dezember 2016 berichtet hatte, ist z. B. ein massiver Cyberangriff auf Thyssen Krupp dadurch aufgefallen, dass mehrere fehlerhafte Anmeldeversuche auf einem Server verzeichnet wurden.

Während der Phase 4 eines zielgerichteten Angriffs können große Datenbestände an ungewöhnlichen Speicherorten und / oder komprimierte Daten in einem für die betreffende Institution unüblichen Format auffallen. Auch ausgehende Verbindungen zu Servern mit schlechter Reputation, z. B. für schadenstiftende Inhalte bekannte Server oder bekannte C&C Server, deuten auf einen zielgerichteten Angriff hin. Ein weiteres Indiz können ungewöhnliche bzw. große insbesondere ausgehende Datenströme oder ungewöhnliche verschlüsselte Netzverbindungen sein.

4. Maßnahmen

Um zielgerichtete Angriffe erkennen und abwehren zu können, werden system- und anwendungsübergreifende Strategien benötigt. Hierzu reichen jedoch technische Maßnahmen alleine nicht aus! Mindestens genauso wichtig sind organisatorische Maßnahmen, wie beispielsweise die Sensibilisierung aller Mitarbeiter. Damit diese Maßnahmen nachhaltig zusammenwirken und sich ergänzen, ist als Basis ein Information Security Management System (ISMS) unentbehrlich (siehe Abbildung 2).

4.1 Was taugen traditionelle Maßnahmen zur Abwehr von APTs?

Zunächst muss an dieser Stelle festgehalten werden, dass bestehende, traditionelle technische IT-Sicherheitsmaßnahmen ihren festen Platz auch in der Bekämpfung zielgerichteter Angriffe haben (siehe Abbildung 3). Denn jede Maßnahme, die es einem Angreifer erschwert seinen Angriff durchzuführen, ist eine sinnvolle Maßnahme.

Traditionelle technische IT-Sicherheitsmaßnahmen

Intrusion Detection and Prevention Systems (IDPSs) ermöglichen auf der Basis von Signaturen und mit statistischen Methoden eine Erkennung von Anomalien im Netzverkehr, die auf Schadsoftware bzw. allgemein auf einen Angriff hindeuten können. Je nach Policy kann dann ein als schadenstiftend erkannter Verkehr vom IDPS geblockt werden. Da der Einsatz einer IDPS-Funktion z.B. in einer Firewall mit