ComConsult Research

Der Netzwerk Insider

Mai 2018

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Sicherer Zugang zu Cloudanwendungen

von Dipl.-Math. Cornelius Höchel-Winter

Mit der rasanten Zunahme von Anwendungen aus der Cloud (Software as a Service) und der verbreiteten Nutzung mobiler Endgeräte, rückt ein altes Thema erneut in den Vordergrund: die Absicherung des Zugriffs auf Unternehmensdaten. Cloudanwendungen greifen per Design sowieso nur auf Daten in der Cloud zu und die Nutzung von mobilen Endgeräten setzt voraus, dass auf die Daten von der jeweiligen Anwendung aus zugegriffen werden kann – unabhängig davon, wo sich diese Daten befinden: On-premises oder in der Cloud.

Natürlich gibt es eine Reihe von technischen Lösungen den direkten Zugriff von Endgeräten außerhalb des Unternehmensnetzes auf Daten innerhalb zu unterbinden, aber selbst wenn Sie auf VPNs (Virtual Private Networks) oder Application Streaming setzen, am zugrunde liegenden Problem ändert das nichts: Endgeräte haben von außerhalb Ihres Unternehmensnetzes Zugriff auf Ihre Daten.

Vorbemerkung

Wie immer, wenn es um die Sicherung von Zugängen geht, gibt es eine drastische Lösung: die komplette Blockierung des Zugriffs auf die Daten von unsicheren Netzbereichen aus.

weiter ab Seite 9

Best Practice für die sichere Administration der IT

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

Je mächtiger die Berechtigungen eines Nutzers für den Zugriff auf IT-Systeme oder Anwendungen ist, desto wichtiger ist die Absicherung solcher Zugriffe. Dies gilt insbesondere für administrative Zugriffe auf IT-Komponenten und erfordert einen umfassen spezifischen Maßnahmenkatalog, der sich verschiedenster Techniken der Informationssicherheit von Sicherheitszonen, Firewall-Techniken über Authentisierung & Autorisierung bis hin zur Protokollierung und Verhaltensanalyse bedient.

Dieser Artikel beschreibt die Techniken, die sich dabei als Best Practice in verschiedensten IT-Infrastrukturen bewährt haben.

weiter auf Seite 17

Geleit

Power over Ethernet als generelle Stromversorgung: alles Wahnsinn oder was? Und wer bitte ist denn zuständig?

auf Seite 2

Standpunkt

Vorsicht mit asymmetrischem Routing!

auf Seite 26

Aktuelle Sonderveranstaltung

Der Arbeitsplatz der Zukunft

ab Seite 7

Neues Seminar

Law Camp 2018

auf Seite 25

Aktuelle Seminare

Sommerschule – Intensiv-Update auf den neuesten Stand der Netzwerktechnik

ab Seite 4

Netzwerk-Sicherheit

auf Seite 27

Geleit

Power over Ethernet als generelle Stromversorgung: alles Wahnsinn oder was? Und wer bitte ist denn zuständig?

Das Smart Building klopft an und es fordert neue Konzepte zur Integration einer Vielzahl von Sensoren und Aktoren. Auf den ersten Blick wird man da vorwiegend an Funktechniken denken. Das macht auch sicher Sinn. Allerdings kommen Funktechniken nicht überall zum Einsatz. Immer wenn eine Garantie für die Übertragung gefordert wird, wird Funk außen vor bleiben müssen. Und außerdem: auch Funk und die entsprechende Sensorik brauchen Strom (überwiegend).

Also worum geht es? Die Diskussion wurde in der Beleuchtungstechnik gestartet. Am Anfang haben vor allem Phillips und Cisco in einigen Vorzeigeprojekten das Thema getrieben. Inzwischen springt die gesamte Branche auf den immer schneller fahrenden Zug. Die Grundidee ist, dass moderne LED-Beleuchtungen so wenig Strom brauchen, dass eine Versorgung über PoE möglich ist. Dies gilt schon für die bisherige proprietäre 60W-Variante, die Cisco etwas überteuert anbietet. Es gilt aber noch mehr für die 100W, die wir in Zukunft als internationalen Standard bekommen werden.

Aber warum sollte man das machen, warum nicht einfach wie bisher ein Stromkabel zur Lampe bringen? Nun, die Motivation kommt aus der Kombination aus Strom und Kommunikation in einem Kabel. Mit PoE bringe ich eben nicht nur Gleichstrom zur Lampe, sondern auch den Netzwerk-Anschluss. Und dieser betrifft nicht nur die Steuerung der Beleuchtung, sondern vor allem auch die Idee, dass Lampen zum generellen Träger von Intelligenz und Sensorik werden können. Damit werden Anwesenheitssensoren integriert, WLAN-Access Points, Temperaturfühler und was immer sonst als Intelligenz gewünscht wird.

Und warum sollte diese Idee bei der Beleuchtung halt machen? Gilt diese Überlegung der Kombination aus Strom und Kommunikation nicht für viele Orte und Technologien im Gebäude der Zukunft?

Das Konzept hinter dieser ganzen Diskussion ist, dass das Gebäude der Zukunft dem Benutzer in Abhängigkeit von dem jeweiligen Ort die Möglichkeit bietet, diesen Ort nach seinen Wünschen zu gestalten. Die Annahme dahinter: zufriedene Mitarbeiter sind motivierte und effiziente Mitarbeiter. Effiziente Mitarbeiter motivieren höhere Mieten und machen Gebäude im Markt attraktiver. Soweit die Theorie. Allerdings gibt es herausragende Modellprojekte, die einem ernsthaft zu denken geben. Dazu gehört das Bloomberg-Gebäude in London. Die Wirtschaftlichkeit solcher extremen Gebäude muss man im Moment vermutlich noch in Frage stellen, aber sie zeigen eine Richtung auf. Und sie erlauben einen Proof-of-Concept im Sinne der Bewertung einer Verbindung zwischen Gebäude, Zufriedenheit und Effizienz. Die Psychologie hinter einigen dieser Konzepte existiert, ist aber umstritten. Dazu gehört die Annahme, dass ein bewusst erzeugtes Chaos die Kreativität steigert

(positiv denkend würde man das Wort Chaos durch Vibrance ersetzen). Die Kernfrage ist: Kann man Vibrance schaffen und trotzdem eine Konzentration am Arbeitsplatz ermöglichen ohne die Störeinflüsse aus der Umgebung? Und genau hier setzt das Bloomberg-Gebäude an. Es schafft sehr offene Flächen und viel Interaktion, liefert aber gleichzeitig so etwas wie akustische Privatheit. Aber zurück zu PoE.

Die Basis zur Umsetzung individueller Zufriedenheit sind Apps, die auf den Smartphones von Mitarbeitern und Besuchern aktiv sind. Beispiele dafür sind:

- Die individuelle Gestaltung der Beleuchtung am Arbeitsplatz
- Die individuelle Beeinflussung von Klimatisierung
- Eine Integration mit der Medientechnik zur schnellen Buchung und Findung freier Besprechungsräume
- Die Wegführung von Besuchern hin zu ihrem Ziel im Gebäude

Gleichzeitig geht man davon aus, dass die Nutzung des Gebäudes der Zukunft dynamischer ist. Räume oder Flächen und ihre Nutzung ändern sich über die Zeit. Und man möchte im Sinne einer optimalen Ausnutzung des Gebäudes bei gleichzeitiger Reduzierung der Betriebskosten analysieren können, ob die aktuelle Nutzung des Gebäudes der angestrebten Flächennutzung entspricht.

Sicherer Zugang zu Cloud-anwendungen

Fortsetzung von Seite 1

Dipl. Math. Cornelius Höchel-Winter ist Leiter des Technologie-Labors und des Bereichs Systemintegration bei der ComConsult Research GmbH. In dem Labor werden regelmäßig Messungen und Evaluierungen neuester Hard- und Softwareprodukte durchgeführt und ausgewertet. Herr Höchel-Winter besitzt langjährige Erfahrung in der Konzeptionierung, im Aufbau und Betrieb von RZ- und Campusnetzen und von Windows- und Linux-Umgebungen. So hat er als verantwortlicher Projektmanager die Rechenzentren und Netzwerke auf dem Gelände der EXPO2000 in Hannover aufgebaut und während der Weltausstellung betrieben. Für die ComConsult Akademie ist er außerdem seit 2001 als Autor, Trainer und Referent auf Seminaren und Kongressen schwerpunktmäßig in den Bereichen Data Center, Virtualisierung, Storage, Netzwerke und Cloud Computing tätig.

Solange Ihre Daten innerhalb Ihres Netzes liegen, ist das technisch vergleichsweise einfach: Solange Ihre Perimeter-Firewall das tut, was sie soll, sind Zugriffe von außen nach innen blockiert und Ausnahmen, zum Beispiel VPN, müssen explizit freigegeben werden. Und die Frage, wie man verhindert, dass Daten von innen nach draußen kommen, liegt außerhalb dessen, was wir in diesem Artikel beleuchten wollen. Themen hier sind: Virenschutz, Data Loss Prevention (DLP), Gerätemanagement.

Liegen Ihre Daten aber sowieso schon in der Cloud, weil Sie beispielsweise CRM-Anwendungen wie Salesforce oder Kollaborationsplattformen wie Office 365 oder die Google G-Suite nutzen, müssen zusätzliche Funktionen eingeführt bzw. aktiviert werden, um den, in diesen Fällen ja standardmäßig erlaubten Zugriff auf diese Daten doch noch einzuschränken. Im Wesentlichen stehen Ihnen hier drei Möglichkeiten zur Verfügung:

1. Der Service-Provider bzw. die Anwendung selbst bieten Funktionen an, um den Zugriff einzuschränken.

2. Der Service-Provider bietet SSO-Funktionalität (Single Sign-On) an und Ihre SSO-Lösung bietet Funktionen an, um den Zugriff einzuschränken.

3. Sie verschlüsseln die Daten so, dass Entschlüsselungsfunktionen nur innerhalb Ihres Netzwerks zur Verfügung stehen. Auch das geht meist nur mit der Unterstützung des Service-Providers, Azure Rights Management (Azure RMS) zusammen mit einem selbst verwalteten Schlüsselmanagement (HSM - Hardware Security Module) ist ein Beispiel für eine als HYOK (Hold Your Own Key) bezeichnete Lösung.

Wir werden die beiden erstgenannten Fälle weiter unten noch diskutieren.

So oder so, in beiden Fällen muss klar sein, dass Sie letztlich die Produktivität Ihrer Mitarbeiter zugunsten der Sicherheit Ihrer Daten einschränken! Hierfür mag es in besonderen Umgebungen oder bestimmten Situationen Gründe geben, Sie sollten solche Einschränkungen aber auf Ausnahmen beschränken, die Idee von Cloud-Anwendungen sowie der Nutzen von mobilen Endgeräten liegen im unbeschränkten Einsatz „jederzeit und von überall“ und der damit verbundenen Produktivitätssteigerung.

Anforderungen

Kommen wir zurück zum eigentlichen Thema: Wie sichere ich den – generell erlaubten – Zugriff auf Unternehmensdaten zuverlässig ab?

Im Zeitalter der Cloud bedeutet das zweierlei:

1. Wie verhindere ich den nicht autorisierten Zugriff auf Endgeräte, auf denen gegebenenfalls Unternehmensdaten (zwischen)gespeichert sind, oder die Zugang zu Unternehmensanwendungen zum Beispiel via VPN haben?

2. Wie sichere ich den Zugang zu Clouddaten respektive die Nutzung von Cloudanwendungen ab?

Sichere Passwörter

Beginnen wir ganz generisch. Egal ob Endgerät oder Anwendung, die klassische Authentifizierung – also die Prüfung der Authentizität des Benutzers – geschieht nach wie vor über Benutzername und Passwort. Die Nutzung sicherer Passwörter ist also essentiell für jedes Sicherheitskonzept, das Passwörter nutzt. Ansonsten könnte man gleich darauf verzichten.

Sichere Passwörter gerade für Endgeräte – auch für den Zugang zum Arbeitsplatzrechner – sind im Übrigen kein übertriebener Selbstzweck, um zu verhindern, dass sich die Kollegen Ihre Urlaubsbilder anschauen. Der Gesetzgeber verlangt sehr deutlich, dass es klare (und dokumentierte!) Regeln gibt, wer wann auf welche Daten zugreifen darf. Nachweisen können Sie das nur, wenn Sie ein paar offensichtliche Grundregeln einhalten:

1. Sie verwenden ausschließlich persönliche Benutzerkonten.

   Mit funktionalen Benutzerkonten haben Sie in der Regel keine Möglichkeit nachzuweisen, wer tatsächlich an dem Rechner gearbeitet hat.

   Spannend in diesem Zusammenhang ist im Übrigen der Umgang mit sogenannten Administrator-Konten! Einerseits ist es zwar übliche Best-Practice, auch Administratoren und andere Mitarbeiter nicht standardmäßig mit administrativen Rechten auszustatten, andererseits sehen einige spezielle Geräte und auch eine Reihe von Cloud-

Sicherer Zugang zu Cloudanwendungen

anwendungen nur ein einziges Administrator-Konto vor. In diesen Fällen ist es angebracht, über Logging und Dokumentationspflichten (Stichwort „Change Management“) den Zugang und die Nutzung solcher Konten extra zu protokollieren.

2. Kurze Inaktivitätszeitspannen bis der Bildschirm gesperrt ist. Benutzer neigen dazu, selbst in die Mittagspause oder abends nach Hause zu gehen, ohne ihren Arbeitsplatz zu sperren.

3. Sichere Passwörter und der sichere Umgang damit. Selbstverständlich sollten Passwörter auch unter Kollegen nicht weitergegeben werden oder auf einem Post-it am Bildschirm kleben.

Mit Inkrafttreten der neuen Datenschutzgrundverordnung (DSGVO) der EU in ein paar Tagen sind Probleme in diesen Bereichen zumindest im Zusammenhang mit personenbezogenen Daten mit happigen Bußgeldern belegt! Übersehen Sie nicht, dass Sie als Unternehmen hier in der Beweispflicht stehen, alle Vorkehrungen getroffen zu haben, dass Ihre eigenen Regeln auch eingehalten werden. Bußgelder werden aber immer nur gegen natürliche Personen verhängt. Das heißt, auch Sie als Mitarbeiter stehen in der Verantwortung. Bei einem Fehlverhalten oder dem fahrlässigen Umgang mit sensiblen Daten trifft Sie nicht nur der Zorn Ihres Arbeitgebers, Sie müssen auch ganz persönlich mit rechtlichen und finanziellen Konsequenzen rechnen.

Rein formal haben Sie aber, unter Beachtung der oben aufgeführten Grundregeln, mit einer klassischen Zugangssteuerung via Benutzernamen und Passwort Ihre Anforderungen erfüllt. Der Großteil der Produkte bietet ja auch gar keine andere Form der Authentifizierung an.

Wie aber stellt man „sichere Passwörter“ sicher – und was ist das überhaupt?

Jahrzehntelang wurden wir mit Passwortrichtlinien gequält, die sicherstellen sollten, dass wir möglichst komplexe Passwörter nutzen und die dann auch noch alle paar Wochen wechseln. Ob und wie man sich solche Passwörter merken kann, bleibt üblicherweise unberücksichtigt.

Merkwürdigerweise hat kaum jemand diese Richtlinien je hinterfragt – und trotzdem wird man schon von jedem zweitklassischen Webshop aufgefordert, sein Passwort mit „mindestens einem Sonderzeichen, zwei Ziffern und drei Buchstaben“ auszustatten.

Erst in den letzten Jahren setzt hier ein Überdenken (von einem Umdenken sind wir noch etwas entfernt) ein.

Das NIST (National Institute of Standards and Technology) hat beispielsweise im vergangenen Jahr seine Richtlinie „Digital Identity Guidelines“ (800-63-3) komplett überarbeitet und eine Reihe klassischer Empfehlungen für den Umgang mit Passwörtern komplett gekippt. Hierzu gehören:

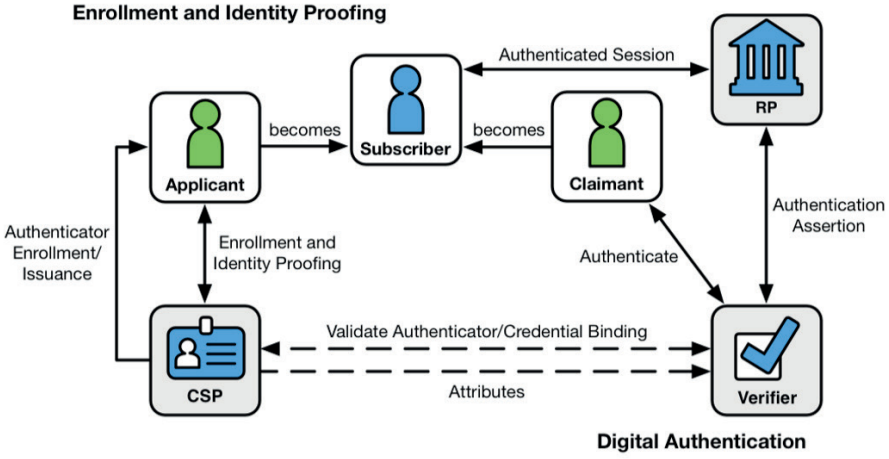
- Regeln zur Zusammensetzung von Passwörtern wie mindestens ein Sonderzeichen und eine Ziffer oder sowohl Groß- als auch Kleinbuchstaben,
- feste Zeiträume, in denen Passwörter ablaufen und ersetzt werden müssen,
- sogenannte Hinweise zum Passwort oder die bekannten Fragen zum Geburtsnamen der Mutter oder Kosename des Haustiers.

Tatsächlich hat sich die Vorstellung „komplexe“ Passwörter (mit einem Mix aus großen, kleinen Buchstaben, Ziffern und Sonderzeichen) seien per se sicher als weniger komplexe Passwörter als nicht haltbar herausgestellt. (siehe Abbildung 1)

Die Motivation, die hinter dieser Regel steht, ist die Annahme, dass Angriffe auf Passwörter in erster Linie Brute-Force-Angriffe sind. Das ist falsch. Die Mehrzahl der erfolgreichen Angriffe basiert auf Angriffen auf schlecht gesicherte Datenbanken, über Schwachstellen der Serverbetriebssysteme, über Dictionary Angriffe, bei denen Sammlungen bekannter Passwörter ausprobiert werden, und über sogenanntes Social Engineering. Letzteres erstreckt sich von einfachen Phishing-Mails („Wir haben ein XY-Problem festgestellt, geben Sie hier Ihr Passwort ein.“), unverlangt zugesandten Gutscheinen für personalisierte Kaffeebecher (womit der Angreifer schon mal die Namen der Familienangehörigen kennt) bis zum konkreten Ausspähen des Arbeitsplatzes (wo ja auch gerne die Zettel mit den Passwörtern „versteckt“ werden).

Darüber hinaus zerschellen Forderungen nach komplexen Passwörtern aber auch geradezu an der Realität. Benutzer neigen dazu, leicht zu merkende Passwörter zu wählen. Aber „Pa$$w0rd“ ist eben kein besonders gutes Passwort, auch wenn alle vier Kategorien von Zeichensätzen verwendet werden. Das NIST empfiehlt in den neuen Richtlinien, keine übertriebenen Forderungen an Passwörter zu stellen. Tatsächlich kann man nachweisen, dass der Sicherheitsgewinn durch komplexe oder etwas längere Passwörter marginal ist – auch wenn solche Policies auf dem Papier durchaus gut aussehen und ein hohes Sicherheitsniveau vorgaukeln.

Wesentlich schwerer wiegt jedoch der Schaden, der mit solchen Richtlinien angerichtet wird. Frustrierte Benutzer sind erfindungsreich und suchen nach leichten Auswegen. Also werden Passwörter wie „FranzJosef-01“ oder „Pa$$word1“ gewählt und die hinteren Ziffern bei Ablauf des Passworts einfach hochgezählt. Offensichtlich erreicht man so kein sicheres Passwort. Ganz im Gegenteil: Solche schwachen Passwörter sind das Einfalls-



Die linke Seite zeigt den Enrollment-Prozess, in dem sich ein Antragsteller (applicant) an einen Provider CSP (Credential Service Provider) wendet, um Zugangsdaten zu vereinbaren.

Die rechte Seite zeigt die Authentifizierung eines Bewerbers (claimant), der auf Ressourcen der RP (Relying Party) will. Die überprüfende Stelle (verifier) ist im Modell getrennt vom CSP dargestellt, wird sich in der Regel aber im selben System befinden.

Abbildung 1: NIST: Digital Identity Model

Best Practice für die sichere Administration der IT

Fortsetzung von Seite 1

Dr. Simon 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.

1. Warum ist eine sichere Administration der IT so wichtig?

Administrative Zugriffe bieten Zugang zu IT-Komponenten und deren Konfiguration, die sowohl Einblick in die IT-Umgebung als auch Zugriff auf Einstellungen und Komponenten ermöglichen, der für Angreifer weitaus interessanter ist, als ein normaler Zugriff auf eine IT-Komponente. Außerdem sind mit den administrativen Zugriffen auch meist höhere Berechtigungen verbunden, die für einen Angreifer lukrativ für seine Zwecke sind. Damit bietet also administrativer Datenverkehr ein hohes Angriffspotential. Gefahren liegen dabei in verschiedenen Bereichen:

Die besondere Rolle des IT-Administrators

Ein IT-Administrator benötigt zur Erfüllung seiner Aufgaben weitergehende Rechte als ein normaler IT-Nutzer. Letzterer kann aber bereits erheblichen Schaden anrichten. Bei einem Administrator jedoch kann der Schaden immens sein, ob beabsichtigt oder nicht.

So kann eine unbewusste Fehlkonfiguration eines IT-Administrators die IT lahmlegen oder einem Angreifer ungewollt Zugriff verschaffen. Allerdings kann ein Administrator auch bewusst Schaden verursachen, wie im Fall des „Revenge Wipe“ vom Juni 2017, als ein ehemaliger Administrator bei einem niederländischen Provider Daten gelöscht und damit großen Schaden angerichtet hat [1].

Das Problem des direkten unkontrollierten Zugriffs auf IT-Komponenten

Zur schnellen und einfachen Ausführung seiner Aufgaben wünscht sich ein IT-Administrator natürlich einen direkten Zugriff auf die von ihm zu administrierenden IT-Komponenten von seinem PC aus, egal wo dieser gerade angeschlossen ist. (siehe Abbildung 1).

Wenn aber die Administrationsschnittstelle einer IT-Komponente von jedem beliebigen System im Netz erreicht werden kann, bietet dies eine große Angriffsfläche. Dann steht und fällt die Sicherheit mit der Absicherung der Administrationsschnittstelle auf der IT-Komponente. Hier muss eine angemessene Authentisierung erfolgen, so dass nur ein berechtigter IT-Administrator über die Administrationsschnittstelle Zugriff zu der IT-Komponente erlangen kann. Außerdem müssen für den administrativen Zugriff sichere Protokolle eingesetzt werden, um ein Abhören oder eine Manipulation des Administrationsverkehrs zu verhindern.

Das Problem von Schwachstellen in Administrationsschnittstellen

Auch Schwachstellen in Administrationsschnittstellen kommen immer wieder vor, z. B. nicht ersetzte Default-Passworte, „vergessene“ Backdoors oder eine unzureichende Input-Validation bei Web-Anwendungen. Ende März gab es hierzu beispielsweise eine Warnung des BSI,

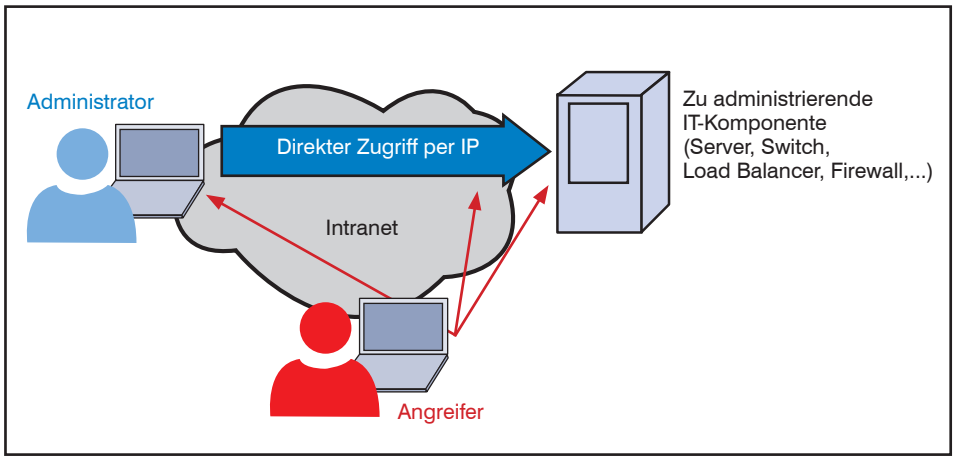


Abbildung 1: Gefährdungspotential eines direkten IP-Zugriffs eines IT-Administrators auf die zu administrierenden IT-Komponenten

die eine Schwachstelle bei Cisco Routern und Switches betraf und die eine komplette Systemübernahme möglich machte [2].

Daher ist eine systematische Berücksichtigung der Administrationsschnittstellen im Schwachstellenmanagement als Bestandteil eines Information Security Management System (ISMS) unerlässlich.

Zielgerichtete Angriffe

Ein zielgerichteter Angriff (englisch: Advanced Persistent Threat, APT) hat ein fest umrissenes Angriffsziel und dient der (Industrie-)Spionage und Sabotage. Er läuft typischerweise in mehreren Phasen ab und kombiniert unterschiedliche, aufeinander aufbauende Angriffstechniken.

Die Erstinfektion erfolgt oft per Spear Phishing. Ein Mitarbeiter erhält dabei eine Phishing Mail, die entweder bereits einen Anhang mit Schadsoftware enthält oder einen Link auf eine schadenstiftende Web-Seite. Wenn nun der Nutzer den Anhang öffnet oder auf den Link klickt, wird der Schadcode ausgeführt.

Das Ergebnis ist die Infektion des Rechners des Nutzers mit einem Trojaner über den der Angreifer aus der Ferne die Kontrolle über den Rechner erhält. Ein solcher Trojaner heißt dann auch feinsinnig Remote Administration Tool (RAT). Der Angreifer erhält über das RAT damit alle Rechte, die der Nutzer des Rechners auch hat. Ist dies ein Administrator, ist bereits zu Beginn der Schaden hoch.

2. Was fordern Standards?

Im Zusammenhang mit der Administration der IT empfehlen mehrere Standards die Trennung von administrativem und produktivem bzw. funktionalem Datenverkehr.

So wird diese Trennung etwa in ISO/IEC 27033 – Network security – Part 3 in Abschnitt 11 Network Segmentation nahegelegt: „segregate administrative and maintenance capabilities from routine user access to business applications“

Auch die IT-Grundschutz-Kataloge des Bundesamts für Sicherheit in der Informationstechnik (BSI) empfehlen in Baustein 4.1 Lokale Netze in der Maßnahme M 5.77 Bildung von Teilnetzen eine Trennung von administrativem und produktivem Datenverkehr durch eine Grundaufteilung des IT-Netzes in vier Zonen: Internes Netz, Sicherheitsgateway-Zone (ALG-Zone), Internet-Anbindung und Management-Zone. Über die Management-Zone heißt es dort: „In der Management-Zone könnten alle Management-Daten zentral gesammelt und verarbeitet werden. Hier könnte auch ein Zeitserver untergebracht werden, mit dem sämtliche Systemuhren im Netz synchronisiert werden.“

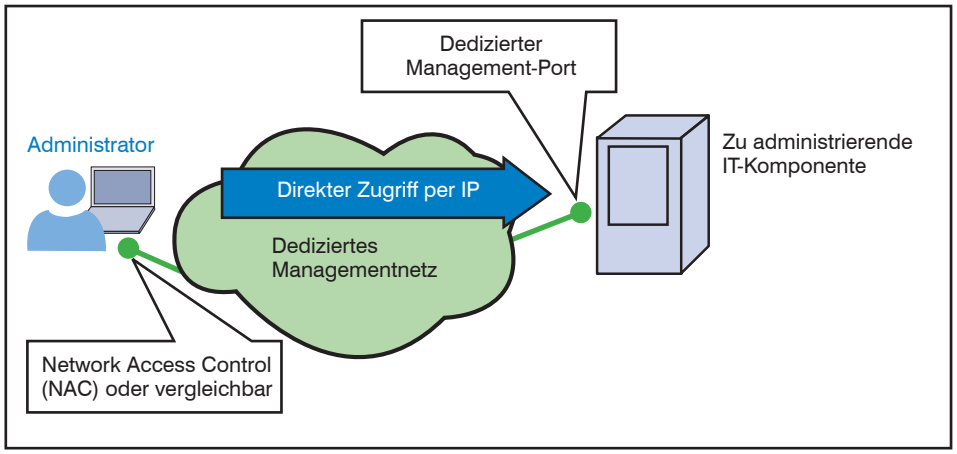


Abbildung 2: Aufbau eines dedizierten Managementnetzes

Dies ist insbesondere für Provider, speziell im Bereich Cloud Computing, relevant. Hier fordert auch der vom BSI im Februar 2016 veröffentlichte „Anforderungskatalog Cloud Computing (C5[3]) - Kriterien zur Beurteilung der Informationssicherheit von Cloud-Diensten“ eine Trennung funktionaler und administrativer Kommunikation: „Es existieren gesonderte Netzwerke zur administrativen Verwaltung der Infrastruktur und für den Betrieb von Managementkonsolen, die logisch oder physisch vom Netzwerk der Cloud-Kunden getrennt und durch Multi-Faktor-Authentifizierung vor unberechtigten Zugriffen geschützt sind“.

Besonders ins Detail geht hier der Baustein NET.1.1 „Netzarchitektur und -design“ des neuen BSI IT-Grundschutz-Kompendiums vom Februar 2018, der in Anforderung A21 ebenfalls eine „Separierung des Management-Bereichs“ spezifiziert: „Es SOLLTE durchgängig ein Out-of-Band-Management genutzt werden, um die Infrastruktur zu managen. Dabei SOLLTEN alle Endgeräte, die für das Management der IT-Infrastruktur benötigt werden, in dedizierten Segmenten positioniert werden. Die Kommunikation mit diesen Endgeräten SOLLTE durch einen zustandsbehafteten Paketfilter (Firewall) kontrolliert werden.“ Hier werden auch Empfehlungen für die weitere Segmentierung der Management-Umgebung in verschiedene Managementzonen gegeben.

3. Welche Sicherheitsaspekte müssen also bei der Administration betrachtet werden?

Um den unter 1. genannten Gefahren entgegen zu wirken und die in 2. aufgeführten Anforderungen in Standards zu erfüllen, sind für eine sichere Administration der IT die folgenden Punkte wesentlich:

- Angemessene Authentisierung für den administrativen Zugriff
- Rollen- und Berechtigungskonzepte für administrative Zugriffe
- Angemessene Trennung von administrativem und produktivem Netzverkehr
- Kontrolle von Managementzugriffen
- Entkopplung von Managementzugriffen
- Monitoring von Managementzugriffen
- Protokollierung der Zugangsdaten und ggf. der kompletten Sitzungen
- Privileged Access Management (PAM) und
- Integration in ein Security Information and Event-Management (SIEM)

Kontrolle von Managementzugriffen

Zunächst ist wichtig sicherzustellen, dass Managementzugriffe auch tatsächlich nur von Administratoren ausgeführt werden, d.h. Managementzugriffe müssen angemessen authentisiert werden und diese Authentisierung sollte nicht erst am zu administrierenden IT-System erfolgen.

Hier werden in der Praxis verschiedene Techniken eingesetzt:

Wenn PCs dediziert Administratoren zugeordnet sind, können diese PCs durch eine Network Access Control (NAC) am Netzzugangspunkt (Switch oder WLAN Controller) identifiziert, authentisiert und dann einem isolierten Managementnetz zugewiesen werden, über das die Management-Ports der zu administrierenden IT-Systeme erreichbar sind (siehe Abbildung 2). Der Administrator kann dann direkt per IP z. B. auf das Command Line Interface (CLI) des IT-Systems zugreifen.

Nun kommt es aber nicht selten vor, dass IT-Systeme entweder keinen dedizierten Management-Port haben oder aus anderen Gründen über das produktive Inter-