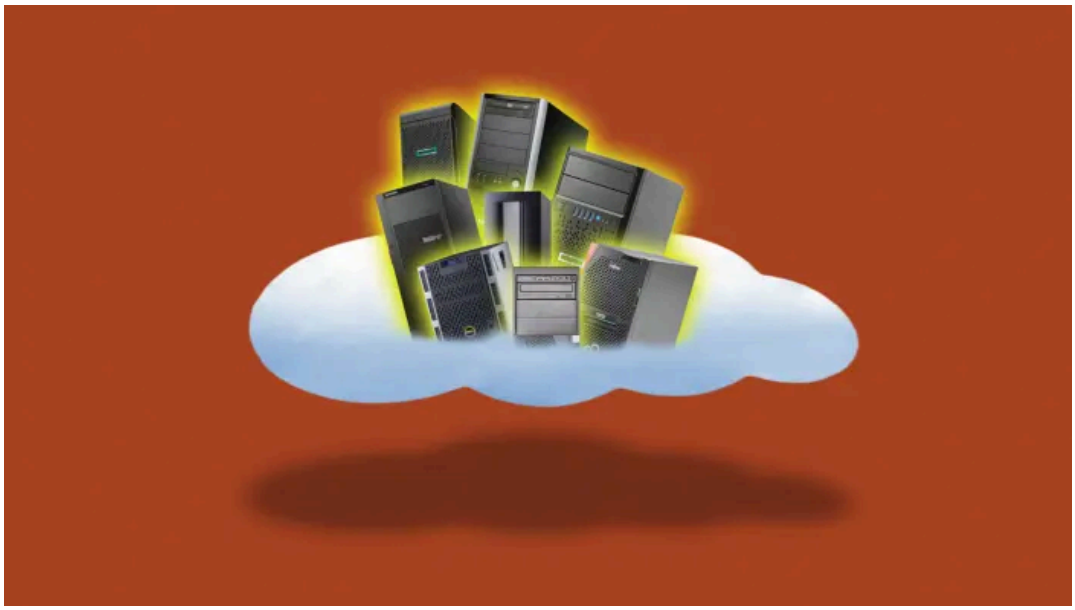
MAGAZIN FÜR PROFESSIONELLE INFORMATIONSTECHNIK

Serverstrukturen in Unternehmen: lokal vorhalten oder in die Cloud verlagern?

12.02.2019 09:55 Uhr Christoph Puppe



Cloud-Dienste sparen Geld und Ressourcen, jedoch ist der Datenschutz bei solchen Systemen brisant. Was spricht für Abteilungs- und was für Cloud-Server?

Für Unternehmen gibt es gute Gründe, ihre Daten auf einem Server in den eigenen vier Wänden zu lagern. Der mangelnde Ausbau der Breitbandanschlüsse oder die Sorge, dass Daten in der Cloud in fremde Hände gelangen können sind nur zwei Beispiele. Was aber ist sicherer – Onlinedienste oder eigene Datenspeicherung?

Von der physischen Gefährdung der Hardware durch Feuer, Wasser und Luft bis hin zu Hackerangriffen über die DSL-Leitung drohen einem Abteilungsserver die gleichen Gefahren wie einem Server bei einem der großen Cloud-Anbieter oder bei einer Firma mit Dutzenden Rechenzentren.

Für kleinere Unternehmen bildet ein solcher Server oft das Nest, in dem sämtliche Eier liegen. Daher ist es gerade für sie überlebenswichtig, die dort lagernden Daten zu schützen und über Notfallpläne zu verfügen, falls dieser Server mal nicht zur Verfügung steht.

MEHR ÜBER SERVER

Mainboard für kleine Server und Workstations mit Intel Xeon E-2100 [15]

HPE-Kleingruppenserver ProLiant ML30 Gen10 [16]

Das planen Server-Hersteller bis 2022 [17]

Server des Open Compute Project von Wiwynn im Test [18]

Berechtigte Sorgen

Viele Unternehmen scheuen noch den Gang in die Cloud – also die Computer nicht mehr selbst zu betreiben, sondern Dienste von Anbietern über das Internet zu nutzen. Die Sorgen sind oftmals berechtigt. Sobald die Daten auf einem Server oder bei einem Dienst in der Cloud liegen, sind sie von überall erreichbar. Jeder Angreifer mit einem Internetanschluss kann versuchen, an sie zu gelangen. Dabei vergisst man gerne, dass so gut wie jeder Computer, den wir üblicherweise nutzen, mit dem Internet verbunden ist.

Wer seine Server selbst betreibt, hat sie im eigenen Netz und kann zumindest versuchen, sie vor Angriffen aus dem Internet zu schützen. Besonders für die hier im Fokus stehenden Abteilungsserver ist dies eine valide Strategie. Immerhin muss ein Angreifer zuerst in das Netzwerk eindringen und kann erst dann den Server angreifen. Dass dies letztlich aber nicht unbedingt eine große Hürde darstellt, sollte jedem klar sein, der die Nachrichten verfolgt. Wenn selbst Großbanken und Bundesbehörden Opfer solcher Angriffe werden, kann dies auch einer kleinen Firma jederzeit passieren.

Sobald der Abteilungsserver auch Dienste über das Internet anbietet, weil etwa ein Dateiaustausch über Nextcloud gewünscht wird oder die Mails auch vom Handy abrufbar sein sollen, sieht das Bedrohungsszenario allerdings komplett anders aus. Jetzt ist der Abteilungsserver genauso aus dem Internet angreifbar wie jeder andere Server in der Cloud.

Der bedeutende Unterschied ist hier, dass die Anbieter von Diensten zumeist erheblich mehr in die Absicherung der Server und Daten investieren als eine kleine oder mittelständische Firma, geschweige denn eine Privatperson. Ganze Abteilungen beschäftigen sich mit der Absicherung und Überwachung der Systeme. Der Überwachung kommt dabei ein besonderes Augenmerk zu, denn niemand kann hundertprozentig verhindern, dass es einen Einbruch gibt. Es zu bemerken, ist die Kunst. Oft bleiben Einbrüche monate- oder gar jahrelang unentdeckt.

[19]

Spezielle Risiken in der Cloud

Zwei Risiken gibt es allerdings bei der Nutzung von **Cloud-Diensten [20]**, die bei einem Abteilungsserver nicht existieren. Das erste ist, durch Zufall zum Opfer zu werden: Ein Einbruch in einen Cloud-Dienst, der eigentlich einem anderen Kunden gilt, kann auch die Daten aller weiteren Kunden exponieren. Auch sind die Cloud-Dienste ein sehr viel lohnenderes Ziel, da hier nicht nur die Daten einer Firma lagern, sondern von vielen gleichzeitig. Der zusätzliche Aufwand für die Absicherung wird also durch die stärkere Motivation der Angreifer teilweise wieder ausgeglichen.

Das zweite Risiko betrifft die Authentifizierung. Wer Cloud-Dienste nutzt, muss sicherstellen, dass nur berechtigte Personen darauf zugreifen können. Schlechte Passwörter können hier sehr viel schneller zu Vorfällen führen als im eigenen Netzwerk. Aber auch hier gilt, dass die Cloud-Anbieter die Anmeldungen besser schützen können als eine kleine Sicherheitsabteilung oder gar eine kleine Firma. Wer hier auf Nummer sicher gehen will, kann auch die Dienste von Firmen nutzen, die sich auf die Verwaltung von Identitäten spezialisiert haben. Diese lassen sich an die meisten Anwendungen anbinden und bieten so eine Verwaltung aller Benutzer in allen Cloud-Plattformen, wie man das vom Active Directory kennt. Selbst die lokalen Anmeldungen lassen sich darüber abwickeln, sodass

alle Benutzer nur bei einer Plattform liegen. Unter dem Schlagwort "Identity as a Service" (IDaaS) findet man diverse Anbieter.

Damit Unternehmen die Vorteile der Cloud-Dienste nutzen können, muss der gewählte Anbieter die Daten auch wirklich schützen. Die Qualität von Anbietern auf Anhieb zu erkennen, ist nicht einfach. Eine Möglichkeit besteht darin, auf Zertifikate zu achten. Für die Cloud gibt es hier mittlerweile eine große Auswahl: **ISO 27001 nativ [21]** oder nach Grundschutz, den **Compliance Controls Catalogue (C5) des BSI [22]** und weitere. Insbesondere sollte ein Anbieter die Zwei-Faktor-Authentifizierung implementieren, um die Risiken bei der Identifikation der Mitarbeiter zu reduzieren.

Fazit

Wer seine IT selbst betreibt, muss auch selbst für die Sicherheit sorgen. Dies ist keine einfache Aufgabe und man sollte sich nicht alleine deswegen in Sicherheit wiegen, weil das Gerät in den eigenen Räumen steht. Denn auch der Abteilungsserver ist Bedrohungen ausgesetzt und benötigt einen ausreichenden Schutz.

WIE MAN ABTEILUNGSSERVER SCHÜTZT

Um den Abteilungsserver gegen die alltäglichen und auch die selteneren Gefahren zu schützen, bietet das BSI mehrere Dokumente zur Unterstützung: zum einen **das Grundschutz-Kompendium [23]**, zum anderen die **BSI-Studie "Notfallmanagement mit der Cloud für KMU" [24]**von 2013. Die Herangehensweise ist hier, sich zuerst vor allen Gefahren zu schützen, die den Server treffen können. Das Grundschutz-Kompendium mag auf den ersten Blick etwas zu viel des Guten sein, aber wer es schrittweise umsetzt, kann sich sicher sein, dass er nichts Wichtiges übersieht.

Zuallererst sollte man darauf achten, dass niemand den Abteilungsserver einfach stehlen kann. Immerhin liegen hier alle Daten, Anwendungen und Geschäftsgeheimnisse, die auch für die Konkurrenz von Interesse sein könnten. Datendiebstahl mag für viele wie ein Krimi klingen, aber das täuscht – in der Realität kommt er sehr häufig vor. Die Bausteine der Schicht **"INF: Infrastruktur" [25]** sind eher für größere Firmen ausgelegt. Aber auch für eine kleine Firma mit nur einer oder wenigen Niederlassungen finden sich im Baustein **"INF.1 Allgemeines Gebäude" [26]** gute Hinweise, worauf zu achten ist. Ausreichender Schutz vor unbefugtem Betreten der Räumlichkeiten etwa ist nicht nur für den Abteilungsserver empfehlenswert.

Die Büros sind mit dem Internet verbunden, entweder über einen Festanschluss oder über die Telefone der Mitarbeiter. Für einen Angreifer gibt es also viele Wege in das lokale Netz. Mindestens eine UTM-Appliance (Unified Threat Management) sollte Gefährdungen reduzieren, die aus der Nutzung des Internets resultieren: Dazu gehört Malware auszufiltern, den Zugang zu gefährlichen Webseiten zu blockieren und direkte Angriffe zu verhindern. Die Anforderungen des Bausteins **"NET.3.2 Firewall" [27]** sind hier eine gute Unterstützung. Wer selbst kein Personal für die Konfiguration der Firewall hat, kann Cloud-basierte Dienste oder einen Dienstleister einbinden. Viele erfolgreiche Angriffe finden auch über schlecht gesicherte WLANs statt. Auf eine gute Verschlüsselung ist mindestens zu achten, darüber hinaus helfen die weiteren Anforderungen des Bausteins **"NET.2.1 WLAN-Betrieb" [28]**.

Die Server sollten gehärtet sein, also gegen unbefugte Benutzung abgesichert. Die Bausteine **"SYS.1.1 Allgemeiner Server" [29]** und **"SYS.1.3 Server unter Unix" [30]** respektive **"SYS.1.2.2 Windows Server 2012" [31]** sind ein guter Ausgangspunkt. Hier finden sich Basismaßnahmen wie eine restriktive Rechtevergabe, Schutz der Administrationsschnittstellen oder auch Deaktivierung nicht benötigter Dienste und Kennungen.

Viele erfolgreiche Angriffe erfolgen auch über die PCs der Mitarbeiter. Hier helfen die Bausteine **"SYS.2.1 Allgemeiner Client" [32]** und **"SYS.2.2.3 Clients unter Windows 10" [33]** sowie **"SYS.3.1 Laptops" [34]**. Benutzerauthentifizierung, Rollentrennung sowie Autoupdate-Mechanismen und regelmäßige Datensicherungen sind nur ein paar der Mindestanforderungen. Ist der Abteilungsserver virtualisiert, wendet man den Baustein **"SYS.1.5 Virtualisierung" [35]** an. Beispiele für Schutzmaßnahmen sind hier das Einschränken sämtlicher Administrations- und Managementzugänge zum Managementsystem und den Hostsystemen oder das Protokollieren der virtuellen Infrastruktur.

Die Grundlage für die Absicherung der Server, der Firewall, der Clients und des WLAN ist immer der Betrieb aktueller Software. Das Einspielen von Updates ist die oberste Pflicht und dies betrifft alle Komponenten, seien sie noch so klein. Das fängt bei den Handys der Mitarbeiter an und setzt sich bis zu sämtlichen Servern des Betriebs fort. Hilfreich sind hier die Kapitel **"OPS.1.1.4 Schutz vor Schadprogrammen" [36]** und **"OPS.1.1.3 Patch- und Änderungsmanagement" [37]**.

Für kleine Betriebe bedeutet das Erkennen von Vorfällen eine besondere Herausforderung. Nicht umsonst ist das die Königsdisziplin der IT-Sicherheit, vor der selbst große Firmen oft kapitulieren. Auch wer nur einen Server hat, sollte mindestens die Protokolldaten sammeln, um im Fall der Fälle den Vorfall aufklären zu können. Der Baustein **"OPS.1.1.5 Protokollierung" [38]** gibt hier gute Hinweise.

Auch wenn der Abteilungsserver aus anderen Gründen nicht mehr verfügbar ist, weil zum Beispiel das Gebäude unter Wasser steht oder die Feuerwehr zu spät da war, muss die Arbeit weitergehen. Ohne Datensicherung, beschrieben im Baustein **"CON.3 Datensicherungskonzept" [39]**, kann dies nicht gelingen. Die einfachste Option ist die Wechselplatte, die mindestens wöchentlich mit allen überlebenswichtigen Daten in ein Schließfach wandert. Wer hier etwas mehr Sicherheit haben möchte, kann die Hinweise der BSI-Studie beachten. Eine der Empfehlungen lautet, die Daten in die Cloud auszulagern und dort Kopien auch der Server vorzuhalten. So kann ein Unternehmen bei einem Verlust aller Daten, des Servers und vielleicht sogar des Büros weiterarbeiten.

Beispielhafte Entscheidungskriterien für oder gegen die Cloud

Kriterium	nein	ja
Ist ein geschützter Serverraum vorhanden?	☐	☐
Sind ausreichend (personelle, finanzielle) Ressourcen für den eigenen Betrieb vorhanden?	☐	☐
Werden Dienste (z. B. E-Mail, Webseiten, Anwendungen, Filesharing) über das Internet angeboten?	☐	☐
Hat das Büro einen Breitbandanschluss?	☐	☐
Sind weitere Dienste aus der Cloud im Einsatz?	☐	☐
Sind große Datenmengen zu verarbeiten?	☐	☐

Wer mehr „nein" angekreuzt hat, sollte erwägen, in die Cloud zu gehen, wer mehr „ja" hat, erfüllt die Basisvoraussetzungen für den Betrieb eines Abteilungsservers. Die Kriterien sind nur beispielhaft und nicht vollständig, sie lassen sich um weitere individuelle Argumente ergänzen.

Die letzte Entscheidung für oder gegen Abteilungsserver oder Cloud liegt bei der Geschäftsführung, die alle Vor- und Nachteile sorgsam abwägen sollte. Hilfreich kann dabei eine Checkliste wie die oben gezeigte sein, die man mit eigenen Entscheidungskriterien ergänzen kann.

Christoph Puppe ist Security Consultant bei SVA, Audit-Teamleiter, IS-Revisor, Mitautor der Grundschutzkataloge und ehemaliger Penetrationstester. (**ur** [40])

URL dieses Artikels:

https://www.heise.de/-4275598

Links in diesem Artikel:

[1] https://www.heise.de/hintergrund/ARM-Server-aus-der-Cloud-im-Vergleich-6302049.html

[2] https://www.heise.de/hintergrund/ARM-Revolution-im-Rechenzentrum-Wie-es-ARM-Prozessoren-in-Server-schafften-6291991.html

[3] https://www.heise.de/ratgeber/Rechenzentrums-Hardware-ARM-Server-im-Ueberblick-6291422.html

[4] https://www.heise.de/tests/ARM-Server-fuers-Rechenzentrum-im-Test-Gigabyte-R152-P30-mit-80-ARM-Kernen-6291283.html

[5] https://www.heise.de/ratgeber/Weg-in-die-Cloud-Cloudserver-automatisiert-bestellen-und-einrichten-6204188.html

[6] https://www.heise.de/tests/Weg-in-die-Cloud-Sechs-europaeische-Cloud-Provider-im-Vergleich-6203884.html

[7] https://www.heise.de/ratgeber/Serverinfrastruktur-flexibel-mieten-in-der-Cloud-6203676.html

[8] https://www.heise.de/ratgeber/Eigenen-Server-selbst-bauen-Starthilfe-fuer-Betrieb-und-Ausstattung-6179529.html

[9] https://www.heise.de/tests/AMDs-zweite-Epyc-Generation-mit-64-Kernen-uebertrumpft-Intels-Xeon-4495501.html

[10] https://www.heise.de/tests/Vom-maechtigen-NAS-bis-zur-Abteilungszentrale-Xeon-Server-fuer-kleine-Netze-4350988.html

[11] https://www.heise.de/tests/Tower-und-NAS-Systeme-fuer-Abteilungen-4274836.html

[12] https://www.heise.de/hintergrund/Serverstrukturen-in-Unternehmen-lokal-vorhalten-oder-in-die-Cloud-verlagern-4275598.html

[13] https://www.heise.de/ratgeber/Mini-PCs-fuer-energiesparenden-Dauerbetrieb-konfigurieren-4296996.html

[14] https://www.heise.de/tests/Rack-Server-Lenovo-ThinkSystem-SR850-mit-Intel-Xeon-CPUs-4288221.html

[15] https://www.heise.de/tests/Mainboard-fuer-kleine-Server-und-Workstations-mit-Intel-Xeon-E-2100-4247575.html

[16] https://www.heise.de/tests/HPE-ProLiant-ML30-Gen10-Kleingruppen-Server-mit-ueberzeugenden-Transferraten-4451616.html

[17] https://www.heise.de/hintergrund/Power-Effizienz-Speicher-Geplante-Neuerungen-der-Server-Hersteller-bis-2022-4553549.html

[18] https://www.heise.de/tests/Wiwynn-SV7220G3-Server-des-Open-Compute-Project-im-Test-4662387.html

[19] https://www.heise.de/ix/

[20] https://www.heise.de/thema/Cloud_Dienste

[21] https://www.heise.de/ratgeber/Aktualisierter-ISO-IEC-27000-beschreibt-ISMS-Verantwortlichen-4219716.html

[22] https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Anforderungskatalog/Anforderungskatalog_node.html

[23] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html

[24] https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Publikationen/BCM/bcm_node.html

[25] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/INF/INF_Uebersicht_node.html;jsessionid=9

[26] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/INF/INF_1_Allgemeines_Geb%C3%A4ude.html

[27] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/NET/NET_3_2_Firewall.html

[28] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/NET/NET_2_1_WLAN-Betrieb.html

[29] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_1_1_Allgemeiner_Server.html

[30] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_1_3_Server_unter_Unix.html

[31] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_1_2_2_Windows_Server_2012.html

[32] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_2_1_Allgemeiner_Client.html

[33] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_2_2_3_Clients_unter_Windows_10.ht

[34] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_3_1_Laptops.html

[35] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_1_5_Virtualisierung.html

[36] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_1_1_4_Schutz_vor_Schadprogrammen.

[37] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_1_1_3_Patch-_und_%C3%84nderungsmanagement.html

[38] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_1_1_5_Protokollierung.html

[39] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_3_Datensicherungskonzept.html

[40] mailto:ur@ix.de