
# Glauben statt wissen

**Lukas Grunwald**

Wer bei T-Systems eine Azure-Instanz mietet, dem wird versprochen, dass seine Daten Deutschland nicht verlassen und keine unbefugte Datenweitergabe stattfindet. Doch die Realität sieht anders aus.

Wenn Unternehmen die von T-Systems betriebene Azure-Instanz in Deutschland benutzen, fungiert die Deutsche Telekom als „Datentreuhänder“, die „Kundendaten werden ausschließlich in Deutschland vorgehalten und der Zugriff darauf unterliegt den strengen deutschen Datenschutzgesetzen“ – so das Versprechen auf der Website (siehe ix.de/ix1809082).

Dieses im zweiten Halbjahr 2016 gestartete Angebot umfasst Azure, Office 365 und Dynamics CRM Online. Microsoft Deutschland bietet das aus zwei deutschen Rechenzentren heraus an, mit der Deutschen Telekom als Treuhänder. Zahlreiche Papiere und Zertifikate sollen diese Behauptung untermauern. So gibt es eigens eine Abteilung „Compliance“ im sogenannten Microsoft Trust Center, in dem alle relevanten ISO-Normen von ISO 27001 über ISO 27017 und ISO 27018 bis zum BSI-Grundschutz aufgeführt sind. Auf den ersten Blick recht beeindruckend.

Mit dem Inkrafttreten der EU-DSGVO Ende Mai 2018 ist der Datenschutz natürlich noch stärker in den Fokus gerückt, und das Angebot von Microsoft und der Telekom dürfte auf verstärktes Kundeninteresse stoßen. Das Schöne dabei: Mit dem Azure Network Watcher stellt Microsoft dem Kunden ein Werkzeug zur Verfügung, mit dem er selbst überprüfen können soll, ob seine Daten nicht auf Abwege geraten.

## Kontrolle per Netzwerksniffer

*iX* hat auf zwei Instanzen der deutschen Azure-Cloud diese Versprechen überprüft. Installiert wurden Windows 2016 Server und Ubuntu Linux.

Zur Untersuchung des Datenverkehrs kamen neben dem Azure Network Watcher – dazu später – eigene Tools zum Einsatz. Auf Windows Server 2016 wurde der aktuelle 64-Bit-Wireshark- nebst WinPCAP-Treiber installiert. Falls das jemand nachvollziehen möchte: Das funktioniert nicht über Azures Web-Dashboard. Man muss sich bei der ersten Installation als Administrator via RDP einloggen und auch den Wireshark per RDP zum Server transportieren.

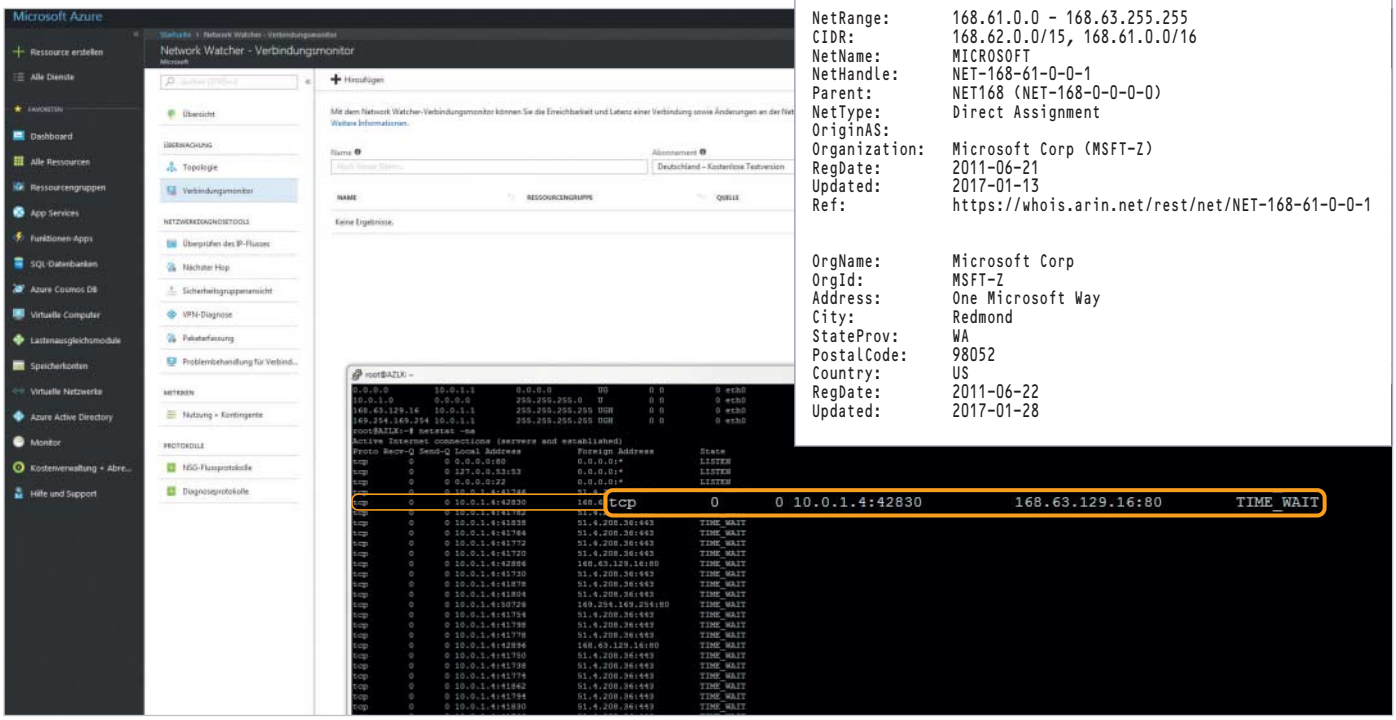
Noch schwieriger war der Root-Login unter Linux. Das Azure-Dashboard akzeptiert keinen ED25519-Schlüssel als SSH-Key. Darum mussten wir temporär einen Benutzer mit Usernamen und Passwort anlegen und uns als dieser durch *sudo bash* zum Root-Account vorarbeiten. Anschließend ließ sich die Authorized-Key-Datei auf dem virtuellen Computer in der Cloud installieren.

Auf dem Linux-System wurden *strace*, *tcpdump* und *ngrep* installiert, was einen tiefen Einblick in das virtuelle Netzwerkinterface erlaubte. Zuvor hatten wir den Root-Account mit einem ED25519-SSH-Key remote zugänglich gemacht.

Die genannten Tools ermöglichen das Ausfiltern von Quell- und Zieladresse gesendeter Pakete. Schon nach wenigen Minuten fiel eine Kommunikation mit einer öffentlichen IP-Adresse auf, die nie für einen Datenverkehr autorisiert worden war. Und zwar zur IP-Adresse 168.63.129.16, die zum 168.63.0.0/15-Netz gehört.

## USA, Hongkong, EU?

Dieses Netz wird laut Whois-Abfrage in den USA reguliert: Den gesamten Bereich von 168.61.0.0 bis 168.63.255.255 hat die American Registry for Internet Numbers (ARIN) an Microsoft vergeben.




**Whois-Ausgabe, gekürzt**

```
# whois 168.63.129.16

NetRange:       168.61.0.0 - 168.63.255.255
CIDR:           168.62.0.0/15, 168.61.0.0/16
NetName:        MICROSOFT
NetHandle:      NET-168-61-0-0-1
Parent:         NET168 (NET-168-0-0-0-0)
NetType:        Direct Assignment
OriginAS:
Organization:   Microsoft Corp (MSFT-Z)
RegDate:        2011-06-21
Updated:        2017-01-13
Ref:            https://whois.arin.net/rest/net/NET-168-61-0-0-1


OrgName:        Microsoft Corp
OrgId:          MSFT-Z
Address:        One Microsoft Way
City:           Redmond
StateProv:      WA
PostalCode:     98052
Country:        US
RegDate:        2011-06-22
Updated:        2017-01-28
```

**Was das GUI des Azure Network Watcher nicht zeigt, bringt Netstat an den Tag: Datenübermittlung an die US-Adresse 168.63.129.16.**

Das wird auf dem Blog des Microsoft Azure Support Teams unter der Überschrift „What is the IP address 168.63.129.16?“ folgendermaßen erklärt: 168.63.129.16 sei eine virtuelle öffentliche IP-Adresse, die weltweit einheitlich sei und als Kommunikationskanal mit internen Ressourcen genutzt werde. Es dürfe keine private Adresse sein, da dies zu Kollisionen mit den von Kunden vergebenen privaten Adressen in deren Azure-Installationen führen könne (siehe auch ix.de/ix1809082).

Nun müssen nicht unbedingt alle Rechner in den besagten Netzen in den USA stehen – obwohl die Regulierungsvorschriften der ARIN dies eigentlich vorsehen. Aber auch ein Konzern wie Microsoft muss sich nicht unbedingt an die ARIN-Regularien halten. Dass die Adresse 168.63.129.16 von Geolokationsdiensten wie Ip2location in Hongkong verortet wird, verbuchen wir als Gag am Rande – die Ergebnisse dieser Dienste sind nicht sehr valide.

Microsoft betonte ergänzend zum Blog-Eintrag, dass zwar die virtuelle IP weltweit gleich sei, aber „das Ziel des Routings in Abhängigkeit der Rechenzentrumsregion unterschiedlich sein kann. Es ist also nicht so, dass es nur einen Endpunkt für diese IP-Adresse innerhalb der weltweiten Infrastruktur gibt, sondern es gibt in der Regel je nach Rechenzentrumsregion einen eigenen Endpunkt.“ Das ist auch technisch plausibel, allerdings muss der Kunde das glauben - selbst nachprüfen kann er es nicht.

Wichtiger aber: Spätestens seit dem jüngst verabschiedeten CLOUD Act dürfen US-Behörden auch auf die Server amerikanischer Firmen zugreifen, die im Ausland stehen. Dazu dürften solche mit IP-Adressen, die Microsoft USA gehören, zweifellos zählen.

Sowohl bei der Windows- als auch bei der Linux-Instanz handelte es sich bei den übermittelten IP-Paketen um Telemetriedaten. Das wird aber im Blogeintrag nicht explizit erwähnt. Langer Rede kurzer Sinn: Es ist keineswegs so, dass die Azure-Instanzen datenschutzrelevante Daten im Geltungsbereich deutscher Datenschutzgesetze halten. Obendrein werden die Linux-Telemetriedaten von der Azure-Instanz unverschlüsselt über Port 80 verschickt, sodass sie mittels NGREP auf der Leitung einsehbar sind.

## Überblick ohne Einblick

Eigentlich ist es natürlich ein löbliches Unterfangen, dem Kunden ein Werkzeug zur Überwachung des Datenverkehrs an die Hand zu geben. Doch beim Einrichten des Azure Network Watcher schlug plötzlich die Browsererweiterung Ghostery (ein Anti-Tracking-Modul) Alarm: Die Azure-Komponente, die im Webbrowser läuft, sendet selbst Telemetriedaten an Microsoft. In diesem Fall zwar nur an die deutsche Dependance, aber auch das ist, da nicht durch den Anwender autorisiert, nicht datenschutzkonform.

Hinzu kommt, dass das Einrichten des – kostenpflichtigen – Network Watcher sehr umständlich ist und dass die Diagnosefunktionen es nicht ermöglichen, sich aktuelle Netzwerkverbindungen anzeigen zu lassen. Während die PCAP-Daten geschrieben werden, kann man sich diese nicht anschauen.

Zur Auswertung der Daten muss man das Packet-Capture stoppen, erst dann kann man sie sich mit Tools wie Wireshark ansehen. Immerhin könnte man dann auch feststellen, dass es eine Kommunikation mit US-Adressen gibt – die grafische Aufbereitung der Daten verrät das dem Kunden nicht.

Fazit: Auch unter der Obhut des „Treuhänders“ T-System sind die Daten der Azure-Instanzen nicht nachprüfbar sicher, nicht einmal vor US-Zugriff. Warum dieser Dienst trotzdem mit etlichen Zertifizierungen aufwarten kann, wissen wohl nur die Zertifizierer selbst. Tatsächlich die Systeme untersucht hat da offenbar niemand. (js@ix.de)

**Lukas Grunwald**

ist Consultant bei der DN-Systems GmbH in Hildesheim.

Alle Links: ix.de/ix1809082