Schweizerische
Fachschule
TEKO

DIPL. TECHNIKER HF INFORMATIK FACHRICHTUNG SYSTEMTECHNIK

Automatisierung Microsoft Cloud IP und URL Adressen

"Cloud is about how you do computing, not where you do computing."
Paul Maritz, CEO of VMware.

Hintergrund

Ralf Thomet
Microsoft Cloud Engineer @ Post CH AG

E-Mail
ralf.t@hotmail.com

Telefon
078 885 87 80

Social
XING

Die Schweizerische Post setzt seit ein paar Jahren auf die Microsoft Cloud Services Azure und Office 365 in einem Hybrid Modus. Da ein Post Client keinen direkten Zugang ins Internet hat, wird der Traffic via Proxy und Firewall ins Internet geroutet. Ausnahme dabei bilden die beiden Services Azure und O365, die direkt ins Internet geroutet werden. Um diese Ausnahmen umsetzen zu können, wird der Traffic via einem Proxy File und den speziell dafür geöffneten Firewall Rules ermöglicht.

Aus Regulatorischen- und Sicherheitsbedingten Vorgaben, dürfen nicht alle Regionen und Services von Microsoft freigeschalten werden, weshalb die IP- und URL-Listen jeweils erst aufgearbeitet werden müssen, bevor sie freigeschalten werden dürfen. Das aufbereiten der Adressen wurde bisher manuell und sehr aufwändig verschiedenen Listen umgesetzt. Dies verursachte einen extremen Aufwand von ca. 4h pro Monat und war ausserdem sehr Fehleranfällig. Da die Periodizität an neuen Adressen von Microsoft auf ein Update pro Woche verkürzt wurde, verursacht dies einen erheblichen Mehraufwand von ca. 2 Arbeitstagen pro Monat.

Ziele und Rahmenbedingung

Es muss unbedingt eine Lösung geschaffen werden, um den Aufwand, als auch die Fehleranfälligkeit auf ein Minimum zu reduzieren. Durch diese Diplomarbeit soll eine Lösung erarbeitet werden, mit der die IP- und URL-Adressen automatisiert heruntergeladen, gefiltert und aufgearbeitet werden können. Diese Listen sollen dann an einem zentralen Ort gespeichert und verwaltet werden können.

Umsetzung

Die neue Lösung besteht aus drei Komponenten. Den Sharepoint Listen, ein Master Script und PowerAutomate (Flow). In den Sharepoint Listen werden die aktuellen Adressen gespeichert, die dann vom Firewall- und dem Proxy-Team bezogen werden können. Mit dem Master Script werden die Adressen aufbereitet und in die Listen geschrieben und mit PowerAutomate (Flow) wird der Business Prozess darüber umgesetzt. So werden die Teams informiert, wenn es neue Adressen zu bewilligen oder implementieren gibt.

Mittelbedarf

Für das Projekt musste keine Soft- oder Hardware speziell beschaffen werden. Die notwendigen Mittel waren bereits alle vorhanden. Insbesondere die Lizenzen über das Enterprise Agreement zwischen der Post und Microsoft waren wichtig. Ausser den Lohnkosten für den Projektmitarbeiter, entstanden keine zusätzlichen Kosten.

Zukünftige Vorhaben

Aktuell läuft auch das Projekt Windows Virtual Desktop auf Azure. Dabei muss der Internet-Traffic der Clients dort sehr ähnlich wie in diesem Projekt geroutet werden. Aufgrund der starken Ähnlichkeit, haben wir bereits eine Anfrage auf Weiterentwicklung zur Version 2 erhalten.

Fazit

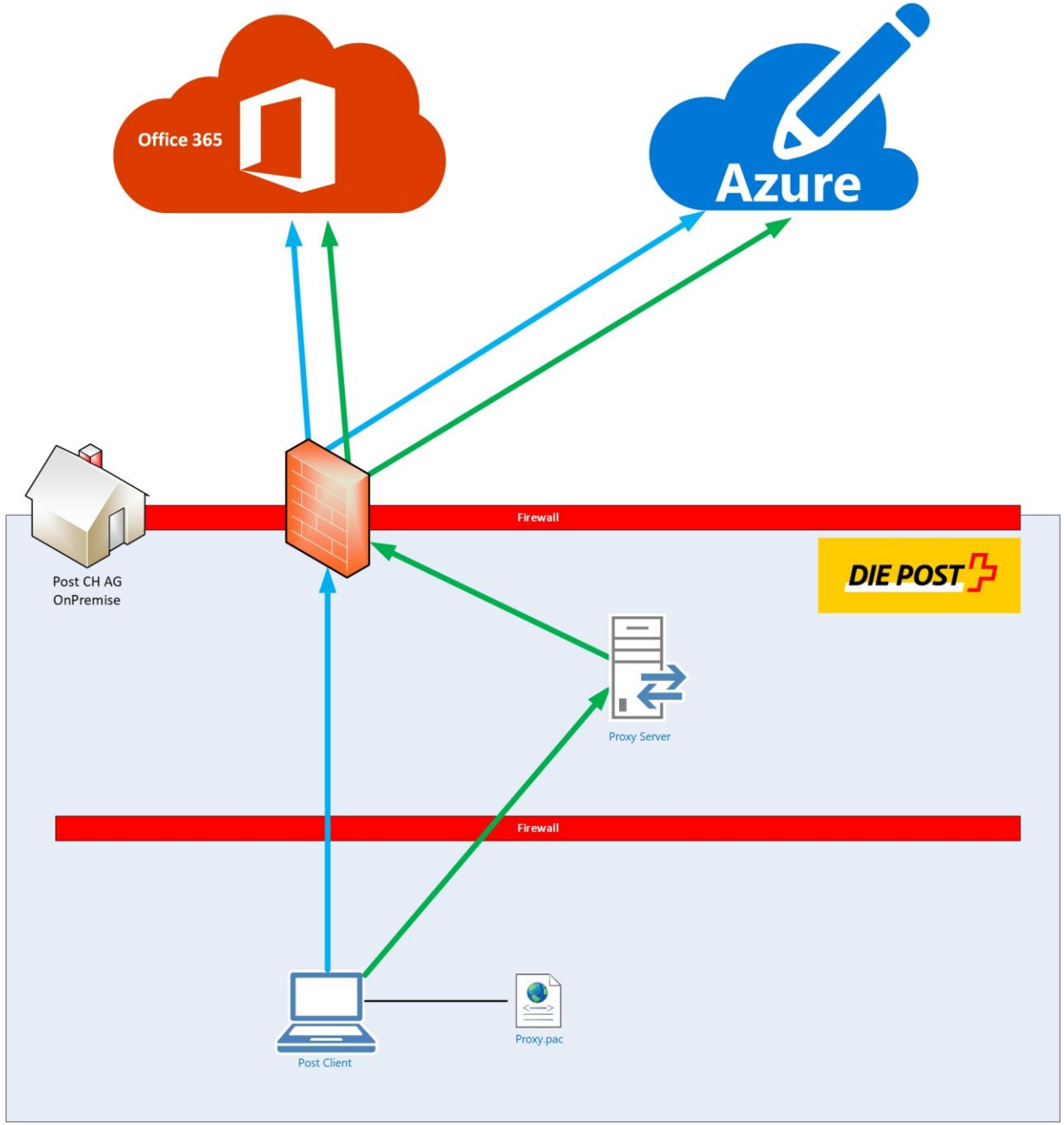
Das Projekt war eine sehr aufschlussreiche und interessante Zeit. Mit dieser Lösung wird der Post eine grosse Bürde abgenommen. Bisher wurde pro Update ca. 4h benötigt, was mit der neuen Periodizität von Microsoft auf ca. 16h pro Monat ansteigen wird. Durch diese Automatisierung wird der Aufwand für das Microsoft Application Engineering Team auf nahezu Null gesenkt. Wird Microsoft noch schneller neue Adressen veröffentlichen, ist dies ab sofort kein Problem mehr. Es muss lediglich die Ausführungszeit der Lösung angepasst werden. Einziger kleiner Aufwand denn wir nun mehr haben ist, dass neue Adressen in die Ausnahmeliste oder zu den Standardadressen hinzugefügt werden müssen. Ansonsten läuft diese Lösung komplett Eigenständig. Ein weiterer Vorteil ist, dass nun sehr leicht die aufbereiteten Daten für andere Projekte weiterverwendet werden können.

Schweizerische
Fachschule
TEKO

Cloud Client Connection

Grün – Normaler Internet Traffic
Blau – O365 und Azure Traffic

Schritt 1 – Client versucht eine Website / Service zu öffnen
Schritt 2 – Das Proxy.pac auf dem Client gibt an, welche Route zu wählen ist
Schritt 3 – Client nimmt die vorgegebene Route zum Zielservice



Schweizerische
Fachschule
TEKO

Zielarchitektur