indevis
Sicherheit in einer vernetzten Welt

CASE STUDY

indevis Firewall

MEDIZINTECHNIK-UNTERNEHMEN STARTET MIT INDEVIS EINE SICHERE CLOUD-FIRST-STRATEGIE

Wir wollen unsere Rechenzentren zu Microsoft Azure migrieren: Das beschloss ein deutsches Medizintechnik-Unternehmen mit mehreren Tochtergesellschaften und zirka 700 Mitarbeitern. Aber wie bindet man die Cloud am besten sicher an? Reichen die Bordmittel von Azure oder ist eine andere Firewall-Lösung besser geeignet? indevis entwickelte und realisierte ein passgenaues Security-Konzept, welches das Unternehmen optimal bei seiner Cloud-First-Strategie unterstützt.

Die Verfügbarkeit seiner Rechenzentren hat für das Medizintechnik-Unternehmen aus Süddeutschland oberste Priorität. Hier laufen wichtige Applikationen und Services, ohne die die Entwicklung und das Tagesgeschäft stillstehen. Da das Unternehmen in den vergangenen Jahren mehrfach von Hochwasser betroffen war, entschied die Geschäftsleitung, die Rechenzentren in die Cloud zu verschieben. In den nächsten drei bis fünf Jahren sollte die IT-Abteilung sukzessive die On-Premises-Systeme abbauen und zu Azure migrieren. Dabei war es wichtig, von Anfang an für angemessene Security zu sorgen. Aber wie?

Da die IT-Abteilung indevis bereits aus einem Datacenter-Projekt kannte, wandte sie sich an den bewährten Partner. Die indevis-Consultants konnten nicht nur mit Erfahrung in Cloud-Infrastrukturen punkten. Sie überzeugten auch, weil sie in der Lage waren, passgenau auf die technischen und geschäftlichen Anforderungen des Unternehmens einzugehen. Jakob Niederbacher, Team Manager Consulting bei indevis, erklärt: „Es ist extrem wichtig, den Fokus am Anfang nicht zu eng zu setzen, sondern sich erst einmal die Business- und Cloud-Strategie des Kunden genau anzusehen. So kann man eine Lösung finden, die stimmig ist und die Kundenprozesse bestmöglich unterstützt. Unser Ziel ist es, unseren Kunden sichere Innovation zu ermöglichen."

DIE ANFORDERUNGEN: EINFACHES MANAGEMENT, SKALIERBARKEIT UND FLEXIBLE ABRECHNUNG

indevis analysierte zunächst das Grobkonzept des Kunden für das Cloud-Design in Azure und ermittelte die Security-Anforderungen für die Anbindung. Zunächst sollten On-Premises-Applikationen per Lift-and-Shift-Ansatz in die Cloud migriert werden. Außerdem wollte man perspektivisch von selbstbetriebenen SQL-Services auf MS SQL in Azure wechseln. Das Medizintechnik-Unternehmen wünschte sich eine Security-Lösung, die einfach zu managen ist und flexibel skaliert, sodass sie mit der zunehmenden Cloud-Nutzung mitwächst. Außerdem war eine Abrechnung nach Verbrauch gefragt: OPEX statt CAPEX.

On-Premises setzt das Medizintechnik-Unternehmen Firewall-Technologie von Fortinet ein. Microsoft bietet in der Azure Cloud aber auch eine integrierte Azure Firewall. Grundsätzlich stellte sich die Frage, ob diese für das Unternehmen geeignet ist oder ob auch in der Cloud eine Fortinet-Lösung besser wäre. Dabei sollten vier Use Cases betrachtet werden: die Absicherung der Verbindung von On-Premises zur Azure Landing Zone, die Absicherungen von PaaS- und IaaS-Ressourcen, die sichere Verbindung des Remote Access Service Gateways zu Azure Ressourcen und die Absicherung von User Traffic über einen Terminal Server in der Cloud.

VOM PROOF OF CONCEPT ZUR UMSETZUNG

Um die Funktionalität und Bedienbarkeit der beiden Lösungen gegenüberzustellen, baute indevis parallel zur Azure Firewall eine FortiGate VM02 Active/Passive HA mit Azure Loadbalancer Deployments auf und implementierte die Test-Cases.

ECKDATEN

- Kunde: Entwickler von Medizintechnik
- Branche: Gesundheit
- Standort: Deutschland

PROJEKT & VORTEILE

- Einheitliches Management des gesamten Firewall-Ökosystems – sowohl der bestehenden On-Premises-Systeme in der Zentrale und den Zweigstellen als auch der in der Azure Cloud
- Kontrolle und Sichtbarkeit des gesamten Datenverkehrs via Analysefunktionalitäten
- Maximale Flexibilität bei der Lizensierung dank monatlicher Abrechnung

indevis
Sicherheit in einer vernetzten Welt

indevis Firewall

„Es ist extrem wichtig, den Fokus am Anfang nicht zu eng zu setzen, sondern sich erst einmal die Business- und Cloud-Strategie des Kunden genau anzusehen. So kann man eine Lösung finden, die stimmig ist und die Kundenprozesse bestmöglich unterstützt. Unser Ziel ist es, unseren Kunden sichere Innovation zu ermöglichen.“

Jakob Niederbacher
Team Manager Consulting bei indevis

Jakob Niederbacher erzählt: „Es hat sich schnell gezeigt, dass die IT-Abteilung mit der Azure Firewall schlechter zurechtkam, weil sie hier keine Betriebserfahrung hatte. Trouble Shooting, Logging und die Steuerung der Next Generation-Features funktionieren in der Cloud anders als On-Premises.“ Die FortiGate VM02 konnten die Administratoren dagegen wie gewohnt bedienen. Da diese Lösung zudem mit einem attraktiven, flexiblen Abrechnungsmodell aufwarten konnte, stand die Entscheidung fest.

Nach erfolgreich abgeschlossenem Proof of Concept setzte indevis das Projekt um und band die entsprechenden Ressourcen an die Firewall-Infrastruktur an. Weil das automatisierte Standard-Deployment der FortiGate VM02 eigentlich eine größere virtuelle Maschine voraussetzte, passten die Consultants dies manuell an die Kundenanforderungen an. Darüber hinaus führte indevis auch einen Security-Review der bestehenden Umgebung durch. Die Consultants prüften die Konfiguration auf Best Practices, nahmen Änderungen vor und brachten die Systeme auf den aktuellen Stand. Anschließend machten Sie die IT-Abteilung fit, um den ersten Schritt in die Cloud zu wagen.

HOMOGENE SECURITY, SICHERE INNOVATIONEN, FLEXIBLE ABRECHNUNG

Das Medizintechnik-Unternehmen kann jetzt die gewohnten On-Premises-Features der FortiGate auch in der Cloud nutzen und sein gesamtes Firewall-Ökosystem einheitlich über den FortiManager administrieren – sowohl die bestehenden On-Premises-Systeme in der Zentrale und den Zweigstellen als auch die in der Azure Cloud. Das vereinfacht das Management erheblich im Vergleich zu einer separaten Cloud-Security-Lösung. Über die Analysefunktionalität des FortiAnalyzers gewinnt die IT-Abteilung zudem Sichtbarkeit über den gesamten Datenverkehr. Alles, was in die Cloud hinein- und aus der Cloud herausfließt, wird kontrolliert. Das Unternehmen kann jetzt Applikationen für die Produktentwicklung und das Tagesgeschäft sicher in der Cloud betreiben, sicher auf virtuellen Desktops in der Cloud arbeiten und sicheren Remote Access nutzen.

indevis stellt die Firewall über einen Partnervertrag mit Fortinet als Managed Service im OPEX-Modell bereit und leistet technischen Support. Abgerechnet wird monatlich nach Nutzung. Dadurch profitiert das Medizintechnik-Unternehmen von maximaler Flexibilität bei der Lizensierung. Es kann zunächst mit einer kleinen Firewall-Instanz starten und später aufstocken, je mehr Applikationen und Services es in die Cloud migriert. Die Betriebsverantwortung bleibt vorerst im eigenen Haus. Jakob Niederbacher fasst zusammen: „Der Kunde hat jetzt eine homogene Security-Lösung für seine gesamte IT-Umgebung, die er einfach managen kann. Sollte er später einmal Bedarf haben, kann er die Betriebsverantwortung jederzeit an uns übergeben. Er ist jetzt in der Lage, die Cloud sicher zu nutzen und seine Firewall genauso flexibel zu skalieren und abzurechnen wie seine Azure-Umgebung. Damit ist die Basis für eine sichere Cloud-First-Strategie gelegt.“

Über FortiGate-VM sowie indevis und das neue Fortinet Flex-VM Programm

Die FortiGate-VM überwacht als virtuelle Firewall den gesamten Datenverkehr eines Unternehmens auf führenden Virtualisierungs-, Cloud- und SDN-Plattformen wie AWS, Azure, VMware vSphere oder Hyper-V. Physische Appliances sind nicht notwendig, sodass sich Firewalls einfach und schnell auch global ausrollen lassen. Dank der neuen Pay-per-Use-Lizenzierungsmöglichkeiten gewinnen Kunden zudem eine bisher nicht gekannte Flexibilität: Sie können die benötige Anzahl und erforderlichen Kapazitäten der VMs und der zugehörigen Dienste bedarfsgerecht und sogar tagesaktuell anpassen. Monatliche Abrechnungen anstelle einer Einmalabrechnung sorgen durch vorhersehbare Kosten für Planungssicherheit. Die verkürzten Abrechnungszeiträume vereinfachen außerdem die Anpassung der virtuellen Firewalls an die Cloud-Infrastruktur des Unternehmens. Nutzen können Kunden ihre virtuellen Firewalls in jeder Private oder Public Cloud – jeweils in Eigenverantwortung oder über den Managed Service *indevis Firewall*.

SIE WOLLEN
MEHR ERFAHREN?

Ihr persönlicher Ansprechpartner berät Sie gerne und findet mit Ihnen heraus, welches Konzept am besten zu Ihnen passt.

indevis GmbH

Koppstraße 14
81379 München

Tel. +49 (89) 45 24 24-100
Fax: +49 (89) 45 24 24-199

sales@indevis.de
www.indevis.de