Mai 2022

ComConsult GmbH
Beratung + Planung + Schulung

Der Netzwerk Insider

Was ist eigentlich los bei der Künstlichen Intelligenz?

von Nils Wantia
Wer die Öffentlichkeitsarbeit großer Hersteller aus dem Umfeld der Kommunikations-IT in den letzten Jahren verfolgt hat, dem wird aufgefallen sein, welchen Stellenwert das Thema Künstliche Intelligenz (KI) dort einnimmt: Egal ob in Blogs, Videos, Newslettern oder Veranstaltungen – das Thema war und ist geradezu allgegenwärtig. Und das mittlerweile schon seit einigen Jahren. Grund genug, um noch einmal einen Blick auf das Feld zu werfen und zu bewerten, was hinter diesem hartnäckigen Hype steckt, wieviel davon gerechtfertigt ist und worauf man in Zukunft hoffen darf.

Seite 8

Gegen eine „Hidden Agenda“ bei der IT-Vergabe

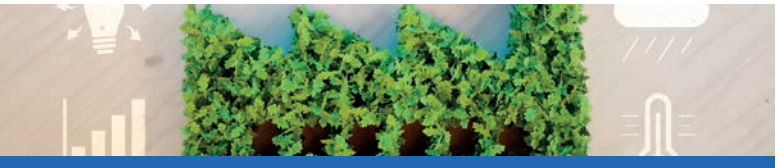
von Dr. Behrooz Moayeri
Die Informationstechnik (IT) durchdringt immer mehr Bereiche der Produktion und der Arbeitswelt. Dadurch entsteht Bedarf an Hardware, Software und IT-Dienstleistungen. Zudem müssen Hardware und Software am Ende ihrer Lebenszeit durch neue Hardware und Software ersetzt werden. All das erfordert IT-Beschaffung und Vergabe von IT-Aufträgen.

Seite 2

RADIUS aus der Cloud – Marketing oder Mehrwert?

von Sebastian Matzigkeit
Neben Netzwerkmanagement-, Proxyserver- und SIEM-Diensten gibt es vermehrt auch Her-steller von RADIUS-Lösungen, die Ihr Produkt teilweise oder gar komplett als Cloud-Lösung bereitstellen. Welche Bereitstellungsszenarien existieren und für welche Anwendungsfälle diese sinnvoll sind, klären wir im Folgenden.

Seite 22



Webinar der Woche

Wie smarte Gebäude Klima schützen

Seite 21

Multifaktor-Authentisierung aushebeln

Wie auch hier Social Engineering helfen kann

von Dr. Markus Ermes
Kürzlich wurde ein Social-Engineering-Angriff auf Microsoft-Konten bekannt, bei denen auch die Multifaktor-Authentisierung (MFA) ausgehebelt wurde. Doch was genau ist passiert? Ist MFA nicht viel sicherer als eine einfache Authentisierung mit Benutzername und Passwort?

Seite 19

Gegen eine „Hidden Agenda“ bei der IT-Vergabe

von Dr. Behrooz Moayeri

Fortsetzung von Seite 1

IT-Vergabe ist ein interdisziplinäres Gebiet, das Bedarfsträger, IT-Experten sowie Einkaufs-und Rechtsabteilungen betrifft. Jede Organisation hat Compliance-Regeln für die Vergabe von Aufträgen. Bei der öffentlichen Verwaltung sind diese Regeln Gegenstand des Vergaberechts. Doch auch andere Organisationen folgen Vergaberegeln. In manchen von ihnen kommt zum Beispiel der Revisionssicherheit bei Auftragsvergabe eine zentrale Bedeutung zu. Dabei geht es um dieselben Prinzipien wie die des öffentlichen Vergaberechts: Transparenz, Wirtschaftlichkeit, Bekämpfung von Korruption usw. Allerdings geht das öffentliche Vergaberecht über diese Ziele hinaus und enthält Vorkehrungen für die sogenannte Mittelstandsfreundlichkeit und das Klagerecht.

Wir befassen uns im Folgenden mit einigen Aspekten der IT-Vergabe, die nicht nur die öffentliche Verwaltung, sondern auch die meisten anderen Organisationen betreffen.

Verschiedene Interessen

In Zusammenhang mit der Vergabe von IT-Aufträgen gibt es oft Interessenkonflikte innerhalb einer Organisation. Zu einem solchen häufigen Konflikt kommt es dann, wenn Bedarfsträger bzw. IT-Experten keinen echten, offenen Wettbewerb zwischen Anbietern verschiedener Lösungen wollen, während ein solcher offener Wettbewerb aufgrund der Compliance-Regeln geboten ist, denen die Organisation unterliegt.

Die Abneigung der Bedarfsträger bzw. IT-Experten gegen einen ergebnisoffenen Wettbewerb kann verschiedene Gründe haben, zum Beispiel:

- Jeder Technik- bzw. Anbieter-Wechsel verursacht Mehrarbeit.
- Es ist zu befürchten, dass die neue Lösung erst im Betrieb Probleme aufweisen wird, die bis zur Vergabe nicht bekannt waren oder an die man nicht gedacht hat.
- Es gibt die Sorge, dass es im Betrieb aufgrund fehlender Kenntnisse über die neue Lösung zu Problemen kommt.
- Der bisherige Lösungsanbieter wird bevorzugt, weil man in der Zusammenarbeit mit ihm bereits geübt ist.
- Es kann auch umgekehrt sein, dass man die bisherige Lösung aufgrund schlechter Erfahrungen unbedingt durch eine andere Lösung ersetzen will.

Dass ein ergebnisoffener Wettbewerb aufgrund von Compliance-Regeln häufig geboten ist, liegt auf der Hand:

- Die Auftraggeberin kann mit einem offenen Wettbewerb wirtschaftliche Vorteile erreichen.
- Ein offener Wettbewerb beugt Korruption vor.
- Transparente Vergabe anhand offengelegter Kriterien dient der Pflege von fairen Beziehungen zu Lieferanten, die für die Organisation wertvoll sind.

Wie wird mit dem Interessenkonflikt umgegangen?

Eine schlechte Praxis wird durch Geläufigkeit nicht besser

Leider sehr geläufig ist die schlechte Praxis, den oben genannten Konflikt zwischen der Abneigung gegen Wettbewerb und dem Gebot desselben scheinbar aus dem Weg zu gehen, indem man nur so tut, als gäbe es einen offenen Wettbewerb. Das nenne ich eine „Hidden Agenda“ im Vergabeverfahren.

Das eigentliche Ziel des Vergabeverfahrens, nämlich die Auswahl oder umgekehrt der Ausschluss einer bestimmten Lösung, wird dabei „versteckt“. Potentielle Bieter sollen im Glauben an einen ergebnisoffenen Wettbewerb gelassen werden. Darüber hinaus soll die Hidden Agenda manchmal sogar anderen Instanzen innerhalb der eigenen Organisation verborgen bleiben, etwa der Beschaffungsstelle, der Revision, der Rechtsabteilung oder gar den eigenen Vorgesetzten.

Egal wem das Versteckspiel gilt: Es ist eine schlechte Idee, die nicht etwa dadurch besser wird, dass man es immer schon so gemacht hat oder andere es genauso tun. Warum ich dagegen bin, werde ich nun erläutern.

Unfairer Umgang

Unfairer Umgang innerhalb einer Organisation ist schlecht für alle Betroffenen. Ich brauche hier nicht darauf einzugehen, welche Belastung es bedeutet, in einem Umfeld zu arbeiten, in dem Täuschung zum Repertoire der Arbeit zählt.

Doch auch in Beziehungen zu Lieferanten ist eine Hidden Agen-

Was ist eigentlich los bei der Künstlichen Intelligenz?

von Nils Wantia

Fortsetzung von Seite 1

Was ist eigentlich Künstliche Intelligenz?

Eines vorweg: Niemand sollte damit rechnen, dass wir kurz vor dem Durchbruch für eine künstliche Superintelligenz à la HAL 9000, Skynet etc. stehen. Selbst wenn in der Werbung teilweise mit solchen (dann allerdings positiven) Ausblicken kokettiert wird, reden wir hier ausschließlich von sogenannter "schwacher" Künstlicher Intelligenz. Dahinter verbergen sich Methoden, welche nur für die Bearbeitung spezieller Aufgabenstellungen gedacht sind und kein tatsächliches intelligentes Bewusstsein schaffen sollen, wie das bei einer "starken" Künstlichen Intelligenz der Fall wäre.

Darüber hinaus wird es knifflig, was die Definitionen zur Künstlichen Intelligenz betreffen: Während wir im Bereich der natürlichen Intelligenz zumindest einen groben Konsens zur Definition oder zumindest zu dem Nachweis der Intelligenz von Individuen haben, wird es bei der Künstlichen Intelligenz deutlich schwieriger.

Eine echte Bestimmung des Begriffs hatten wir noch nie, und dass das Thema in den letzten Jahren durch Werbung und medialen Hype wieder und wieder aufgegriffen wurde, hat die Sache nicht besser gemacht. Inzwischen beobachte ich immer wieder, dass maschinelle Entscheidungen, die durch einfache Wenn-Dann-Beziehungen (if-then-else) getroffen werden können, als Künstliche Intelligenz verkauft werden. Da fragt man sich natürlich, was demnach nicht mehr intelligent ist. Schließlich geht es um Aufmerksamkeit, und da lässt sich ein unklar definierter Hype-Begriff immer gut verwenden.

Tatsächlich ist der Begriff, oder vielmehr das Forschungsfeld dahinter, alles andere als neu. Gegründet wurde das akademische Fachgebiet der Künstlichen Intelligenz im Jahr 1956 auf der Dartmouth-Konferenz. Damals ging man noch davon aus, dass man die Intelligenz eines Menschen in weniger als einer Generation erreichen konnte. Man glaubte also, innerhalb relativ kurzer Zeit sogar eine starke KI entwickeln zu können.

Im folgenden Jahr prognostizierte man, dass es innerhalb der nächsten zehn Jahre ein auf Künstlicher Intelligenz basierenden Schachweltmeister geben würde. Inzwischen wissen wir, dass beide Prognosen viel zu optimistisch waren.

Der Hintergrund ist ein grundlegendes Problem der Künstlichen Intelligenz: Die zu lösenden Probleme sind sehr komplex und skalieren sehr ungünstig. So können zwar vielversprechende Ansätze gefunden werden, die kleine Beispielprobleme lösen können. Sobald diese Problemstellungen jedoch ausgeweitet werden, steigt die Komplexität enorm an, sodass die notwendigen Rechen- bzw. Speicherressourcen und somit auch die benötigten Zeiten schlagartig durch die Decke gehen. Reale Probleme bleiben damit häufig unlösbar, und die Ansätze sind nicht allgemeingültig.

Man könnte also sagen, die Geschichte der KI sei eine Folge von großen Erwartungen und noch größeren Enttäuschungen, denn sie handelt von einem Zyklus neuer Ansätze, welche aufgrund der Komplexität der realen Probleme doch wieder im Sand verlaufen. Auf neue Ansätze folgten zuweilen Jahre der Ernüchterung, in denen das Feld der Künstlichen Intelligenz wenig angesagt war, bevor es mit einem neuen Ansatz wieder von vorne losging.

Dementsprechend liegt die Vermutung nahe, dass es sich dieses Mal ebenfalls nur um eine weitere Iteration des ewigen Zyklus handelt. Und darin liegt sicherlich ein gehöriges Stück Wahrheit. Nichtsdestotrotz wäre es zu kurz gegriffen, das Thema damit einfach abzuhaken, denn es gibt durchaus einige Argumente, die dafürsprechen, etwas genauer hinzusehen.

Es steckt mehr als nur Hype hinter dem Thema

Zunächst einmal muss festgehalten werden, dass neben den Enttäuschungen der Vergangenheit durchaus auch bedeutende Erfolge erzielt werden konnten. Allerdings werden diese vielfach nicht dem Feld der Künstlichen Intelligenz zugeschrieben. Interessanterweise liegt dies häufig an der bereits thematisierten fehlenden Definition des Begriffs, wodurch Themengebiete, die ehemals zum Forschungsgebiet der Künstlichen Intelligenz gezählt wurden, in der Folge nicht mehr darunterfielen. Dies gilt beispielsweise für Anwendungen im Compilerbau oder in der Regelungstechnik. Heute hingegen wird gern das Gegenteil getan, wenn simple Anwendungen als "intelligent" angepriesen werden.

Ebenso gibt es im aktuellen KI-Hype viele Anwendungen, die nicht nur beeindruckende, sondern auch in der realen Welt nutzbare Ergebnisse liefern, von denen ich nachfolgend noch einige nennen möchte. An dieser Stelle sei exemplarisch lediglich eine Anwendung genannt: Autonomes Fahren. Seit vielen Jahren gibt es diverse Prototypen autonom fahrender Autos, die teilweise bereits viele tausend Kilometer im realen Straßenverkehr vollständig autonom gefahren sind. Als Beispiel sei hier nur das „Self-driving car“ von Google bzw. der Alphabet-Tochter Waymo genannt, die unter dem Label Waymo One als Roboter-Taxi in Phoenix fährt.

Natürlich müssen hier noch schwierige technologische, juristische und sogar ethische Fragen beantwortet werden. Doch braucht es auf der anderen Seite nicht allzu viel Phantasie, um sich das disruptive Potenzial einer solchen Technologie sowie die Konsequenzen auszumalen, die sich daraus für das gesamte Verkehrswesen und der zugehörigen Wirtschaftszweige ergeben können.

Die Frage ist dabei längst nicht mehr ob, sondern wann wir eine solche Technologie erleben werden. Dementsprechend groß sind das Interesse und die Investitionen auch aus der Wirtschaft. Darum haben wir schon lange aufgehört, nur von grauer Forschung zu sprechen, denn schließlich geht es um konkrete Anwendungen. Letztendlich haben wir inzwischen auch unseren künstlichen Schachweltmeister bekommen. Zwar hat es dann noch satte 40 statt der zunächst erwarteten zehn Jahre gedauert, doch 1997 war es mit Deep Blue dann endlich soweit.

Nicht zuletzt werden die Randbedingungen für KI-Anwendungen fortlaufend besser. Entscheidend ist dabei eher weniger die stetige Steigerung der Rechenleistung moderner Computersysteme (da KI-Probleme schlecht skalieren), sondern vielmehr die Fortschritte in benachbarten Feldern, zum Beispiel im Bereich der Bereitstellung von Daten. Hier kommen andere Hype-Themen wie IoT oder Sensorfusion zum Tragen, da sie wertvollen Input für so manchen KI-Ansatz liefern können.

Grundlage des aktuellen Zyklus

Der aktuelle Zyklus begann mit dem Ansatz des sogenannten Deep Learning, der in den Medien ebenfalls gern genannt wird, weil er schön griffig ist und die Phantasie anregt. Dabei handelt es sich um eine spezielle Ausprägung des Maschinellen Lernens, die wiederum auf dem erweiterten Ansatz der Neuronalen Netze basiert, den es bereits seit den 60er oder teilweise sogar 40er Jahren gibt. Er fußt auf einem Modell des menschlichen Gehirns bzw. der Neuronen, aus denen das Gehirn besteht. Deep Learning erweitert diesen Ansatz um einige technische Ansätze, die die praktische Anwendbarkeit dieser Technologie vergrößern und zu neuen Anwendungen, insbesondere in dem Bereich der Sprach- und Bildverarbeitung geführt haben. Trotz des Namens und der Inspiration durch ein (mittlerweile veraltetes) Modell echter Neuronen handelt es sich um einen reinen technischen Ansatz, welcher niemals zu einem künstlichen Gehirn, sprich starker KI, skalieren wird. Die Nachbildung des menschlichen Gehirns wird derweil durch einen vollkommen anderen Ansatz im „Human Brain Project“ verfolgt.

Die Netze der künstlichen Neuronen müssen mit realen Beispieldaten "trainiert" werden. Bei diesem Prozess spielt der Zufall eine wichtige Rolle, denn gleich an mehreren Stellen wird ganz bewusst mit Zufallszahlen gearbeitet. Dementsprechend ist das Ergebnis eines solchen Trainings nicht deterministisch, d.h. wenn es mehrmals durchlaufen wird, kommen jeweils unterschiedliche Ergebnisse dabei heraus. Das ist einer der Gründe, weswegen mein Professor seinerzeit skeptisch gegenüber diesen Ansätzen war, da die Entwicklung solcher Systeme in Teilen einem Glücksspiel gleicht und das Ergebnis nicht vollständig nachvollzogen oder gar nach Fehlern untersucht werden kann. Niemand kann letztlich sagen, warum genau das System eine konkrete Entscheidung getroffen hat. Das kann bei fatalen Fehlentscheidungen (zum Beispiel beim Autonomen Fahren) durchaus problematisch sein.

Gleichzeitig bedarf es neben technischen Grundlagen auch einer gewissen Menge Erfahrung und Fingerspitzengefühl (und nicht zuletzt Glück), um die Trainingsdaten und Algorithmen derart aufzubereiten, dass für einen konkreten Anwendungsfall ein brauchbares Ergebnis herauskommt.

Inzwischen haben sich Ansätze etabliert, bei denen der Prozess des Anlernens von mehreren KI-Systemen durchgeführt wird. Dabei erzeugt ein KI-System Ergebnisse (zum Beispiel Bilder von Katzen), und das andere KI-System bewertet die Ergebnisse (Ist das ein Bild einer Katze?).

So können deutlich mehr Daten verarbeitet werden, und das Erzeugersystem erhält eine umfassende Trainingsbasis, ohne dass das Training mühselig durch Menschen überwacht werden muss. Sogenannte Generative Adversarial Networks (GAN) verfolgen genau diese Idee und sind Grundlage etlicher Systeme, die Inhalte wie zum Beispiel Bilder, Videos oder Text erzeugen sollen.

Viele Anwendungen dieser Technologien liegen im Bereich der Kommunikation und sollen die modernen Enterprise-Lösungen aufwerten. Dort können sie durchaus Sinn ergeben, denn es werden insbesondere Sprache, Ton, Bild und jede Menge weitere Daten verarbeitet. Wenn man sich jedoch die aktuellen Enterprise-Lösungen anschaut, dann hält sich die Begeisterung bei den Anwendern oft noch in Grenzen.

Grund dafür sind die hohen Ansprüche, die an Lösungen aus dem Enterprise-Segment gestellt werden. Hier liegt der Fokus traditionell auf Zuverlässigkeit, Robustheit und Sicherheit. All das sind Themen, die bei diesen jungen Technologien erst nach und

Multifaktor-Authentisierung aushebeln – wie auch hier Social Engineering helfen kann

von Dr. Markus Ermes

Fortsetzung von Seite 1

MFA – die Grundlagen und Umsetzungsmöglichkeiten

Prinzipiell stimmt die Aussage, dass MFA mehr Sicherheit bietet als die reine Kombination aus Benutzername und Passwort. Die Idee ist, dass man zusätzlich einen weiteren Faktor hat, der sich im Besitz des Benutzers befindet und für Angreifer nicht verfügbar ist. Doch wie genau dieser Faktor aussieht, ist nicht festgeschrieben. Daher haben sich im Laufe der Jahre mehrere verschiedene Ausprägungen ergeben. Im Folgenden sind die aktuell am weitesten verbreiteten Verfahren kurz dargestellt:

Sehr häufig ist die Verwendung eines entsprechenden Codes, der über einen weiteren Kanal an den Benutzer übermittelt und von diesem zusätzlich zu Benutzername und Passwort eingegeben wird. Dabei handelt es sich typischerweise um einen 5- bis 6-stelligen Code, der aus Zahlen oder Zahlen und Buchstaben besteht. Dieser kann auf verschiedene Arten an den Benutzer übermittelt werden:

- Der physische RSA-Token: Der Klassiker ist der Schlüsselanhänger, der alle 60 Sekunden eine neue 6-stellige Zahl ausgibt, die nur dem Token und einem Server innerhalb des Unternehmens bekannt sind.
- Der „Software-Token“: Die Funktion des Hardware-Tokens wird über eine spezielle App reproduziert, die nach der Installation auf dem Smartphone mit dem Dienst verbunden wird. Statt alle 60 Sekunden auf wechselnde Codes eines Schlüsselanhängers schauen zu müssen, öffnet man eine App.
- Eine E-Mail: Der Zugangscode lässt sich ggf. auch per E-Mail an eine vorgegebene Adresse schicken.
- SMS: Eine weitere Möglichkeit ist eine SMS-Nachricht, die an eine im System hinterlegte Mobiltelefonnummer geschickt wird. In dieser steht ebenfalls ein solcher Code, der identisch zu anderen Tokens funktioniert.

Dann gibt es noch die Authenticator-App: Sie wird immer beliebter und ist auch bei Microsoft im Einsatz. Dabei wird bei der Anmeldung mit Benutzername und Passwort eine Zeichenfolge angezeigt, die man in einer dafür vorgesehenen App (nach der Eingabe einer PIN für die App oder der Nutzung von Fingerabdruck oder Gesichtserkennung) nur noch mit einem Klick bestätigen muss. Dies ist der komfortabelste und häufig schnellste Weg. Und last but not least gibt es mittlerweile ebenfalls spezielle USB-Geräte, die per FIDO2 die Authentisierung unterstützen. Diese Geräte speichern für verschiedene Dienste verschiedene Zugangsdaten und müssen für die Nutzung der Zugangsda-

RADIUS aus der Cloud – Marketing oder Mehrwert?

von Sebastian Matzigkeit

Fortsetzung von Seite 1

Warum Cloud?

RADIUS-Server bieten Möglichkeiten zur Authentisierung, Autorisierung und Accounting (AAA) für u.a. administrative Anmeldungen an Netzwerkkomponenten, Authentifizierungen von VPN-Verbindungen, Anmeldung im WLAN mit WPA-Enterprise oder an lokalen, kabelbasierten Netzwerken mit einer Netzzugangskontrolle. In den meisten Fällen stehen diese Server redundant verteilt in (On-Prem-)Rechenzentren. Ein RADIUS-Cluster eines großen Unternehmens kann schon mal aus mehr als 30 Servern bestehen, die auf der gesamten Welt verteilt sind und über ein WAN miteinander synchron gehalten werden.

Alle RADIUS-Clients (Netzwerkkomponenten wie VPN-Gateways, Access Points oder WLAN-Controller, Access Switches, usw.) müssen mit der RADIUS-Lösung kommunizieren können. Wie soll das funktionieren, wenn die Leistung “RADIUS-Authentifizierung” an vielen Standorten bereitgestellt werden muss, diese jedoch weder eine entsprechend performante WAN-Anbindung noch einen lokal vorgehaltenen On-Prem-RADIUS-Server haben? VPN-Verbindungen wären eine Lösung, doch geht dies eventuell auch einfacher.

Ein anderes Szenario ist der Einsatz von RADIUS für Netzwerklösungen, die ohnehin schon cloudbasiert sind. Wenn ein VPN-Gateway, ein Netzwerk-Management oder gar eine ganze WLAN-Lösung in der Cloud sind, könnte eine cloudbasierte RADIUS-Lösung das Ganze vereinfachen.

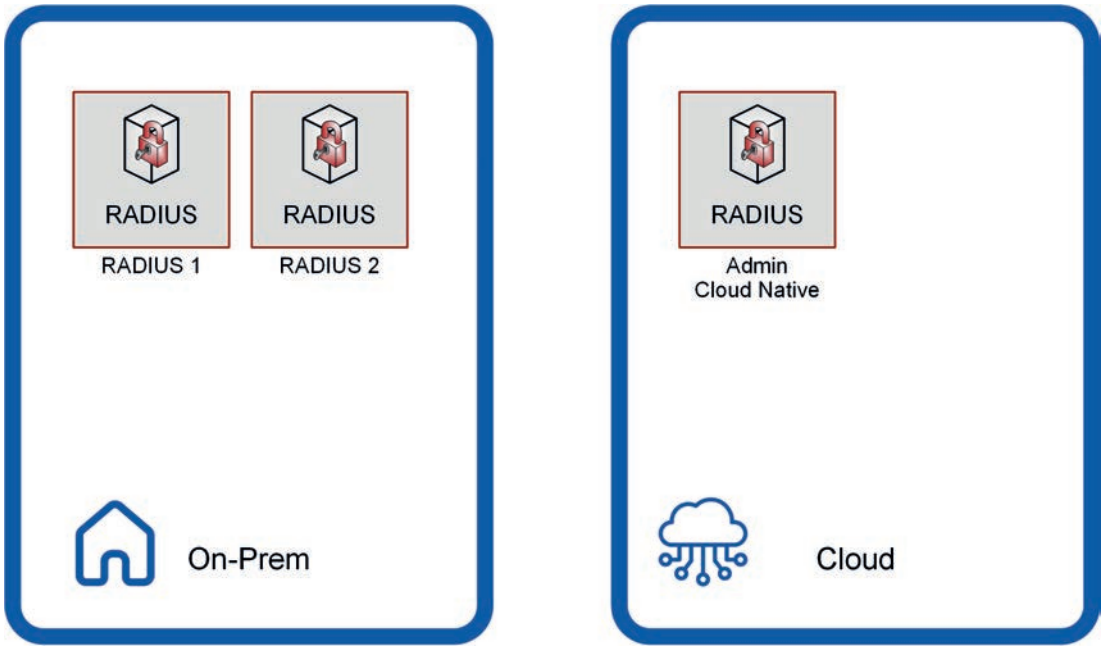


Abbildung 1: Hybride Lösung

Verschiedene Ansätze

Beim Thema Cloud-RADIUS setzen verschiedene Hersteller auf durchaus unterschiedliche Ansätze. Während in manchen Fällen der vermeintliche Cloud-Server eine im Rechenzentrum installierte VM mit optionalem Monitoring in der Cloud ist, bieten andere Hersteller eine Management-Lösung in der Cloud an, welche die On-Prem-RADIUS-Server zentral verwaltet (siehe Abbildung 1).

Wiederum andere bieten an, ihre bekannten virtuellen Appliances in