AIRLOCK®
SECURE ACCESS HUB

WHITEPAPER

Zero Trust ist eine Reise

Von der Perimeter-Sicherheit zum umfassenden Sicherheitskonzept

Inhaltsverzeichnis

Sicherheitsrisiken in einer immer digitaleren Welt

Die kontinuierliche digitale Transformation der Welt schreitet voran und wirkt sich tiefgreifend auf das Privat- und Berufsleben in einer Weise aus, die vor wenigen Jahren noch schwer vorstellbar war. In dieser Arbeit werden wir die Effekte der kontinuierlichen Digitalisierung und ihre Auswirkungen auf die moderne Informationstechnologie im Allgemeinen und auf die Informationssicherheit im Besonderen behandeln.

Weiterentwicklung der Geräte

Der sichtbarste Effekt der Digitalisierung ist die Weiterentwicklung von Endnutzergeräten. Am Anfang setzten Unternehmen Desktop-Computer für ihre Mitarbeiter ein. Dann, vor 25 Jahren, nutzten Geschäftsreisende Laptops für ihre Termine bei Kunden und Partnern. In den letzten Jahren wurden diese Geräte nicht mehr von den Unternehmen bereitgestellt, sondern von den Mitarbeitern selbst mitgebracht (BYOD). Vor allem in technologiegestützten Unternehmen konnten Mitarbeiter und Mitarbeiterinnen frei entscheiden, welches Betriebssystem sie installieren wollten. Noch neuer ist der Trend zu Tablets, die zunächst eine Ergänzung für normale Computer waren, sie aber zunehmend als Arbeitsgeräte ersetzen.

Weiterentwicklung der Anwendungen

Parallel zur Entwicklung der Endnutzergeräte beobachten wir eine Weiterentwicklung der auf diesen Geräten installierten Anwendungen. Im Zeitalter des Desktop-Computers waren Client-Server-Architekturen mit proprietären Protokollen und einfachen Firewall-

Sicherheitsregeln die Norm. Mit dem Aufkommen von Browsertechnologien verschwand der Grossteil der Geschäftsfunktionen vom Endgerät (Client). Server wurden nun Portale genannt und boten Funktionen für E-Commerce, E-Banking und viele weitere Anwendungen. Firewalls für Webanwendungen zur Filterung von HTML-Datenverkehr wurden zum bevorzugten Sicherheitstool. Im letzten Entwicklungsschritt wird ein Teil der Logik in Form von mobilen Apps und browserbasierten Einzelseitenanwendungen zurück auf den Client verlagert. Diese Apps werden über App Stores einfach verteilt und verkauft. Der Server heisst nicht länger Portal, sondern Ressource und REST ist das bevorzugte Protokoll, um mit diesen Ressourcen zu interagieren. Natürlich muss es auch neue Sicherheitslösungen geben, um den Datenstrom zwischen App und Ressourcen zu schützen. API-Gateways erfüllen genau diese Anforderungen.

Von der Perimeter-Sicherheit zu Zero Trust

Die beschleunigte Transformation im Bereich der Client-Geräte birgt das Risiko, die Sicherheitsarchitektur zu vernachlässigen, weil die Zeit fehlt, um notwendige Änderungen am Betriebsmodell vorzunehmen. Die Entwicklung der Client-Technologie und der entsprechenden Nutzungsmuster finden parallel zur Entwicklung von geschützten internen Netzwerken und Remote-Verbindungen über VPN für den Fernzugriff über das Internet statt. Ebenso gab es Paradigmenwechsel in der Informationssicherheit. Zunächst galt das klassische «Castle and Moat»-Konzept als ausreichend, um den Perimeter des internen Netzwerks zu schützen und alles und jeden im internen Netzwerk als «vertrauenswürdig» zu akzeptieren. Die heute bewährte Sicherheitspraxis empfiehlt eine Architektur, welche die Zugriffskontrolle vom Perimeter in Richtung der Dienste verschiebt. Das heisst die Zugriffskontrolle erfolgt durch die Applikation selbst oder eine Sicherheitskomponente, welche unmittelbar davor steht. Es stellt sich die Frage, welche Sicherheitstools am besten geeignet sind, um den Wechsel zu einer Zero Trust-Architektur zu bewerkstelligen.

Containerisierung und SaaS

Betriebsmodelle ändern sich ebenfalls. Früher besassen Unternehmen ihre eigene Hardware und betrieben ihre eigenen Rechenzentren vor Ort. Die Virtualisierung und später die Containerisierung wurden eingeführt, um Hardwareressourcen effizienter zu nutzen.

Doch diese Technologien entwickeln sich weiter. Rechenressourcen werden nun als Service genutzt, je mehr Unternehmen ihre IT-Dienste teilweise oder vollständig in ein Cloud-Modell verlagern. Dies beinhaltet einen gewissen Verlust der Kontrolle über die Infrastruktur und ihre Pflege, da die betriebliche Kontrolle an den Anbieter der Cloud-Infrastruktur delegiert wird. Demzufolge müssen Unternehmen, die Cloud-Dienste nutzen, neue Bedrohungen abwehren, die aus diesem Betriebsmodell entstehen.

DevOps

DevOps ist ein weiterer Paradigmenwechsel. Er fordert Unternehmensstrukturen mit separaten Verantwortlichkeiten für Netzwerke, Speicher, Betriebssysteme und Anwendungen heraus. Dieser Wechsel wird durch die Verlagerung in die Cloud beschleunigt, weil der gesamte Infrastrukturbetrieb ausgelagert wird. Cloud-Anbieter stellen weitere Dienste für die Integration in Anwendungen und Tools bereits, um die Entwicklung und automatische Installation von Anwendungen zu ermöglichen. Im Wesentlichen ermöglicht der Cloud-Anbieter den Wechsel zu DevOps, indem er Dienste für Entwickler und DevOps bereitstellt, auf denen diese aufbauen können, um in der Lage zu sein, sich voll und ganz auf die Implementierung der Geschäftsfunktionen zu konzentrieren.

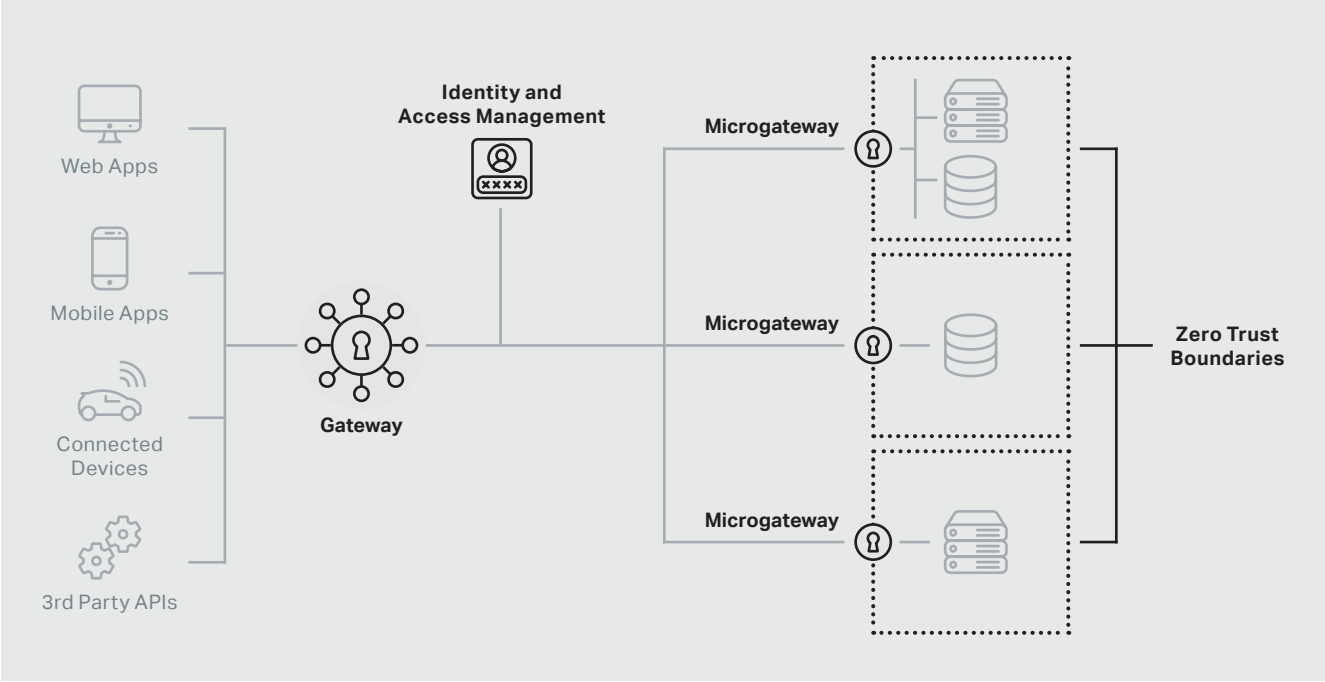
Angriffe sind die neue Normalität

Der allgegenwärtige Wandel der Informationstechnologie ist auch in den heutigen Bedrohungsszenarien erkennbar. Denken wir zum Beispiel an Phishing-Attacken. Vor zwanzig Jahren hätte eine erfolgreiche Phishing-Attacke[1] keine Schlagzeilen gemacht, weil ihre Folgen noch zu unbedeutend waren. Heute machen sie keine Schlagzeilen, weil sie zu oft passieren und Menschen sie nicht länger als berichtenswert erachten. Bruce Schneier schrieb 2014: «*Wenn etwas in den Nachrichten ist, machen Sie sich keine Sorgen. Die eigentliche Definition von «Nachricht» bezieht sich auf etwas, das kaum jemals passiert. Erst wenn etwas nicht in den Nachrichten ist, wenn etwas so gewöhnlich ist, dass es nicht länger neu ist – Autounfälle, häusliche Gewalt – sollte man sich Sorgen machen. Wenn wir uns die Erfolgsraten von Phishing-Attacken ansehen, ist das kein Wunder. Laut einer Studie von Proofpoint[2] haben 65 % der US-amerikanischen Unternehmen im letzten Jahr (2019) eine erfolgreiche Phishing-Attacke erlebt*». Aus der Sicherheitsperspektive gesehen weist der anhaltende Erfolg von Phishing-Attacken insbesondere und Social Engineering- Angriffen im Allgemeinen darauf hin, dass Menschen ein ausnutzbares Ziel sind, das geschützt werden muss.

[1] https://www.phishprotection.com/resources/history-of-phishing

[2] https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-state-of-the-phish-2020.pdf

Digitalisierung der Informationssicherheit



Informationssicherheit muss mit all diesen Veränderungen Schritt halten. Die neueste Antwort, die die Informationssicherheit liefert, ist die Zero Trust-Architektur. Die Frage ist: Warum und wie sollte diese neue Architektur die Probleme lösen, die aus der Entwicklung der Informationstechnologie entstehen?

Die Grundlagen von Zero Trust

Die Zero Trust-Architektur ist ein recht modernes Konzept (John Kindervag, Forrester, 2010), das einen wesentlichen Aspekt der Informationssicherheit von Grund auf ändert. Anstatt zu versuchen, eine interne und sichere Vertrauenszone vor böswilligen Angreifern von aussen zu schützen, schreibt Zero Trust vor, dass jede einzelne Anfrage als nicht vertrauenswürdig gilt, bis das Gegenteil bewiesen ist. Das neue Paradigma könnte zusammengefasst werden mit: Vertrauen ist gut, Kontrolle ist besser.

Blaupause für eine Zero Trust-Architektur

Für die Umsetzung einer Zero Trust-Architektur ist eine kompakte Lösung für den Schutz von Diensten oder Anwendungen nötig: ein Microgateway. Das Microgateway ist im Kern ein Reverse-Proxy, der den durchlaufenden Datenverkehr filtert und die Identitäten der Beteiligten jeder Anfrage prüft. Abhängig von der Art des Datenverkehrs agiert das Microgateway als Web Application Firewall (HTML-Datenverkehr) oder als API-Gateway (REST-Anfragen).

Sicherheitsvorteile von Zero Trust

Der Zero Trust-Ansatz hat viele Vorteile gegenüber herkömmlichen «Castle and Moat»-Sicherheitsdesigns. Er schützt nicht nur interne Ressourcen vor Angriffen von aussen, sondern auch vor lateralen Attacken. Wenn jede Ressource im Netzwerk von einem Microgateway geschützt wird, das die Gültigkeit jeder einzelnen Anfrage prüft, ist es für einen Angreifer sehr viel schwerer, von einem System zum nächsten zu gelangen. Zugangsdaten, die über Social Engineering abgegriffen werden, sind weniger hilfreich für einen Angreifer, da ein Dienst einem «Benutzer» keine Zugriffsrechte ausserhalb der regulären Nutzung des Dienstes gewähren muss.

Zero Trust-Architekturen verteilen die Komplexität des Sicherheitssystems und machen es überschaubarer. In einem Szenario mit Perimeterschutz muss der Perimeter eine Sicherheitsrichtlinie implementieren, die den gesamten Datenstrom im Unternehmen berücksichtigt. Wenn Sie jemals die Firewall-Regeln eines mittelständischen Unternehmens gesehen haben, wissen Sie bereits, dass diese Regeln extrem umfangreich und schwer zu steuern sind. Bei der Anwendung einer Zero Trust-Architektur ist der Geltungsbereich der Richtlinie auf einen einzelnen Dienst begrenzt. Dieser Geltungsbereich ist leicht verständlich und beherrschbar. Ein weiterer Vorteil der reduzierten Komplexität ist die Verringerung der Betriebsrisiken, weil Fehlkonfigurationen seltener passieren. OWASP führt «Sicherheits-Fehlkonfiguration» als Bedrohung «A6» in ihrer Top Ten-Liste[3] und als Bedrohung «API7» in der API-Sicherheitsliste[4].

Betriebliche Vorteile von Zero Trust

Die verteilte Struktur von Zero Trust-Architekturen lässt sich gut mit DevOps-Paradigmen vereinbaren. Der Vorschlag, dass DevOps-Teams die Sicherheitsregeln für die Ressourcen, die sie entwickeln, verwalten sollten, könnte einige Fragen in Bezug auf die Kontrolle dieser Regeln aufwerfen. Jedoch gibt es auch hier Argumente, die den Vorschlag zumindest zur Diskussion stellen. Bei einem DevOps-Setup ist das Team für die Entwicklung, Konfiguration und den Betrieb eines Dienstes verantwortlich. Dieses Team ist besonders qualifiziert, Sicherheitsbedrohungen und Gegenmassnahmen zu bewerten. DevOps-Teams, die moderne REST-Dienste pflegen, stellen mit hoher Wahrscheinlichkeit bereits OpenAPI-Spezifikationen zusammen mit ihrem Dienst bereit. Diese Spezifikation wird an die Entwickler inner- und ausserhalb des Unternehmens weitergeleitet, damit sie Client-Anwendungen, die REST-Dienste nutzen, entwickeln können. Die gleiche Open-

[3] https://owasp.org/www-project-top-ten/

[4] https://owasp.org/www-project-api-security/

API-Spezifikation kann vom API-Gateway als Regelsatz verwendet werden, um Datenverkehr zu filtern. Das Gateway kann zusätzliche Sicherheitsdienste wie Authentifizierung, Protokollierung, Durchsatzratenbegrenzung usw. bereitstellen, die Entwickler nicht erneut in die Anwendungslogik implementieren müssen. Das gewährleistet, dass nur wohlgeformte Anfragen an den gefährdeten Endpunkten des Dienstes eintreffen. Alle anderen Anfragen werden vorher gefiltert und können nicht zur Bedrohung werden.
Die Pflege dieser OpenAPI-Spezifikation schafft keinen Zusatzaufwand für das DevOps-Team, da sie ohnehin erfolgen muss, um sicherzustellen, dass Entwickler von Client-Anwendungen immer die neueste API-Version haben. Das gehört für gewöhnlich zum Entwicklungswerkzeug (Code ausgehend von einer Spezifikation oder eine Spezifikation ausgehend von Annotationen im Code zu generieren). Der erforderliche Aufwand ist also sehr begrenzt und viele Software-Entwicklungstools erzeugen automatisch die OpenAPI-Spezifikation anhand von Annotationen im Code (oder umgekehrt). Die Delegation der Ressourcensicherheit an ein spezialisiertes DevOps-Team, das mit der kontinuierlichen Weiterentwicklung dieser Ressource betraut ist, reduziert nicht nur die Kosten, sondern erhöht auch die Sicherheit und den Schutz im Vergleich zu einem zentralisierten und generischen Ansatz.

Zero Trust passt nicht nur gut zu DevOps, sondern unterstützt auch den Wechsel in die Cloud. Jeder Dienst benötigt eine gewisse Form von Sicherheit, um ihn vor unbefugtem Zugriff zu schützen, insbesondere beim Wechsel in die Cloud und beim gleichzeitigen Verzicht auf eine VPN-basierte Netzwerkarchitektur. Das Microgateway könnte die Antwort sein, wenn es die mit Cloud-Implementierungen verbundenen Anforderungen erfüllt. Ein Microgateway muss einfach implementierbar sein, vorzugsweise in einer Container-Architektur, da dies kostenintensive Cloud-Rechenressourcen im Vergleich zu virtualisierten Lösungen spart. Das Microgateway muss vollautomatisch imstallierbar sein, um gut in die Werkzeuge für das Cloud-Management und DevOps integriert werden zu können.

Grenzen von Zero Trust

Die Stärke von Zero Trust ist seine Fähigkeit, die Ressourcenentwicklung, Prozessabläufe und Sicherheit zu verteilen und zu skalieren. Doch das ist gleichzeitig auch seine Schwäche, weil sich nicht alles so einfach verteilen lässt. Um den Benutzerkomfort über Single Sign-on und Self-Services zu erhöhen, ist eine Form der zentralen Identitäts- und Zugriffsverwaltung erforderlich. Um die Sicherheit zu gewährleisten, ist eine Form der zentralen Verwaltung erforderlich. Zudem müssen Unternehmen die Fähigkeit behalten auch Legacy-Anwendungen zu betreiben, die nicht geeignet sind, in Zero-Trust-Architekturen integriert zu werden.

Identitäts- und Zugriffsverwaltung als zentraler Service

Die Identitäts- und Zugriffsverwaltung (Identity and Access Management, IAM) ist eine Kernfunktion für viele Unternehmen, die stets der erste Dienst ist, den bestehende und potenzielle Kunden sehen, wenn sie mit dem Unternehmensangebot interagieren. Das IAM ist immer ein zentraler Bestandteil der Benutzererfahrung und erlaubt einen nicht zu unterschätzenden Komfort. Eine zentrale Lösung für alle Anwendungen und Dienste ist die einzige sinnvolle Methode, um dies zu erreichen.

Die Integration eines bereits vorhandenen IAM in eine Lösung für die Perimetersicherheit (API-Gateway, Firewall für Webanwendungen) hat Vorteile für beide Seiten. Für alle gefährdeten Dienste oder Anwendungen kann die Entscheidung, ob Anfragen authentifiziert werden müssen oder nicht, bereits am Perimeter durchgesetzt werden. Die Komplexität mehrfacher Authentifizierungsmethoden ist von den Geschäftsdiensten losgelöst. Sie interagieren erst mit den Kunden, wenn diese vollständig authentifiziert sind. Die Authentifizierung funktioniert für alle Dienste, die berechtigt sind, Authentifizierungs-

daten abzufragen. Selbstregistrierung, Self-Services, Passwortzurücksetzung sind alles Funktionen, die ein modernes IAM für Benutzer bereitstellt, ohne dass ein Geschäftsdienst sie noch einmal implementieren muss.

Trennen Sie sich nicht vom zentralen Gateway

Die Erhaltung eines API-Gateways am Perimeter bringt weitere Vorteile. Die Entscheidung, ob ein Dienst oder eine Anwendung für die Aussenwelt geöffnet wird, kann weiterhin am Perimeter getroffen werden. Bewährte Change-Management-Prozesse sind nicht überflüssig. Sie behandeln nun die wirklich wichtigen Entscheidungen, anstatt im Tagesgeschäft jedes einzelnen Dienstes verloren zu gehen.

Intrusion Detection und Intrusion Prevention Systeme sind ein weiteres Beispiel für nützliche Technologie, die von einer starken Netzwerksegmentierung profitiert. Die Sammlung der Netzwerkdaten zur Analyse von Datenverkehrsmustern, um nach Abweichungen zu suchen, ist von zentralen Zugriffspunkten aus einfacher.

Zero Trust ist eine Reise

Der Wechsel zu einer Zero Trust-Architektur geschieht nicht über Nacht. Er benötigt Zeit, Aufwand und Geld. Er betrifft nicht nur die Technologie, sondern erfordert auch organisatorische Veränderungen, um alle potenziellen Vorteile möglichst gut auszuschöpfen. Das klingt sehr viel komplizierter, als es eigentlich ist, weil der Weg zu Zero Trust nach und nach in einfachen Schritten zurückgelegt werden kann.

Zentraler Punkt für die stufenweise Migration ist das API-Gateway der Perimetersicherheit. Es wird nicht ersetzt, sondern genutzt, um Sicherheitsaufgaben zwischen Perimeter und neu eingeführten Microgateways zu verteilen. Es wird weiterhin sicherstellen, dass nur die Dienste offen stehen, die dafür freigegeben wurden. Das API-Gateway am Perimeter wird eine allgemeine Zugriffskontrolle zu den geschützten Diensten sicherstellen und schliesslich die Authentifizierung für die Dienste durchsetzen. Die Microgateways werden Verantwortung für die feingranulare Filterung aller Anfragen übernehmen und auf der Basis der vom IAM-System gelieferten Identitätsdaten den Zugriff auf die Geschäftsressource erlauben oder verweigern. Auf diese Weise kann die Anzahl der durch ein Microgateway geschützten Geschäftsdienste bei Bedarf erweitert werden.

Das API-Gateway, das die Perimetersicherheit gewährleistet, wird ebenfalls zentraler Punkt für die neue Organisation sein. Jeder Change-Management-Prozess, der vorhanden ist, um Veränderungen am Perimeter zu prüfen und zu genehmigen, bleibt bestehen. Die vorhandene Dienstinfrastruktur bleibt weiterhin ein wichtiger Teil des gesamten Dienstangebots und muss auf dem weiteren Weg zu Zero Trust gepflegt werden. Change-Management-Prozesse müssen angepasst werden, um die neuen Paradigmen aufzunehmen. In einer verteilten Architektur muss die zentrale Autorität sicherstellen, dass Rechte und Pflichten, die an ein für einen Geschäftsdienst verantwortliches DevOps-Team delegiert werden, gut gesteuert werden. Die Prüfung umfasst sowohl techni-

sche als auch organisatorische Aspekte, damit die Einrichtung, Kontrolle und Steuerung des Microgateways, das den eigentlichen Geschäftsdienst schützt, alle Anforderungen während des gesamten Lebenszyklus des Dienstes erfüllt. DevOps-Teams werden auf die Unterstützung von Sicherheitsexperten zählen können, die ihnen helfen, ihren jeweiligen Anwendungsverantwortlichen einen sicheren Unternehmenswert zu liefern. Und diese Zusammenarbeit zum Erreichen gemeinsamer Geschäftsziele ist genau der Kern der DevSecOps-Transformation: die proaktive Unterstützung der internen Teams mit Fachkenntnis und Tools, damit diese ihre Ziele schneller und mit weniger Risiken erreichen können – eine Win-Win-Situation für das gesamte Unternehmen.

Schlussfolgerung

Die Tage, als Zero Trust-Architekturen, Cloud-Implementierungen und Microgateways das Revier von kleinen Startups mit einfachen Setups waren, sind vorbei. Das gilt aber auch für die reine Perimetersicherheit. Das Zero Trust-Paradigma erfordert Veränderungen im Unternehmen sowie neue Tools wie Microgateways zur Implementierung. Auch erfordert es viel Aufwand, bis ein grosses Unternehmensnetzwerk migriert ist. Die bestehenden Lösungen für die Perimetersicherheit werden nicht ersetzt. Ihre Funktion wird von lediglich von einer Alltagsrolle auf eine strategische Position im gesamten Verteidigungssystem aufgewertet. Die Vorteile, die ein Unternehmen mit einer Zero Trust-Architektur sowohl technisch als auch betrieblich gewinnt, sind enorm. Vielleicht ist jetzt der Zeitpunkt gekommen, um das erste Projekt zu beginnen und den ersten Schritt in Richtung Zero Trust zu gehen. Sprechen wir darüber.

Autoren

Aarno Aukio

CTO & Partner VSHN AG

Traumberuf Software Operations Engineering – damit hat Aarno gestartet und daraus in 6 Jahren die VSHN (ausgesprochen vɪʒn wie «vision») mit 45 Mitarbeitern aufgebaut. Als erster Schweizer Kubernetes Certified Service Provider und führender Partner für DevOps, Docker, Kubernetes, OpenShift, Rancher & 24/7 Cloud Operations. Als Open Source Unternehmen sind nicht nur Sourcecode sondern auch Servicedefinitionen öffentlich verfügbar und verkörpern die Kernwerte des Unternehmens: Offenheit, Kollaboration und Verantwortung übernehmen (wie im öffentlichen Mitarbeiterhandbuch unter https://handbook.vshn.ch/hb/values.html dokumentiert).

Michael Doujak

Product Manager Airlock

Michael Doujak hat nach seinem Studium an der ETH Zürich verschiedene Stationen durchlaufen. Seit 20 Jahren hat er verschiedene Projekte und Lösungen im Bereich von Identity Management geplant und umgesetzt. Besonders herauszustreichen ist der Aufbau von SwissSign als Herausgeber von qualifizierten Zertifikaten in der Schweiz, der Aufbau der Patientendossier Plattform «MonDossierMedical», der Aufbau der EPD Infrastruktur und der Zuweiser Plattform Lösung der Schweizerischen Post. Er ist ein profunder Kenner der Materie, von der tiefen Technik bis in die geschäftlichen Anwendungsfälle hinauf. Michael Doujak ist heute als Product Manager für Airlock bei Ergon Informatik tätig.