IT-Security für den Swisseldex-Datahub

Sicherheit von Anfang an | Bei der Entwicklung des Swisseldex-Datahubs wurden die IT-Security und die Zuverlässigkeit der Applikation von Anfang an berücksichtigt. Das detaillierte Security Konzept wurde extern reviewt und nach Abschluss wurde die Plattform einem Penetration-Test unterzogen.

GUIDO SANTNER ET AL.

Der Swisseldex-Datahub ist eine Plattform der Energiebranche, über die Stromlieferanten, Netzbetreiber und andere Marktteilnehmer Daten austauschen können, sogenannte SDAT-Nachrichten. Das sind zum Beispiel Messdaten von Stromzählern (Routing-Funktionalität). Der Datahub beinhaltet auch ein Verzeichnis aller Stromzähler, das sogenannte Messpunktregister, worin definiert ist, wer der Netzbetreiber und wer der Stromlieferant eines Endverbrauchers ist. Auf diesem Messpunktregister können automatisierte Wechselprozesse ausgeführt werden, beispielsweise wenn ein Endverbraucher seinen Stromlieferanten wechselt. Durch diese SDAT-konforme Automatisierung lassen sich Fehler und Missverständnisse vermeiden. In Zukunft kann der Datahub gemäss den Anforderungen im Mantelerlass erweitert werden und auch Energiedaten der Messpunkte auf dem Datahub speichern.

Der Austausch von SDAT-Nachrichten ist seit April 2020 über die Swisseldex-Plattform möglich. Mittlerweile können Messdaten aus 90 % des Verteilnetzgebiets der Schweiz über die Plattform geroutet werden, und es werden wöchentlich rund 60 000 Nachrichten ausgetauscht – Tendenz steigend. Wechselprozesse können seit Oktober 2021 über den Datahub abgewickelt werden. Fünf Netzbetreiber nutzen das Messpunktregister bereits für die Wechselprozesse – was rund 20 % der wechselberechtigten Messpunkte der Schweiz entspricht. Im April 2022 wurde zusätzlich der SDAT-Webclient aufgeschaltet, worüber Wechselprozesse manuell erfasst werden können. Hier werden kleinere Netzbetreiber angesprochen, für die sich der Aufwand für einen automatischen Datenaustausch (noch) nicht lohnt.

Sensible Daten

Es ist offensichtlich, dass auf dem Datahub sensible Daten von Kunden gespeichert werden, zu denen nur die berechtigten Marktteilnehmer Zugriff haben dürfen. Bei der Entwicklung der Plattform wurde deshalb von Anfang an grosser Wert auf die IT-Sicherheit und den Datenschutz gelegt.

Der Datahub soll aber nicht nur sicher, sondern auch zuverlässig laufen. Es ist eine businesskritische Appli-

Bilder: Supercomputing Systems AG; Swisseldex AG

kation, die jederzeit verfügbar sein soll. Die Server-Standorte sind deshalb geografisch redundant ausgelegt in Datenzentren in Zürich und der Westschweiz. Dass die Daten innerhalb der Schweiz bleiben müssen, war von Anfang an klar. Eine weitere Anforderung war, dass auch der Betreiber des Datahubs die Daten nicht sehen kann. Sie müssen verschlüsselt abgelegt und übertragen werden – mit individuellen Schlüsseln für jeden Netzbetreiber.

Security Development Lifecycle

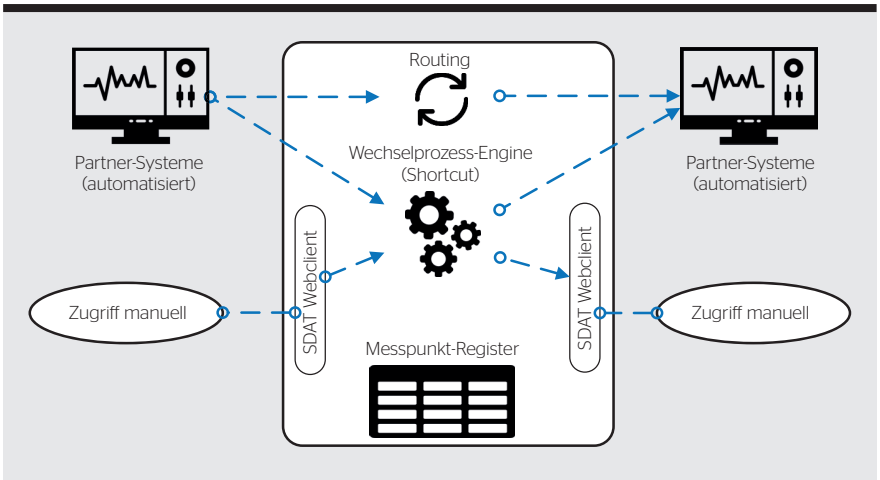
Die Entwicklung des Swisseldex-Datahubs richtete sich nach dem Microsoft Security Development Lifecycle, einem von Microsoft entwickelten Konzept, wie sichere Software entwickelt werden kann. So wird beispielsweise schon in der Planungsphase auf die Sicherheitsbelange der Software eingegangen. Es werden Bedrohungen identifiziert (z.B. via Threat Modeling) und schon während der Entwicklung entsprechende Sicherheitsmassnahmen implementiert. Dazu gehört auch, dass die Effektivität der Sicherheitsmassnahmen am Schluss beurteilt wird.

IT-Security-Konzept

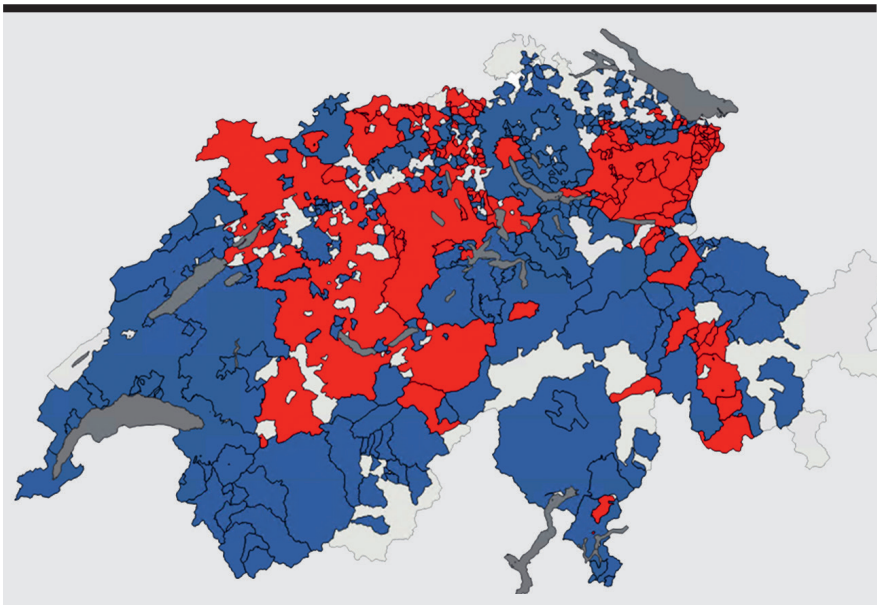
Zu Beginn des Projekts wurde ein detailliertes IT-Security-Konzept erstellt und durch eine externe Firma reviewt. Ein erneutes Review folgte am Ende der Entwicklung. Zusätzlich wurde die Software von der externen Firma auf Sicherheitslücken getestet.
Auf eine Business-Value-Analyse musste bei diesem Projekt verzichtet werden. Hier geht es darum, wie gross ein Schaden finanziell sein könnte. So wäre es möglich abzuschätzen, welcher Aufwand sich lohnt, um die Software sicher zu machen. Aufgrund der sensiblen Daten und der verschiedenen Marktteilnehmer auf der Swisseldex-Plattform war von Anfang an klar, dass die Sicherheit eine hohe Relevanz hat.

Microservice-Architektur

Als Plattform für den Datahub wurde eine Microservice-Architektur auf der Azure Cloud gewählt. Microservice-Architektur bedeutet, dass die Anwendung in eine Reihe von unabhängigen Services aufgeteilt wird. Diese kommunizieren über schlanke APIs (Schnittstellen) miteinander. Dies hat den Vorteil, dass mehrere Entwickler unabhängig voneinander ihre Services programmieren und damit parallel am Projekt arbeiten können. Ein weiterer Vorteil ist die Unterstützung des Least Privilege. Wenn ein Microservice je eine Lücke aufweisen sollte, ist nur ein Teil der Applikation kompromittiert.



Über den Datahub werden Messdaten ausgetauscht und Wechselprozesse von Kunden koordiniert.



90 % der Anschlüsse (rot und blau) sind über den Swisseldex-Datahub erreichbar.

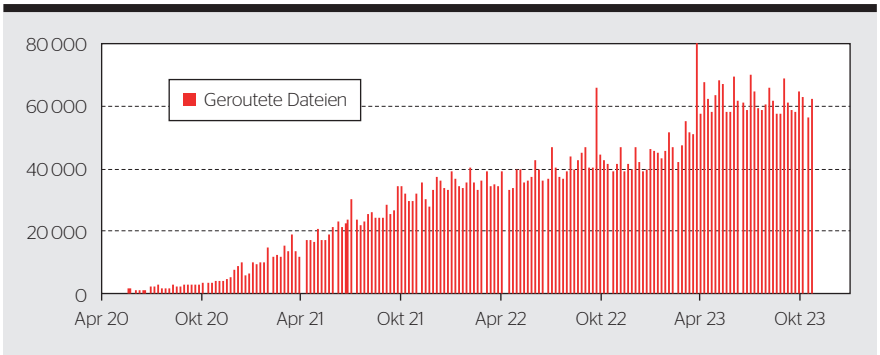
Threat Modeling

Beim Threat Modeling wird das Design der Plattform systematisch darauf geprüft, ob und wo Schwachstellen sind, die unter Umständen von Angreifern ausgenutzt werden könnten. Anschliessend werden Sicherheitsmassnahmen identifiziert und implementiert, um diese Schwachstellen zu beseitigen.

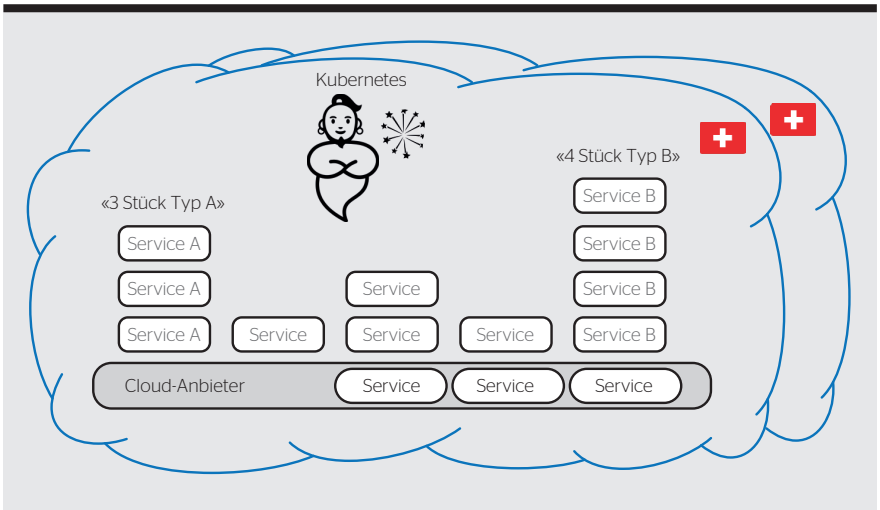
Typische Angriffe und dazugehörige Gegenmassnahmen sind:

- Spoofing > Authenticity
- Tampering > Integrity
- Repudiation > Non-repudiability
- Information disclosure > Confidentiality
- Denial of service > Availability
- Elevation of privilege > Authorization

Beim Spoofing täuscht der Angreifer eine Identität vor. Er versucht, Authentifizierungs- und Identifikationsverfahren zu untergraben. Beim Tampering versucht ein Angreifer, Daten zu modifizieren, um an sensible Daten zu kommen. Repudiation bedeutet wiederum, dass ein Angreifer oder auch ein legitimer Nutzer Aktionen durch-



Das Datenvolumen über den Hub steigt stetig an – entsprechend wichtig ist der zuverlässige Betrieb des Datahubs.



Deklarative Cloud-Infrastruktur mit Kubernetes und Docker für eine hohe Verfügbarkeit und Updates im laufenden Betrieb.

führt, die nachträglich nicht mehr dem Verursacher zugeordnet werden können.

Information Disclosure wird auch Information Leakage genannt – wenn sensible oder private Daten in falsche Hände geraten. Dies kann ein Programmierfehler sein oder ein Angreifer, der die Software bewusst manipuliert und damit Daten abgreift.

Bei einer Denial-of-Service-Attacke versuchen Angreifer, die Verfügbarkeit des Service zu beeinträchtigen oder sogar zu verhindern. So kann der Server die echten Anfragen nicht mehr beantworten. Bei einer Elevation of Privilege versucht ein Angreifer, seine Privilegien zu erhöhen, um in sensible Bereiche einzudringen.

Vulnerability Management

100 % Sicherheit gibt es nicht. Auch im Betrieb muss ständig überwacht werden, ob neue Sicherheitslücken bekannt werden und ob die Plattform angegriffen wird. Dazu werden die Infrastruktur und alle Microservices und ihre Abhängigkeiten regelmässig auf neu bekannt gewordene Schwachstellen geprüft. Wird eine solche Schwachstelle detektiert, wird deren Auswirkung auf das System analysiert und gegebenenfalls beseitigt.

Identitäts- und Accessmanagement

Ein wichtiges Element für den sicheren Datahub ist ein durchdachtes Benutzerkonzept. Alle registrierten natürlichen Personen müssen sich mit 2-Faktor-Authentifizierung anmelden. Dazu gehört ein mehrstufiges Identitäts- und Accessmanagement (IAM).

Sämtliche Daten werden verschlüsselt übertragen und gespeichert – innerhalb und ausserhalb der Cloud Services. Dazu werden verbreitete Protokolle wie FTPS und HTTPS genutzt (Vorgabe von SDAT-CH). Alle gespeicherten Daten werden abhängig vom Marktpartner verschlüsselt. Selbst Swisseldex oder SCS als Betreiber der Plattform haben keinen Zugriff auf die Daten.

Datahub in der Cloud

Der Entscheid, den Datahub in einer Cloud zu betreiben, lag vor allem am hohen Anspruch an die Verfügbarkeit, der Skalierbarkeit und den Kosten. Ein eigenes Datacenter oder eigene Server in Datacentern hätten zwar den Vorteil, dass man als Betreiber die volle Kontrolle hat. Für Betrieb und Wartung wäre jedoch der physische Zugang nötig, beispielsweise um Updates der Firmware von Routern einzuspielen.

Da Cloud-Anbieter auf diesen Service spezialisiert sind, ist die Verfügbarkeit sehr hoch. Zudem lässt sich die Anwendung gut skalieren.

Container Images

Der Datahub läuft als verschiedene Services in der Azure Cloud. Die Services werden als sogenannte Container Images verpackt. Diese Images enthalten sowohl die Anwendung wie auch die dazu nötigen Bibliotheken und Treiber. Über die Software Kubernetes werden die Container verwaltet. Kubernetes fasst einen oder mehrere Container zu einem Pod zusammen. Je nach Last werden zusätzlich Pods gestartet. So skaliert die Anwendung mit der anfallenden Last. Der Datahub wurde erfolgreich für den Vollausbau mit 5 Mio. Messpunkten bezüglich Leistungsfähigkeit getestet.

Sichere Container

Container sind mit einer sehr leichtgewichtigen VM (virtuellen Maschine) vergleichbar. Jeder Container läuft in seinem eigenen Kontext und enthält alle notwendigen Abhängigkeiten, um ausgeführt werden zu können. Besteht eine Sicherheitslücke im Container, ist nicht gleich die gesamte Applikation betroffen, sondern nur der Microservice im Container selbst.

Ein entscheidender Punkt für die Sicherheit der Applikation: Container Images sind unveränderbar und können signiert werden. Dadurch hat eine persistente Malware wenig Möglichkeiten, das System zu befallen.

Datenhoheit

Dem gesetzlichen Datenschutz unterworfen sind grundsätzlich die perso-

nenbezogenen Daten auf dem Datahub, d.h. es geht um den Schutz der Privatsphäre von Personen. Hinzu kommen Daten, welche von den involvierten Organisationen und Firmen als Geschäftsgeheimnisse gehandhabt werden, beispielsweise Kundenbeziehungen. Diese beiden Datenarten werden auf dem Datahub gleich gut und stark geschützt. Der Zugriff wird durch ein klar definiertes Rechtemanagement geregelt. So sieht der Verteilnetzbetreiber nur seine eigenen Messpunkte mit den zugehörigen Daten. Die Lieferanten sehen nur die Messpunkte ihrer Kunden und nur die Daten der Zeitperiode, in der sie den Kunden beliefern und somit eine Geschäftsbeziehung besteht. Der Betreiber des Datahubs (SCS) hat keinen Zugriff auf die Daten.

Bald auch Energiedaten?

Der Swisseldex-Datahub fokussiert bis anhin auf Wechselprozesse sowie das Routing von SDAT-Nachrichten. Der Datahub kann erweitert werden mit den Funktionalitäten der Datenplattform gemäss Mantelerlass. Ein Teil dieser Funktionalitäten bedingt die zentrale Speicherung von Energiedaten. Der Swisseldex-Datahub ist eine Vorstufe davon und kann bei Bedarf entsprechend erweitert werden. Der neue Use Case Kontingentierung von Grossverbrauchern im Fall einer Strommangellage geht bereits in diese Richtung. Der Bundesrat würde als Eskalationsstufe im Bereitschaftsgrad 4 individuelle Kontingente für alle Grossverbraucher verfügen, wobei Firmen mit mehreren Standorten (sog. Multi-Site-Verbraucher) ihr Kontingent gesamthaft erfüllen dürfen. Firmen können mit einem Account auf dem Datahub die Übersicht über alle ihre Standorte halten, auch verteilnetzübergreifend für diejenigen Verteilnetze, für welche die Verteilnetzbetreiber die effektiven Verbrauchsdaten tagesaktuell anliefern. Mit diesem Use Case wird der Datahub erstmals zum Messdatenspeicher.

Autoren

Guido Santner ist Marketingverantwortlicher bei SCS.
→ Supercomputing Systems AG, 8005 Zürich
→ guido.santner@scs.ch

Maurus Bachmann ist CEO von Swisseldex.
→ Swisseldex AG, 3011 Bern
→ maurus.bachmann@swisseldex.ch

Torben Griebe ist Lead Information Security Expert bei SCS.
→ torben.griebe@scs.ch

Matthias Oster ist Projektleiter bei SCS.
→ matthias.oster@scs.ch

Stephan Moser ist Department Head Energy Systems & Public Safety bei SCS.
→ stephan.moser@scs.ch

RÉSUMÉ

Sécurité informatique pour le Swisseldex Datahub

La sécurité dès le départ

Le Swisseldex Datahub est une plateforme du secteur de l'énergie qui permet aux fournisseurs d'électricité, aux gestionnaires de réseau et à d'autres acteurs du marché d'échanger des données – les fameux messages SDAT. Il s'agit là par exemple de données de mesure de compteurs d'électricité. Le Datahub contient un registre de tous les compteurs d'électricité – appelé registre des points de mesure – qui définit qui est le gestionnaire de réseau et qui est le fournisseur d'électricité d'un consommateur final. Des processus de changements automatisés peuvent être exécutés sur ce registre, par exemple lorsqu'un consommateur final change de fournisseur d'électricité. Cette automatisation conforme au SDAT (Standardisierter Datenaustausch für den Strommarkt Schweiz, échange de données standardisé pour le marché du courant) permet d'éviter les erreurs et les malentendus. À l'avenir, le Datahub pourra être étendu conformément aux exigences de l'acte modificateur unique (Mantelerlass) et enregistrer également les données énergétiques des points de mesure sur le Datahub.

L'échange de messages SDAT est possible depuis avril 2020 via la plateforme Swisseldex. Entre-temps, les données de mesure de 90 % du domaine du réseau de distribution suisse peuvent être acheminées via la plateforme, et environ 60 000 messages sont échangés chaque semaine – avec une tendance à la hausse. Les processus de changements peuvent être traités via le Datahub depuis octobre 2021. Cinq gestionnaires de réseau utilisent déjà le registre des points de mesure pour les processus de changements – ce qui correspond à environ 20 % des points de mesure autorisés à changer de fournisseur en Suisse. Le SDAT-Webclient a en outre été mis en service en avril 2022. Celui-ci permet de saisir manuellement les processus de changements, et est essentiellement destiné aux petits exploitants de réseau, pour lesquels le passage à un échange automatique de données ne vaut pas (encore) la peine.

La sécurité informatique et la fiabilité de l'application ont été prises en compte dès le début du développement du Swisseldex Datahub. Le concept de sécurité détaillé a été contrôlé par des experts externes et, une fois terminée, la plateforme a été soumise à un test d'intrusion afin de pouvoir garantir une sécurité maximale.