In Zusammenarbeit mit

aws PARTNER Premier Tier Services

Fallstudie

AWS Sicherheits Architektur für T-Mobile NL

Zusammenfassung

T-Mobile Netherlands (TMNL), das größte niederländische Mobilfunkunternehmen, das drahtlose Daten- und Sprachkommunikationsdienste anbietet, war auf der Suche nach einer neuen AWS Landing Zone Lösung, die alle bestehenden kritischen Systeme und Konten in AWS sichert.

T-Systems leistete Support, um einen Cloud-nativen Ansatz für die Sicherheit zu entwickeln. Die wichtigsten Erfolgsfaktoren waren Wartungsfreundlichkeit, Automatisierung, Erweiterbarkeit und Zuverlässigkeit sowie zentralisierte Sicherheitsprotokolle, Überwachung und Audits. Die Zielsetzung des Projekts umfasste die detaillierte Planung, das Design und die Umsetzung der sicheren AWS Landing Zone unter Verwendung von Infrastructure-as-Code (IaC) und der integrierten, zentralisierten Sicherheitsverwaltung in einer Multi-Account-Umgebung.

Über T-Mobile NL

T-Mobile Netherlands ist mit mehr als 5,7 Millionen Kunden, der größte Telekommunikationsanbieter in den Niederlanden, der sich auf die Bereitstellung kostengünstiger und hochwertiger Lösungen für die Mobil- und Breitbandkommunikation konzentriert. Das Unternehmen bietet Mobiltelefone und -tarife, Internetdienste, Applikationen, gebündelte Pakete sowie andere bezogene Produkte und Dienste an.

Die Herausforderung

Als Telekommunikationsanbieter gab es zahlreiche Anforderungen, die bei der Einrichtung der neuen Lösung berücksichtigt werden mussten:

1. Netzwerkeinrichtung, um eine sichere Verbindung vom T-Mobile NL-Rechenzentrum über das Internet zu den Applikationen zu ermöglichen.
2. Zentralisierte Überwachung und Alarmierung in allen Unternehmen: T-Mobile NL benötigte eine Gesamtsicht, um die Sicherheitslage des Unternehmens zu überblicken und Sicherheitsvorfälle zu verwalten.
3. Strenge Anforderungen an Datenschutz und Datenhaltung: Ausschließlich in der EU.
4. Zentralisierte Sicherheitsverwaltung und Einsatz: Alle Sicherheitsmittel und -lösungen sollten zentral eingesetzt und verwaltet werden.
5. Erkennung von Missbrauch und Anomalien durch strenge Kostenkontrollen: Benachrichtigung über eventuelle Unstimmigkeiten und Muster.

T · · Systems ·

Let's power higher performance

Lösungsarchitektur

T-Systems wurde als AWS Premier Consulting Partner ausgewählt, um die Lösung zu entwickeln, über die beste Vorgehensweise für die Nutzung von AWS zu beraten und diese im Rahmen des Projekts umzusetzen. T-Systems erstellte gemeinsam mit T-Mobile NL einen Projektplan, legte Meilensteine fest, verhandelte Prioritäten und führte die Umsetzung und Tests durch. T-Systems vollzog die Umstellung von einer klassisch automatisierten Kontobereitstellung zu einer neuen, vollständig verwalteten und gesicherten Landing Zone. Der erste Meilenstein war der Aufbau eines überarbeiteten Multi-Account-Setups, das aus verschiedenen Organisationseinheiten bestand, auf die je nach Account Typ und -Zweck unterschiedliche Service Control Policies angewendet wurden. Die Infrastruktur wurde vollständig automatisiert entwickelt und bereitgestellt. Für die nahtlose Bereitstellung kam Terraform als Infrastruktur-as-Code-Tool zum Einsatz.

Präventive Kontrollen

Nach der initialen organisatorischen Einrichtung und Bereitstellung der Accounts, wurden **Service Control Policies** eingesetzt, um die **Anforderungen an den Datenschutz** und die **Datenhaltung** zu erfüllen. Für **Regionale Beschränkungen** wurden Service-Kontrollrichtlinien angewendet, wodurch sichergestellt wurde, dass die Daten und der Zugriff nur in der angegebenen Region erfolgen. Zudem wurden Restriktionen für die Entwicklung von Ressourcen eingesetzt, die nicht über die **erforderlichen Kennzeichnung** verfügen, um Kosten unter Kontrolle zu halten und die Sicherheit zu erhöhen.

Alle Accounts sind mit dem Azure Active Directory von T-Mobile NL verbunden und bieten **Single-Sign-On**-Funktionalität an, sodass Benutzer mit der AWS-Konsole und der CLI interagieren können.

Zusätzlich zu den Dienstkontrollrichtlinien wurde **AWS Config** so konfiguriert, dass es Anforderungen vom Privacy and Security Assessment (PSA) erfüllte. Zahlreiche Regeln werden konfiguriert und bei Nichteinhaltung automatisch korrigiert.

Der Kunde erhält einen vollständig automatisierten Prozess für eine konforme Architektur und die proaktive Verwaltung von Konfigurationsproblemen.
Als Teil der Anforderungen, werden definierte Compliance Regeln mithilfe AWS Config analysiert und bei **Nichteinhaltung behoben**.

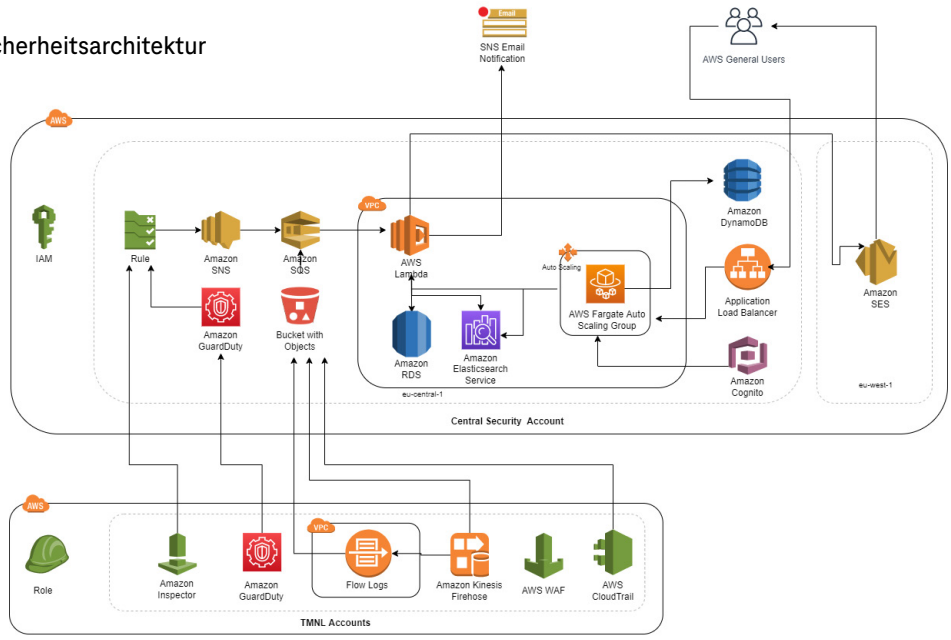
Durch die Umsetzung dieser Regeln kann T-Mobile NL jede Regel-Abweichung schnell erkennen und die meisten Probleme automatisch beheben. Wöchentliche Berichte über die Einhaltung der Vorschriften werden an T-Mobile NL übermittelt. Die Daten zum Compliance Status werden an die zentrale Überwachungslösung weitergeleitet, damit T-Mobile NL ihn visualisieren und in Fällen, in denen keine automatische Behebung vereinbart wurde, die nötigen Maßnahmen treffen kann.

Zentralisierte Sicherheitsanalyse und Dashboard

Protokolle von allen Konten (Cloudtrail, Config, Guard Duty, VPC Flow Protokolle, Inspector) werden an einen zentralen SecDevOps-Account gesendet und dann in einem **zentralen Dashboard** auf Basis von Grafana analysiert und visualisiert. Sicherheitsvorfälle werden gemäß dem Incident Management Prozess von T-Mobile NL verwaltet und an das Betriebs-Ticketing-Tool gesendet.

Technisch gesehen wird jedes Mal, wenn ein neuer Protokolleintrag erfolgt, eine SQS-Warteschlange ausgelöst, die eine Lambda-Funktion „Log-Aggregator“ aufruft und speichert Protokollen in Elasticsearch und Aurora DB. Die Lambda-Funktion ist außerdem so konfiguriert, dass sie Probleme sofort erfasst und das Betriebsteam benachrichtigt. In ähnlicher Weise kann die automatische Behebung, eine separate Lambda-Funktion, auf Basis von bestimmter Filter ausgelöst werden.

Zentralisierte Sicherheitsarchitektur



Verbesserte Sicherheit

Mit dieser Lösung hat T-Mobile NL einen zentralen Überblick der Sicherheitslage geschaffen und die folgenden Vorteile erzielt:

Sicherheitsrichtlinien und -standards
Verfolgung von Informations-sicherheitsrichtlinien und -standards und Sicherstellung, dass die IT-Systeme die Richtlinien und Standards einhalten. Alarmierung bei Verstößen in Echtzeit.

Netzwerksicherheit Überwachung von Alarmierungen durch Cloudtrail, VPC Flow-Protokolle Guarduty und WAF usw. und Identifizierung bekannter Angriffsmuster im Netzwerkverkehr.

Zugriff und Authentifizierung
Überwachung der Erstellung von Konten, Änderungsanfragen und Aktivitäten von Benutzern.

Protokollüberwachung - Aggregation von Sicherheitsvorfällen und Alarmierung bei ungültigen Anmeldeversuchen, Port-Scans, Eskalierungen Privilegs usw.

Aufgabentrennung – Anwendung von Richtlinien gemäß Least-Privilege-Prinzip und Single-Sign-On

Identity Federation - Nahtlose Anmeldung durch die Nutzung von Unternehmensanmeldedaten

Deshalb Amazon Web Services

AWS bietet noch mehr Skalierbarkeit, höhere Zuverlässigkeit, schnellere Markteinführung und die Möglichkeit, Innovationen voranzutreiben. Von Entwicklern für Entwickler entwickelt, um schnell und nahtlos skalierbare, sichere Infrastrukturen bereitzustellen. Diese Funktionen ermöglichen es Entwicklern und Unternehmen, sich auf die Verbesserung und Innovation ihrer Anwendungen zu konzentrieren, anstatt sich um die Erstellung und Ausführung der Identität zu kümmern.

AWS betrachtet Sicherheit als Job Zero und bietet integrierte Sicherheitsservices sowie bewährte Verfahren für die Cloud-Sicherheit im AWS CAF, AWS Security Incidence Response Guide, und Well-Architected Framework.

Unternehmensprofil

Mit Standorten in mehr als 20 Ländern ist T-Systems einer der weltweit führenden, herstellerunabhängigen Anbieter digitaler Dienstleistungen mit Hauptsitz in Europa. Das Tochterunternehmen der Deutschen Telekom bietet alles aus einer Hand: vom sicheren Betrieb von Legacy-Systemen und klassischen ICT-Services über den Übergang zu Cloud-basierten Diensten bis hin zu neuen Geschäftsmodellen und Innovationsprojekten im Internet der Dinge. T-Systems ist auch ein akkreditierter AWS Managed Service Provider und Premier Consulting Partner mit mehr als 500 Experten in AWS und Kompetenzen wie AWS Migration, SAP Services, Well-Architected und Direct Connect.

In Zusammenarbeit mit

aws PARTNER Premier Tier Services

Kontakt

T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main, Deutschland
Tel: 00800 33 090300
E-Mail: info@t-systems.com
Internet: www.t-systems.com

Herausgeber

T-Systems International GmbH
Marketing
Hahnstraße 43d
60528 Frankfurt am Main, Deutschland

T · · Systems ·

Let's power higher performance

Letzte Aktualisierung: 03/2022 | Entworfen: Creative Factory, TSIN