NetEye User Group 2023

SALZBURG AG

Gerfried Schweiger

NetEye:

Die Rundum-Lösung für IT/OT/TK-Überwachung und Analyse

Portrait Salzburg AG

NetEye User Group 2023

SALZBURG AG

Gerfried Schweiger

Heute

- **Produkte und Dienstleistungen**:
  - Nachhaltige, vernetzte und komfortable Lösungen in den Bereichen Energie, Mobilität und Kommunikation
- **Zusammenarbeit mit der Salzburg Netz GmbH:**
  - Rund 2.400 Mitarbeiter im ganzen Bundesland Salzburg
  - Bereitstellung von Strom, Wasser, Wärme, Internet, Fernsehen und Telefon
  - Sicherer Nahverkehr durch Obusse und Lokalbahnen für die Salzburgerinnen und Salzburger

Portrait Salzburg AG

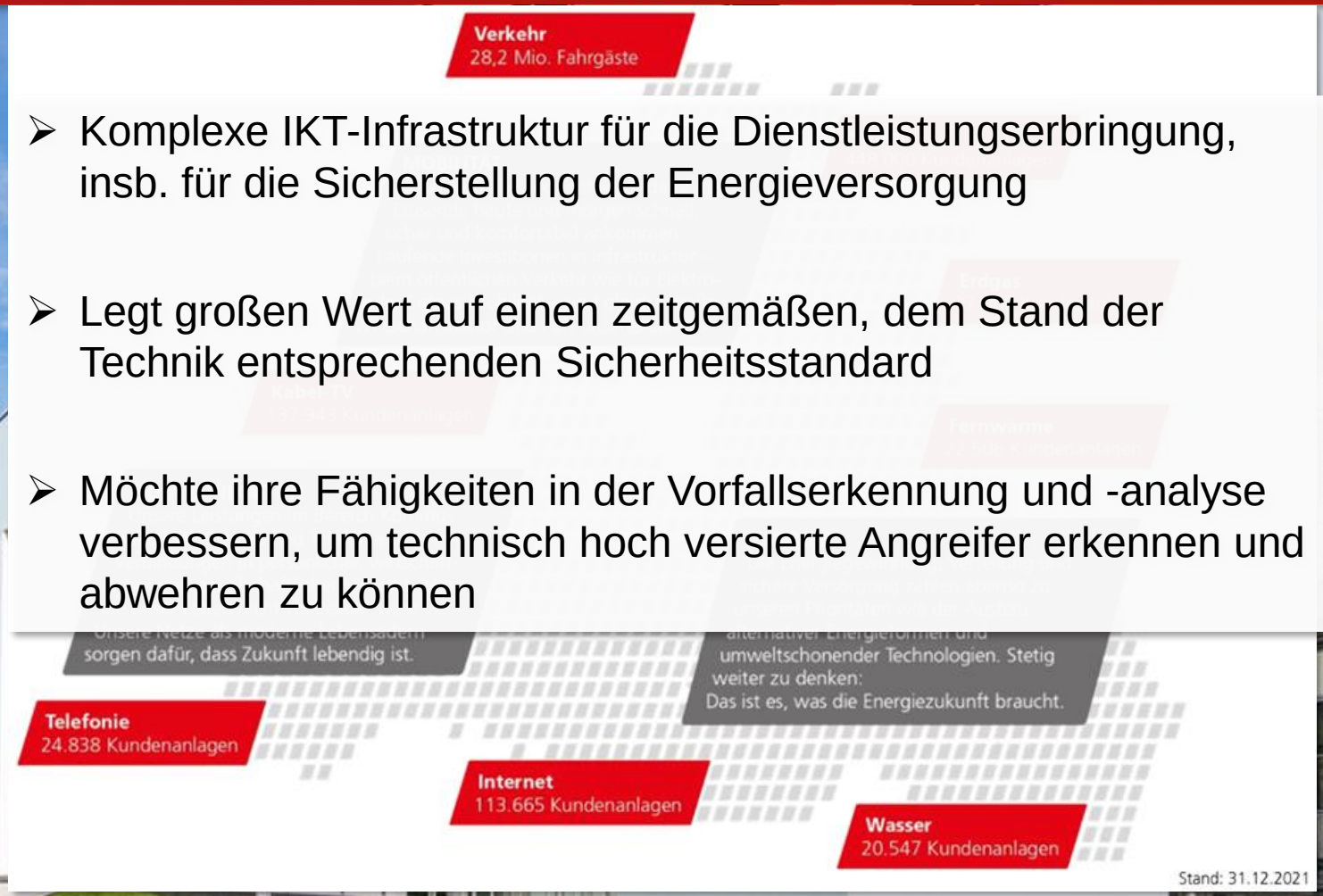
NetEye User Group 2023

SALZBURG AG

Gerfried Schweiger

Überblick über die verschiedenen Tätigkeitsbereiche und Anzahl der Kundenanlagen

- Komplexe IKT-Infrastruktur für die Dienstleistungserbringung, insb. für die Sicherstellung der Energieversorgung
- Legt großen Wert auf einen zeitgemäßen, dem Stand der Technik entsprechenden Sicherheitsstandard
- Möchte ihre Fähigkeiten in der Vorfallserkennung und -analyse verbessern, um technisch hoch versierte Angreifer erkennen und abwehren zu können



NetEye User Group 2023

SALZBURG AG

Gerfried Schweiger

Portrait
Schweiger Gerfried

BJ 1975

- Analytisches Denken (Ursachenanalyse)
- über den Tellerrand blicken
- genau

+

4 Kinder
(21, 7, 6)
& Lotti (8 Monate)

Kommunikation −

MSc

Seit 2019 in der Salzburg AG

Über 20 Jahre Selbstständigkeit im Bereich Telekommunikation und Netzwerktechnik

Aufgaben:
Notfallpläne, ServiceDesk, CMDB, NetEye, ISO27001, NISG, SOC/SIEM

SALZBURG AG
Gerfried Schweiger

Ausgangslage Telekom Technologies

1. **Unzählige dezentrale Monitoring**
   Jedes operative Team verfügt über eine eigene Monitoring-Lösung für seine Geräte, zum Beispiel LWL, KOAX und FUNK

2. **Kein zentrales Logmanagement**
   In den operativen Teams existieren jeweils separate Datensammlungen, eine Gesamtsicht ist nicht möglich

3. **Externe Anbieter**
   Dienstleister überwachen die von uns eingekauften Services und tragen letztendlich das Risiko. Allerdings erhalten wir nur rudimentäre Berichte

4. **Private Cloud**
   Viele unserer Services werden in einer privaten Cloud von einem Tochterunternehmen betrieben, shared root ist kaum möglich

5. **Interne IT geht in die Cloud, die OT nicht**
   Die 'Cloud-First'-Strategie führt zu Problemen mit der Resilienz

NetEye User Group 2023

SALZBURG AG

Gerfried Schweiger

NetEye Umsetzung so far

Monitoring OT und TK:

- TK Icinga erhält neue Hosts direkt aus der CMDB mit „standard“ Templates
- OT Icinga ist manuell gepflegt
- Koppelung an CMDB, JIRA, MAIL und SMS Gateway

~ 3800 Hosts
~ 17.000 Services

Raumsensoren

Controller liefern Daten via MQTT an Satelliten, diese Daten werden in Elastic gespeichert. Icinga kann diese Daten automatisiert aus Elastic lesen, neue Sensoren automatisch erkennen und integrieren, alarmieren, …

Logging:
Elastic nur in der TK Instanz

Logging aus der OT kommt über „Satelliten der TK“ welche in der OT stehen und nur abgehend kommunizieren dürfen
Logging auch über Elastic Agent (+WinRM Windows Logging), Filebeat, Auditbeat, Metricbeat

~80.000 Logs/min
~3GB/day

Test für Capacity Monitoring via telemetry stream

Probleme bei der automatisierten Auswertung der Kundendaten (HFC)
Aktuell werden Geräte via SNMP gecheckt

Zertifikatsmanagement

X509

NetEye User Group 2023

SALZBURG AG

Gerfried Schweiger

NetEye Wohin geht die Reise?

JIRA-Koppelung bidirektional

Wartungen müssen aus dem Wartungskalender in die Maintenance in Icinga geschoben werden

SNMP Trap Integration

Viele Assets schicken Traps, diese müssen am Asset dargestellt und wenn notwendig eine Benachrichtigung getriggert werden

Echtzeit Monitoring der CORE-Netzwerkkomponenten

CISCO, CIENA, …

Darstellung

Räume und Verbindungen müssen grafisch abgebildet werden

SIEM für die OT / TK

Erweitertes use case Design und Implementierung

NetEye User Group 2023

SALZBURG AG

Gerfried Schweiger

Vielen Dank!

Diskussion

Fragen