DI Dietmar Wieland
SVD Geschäftsführer

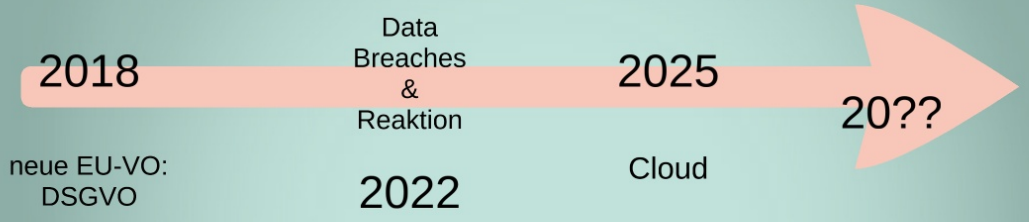
Stefan Höller, BA
SVD CISO

11/10/2022

Wer wir sind:

- 500 MitarbeiterInnen
- 10.000 Clients
- 2.000 Server
- 2 Rechenzentren

Herausforderungen



neue EU-VO:
DSGVO

2022

Cloud

- **Dienstleister der SV**
- **öffentliche Verwaltung**
- **technische Neuerungen**

Planung

Was? Warum? Wie?

- Vertraulichkeit
- Verfügbarkeit
- Integrität

Daten - das neue Gold

- ISMS / Richtlinien - gültig für **alle** im Unternehmen
- interne Audits
- Risikomanagement
- techn. Werkzeuge (Tools)

SVD:

- ISO/IEC 27001 **und**
- ISO/IEC 27701 zertifiziert (InfoSec & Datenschutz)

seit **2020**

Prävention

- Technische Maßnahmen
- Organisatorische Maßnahmen
- Kontrollen

Maßnahme

- Vulnerability Scans (techn. Schwachstellen)
- Pentests
- SSL-Tests (Verschlüsselung)
- ...

Herausforderung:
- sehr reaktiv
- wenig treffsicher
- "Gießkannenprinzip"

Maßnahmen in Evaluierung

Breach & Attack Simulation

- 24/7 Pentest
- durch Abgreifen von Informationsständen
- Simulation von Angriffen
- Vorschläge zur Behebung

dadurch:

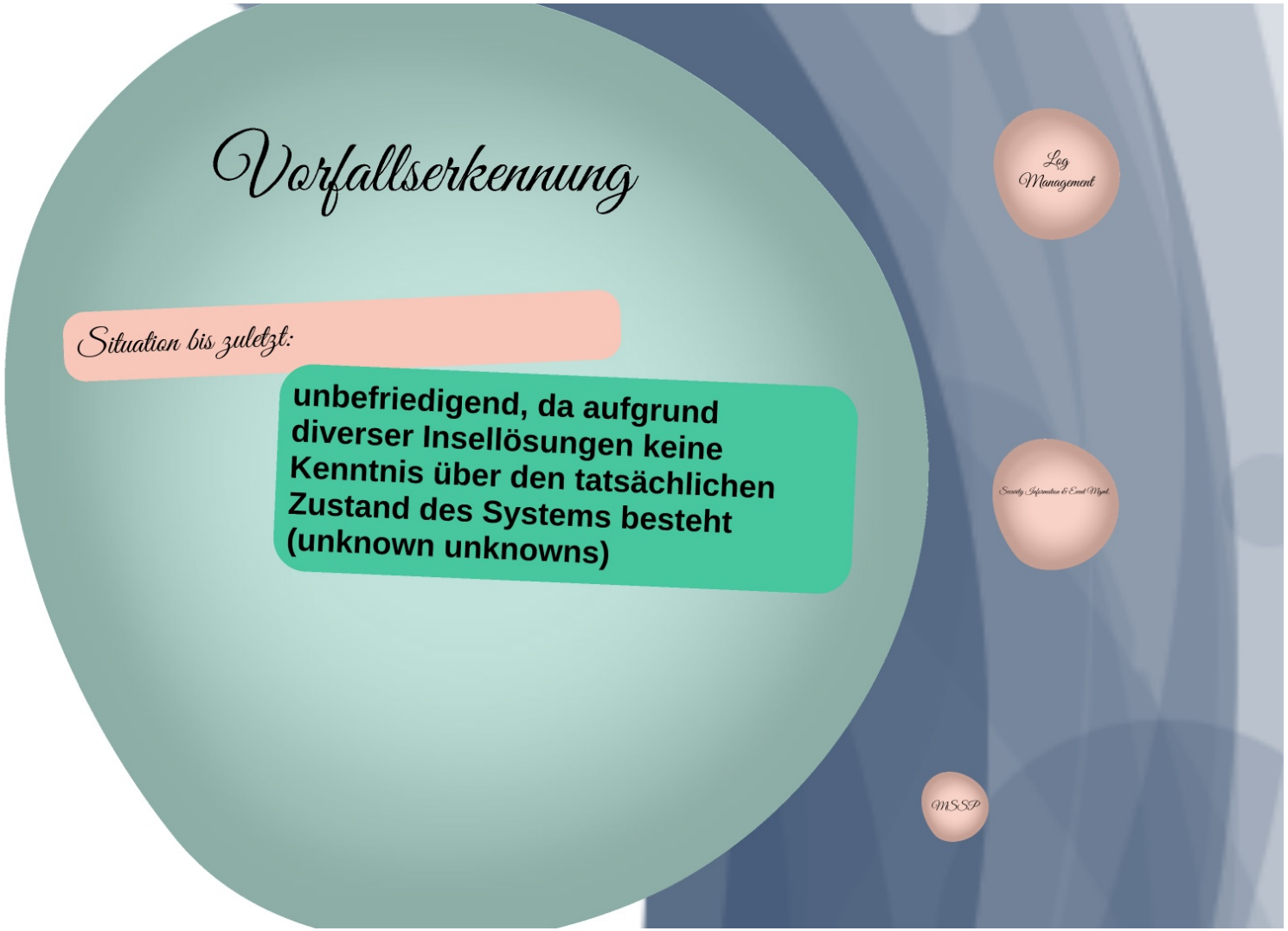
- zielgenaues Fixen von Schwachstellen
- rasche Reaktion auf Zero Days

in weiterer Folge:

- **Steigerung der Effizienz**
- **Entlastung** des Betriebes

Backup Strategie

- Air Gap - Verbindung zu Backup Storage nur temporär
- Clean Room - zur Analyse der Backups
- Cyber Sense - zur Ransomware-erkennung im Backup


Vorfallserkennung
Log Management
Situation bis zuletzt:
unbefriedigend, da aufgrund diverser Insellösungen keine Kenntnis über den tatsächlichen Zustand des Systems besteht (unknown unknowns)
Security Information & Event Mgmt.
MSSP


Log Management
Umsetzung:
• Anbindung in Phasen
• sämtliche Logquellen
• dadurch vollständige Sicht auf sämtliche Systeme
• keine Einschränkungen (aufgrund des Lizenzmodells)
• läuft im eigenen RZ
• Cloud Connectoren vorhanden
Unterstützung/Erleichterung für Entwicklungsabteilungen der Kunden in Bezug auf Logging

Security Information & Event Management

Besispiele für Use Cases:

Beschreibung
Admin- Accounts mit hohen Privilegien / versuchte Privilege escalation - Überwachung der Admin Accounts - Feststellung ob eine Privilege Escalation im AD versucht wurde
Alarmierung/Benachrichtigung aller Authentifizierungen des Built-In Admins und Domain Admins - Authentifizierungs-Überwachung der AD Admins
Zugriffsversuche auf VIP-Benutzer (zb. Geschäftsleitung) mit Berechtigungen auf streng vertraulichen Daten - Zugriffe erkannt anhand vorbereiteter VIP Userliste - Streng vertrauliche Daten sind im Zugriff (vorab Definition durch AG)

Managed Security Service Provider

durch enges Zusammenspiel mit einem MSSP

- tiefgreifendes Know-how
- hoher Automatisierungsgrad
- Use Cases auf das Unternehmensumfeld abgestimmt
- laufender Know-how Transfer
- proaktives Monitoring und Alerting
- Unterstützung bei forensischer Analyse

Behebung

Wie erfolgt Response?

- Security Incident Response Prozesse
- Security Incident Modelle
- zusammen mit externem Partner
- Lessons Learned inhouse

Vielen Dank für die Aufmerksamkeit!

Kontaktdaten:

Ing. DI Dietmar Wieland
allgemein beeideter und gerichtlich
zertifizierter Sachverständiger für IKT
Mail: Dietmar.Wieland@svdgmbh.at
Tel: 0676/888288201

Stefan Höller, BA
Mail: Stefan.Hoeller@svdgmbh.at
Tel: 0676/888288719