

Cyber Security und Datensicherheit

Praxisnahe Einblicke ins Zusammenspiel zwischen Gemeinde und IT-Dienstleister.

VGSo-Jahresversammlung vom 11. November 2022

Michael Steiner, Verwaltungsleiter und Gemeindeschreiber Dulliken

Dominic Müller, System Engineer AEK Build Tec AG

AEK Build Tec AG – Unsere Entwicklung seit der Gründung

Wir sind regional verankert und Gruppenweit vernetzt!

AEK Build Tec AG

Gründung

▪ 2019

Niederlassungen

▪ 8

Mitarbeiter

▪ 150

ICT der AEK Build Tec AG

Kunden ICT

▪ 1000

Kunden AEK Cloud

▪ 36

Mitarbeiter ICT

▪ 25



AEK Build Tec AG

Client-Server

- Notebook
- Desktop
- Server
- Storage
- Workplace



Netzwerk

- Firewall
- Switching
- Wireless
- Netzwerkanalysen
- Netzwerkmanagement



Swiss-Cloud

- Cloud-Center Schweiz
- Microsoft 365
- Telekommunikation/UCC
- Backup
- Archivierung



Telekommunikation

- IP-Telefonie / Alarmserver
- Unified Communication
- Pflegerufsysteme
- Personenschutz / Notruf
- Videokonferenzsystem



Security-Lösungen

- Cyber Security
- IT Audits
- Virenschutz
- Spamschutz
- Videoüberwachung



Managed-Services

- Aktuelle Geräte / Software
- Monatlicher Fixpreis
- Überwachung
- Umfassend
- Zeitsparend



1

System-Architektur

2

Technische
Vorkehrungen

3

Der Faktor Mensch

4

Cyber-Versicherung

5

Zertifizierung
Label «Cyber Safe»

6

Regelmässiges Monitoring /
Aufnahme im IKS

7

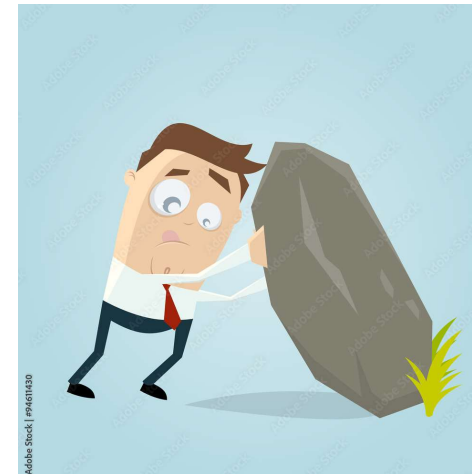
Mindset

8

Notfallkonzept

9

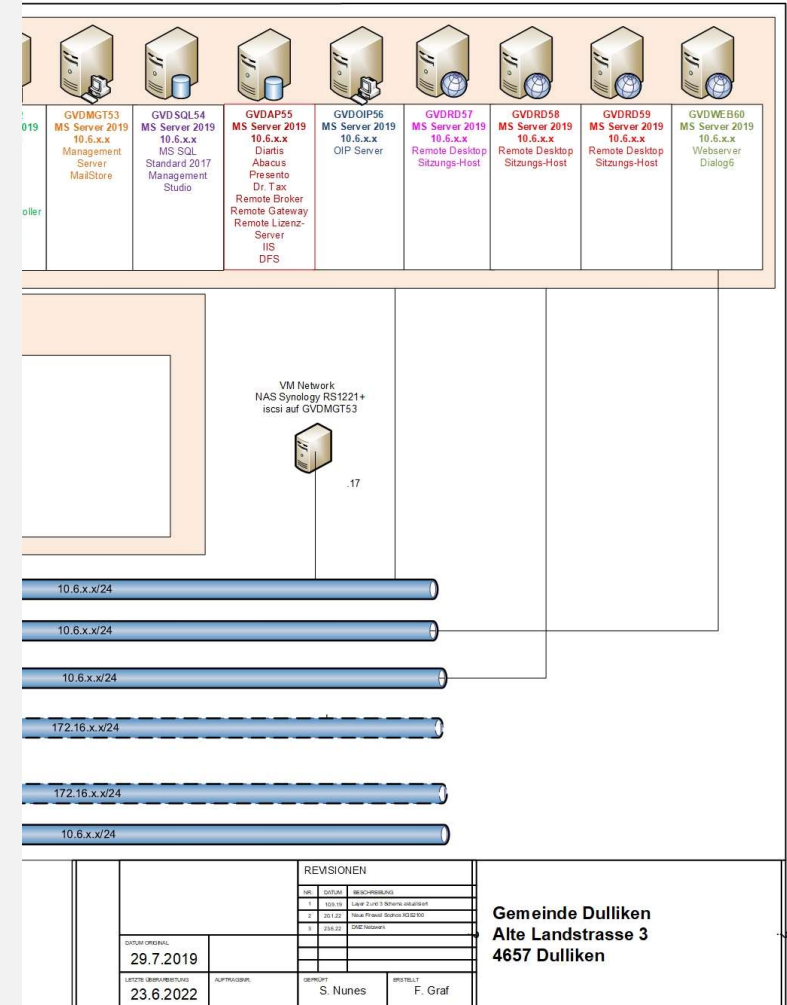
Zusammenarbeit zwischen
Gemeinde und IT-Dienstleister



System-Architektur.

1

- Kennen Sie die Architektur Ihrer IT-Systeme?
- Wissen Sie, welche Anwendungen über Ihre IT-Systeme betrieben werden?
- Wissen Sie, wo Ihre Daten liegen?
- Gibt es eine aktuelles System-Handbuch oder eine aktuelle System-Dokumentation?



Technische Vorkehrungen treffen.

2

Endpoint, Network Protection

- Antivirensoftware mit EDR Funktion
- Monitoring
- Systeme Aktualisieren (Patchmanagement)

Datenstruktur und Zugriffskonzepte

- principle of least privilege (PoLP)

Multi Faktor Authentifizierung (MFA)

- Etwas Wissen (Credentials) und etwas Haben (Handy, SMS, E-Mail)
- M365, VPN, WindowsLogon, RDS/Citrix

Backup

- Backup-Konzept
- Wo werden die Backups gespeichert (Architektur Backup-Server)
- Prüfung der Backups auf Vollständigkeit und Funktionsfähigkeit
- 3-2-1-(0) Strategie

Der Faktor Mensch als grösste «Fehlerquelle».

3

Sensibilisierung

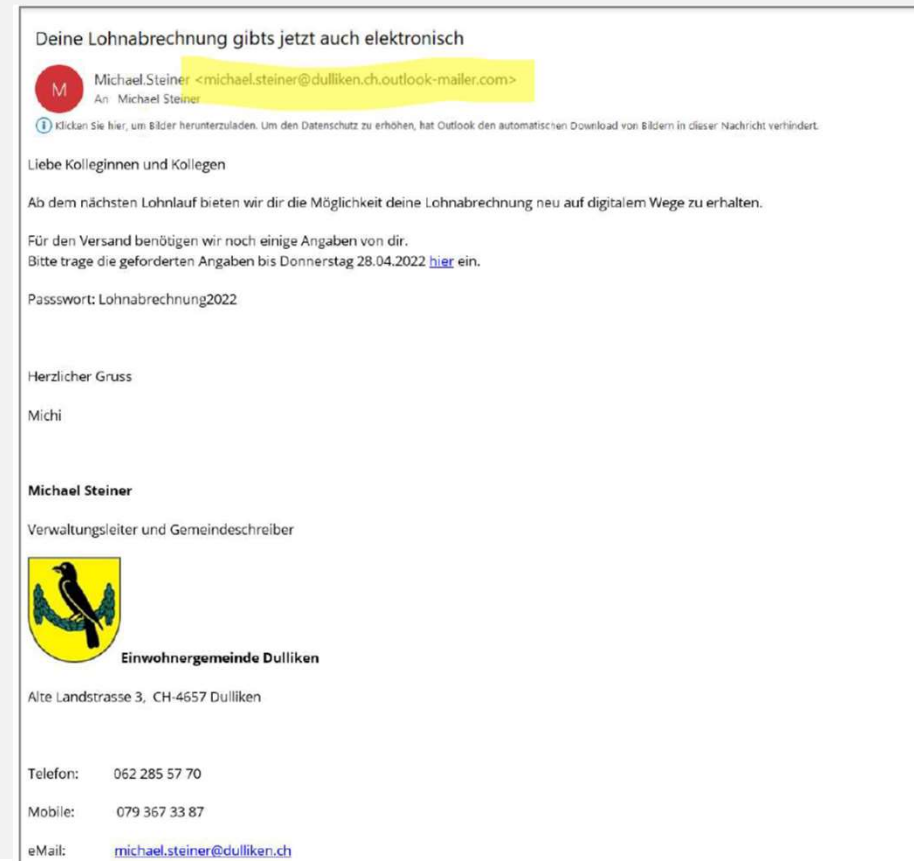
- Regelmässige Thematisierung von Cyber Security-Risiken
- Transparente Kommunikation
- Fehlerkultur
- Vorbildrolle

Schulung

- Digitale Schulungs-Module zu den wichtigsten Risikofeldern

Phishing Tests

- Gezielte, möglichst realitätsnahe Test-Szenarien mit Fokus auf Lerneffekte und nicht aufs «Blossstellen»



Weitere Aufpassfelder.

4

Cyber Versicherung

- Cyber-Versicherungen sind eine sinnvolle Ergänzung, aber kein Rundum-Sorglos-Paket (Abdeckung von kritischen Infrastrukturen ebenfalls beachten)
- Ihr Versicherungsberater/-broker ist ein guter Sparring-Partner im Bereich Cyber Security

5

Zertifizierung (z.B. «Cyber Safe»)

- Qualifizierte Dritteinschätzungen sind sinnvoll und willkommen – auch für den eigenen IT-Dienstleister. Zertifizierung ist vielfach ein politisches Bedürfnis
- Dauerhaft greifende Massnahmen und Sensibilisierung sind wichtiger als die Momentaufnahme eines Zertifikats.

6

IKS (Internes Kontrollsystem)

- Berücksichtigen Sie Datenschutz-, Cyber Security- und Datensicherungs-Themen beim Aufbau ihres IKS – ggf. als zusätzliche Risikofelder.
- Die IKS-Kontrollmassnahmen eignen sich gut zur Etablierung von institutionalisierten Kontrollen und Zuweisung von klaren Verantwortlichkeiten

Abschliessende Gedanken.

7

Mindset / Grundeinstellung im Umgang mit Cyber Risiken

- Sich in (falscher) Sicherheit wiegen, kann fatal enden
- Es gibt keine dummen Fragen
- Jede Beobachtung / Feststellung ist wichtig und wertvoll
- Basis-Szenario: Es wird irgendwann zu einem Cyber-Vorfall kommen

8

Notfallkonzept / Seriöse Vorbereitung und Dokumentation

- Festlegung von klaren Szenarien für die Bewältigung eines unerlaubten System-Zugriffs oder eines Verschlüsselungs-Angriffs
- Berücksichtigung von technischen, organisatorischen und kulturellen Elementen

9

Zusammenarbeit Gemeinde / IT-Dienstleister

- Ein guter Schutz gegen Cyber-Risiken kann nur gemeinsam entstehen
- Vertrauen, Offenheit und Transparenz als zentrale Elemente
- Bereitschaft seitens Gemeinde, sich eine minimales technisches Verständnis anzueignen, um einen Dialog auf Augenhöhe mit dem IT-Dienstleister führen zu können.

Maßnahmen

Top 10+1

- 1) Revisionstaugliche Datensicherung
- 2) Nutzungs- und Überwachungsreglemente erstellen
- 3) Schulung der Mitarbeiter
- 4) Keine Adminrechte auf Clients
- 5) Lange und komplexe Passwörter (mind. 12 Zeichen)
- 6) Regelmässige Updates von Hardware und Software
- 7) Virenschutzlösung
- 8) Physischer Schutz der Client/Serversysteme
- 9) Whitelisting von Applikationen (Applocker)
- 10) Notfallmanagement
- 11) Proaktives Monitoring der Systemlandschaft

**Vielen Dank für Ihre
Aufmerksamkeit.**

Haben Sie Fragen?