

# IT Security

Erfahrungen aus einem Rechenzentrumsbetrieb

---

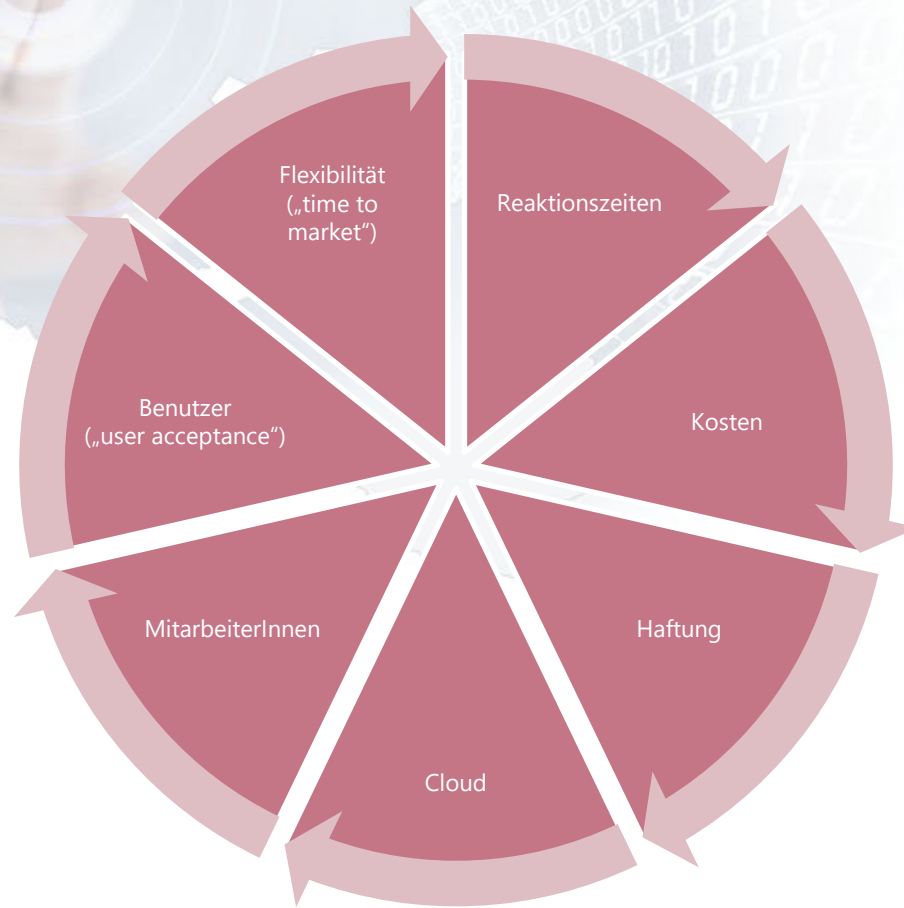
# Daten-Verarbeitung-Tirol GmbH

- Gründung per Landesgesetz 1997
- 100% Tochterunternehmen des Landes (GmbH)
- 120 Mitarbeiter
- Klassisches IT Unternehmen
- Rechenzentrumsbetrieb inkl. Servicedesk
- 3 Benutzerkreise
  - Tiroler Landesregierung (TLR)
  - Tiroler Schulnetz (TSN)
  - Tiroler Gemeindenetz (TGN)

# Daten-Verarbeitung-Tirol GmbH

- 100 Standorte im Netzverbund
- 2 zentrale Datacenter, kleinere Systemräume in ausgewählten Außenstandorte
- 800 Systeme (Server, Appliances, etc.)
- 4.500 PC Arbeitsplätze
- 110.000 Benutzer Accounts
- 300 IT Services (Anwendungen)
- 250 Basisdienste

# Herausforderung IT Security



# Zentrale Elemente IT Security



# Organisation IT Security

- ISO Zertifizierung als Weg zur richtigen Organisation
- **Richtlinien und Prozesse**
  - Informationssicherheitsvorfälle
  - Change Management
  - Schwachstellen- und Patchmanagement
- **Information Security Management System (ISMS)**
  - Notfallvorsorge
  - Notfallübungen und Tests
  - Notfallbewältigung
- **Risikomanagement & Business Impact Analyse**



# Organisation IT Security

## Erfolgsfaktoren

Mehrwert schaffen

Technische Unterstützung  
bzw. Automatisierung

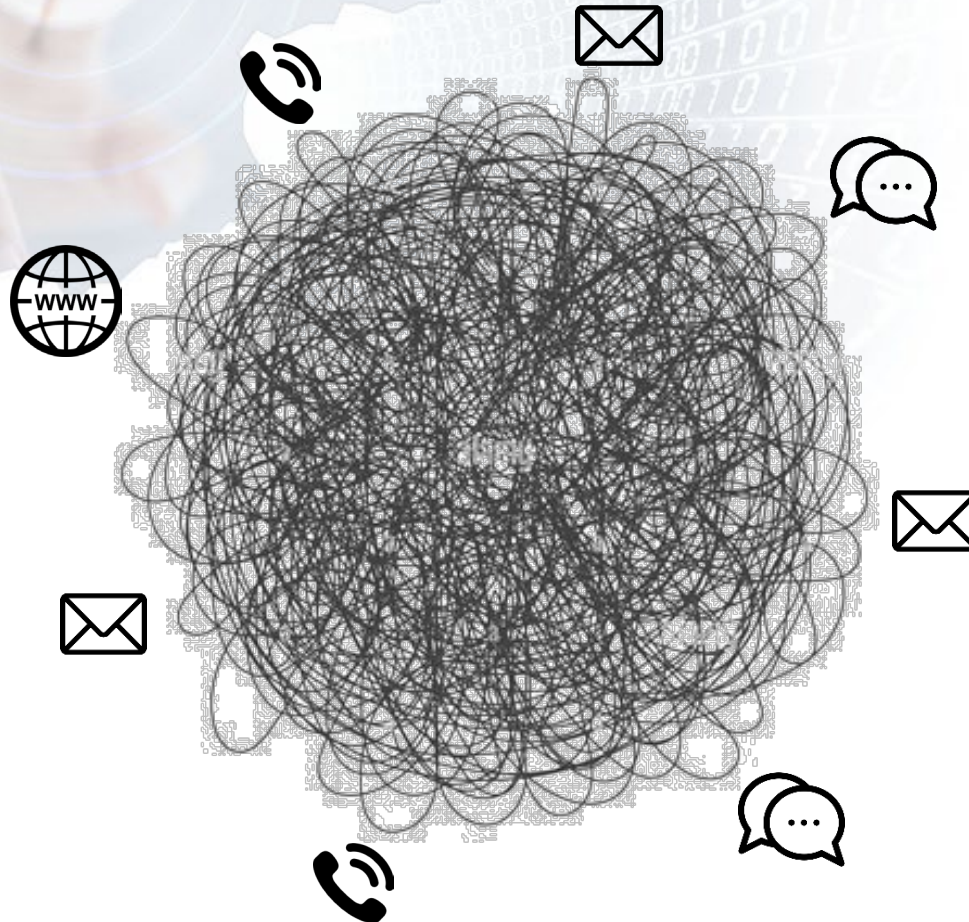
Praxisnahe Umsetzung

Redundanzen & Bürokratie  
vermeiden



# Organisation IT Security

## Schwachstellen-Management (CVEs)





# Organisation IT Security

## Schwachstellen-Management (CVEs)

### PROZESS

mit  
Verantwortlichen /  
Rollen (CISO, ISB, ..)

### QUELLEN

Internet, Infos von  
CERTs, Vulnerability  
Scanner, „CVE  
Crawler“

### TICKET

Bearbeitung wird  
lfd. dokumentiert

### BEWERTUNG

Reaktionszeit und  
ggf.  
Notfallmanagemen  
t

### RFC

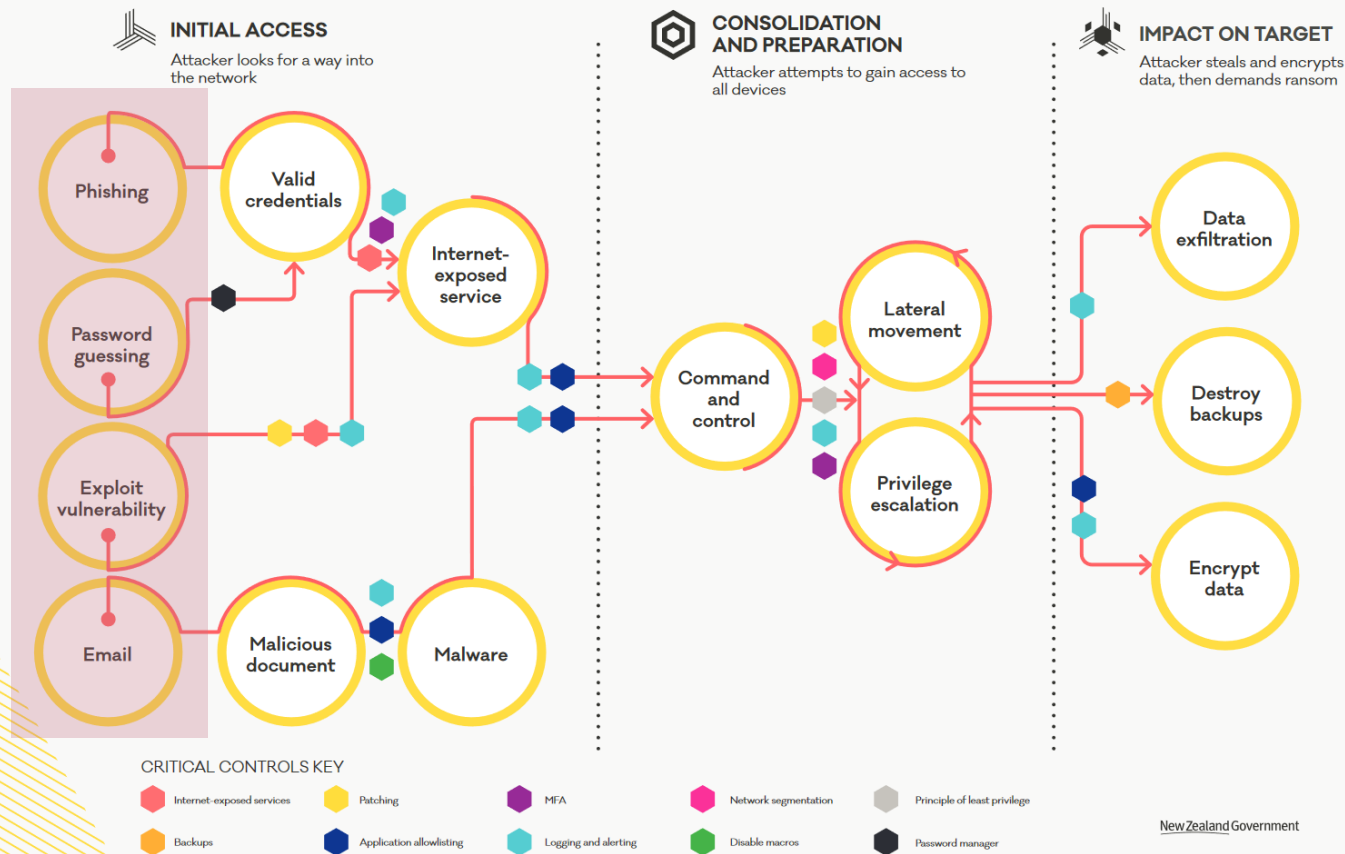
Change  
Management

# IT Security - Technik

## LIFECYCLE OF A RANSOMWARE INCIDENT



How the CERT NZ Critical Controls can help you stop a ransomware attack in its tracks.



# IT Security - Technik

- Awareness Programm
- MFA / 2FA
- Netzwerk-Segmentierung
- Sicherheit Clients & Server
- Firewall / Webproxy
- Mail Security
- Monitoring, Logging & SIEM
- Identity Management
- Backupsystem

# Aktuelle Themen

- NIS2
- Security Operation Center (SOC)
  - 7x24 Betrieb bzw. Bereitschaften
- Privileged Access Management
  - Dedizierte Admin Workstations
- Notfallszenario „Internet Offline“ - kein kommerzielles Internet



Daten-Verarbeitung-Tirol GmbH  
Adamgasse 22  
6020 Innsbruck  
Tel. +43 512 508 3319  
[www.dvt.at](http://www.dvt.at)

---

DANKE FÜR IHRE AUFMERKSAMKEIT