

# BUSINESS BREAKFAST ONLINE

## DATA RECOVERY IN KMU – VORSORGEN ODER ZAUBERN

first frame  
networkers  
IT, die Sie weiterbringt

VEEAM



START  
UM  
08.05 UHR

## — HERZLICH WILLKOMMEN

**first frame  
networkers**  
IT, die Sie weiterbringt

**Vielen Dank, dass Sie sich die Zeit für uns nehmen!**

**Was Sie heute erwartet:**

Ein spannendes Referat über Bedrohungsszenarien in der IT-Welt, über das Vorgehen dagegen.

Über Klassifizierung und Verantwortung bei der Datenhaltung und über Backup- und Wiederherstellungs-Strategien.



**JÖRG KOCH**

Leiter Marketing

first frame networkers ag

## — DER HEUTIGE REFERENT

**first frame  
networkers**  
IT, die Sie weiterbringt



**IVAN CIOFFI**

**Teamlead Systems Engineers  
Switzerland, Veeam Software**

**VEEAM**

## AGENDA

**first frame  
networkers**  
IT, die Sie weiterbringt

- ⇒ 08:05 Begrüssung, Jörg Koch / first frame networkers ag
- ⇒ 08:10 Referat Data Recovery in KMU, Ivan Cioffi / Veeam
- ⇒ 08:50 Fragen & Antworten

Fragen können mit der Chatfunktion gestellt werden.

Das Webinar wird in Schweizerdeutsch gehalten.

The Veeam logo is displayed in white lowercase letters on a bright green rectangular background. To the right of the logo, a cluster of small, semi-transparent green dots is arranged in a diagonal pattern, extending from the top left towards the center of the slide.

veeam

# Data Recovery in KMU– vorsorgen oder zaubern

A 3D illustration of a server rack is positioned on the right side of the slide. The server units are rendered in a dark green, semi-transparent style. In the foreground, two square icons are visible: one on the left containing a network diagram with nodes and lines, and one on the right containing a bar chart with an upward-pointing arrow, symbolizing data recovery and business growth.

Ivan Cioffi

Systems Engineering Teamlead Switzerland  
[ivan.cioffi@veeam.com](mailto:ivan.cioffi@veeam.com)

# Agenda

- Bedrohungsszenarien - Vorgehen
- Klassifizierung
- Verantwortungen
- Backup- und Wiederherstellungs Strategien

# Szenarien



# Bedrohungsszenarien

- Interne
  - Fehlmanipulationen, Böswilligkeit, SLA's, Schwachstellen
- Externe
  - Ransomware, Phishing, Virus
- Insider
  - Partner
- Technik
  - Ausfälle, Bugs



# Bedrohungsszenarien

- Interne
  - Fehlmanipulationen, Böswilligkeit, SLA's, Schwachstellen
- Externe
  - **Ransomware**, Phishing, Virus
- Insider
  - Partner
- Technik
  - **Ausfälle, Bugs**

# Daten Klassifizieren



# Daten & Dienste / Klassifizierung

- Dienste Klassifizieren
  - E-Mail, CRM, Auftragsabwicklung, Logistik, Rezepte, Herstellungsprozesse
- Daten Klassifizieren
  - Dokumente, Pläne, Zeichnungen, Verträge, Fotos,
- Schutzgrad
  - Essentiell, Speziell Schützenswert, Schützenswert, Nice to have

# Verantwortungen



Nicht abschliessend

# Verantwortungen <sup>1/4</sup>

- Aktuelle Versionen und regelmäßige Updates der Antivirenprogramme
- Klassifizierung der Daten & Dienste
- SLA's, intern mit dem Business, extern mit Partner
- Reaktiver Schutz (Virensignaturen)
- Proaktiver Schutz (Zero Day Exploit)
- Sicherheitsrichtlinien definieren
- Einheitliche Infrastruktur
- Gelebte Passwortkultur

Nicht abschliessend

VEEAM

# Verantwortungen <sup>2/4</sup>

- Aktuelle Dokumentation
- Monitoring
- Verantwortlichkeiten für DR & Restore Entscheid
- Prioritätenliste (Daten & Dienste)
- Deutlich höhere Sicherheitsexpertise
- Firewall-Regeln up to date halten, eigene definieren
- Machine Learning/ SaaS-AI Intrusion als 24/7 Service
- MFA auch intern

Nicht abschliessend

VEEAM

# Verantwortungen <sup>3/4</sup>

- Backup- und DR Konzepte
- SLA's
- Restore Tests
- Zugänge (virtuell & physisch)
- Cyber Attack Detection & Response
- Organisatorische Massnahmen (Einschränkungen)
- Planspiele
- Kontaktlisten (NCSC, IT Partner, ...)
- Passwortmanager

Nicht abschliessend

VEEAM

# Verantwortungen 4/4

- BYOD
- SLA mit Business und GL definieren
- Machine learning
- Mehrstufige Absicherung (Provider, Lokal, ...)
- Training (Phishing Tests)
- Daten Hoheit sicherstellen
- Regelmässige Audits nach Compliance Vorgaben (BSI, Basel, SOX)
- Schnellere Bereitstellung von Security-Lösungen
- Individuelle Strategie die auf bisherige Massnahmen angepasst ist

Nicht abschliessend

VEEAM



# Strategien (Ransomware)



# 6 Stages of an Advanced Ransomware Attack

## Stage 4: Elevate Access

Snooping around without being detected and comprise higher value targets

## Stage 5: Cripple Recoverability

Alter routines, documentation and systems to reduce/deny restore capabilities

## Stage 3: Setting up Shop

Creating a base of operations and let's make it redundant and highly available

## Stage 6: Ransom Declared!

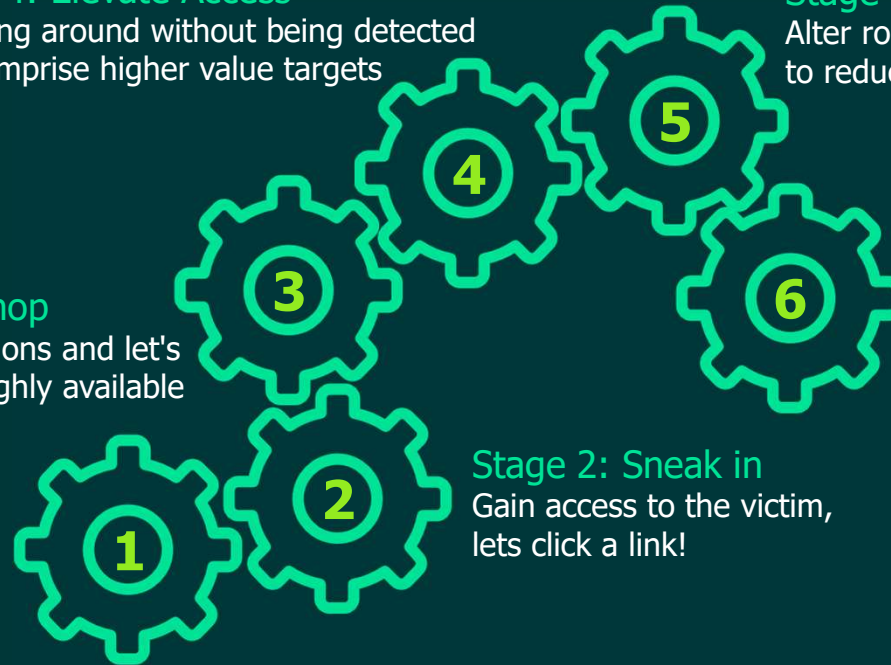
Encrypt victim's data, wipe archives/backup/data, issue ransom demands!

## Stage 2: Sneak in

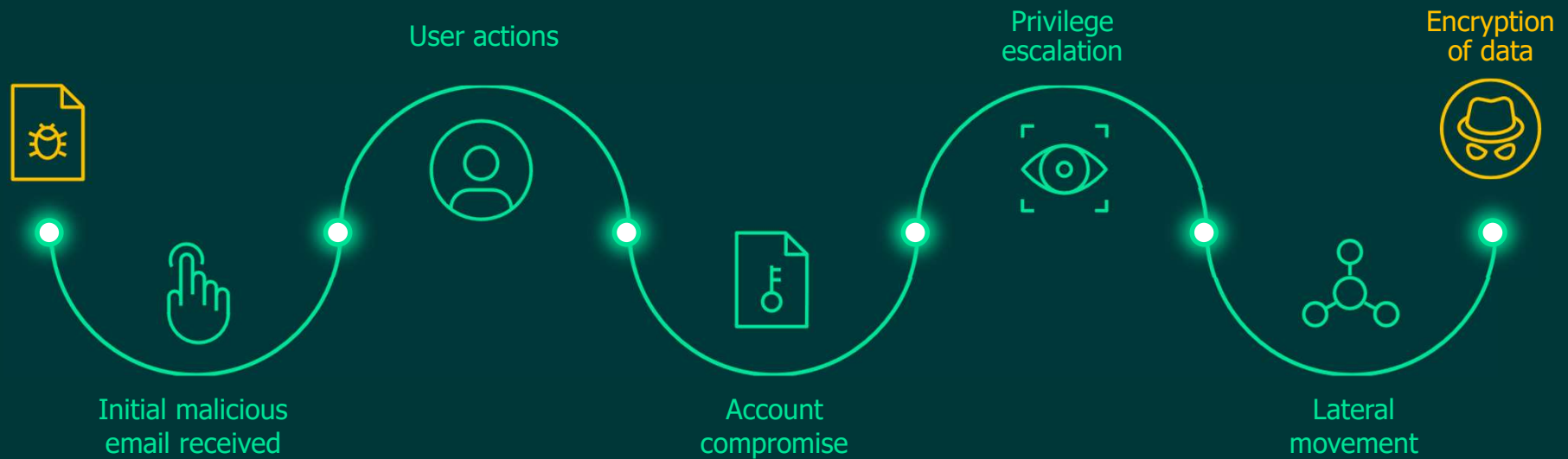
Gain access to the victim, lets click a link!

## Stage 1: Observation

Information is gathered on the victim's people, processes and technology in play

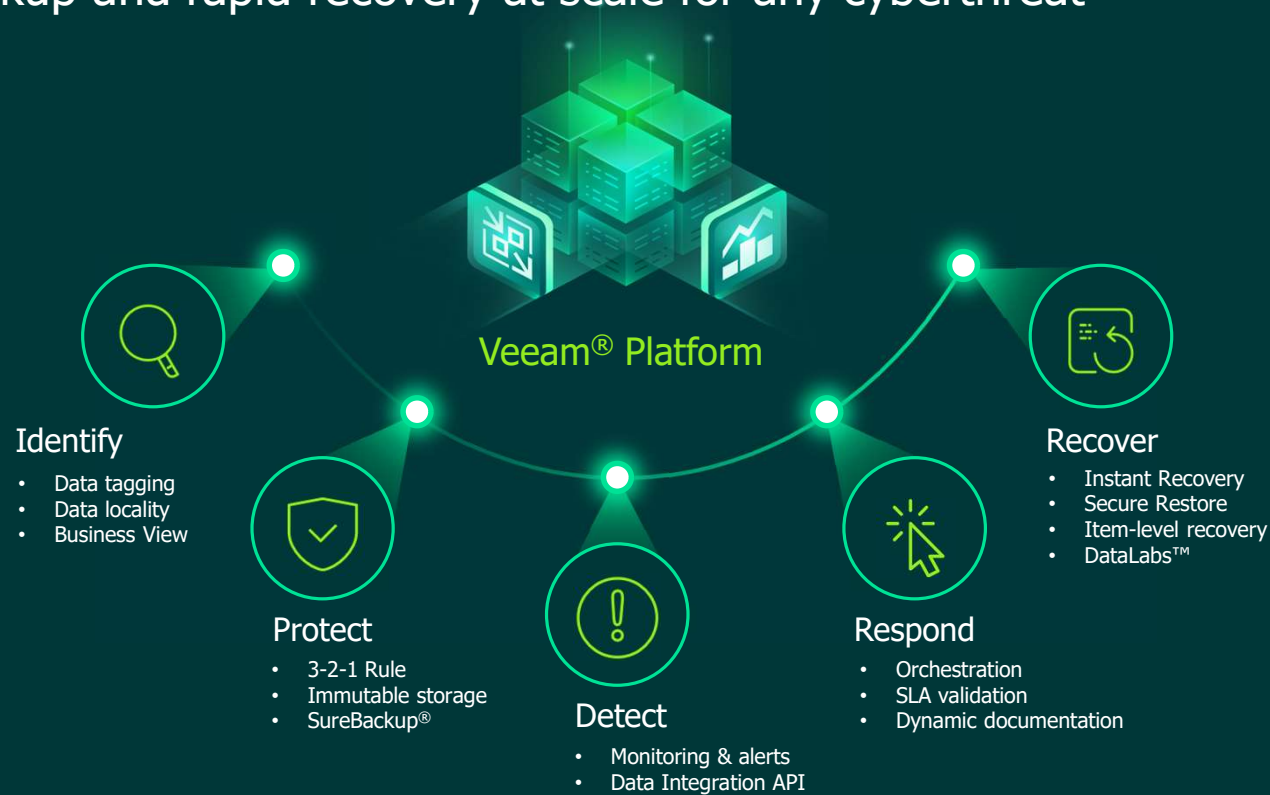


# Backup ist die letzte Verteidigungslinie



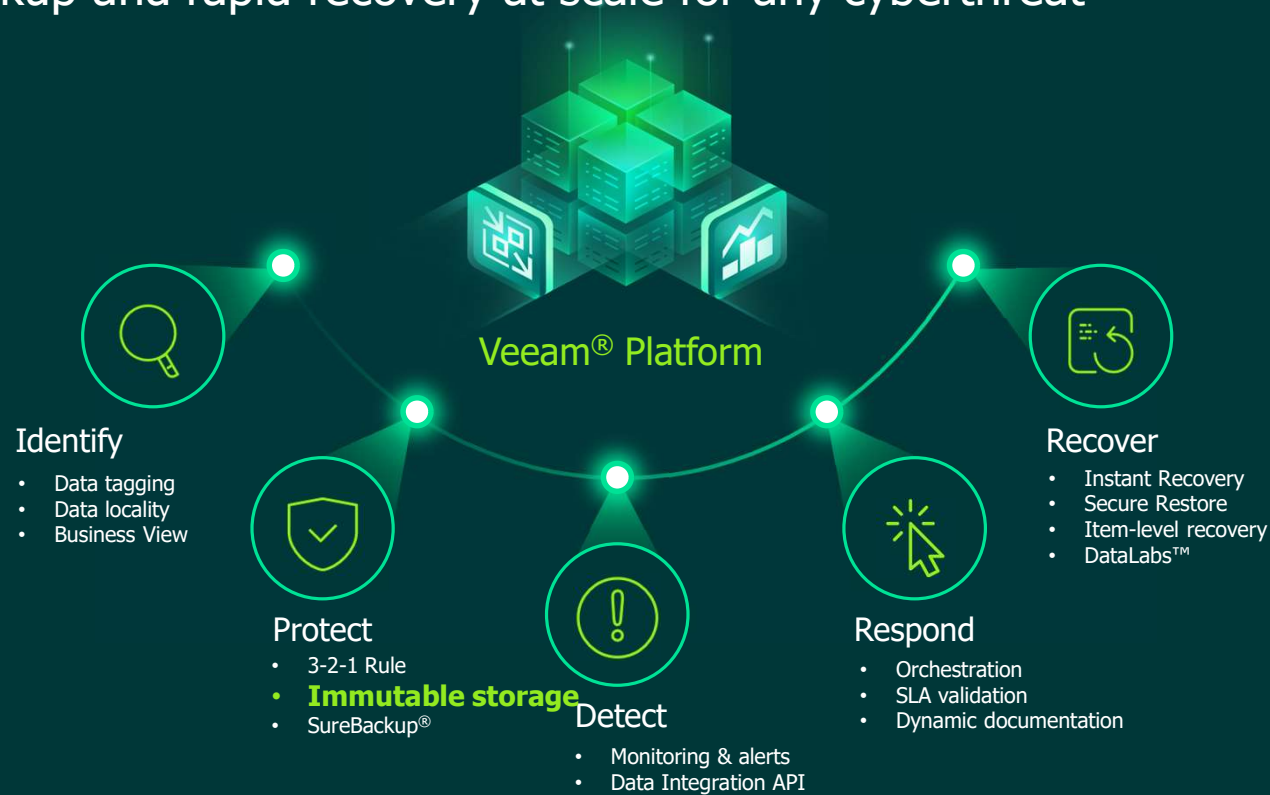
# #1 Ransomware Schutz

Secure backup and rapid recovery at scale for any cyberthreat



# #1 Ransomware Schutz

Secure backup and rapid recovery at scale for any cyberthreat



# 3-2-1 Ransomware Schutz



Three different copies of data



Two different media



One off-site copy

## VEEAM



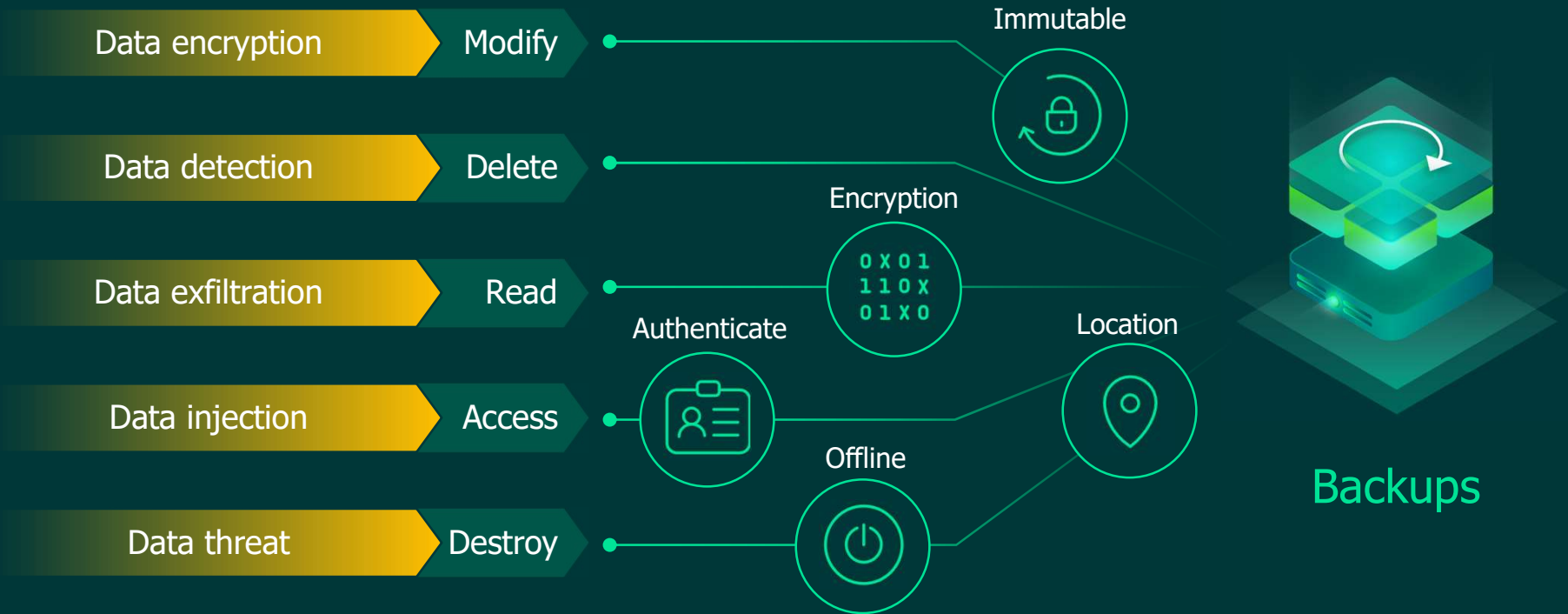
Of which is:  
offline, air-gapped  
or immutable



No errors after  
automated backup  
testing &  
recoverability  
verification

# Immutability ist nicht genug

## Measures to protect your backups



# Veeam Platform

Cloud



SaaS



Apps



Virtual



Physical



Data Reuse



Disaster Recovery Orchestration



Monitoring and Analytics



Backup and Recovery



Storage, Analytic and Management APIs



On Premises



Public Cloud



BaaS & DRaaS



Veeam Availability Suite



Veeam Backup & Replication



Veeam Backup *for Microsoft Office 365*



Veeam DR Orchestrator



Kasten K10 by Veeam



# — CLOUD-BACKUP FÜR IHRE WERTVOLLEN DATEN

**first frame  
networkers**  
IT, die Sie weiterbringt



Mehr Infos: [www.first365.swiss](http://www.first365.swiss)

Daten sind das wichtigste Gut im digitalen Zeitalter. Da ist nur der beste Service gut genug. Wir sichern Ihre Daten per Online-Backup in die leistungsfähigen «first 365»-Rechenzentren in Bern und Zürich. So sind Sie jederzeit auf der sicheren Seite.

## UNSER ANGEBOT

- ◇ first 365 backup on premises
- ◇ first 365 backup e-mail
- ◇ first 365 backup microsoft 365
- ◇ first 365 backup cloud connect

## IHRE VORTEILE

- ◇ sichere Übertragung der verschlüsselten und komprimierten Daten
- ◇ lückenlose Überwachung
- ◇ Datenhaltung und Leistungserbringung in der Schweiz
- ◇ weniger Investitionen in eigene Infrastruktur

## — MANAGED BACKUP



Unsere «Managed Services» sorgen dafür, dass sich IT-Abteilungen voll auf die Geschäftsanwendungen und den Benutzer-Support konzentrieren können.

### FÜR IHRE DATEN IST NUR DER BESTE SERVICE GUT GENUG.

Beim Service «Managed Backup» kümmert sich die first frame networkers ag um Backup-Systeme mit Veeam Backup and Replication. Ausgebildete Veeam Administratoren überwachen die Basis-Backup-Infrastruktur und machen monatliche Wartungen.

Zwei Mal im Jahr wird die Veeam-Infrastruktur auf die neuste Version aktualisiert und Backupfehler werden beim Auftreten behoben.

### LEISTUNGEN

- ◆ Monatliche Wartung des Backupserver (Windows Updates)
- ◆ Unterhalt der Backupsoftware (2 Wartungen pro Jahr)
- ◆ Überwachung der Backup Jobs und Störungsbehebung im wiederholten Fehlerfall (first monitoring)
- ◆ Individuelle Backup-Konfiguration anhand der Bedürfnisse des Kunden (Daily, Weekly usw.)

[firstframe.net](http://firstframe.net)

[first365.net](http://first365.net)

**Herzlichen  
Dank**