validdata
we make IT simple.

Cybercrime-Risiken abwehren, aber wie?

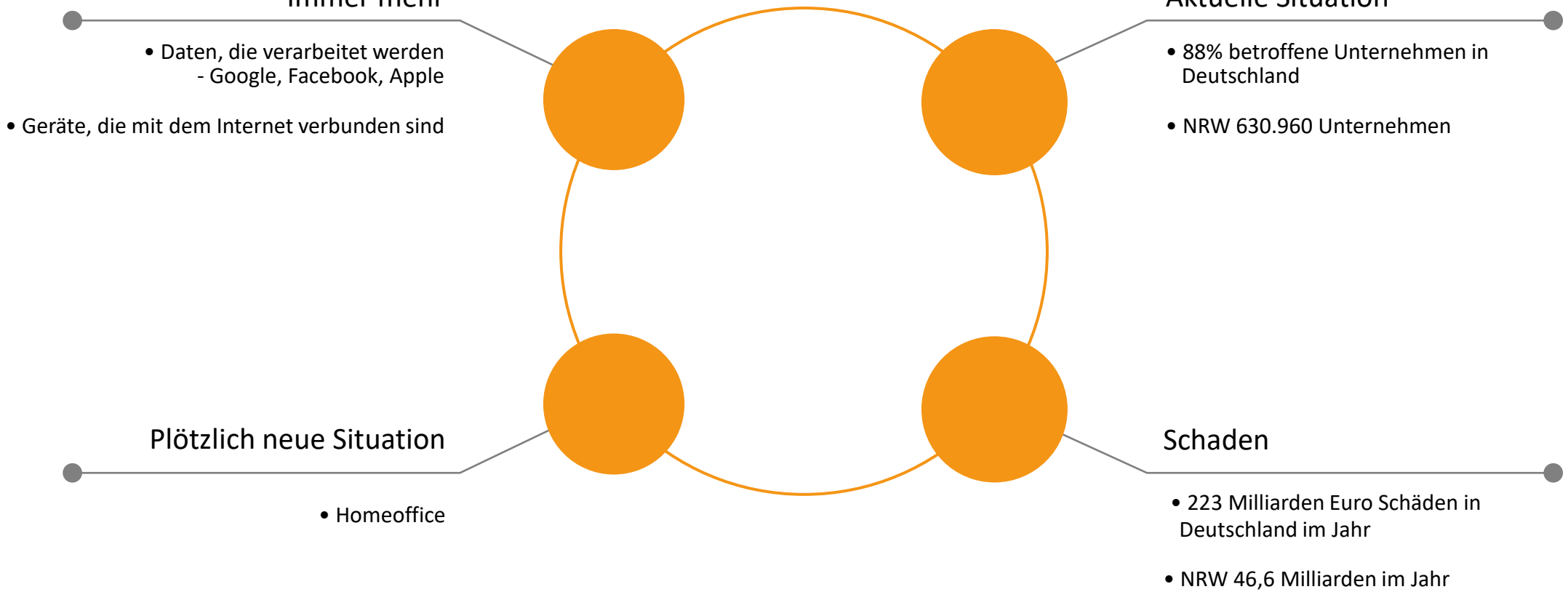
Henrik Stoverink , Maurice Heßing

validdata
we make IT simple.

van Clewe validdata GmbH

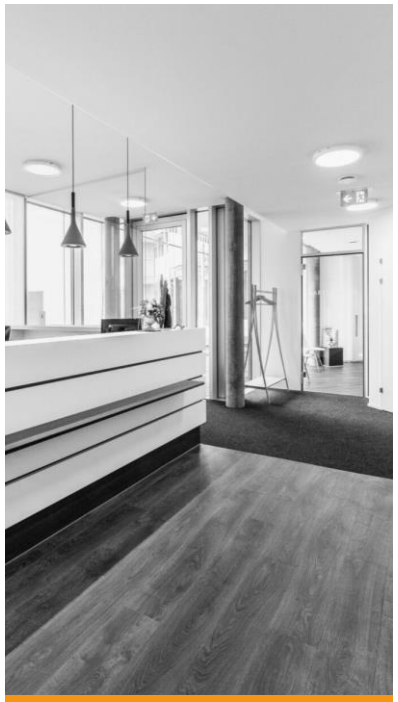
- Gegründet 2001 aus der IT-Abteilung der Gerhard van Clewe GmbH & Co. KG
- ca. 20 Mitarbeiter
- IT FullService-Dienstleister
  - IT-Infrastruktur
  - Software-Entwicklung
  - Digitale Geschäftsprozesse (DMS, ERP)
  - Microsoft 365 Spezialist
  - Fördermittelberatung
- Kleine und mittlere Unternehmen

Cybercrime Vortrag – Peter Vahrenhorst



Fallbeispiele - Peter Vahrenhorst

Hackerangriffe auf Autos



Gesundheitsdaten in Arztpraxen

zoom

Zoom-Bombing

UNI-Klinikum Düsseldorf

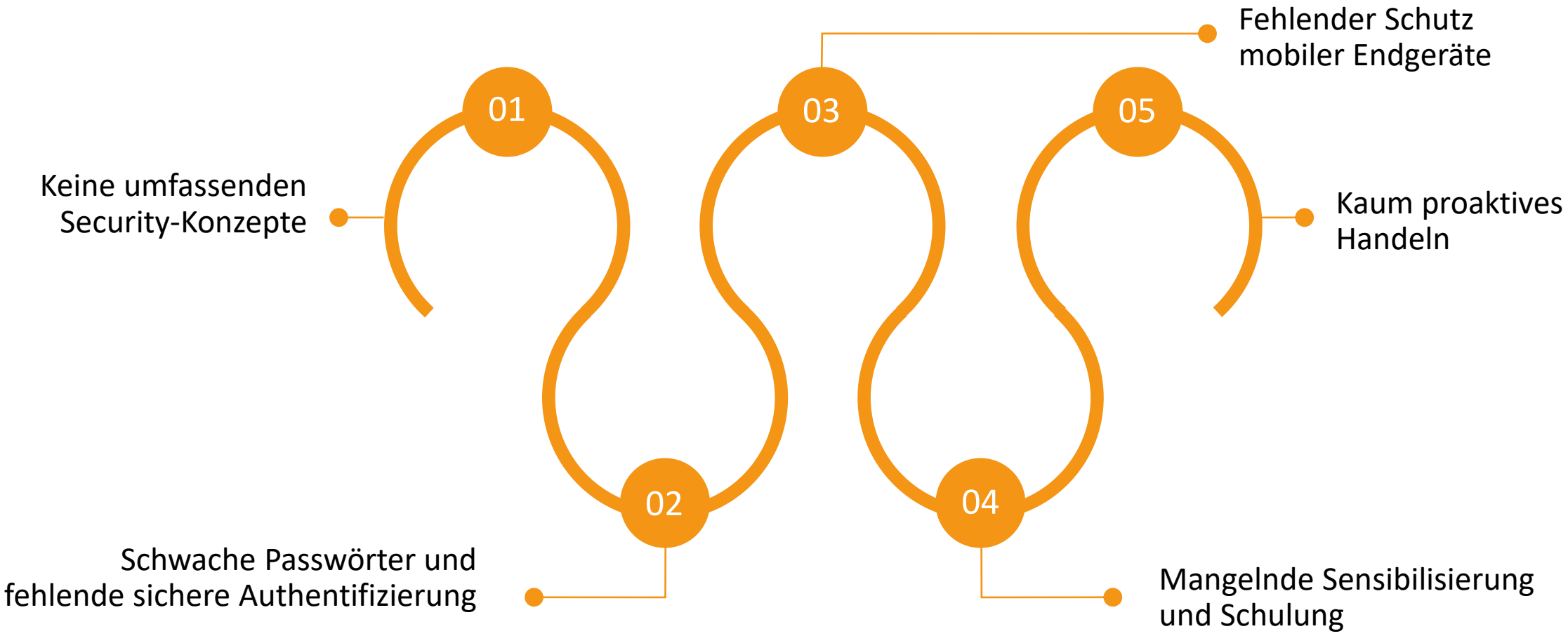
Hackerangriff auf Wasserwerk in Florida

validdata

we make IT simple.

Die 5 größten Security-Schwachstellen im Mittelstand

Die 5 größten Security-Schwachstellen



Handlungsoptionen

Mögliche Handlungsoptionen

- Arbeiten im Homeoffice & unterwegs
- Client- & mobile Device-Management
- Passwörter & Co.
- Benutzerschulungen & -sensibilisierung (Awareness)
- Datensicherungsstrategien, Data Loss Prevention
- Virenschutz & Firewall
- Notfallplan / Maßnahmenkatalog

Homeoffice & unterwegs

Homeoffice & unterwegs

- Keine Verwendung von privaten Endgeräten
- Getrenntes Netzwerk für Firmengeräte
- Gesicherte Verbindung ins Firmennetzwerk
  - VPN Verbindung
  - Professionelle Firewalls im Unternehmen
- Leitfaden
- Zentrale Verwaltung / Monitoring aller Firmengeräte

Client- & mobile Device-Management

Client- & mobile Device-Management

- Wissen Sie, was auf den PCs, Tablets & Smartphones Ihrer Mitarbeiter passiert?
- Ungewünschte Apps auf PC & mobilen Endgeräten erkennen
- Monitoring über den Gesundheitszustand der Firmengeräte
- Umsetzung von Unternehmensrichtlinien
  - Vorgabe von möglichen Applikationen
  - Zentrale Verteilung von Updates

Passwörter & Co.

Passwörter & Co.

- Typisches Kundenverhalten
  - Passwort steht bei allen Mitarbeitern unter der Ablage / Monitor
  - Passwort nicht so wichtig, da Zugriff nur intern
  - Alle Mitarbeiter haben das gleiche oder kennen alle Passwörter in einer Abteilung
- Wichtigkeit von Passwörtern
- Häufige Zugriffsmöglichkeiten
  - Abruf von E-Mails von unterwegs (Handy oder Homeoffice)
  - Einwahl in das Firmennetzwerk über VPN
- Passwortkomplexitäten anpassen
- Multi-Faktor-Authentifizierung
- Passwortmanagement

Benutzerschulung und -sensibilisierung (Awareness)

Benutzerschulung und -sensibilisierung (Awareness)

- Umgang mit Passwörtern
- Aufklärung
  - Viren / Phishing-Mails häufiges Angriffsziel
  - Keine Bestrafung bei Fehlverhalten (Mut zur Wahrheit)
- Testen Sie Ihre Mitarbeiter
- Awarenesstraining

Datensicherungsstrategien, Data-Loss Prevention

Datensicherungsstrategien, Data-Loss Prevention

- Datensicherung – Wichtiger als Virenschutz
- Sicherungsstrategie
  - Zweistufig
  - Intervall
  - Aufbewahrung
- Überprüfung
- Desaster Recovery
- Mitarbeiter an der Herausgabe von internen Informationen hindern
- Wichtige Dokumente automatisch verschlüsseln

Virenschutz und Firewall

Virenschutz und Firewall

- Unterschied Firewall & Virenschutz
- Business-Virenschutzlösungen
  - Sonderfunktion wie z.B.: Verhaltensüberwachung, SPAM-Filter etc.
  - Zentrale Verwaltung
  - Benachrichtigung bei Vorfällen
- Business-Firewall
  - Keine Consumerhardware wie z.B. Fritzbox
  - Sonderfunktionen wie z.B. Website / Content-Filter
  - Sicherer VPN-Zugang ggf. mit Multi-Faktor-Authentifizierung

Notfallplan / Maßnahmenkatalog

Notfallplan / Maßnahmenkatalog

Mitarbeiter

- Verhalten bei IT-Notfällen
- Schulung der Mitarbeiter

IT-Verantwortliche

- Ausarbeitung Notfallkonzept für verschiedene Szenarien
  - Virenbefall
  - Hardware-Ausfall
  - Verlust von Hardware

IT-Sicherheitsseminare / Schulungen

- z.B.: BSI – IT-Grundschutz - Praktiker

ISO-Relevant / Cyber-Versicherungen