
dataport

IT-Sicherheit bei Dataport

Dr. Martin Meints

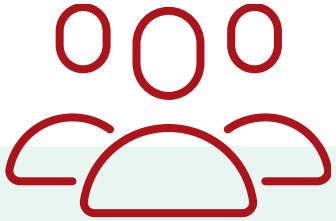
Dataport-Verbund

Dataport ist der IT-Partner für den öffentlichen Sektor:

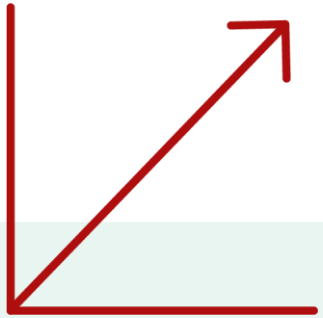
- Für die Länder Schleswig-Holstein, Hamburg, Bremen, Sachsen-Anhalt
- Für die Kommunen in Schleswig-Holstein
- Für die Steuerverwaltungen in Mecklenburg-Vorpommern und Niedersachsen

Zahlen und Fakten (2018)

8 Standorte

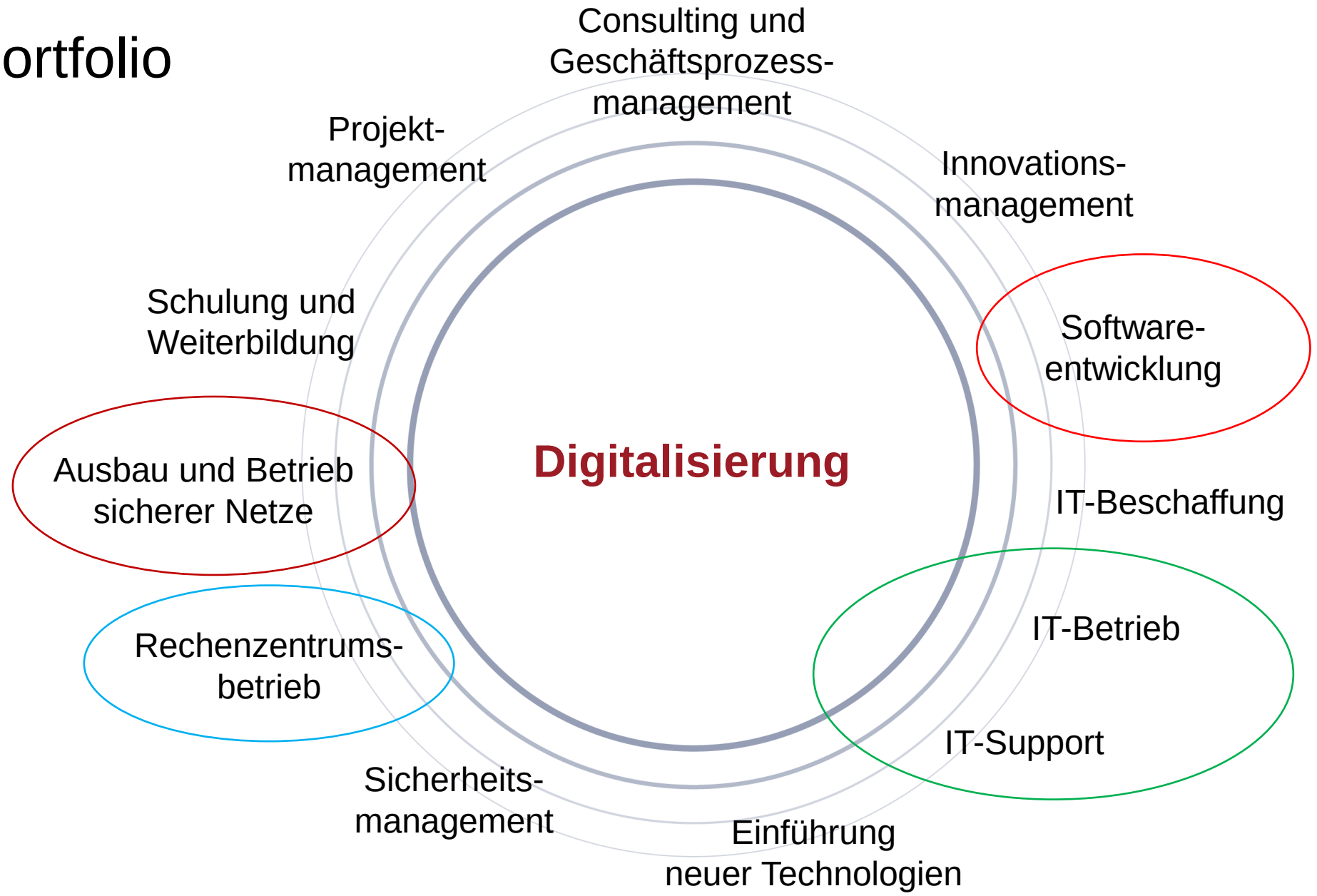


3.000 Mitarbeiter



636 Mio. Euro Umsatz

Portfolio


Consulting und Geschäftsprozess-management
Projekt-management
Innovations-management
Schulung und Weiterbildung
Software-entwicklung
Digitalisierung
Ausbau und Betrieb sicherer Netze
IT-Beschaffung
Rechenzentrums-betrieb
IT-Betrieb
IT-Support
Sicherheits-management
Einführung neuer Technologien

Informationssicherheit in Zahlen

- Über 50 Funktionsträger mit ca. 40 Vollzeitequivalenten in drei Kernrollen im Sicherheitsmanagement
  - Zzgl. 4 MA im Stab
  - Zzgl. mehr als 90 betrieblich-operative Sicherheitsspezialisten
- 3 gültige Zertifikate nach ISO 27001 auf Basis von IT-Grundschutz
- Ein gültiges PS 951 Testat
- Ein TÜV-IT Trusted Site Level 4 zertifiziertes Rechenzentrum an zwei Standorten (Twin Datacenter)
- 2018 flossen ca. 10% des Umsatzes in Sicherheitsaufgaben (nach Gartner Benchmark)

1. Was fordert uns im Sicherheitsmanagement bei Dataport?

2. Bedrohungen und Verwundbarkeiten – was erleben wir?

3. Wie begegnen wir dem?

4. Was kann man KMU empfehlen?

Anforderungen

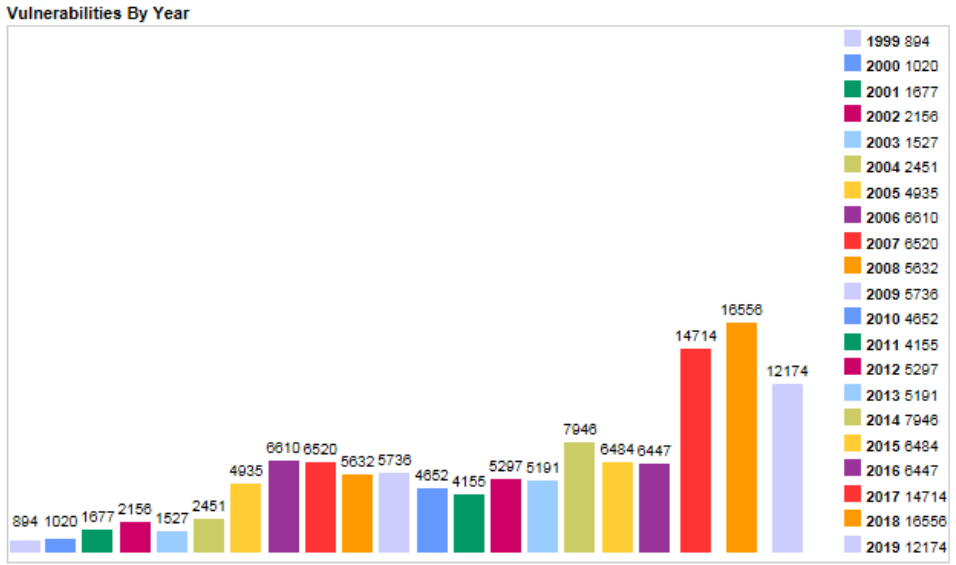
- Normanforderung: ISO 27001 auf Basis von IT-Grundschutz
- Spezifische Sicherheitsanforderungen von Kunden:
  - Polizei
  - Justiz
  - (Teil-) Banken
- BSI-Gesetz und KRITIS-VO
  - Aufwachsend: Landesbetriebe unserer Träger
- Ergebnis: Wir müssen **sehr hohe Sicherheitsanforderungen** erfüllen können

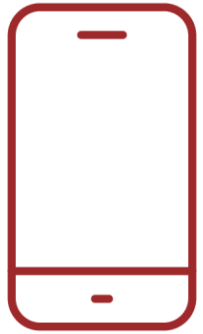
Anforderungen

- Stichwort Digitalisierung: IT spielt in der öffentlichen Verwaltung eine wachsende Rolle (z.B. durch Einführung der eAkte)
- Komplexität der IT-Verfahren steigt
- Vernetzung nimmt zu
- Öffnung der IT gegenüber dem Bürger und damit dem Internet wächst rasant (Online-Zugangsgesetzt bringt die Anbindung von 575 Verwaltungsverfahren an das Internet innerhalb von drei Jahren)

Bedrohungslage und Verwundbarkeiten – Was erleben wir?

- Zahl der Sicherheitslücken wächst erheblich
- Lebenszyklen von IT-Produkten werden kürzer
- „Consumerization“ von IT:
  - Softwarelizenzen werden zunehmend durch (für Endkunden entwickelte) IT-Dienste (Software as a Service, SaaS) ersetzt
  - Produkte aus dem Consumerbereich (Mobiltelefone, SmartTVs, IoT-Devices etc.) dringen oft ohne Anpassung in den Enterprise-Bereich vor





Bedrohungslage und Verwundbarkeiten – Was erleben wir?

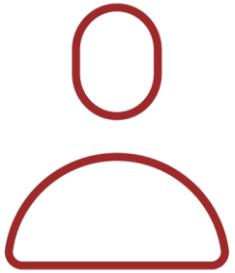
- Phishing, Spearphishing etc.
  - Wird in geringem Umfang, aber regelmäßig beobachtet
  - Angriffs-Mails werden immer besser auf die Situation in den Behörden / bei uns zugeschnitten
- Informationsquellen der Angreifer sind:
  - Öffentlich zugängliche Informationen (u.a. Webseiten und Social Media)
  - Abgeflossene Daten (Mailpostfachinhalte mit Adressen, Kommunikationsbeziehungen, inhaltlichem Kontext)

Bedrohungslage und Verwundbarkeiten – Was erleben wir?

- Schadsoftware entwickelt sich rasant
  - Haupteingangsweg: E-Mail
  - Multifunktionale Schadsoftware-Toolkits (z.B. Emotet)
  - Infektionsroutinen immer ausgefeilter
  - Funktionen zur Ausbreitung in der befallenen Infrastruktur werden immer raffinierter
  - Schadfunktion wird immer wirksamer (z.B. bei Verschlüsselungstrojanern)

Bedrohungslage und Verwundbarkeiten – Was erleben wir?

- Wir können nicht verlässlich verhindern, dass Benutzer Schadsoftware ausführen
  - Awareness hat Grenzen und ersetzt kein Training
  - In bestimmten Funktionen muss man Mails mit Anhängen von unbekannten Absendern öffnen (z.B. Initiativbewerbungen in der Personalabteilung oder Kundenanfragen im Vertrieb)
- DoS kommt gelegentlich mit oder ohne erkennbaren Grund vor
- Hacking spielt aktuell bei uns keine große Rolle



Was unternehmen wir dagegen (strategisch)?

- Standardisierung
  - Informationssicherheit lässt sich nur in einem IT-betrieblich standardisierten Umfeld wirtschaftlich umsetzen
  - 20% der nicht standardisierten Geräte und Verfahren verursachen 80% Aufwand im Sicherheitsmanagement
- Norm-Orientierung (ISO 27001 auf Basis von IT-Grundschutz)
- Umsetzung einer Zertifizierungsstrategie

Was unternehmen wir dagegen (operativ präventiv) (1)?

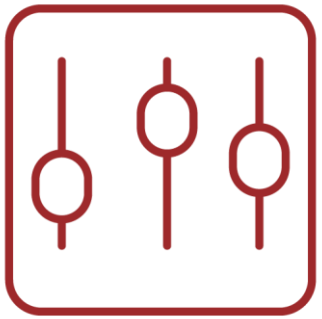
- Systemhärtung (Abschaltung nicht benötigter Betriebssystemfunktionen und –Dienste)
- Patchmanagement
- Restriktives Berechtigungsmanagement
- Trennung von Client- und Serveradministration
- Einsatz des AppLockers mit geeigneten Policies auf Endgeräten
- Sandboxing gefährdeter Anwendungen (v.a. Browser)

Was unternehmen wir dagegen (operativ präventiv) (2)?

- Makrosicherheit
- SPAM-Schutz
- Automatisierte Sperrung des Internetverkehrs zu bekannten C&C-Servern
- …
- Virenschutz (zentral z.B. am Maileingang / dezentral auf dem Client)

Was unternehmen wir dagegen (reaktiv)?

- Monitoring und Überwachung von Systemen, Einsatz eines Security Incident und Eventmonitoring (SIEM)
- Überwachung von Schadsoftware- und SPAM-Ereignissen
- Monitoring des Kommunikationsversuches zu bekannten C&C-Servern
- Schadsoftwareforensik
- Koordination und Steuerung von Gegenmaßnahmen im Security Operation Center (SOC)
- Sicherheitsvorfallmanagement (Haupteingang: Meldungen von Benutzern)



Was erreichen wir mit diesen Mitteln?

- Bei ca. 40.000 standardisiert bereitgestellten Endgeräten in Hamburg gab es 2019 nur 2 Schadsoftwareinfektionen
  - In beiden Fällen handelte es sich um Sonderclients mit erweiterten Benutzerrechten
  - Schadcode: Emotet-Loader
  - Datenabfluss: keiner

Woran arbeiten wir?

- Einführung neuer Monitoring- und Reaktions-Technologien
  - Netzverkehrsanalyse
  - Endpoint-Protection (erweiterte Host-Intrusiondetection)
  - NG-Firewalling
- Optimierung der Endgerätekonfiguration
  - Win10 hat neue Funktionen zur Steuerung der Ausführung von Code über Netze (Remote Execution)

Was kann man KMU empfehlen?

- Achten Sie auf aktuelle und gepatchte Betriebssysteme
- Trennen Sie Gerätenutzung von Geräteadministration, beschränken Sie Benutzerrechte
- Nutzen Sie neben einem Virenschutz den AppLocker
- Tragen Sie Sorge für eine funktionierende Datensicherung
- Schützen Sie den Übergang zum Internet (Firewall)
- Kaufen Sie ggfs. Sicherheitsdienstleistungen wie Firewallmanagement, SPAM-Schutz etc. ein

Dr. Martin Meints
IT-Sicherheitsbeauftragter
martin.meints@dataport.de

Anstalt des öffentlichen Rechts
Altenholzer Straße 10–14
24161 Altenholz
dataport.de

dataport