TRENDS IN DER IT

Kapitel 8
Sicherheit als kritischer Erfolgsfaktor
Standards und ITIL Version 4.0

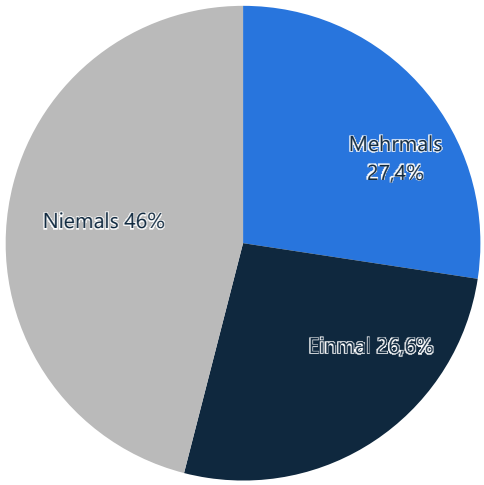
Das Update für Experten

Security-Trends 2020

Die Top-10-Bedrohungen 2020:

- Social Engineering und Phishing
- 2. Einschleusen von Schadsoftware über externe Geräte
- 3. Infektion mit Schadsoftware über Internet oder Intranet
- 4. Einbruch über Fernwartungszugänge
- 5. Menschliches Fehlverhalten und Sabotage
- 6. Internet-verbundene Steuerungskomponenten
- 7. Technisches Fehlverhalten und höhere Gewalt
- 8. Kompromittierung von Extranets und Cloud Komponenten
- 9. (D)Dos Angriffe
- 10. Kompromittierung von Smartphones im Produktionsumfeld

War Ihre Organisation jemals Opfer einer Cyberattacke oder eines Datendiebstahls?

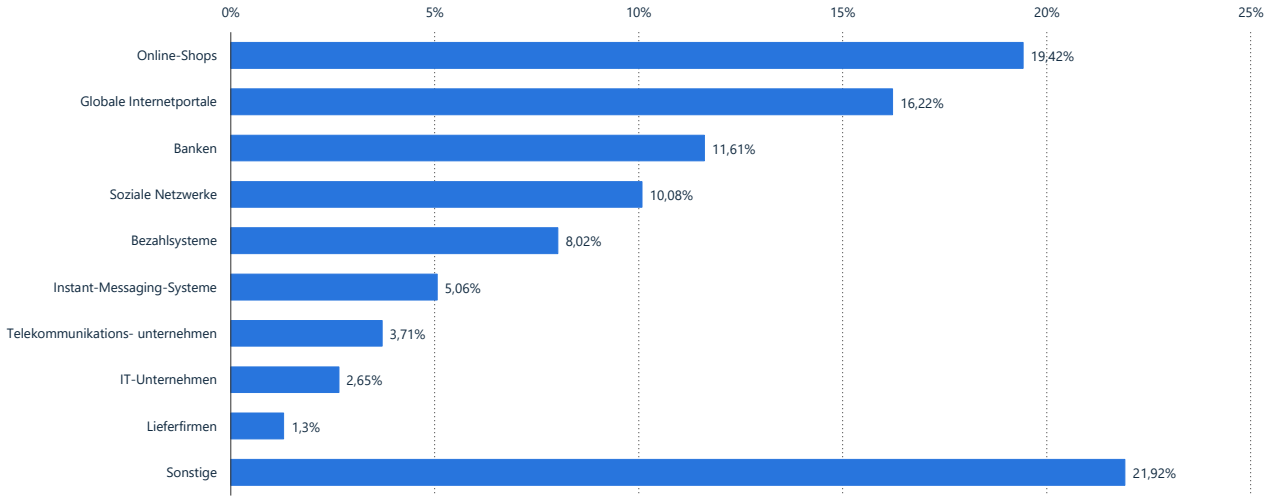


IT-Sicherheit

Folie: 3

3

Verteilung der Phishing-Angriffe nach Kategorie der angegriffenen Organisationen im 2. Quartal 2020



Quelle(n): Kaspersky

IT-Sicherheit

Folie: 4

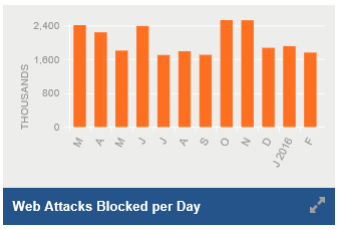
4

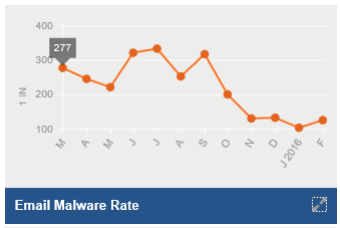
Der sichere Arbeitsplatz im Unternehmen

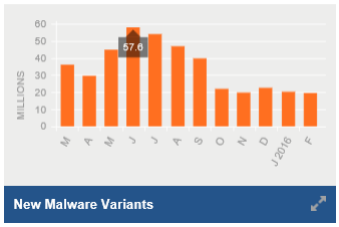
- Patch-Management für OS
- zentraler Virenschutz
- Authentifizierung und VPN
- Patch-Management für BIOS/UEFI

  - Software-Verteilung
    (Terminalserver oder Verteilungstools)
  - Inventarisierung
  - Richtlinien
  - Remotesteuerung
  - Standard-Arbeitsplätze
  - Wiederherstellung und Wiederherstellungspläne

Ausgangslage Virenschutz

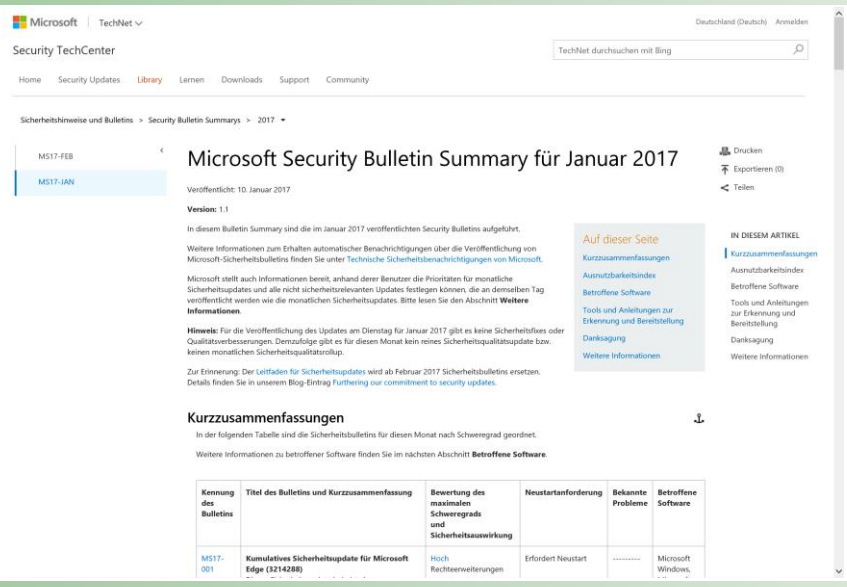






Quelle: Symantec

Ausgangslage Patch-Management
März 2016 mit 14 Patche, 01/2017 nur vier

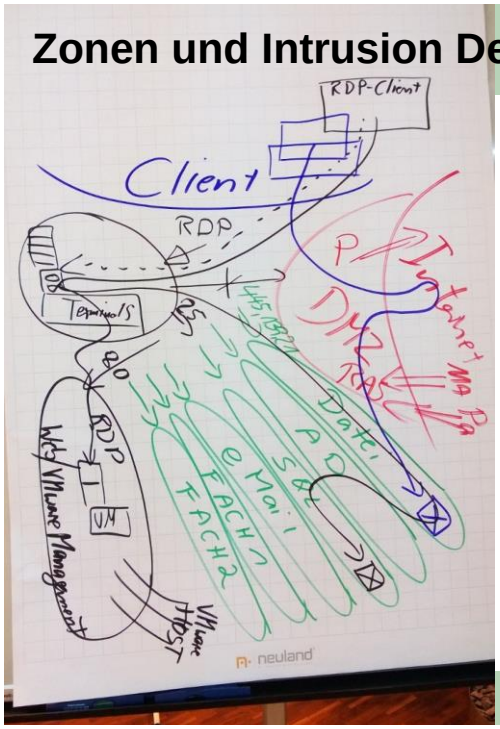


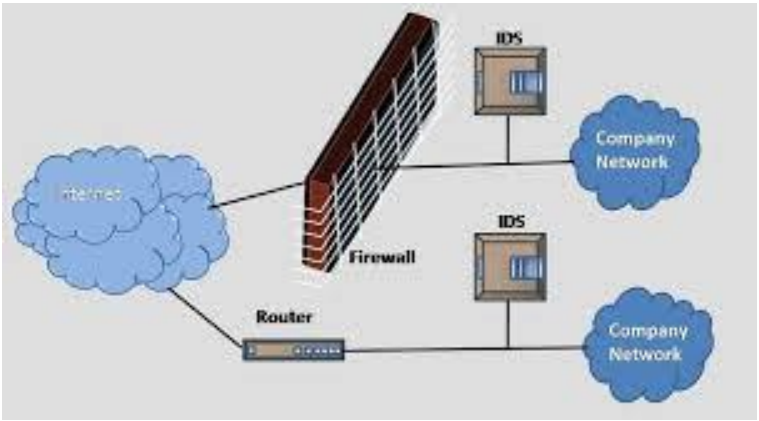
Der sichere Arbeitsplatz für den Administrator

- Patch-Management
- zentraler Virenschutz
- Authentifizierung und VPN

- kein eMail
- kein Internet
- kein externer Datenträger

Zonen und Intrusion Detection System





Welches Zertifikat?

• ISO/IEC 20000	ITIL 4.0
• ISO/IEC 27001:2014	ISMS
• IT-Sicherheitsgesetz	vom 12.06.2015
• DSGVO	Datenschutz
• BSI	IT-Grundschutz
• ISO 9000	QS
• 15408	Bewertung
• COBIT	IT- Governance
• ISO/IEC 31000	Risikomanagement
• COSO ERM	RISK
• SAS70/ISAE 3402	Outsourcing

IT-Sicherheitsgesetz vom 12. Juni 2015

- Über 100 neue Stellen für das BSI
- Anpassung des IT-Grundschutz in Abstimmung mit der ISO/IEC 27001:2013
- Für:
  - Betreiber Kritischer Infrastrukturen wie Banken und Versicherungen
  - Genehmigungsinhaber nach dem Atomgesetz
  - Energieversorger
  - Telekomanbieter
  - voraussichtlich Mai 2017: Rechtsverordnung zur Bestimmung Kritischer Infrastrukturen in den KRITIS-Sektoren Transport und Verkehr, Gesundheit, Finanz- und Versicherungswesen
- Noch immer keine klaren Vorgaben
- ISO/IEC 27001:2013 geht am weitesten

- IT-Sicherheitsgesetz 2.0 – Entwurf liegt vor.
  - Lebensmittelversorgung, Krankenhäuser, Laborinformationssystems und Abfallentsorgung

DIN ISO/IEC 27001:2014 und 27002:2016

- ISO 27001:2013 ist das ISMS
  (Information Security Management System)

- ISO 27001 ist vornehmlich ein Managementsystem für Information Security
- Garantiert die richtige und ganzheitliche Strategie der Firma beim Umfeld Security

- Neu überarbeitet und am 10.01.2014 wurde die deutsche Übersetzung veröffentlicht
- Überarbeitung der ISO 27002 im November 2016 abgeschlossen

DSGVO Datenschutz-Grundverordnung

- Die DS-GVO ist wegen Auslegungsoffenheit, Inkohärenzen, Wertungswidersprüchlichkeiten und Lückenhaftigkeit
- **Stichtag ist der 25. Mai 2018 für Alle!**
- Die wichtigsten Bereiche sind:
  - Die Einführung eines Enterprise Content Management (ECM) unter Berücksichtigung der DS-GVO
  - Überprüfung der ERP-Systeme wie SAP
  - Technische und organisatorische Maßnahmen, um Mitarbeiter zum Verantwortlichen Umgang mit personenbezogenen Daten zu verpflichten (Stichwort: Bewerbungsunterlagen und Outlook)
  - Aufbau eines Verarbeitungsverzeichnisses
  - Überprüfung der Aufbewahrungsfrist für persönliche Daten in allen Systemen
  - ….

Datensicherheit und Datenschutz in der Cloud

- Anforderungskatalog Cloud Computing (C5) der BSI
- Einhaltung Trusted Cloud Datenschutzprofil (TCDP)
- DSGVO-Konformität (TCDP gilt noch nicht als ausreichend)
  - Vor allem Einhaltung der DSGVO § 15 – Auskunftsrecht
- ISO 27001-Konformität
  - Identitäts- und Zugriffsverwaltung
  - Zugangsschlüssel
  - Dienst- und Ressourcen-Isolierung
  - Ereignisüberwachung
  - Automatisierte Kontrollen
  - Frühwarnsysteme und Audit-Dienste
  - Datenverschlüsselung
  - Penetrationstests
  - KI-gestützte Compliance

ITIL V4

Februar 2019 veröffentlicht

Weiterführung von ITIL V3 Prozessen

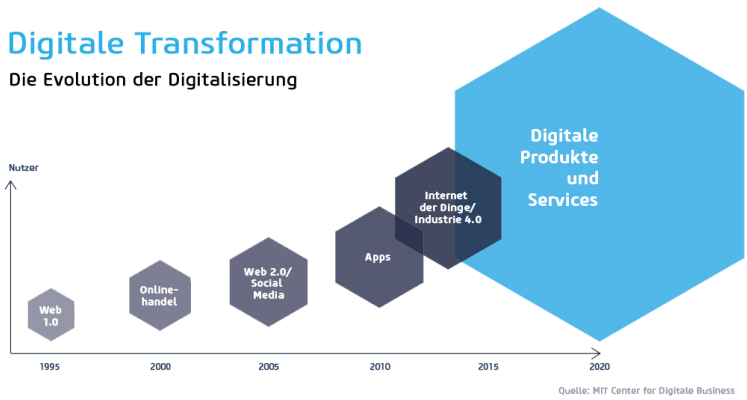
Wie V3 schon: ganzheitlicher Ansatz für das Service-Management

Neuer Ausrichtung:

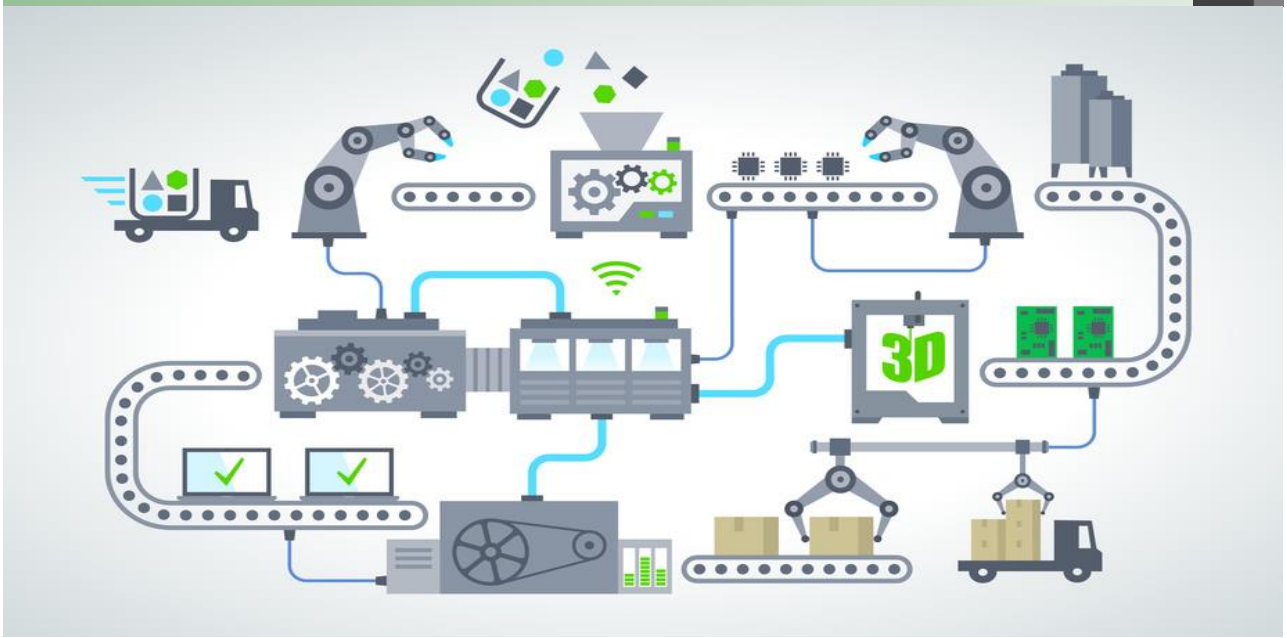
- Unterstützung der digitalen Transformation
- Schaffung von Mehrwert
- Integration von Agile und DevOps in ITSM-Strategien
- Konzentrierung auf Kosten, Ergebnissen, Risiken und Werte
- Teamarbeit und Kommunikation erhalten zusätzliches Gewicht

„digitale Transformation“

- Digitale Transformation und Digitalisierung werden häufig synonym gebraucht.
- Unter Digitalisierung versteht man den Prozess analoge Unternehmensprozesse zu digitalen Unternehmensprozessen – häufig in Form von Automatisierung – umzuformen.



Digitale Transformation im Unternehmen



17

- **DevOps** beschreibt einen Prozessverbesserungs-Ansatz aus den Bereichen der Softwareentwicklung und Systemadministration.
- **DevOps** ist ein Kunstwort aus den Begriffen Development (englisch für Entwicklung) und IT Operations (englisch für IT-Betrieb).

DevOps

Folie: 18

18

Herzstück von ITIL V4 die vier Dimensionen

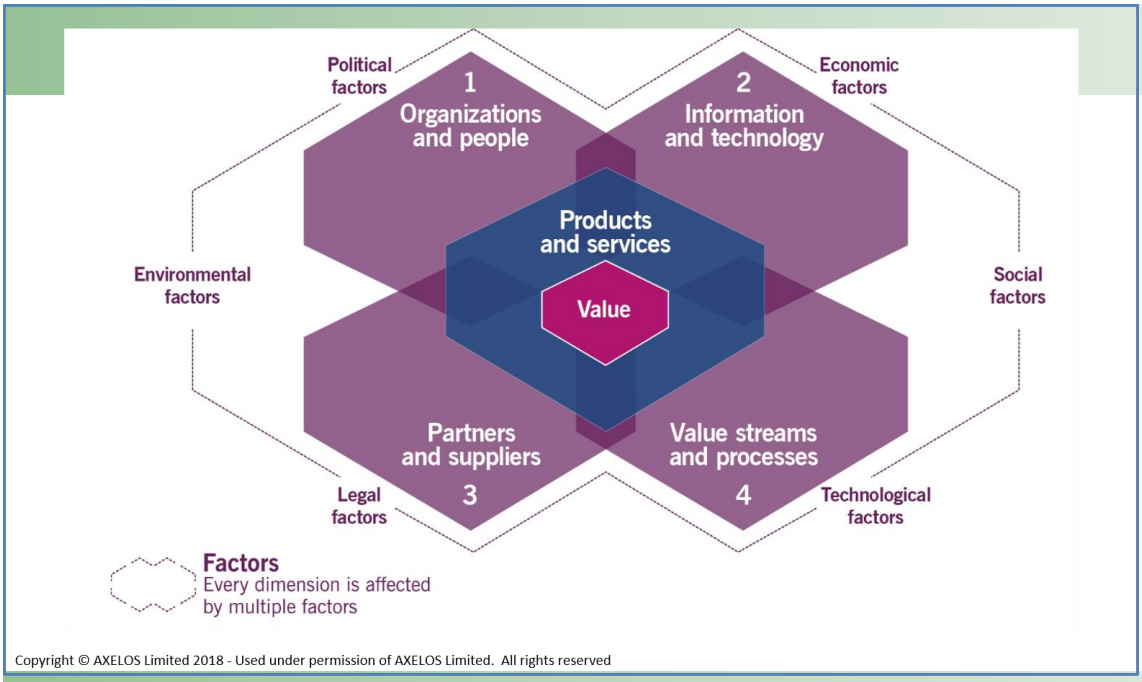
- Organisationen und Menschen
  - **Menschen**: Die Mitarbeiter, die für die Erbringung von IT-Dienstleistungen verantwortlich sind. Diese Fachleute sollten, über die für die Erbringung von Dienstleistungen erforderlichen Fähigkeiten und Kompetenzen verfügen.

- Informationen und Technologien
  - **Produkte**: Unter Produkte verstand man die Werkzeuge, Dienstleistungen und Technologien, die bei der Bereitstellung und Unterstützung der Dienstleistungen verwendet werden.

Herzstück von ITIL V4 die vier Dimensionen

- Partner und Lieferanten
  - **Partner**: Bei der Gestaltung von Diensten sollten Anbieter, Hersteller und Lieferanten berücksichtigt werden, da sie zur Unterstützung des Dienstes verwendet werden, sobald dieser in Betrieb ist.

- Wertströme und Prozesse
  - **Prozesse**: Prozesse sind zentral und wichtig zur Unterstützung und Verwaltung der angebotenen Dienstleistungen, so dass die Dienstleistungen den Kundenerwartungen und den vereinbarten Service Levels entsprechen. Alle Prozesse müssen messbar sein.



ITIL V3 versus ITIL V4

- In ITIL 4 geht es nicht um die Einführung grundlegend neuer Ideen für das Service-Management.
- Das bewährte ITIL-Framework soll nicht ersetzt, sondern erweitert werden.
- Im Grunde enthalten ITIL 4 und ITIL V3 Empfehlungen, die auf denselben Prinzipien beruhen - aber die neue Version 4 verfolgt einen anderen Ansatz zur Darstellung dieser Empfehlungen.

- Der Service-Lifecycle wurde in ITIL 4 aufgegeben und die Prozesse mit Praktiken ersetzt. Aber viele der Praktiken in ITIL 4 entsprechen eindeutig den früheren ITIL-V3-Prozessen.