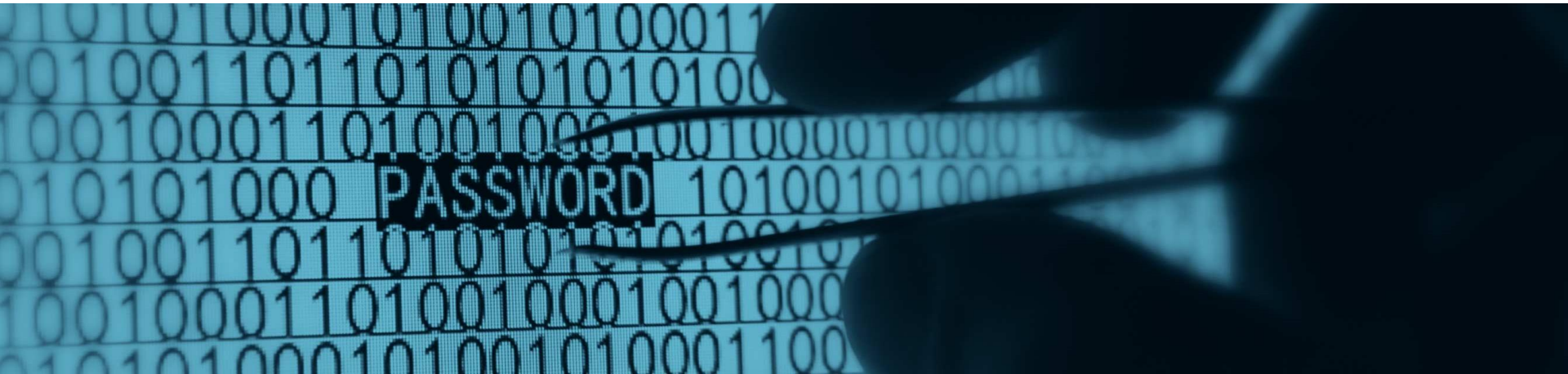
AMT FÜR INFORMATIK
FÜRSTENTUM LIECHTENSTEIN

Informationssicherheit «Umsetzung in der Praxis»

"Falls man glaubt,
dass Technologie alle Sicherheitsprobleme lösen kann,
versteht man die Probleme nicht
und hat von Technologie keine Ahnung."

Bruce Schneier

27. Oktober 2016



Zu meiner Person

Thoma Patrik - 1972

- Information Security Manager – Liechtensteinische Landesverwaltung
  - patrik.thoma@llv.li
  - +423 236 76 07

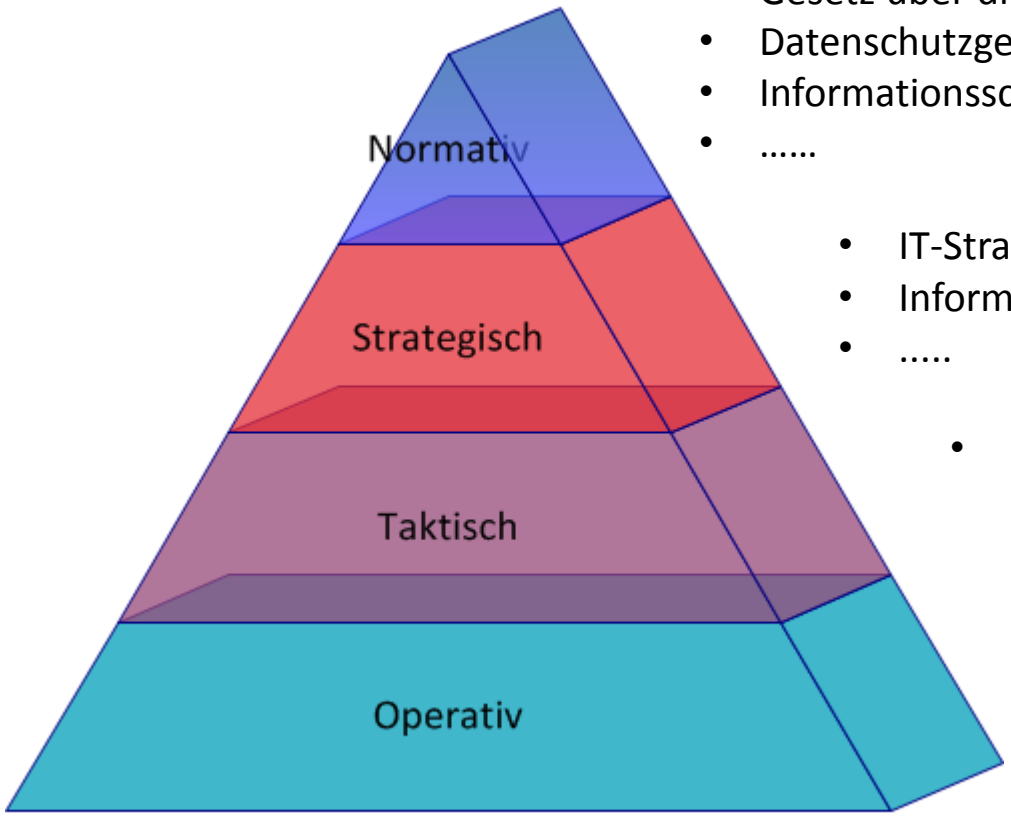
Aufgaben

- Sicherheitskonzepte & -analysen überprüfen
- Aufbau, Einführung & Weiterentwicklung ISMS
- Awareness
- Ausarbeitung & Anpassung von Sicherheitsvorschriften
- Umsetzung & Weiterentwicklung der Sicherheitsvorschriften
- Security-Audits
- Risikoeinschätzungen

Agenda

1. Sicherheitspyramide
2. ISMS – Grundschutz
   - ISO 27000er Familie
   - IST-SOLL-Zustand
3. Projekt-Management
   - ISDS-Schutzbedarfsanalyse
   - Datenschutz-Prüffragen
4. Risikobasierter Ansatz
   - Malware

1 - Sicherheitspyramide



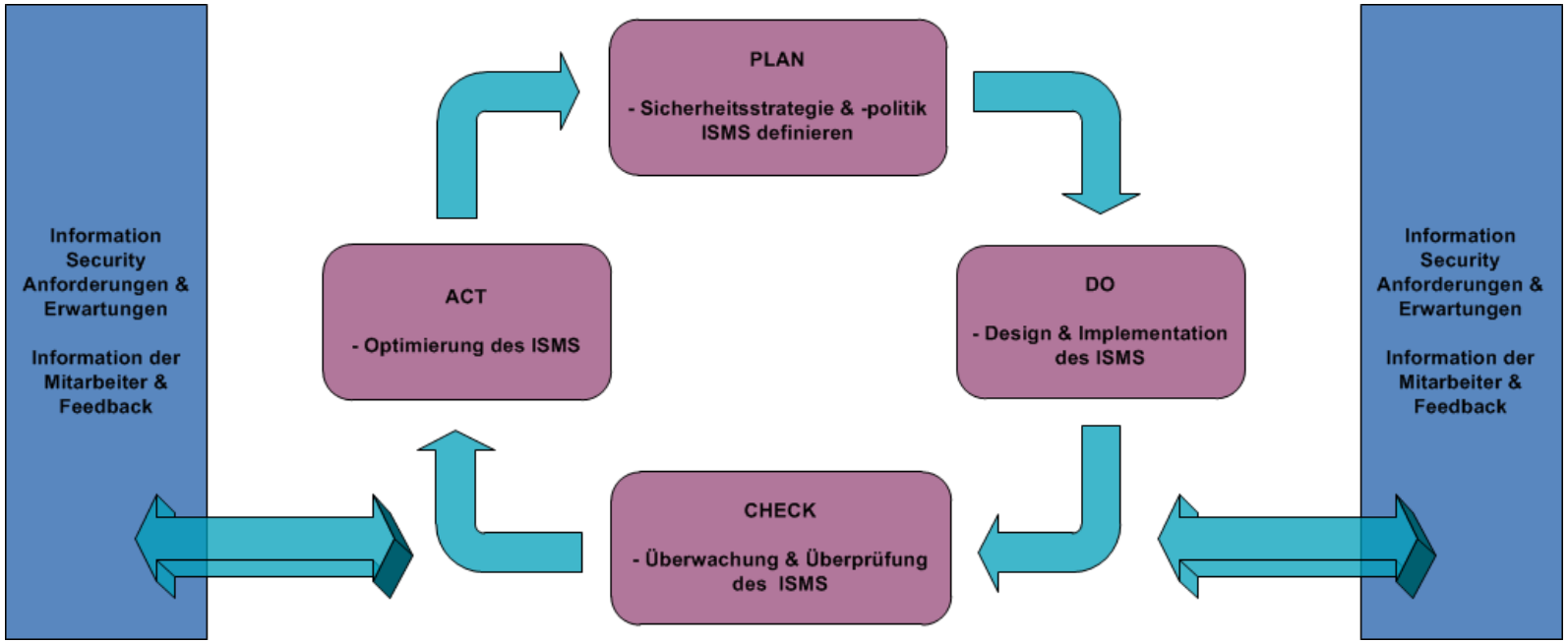
- Verfassung
- Gesetz über die Regierungs- und Verwaltungsorganisation
- Datenschutzgesetz
- Informationsschutzverordnung
- ……

- IT-Strategie 2015 - 2018
- Informations-Sicherheitspolitik
- .....

- Betriebs-Konzepte
  - Backup-Konzept
  - Anti-Malware-Konzept
  - .....

- Massnahmen
  - ITSM
  - Informatik-Handbuch
  - .....

2 - Information Security Management System «Grundschutz»



Der PDCA-Zyklus, oder auch Demingkreis, beschreibt einen iterativen vierphasigen Problemlösungsprozess, der seine Ursprünge in der Qualitätssicherung hat. PDCA steht hierbei für das Englische „Plan-Do-Check-Act“ was im Deutschen mit Planen Umsetzen-Überprüfen-Handeln übersetzt werden kann.

2 - ISO/IEC 27001:2015

ISO 27001:2015

Der internationale Standard ISO/IEC 27001:2015 beschreibt eine **Methode**, welche die **Ausarbeitung, Umsetzung, Beherrschung und ständige Verbesserung** der Informationssicherheit ermöglicht.

- **international führender Standard** für den Aufbau eines Information Security Management Systems
- seit 1993 **ständig weiterentwickelt und verbessert**
- **systematisch und strukturierter** Ansatz
- **tausendfach** in der Praxis **erprobt**
- **weltweit anerkanntes Qualitäts- & Gütesiegel** für Informationssicherheit

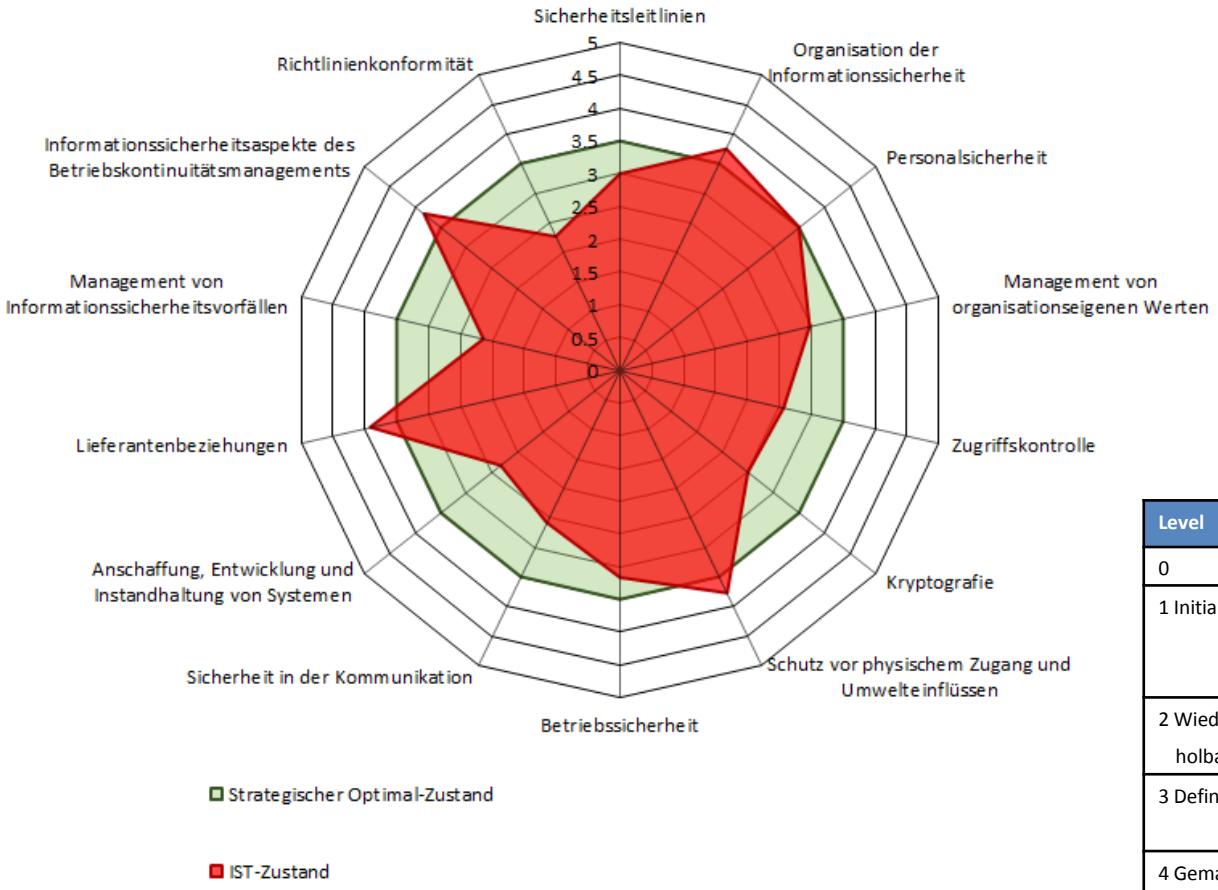
2 - ISO/IEC 27002:2013

ISO 27002:22013

Der internationale Standard ISO/IEC 27002:2013 beinhaltet diverse **Empfehlungen** betreffend **Kontrollmechanismen** für die Informationssicherheit. Der aktuelle ISO/IEC 27002:2013 Standard gliedert sich in **14 Abschnitte**, welche in **35 Hauptkategorien** mit **113** einzelnen **Sicherheitsmassnahmen** unterteilt sind.

1. Sicherheitsleitlinie
2. Organisation der Informationssicherheit
3. Personalsicherheit
4. Management der organisationseigenen Werten
5. Zugriffskontrolle
6. Kryptographie
7. Schutz vor physischem Zugang & Umwelteinflüssen
8. Betriebssicherheit
9. Sicherheit in der Kommunikation
10. Anschaffung, Entwicklung & Instandhaltung
11. Lieferatenbeziehungen
12. Management von Informationssicherheitsvorfällen
13. Informationssicherheitsaspekte des BCM
14. Richtlinienkonformität

2 - IST-SOLL-Zustand – ISO 27002:2013



Level	Beschreibung
0	Keine Prozessumsetzung geplant
1 Initial	Prozess ist in Entwicklung. Teilweise bestehen einzelne Beschreibungen. Arbeiten werden grundsätzlich Ad-Hoc ausgeführt.
2 Wieder-holbar	Prozess und Umsetzung ist ansatzweise dokumentiert. Fehler in der Abwicklung gibt es regelmässig.
3 Definiert	Prozess ist standardisiert, klar dokumentiert und es gibt eine gute Tool-Unterstützung. Prozess wird eingehalten.
4 Gemanagt	Prozess wird laufend überwacht und stetig verbessert sowie regelmässig ausgebildet.
5 Optimiert	„Best in Class“-Einführung und -Nutzung.

CMMI - Maturitätsmodell

2 - Stärken & Schwächen ISO 2700x

- **Stärken:** „Best Practices“-Vorgaben, konkrete Schritte / pragmatischer Ansatz, Umsetzbarkeit / Anpassbarkeit, praxis- und massnahmebezogen, übersichtliche Struktur, Branchenunabhängigkeit, ISO-Standard (Standardisierung), Zertifizierung

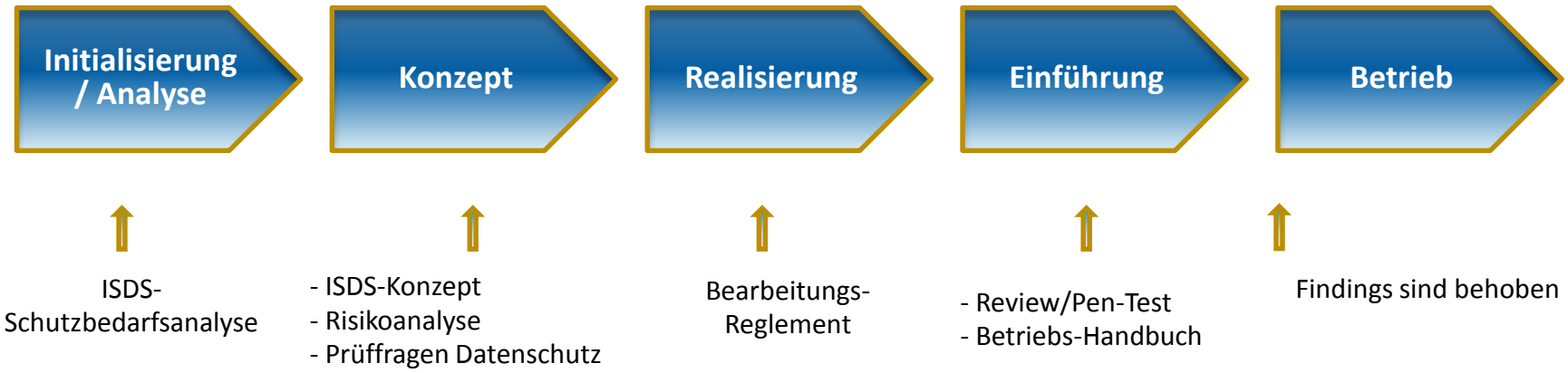
- **Schwächen:** Kontrollen nicht nach Vertraulichkeit, Integrität und Verfügbarkeit gruppiert, Prozessrisiken nicht berücksichtigt, für Grundschutz ausgelegt, kein Vorgehensplan

- **Einsatz primär für:** Risiko- und Grobanalysen, Benchmarking, Grundlage für Sicherheitskonzepte

- **Nicht unbedingt geeignet für:** Erstellung eines Sicherheitshandbuches mit detaillierten Umsetzungsvorgaben

3 - Informationssicherheit im Projekt-Management - HERMES

http://www.hermes.admin.ch/



- strukturierte Vorgehensweise
- verbesserte Kommunikation zwischen Fachabteilung/Anwendern, Entwicklern und Betreibern
- kleinere Projektrisiken
- Transparenz bei den Projektphasen

3 - ISDS-Schutzbedarfsanalyse

Kriterien	Fragen	Antwort (DropDown-Menu)
Vertraulichkeit	Werden schutzwürdige Daten (nicht DSG / ISchV relevant) bearbeitet?	Keine erhöhten Anforderungen an die Schutzwürdigkeit (nicht DSG/ISchV relevant)
		Erhöhte Anforderungen an die Schutzwürdigkeit (nicht DSG/ISchV relevant)
	Welche Art von Personendaten werden bearbeitet (nach Datenschutzgesetz, DSG)?	Kein Schutzbedarf (keine Personendaten)
		Personendaten mit normalem Schutzbedarf
		Personendaten mit mittlerem Schutzbedarf
		Personendaten mit hohem Schutzbedarf
	Sind die Daten / Informationen zu klassifizieren (nach Informationsschutzverordnung ISchV)?	NICHT KLASSIFIZIERT
		EINGESCHRÄNKT
		VERTRAULICH
		GEHEIM
	Wie hoch schätzen Sie den Schaden, falls Datensätze der Applikation in den Medien (Internet, Zeitung etc.) publiziert werden?	Geringe Auswirkung und kein Imageverlust (fast niemand nimmt Kenntnis)
		Mittlere Auswirkung und mittlerer Imageverlust (nationale Medien berichten)
		Grosse bis katastrophale Auswirkung und grosser Imageverlust (internationale Medien berichten)

3 - ISDS-Schutzbedarfsanalyse

Kriterien	Fragen	Antwort (DropDown-Menu)
Verfügbarkeit	Max. zulässige Ausfalldauer während der gewährleisteten Servicezeit?	Ausfalldauer Priorität 4 – 40 Std.
		Ausfalldauer Priorität 3 – 20 Std.
		Ausfalldauer Priorität 2 – 10 Std.
		Ausfalldauer Priorität 1 – 4 Std.
	Wie stufen Sie einen Ausfall der Applikation ein?	Dienstleistungserbringung der LLV nicht wesentlich gestört (Abteilungsweiter Ausfall)
		Dienstleistungserbringung der LLV wesentlich gestört (Amtsstellenweiter Ausfall)
		Dienstleistungserbringung der LLV verunmöglicht (LLV-weiter Ausfall)
	Servicezeiten?	Basis Servicezeit Mo-Fr 07:00 – 18:00 (exkl. Feiertage & Dienstfrei)
		7 x 24 Std. (365 Tage)
	Bedarf nach Katastrophenvorsorge (Business Continuity Management)?	Katastrophenvorsorge notwendig: Nein
		Katastrophenvorsorge notwendig: Ja

Kriterien	Fragen	Antwort (DropDown-Menu)
Integrität	Muss die Echtheit, Korrektheit und/oder Unversehrtheit der Daten nachgewiesen werden können?	Keine speziellen Anforderungen
		Spezielle Anforderungen
Nachvollziehbarkeit	Müssen bestimmte Arbeitsvorgänge nachgewiesen werden können?	Keine speziellen Anforderungen
		Spezielle Anforderungen

3 - Datenschutz-Prüffragen

	Datenberabeitung allgemein sowie Prüfung Voraussetzungen für Bearbeitungsreglement (Art. 21 Abs. 1 DSV)	Ja	Nein
1	Wurde der behördliche Datenschutzverantwortliche des Dateninhabers - jenes Amt ist Dateninhaber, welches über Zweck und Inhalt entscheidet - in die Planung eingebunden?		
2	Werden Daten über die religiösen, weltanschaulichen und politischen Ansichten oder Tätigkeiten einer Person bearbeitet?		
3	Werden Daten über die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit einer Person bearbeitet?		
4	Werden Daten über die Massnahmen der sozialen Hilfe von Personen bearbeitet?		
5	Werden Daten über administrative oder strafrechtliche Verfolgungen und Sanktionen einer Person bearbeitet?		
6	Werden Daten bearbeitet, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlauben? (Persönlichkeitsprofile)		
7	Werden die bearbeiteten Daten durch mehrere Behörden benutzt? (z. B. Weitergabe auf Anfrage)		
8	Greifen Dritte (Behörden oder Private, wie bspw. Unternehmen) direkt (auch auszugsweise) auf die bearbeiteten Daten zu? (vgl. Abrufverfahren; Art. 23 Abs. 3 DSG).		
9	Werden Daten ausserhalb des LLV-Netzes (bspw. bei externen Dienstleistern) bearbeitet oder gespeichert?		
10	Findet eine Datenbearbeitung, wie das Beschaffen, Aufbewahren (Speichern), Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten, ausserhalb Liechtensteins statt?		
11	Ist die Datenbearbeitung über das Internet abrufbar? (z. B. Webapplikation, Web-Login)		
12	Werden die bearbeiteten Daten ausländischen Behörden zugänglich gemacht?		
13	Werden die bearbeiteten Daten internationalen Organisationen zugänglich gemacht?		
14	Werden die bearbeiteten Daten privaten Personen zugänglich gemacht?		
15	Ist die Datenbearbeitung mit anderen Datensammlungen verknüpft (z. B. Schnittstellen)?		

3 - Stärken & Schwächen

Stärken

- frühzeitiger Einbezug der Security
- kontinuierliche Begleitung des Projektes aus Sicherheitssicht
- frühzeitige Korrekturmöglichkeiten
- aktive Integration der Security
- klare, einfach verständliche Methodenstruktur

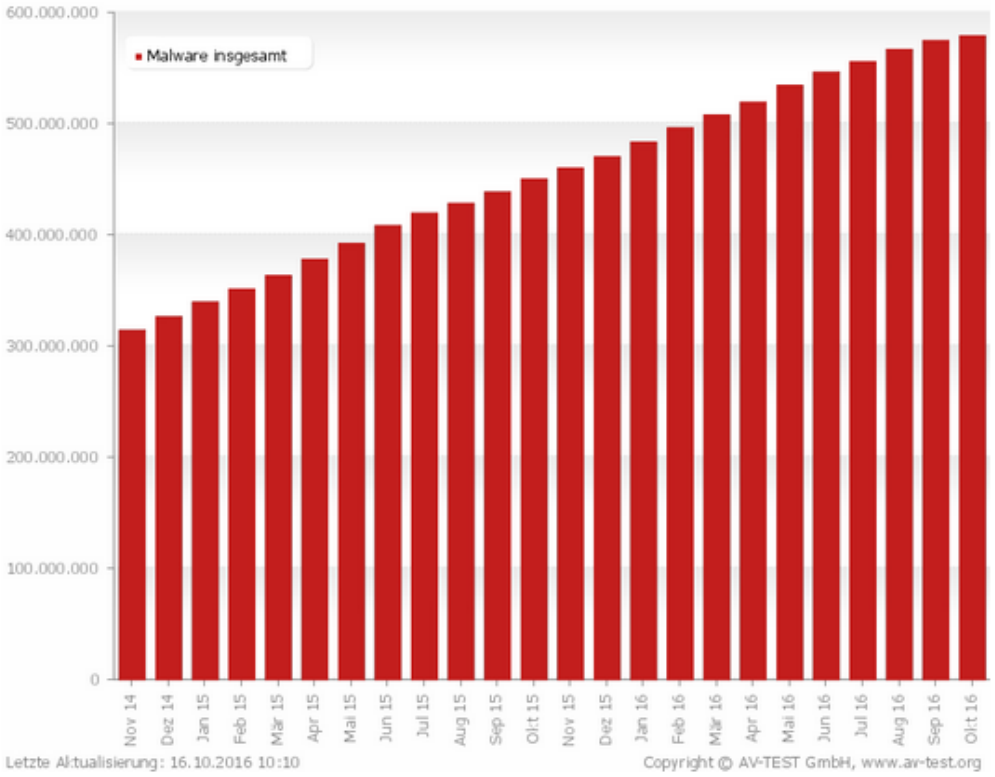
Schwächen

- Erstellen der Vorlagen (Initialaufwand)
- Schulung aller Projektleiter & -mitarbeiter

4 - Risikobasierter-Ansatz

Rang	Bedrohung (IT-Gefahrenbereich)
1	Malware (Viren, Würmer, Trojanische Pferde,...)
2	Irrtum und Nachlässigkeit eigener Mitarbeiter
3	Hacking (Vandalismus, Probing, Missbrauch,...)
4	unbefugte Kenntnisnahme, Informationsdiebstahl, Wirtschaftsspionage
5	Mängel der Dokumentation
6	Software-Mängel-/Defekte
7	Sabotage (inkl. DoS)
8	Hardware-Mängel-/Defekte
9	unbeabsichtigte Fehler von Externen
10	Manipulation zum Zweck der Bereicherung
11	höhere Gewalt (Feuer, Wasser,...)
12	Sonstiges

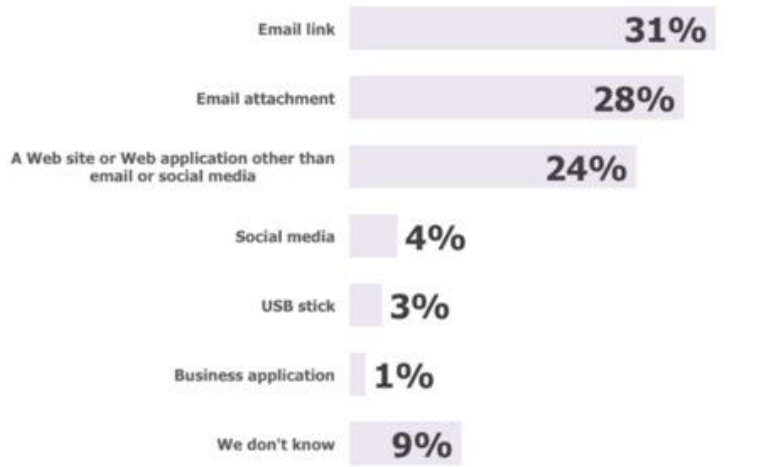
Quelle: Sicherheitsbedrohungen nach <kes> Sicherheitsstudie 2016



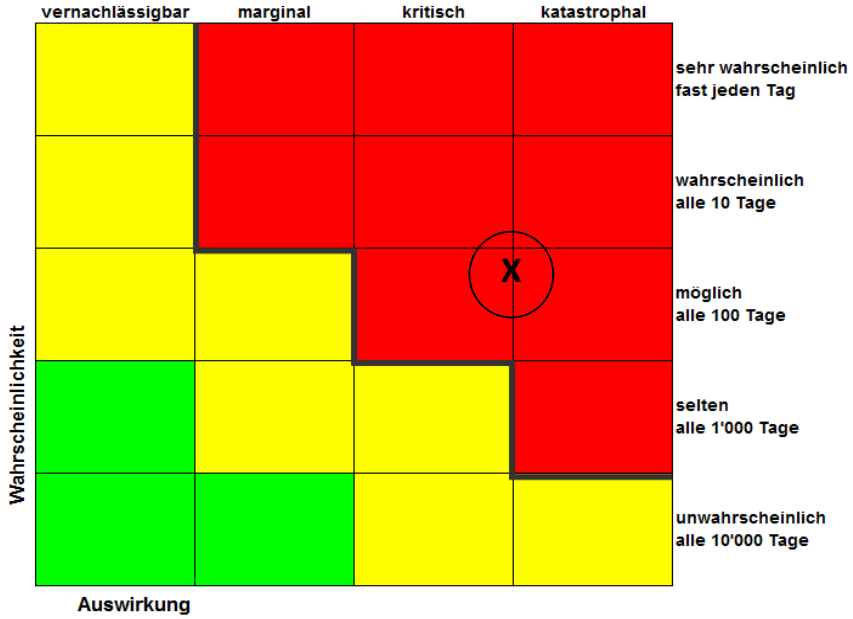
4 - Malware

Email is the #1 delivery vehicle for ransomware

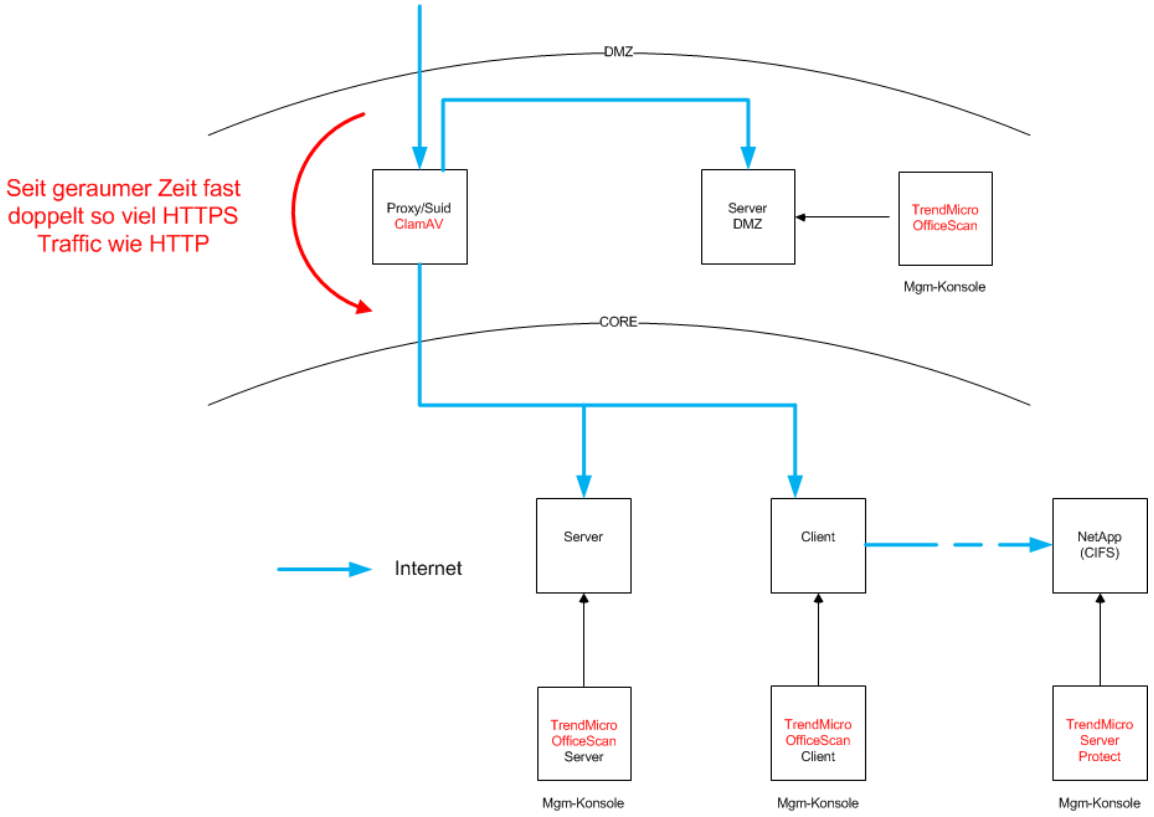
Figure 12
Applications by Which Ransomware Entered the Organization



Source: Osterman Research, Inc.



4 - Malware



Massnahme zur Risiko-Reduzierung – SSL-Interception & Sandboxing

Fragen

Besten Dank für Ihre Aufmerksamkeit