TEMET
end-to-end IT security

Cybersecurity Defense Plan

Information Security in Healthcare Conference

Marcel Hausherr

22.06.2017

Bezug zu Cybersecurity?

Quelle: zazzle.de

- Was sind die Folgen eines seltenen unwahrscheinlichen Ereignisses
- Wir wollen im Nachhinein immer alles einfach erklären können
- Ziel ist es Robustheit und Stabilität zu erreichen

Agenda

TEMET
end-to-end IT security

- Wahrnehmung von Cyberrisiken
  - Bedrohungslage
  - Treiber für Massnahmen
  - Awareness in Unternehmen
- EU Datenschutz-Grundverordnung
  - «In a Nutshell»
- Der Weg zum Cybersecurity Defense Plan
  - Angriffsanalyse / Verteidigungsmöglichkeiten
  - Cybersecurity «Big Picture»
  - Maturitätsbewertung
  - Vorgehensplan
- Schlusswort

Über den Referenten

Marcel Hausherr

Dipl. El.-Ing. HTL, CISA, CRISC, CISSP
M.Sc. Data Communications Systems

Expert IT Security Consultant
In der IT Security tätig seit 1998

Spezialgebiete
Cybersecurity
Identity und Access Management (IAM)
Information Security Management
Risikoanalysen und Sicherheitskonzepte

Kontakt
Tel: +41 79 216 75 50
E-Mail: marcel.hausherr@temet.ch

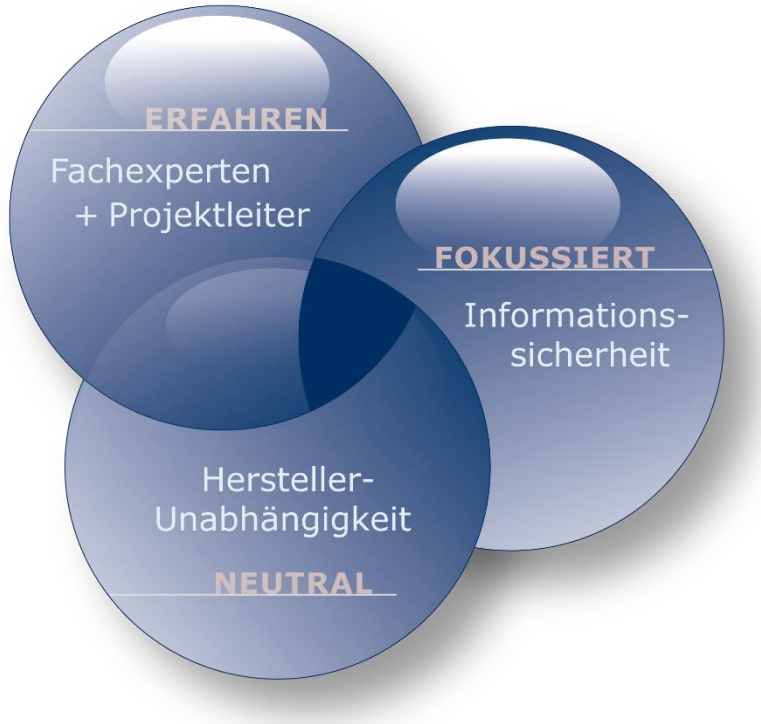
Über die TEMET AG

Mission

- Wir planen, konzipieren und realisieren Sicherheitsprojekte

Alleinstellungsmerkmale

- Wir vereinen fachliche Expertise mit Projektleiterkompetenz
- Wir konzentrieren uns auf die Informationssicherheit
- Wir sind neutral und nur unseren Kunden verpflichtet



Unternehmen

- Gründung im März 2010
- Inhabergeführte Aktiengesellschaft
- 12 Information Security Consultants
- Über 75 Kunden, welche höchste Anforderungen an die nachhaltige Gewährleistung ihrer Informationssicherheit stellen

Über die TEMET AG

Ausgewählte Referenzprojekte im Gesundheitswesen

- Aufbereitung, Durchführung und Dokumentation einer Bedrohungs- und Risikoanalyse für das **Elektronische Patientendossier** (ePD) inkl. Erarbeitung der Sicherheitsgrundlagen für das Bundesgesetz zum ePD (EPDG)
- Definition der **Aufgaben, Kompetenzen und Verantwortlichkeiten (AKV)** für Informationssicherheit sowie Zuweisung der **Risiko-Ownership** innerhalb einer Stammgemeinschaft für das elektronische Patientendossier (ePD) nach EPDG
- Erstellung einer **Cybersecurity Strategie** in Abstimmung mit der Geschäftsleitung, den Fachbereichen und der Informatik
- Ausarbeitung der **eHealth & mHealth Sicherheits-architektur** für ein Spital
- Unterstützung bei der Überarbeitung des **IT Compliance Frameworks** zur Sicherstellung der **HIPAA Compliance** in Hinblick auf ein externes Audit
- **Chief Information Security Officer** (CISO) as a Service bei einer Krankenversicherung
- Durchführung eines Proof of Concept (PoC) für die Einführung einer **Role Based Access Control** (RBAC) für ein Spitalverbund
- Planungs- und Konzeptverantwortung beim Ausbau des **Authentication Layers** einer Internet-Plattform für die Patienten-orientierte Sicht auf **Gesundheitsdaten** (eHealth)
- Compliance- und Datenschutz-Audit eines Lieferanten für die **elektronische Rechnungseinlieferung** (Transfer und Verarbeitung von Arztrechnungen und von sensitiven Unfall- und Patientendaten)
- Projektleitung und Fachberatung bei der Einführung des firmenweiten **globalen Privileged Account Management** (PAM)

Cyberrisiken allgegenwärtig

TEMET
end-to-end IT security

- Massiv veränderte Bedrohungslage, neue Risiken
  - Klare Verlagerung zu organisierter Kriminalität, Spionage, politisch und militärisch motivierte Aktionen
  - Steigende Professionalisierung, Angreifer sind perfekt organisiert, sehr gut informiert und verfügen über immense Ressourcen (Botnets sei Dank).

- Reaktion darauf
  - Neue Frameworks, wie z.B. NIST Cybersecurity Framework
  - Spezifische Sicherheitsvorgaben, wie z.B. NIST Securing Wireless Infusion Pumps In Healthcare Delivery Organizations
  - Erweiterung regulatorischer Vorgaben, wie z.B. FINMA RS 08/21 mit Cybersecurity spezifischen Anforderungen
  - Neue Vorgaben, wie z.B. EU DSGVO (Datenschutz-Grundverordnung)
  - Aufkommen von Versicherungen gegen Cyberrisiken

Top 10 Unternehmensrisiken (1)

Top 10 business risks by region in 2017: Europe

Top 10 business risks			2016 Rank	Trend
1	Business interruption (incl. supply chain disruption, and vulnerability)	35%	1 (53%)	-
2	Cyber incidents (cyber crime, IT failure, data breaches, etc.)	32%	3 (40%)	▲
3	Market developments (volatility, intensified competition/new entrants, M&A, market stagnation, market fluctuation)	32%	2 (52%)	▼
4	Changes in legislation and regulation (goverment change, economic sanctions, protectionism, etc.)	28%	4 (39%)	-
5	Macroeconomic developments (austerity programs, commodity price increase, deflation, inflation)	23%	5 (31%)	-
6	Natural catastrophes (e.g. storm, flood, earthquake)	21%	6 (31%)	-
7	Political risks and violence (war, terrorism, etc.)	16%	10 (17%)	▲
8	Fire, explosion	15%	8 (22%)	-
9	Loss of reputation or brand value	12%	7 (29%)	▼
10	New technologies (e.g impact of increasing interconnectivity, nanotechnology, artificial intelligence, 3D printing, drones, etc.)	12%	9 (19%)	▼

Source: Allianz Global Corporate & Specialty. Figures represent a percentage of all relevant responses. 516 respondents. More than one risk selected.

Top 10 Unternehmensrisiken (2)

TEMET
end-to-end IT security

The most important risks for businesses in Switzerland

Figures represent a percentage of all responses.

Respondents: 19

Respondents for Europe: 516

More than one risk and industry selected

Top 10 business risks for Switzerland			2016 Rank	Trend
1	Business interruption (incl. supply chain disruption, and vulnerability)	50%	2 (39%)	▲
2	Market developments (volatility, intensified competition/new entrants, M&A, market stagnation, market fluctuation)	46%	1 (44%)	▼
3	Cyber incidents (cyber crime, IT failure, data breaches, etc.)	42%	3 (28%)	-
4	Changes in legislation and regulation (goverment change, economic sanctions, protectionism, etc.)	23%	5 (22%)	▲
4	Natural catastrophes (e.g. storm, flood, earthquake)	23%	7 (11%)	▲
6	Macroeconomic developments (austerity programs, commodity price increase, deflation, inflation)	19%	3 (28%)	▼
7	New technologies (e.g impact of increasing interconnectivity, nanotechnology, artificial intelligence, 3D printing, drones, etc.)	15%	NEW	▲
8	Brexit, Euro-zone disintegration	12%	NEW	▲
8	Climate change/increasing volatility of weather	12%	NEW	▲
8	Quality deficiencies, serial defects, product recall	12%	NEW	▲

Quelle: Allianz Global Corporate & Speciality

Treiber für Massnahmen (1)

TEMET
end-to-end IT security

Risiken die zu Einbussen in - oder Verlust der Geschäfts-tätigkeit führen

- Datenverlust (kein Zugriff mehr auf die Daten, Ransomware, etc.)
- Verlust der Vertraulichkeit (Daten werden publik)
- Verlust der Integrität oder Verfügbarkeit (Gesundheitsrisiken für Patienten, Cyber-Mord, etc.)
- Missbrauch der Infrastruktur für weitere Angriffe

Treiber für Massnahmen (2)

TEMET
end-to-end IT security

Vorgaben

- Rechtliche Vorgaben (Gesetz und Verträge) z.B. Datenschutzrecht, OR
  - DSG
    - Sehr generisch formuliert: «Mit Angemessenen technischen und Organisatorischen Massnahmen Schutz der Persönlichkeit sicherstellen»
    - Für die Beurteilung von «Angemessen» wird meistens an ein Security Framework angeknüpft

- Weitere Vorgaben wie branchenspezifische Regulative, FINMA, BAG, SRO SVV, Kantonales Recht
  - Branchenspezifische Vorgaben
    - Detaillierung der Ausführung innerhalb einer gesetzlichen Bestimmung

Datenschutz-Grundverordnung

TEMET
end-to-end IT security

EU DSGVO (Konkretisierung auf Gesetzesebene)

- Konkrete Vorgaben
  - Risikofolgenabschätzung
  - Privacy by Design and by Default
  - Sanktionen (sind viel massiver als bisher)
  - Auskunftspflicht an betroffene Personen

- Geltungsbereich
  - Es gilt das Marktortprinzip, d.h. es können auch Schweizer Firmen die Dienstleistungen oder Produkte in der EU anbieten betroffen sein.
  - Die Gültigkeit kann auch für Hersteller und Händler von Geräten nicht ausgeschlossen werden, sobald die Datenbearbeitung nicht ausschliesslich auf anonymen Daten erfolgt (Erhebung und Übermittlung ist eine Bearbeitung).

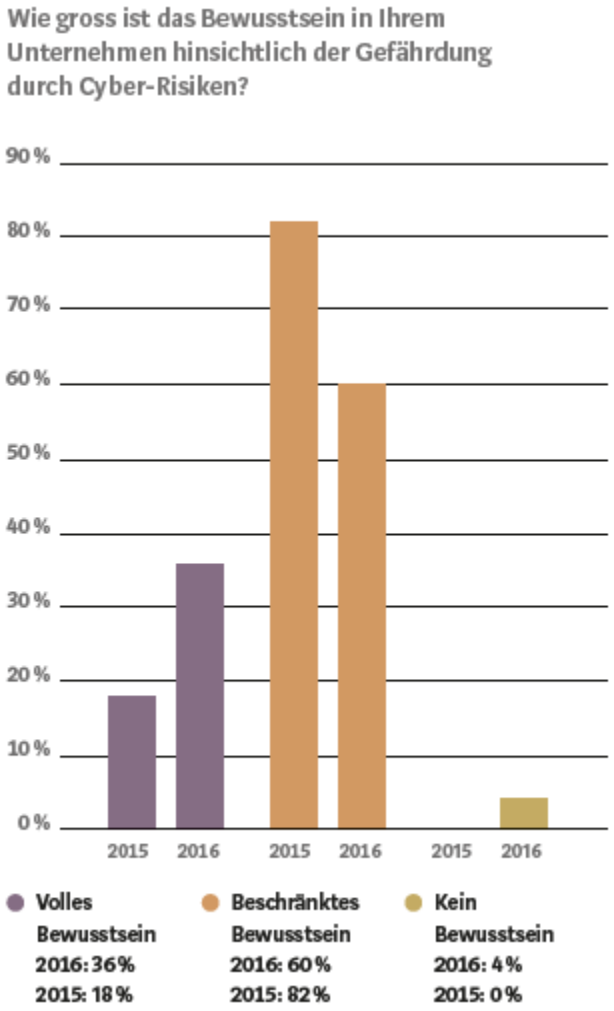
Cyberrisiken Erwartungshaltung

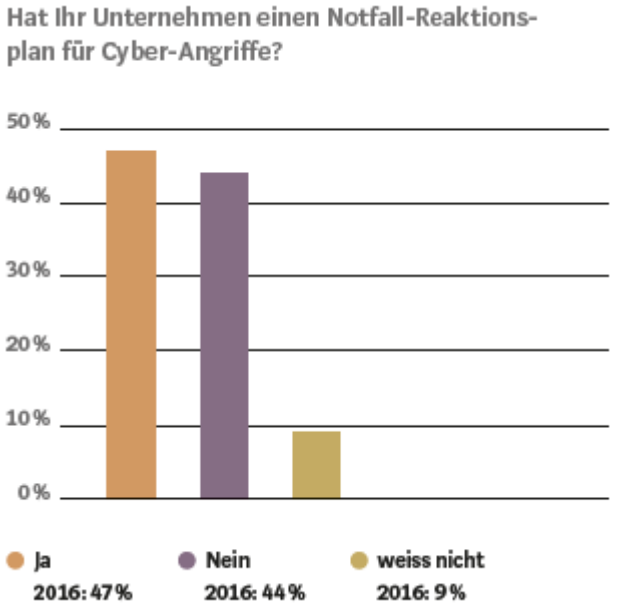
TEMET
end-to-end IT security

- Die Frage ist nicht ob ein Einbruch möglich ist, sondern ob ein Unternehmen darauf vorbereitet ist wenn er passiert, d.h. den Einbruch zeitnah feststellt und sich schnell genug davon erholen kann.

  - Massnahmen in den Bereichen Detektion und Reaktion müssen verstärkt werden (Verlagerung von Prävention)

Sind Unternehmen vorbereitet?





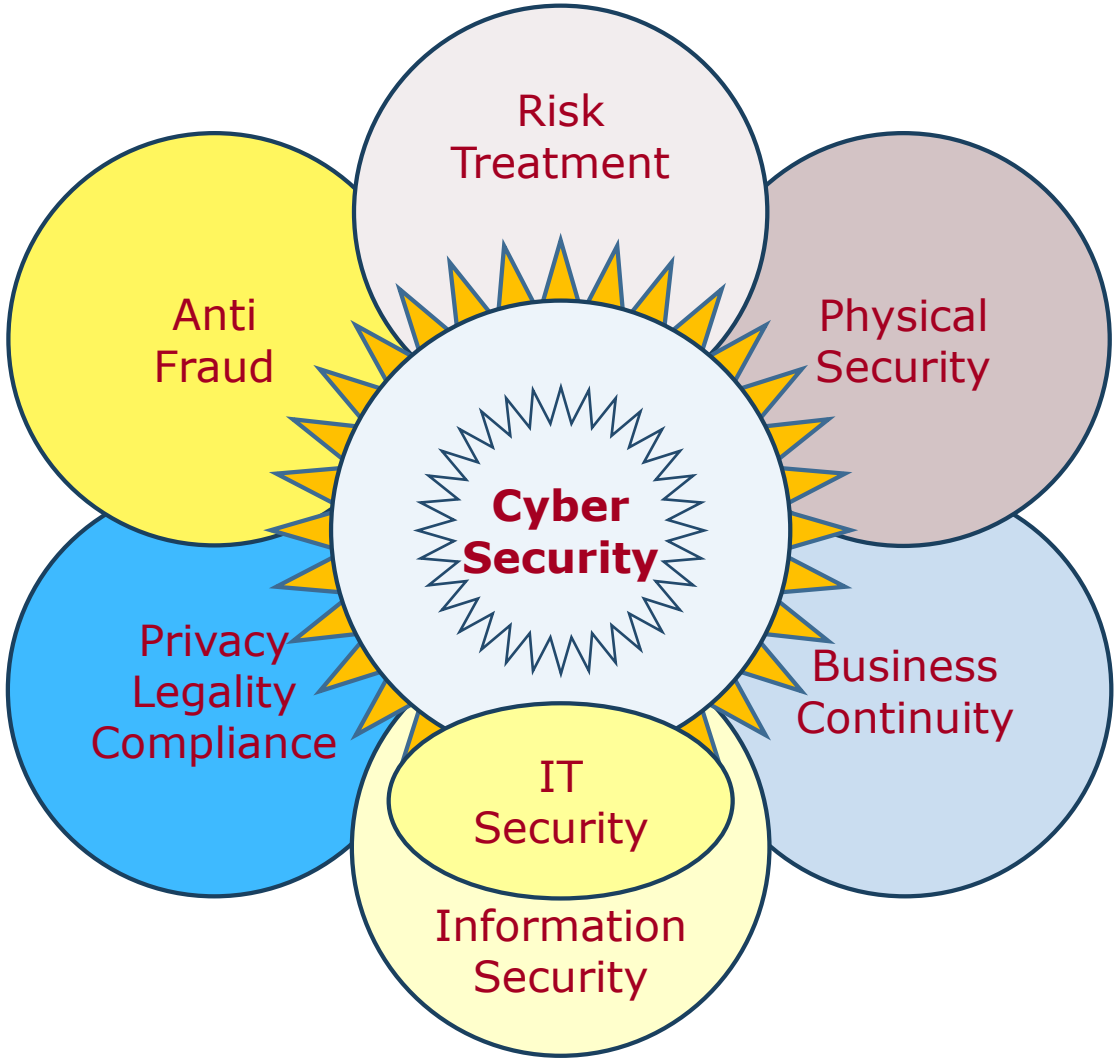
Quelle: Kessler, Cyber Risk Survey Report 2016

Wo steht ihr Unternehmen?

Erste Schritte

- Wie kann das Thema Cybersecurity strukturiert angegangen werden?
  - Basis bildet das NIST Cybersecurity Framework
- Wie steht das Unternehmen aktuell da?
  - Durchführen einer Maturitätsbewertung
- Welche Massahmen sind notwendig?
  - Erstellung/Umsetzung Cyber Defense Plan

Einbettung in klassische Security Domänen



Ablauf eines Angriffs

TEMET
end-to-end IT security

Informationsbeschaffung und Vorbereitung → Zustellung → Einbruch und Entfaltung → Ziel erreicht

Einbruch und Entfaltung: Infek-tion → C & C → Ausbrei-tung

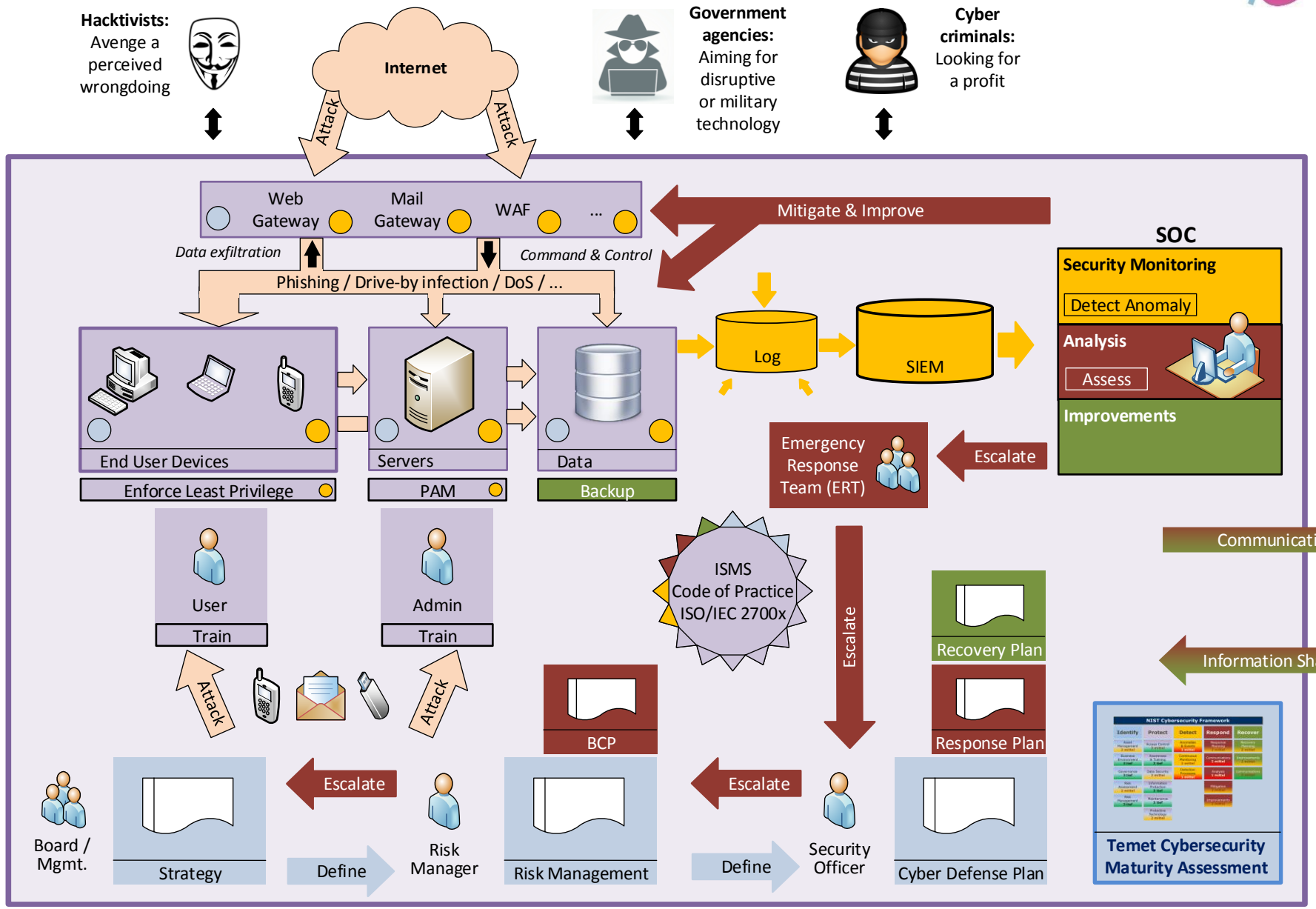
• Social Engineering • Perimeter Scans	• Phishing • Spear Phishing • Drive by • Memory Stick • Mobile	• Einnisten • Code nachladen • Weiter ausbreiten	• Datenabzug • Ressourcenmissbrauch • Service Unterbruch

NIST Framework

TEMET
end-to-end IT security

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies & Events	Response Planning	Recovery Planning
Business Environment	Awareness & Training	Continuous Monitoring	Com-munications	Improvements
Governance	Data Security	Detection Processes	Analysis	Com-munications
Risk Assessment	Information Protection		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
Supply Chain Risk Management	Protective Technology			

Cybersecurity «Big Picture»



Ablauf eines Angriffs und Massnahmen

TEMET
end-to-end IT security

Informationsbeschaffung und Vorbereitung → Zustellung → Einbruch und Entfaltung → Ziel erreicht

Einbruch und Entfaltung: Infek-tion → C & C → Ausbrei-tung

- Mitarbeiter Awareness
- Minimaler System Footprint

- Perimeterschutz
- Malware Schutz
- Passwort Policy
- Hardening
- Device Control
- Mitarbeiter Awareness

- Patchmanagement
- Privileged Access Management
- Netzwerk Segmentierung
- Hardening (Endpoints und Servers)
- Malware Schutz
- Vulnerability Scanning und Pen-Testing
- Schutzmassnahmen Ausgehender Verkehr

- Response und Recovery Plan
- Backup
- Kommunikationsplan
- Sicherstellen von forensischen Daten

- Risk- und Assetmanagement
- SIEM

Cyber Defense Plan (1)

TEMET
end-to-end IT security

1. Risiken managen
   - Unternehmensrisiko, Awareness im Management, Bedrohung richtig einschätzen
2. Unternehmenswerte kennen
   - Inventarisierung, Güterbewertung, Kritikalität, Verantwortlichkeiten
3. Maturitätsbewertung durchführen und Strategie festlegen
   - Cybersecurity-Strategie, Maturitätsbewertung, Compliance/Datenschutz
4. Einfallstore schliessen
   - „Do the simple stuff first", Perimeter-Schutz (E-Mail, Web), Client-Schutz, Berechtigungen
5. Auswirkungen minimieren
   - Datenredundanz minimieren, Datensicherung, Data Leakage Prevention, BCM, Privileged Access Management

Cyber Defense Plan (2)

TEMET
end-to-end IT security

6. Kommunikation und Informationsaustausch etablieren
   - Kommunikationskonzept, Reputationsschutz, Foren, Knowhow und Erfahrungsaustausch
7. Informationen sammeln (Logging)
   - Zentrales Logging, Kategorisierung und Klassifizierung, Aufbewahrungsfristen
8. Sicherheitsinformationen und -Ereignisse managen (SIEM)
   - Vorgaben, Daten Aggregierung/Korrelation, Angriffsmuster verstehen, Anomalien erkennen, Alarmierung, Monitoring
9. Cyber Defense Center etablieren
   - Sicherheitsüberwachung, Analyse, Eskalation, Verbesserungen, Incident Response Team
10. Kontinuierliche Verbesserung stärken
    - Information Security Management System, Best Practices, KPIs definieren (Effektivität, Effizienz), Awareness

Schlusswort

TEMET
end-to-end IT security

- Bewusstsein für Cyberrisiken im Unternehmen schärfen
- Erwartungshaltung prüfen — Einbruch findet statt
- Ist-Zustand kennen, Maturitätsbewertung durchführen
- Vorgehen festlegen und Massnahmen gemäss Cyber Defense Plan umsetzen
- Informationsaustausch fördern

… zum Erfolg

Besten Dank
für Ihre Aufmerksamkeit!

TEMET AG
Basteiplatz 5
8001 Zürich
044 302 24 42
info@temet.ch
www.temet.ch