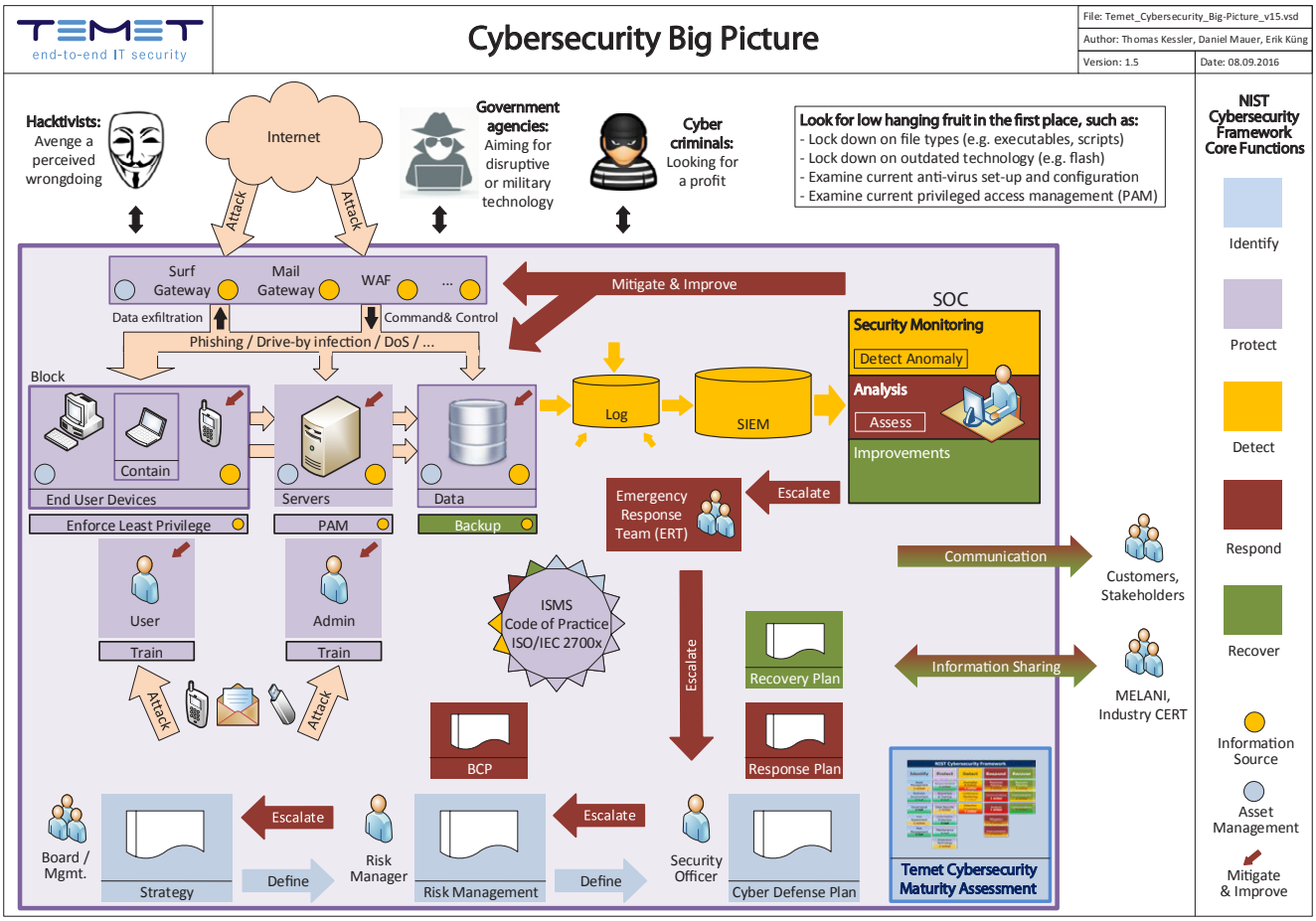
Cybersecurity Standortbestimmung

Die TEMET AG unterstützt Sie dabei, den Reifegrad Ihrer Organisation in Bezug auf Cybersecurity zu ermitteln und aufzuzeigen.



Das **Temet Cybersecurity Big Picture** illustriert die Umsetzung der fünf Funktionen des NIST Framework for Improving Critical Infrastructure Cybersecurity mit ihrem Fokus auf Attacken aus dem Cyberspace, d.h. dem Internet:

Der präventive Schutz **(Protect)** setzt vorab am Perimeter an, zu dem wir neben den Gateway-Systemen auch die Endgeräte und deren Benutzer zählen. Durch Optimierung vorhandener Sicherheitssysteme kann hier schon viel gewonnen werden. Eventuell müssen auch Infrastrukturen für Netzwerk-, Plattform- und Applikationssicherheit ausgebaut oder neu ausgerichtet werden. Ebenfalls wichtig ist die laufende Sicherheitsüberwachung aller IT-Systeme, damit Cyberangriffe frühzeitig erkannt werden **(Detect)**.

Hierfür muss ein **Security Operations Center** eingerichtet und mit den nötigen Werkzeugen für die Sammlung und Auswertung von Echtzeitdaten ausgestattet werden. Der professionelle Umgang mit erkannten Anomalien **(Respond)** stellt hohe Ansprüche an die Kommunikation und erfordert Eskalationsprozesse, die vorab geplant und geübt werden. Zur Wiederherstellung des normalen Geschäftsbetriebs **(Recover)** schliesslich gehört auch die Anwendung der gelernten Lektion.

Organisation, Prozesse und Hilfsmittel für die Analyse, Planung und Steuerung der Cybersecurity ordnen wir der identifizierenden Funktion zu **(Identify)**. Hierzu zählen wir insbesondere eine Standortbestimmung und einen Cyber Defense Plan.

Cybersecurity stützt sich auf eine etablierte **Basissicherheit** z.B. nach ISO/IEC 2700x, die bezüglich der Funktionen Detect, Respond und Recover gezielt ausgebaut wird.

Aufgabenstellung und Zielsetzung

Finanzielle und personelle Ressourcen sind begrenzt verfügbar und sollen optimal eingesetzt werden. Die Kenntnis des aktuellen Cybersecurity Reifegrads hilft Ihnen, die richtigen Vorhaben zu starten oder diese angemessen zu priorisieren.
Damit Massnahmen nicht nur punktuell wirken, sollten sie Teil eines Cyber Defense Plans sein. Dieser Plan setzt die vorhandenen Mittel gewinnbringend ein, um das angestrebte Niveau Ihrer Organisation im Bereich Cybersecurity zu erreichen und zu halten.

Temet Cybersecurity Dienstleistungen

Die Berater der Temet sind Experten im Thema Cybersecurity. Durch ihre langjährige Tätigkeit in weit über 100 Sicherheitsprojekten bei rund 60 Kunden konnten sie ein um-fassendes Know-how aufbauen, das heute im Cybersecurity Bereich voll zum Tragen kommt. Die Temet bietet beispielsweise folgende Dienstleistungen an:

- Ausarbeiten einer **Cybersecurity Strategie**
- Durchführen einer **Cybersecurity Standortbestimmung**
- Erarbeiten eines **Cyber Defense Plans,** auch im Sinne des im FINMA Rundschreiben 2008/21 «Operationelle Risiken Banken» verlangten Konzepts für den Umgang mit Cyberrisiken
- Unterstützung bei der Umsetzung des Cyber Defense Plans

Referenzprojekte

Die Berater der TEMET AG verfügen über einen grossen Cybersecurity Erfahrungsschatz in diversen Branchen. Sie sind insbesondere in der Lage, Risiken korrekt und sachgerecht zu bewerten. Dies ist eine Auswahl an Projekten:

Kunde	Gegenstand der Risiko-analyse	Besonderheit
Gesundheits-wesen	Durchführung eines **Cyber-security Maturity Assess-ments** (CSMA) nach NIST und COBIT 5.	In Abstimmung mit der Geschäftsleitung, den Fachbereichen und der Informatik; im Rahmen der Erarbeitung einer Cyber-security Strategie.
Bank	Unterstützung in Projekten der **Security Roadmap** zur Begrenzung von Informa-tions- und Cyberrisiken.	Network-Zoning-Schutz vor Advanced Inside-Out Attacken, Lock-down von Datentypen, Autorisierung (PAM, Jump Host Konzept), FINMA Compliance, New Technologies.
Versicherer	Vorgehensempfehlungen zu den **Präkonditionen** im **Incident- und Forensik-Prozess.**	Beratung bei der Einführung von Gefähr-dungsanalysen und dem Design des Forensik- und CERT-Prozesses; Evaluation eines Service Providers für forensische und Cybersecurity-Dienstleistungen.
Bank	Erarbeitung einer Strategie zur **Data Leakage Preven-tion** (DLP)	Entscheidungsfindung bezüglich der Ein-führung eines DLP-Tools für Internet und E-Mail (Verschlüs-selung, Monitoring, Content Scanning, Whitelisting, Pop-Ups/ Notifications, Sandboxing).

Kundennutzen

Eine professionell durchgeführte Cybersecurity Standortbestimmung zeigt die Stärken und Schwächen Ihres heutigen Cybersecurity Dispositivs. Sie ermöglicht Transparenz und eine sachliche Diskussion bezüglich der aktuellen Situation und der notwendigen nächsten Schritte.

Unser Angebot

Wir bieten die Durchführung einer Cybersecurity Standortbestimmung zum Fixpreis an. Der Fixpreis richtet sich nach der Grösse und Komplexität Ihrer Organisation und bewegt sich im Rahmen von CHF 9'000.– bis CHF 27'000.–.

Die Dienstleistung umfasst die folgenden Arbeitspakete:

- Ist-Aufnahme in Bezug auf die 22 Funktionen des NIST Framework mittels Checkliste, Dokumentenstudium und strukturierten Interviews oder Workshops;
- Standortbestimmung in Bezug auf den Reifegrad und die damit verbundenen Risiken des aktuellen Sicherheitsdispositivs. Die Beurteilung basiert auf der Expertise und den Branchenkenntnissen der Temet Berater;
- Abstimmung mit den Auftraggebenden und Dokumentation aller Ergebnisse.

Temet Cybersecurity Maturity Matrix Beispiel (Funktionen, Reifegrade, Risiken):

Temet Cybersecurity Maturity Matrix

Identify	Protect	Detect	Respond	Recover
Asset Management **3 mittel**	Access Control **2 mittel**	Anomalies & Events **2 mittel**	Response Planning **2 mittel**	Recovery Planning **2 mittel**
Business Environment **4 tief**	Awareness & Training **3 mittel**	Continuous Monitoring **1 hoch**	Communications **2 mittel**	Improvements **1 mittel**
Governance **4 tief**	Data Security **2 hoch**	Detection Processes **2 mittel**	Analysis **1 hoch**	Communications **2 mittel**
Risk Assessment **3 mittel**	Information Protection **3 mittel**		Mitigation **1 mittel**	
Risk Management **4 tief**	Maintenance **4 tief**		Improvements **1 mittel**	
	Protective Technology **2 hoch**			

TEMET AG – Alleinstellungsmerkmale

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

Wir freuen uns darauf, Sie von unserer Kompetenz zu überzeugen.

TEMET
end-to-end IT security

Cybersecurity Big Picture

File: Temet_Cybersecurity_Big-Picture_v15.vsd	
Author: Thomas Kessler, Daniel Mauer, Erik Küng	
Version: 1.5	Date: 08.09.2016

Hacktivists: Avenge a perceived wrongdoing

Internet

Attack

Attack

Government agencies: Aiming for disruptive or military technology

Cyber criminals: Looking for a profit

Look for low hanging fruit in the first place, such as:
- Lock down on file types (e.g. executables, scripts)
- Lock down on outdated technology (e.g. flash)
- Examine current anti-virus set-up and configuration
- Examine current privileged access management (PAM)

Surf Gateway

Mail Gateway

WAF

...

Data exfiltration

Command& Control

Phishing / Drive-by infection / DoS / ...

Mitigate & Improve

Block

Contain

End User Devices

Servers

Data

Enforce Least Privilege

PAM

Backup

Log

SIEM

SOC

Security Monitoring

Detect Anomaly

Analysis

Assess

Improvements

Escalate

Emergency Response Team (ERT)

Communication

Customers, Stakeholders

User

Train

Admin

Train

ISMS Code of Practice ISO/IEC 2700x

Escalate

Recovery Plan

Information Sharing

MELANI, Industry CERT

Attack

Attack

BCP

Response Plan

Board / Mgmt.

Strategy

Escalate

Define

Risk Manager

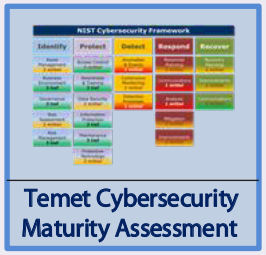
Risk Management

Escalate

Define

Security Officer

Cyber Defense Plan



Temet Cybersecurity Maturity Assessment

NIST Cybersecurity Framework Core Functions

Identify

Protect

Detect

Respond

Recover

Information Source

Asset Management

Mitigate & Improve