
Fortsetzung von Intro …
2. Moderne Infrastrukturen, Endpunte & Sicherheit

Nimmt die Verfügbarkeit in der Cloud ab?

(drei CI2C Slides folgen: Energie Transport: da gilt es ernst)

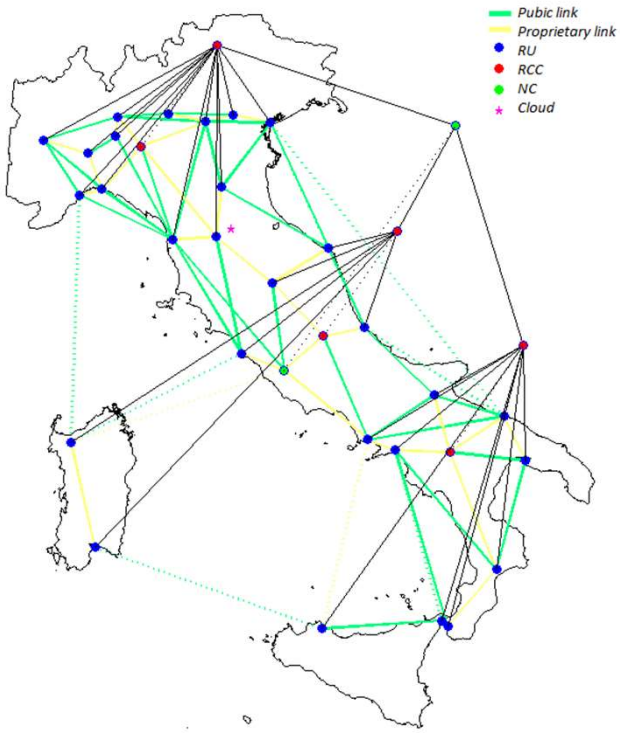
- Eine Italienische Studie bezüglich des Energietransportes gibt Auskunft
- Die Arbeit wurde an der www.critis2016.org Konferenz vorgestellt.
- Dabei werden 4 Architektur-Optionen des verteilten Systems untersucht

➔ Resultat: Die Cloud schneidet recht gut ab: lassen sie uns sehen.

Von Stefano Sebastio[a], Antonio Scala[b,a], and Gregorio D'Agostino[c,a]
Im Critical Infrastructure Cloud Computing (CI2C) EU Projekt

[a] LIMS London Institute of Mathematical Sciences, London, UK
[b] ISC-CNR Sapienza Università di Roma, Rome, Italy
[c] ENEA, CR "Casaccia", Rome, Italy

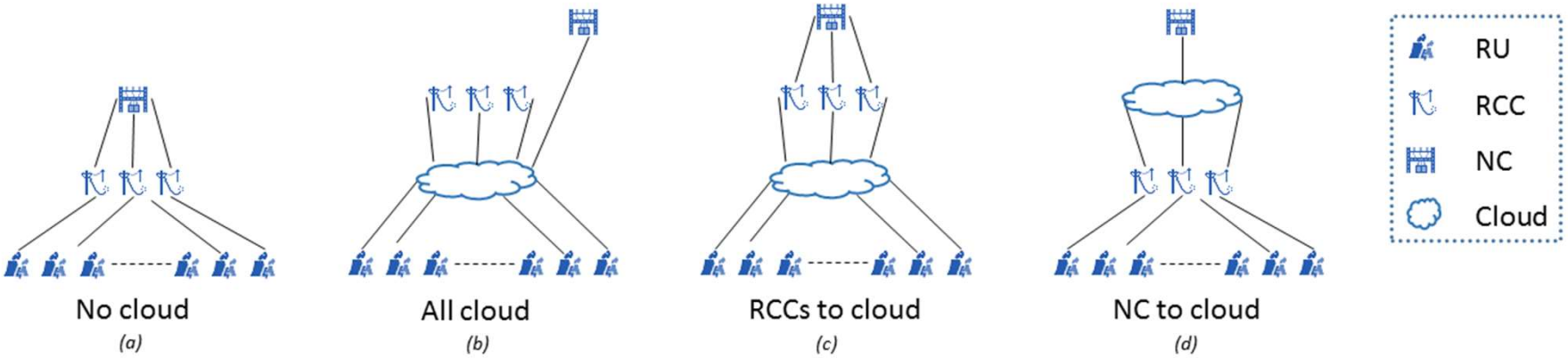
The Hierarchical SCADA system – Italian case



- **Remote units (RU)** or terminals: Real-time interventions on voltage to manage load and events of interruptions
- **Regional Control Center (RCC)**: group and supervise RUs in larger geographical zones
- **National Center (NC)**: gathering data from and dispatching relaxed timing commands to RCCs & non time-critical operations (e.g., command planning, critical events analysis and statistics)
- *ENTSO-E*
- Connections of interest
- On a virtual proprietary network

Architektur-Optionen:
Cloud Deployments for a Nationwide SCADA

- Data analytics & data access
- Real-time command and historical data on cloud



Availability Analysis

Connection	Proprietary	Public	All cloud	RCCs to cloud	NC to cloud
	0.699995	0.699988	-	-	0.699988
$RUs \leftrightarrow RCC_i$	0.697129	0.699426	-	-	0.699426
	0.699816	0.699816	-	-	0.699816
$RCCs \leftrightarrow NC$	0.778379	0.778400	-	0.778400	-
$RUs \leftrightarrow Cloud$	-	-	0.998999	0.998999	-
$RCCs \leftrightarrow Cloud$	-	-	0.972027	0.972027	0.972027
$NC \leftrightarrow Cloud$	-	-	0.799200	-	0.799200
Total	0.993955	0.994001	0.999988	0.999993	0.998479

2 days | 6 mins | 3mins | 13 hours

Eine seriöse Studie im heiklen Energiesektor zeigt, dass Cloud-Sicherheit robust da steht.

Moderne Infrastruktur

www.nist80037rmf.com/disa-cloud-computing-documents-released-for-comment/

Security Cloud Seite

www.nist80037rmf.com/disa-cloud-computing-documents-released-for-comment/

Für Security spielt die Grösse des Cloud-Provider eine Rolle:

- Je grosser der Provider, um so sicherer
- Je besser vernetzt (ISAC, Threat Intelligence, etc), um so sicherer
- Es gilt, was im Vertrag geregelt wird.
- Seit kurzer Zeit ist auch Cyber-Insurance ein Thema.

Security Endgeräte (Endpoint Security)

- Any device, any time, any where may be connected
- To the device nearfield communication of any uncontrolled and possibly insecure devices must be assumed
- IoT: camera, sensor and actors may be connected (ddos case of hacked cameras)
- Control of behavioural application footprint
- Configuration, security and logs must be controlled
- Forensic readiness is desirable
- Remote control function in case of loss is important
- Multiple context (private, business +++) should be supported
- GDPR compliance is paramount (consent)

Finding 2: Security Requirements für moderne Infrastruktur und Endpunkte

- Netzwerke: Transportieren Daten sicher (nicht abhörbar) und zuverlässig (Verfügbarkeit)
- Im Szenario müssen multiple home Clouds berücksichtigt werden (mehrere private und mehrere öffentliche)
  Sicherheitslösungen müssen diese Situation unterstützen
- Endpunkte: Mehrere Endpunkte pro Person müssen angenommen warden (PC, Laptop, Tablet, Smartphone …)
- Endpunkte können auch IoT Devices (Kameras, Aktoren und Sensoren) und Bluetooth (Fitness tracker, Smart Watch, …)
- Beide Protokolle, IPv4 und IPv6 müssen gleichermassen gesichert werden …


3. Modernes Arbeiten

Modernes Arbeiten: überall, jederzeit, jedes Gerät

Bildnachweis:

https://www.gettyimages.co.uk/detail/photo/businessman-traveling-with-a-bus-and-using-smart-royalty-free-image/675035664

https://www.huffingtonpost.com/mike-desimone-and-jeff-jenssen/mothers-day-gifts-for-the-mom-who-travels_b_7147934.html

https://cdn.uconnectlabs.com/wp-content/uploads/sites/5/2017/10/canstockphoto9041519.jpg

Awareness, attitude & behaviour
Die Kunst sicherer zu arbeiten

Awareness requires creative communications

Behaviour is influenced by perception, experiences and external cues

Attitudes can only be changed through self-discovery

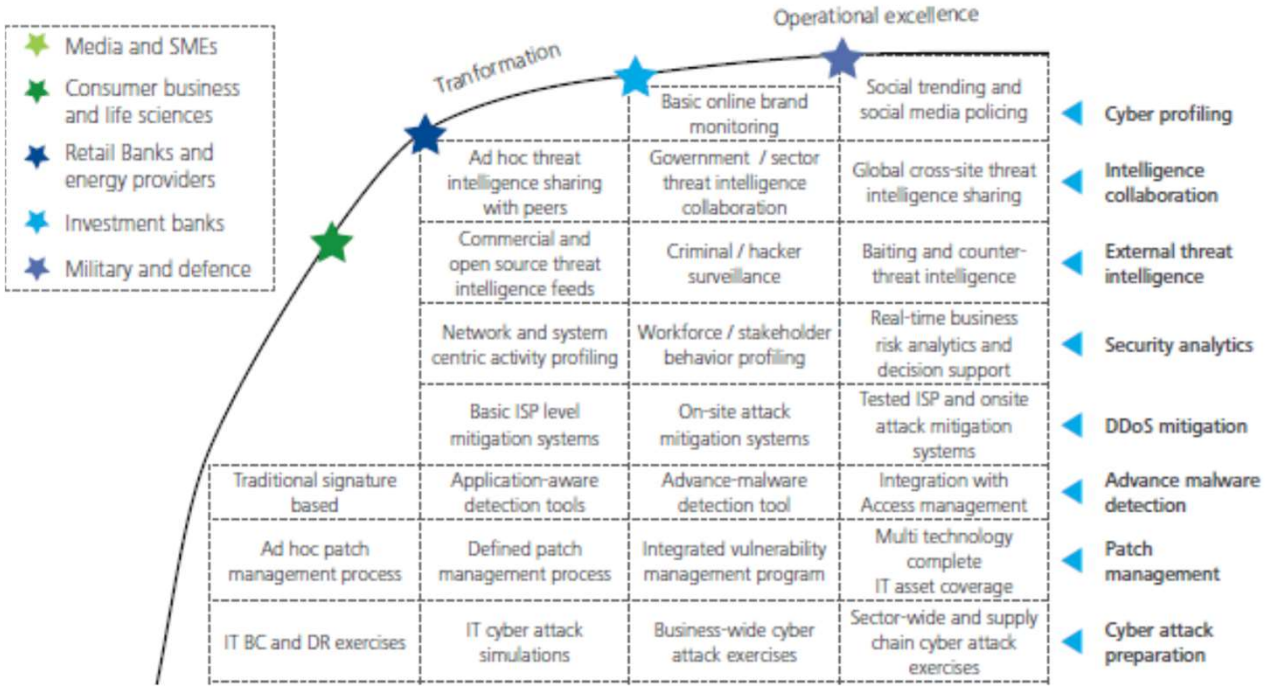
Finding 3:

Modernes Arbeiten verlangt mehr Verantwortung vom Mitarbeiter, mehr Kontrolle durch Technologie und Arbeitgeber.

- **Breaches sind unvermeidbar:** Jeder von uns kann verletzt werden (Keine Unterscheidbarkeit, Statistik der grossen Zahlen)
- Beste Awareness muss sein (Reduktion der Malwarewahrscheinlichkeit)
- Beste Incident Detection und Response sind zwingend notwendig für den **Umgang mit unvermeidbaren Breaches**


4. Requirements of
- CMMI für Cyber Security &
- Minimalstandard zur Verbesserung der IKT Resilienz (BWL)

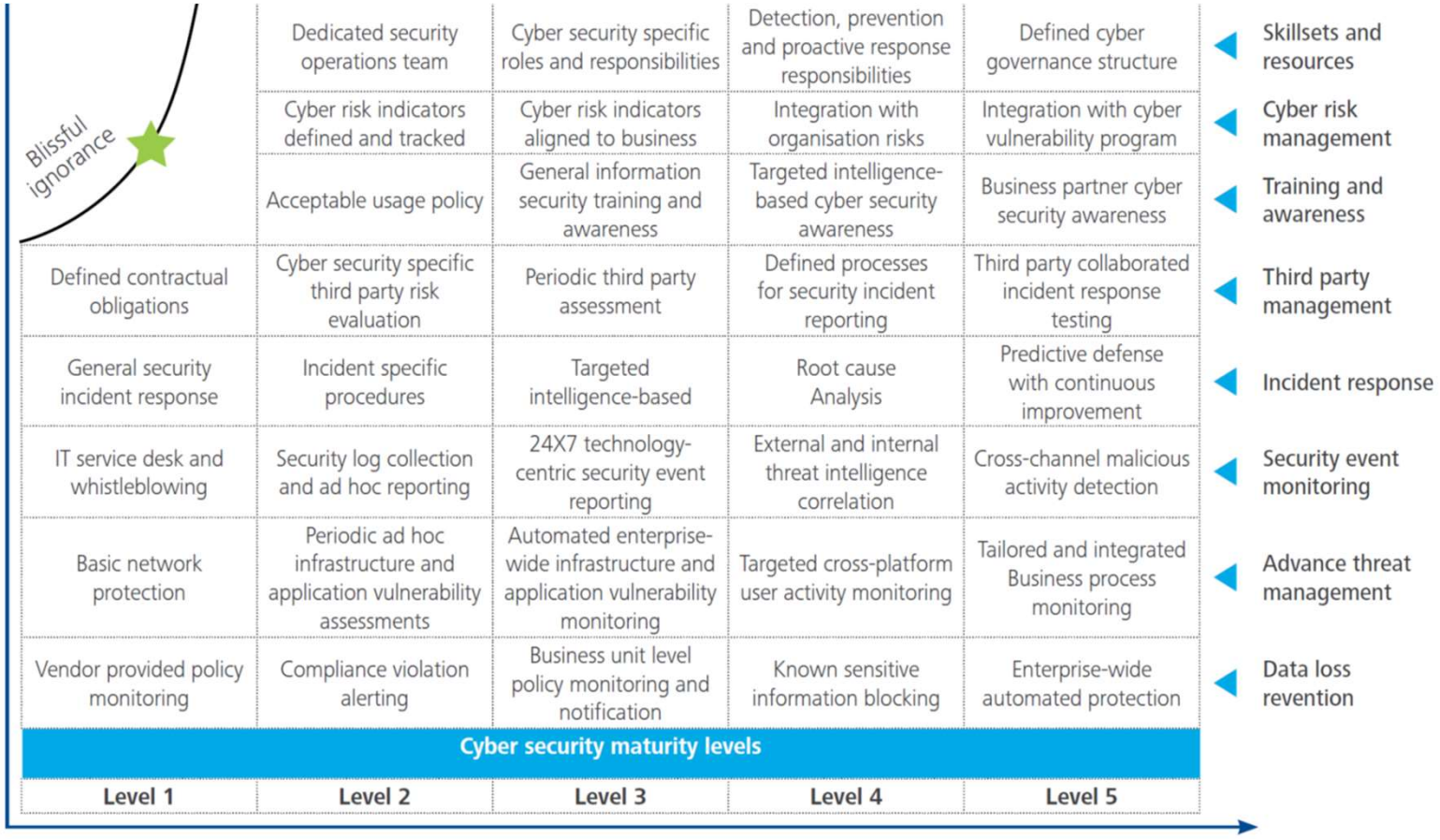
CMMI Capabilities I (advanced)



Die neuen Fähigkeiten im Cyber-Verteidigung

Aus Deloitte Studie „Cyber security: Empowering the CIO“

CMMI Capabilities I (advanced)



Minimalstandard zur Verbesserung der IKT Resilienz (BWL)

Bundesamt für wirtschaftliche Landesversorgung (BWL) IKT-Minimalstandard erarbeitet und diesen am 27. August 2018 vorgestellt.

Der IKT-Minimalstandard im Überblick: 106 Massnahmen

Der Standard gliedert sich in drei Teile:

1. Grundlagen: Dieser Teil dient als Nachschlagewerk und vermittelt Informationen zur IKT-Resilienz.

2. Framework: Es bietet den Anwendern, gegliedert nach den fünf Phasen (Themenbereichen)
   «Identifizieren»,
   «Schützen»,
   «Detektieren»,
   «Reagieren» und
   «Wiederherstellen» ein Bündel konkreter Handlungsanweisungen.

Nach NIST: **Deter (Abschreckung)** fehlt

3. Bewertungstool: Mit diesem können Unternehmen den Grad ihrer IKT-Resilienz beurteilen, respektive auch durch externe Firmen prüfen lassen.

Leitfaden – in Übereinstimmung mit bestehenden Standards (NIST, Cobit etc.)

Cybersecurity-Architektur	• Standards/Empfehlungen • Richtlinien • Vorgehensweise
Physische Sicherheit	• Schutz von Endgeräten • Kontrollzentrum, Zugangskontrollen • Videoüberwachung, Zugangskontrollen & Barrieren
Netzwerk-Architektur	• Typische Sicherheitszonen • Demilitarized Zones (DMZ) • Virtual LANs
Netzwerk Perimeter Security	• Firewalls • Fernzugriff & Authentifizierung • Jump Servers/Hosts
Host Security	• Patch- & Schwachstellen-Management • Endgeräte • Virtuelle Geräte
Security Überwachung	• Intrusion Detection Systems • Sicherheits-Audit-Logging • Sicherheitsvorfall und Event-Überwachung
Vendor Management	• Lieferketten Überwachung & Management • Managed Services & Outsourcing • Nutzung von Cloud-Diensten

Reagieren (Respond): Beispiel für Anlehnung an Standards

2.5.1 Reaktionsplanung (Response Planning)

Erarbeiten Sie einen Reaktionsplan zur Adressierung erkannter Cybersecurity-Vorfälle. Stellen Sie sicher, dass dieser Reaktionsplan im Ereignisfall korrekt und zeitgerecht ausgeführt wird.

Bezeichnung	Aufgabe
RS.RP-1	Stellen Sie sicher, dass der Reaktionsplan während oder nach einem detektierten Cybersecurity-Vorfall korrekt und zeitnah durchgeführt wird.

Tabelle 33: Aufgaben RS.RP

Standard	Referenz
COBIT 5	BAI01.10
ISA 62443-3:2013	
ISO 27001:2013	A.16.1.5
NIST-SP-800-53 Rev. 4	CP-2, CP-10, IR-4, IR-8
BSI	B 1.8

Faktor Mensch

ID.RA-3	Identifizieren und dokumentieren Sie interne und externe Cyber-Bedrohungen.
ID.RA-4	Identifizieren Sie mögliche Auswirkungen der Cyber-Bedrohungen auf die Geschäftstätigkeit und bewerten Sie ihre Eintretenswahrscheinlichkeit.
ID.RA-5	Bewerten Sie die Risiken für Ihre Organisation, basierend auf den Bedrohungen, Verwundbarkeiten, Auswirkungen (auf die Geschäftstätigkeit) und Eintretenswahrscheinlichkeiten.

Das Element Mensch	• Richtlinien • Vorgehensweisen • Training und Wahrnehmung

Security Requirement &
Secure Programming / Systems

Sichere System-entwicklung (Secure Software Development)	Integraler Teil des Entwicklungs-prozesses.	ICS wurden historisch meist als physisch isolierte Systeme konzipiert. Sicherheit als integraler Teil der Systementwick-lung war entsprechend wenig verbreitet. Anbieter von ICS haben diesbezüglich Fortschritte gemacht, jedoch langsamer als in der IKT- Welt. Kernelemente von ICS lassen oft keine nachträglichen Sicherheitslösungen zu, bzw. diese sind nicht verfügbar.

Beispiel folgt mit **Secure Programming**, stellvertretend für **Secure Systems**.

Finding 4:

Die heute dargebotenen Lösungen werden von den neuesten Standards wie

CMMI Cybersecurity (Frühjahr 2018) und
BWL Minimal Standards

sind Voraussetzungen um eine Compliance mit BWL oder um eine venünftige Maturität mit CMMI zu erreichen.


5. Post Snowden
Protect, Detect, Respond

Post Snowden

Breaches are the new normal

Operation under peramanent Attack

Finding 4: Detection & Response

Information Sharing / Threat Intelligence: Large variety of models:

- Online and real time information sharing
- CERT level information sharing
- Mid management information sharing
- Strategic information sharing

Nur neuste Technologien (AI, ML, Big Data)
mit innovativsten Algorithmen sind gut genug:
Deshlab sind wir heute hier in IBM Research

Goal:

- **Be faster informed**
- **Isolate incidents down to one per malware**
- **Be warned, by strategic exchange**

Threat Intelligence

- Real time data gathering of many enterprises
- Big Data analytics for chasing zero day exploits
- Relevant progress in recent years


Empfehlungen und Schlussfolgerungen

Empfehlungen und Schlussfolgerungen

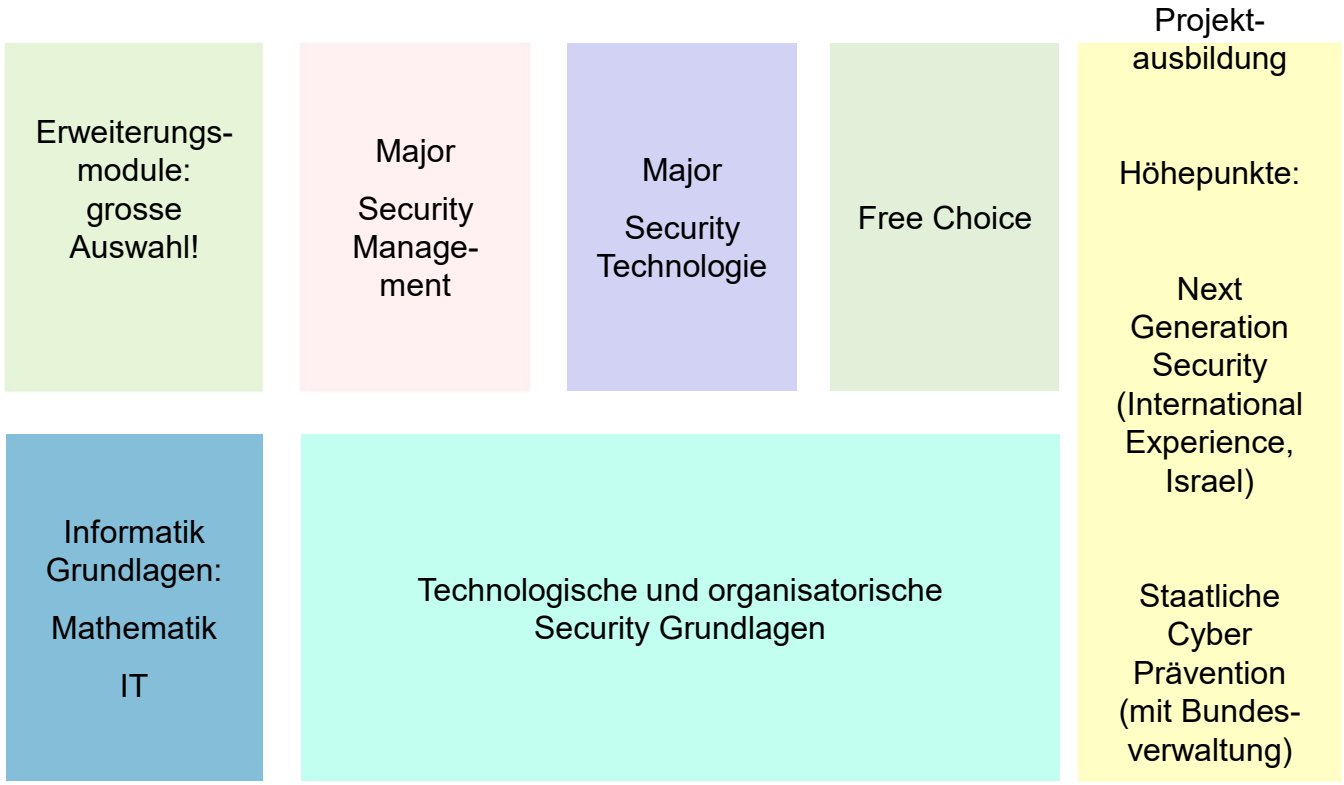
- Das Cloud Zeitalter lässt sich nicht stoppen. Die Sicherheit in der Cloud und aus der Cloud ist wesentlich grosser! Security does not Scale!
- Modernes Arbeiten braucht Investionen bei Endpoint Security!
- Human Factor: Wir brauchen Schulung um Resilient gegen Trickbetrüger zu sein.
- Neueste Standards CMMI BWL verlangen neuste Lösungen.
- Breaches sind unvermeidbar ➔ Detection & Response: Nur neuste Technologien (AI, ML, Big Data) mit innovativsten Algorithmen sind gut genug:
- Security Requirement Specification ist Voraussetzung, dass Sicherheit professionell angegangen werden kann.

Anhang: About new Study Program

BSc Information & Cyber Security

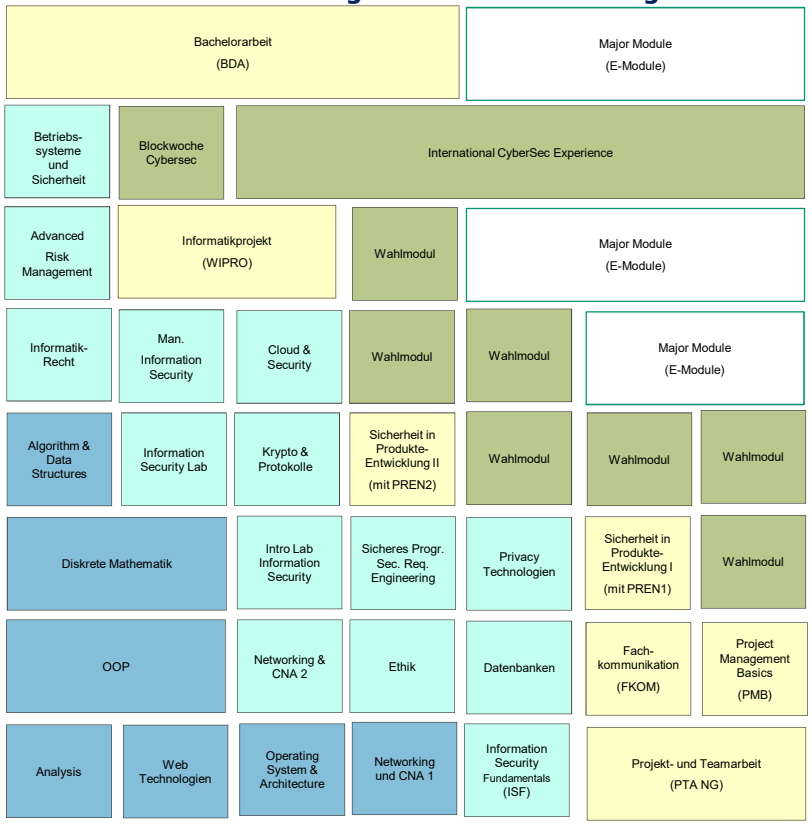
(In eigener Sache: HS18: 50 Stud.
HS19: 70 Stud.)

3. Ausbildungsprogramm: Module



Curriculum Studiengang Information & Cyber Security: Die Module Edition H19 BB, Israel 7. Sem

3. Jahr: In Entwicklung. Generell Änderungen vorbehalten.



8 * 21 ECTS = 168 ECTS
Sie müssen aber nur 162 Credits erwerben. Credits von Wahlmodulen

können in unterschiedlichen Semestern erworben werden.

Praxisanrechnung

Max. 18 Credits aus Praxis, normal-erweise in den Semestern 4-7 anger-echnet. Es werden in drei Semestern auf Antrag je 6 ECTS Praxisleistungen im Beruf angerechnet.
Sie müssen drei Mal Antrag stellen.

Wahlmodule Minimal Anforderungen:

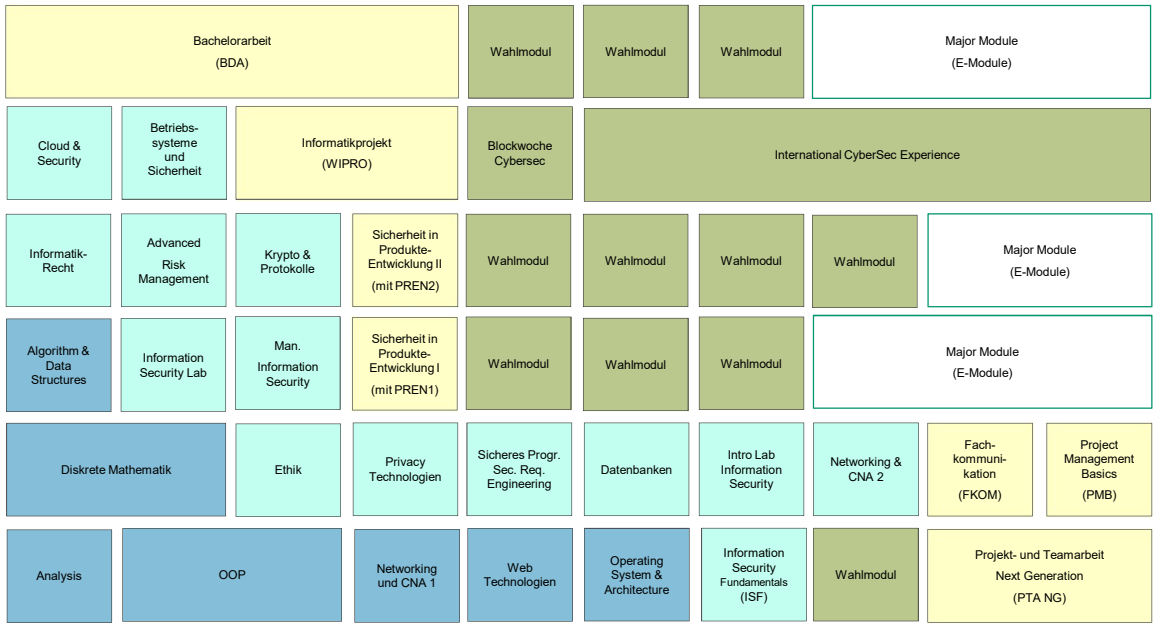
Mind. 3 Z- oder ISA-Module

Mind. 60 Credits im Wahlbereich

Bemerkung:
Das 7. Semester (Israel Aufenthalt) kann mit dem 5. Semester auf Antrag abgetauscht werden.
D.h. Der Israel Aufenthalt wäre dann im 5. Semester und auch das Modul «Betriebssysteme und Sicherheit».

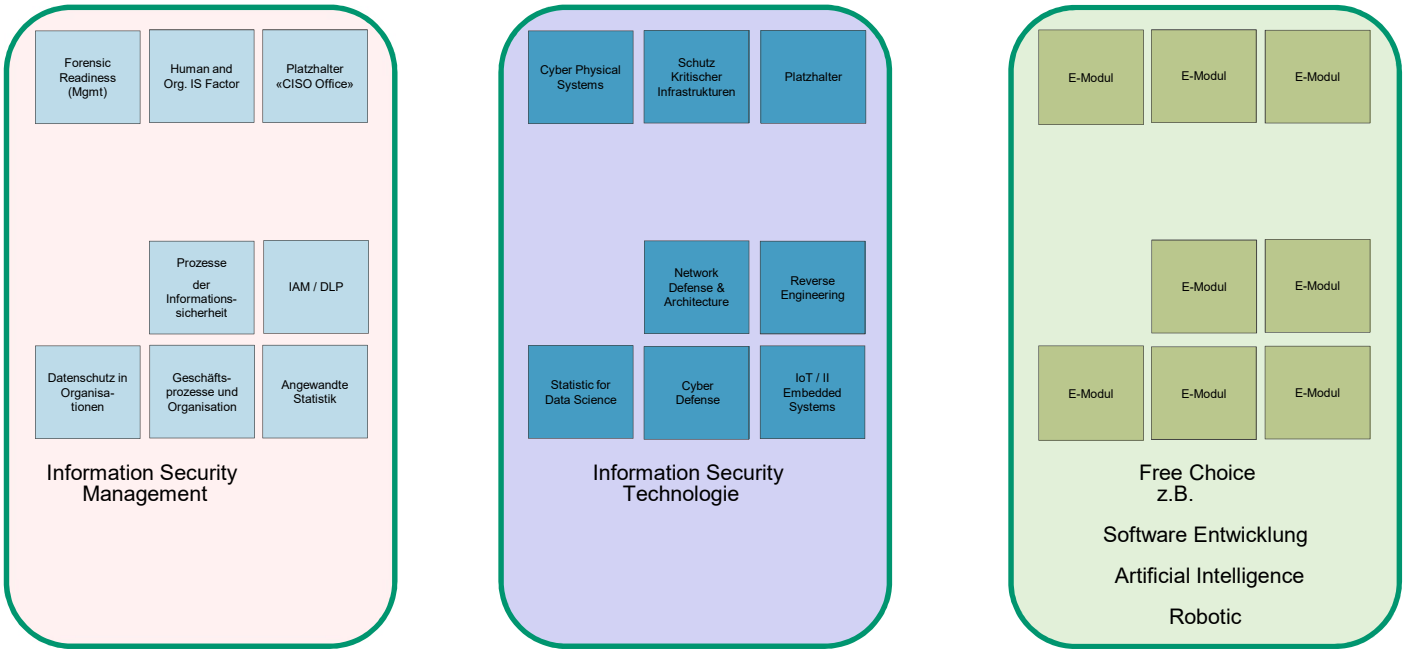
Curriculum Studiengang Information & Cyber Security: Die Module Edition H19 VZ

3. Jahr: In Entwicklung, Änderungen vorbehalten



Studiengang Information & Cyber Security:

Die Wahl der Majors



Ausbildungsprogramm: Concept