Cyber Risk Use Cases im Banking Umfeld – Bedrohungen, Auswirkungen und Mitigationen

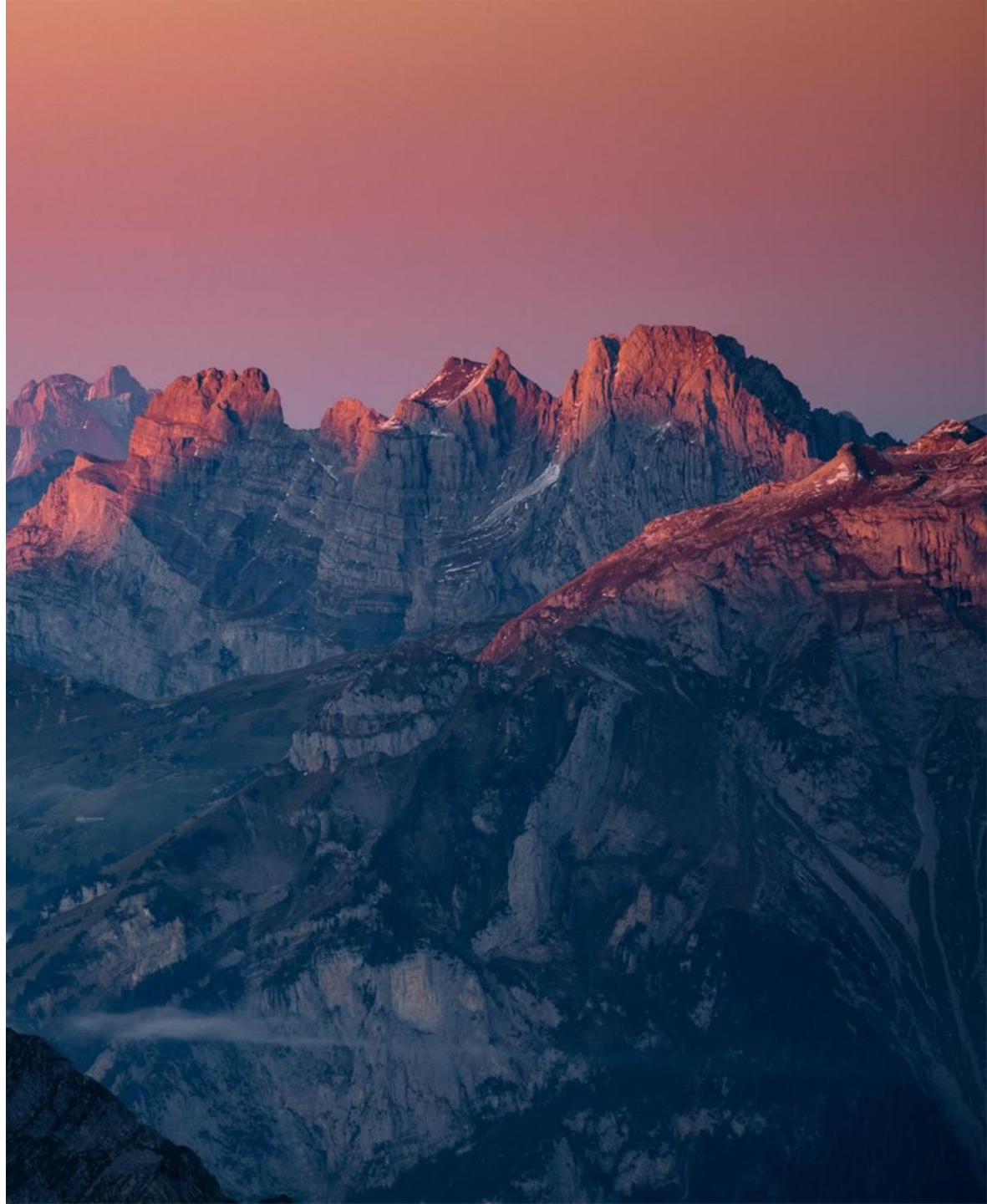
Paul Stiffler
Information Security Officer Swisscom Banking

17. September 2024

swisscom

Agenda

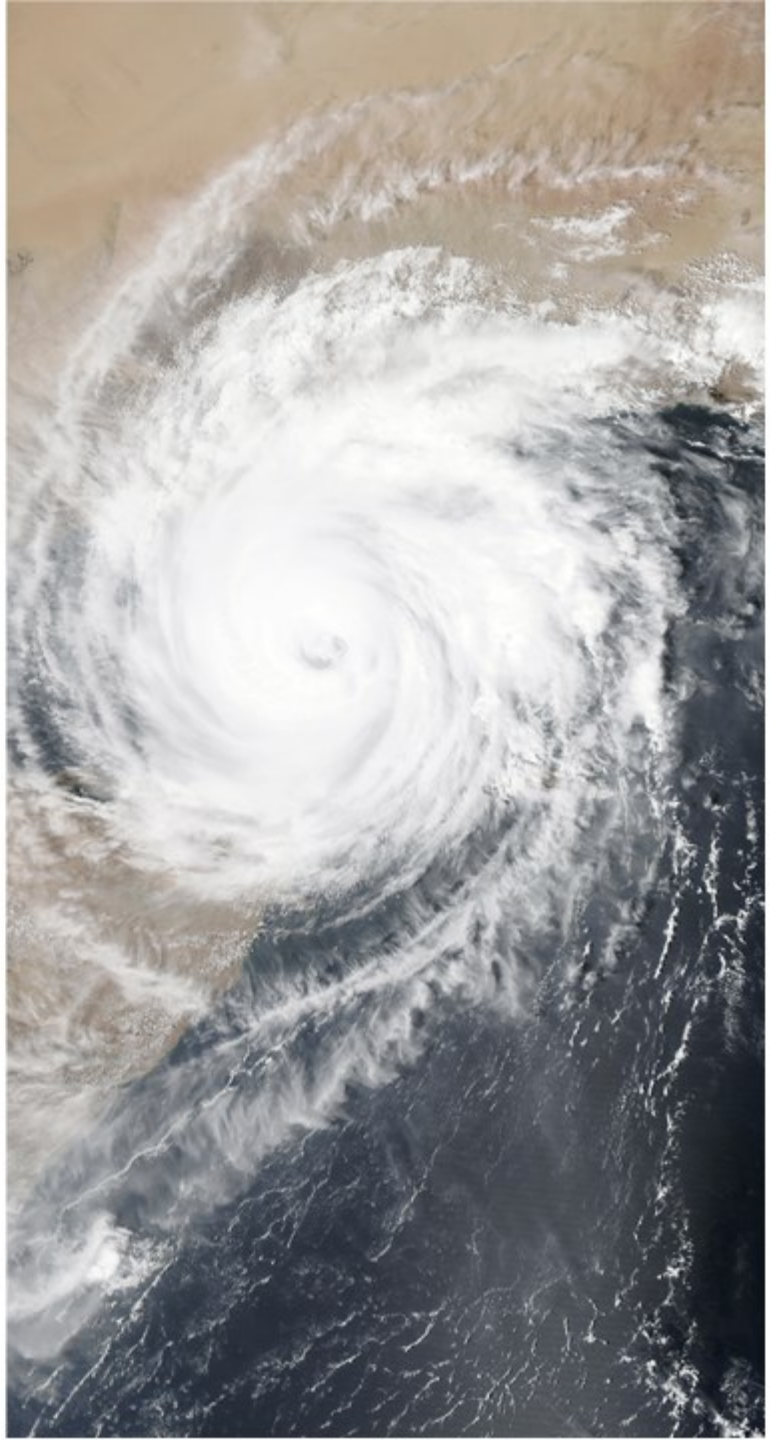
1. Aktuelle Bedrohungslage
2. Top 5 Cyber Risk Szenarien für Banken
3. Fokus: Ransomware



2. Aktuelle Bedrohungslage

Die Bedrohung ist real

Jeden Monat…



39

Sicherheitszwischenfälle, die vom Swisscom **CSIRT** bekämpft wurden

3'660

DDoS-Angriffe gegen die Swisscom-Infrastruktur

1'739

Kontaktierte Privatkunden wegen **gehackter Accounts**

343

Erkannte und blockierte **Phishing-Attacken**

134'324'130

Angriffsversuche gegen die Swisscom Infrastruktur blockiert

Update Mai 2024

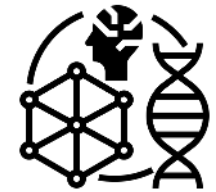
2. Top 5 Cyber Risk Szenarien für Banken

Top 5 - Cyber Risk Szenarien für Banken -> Sicht Swisscom als Provider

Data Breaches

Ransomware

Supply Chain Attacks



Emerging Technologies

Insider Threats

Szenario 1 – Data Breach

Bedrohung:
Ein ausgeklügelter Angriff einer Hacker Gruppe auf die Kernbankensysteme einer Bank.

Ziele:
Kernbankensysteme, Konten, kritische Daten, CID, Zahlungsinformationen.

Methoden:
- Phishing (gefälschte E-Mails/Texte).
- Malware (Datendiebstahl/Fernzugriff).
- Ausnutzung ungepatchter Sicherheitslücken.

Auswirkungen:
- Vertrauensverlust der Kunden, potenzieller Ausstieg.
- Finanziell: Bußgelder, Anwaltskosten,.
- Rufschädigung, die die Kundenbindung und -gewinnung beeinträchtigt.

Mitigation:

- Datensicherheit: Verschlüsselung, Zugriffskontrolle, Schwachstellenmanagement.
- Mitarbeiterschulung: Bewusstsein für Cybersecurity, Phishing-Betrug.
- Risikomanagement für Drittanbieter: Prüfe und überwache Anbieter.
- Plan zur Reaktion auf Data Breaches

Szenario 2 – Supply Chain Attack

Bedrohung:
Angreifer nutzen Schwachstellen bei Drittanbietern aus, um sich Zugang zu den Systemen und Daten einer Bank zu verschaffen. Angreifer können es auf Drittanbieter abgesehen haben, die IT-Dienstleistungen wie Softwareentwicklung, Cloud Computing oder Datenspeicherung anbieten.

Auswirkungen:
- Datenschutzverletzungen
- Finanzielle Verluste
- Reputationsschaden

Mitigation:

- Prüfen und Überwachen: Due-Diligence-Prüfung, Überprüfung von Sicherheitsnachweisen, regelmäßige Überwachung der Sicherheitslage, Penetrationstests.
- Software Bill of Materials (SBOM): Verfolgen der Herkunft von Softwarekomponenten.
- Multi-Faktor-Authentifizierung (MFA): Starke MFA für den Zugriff Dritter.
- Zugriffsberechtigungen: Regelmäßige Überprüfung und Aktualisierung.
- Cybersicherheitsschulung: Regelmäßige Schulungen für Mitarbeiter von Dritten.

Szenario 3 – Insider Threat

Bedrohung:

Insider-Bedrohungen stellen ein erhebliches und oft übersehenes Risiko für Banken dar. Insider, wie z. B. Angestellte, Auftragnehmer oder ehemalige Angestellte, haben legitimen Zugang zu den Systemen und Daten einer Bank und sind daher in der Lage, Schaden anzurichten, wenn sie es wollen.

- Zugang zu sensiblen Daten und Systemen
- Kenntnis der internen Prozesse und Verfahren
- Fähigkeit, sich in legitime Aktivitäten einzumischen

Auswirkungen:

- Finanzielle Verluste
- Reputationsschaden
- Compliance-Verstöße
- Störungen des Betriebsablaufs

Mitigation:

- Zugangskontrollen: Starke Kontrollen, Zugriff mit geringsten Rechten.
- Schutz vor Datenverlust (DLP): Lösungen zur Verhinderung der Datenexfiltration.
- Verhaltensüberwachung (Behavioral Monitoring): Systeme zur Erkennung verdächtiger Aktivitäten.
- Cybersecurity Training: Sensibilisierung für Insider-Bedrohungen, Phishing, Social Engineering.
- Vier-Augen-Prinzip: Aufgabentrennung für sensible Aufgaben.
- Austausch von Informationen über Bedrohungen: Zusammenarbeit mit Partnern und Strafverfolgungsbehörden.
- Reaktion auf Vorfälle: Entwickle und teste Reaktionspläne für Insider-Vorfälle.

Szenario 4 – Emerging Technologies

Bedrohung:

Die Integrität der Infrastruktur ist ein entscheidender Aspekt der Cybersicherheit für Banken, da sie die physischen und digitalen Komponenten umfasst, die ihren Betrieb unterstützen. Angriffe auf die Integrität der Infrastruktur können verheerende Auswirkungen auf die Fähigkeit einer Bank haben, ihre Kunden zu bedienen
Cyberangriffe: Angriffe, die auf die digitale Infrastruktur einer Bank abzielen, z. B. auf Netzwerke, Server und Anwendungen.

Auswirkungen:

- Systemausfälle: Verlust von kritischem Systemzugang.
- Datenpannen: Diebstahl von sensiblen Kundendaten.
- Finanzielle Verluste: Einnahmeverluste durch Ausfälle und Betrug.
- Reputationsschaden: Auswirkungen von Sicherheitsvorfällen auf die Reputation der Bank

Mitigation:

- Zugangskontrollen: Starke Kontrollen, Zugriff mit geringsten Rechten.
- Physische Sicherheit: Schutz der IT-Infrastruktur vor unbefugtem Zugriff/Unterschlagung.
- Netzwerksicherheit: Firewalls, IDS, IPS gegen Cyberangriffe.
- Datensicherheit: Verschlüsselung, Zugriffskontrolle zum Schutz der Kundendaten.
- Plan zur Reaktion auf Vorfälle: Entwicklung/Test von Plänen für die Reaktion auf Cyberangriffe und deren Wiederherstellung.

3. Fokus: Ransomware

Szenario 5 – Ransomware

Bedrohung:
Ransomware-Angriffe erfolgen in der Regel über Phishing-E-Mails oder andere Social-Engineering-Taktiken. Die Ransomware verschlüsselt die Daten und macht sie damit unbrauchbar. Die Angreifer senden dann eine Lösegeldforderung, in der sie eine Zahlung für die Entschlüsselungsschlüssel fordern.

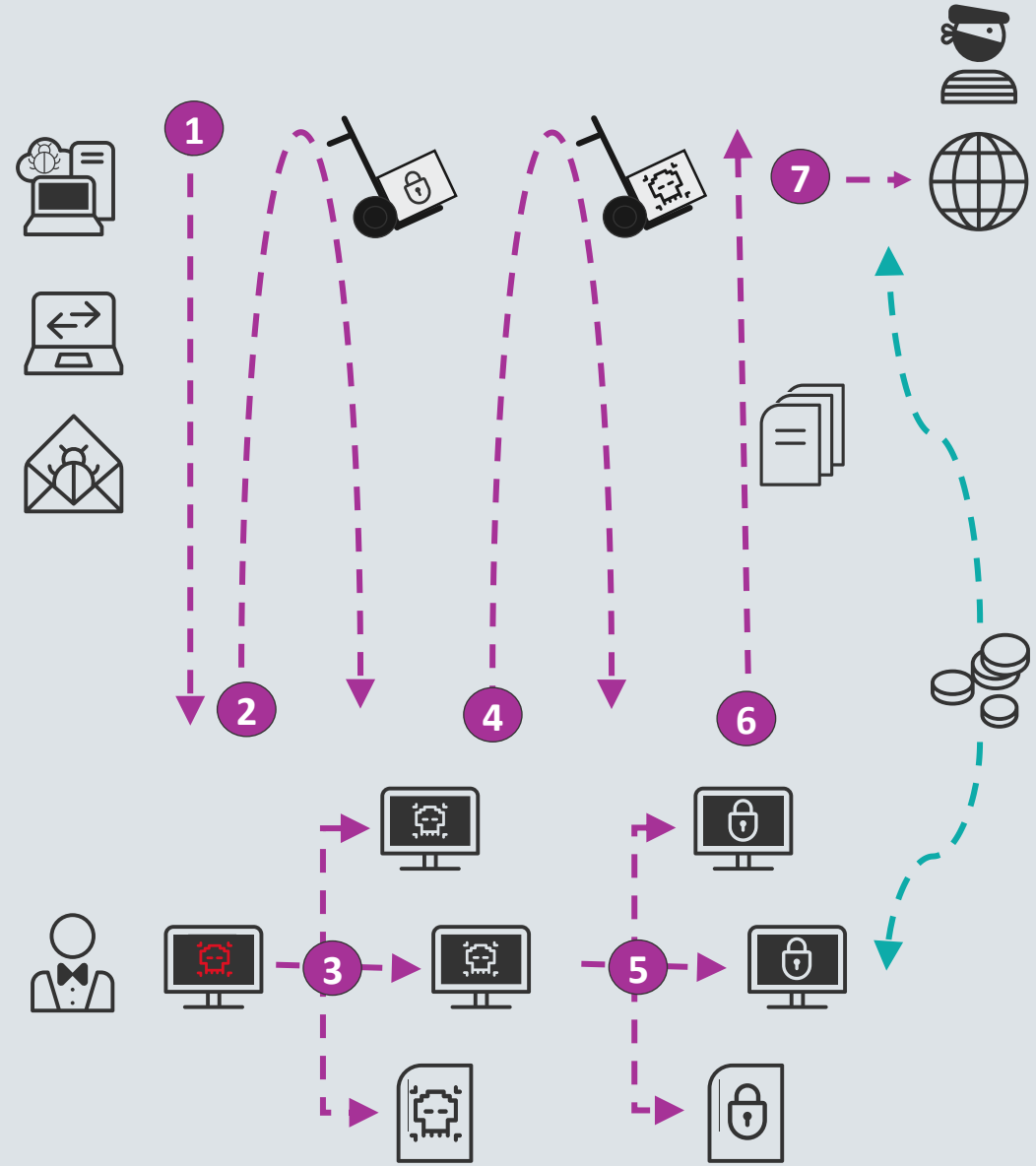
Auswirkungen:
Ransomware-Angriffe können erhebliche Auswirkungen auf den Betrieb einer Bank haben, z. B.

- Datenverlust
- Schädigung des Rufs

Mitigation:

- Datensicherung und -wiederherstellung: Robuste Strategie für die Datenwiederherstellung.
- Netzwerksicherheit: Firewalls, IDS, IPS zur Erkennung und Verhinderung von Angriffen.
- Endpunkt- und Messaging-Sicherheit: Antivirus und Anti-Malware zum Schutz der Geräte.
- Mitarbeiterschulung: Sensibilisierung für Cybersicherheit, Schulungen zu Ransomware-Betrug.
- Anwendungsfallbasierte Erkennung:

Die Phasen eines Angriffs



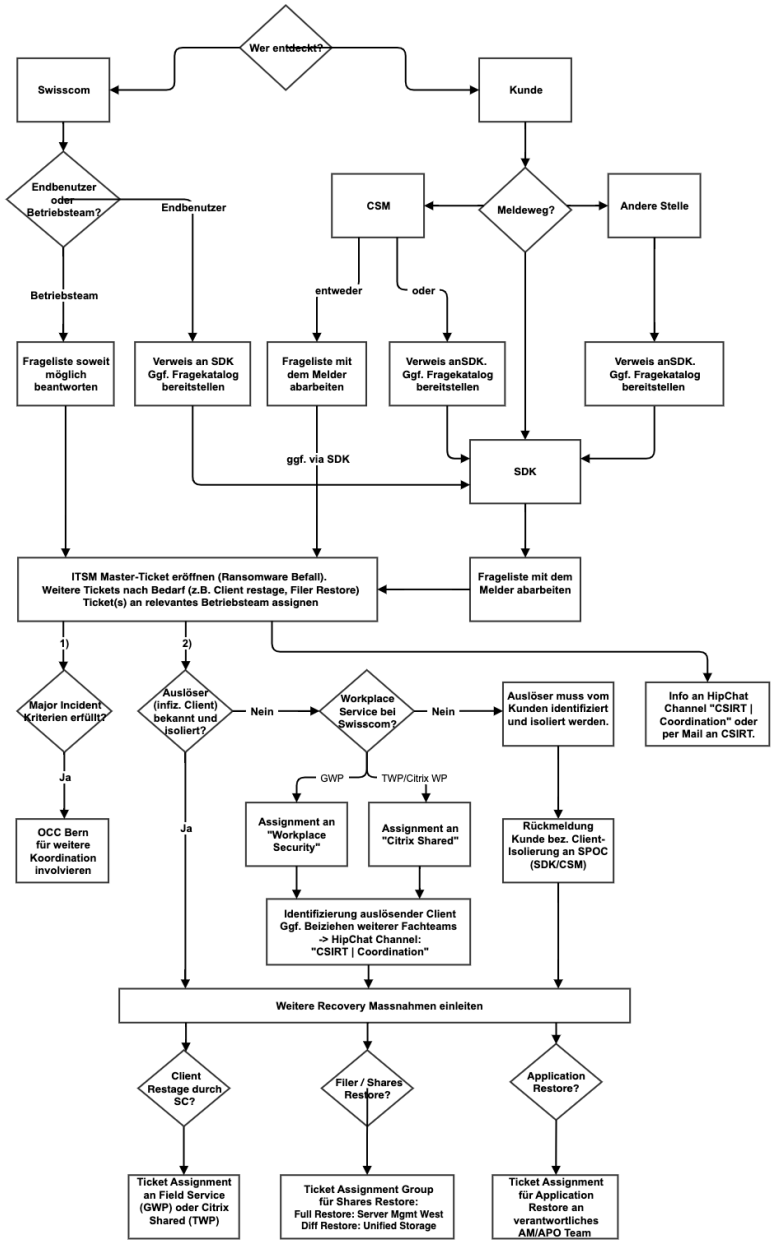
Quelle: MELANI Halbjahresbericht 2020/1

Framework: Ransomware Incident Process

Im Falle einer Entdeckung muss es schnell gehen, um zu verhindern, dass sich die Malware ungehindert ausbreitet.

Um dies zu erreichen, wurde der auf Ransomware spezialisierte (Standard-) Prozess für die Behandlung geschaffen, um Ransomware Infektionen (z.B. Phishing-Mail oder Drive-By) zu erkennen und zeitnah zu mititgieren.

Im Verlauf des Incidents sind typischerweise die Kunden, mehrere Betriebsteams für Identifizierung, Schadensbegrenzung und Wiederherstellung zu involvieren.



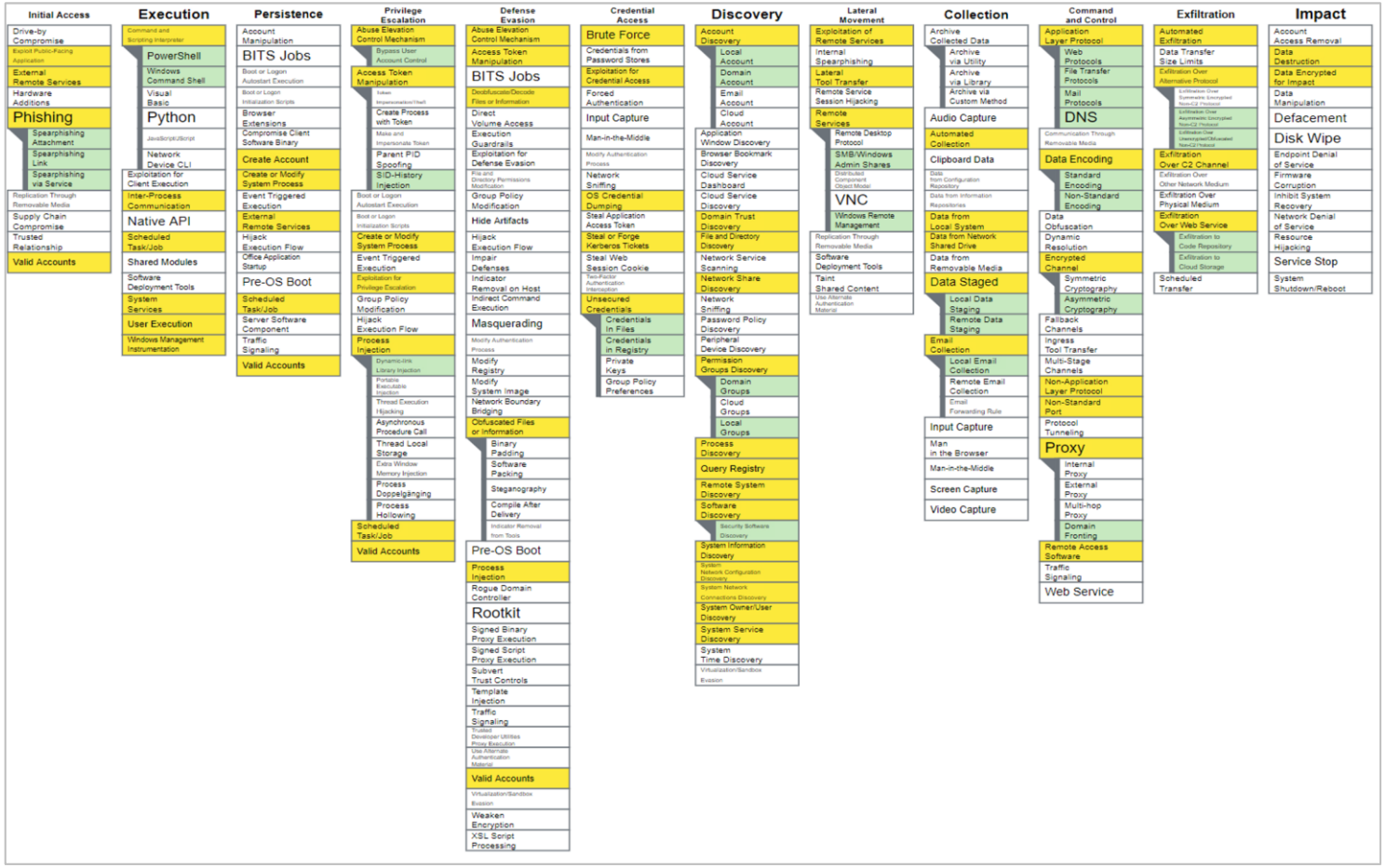
Typical ATT&CK Lifecycle observed during Human Operated Ransomware Attacks

Beispiel der Schutzvorkehrungen und Ansätze bei Human-operated Ransomware (Grüne & gelbe Felder):

Human-operated Ransomware ist ein großer und wachsender Angriffstrend, der eine Bedrohung für Unternehmen in jeder Branche darstellt.

Human-operated Ransomware unterscheidet sich von herkömmlicher Ransomware.

- Diese "Hands-on-Keyboard"-Angriffe zielen auf das gesamte Unternehmen ab und nicht nur auf einzelne Devices .
- Sie nutzen das Wissen der über gängige System- und Sicherheitsfehlkonfigurationen, um in das Unternehmen einzudringen, sich im Unternehmensnetzwerk zurechtzufinden
- und sich an die Umgebung und ihre Schwachstellen anzupassen, während sie sich bewegen.

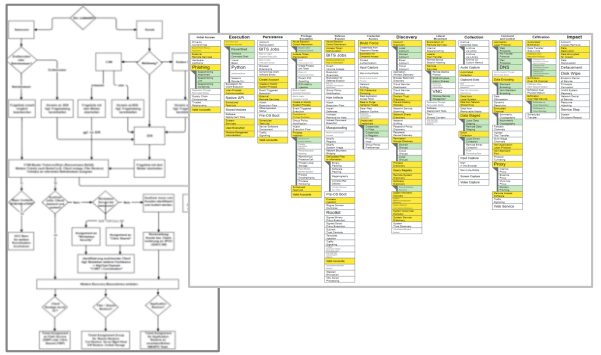


Beispiel - Schutzebenen E2E Ransomware

- Ransomware E2E -

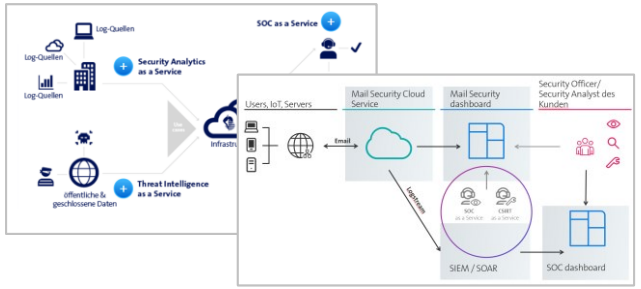
Group Ebene - Swisscom Group Security CSIRT/SOC

- Governance / Policy adressiert Ransomware
- Security Architecture Framework
- Monitoring und standard Incident Prozess
- Spezifische Ransomware-Prozesse
- Recovery Strategien



Ebene Services und Produkte

- Email Security – “Sandboxing”
- Endpoint Detection and Response Service (EDR)
- Threat Detection and Response Service (TDR)
- Filer Protection Option - Storage
- Backup



Ergänzende Massnahmen, durch den Kunden selbst

- Awareness und Mitarbeiter Training (Phishing Übungen / Testmails etc.)
- Cyberübungen (simulierte Angriffe)
- Einfache Meldung verdächtiger Mails an Spezialisten

Kontaktperson

Paul Stiffler
Information Security Officer Swisscom Banking

paul.stiffler@swisscom.com
+41 79 359 12 73