OST
Eastern Switzerland
University of Applied Sciences

Incident Response

Zusammenfassung

Studiengang Informatik
OST - Ostschweizer Fachhochschule
Campus Rapperswil-Jona

Frühjahrssemester 2022

Autor:	Gian Flütsch, Marius Zindel
Version:	28. Juni 2022
Dozent:	Gregor Wegberg

Inhaltsverzeichnis

1 Incident Response Grundlagen

1.1 Definition

Incident Response are actions taken to mitigate or resolve an information security incident, including those taken to protect and restore the normal operational conditions of an information system and the information stored in it.

- Incident Response ist die Aktivität einen Informationssicherheitsvorfall zu behandeln
- Ein Vorfall ist ein oder mehrere Informationssicherheitsereignisse, die (wahrscheinlich) zu einem Schaden für die Organisation führen
- Ein Ereignis verletzt die Aktivitäten eines Unternehmens zur Sicherstellung der Informationssicherheit
  - nicht nur FW deaktivieren etc. → MA, welcher NB entsperrt liegen lässt kann auch ein Security Incident werden
- Incident Response ist die Bewältigung einer Verletzung der Informationssicherheit

1.2 Information Security Incident (Informationssicherheitsvorfall)

Einzelnes oder eine Reihe von ungewollten oder unerwarteten Informationssicherheitsereignissen, die eine erhebliche Wahrscheinlichkeit besitzen, Geschäftstätigkeiten zu gefährden und die Informationssicherheit zu bedrohen.

1.3 Information Security Event (Informationssicherheitserreignis)

Erkanntes Auftreten eines Zustands eines Systems, Dienstes oder Netzwerks, der eine mögliche Verletzung der Politik oder die Unwirksamkeit von Massnahmen oder eine vorher nicht bekannte Situation, die sicherheitsrelevant sein kann, anzeigt.
Bei einem **Ereignis** kann etwas vorhanden sein (z.B. AV Meldung → true positive oder falscher Alarm?) → falls Mimikatz in AV Report steht → befindet man sich schon im **Event** und nicht mehr im **Ereignis**
Bei einem **Event** ist wirklich etwas (effektiver Security Vorfall)!.

1.4 Ziel Informationssicherheit

CIA Triad → Confidentiality, Integrity, Availability

1.4.1 Confidentiality

Information wird unbefugten nicht verfügbar gemacht oder offengelegt.

1.4.2 Integrity

Information ist richtig und vollständig.

1.4.3 Availability

Information ist für eine befugte Entität bei Bedarf zugänglich.

1.5 Schützenswerte Daten

- Kundendaten → DSG (Datenschutz Gesetz)/ GDPR
- Mitarbeiterdaten → DSG
- PII/ PHI → DSG
- Backups
- Trade Secrets

2 Aktuelle Bedrohungslage

2.1 Vishing

Beim Vishing (Voice Phishing) werden Personen mündlich zu Handlungen aufgefordert, von denen sie glauben, sie seien in ihrem Interesse. Vishing setzt oft da an, wo Phishing an seine Grenzen stösst.

2.2 Vishing + E-Mail Phishing

Oft fängt das ganze mit Phishing (z.B. via E-Mail) an und es weitet sich schlussendlich ins Vishing aus.

Beispiel:
Jemand besucht eine Social-Media-Plattform, klickt auf einen verlockenden Link – und schon erscheint ein blauer Bildschirm mit einer Warnmeldung und der Aufforderung, bei der angezeigten gebührenfreien Telefonnummer anzurufen, um ein ernsthaftes Problem mit dem Computer zu beheben.
Am Telefon meldet sich ein freundlicher Techniker, der gerne bereit ist zu helfen – allerdings nur gegen Bezahlung. Nachdem für den Kauf der Software, mit der das Computerproblem behoben werden soll, die Kreditkartendaten zur Verfügung gestellt wurden, ist der Betrug komplett und kommt das Opfer teuer zu stehen.
Die Software funktioniert nicht, und vom hilfsbereiten Techniker wird man nie wieder etwas hören. Der Benutzer ist ein weiteres Opfer der als „Vishing“ bezeichneten Betrugsmethode geworden.

2.3 Mögliche Folgen

- eBanking Trojaner wird installiert
- Zukünftige eBanking-Aktivitäten können durch die Cyberkriminellen manipuliert werden
  - Betrag ändern, Zielkonto ändern, SMS-Verifikation wird ausgehebelt
- Aktuelle Antivirussoftware konnte die Schadsoftware nicht identifizieren
- Hätte jede andere Schadsoftwareart sein können!

2.4 Ransomware

How Ransomware works!

2.4.1 Ransomware Angriffe

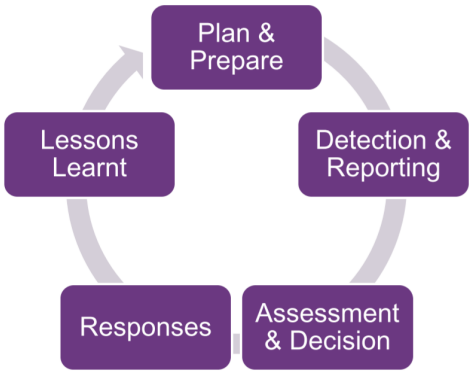
1. Kompromittierung
2. Sensible Daten entwenden
3. Daten verschlüsseln (1. Erpressung)
4. Mit Veröffentlichung der Daten drohen (2. Erpressung)
5. Optional: Öffentlich an den Pranger stellen
6. Optional: Mit DDoS drohen (3. Erpressung)
7. Assoziierten Personen drohen (4. Erpressung)
8. Optional: Business E-Mail Compromise (BEC), Phishing etc.
9. Optional: Veröffentlichung der gestohlenen Daten

2.5 Wie schützen wir uns

- Mehrere, nacheinander gelagerte Schutzmechanismen (Defense in depth)
- Vertrauen nicht einem einzigen Produkt und Mechanismus (z.B. AV-SW, FW)
- 100% Sicherheit gibt es nicht, aber:
  - Wir können die Kosten für Angreifer erhöhen
  - Wir können Angreifer verlangsamen
  - Wir können Angreifer erkennen
  - darum gibt es Incident Response

3 Incident Response Prozess

3.1 ISO/IEC 27035-1



3.1.1 Plan & Prepare

- Organisatorischen Incident Management Rahmen schaffen
- CEO/ Geschäftsführer muss vollstes commitment für Cyber Security zeigen
- Incident Management Plan festlegen
- Incident Response Team (IRT) etablieren
- Klassifikation festlegen, Formulare erstellen
  - Damit im Notfall nicht wichtige Angaben im Formular vergessen gehen (z.B. SN Festplatte)
- Intern & extern vernetzen, vor allem verantwortliche Entitäten für Informationssicherheitsereignisse, -vorfälle & Schwachstellenmanagement
  - Connection/ Beziehungen aufbauen um im Notfall Zeit zu sparen
- Trainieren, schulen, simulieren und Bewusstsein steigern (Red Teaming etc.)
- Fähigkeiten / Maturität überwachen

Ukraine Konflikt aus IR Sicht

- Heute die Projekte starten (jetzt ist Unterstützung GL sehr hoch)
- Geoblocking einschalten (auf FW)
- Logs beobachten/ Monitoring
- Low hanging fruits
- Awareness Kampagne
- Notfallkontakte überprüfen
- Tabletop Übungen
- Genauer Ablauf sollte eine Organisation selber entwickeln (Incident Management Plan)
- Diverse Quellen können ein Ereignis feststellen und/oder melden (SIEM, FW, SOAR, EDR, etc.)
- **Wichtig**:
  - Meldewege sind definiert
  - Meldewege sind allen relevanten Parteien bekannt (Notfallnummernblatt)
  - Empfänger der Meldung wissen, was damit zu tun ist

  - Bei Meldequelle bedanken, Resultat/Folge der Meldung teilen → Meldungen motivieren!
- IT-Sicherheitssysteme (technische Quellen)
  - Proaktive Detektion vs. Reaktive Detektion
  - Protokolle, SIEM, Schwachstellen-Scanner
  - Deception Technologie, z. B. Honeypots, Honeytokens, Honey Accounts etc.
    * Testen, ob Unternehmen Informationen weiterverkauft
    * *Honeypod* wird eine Einrichtung bezeichnet, die einen Angreifer oder Feind vom eigentlichen Ziel ablenken soll oder in einen Bereich hineinziehen soll, der ihn sonst nicht interessiert hätte (z.B. in Form eines Scheinziels).
  - Email Traps (Spamtrap), Sandbox
- Wenn technische Quellen vorhanden sind und genutzt werden: Merkt jemand die Meldung?
  - Automatisierung, unübersehbarer Alarm, SIEM (Aspekte der Cyber Defense)
- Organisation
  - Interne Partner: IT-Betrieb, Netzwerkbetrieb, IT Support
  - externe Partner
    * ISP, MSP (Managed Service Provider), IT-Dienstleister, Security-Partner, etc.
      · Mit Dienstleistern Kommunikationspflicht festlegen
    * Cloud Dienstleister (SaaS, IaaS, PaaS, ...) → Schattendienstleister
      · Security-Kontakt einrichten
    * IT-Security-Partner, nationales CSIRT / NCSC
    * Offene und geschlossene Gemeinschaften zum Informationsaustausch
  - Kommunikation im Vorfeld definieren!
  - Medien
    * Kann das Incident Response Team damit umgehen?
    * Nein! Wenn Medien involviert sind:
      · Public Relations, Marketing, Presseabteilung, ... involvieren
      · Geschäftsleitung sollte im Normalfall informiert werden
- Mitarbeiter
  - Wissen diese wo sie sich melden dürfen?
  - Sind sie motiviert sich zu melden?
- Externe Individuen
  - White/Gray/Black Hats, Sicherheitsforscher, Bug Bounty usw.
  - Have I Been Pwned, „Darknet Monitoring“ / „Cyber Threat Intelligence“
- Weiss der Empfänger/die Empfängerin, was mit einer Meldung zu tun ist?

Reporting

- **Ziel**: Wer, was, wo und wann für die weitere Verarbeitung festhalten.
  - Wer hat es entdeckt? Wie erreichen wir diese Person?
  - Was wurde wann beobachtet? Wo wurde es beobachtet?
  - Wann wurde was bereits gemacht?
- Je nach Organisation, Quelle und Auftrag diverse Formate denkbar:
  - Mündlich am Telefon oder in Person
  - Schriftliches oder digitales, vordefiniertes Formular

3.1.2 Assessment & Decision

- **Ziel**: Feststellen, ob das Ereignis ein Vorfall ist
- Informationen zum Ereignis sammeln
- Entscheidung basierend auf Informationen:
  - Kann es ein Vorfall sein? → Eskalation zum IRT (Incident Response Team)
  - Ist es ein Vorfall? → IRT startet Response-Phase
  - Ist es falschpositive Meldung? → Falschpositivenrate im Lessons Learnt senken
- Wichtig: Spätestens ab hier detailliertes Protokollieren
  - Was wurde wann, wo und von wem festgestellt?
  - Welche Folgen hatte es?

3.1.3 Responses

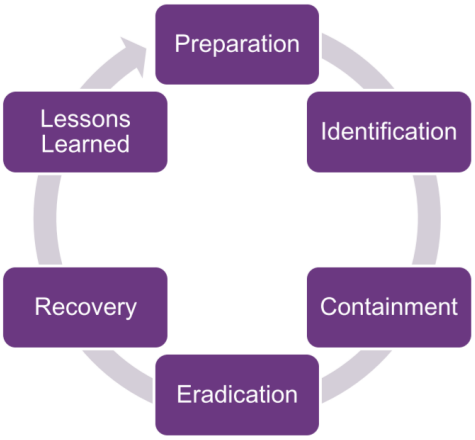
- **Ziel**: Vorfall bewältigen/lösen
- Die Einschätzung (Klassifikation, Schweregrad etc.) fortlaufend neu bewerten
- Alle beteiligten Personen führen detailliertes Protokoll
- Beweise sammeln und sichern für eine mögliche spätere Untersuchung

3.1.4 Lessons Learnt

Lessons Learnt geht oft vergessen, ist aber sehr wichtig dass nicht wiederholt die gleichen Fehler gemacht werden.

- Aus dem geschehenen lernen, analog einer Retrospektive oder einem Post Mortem
  - Welche Schutzmassnahmen anpassen/verbessern?
  - Wie können wir das Incident Management verbessern?
  - Müssen wir unser Risikomanagement anpassen/ergänzen?
- **Wird sehr gerne übersprungen / ignoriert**
- Absolut essenziell zur Steigerung der IT-Sicherheit und Reaktion auf Ereignisse/Vorfälle

3.2 SANS Incident Response Prozess



3.2.1 Preparation

- Richtlinien, Prinzipien, Regeln etc. festlegen
- Prozess und Vorgehen für Vorfallbewältigung definieren
- Kommunikationsplan: intern, extern, Partner etc.
- Computer Incident Response Team (CIRT) definieren
- Notwendige Werkzeuge bereitstellen
- Trainieren
- **Ziel**: Technische und organisatorische Rahmenbedingungen vorbereiten/pflegen

3.2.2 Identification

- Beginnt mit der Meldung eines möglichen Ereignisses
- Entscheiden, ob ein Ereignis vorliegt
- Prüfen, ob es ein Vorfall ist
- Spätestens in dieser Phase muss alles dokumentiert werden: Wer, was, wo, weshalb und wie

3.2.3 Containment

- **Ziel**: Schaden mindern und weiteren verhindern
  1. Kurzfristiges Containment: so früh wie möglich Schaden eingrenzen
  2. System Back-Up: Bevor Systeme zurückgesetzt werden diese forensisch sichern
  3. Langzeit Containment: Temporäre Massnahmen, bis Eradication abgeschlossen ist

Beispiel Containment

- Domain sperren
  - Soll `p.estonine.com` oder `estonine.com` gesperrt werden?
- IP-Adresse vom DNS Resource Record A (IPv4) und AAAA (IPv6) sperren
- In DNS Logs nach Domain suchen
  - Domain ist ein Indicator of Compromise (IOC)!
- In Firewall, Forward Proxy etc. Logs nach IP-Adresse suchen

  - IP-Adresse ist ein IOC!

- *Scheduled Task* ist ein starker *Indicator of Compromise (IOC)*
  - Wird von Schadsoftware erstellt & Name ist oft fest in Schadsoftware einprogrammiert
  - Können mit PowerShell, WMI etc. nach Scheduled Tasks mit diesem Namen auf allen Windows-Systemen suchen

3.2.4 Eradication

- Schädliches und unerwünschtes entfernen
- Betroffene Systeme wiederherstellen ($\neq$ Backup wiederherstellen, zumindest nicht immer)
- System wieder in sauberen Zustand bringen (Malware entfernen, etc.)

3.2.5 Recovery

- Betroffene Systeme wieder in den Betrieb bringen
- Vorsicht! Sollte nicht erneut zum Vorfall führen
  - System überprüfen & überwachen
- Typische Herausforderung: Wann ist ein System *sauber*?

3.2.6 Lessons Learned

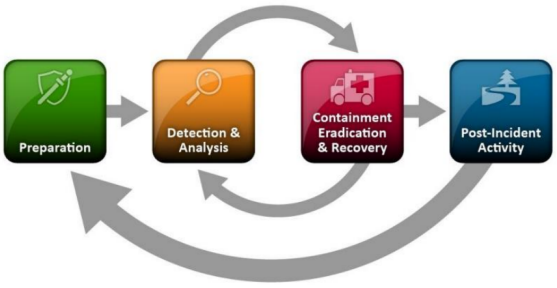
Siehe 3.1.4

3.3 NIST Incident Response LifeCycle

NIST Standard mehr technisch, ISO Standard mehr fürs Management

NIST

1. Preparation
2. Detection and Analysis
3. Containment, Eradication, and Recovery
4. Post-Incident Activity



SANS

1. **P**reparation
2. **I**dentification and Scoping
3. **C**ontainment / Intelligence Development
4. **E**radication / Remediation
5. **R**ecovery
6. **L**essons Learned / Threat Intel Consumption

4 CSIRT aufbauen

4.1 Begriffe

4.1.1 CSIRT (Computer Security Incident Response Team)

Ein *CSIRT* ist ein Team von IT-Sicherheitsexperten, dessen Hauptaufgabe darin besteht, auf Computersicherheitsvorfälle zu reagieren. Es bietet die notwendigen Dienstleistungen an, um diese zu bearbeiten und die Betroffenen bei der Wiederherstellung nach Verstössen zu unterstützen.

- Präziser, Free to use, ca. 19 Teams in CH
- CSIRT wird oft beim Besprechen der Aktivitäten verwendet
- CERT kommt gerne in den Teambezeichnungen vor
- NCSC (National Cyber Security Centre) ist ein verwendeter Betriff für ein „nationales CSIRT“
  - Ein NCSC hat im Normalfall einen Auftrag vom Staat. Dieses kann mehr/anders sein, als von einem CSIRT erwartet

Wird oft als synonym verwendet zu *CERT (Computer Emergency Response Team)*.

Grundlagen eines CSIRT

- Ein CSIRT ist eine Organisationseinheit
- Es bietet einem bestimmten Personenkreis Dienstleistungen und Unterstützung an
- Es ist in der Verhütung, Erkennung, Behandlung und Reaktion auf Sicherheitsvorfälle involviert
- Es hat einen Auftrag

4.1.2 Formen eines CSIRT

Internes Team

- Dediziertes Team innerhalb der Organisation
- Team besteht aus Personen, die nur fürs CSIRT arbeiten
- Typisch für grössere Organisationen, die sich ein dediziertes Team leisten können

Virtuelles Team

- Team besteht aus Personen, die in mehreren Teams arbeiten
- Typisch für kleinere Organisationen und solche, die einen Teil durch Dritte leisten lassen

Externes Team

- CSIRT Dritter als Dienstleistung beziehen
- **Achtung**: Internes Personal zwingend notwendig, mindestens in Form eines virtuellen Teams!

4.1.3 SOC (Security Operations Center)

- Sammelt Aktivitäten und Ereignisse von Servern, Clients, Netzwerken etc.
- Fortlaufende, automatische Analyse dieser Aktivitäten auf verdächtiges Verhalte
- Verifikation der Auffälligkeit (wird Ereignissfall zum Vorfall oder bleibt es beim Ereignis)
- Eskalation zur Nachverfolgung/Lösung (→ Sicherheitsereignis/-vorfall)
- nicht nur Monitoring, sondern kann auch Zertifikate erstellen, Berechtigungen vergeben oder sogar ein „halbes CSIRT“ ist

SOC-Betriebsmodell: Bereitstellungsmethode

	Inhouse	Hybrid	Extern
Beschreibung	• Sämtliche personellen und technischen Ressourcen sind inhouse vorhanden	• Gewisse personellen und technischen Ressourcen sind inhouse vorhanden, die fehlenden werden zugemietet/gekauft	• Sämtliche personellen und technischen Ressourcen werden zugemietet/gekauft • Entlastung interner IT
Vorteil(e)	• Eingefuchstes Team • Interner Wissensaufbau gewährleistet sehr effizient	• Selektives Outtasking • 24/7-Abdeckung möglich • Optimierung des eigenen Personalbestandes • Interner Wissensaufbau möglich	• Ausbildungs- und Spezialtoolkosten externalisiert • 24/7 Abdeckung möglich
Nachteil(e)	• 24/7 Abdeckung teuer • Tendenz zu Unter- bzw. Überkapazitäten • Ausbildungs- und Spezialtoolkosten • Sehr teuer	• Teuer	• Interner Wissensaufbau erschwert • Achillesferse Kommunikation / Schnittstellen • Sehr teuer braucht immer noch interne MA

4.1.4 SIEM (Security Information and Event Management)

- IT-System (Software + Hardware) zur Sammlung von Systemverhaltensdaten und der automatischen Auswertung dieser

4.1.5 MDR (Managed Detection & Response)

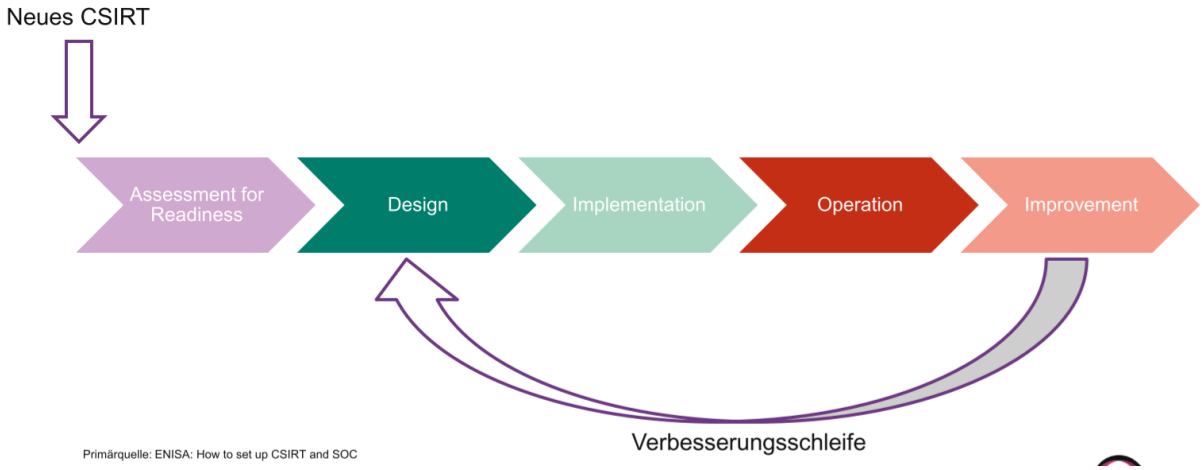
Detect

- Standardwerte und –verhalten feststellen
- Abweichungen von der Norm erkennen
- Informationssicherheitsereignisse erkennen/entdecken
- Festlegen, wann ein Informationssicherheitsvorfall vorliegt
- Verwundbarkeitsscans & Asset Überwachung

Respond

- Informationssicherheitsereignisse analysieren
- Informationssicherheitsvorfall bewältigen

4.2 CSIRT Lifecycle



Verbesserungsschleife ist sehr wichtig → besser werden

4.2.1 Assessment for Readiness

Mandat

- Was ist der Zweck des CSIRT?
- Wieso ist ein CSIRT notwendig?
- Welche Rechte und Pflichten hat das CSIRT?

Struktur

- Wer finanziert das CSIRT?
- Wer ist für das CSIRT verantwortlich?
- Mit welchen Stellen/Organisationen/Abteilungen/... muss es interagieren?

Ziel dieser Phase

- Grober Umsetzungsplan und Budget
- Anforderungen für die Design-Phase
  - Mandat, Umsetzungsplan, Budget
  - Rollen, Fähigkeiten, Ressourcen usw., die für die Design-Phase zur Verfügung stehen

4.2.2 Design

- CSIRT Dienstleistungen definieren
- CSIRT Prozesse und Abläufe definieren
- Organisationsstruktur und die Fähigkeiten der CSIRT Rollen
- Definition des notwendigen Wissens fürs CSIRT und Weiterbildungen
- Anforderungen an die Büroräumlichkeiten und deren Verteilung, Technologien
- Angestrebte interne und externe Partnerschaften
- Informationssicherheitsmanagement
- Anforderungen und Ziele der Implementation-Phase

4.2.3 Implementation

- Notwendiges Personal anstellen oder ins CSIRT integrieren
- Bei Bedarf die Mitarbeitenden gemäss Profilanforderungen weiterbilden
- Umsetzung der Anforderung an die Räumlichkeiten, Technologien, Prozesse, ans Informationssicherheitsmanagement etc. aus der *Design*-Phase
- CSIRT Prozesse trainieren
- Kontaktaufnahme und Vernetzung mit internen/externen Partnern

Was für Dokumente/ Richtlinien sollte ein CSIRT haben?

Diese sollen sicherstellen, dass Information zu Vorfällen, Schwachstellen, Artefakten etc. geschützt sind.

- Klassifizierung von Informationen
- Schutz von Informationen
- Aufbewahrung von Informationen
- Vernichtung von Informationen
- Weitergabe von Informationen
- Zugang zu Informationen
- Nutzungsreglement für die CSIRT-Systeme
- Definition / Klassifikation / Kategorisierung von Ereignissen und Vorfällen
- Behandlung von Vorfällen
- Zusammenarbeit mit anderen Teams

4.2.4 Operations

- Fortlaufend die Arbeit überwachen und messen (Stichwort: Key Performance Indicators (KPI))
- Regelmässige Qualitätsprüfung und Erfüllung der Vorgaben prüfen
- Weiterentwicklungsmöglichkeiten identifizieren und sammeln
- Und die eigentliche CSIRT-Arbeit leisten

4.2.5 Improvement

- Vorschläge für Verbesserungen sammeln
- Vorgehen und Anforderungen für die Entwicklung der Verbesserungen (*Design*-Phase) festlegen
- Notwendige Ressourcen (z. B. Budget) organisieren, damit die *Design*-Phase starten kann

4.3 CSIRT-Dienste

4.3.1 CSIRT Service Areas

Information Security Event Management

- Daten aus Ereignisquellen sammeln, korrelieren, anreichern, auswerten und mögliche Informationssicherheitsereignisse identifizieren
- Fortlaufend Daten aus Ereignisquellen sammeln
- Ereignisdaten durch zusätzliche Informationen anreichern (z. B. Kontext, Threat Intelligence)
- Gesammelte Daten analysieren und verdächtige Muster identifizieren und möglichst alles automatisieren
- Nicht nur «Logs», sondern auch Netzwerkverkehr (z. B. NetFlow), Meldungen von IDS, Meldungen von Externen etc.

Information Security Incident Management

- Zentrales Element der Arbeit des CSIRT
- Beinhaltet das, was wir aus den Incident Response Prozessen bereits gelernt haben
- Schwerpunkte im CSIRT Service Framework
  - *Vorfälle koordinieren*: Fluss und Weitergabe von Informationen zum Vorfall sicherstellen
  - *Krisenmanagement*: Unterstützung, wenn ein Vorfall zur Krise für die Organisation wird

Vulnerability Management

- Die hier erbrachten Dienste sind stark von der Organisation abhängig
- „Klassische“ Vulnerability Management
  - Schwachstellen entdecken (fortlaufend und/oder auch während einem Vorfall)
  - Schwachstellenberichte entgegennehmen & auf Schwachstellen reagieren
- Kann aber auch noch enthalten:
  - Bisher unbekannte Schwachstellen suchen
  - Mit involvierten Parteien koordinieren: Wissensaustausch, z. B. im Rahmen einer koordinierten Offenlegung von Schwachtellen
  - Informationen zum Vermeiden und Auffinden und Massnahmeempfehlungen

Situational Awareness

- Verstehen was in und um die Aktivitäten und Themen des CSIRT geschieht
  - Sowohl interne als auch externe Informationsquellen
  - Sowohl technische, organisatorische und weitere nicht-technische Informationen
- Beispiele
  - Übersicht aller (kritischen) Assets, dafür verantwortliche Personen/Rollen, deren normales Verhalten, Kritikalität für die Organisation etc.
  - Beobachtung relevanter Medien, anderer CSIRTs/PSIRTs, technologische Entwicklungen etc.
  - Beobachtung interner Veränderungen und organisatorischer Aktivitäten innerhalb der Organisation
  - Relevante Daten fürs Security Event Management sammeln
- Unterstützt andere CSIRT Services (Security Event Management, Incident Management, Knowledge Transfer)
- Kann auch eine Quelle zur Bewertung neuer / anstehender Gefahren dienen
- Kann auch juristische, politische, geopolitische Themen abdecken

Knowledge Transfer

- CSIRTs haben einen einmaligen Einblick in die Informationssicherheit
  - Beschäftigen sich im Normalfall mit der aktuellen Bedrohungslage
  - Haben Einblick in Angriffe gegen die Organisation
  - Tauschen sich mit anderen Organisationen/Teams aus und erhalten breiten Einblick in aktuelle Themen
  - Sind meistens gut vernetzt innerhalb der Organisation und haben einen vielseitigen Einblick
- All dies ist ideal für die Weitergabe dieses Wissens zur Steigerung der Informationssicherheit
  - Bewusstsein fürs Thema steigern (Awareness Training/Building)
  - Aus- und Weiterbildung für andere Teams anbieten (z. B. richtiges Verhalten im Ernstfall)
  - Übungen und Simulationen durchführen
  - Sich in Richtlinien, Prozessen, Projekten und anderen organisatorischen Aktivitäten einbringen

5 Digital Forensics

5.1 Definition

- Ein streng methodischer Ansatz zur Analyse von Daten
- Die Untersuchung folgt einem gerichtsfestem Ansatz
  - Die Integrität der Daten wird sichergestellt
  - Wissenschaftlich unvoreingenommene Analyse
  - Grundsätzlich sind geprüfte und akzeptierte Verfahren und Werkzeuge für die Sammlung, Aufbewahrung und Analyse im Einsatz
  - Die Ergebnisse müssen bei Bedarf durch Dritte nachvollzogen und reproduziert werden
- **Digitale Forensik ist die Sicherung, Aufbereitung und Analyse digitaler Spuren in einer Weise, die in einer späteren Gerichtsverhandlung akzeptiert wird**

5.2 Methoden

Live-Forensik

- Wird auf dem laufenden IT-System durchgeführt
- Flüchtige Daten können gesammelt werden
- Beweissicherung kann zu unerwünschten Änderungen am System führen
- Tool: KAPE

Dead-Forensik

- Wird auf dem ausgeschalteten IT-System durchgeführt
- Sammlung kann ohne Änderungen an den Daten vorgenommen werden

5.2.1 Live-Forensik (Online-Forensik oder Live Response)

- Untersuchung während der Laufzeit
- Erlaubt es flüchtige Daten zu sammeln und damit diese zu untersuchen
  - Inhalt des Arbeitsspeichers, Swap / Page Dateien
  - Informationen zu bestehenden Netzwerkverbindungen
  - Informationen zu gestarteten Prozessen
  - Informationen zu offene Dateien, Sockets, Pipes etc.
  - Angemeldete Nutzerkonten
- Damit kann der aktuelle Laufzeitzustand des Systems festgehalten und untersucht werden (z.B. Autoruns mit KAPE)
- Die Reihenfolge, in der Daten gesammelt werden, ist sehr wichtig!
  - Je flüchtiger die Daten sind, desto schneller müssen sie angesehen werden!!!
  - Je schneller sich Daten ändern bzw. durch Systemaktivitäten verändert werden, desto flüchtiger sind diese
- Daten werden in der Reihenfolge ihrer Flüchtigkeit gesammelt: Flüchtigste Daten zuerst
  1. Arbeitsspeicher
  2. „Auslagerungsdateien“: Swap / Page Datei(en)
  3. Netzwerkstatus, Netzwerkverbindungen (Caches nicht vergessen)

4. Laufende Prozesse
5. Offene Dateien
6. ...

5.2.2 Dead-Forensik

Berühre, verändere oder modifiziere niemals etwas, bevor es nicht dokumentiert, gekennzeichnet, vermessen und fotografiert ist.

- Untersuchung eines nicht aktiven Systems
- Untersuchung von Daten, die nach dem deaktivieren/ausschalten eines IT-Systems zur Verfügung stehen
  - Fokus auf die nicht-flüchtigen Datenträger
- Findet häufig nach einem Vorfall statt oder wenn dieser bereits lange her ist

5.3 Datensammlung

- Unabhängig von der Art der Datensammlung, müssen wir zuerst grundlegende Informationen festhalten (dokumentieren!)
  - Was wird gesammelt?, Von welchem System wird es gesammelt?
  - Von welchem Datenträger stammen die Daten?, Wer hat die Daten gesammelt?
  - Wann wurde die Datensammlung gestartet? Wann wurde sie abgeschlossen?
  - Was ist über das System bekannt? Systemzeit, Zeitzone des Systems etc.
  - Wie und mit welchen Werkzeugen wurden die Daten gesammelt?
- **Veränderung der Originaldaten muss zwingend vermieden werden!**
- **Bewehrte Werkzeuge und Vorgehen verwenden (forensically sound)**
- **Die präzise Dokumentation ist absolut zentral und notwendig**

5.3.1 Full Image

- Ein Datenträger wird vollständig kopiert (Kopie ist bitweise / sektorweise)
- Damit werden auch vom System nicht genutzte Speicherbereiche, gelöschte Dateien etc. mitkopiert
- Kann nicht mit Standardwerkzeugen üblicher Betriebssystem (Windows, macOS, Linux) durchgeführt werden

Beim erstellen eines Full Image einen *Write Blocker* dazwischen schliessen, dass alle Write-Befehle des Clients an die zu kopierende Festplatte geblockt werden. Damit kann gewährleistet werden, dass sich die Festplatte nicht während oder wegen dem kopieren ändert!

5.3.2 Memory Image

- Sicherung des Arbeitsspeichers
  - In alltagstauglichen Fällen nur bei Live-Forensik
- **Wichtig**: Werkzeug für die forensische Sicherung des Arbeitsspeichers nutzen
  - Sollte selbst minimalen Arbeitsspeicher einnehmen und soweit wie möglich keine Änderungen am System vornehmen
  - Tool: `volatility`

5.3.3 Triage Image (Triage-Forensik)

- Daten werden zielgerichtet gesammelt
  - Fokus auf typischerweise forensisch relevante Dateien
- Beispiele
  - Historie, Cache, Favoriten, Download-Historie, Cookies etc. von Browsern
  - Logdateien, Registry, Prefetch, Shimcache, Amcache
  - Gelöschte Dateien (Recycle Bin)
- Tool: *KAPE*

5.3.4 Prefetch

- `C:\Windows\Prefetch\`
- Proof of Execution
- Remains after deletion of the Executable
- Shows loaded DLLs (first 10 sec. of execution are logged)
- Goal is to reduce the start time of the application
- ist grundsätzlich auf Servern deaktiviert

5.3.5 Amcache

- `C:\Windows\AppCompat\Programs\`
- Registry-Hive
- records the recent processes that were run and lists the path of the files that's executed which can then be used to find the executed program.

5.3.6 Shimcache (AppCompatCache/ Application Compatability Cache)

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache`
- Provides compatibility for older software running in newer versions of Windows (backward compatibility)
- Executable file name, file path & timestamp are recorded (timestamp = last modification time)
- Stored in the SYSTEM registry hive
- Seit Win10 kann Shimcache nicht mehr genutzt werden um zu sagen, ob ein Programm ausgeführt wurde oder nicht!!
  - Aber es kann gezeigt werden, dass ein File einmal auf dem System existiert hat oder was über ein externes Laufwerk/ UNC-Pfad angesteuert wurde
- Only written on reboot or shutdown
- Shimcache can be used to show executable files present on, or accessed via a given system
- The Shimcache tracks metadata such as the full file path, last modified date, and file size but only contains the information prior to the system's last startup, as current entries are stored only in memory

6 Verhandlung mit Ransomware-Gruppen

6.1 Ablauf Ransomware

1. Kompromittierung
2. Diebstahl sensibler Daten
3. Daten verschlüsseln (1. Erpressung)
4. Mit Veröffentlichung der Daten drohen (2. Erpressung)
5. Optional: Öffentlich an den Pranger stellen
6. Optional: Androhung von DDoS-Angriffen (3. Erpressung)
7. Optional: Kunden/ Nutzer/ Mitarbeiter drohen (4. Erpressung)
8. Optional: Business Email Compromise (BEC), Phishing, etc.
9. Optional: Veröffentlichung gestohlener Daten

6.2 Grundlage für die Verhandlung

- Ransomware-Betreiber haben ein wirtschaftliches Interesse daran, sich an ihre Vereinbarung zu halten
- Unternehmen zahlen, weil sie wissen, dass sie mit hoher Wahrscheinlichkeit das erhalten, was versprochen wird
  - Typisches Argument betroffener Unternehmen für eine Zahlung
- Sie haben ein hohes Interesse daran, eine Zahlung zu leisten. Die Veröffentlichung hat einen geringen wirtschaftlichen Wert
- Sie üben Druck aus mit
  - der Drohung mit der Veröffentlichung
  - kurzen Zeitfenstern für Entscheidungen
  - Variationen im Kommunikationsstil

6.3 Sollen wir verhandeln?

- Meistens: Ja! Unabhängig vom Wunsch Geld zu bezahlen
  - **Vorsicht**: Veröffentlichung der Konversation könnte von der Öffentlichkeit missverstanden werden
- Ziele:
  - Alle Möglichkeiten offen halten
  - Zeit für den Aufbau der Verteidigung / der Schutzmassnahmen gewinnen

6.4 Verhandlung

- Festlegen, was man von der Gegenseite als Gegenleistung haben möchte
  - Was sind unsere Ziele?
- Maximalbetrag und Zielbetrag festlegen
  - Wenn man eine Cyberversicherung hat: Könnte ggf. von der Cyberversicherung gedeckt sein
- Sich stets die Zeit nehmen eine Nachricht zu verarbeiten und darauf zu antworten
- Wenn möglich mit Bitcoins bezahlen
  - Ist für die Strafverfolgung einfacher zu verfolgen

- Juristen sollten involviert werden
  - Gewisse Ransomware-Gruppen sind sanktioniert und es kann zu zusätzlichen negativen Folgen kommen

6.5 Grundlagen für Verhandlung

- Der Preis ist verhandelbar! Grundsätzlich und durch Argumente, wie zum Beispiel:
  - Unternehmensgrösse wurde falsch eingeschätzt
  - Umsatz/Gewinn wurde falsch bewertet
  - Aktuelle ökonomische Situation bzw. Prognosen für die Zukunft
- Wir spielen grundsätzlich immer auch auf Zeit
  - Verteidigung ausbauen
  - Was wenn der Angreifer noch Zugang hat und wir haben diesen noch nicht entdeckt und entfernt?
  - Teilzahlungen machen und bei jeder eine Gegenleistung verlangen
- Ideen, was man als Gegenleistung verlangen kann:
  - Entschlüsselung einer oder mehrerer Dateien als Fähigkeitsnachweis
  - Entschlüsselungsprogramm
  - Bericht, in dem beschrieben wird, wie sie eingedrungen sind, wie und wo sie sich eingenistet haben, was sie ausgenutzt haben usw.
  - Anweisungen zum Entfernen der Schadsoftware
  - Nachweis der gestohlenen Daten (z. B. Verzeichnisliste)
  - Beweis für die Löschung von Daten

6.6 Beispiele

→ siehe Vorlesung Folien 17 - 47.

7 Incident Response Fallbeispiele

7.1 Vorgehen wissenschaftliche Methode

1. Beobachtung/ Fragestellung
   - Vorfall liegt vor
2. Daten sammeln
   - Fortlaufendes Sammeln von Informationen zum Vorfall
3. Hypothese aufstellen
4. Sofortmassnahmen aus Hypothesen ableiten und umsetzen
5. Hypothese prüfen/ testen
   - Durch Incident Response, digitale Forensik, Threat Hunting, Vulnerability Management etc. Hypothese belegen oder wiederlegen
6. Belegt oder wiederlegt die Prüfung/ der Test die Hypothese?
   - Zusätzliche Massnahmen ableiten und umsetzten
7. Zurück zu Schritt 2

“

7.2 Hyptohesen, die wir stets annehmen

- Angreifer haben trotz aller Massnahmen immer noch Software in der Organisation für den Fernzugriff / die Fernkontrolle
- Angreifer setzen nicht nur selbst eingebrachte Software ein, sondern auch die bereits in der Organisation vorhandene
  - Nutzerkonten kompromittiert oder neue angelegt
  - Fernwartungswerkzeuge werden mitverwendet (Teamviewer, Anydesk etc.)
- Angreifer haben Daten eingesehen / entwendet
- Angreifer „hören und „sehen“ uns zu
  - Es muss immer damit gerechnet werden, dass die Angreifer die Kommunikation mitlesen können → z.B. Angreifer klinken sich ins MS-Teams des Incident Response Team ein und bekommen so alle Entdeckungen und weitere Massnahmen mit

7.3 Allgemeingültiges

7.3.1 (Technische) Ziele während der Bewältigung

- Angreifern den Zugriff in die Organisation sperren
  - Organisation vom Internet trennen
  - Strikte Netzwerksegmentierung implementieren und die Kommunikation zwischen diesen unterbinden
  - Bekannte Command & Control (C2) Adressen blockieren
- Angreifern die Möglichkeit nehmen auf Massnahmen zu reagieren
- Präsenz des Angreifers aus der Organisation entfernen
  - Infizierte Systeme vom Netzwerk trennen
  - Zugriff auf kompromittierte Nutzerkonten sperren

- Die Fähigkeit des Angreifers schwächen zurückzukehren
  - Zugriff auf Administratorkonten einschränken
- Es gibt keine Patentlösung und perfekte Reihenfolge
- Das Vorgehen und die Entscheidungen sind komplett vom vorhandenen Wissen abhängig
- Massnahmen müssen geplant, umgesetzt und überprüft/validiert werden
- Falls Netzwerk offline genommen wird, muss dies überprüft werden
  - an einem Client ein ping durchführen um zu überprüfen, dass wirklich keine Verbindung mehr vorhanden ist
  - Angreifer können so oft nciht mehr machen und mithören/ mitsehen und die Incident Responder haben für die Analyse mehr Zeit
  - kann je nach Unternehmen aber nicht komplett offline genommen werden

7.4 Wo fangen wir an

7.4.1 Ausgangspunkte

E-Mail

- Empfang einer unerwünschten E-Mail, z. B. Spam, Phishing, Malspam etc.
- E-Mail-Header
  - E-Mail-Adresse des Absenders, Quell-Server
  - SPF, DKIM und weitere Security-Header mit wertvollen Hinweisen
- Inhalt der E-Mail: Hyperlinks, Quelltext, Dateianhänge

Antimalware-Meldung

- Name der Schadsoftware bzw. der Detektionssignatur oder des -grundes
- Ort des Fundes (Dateipfad der Schadsoftware, Prozess, Netzwerkkommunikation)
- Hashes (Datei-Hash, Hashes bestimmter Teile der Datei (z. B. des PE Import Headers), Hashes für FuzzyMatching,)
- Zeitpunkt der Entdeckung oder Ausführung
- Aktivitäten vor/nach der Ausführung bzw. Entdeckung (EDR-Produkte)

Netzwerk IDS/ IPS

- Zieladresse
- Quelladresse / Quellsystem
- Kategorie der Zieladresse bzw. Grund fürs Detektieren/Blockieren
- Zeitpunkt des Verbindungsversuchs

Ransomware/ Wiper

- Neue Dateiendung der Dateien
- Ransom Note / Statement

Weitere Ausgangspunkte

- Öffentliche Angriffsfläche auf offensichtliche Schwachstellen prüfen
- Social Engineering
- Partnerorganisationen
  - Sind andere Organisationen mit Vertrauensbeziehung zu unserer von einem Angriff betroffen?
  - Site-to-Site VPN, Active Directory Trust, Fernzugriff (Teamviewer, Anydesk, persönlicher VPN etc.)
- Kompromittierte Nutzerkonten
  - Auffällige Anmeldungen (Ort, Uhrzeit, Software) suchen
  - Hinweise auf Angriffe gegen Nutzerkonten (Brute-Force-Angriffe, Password Stuffing etc.)
  - Datenlecks prüfen: Havhaveibeenpwned.com, Threat Intelligence Plattformen
- Schadsoftware
  - Gibt es Meldungen von AV-SW oder von IDS?
  - Systeme mit Full-Scan prüfen

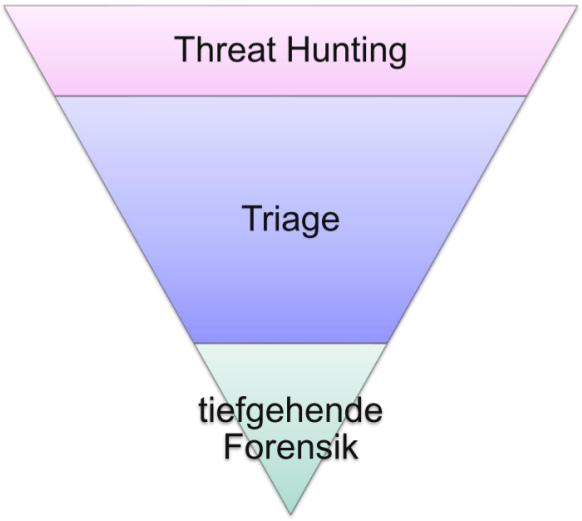
7.5 Indizien finden (Windows Umgebung)

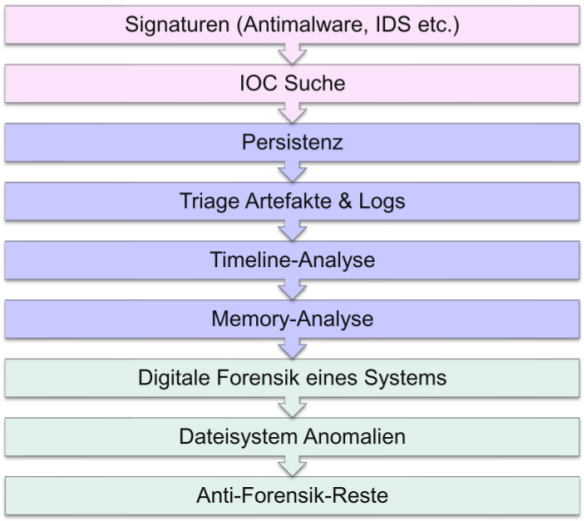
7.5.1 Malware Paradox

All rootkits obey two basic principles:

1. They want to remain hidden
2. They need to run

7.5.2 Suchmethoden





- Threat Hunting
  - Suche über die gesamte Organisation
  - Automatisierbar und skaliert gut
- Triage
  - Für gefundene Systeme aus der organisationsweiten Suche

  - Prüfung auf typische Hinweise
  - Benötigt häufig hohen manuellen Aufwand
- tiefgehende Forensik (Red Poster)
  - Für Systeme, die klare Hinweise auf Kompromittierung/Infektion aufweisen
  - Sehr zeitintensiv, Vorsicht!

7.5.3 Angreifer versuchen nicht aufzufallen

- Schadsoftware nutzt gerne unauffällige Dateipfade oder Elemente davon
  - `\Users\%Username%\AppData\Local\Microsoft\ Windows\Temporary Internet Files`
  - `Temp\`
- Immer Dateipfade der Prozesse überprüfen → Temp Ordner deuten tendenziell auf einen Schadprozess hin
- Auf ähnliche Schreibweise aufpassen
  - `winlogon` → `wimlogom, win1ogo, winIogon, winiogon, winl0gon`
  - `lsass` → `isass, laass, lamss, lass, isass, Isass`

7.5.4 Interesse von Lateral Movement bei IncResp

- Was wurde infiziert/ ist betroffen
- Auf was hat er sich fokussiert (oft Tendenz Richtung DC)?
- Was hat er schon erreicht (z.B. Rechte)
- Wie hat er sich verbreitet? → IOCs/ Massnahmen

7.6 Triage-Akquisition

7.6.1 Standardprozess pro System

1. Arbeitsspeicher sichern
2. Auf Festplattenverschlüsselung prüfen (*edd.exe*)
3. Triage Image erstellen (*KAPE*)
4. Analyse des Triage Image
   - Vom Artefakt abhängige Analyse durchführen
5. Festplatten-Image erstellen
   - Im Normalfall Full-Image erstellen
   - Alternative, falls das System läuft: Logisches Image, zum Beispiel mit FTK Imager

7.6.2 1. Arbeitsspeicher sichern

- Während das System noch läuft:
- Wenn System nicht mehr läuft:
  - Hibernation-Datei: `%SystemDrive%\hiberfil.sys`
  - Page-Dateien: `%SystemDrive%\pagefile.sys`
  - Memory Dump (Crash Dumps): `%WINDIR%\MEMORY.DMP` und `%WINDIR%\Minidump\*.dmp`

7.6.3 2. Sind Festplatten verschlüsselt?

- Typisches Werkzeug: `edd.exe`
  - Organisationen sollten wissen, ob sie ihre Festplatten verschlüsseln
  - Vorsicht, hat der Nutzer oder die Nutzerin vielleicht zusätzliche Laufwerke erstellt oder im Einsatz?
- Falls verschlüsselt
  - Ist der Schlüssel bekannt? → Wenn ja, notieren
  - Falls der Schlüssel nicht bekannt ist und System noch läuft → Logisches Disk Image erstellen

7.6.4 3. Triage Image

- Vor dem Sammeln entscheiden, was gesammelt werden sollte
  - Ausführung von KAPE hinterlässt selbst Spuren
  - KAPE Modules starten zusätzliche Applikationen → dies kann zum Verwischen von wertvollen Spuren führen!

7.7 NTFS

7.7.1 Wichtige NTFS-Merkmale

- Journaling (NTFS nennt es *Transaction Logging*, `$LogFile`)
  - Protokolliert Änderungen an den Metadaten
  - Tracks detailed, low-level transactional changes for NTFS
  - Provides file system integrity and resilience (records actual data that changed)
- USN Journal / Change Journal (`$Extend\$UsnJrnl`)
  - Protokolliert Änderungen an Ordnern und Dateien
  - Nützlich für Antivirus- und Backupsoftware
  - Tracks high-level changes
- Access Control Lists
- Volume Shadow Copy
- Alternate Data Streams (ADS)
  - Es können mehrere Data Streams mit einem Dateinamen in Verbindung gebracht werden
  - Schadsoftware kann sich in diesen verstecken
- Verschlüsselung (Encrypting File System, EFS)
  - Nicht das gleiche wie BitLocker!
  - EFS verschlüsselt einzelne Dateien, BitLocker gesamtes Laufwerk
  - BitLocker ist unabhängig vom Nutzerkonto, EFS verschlüsselt basierend auf dem Nutzerkonto

7.7.2 Master File Table (MFT), $MFT

- Strukturiertes Array / „Datenbank“ aller NTFS-Objekte
- Erste Einträge sind vordefiniert und für NTFS-Metadateien reserviert (Alle `$<Files>`)
- Jede Datei hat mindestens einen Eintrag in der MFT mit diversen Attributen, die gespeichert werden. Unter anderem
  - Grösse, Zeitstempel (`$STANDARD_INFORMATION`), Berechtigungen
  - Jede Datei/ Objekt haben Informationen wie Grösse, Timestamp und Berechtigungen Standard-mässig vorhanden

7.7.3 NTFS-Metadateien

Übersicht, welche Dateien uns helfen einen Angreifer zu finden!

MFT index	Filename	Description
0	$MFT	Master File Table
1	$MFTMirr	Back up of the first 4 entries of the Master File Table
2	$LogFile	Metadata transaction journal
3	$Volume	Volume information
4	$AttrDef	MFT entry attribute definitions
5	.	Root directory
6	$Bitmap	Cluster block allocation bitmap
7	$Boot	Boot record (or boot code)
8	$BadClus	Bad clusters

MFT index	Filename	Description
9	$Quota	Quota information Last used in NTFS version 1.2
9	$Secure	Security and access control information Introduced in NTFS version 3.0
10	$UpCase	Table of uppercase characters used for ensuring case insensitivity in Windows and DOS name spaces.
11	$Extend	A directory containing extended metadata files
12-15		Unknown (Reserved) Marked as in use but empty
16-23		Unused Marked as unused
...	...	...

7.7.4 Volume Shadow Copy (VSC), Volume Shadow Volumes, Volume Snapshot Service / Volume Shadow Copy Service (VSS)

- NTFS-Funktion für Backups auf Block-/Cluster-Ebene
- Wird manuell oder automatisch erstellt
- Für DFIR-Untersuchungen sehr interessant
  - Kann vermeintlich gelöschtes wiederherstellbar machen
  - Kann einen weiteren Blick in die Vergangenheit erlauben (Logs, Prefetch, LNKs etc.)
- Oft gehen die VSS vergessen

7.8 Windows Registry

7.8.1 Registry Hives

Ein Hive in der Windows-Registry ist die Bezeichnung für einen Hauptbereich der Registry, der Informationen als Key-Value-Pair enthält.
Alle Schlüssel, die als Hives gelten, beginnen mit *HKEY* und befinden sich an der Registry-Root.

7.8.2 Security Accounts Manager (SAM)

- SAM Hive gibt uns Informationen zu lokalen Nutzerkonten
  - wenn Nutzerkonten Teil einer Windows Domäne sind, dann sind die Informationen zu den Nutzerkonten auf den Domain-Controller-Systemen
- DFIR-Relevanz:
  - Nutzername zum Relative Identifier (RID, letzter Teil vom SID) identifizieren
  - Nutzerverhalten aus erfolgreichen und fehlgeschlagenen Anmeldeversuchen ableiten
  - Vorsicht: Bei Microsoft Nutzerkonen (SaaS/Cloud) werden die Counter nicht genutzt
  - Diverse Zeitstempel für Korrelation und Identifikation potenziell verdächtiger Nutzerkonten

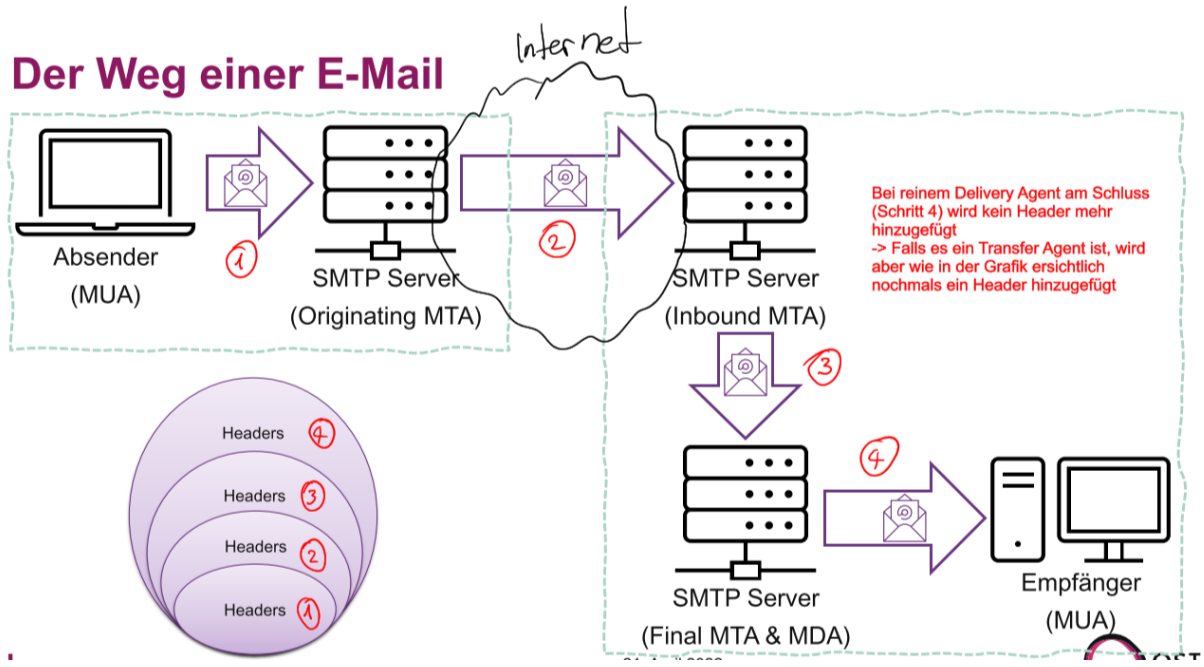
7.8.3 Zeitzone

- Bei jedem Zeitstempel müssen wir die Zeitzone kennen
- Wenn möglich immer mit **UTC** arbeiten
- Gewisse Logs und Dateisystem (z. B. FAT) nutzen die lokal eingestellte Zeitzone

7.9 E-Mail Analyse

7.9.1 E-Mail Header

- **Wichtig**: Der Grossteil der E-Mail-Header lassen sich fälschen!
  - Einzig dem letzten E-Mail-Server, unserem eigenen, können wir (hoffentlich) vertrauen und damit den von ihm eingefügten Header
- Jeder Mailserver der die E-Mail passiert fügt im Normalfall Header hinzu (ganz oben)
- MTA: Mail Transfer Agent ist zuständig für das entgegennehmen und senden von E-Mails
  - MUA: Mail User Agent ist die Software zur Bearbeitung von E-Mails (E-Mail-Client)
  - MDA: Mail Delivery Agent ist zuständig für die Bereitstellung der E-Mails an den MUA verantwortlich
  - MTA $\leftrightarrow$ MTA, MTA $\rightarrow$ MDA und MUA $\rightarrow$ MTA meist über SMTP
  - MDA $\rightarrow$ MUA meist IMAP (früher POP)



7.9.2 Typische Header-Felder

- **Message-ID**: [Eindeutige ID]@[Originating MTA]
  - Eindeutige Identifikation für die E-Mail
  - Erlaubt beispielsweise die Suche nach Protokollereignissen im Zusammenhang mit der E-Mail
- **Received**
  - Erlaubt es den Weg des E-Mails zu verfolgen (von unten nach oben)
  - Der unterste Eintrag ist der Originating MTA und der oberste Eintrag ist der Final MTA

  - Jeder MTA fügt im Normalfall die eigene *IP-Adresse*, seinen eigenen *Namen*, die *Quell-IPAdresse*, den Namen des *Quellsystems* und den *Empfangszeitpunkt inkl. Zeitzone* hinzu

- **X-Originating-IP, X-IP, X-Forwarded-For**
  - Kann existieren und die IP-Adresse des Absenders (MUA) enthalten
  - Müssen dafür dem Originating MTA vertrauen
  - Immer seltener vorhanden zum Schutz der Privatsphäre bzw. wegen Datenschutzbedenken

7.9.3 SPF (Sender Policy Framework)

Mit *SPF* können Absender festlegen, welche IP-Adressen E-Mails für eine bestimmte Domäne senden dürfen. DNS TXT-Entry mit allen IP-Ranges, von welchen ein Mail mit dieser Domain verschickt werden darf. Alles was nicht von den outgoing Mail/MX Servern stammt, ist "Fake"und wird in Spam verschoben oder gar nicht erst zugestellt.

SPF ist besonders effizient gegen **Phishing-Angriffe** & erlaubt es dem Empfänger gefälschte Absender festzustellen.

7.9.4 Ablauf

Auf dem **DNS** kann eingegrenzt werden, wer (welche IP) alles ein Mail verschicken darf.

- MTA macht **DNS-Lookup** und fragt diesen an, welche IPs berechtig sind Mails zu versenden.
  - IP-α (TCP) $\rightarrow$ DNS-Lookup $\rightarrow$ SPF@ost.ch
  - Falls α darin enthalten $\rightarrow$ ok

Wenn Empfänger SPF-Policy nicht enforced, ist egal was der Sender konfiguriert hat. Empfänger-MTA interessiert das nicht.

7.9.5 DKIM (DomainKeys Identified Mail)

DKIM stellt einen Encryption Key und eine digitale Signatur bereit, die nachweisen, dass eine E-Mail-Nachricht nicht gefälscht oder verändert wurde. DKIM fügt dazu dem E-Mail Header eine digitale Signatur hinzu, welche vom Empfänger mit dem *Public Key* (welcher auf dem DNS Server gespeichert ist) validiert werden kann.

Der Mail-Server hat ein Public/Private Key Cert Pair. Der Public Key wird via weltweit verfügbaren DNS veröffentlicht. Der Plaintext in einem Mail wird gehasht und im Header gespeichert. Der Header wird wieder mit dem Private Key signiert (also inkl. dem Hash des Plain Texts). Empfänger Mail-Server kann nun mit dem öffentlich verfügbaren Public Key feststellen, ob der Sender der ist der er angibt (Korrekte Firma mit Zugriff auf Private/Public Pair). Durch das Signieren ist auch klar, dass der Content "in Transit" nicht verändert wurde.

DKIM ist besonders effizient gegen **Man-in-the-middle-Angriffen**.

7.9.6 Ablauf

- Mailserver signiert Mail mit private Key
- Mail kommt beim MTA an und dieser prüft ob Mail signiert ist
  - Wenn Signatur vorhanden $\rightarrow$ **DNS-lookup** für public key $\rightarrow$ prüft Signatur von Mail mit dem public key des **DNS Servers**

Canonicalization

- Während dem Transport werden E-Mails verändert
- Canonicalization normalisiert die E-Mail mit dem Ziel, dass Änderungen während dem Transport keinen negativen Effekt au haben

DFIR

- Indikator, dass bestimmte Header-Felder und/oder E-Mail-Inhalt nicht verändert wurden zwischen dem MTA des Absenders (Absender vertraut diesem) und unserem MTA (wir vertrauen diesem).
- `Authentication-Results` ist das Resultat der Signaturprüfung durch den MTA auf der Empfangsseite. Enthält im `header.b` die ersten 8 Bytes der Signatur

7.9.7 (Versteckte) Zeitstempel in E-Mails

- Offensichtliche Zeitstempel: `X-Received, Received, Date`
- Abweichung von Zeit → Indicator
  - Könnte aber auch sein, dass Admin Zeit falsch eingestellt oder Server geografisch verschoben wurde (ohne Zeit anzupassen) und kein NTP Server konfiguriert ist
- Weniger offensichtlich: Unix Timestamps können an diversen Orten versteckt sein

7.10 Windows Event Logs

7.10.1 Security Log

- **Wichtigstes** Log bei DFIR-Analysen
- Nur der LSASS-Prozess darf in diesen schreiben (Nur Admins können diese sehen)
- Logeinträge werden durch die Audit Policy gesteuert (können spezifisch für einzelne Benutzerkonten eingestellt werden)
- Details zu Authentifizierung, Nutzerverhalten, Zugriff auf Ressourcen (Dateien, Ordner, Netzwerklaufwerke/-ordner), Änderungen an gewissen Einstellungen etc.

7.10.2 Nutzerkontonutzung

- **Anmeldeversuche überwachen/ Audit account logon events**
  - Bestimmt, ob jede Instanz eines Benutzers überwacht werden soll, der sich bei einem anderen Gerät anmeldet oder sich von einem anderen Gerät abmeldet, auf dem dieses Gerät zum Überprüfen des Kontos verwendet wird.
  - Anmelde-/Abmeldeereignisse, die auf dem untersuchten System authentifiziert werden.
  - Es ist aber nicht (zwingend) das System an dem sich eine Person anmeldet.
- **Anmeldeereignisse überwachen/ Audit logon events**
  - Bestimmt, ob jede Instanz eines Benutzers überwacht werden soll, der sich bei einem Gerät anmeldet oder sich von einem Gerät abmeldet.
  - Anmelde-/Abmeldeereignisse, die auf dem System selbst stattfinden

7.10.3 Logon Type

Anmeldetyp	Anmeldetitel	Beschreibung
0	System	Wird nur vom Systemkonto verwendet, z. B. beim Systemstart.
2	**Interactive**	**Ein Benutzer, der sich bei diesem Computer angemeldet hat.**
3	**Network**	**Ein Benutzer oder Computer, der über das Netzwerk bei diesem Computer angemeldet ist.**
4	**Batch**	**Der Batchanmeldetyp wird von Batchservern verwendet, auf denen Prozesse im Namen eines Benutzers ohne direktes Eingreifen ausgeführt werden können.**
5	**Service**	**Ein Dienst wurde vom Dienststeuerungs-Manager gestartet.**
7	Unlock	Diese Arbeitsstation wurde entsperrt.
8	NetworkCleartext	Ein Benutzer, der sich über das Netzwerk bei diesem Computer angemeldet hat. Das Kennwort des Benutzers wurde an das Authentifizierungspaket in seinem nicht gesicherten Formular übergeben. Die integrierte Authentifizierung verpackt alle Hashanmeldeinformationen, bevor sie über das Netzwerk gesendet werden. Die Anmeldeinformationen durchlaufen das Netzwerk nicht im Klartext (auch als Klartext bezeichnet).
9	NewCredentials	Ein Aufrufer hat sein aktuelles Token geklont und neue Anmeldeinformationen für ausgehende Verbindungen angegeben. Die neue Anmeldesitzung hat die gleiche lokale Identität, verwendet jedoch unterschiedliche Anmeldeinformationen für andere Netzwerkverbindungen.
10	**RemoteInteractive**	**Ein Benutzer, der sich remote über Terminaldienste oder Remotedesktop bei diesem Computer angemeldet hat.**
11	CachedInteractive	Ein Benutzer hat sich auf diesem Computer mit Netzwerkanmeldeinformationen angemeldet, die lokal auf dem Computer gespeichert wurden. Der Domänencontroller wurde nicht kontaktiert, um die Anmeldeinformationen zu überprüfen.
12	CachedRemoteInteractive	Identisch mit RemoteInteractive. Dies wird für die interne Überwachung verwendet.
13	CachedUnlock	Arbeitsstationsanmeldung.

7.10.4 Anmeldesitzung nachverfolgen

Je nach dem wie viele Tätigkeiten während der aktiven Sitzung ausgeführt wurden kann auf eine Automatisation geschlossen werden oder nicht.
→ Duzende Tätigkeiten (Service installiert, Scheduled Task erstellt, etc.) in 3 Min → Automation

7.11 Browser

Fragen

- Welche Webseite wurde besucht?
- Wie häufig wurde die Webseite besucht?
- Wann wurde eine Webseite besucht?
- Welche Webseiten hat sich der Nutzer/die Nutzerin gemerkt?
- Was wurde heruntergeladen?
- Welche Nutzerkonten wurden online verwendet?
- Nach was wurde gesucht?

Artefakte zur Beantwortung

- Browser-Verlauf
- Cache
- Cookies
- Sitzungswiederherstellung
- Autovervollständigung
- Favoriten
- Download-Historie
- (Sync-)Einstellungen

7.11.1 In die Tiefen der Browser steigen

- Für tiefgehende Analysen fehlt häufig die Zeit (abhängig von Browser + sehr viele Informationen fürs Auswerten)
- Im IR setzen wir häufig auf alternative Quellen für Hinweise:
  - Logs (DNS, FW, AV)
  - Dateien im Downloads-Ordner oder Papierkorb des Systems
  - E-Mail-Server (E-Mail häufig der Ausgangspunkt einer unerwünschten Browser-Nutzung)

8 Dokumentation

8.1 Gründe für Dokumentation

- Fortlaufend den Überblick behalten
- Entscheidungsfindung ermöglichen und unterstützen
- Lessons Learned ermöglichen
  - Was ist passiert?
  - Wer war wie und wann involviert?
  - Was wurde herausgefunden/festgestellt?
  - Welche Massnahmen wurden aus welchem Grund und wann umgesetzt?
  - Was kann man in Zukunft verbessern?

8.2 Während dem Vorfall

- Generell immer:
  - Zeitstempel des Zeitpunkts als es festgestellt/gefunden/dokumentiert wurde
  - Zeitstempel des Ereignisses selbst (wann hat es stattgefunden?)
  - Person, Ort des Fundes (System, Pfad, IP-Adressen etc.)
- Welche Systeme sind involviert?
  - Hostname, IP-Adresse, relevante Ereignisse
- Was wurde wo gemacht?
- Aufgabenübersicht
  - Was wurde wann durch wen gemacht?
  - Was ist in welchem Durchführungszustand?
  - Priorisierung
  - Warum wurde die Aufgabe aufgenommen? Was ist der Hintergrund/Kontext?

8.3 Nach dem Vorfall

Einführung

- Beschreibung des Vorfalls auf hoher Ebene
- Einstufung / Kategorisierung des Vorfalls
- Zeitlicher Ablauf (auf organisatorischer Ebene)
- Involvierte Personen und deren Rollen / Aufgaben (Projektorganisation)
- Hypothesen oder zu beantwortende Fragen

Lösungsansatz/ Arbeitsweise/ Vorgehen

- Allgemeine Beschreibung des Incident-Response-Prozesses
- Eingesetzte Werkzeuge

Incident Response

- Übersicht der Massnahmen und deren Status (z. B. geplant, erledigt, abgelehnt)
- Verlauf des Informationssicherheitsvorfalls
  - Wann haben welche Personen welche Entscheidungen getroffen auf Basis welcher Informationen?
  - Was wurde als die nächsten Schritte festgelegt
- Details

IT-Forenische Analyse

- Übersicht: Kernereignisse als Ablauf / Zeitstrahl mit Zeitstempel (UTC), Ereignisbeschreibung und Verweis zu den Details
- Übersicht untersuchter Systeme
- Pro Werkzeug, Untersuchungsschritt, Asset und/oder Artefakt die Untersuchung im Detail beschreiben
- Pro Angriffsschritt die Feststellungen dokumentieren

Fazit

- Hypothesen belegen/wiederlegen basierend auf den gesammelten und analysierten Artefakten
- Fragen beantworten
- Empfehlungen für die Zukunft (Lessons Learned)

Anhang

- Hashes (Aller Images & untersuchten Dateien)
- IOCs (Kurzbeschreibung des IOC + Verweis auf relevantes Detailkapitel)
- Screenshots & Fotos
- Kopie relevanter Formulare

8.4 Häufige Fehler und Misskommunikation

- Zeitstempel ohne Kontext
  - Auf was bezieht sich der Zeitstempel? Was ist zu diesem Zeitpunkt passiert?
- Zeitstempel ohne Zeitzone
- Vermischung von Analyseresultaten und deren Interpretation
  - Resultat einer (forensischen) Untersuchung eines Artefakt sind für sich alleine objektiv zu beschreiben
  - Aussagekraft kann durch Kombination zusammenhängender Artefakte gesteigert werden
  - Was wurde auf einem System ausgeführt, welche Hinweise wurden entdeckt, etc.
  - Interpretation der Resultate im Kontext des Vorfalls / Angriffs klar vom Rest trennen und mit Wahrscheinlichkeiten arbeiten
  - Im Normalfall gibt es immer mehrere Erklärungen für ein Resultat!

9 Darknet

9.1 Begriffe

Clear Web/ Surface Web

- Klassisches Internet
- kann von Suchmaschinen indexiert werden

Deep Web

- zuerst Authorisierung notwenig
- kann deshalb von Suchmaschinen nicht indexiert werden
- macht den grössten Teil aus

Darkweb/ Darknet

- Jedes Darknet nutzt einen eigenen Kommunikationsstandard
- Darknet spezifische Software notwendig
- Kann im Normalfall nicht auf einfache Weise indexiert werden
- Bekanntestes Darknet: Tor-Netzwerk

9.2 Tor-Netzwerk

- Nutzt im Normalfall das Internet als Kommunikations-Infrastruktur
  - Tor ist ein *Overlay-Netzwerk*
- Primäres Ziel: Anonymisierung von Verbindungsdaten
  - Kommunikation ist sehr schwer zu überwachen
  - Quelle und Ziel einer Verbindung schwer zu überwachen

10 Incident Response Szenarien

→ siehe Folien „Thema 12 - IR-Szenarien“

10.1 How ro React (Cookbook)

10.1.1 Incident Type

- Phishing (Vishing, Spear Phishing, Whaling etc.)
- Business E-Mail Compromise (BEC)
- Credential Phishing
- Malware Spam (Malspam)

10.1.2 First Response

- Lock user account
- Ask for more details (any clues, out of the ordinary)
- Asses magnitude of the incident (more victims?)
- Raise loglevel
- Check logs on *IDS/ IPS/ EDR/ XDR/ FW/ SIEM* etc.
- Malware scan on machine
- Isolate systems

10.1.3 Further Steps

- Determine entrypoint
- Fix Security issues
- Setup fresh system
- reactivate user accounts
- Determine if data was stolen → NCSC / Data protection Officer
- Modify policies if necessary
- Compare hashes of malware with file