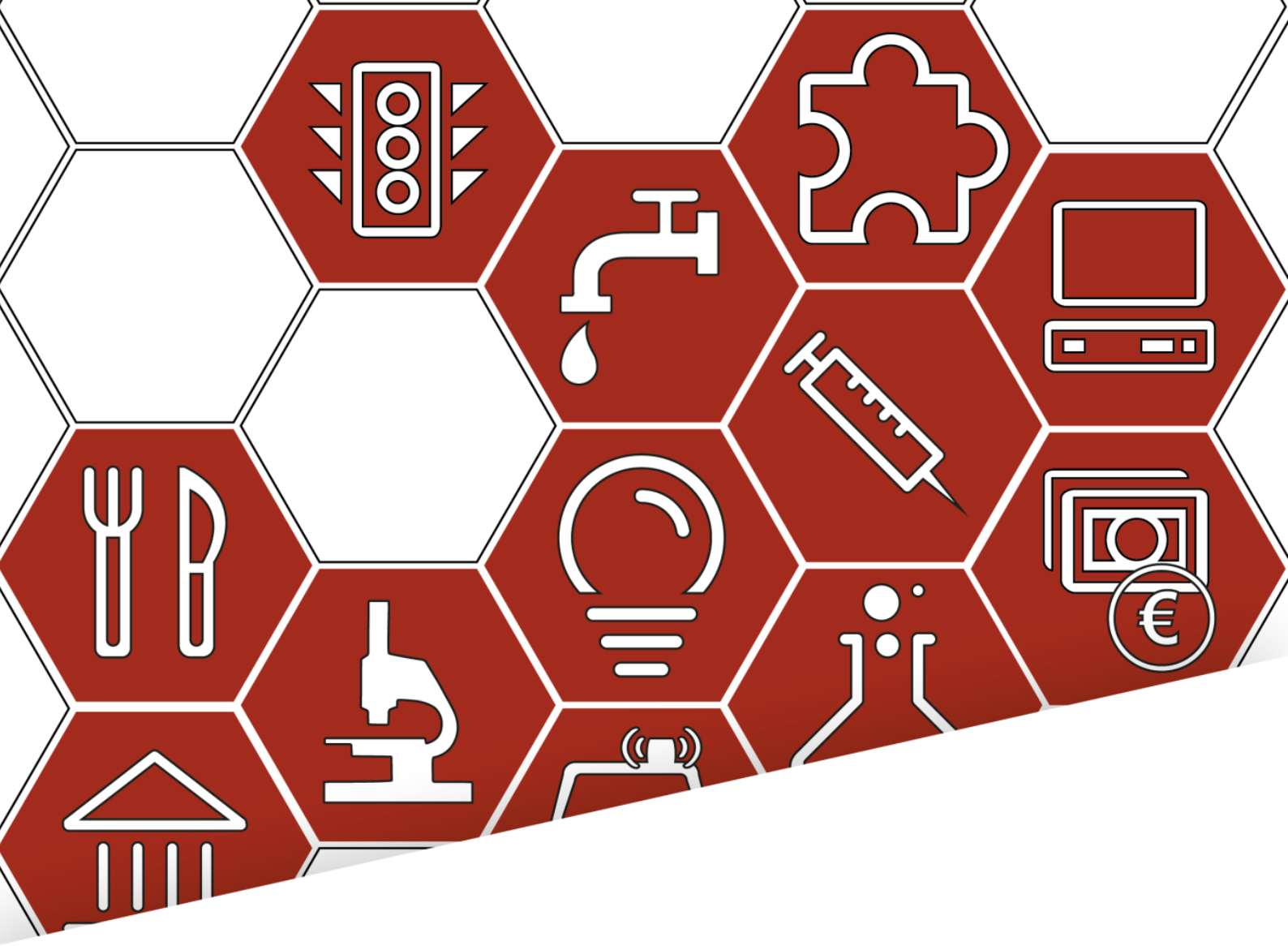

CSC-Schriftreihe 04/2018

Logdaten und Incident Response

Sammlung, Analyse & Weiterverarbeitung

Vorbereitungen auf und Empfehlungen für den Anlassfall

BM.I
REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNERES
BUNDESAMT FÜR VERFASSUNGSSCHUTZ UND TERRORISMUSBEKÄMPFUNG

IMPRESSUM

Medieninhaber/Herausgeber:
Bundesamt für Verfassungsschutz und Terrorismusbekämpfung,
Herrengasse 7, 1010 Wien

Herstellung:
Digitalprintcenter des BMI

CYBER SECURITY .BVT
Dieses Projekt wird durch den Fonds für die Innere Sicherheit kofinanziert.

Inhalt

1. Hintergründe 5
2. Anwendungsbereich 6
3. Vorbereitungen 6
3.1. Datensammlung 7
3.1.1 Netzwerk-und Host-basierte Logs 7
3.1.2 Applikations- und Datenbanklogs 10
3.2. Datenanalyse 10
3.3. Personal 11
4. Im Anlassfall 12
4.1. Auf KEINEN Fall 13
4.2. Auf JEDEN Fall 14
5. Behördenkontakt 15

1. Hintergründe

Seit mehreren Jahren kann ein stetiger Anstieg ideologisch und/oder monetär motivierter Cyber-Angriffe unterschiedlichster Ausprägungsarten beobachtet werden, z.B.:

- **APT** (Advanced Persistent Threats): Hierbei handelt es sich um komplexe, zielgerichtete und aufwändige Angriffe (Unternehmen, Behörden, Institutionen etc.).
- **DoS** (Denial of Service) und **DDoS** (Distributed Denial of Service)[1]
- Beabsichtigte **Datenexfiltration** oder versehentliche **Datenleaks**

Durch die generelle Zunahme computerbasierter Straftaten und Angriffe wird eine effektive und effiziente **Strafverfolgung**, bzw. **Ermittlung der Täter** immer wichtiger**.** Dies gilt sowohl für Fälle, in denen computerbasierte Systeme als Angriffsmittel verwendet werden, als auch für solche, in denen die Systeme selbst das Angriffsziel sind.

Aufgaben forensischer Untersuchungen sind in diesem Zusammenhang der Nachweis digitaler Straftaten (z.B. durch Analyse digitaler Spuren), daraus folgende **Ermittlungen** und die **Nachvollziehbarkeit** von Cyber-Angriffen und deren Auswirkungen, um **effektivere Gegenmaßnahmen** einzuleiten.

Bei der Analyse eines Sicherheitsvorfalls spielen die **vorhandenen Logdaten** eine **zentrale Rolle**. Da diese meist unweigerlich auch personenbezogene Daten beinhalten, kommen hier auch das österreichische Datenschutzgesetz bzw. die Datenschutzgrundverordnung zur Anwendung. Dies erfordert unter anderem eine Einschränkung auf für die Sicherheit bzw. für die Analyse von potentiellen Vorfällen relevanten Daten, als auch ein entsprechendes Sicherungskonzept für Logdaten, um diese vor unbefugtem Zugriff oder Manipulation zu schützen.

Das **Ziel** einer **forensischen Untersuchung** ist die Beantwortung folgendender Fragestellungen: **Was** ist geschehen? **Wo** ist es passiert? **Wann** ist es passiert? **Wie** ist es passiert? Die Beantwortung ebendieser Fragen kann durch zwei Vorgehensweisen ermöglicht werden: (1) der **Post-Mortem** oder (2) der **Live-Response** Analyse.

Bei einer Post-Mortem Analyse handelt es sich um eine Analyse eines ausgeschalteten Systems, bei der digitale Spuren auf einem forensischen Duplikat[2] analysiert werden. Aussagen über den Zustand des Systems zur Laufzeit sind jedoch kaum möglich, da flüchtige Daten durch das Ausschalten des Systems meist verloren gehen und daher nicht analysiert werden können.

Im Unterschied dazu lassen Live-Response Analysen Untersuchungen flüchtiger und/oder temporär zugänglicher Daten zu.

---

[1] Siehe dazu auch CSC-Schriftenreihe: „Distributed Denial of Service - Hintergründe, präventive Maßnahmen und Mitigationsmaßnahmen“

[2] Ein bitweise kopiertes 1:1 Abbild des kompromittierten Systems (HD, RAM…)

2. Anwendungsbereich

Diese Broschüre versteht sich **NICHT als umfassende IT-Forensik-** und/oder **Vorfallsbehandlungsrichtlinie** (Incident Response). Zu diesem Zweck existieren bereits umfangreiche und umfassende Dokumente wie z.B. der Leitfaden IT-Forensik des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI)[3].

Der **Fokus** dieser **Handlungsempfehlung** liegt auf der Beantwortung folgender Fragestellungen:

- Was sind die **wichtigsten** (minimalen) **Vorkehrungen** und **Präventiv-maßnahmen,** die man in einem Unternehmen in Bezug auf eine etwaige Beweissicherung setzen sollte?
- Was ist das **korrekte** (technische) **Verhalten** und was sind die wichtigsten **Schritte** und **Reaktionen** auf einen konkreten **Sicherheitsvorfall**?
- Welche relevanten **Schritte** zur **Beweissicherung** (für Behörden) sind durchzuführen bzw. zu empfehlen?
- Wie geht man bei der **Kontaktaufnahme** mit den zuständigen **Behörden** vor? Und welche sind das?

Wird eine Behörde im Zuge eines Sicherheitsvorfalls hinzugezogen, stehen stets zwei Zielsetzungen im Vordergrund: **(1) Eindämmen** und **(2) Ermitteln**. Aus Punkt 2 ergibt sich für die Behörde **immer eine Verpflichtung zur Meldung an die Staatsanwaltschaft**.

Handlungen und Aufgaben wie z.B. das Clean-Up nach einem Vorfall, die Verbesserung der internen Prozesse, die Durchführung weiterer nachgelagerter Schritte oder die Maßnahmenumsetzung fallen **nicht** in den Aufgabenbereich der zuständigen Behörden, sondern sind liegen im Verantwortungsbereich des Unternehmens.

3. Vorbereitungen

Der Fokus der folgenden Unterkapitel liegt auf den unterschiedlichen Typen von Logdaten und den Möglichkeiten bzw. Schritten zur Ermöglichung einer entsprechenden Analyse.

Auf **infrastrukturelle** und **organisatorische Vorbereitungen** und **Regeln**, wie eine empfohlene **zentrale Speicherung** von Logdaten oder die Sicherstellung eines erhöhten Schutzbedarfes von Logdaten in Bezug auf **Zugriffsrechte**, wird im Folgenden nicht näher eingegangen.

Nichtsdestotrotz muss hier auf die **Wichtigkeit** einer **korrekten Implementierung** von **Schutzmaßnahmen** für Logdaten bzgl. Speicherung, Transfer und Verarbeitung hingewiesen werden.

[3] https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Dienstleistungen/IT-Forensik/forensik_node.html

3.1. Datensammlung

3.1.1 Netzwerk-und Host-basierte Logs

Die folgende Tabelle bietet Informationen über **unterschiedliche Logdaten**, welche geloggt werden können/sollten, inklusive derer Vor- und Nachteile sowie einer Empfehlung bzgl. des empfohlenen Aufbewahrungszeitraums.

Datentyp	Vorteile	Nachteile	Speicher-dauer
Full-Packet Capture (PCAP) beinhalten die originalen komplett oder partiell vollständigen Daten des Netzwerkpakets. **Hinweis:** Die Erfassung und Aufbewahrung von PCAP Daten sollte nur im Anlassfall oder bei hochkritischen Systemen vollzogen werden.	Ermöglicht **tiefe nach-gelagerte Analysen** der Netzwerkpakete und Datenverkehrs mit Hilfe frei verfügbarer **Tools** und **Hilfsmittel**. **Hinweis:** Der volle Datenzugriff besteht nur beim Einsatz **nicht verschlüsselter Kommunikation**.	Anforderungen an **Speicherplatz** und **Analysezeitaufwand** können durch die **Größe** der gesammelten Daten **extrem groß** werden. Ebenso können **rechtliche Rahmenbedingungen,** z.B. in Bezug auf Datenschutz bei der Analyse problematisch werden.	**3 Monate oder länger**[4]
NetFlow Daten beinhalten nicht den Inhalt der Netzwerk-Kommunikation, sondern die Metadaten jeder Netzwerk-verbindung.	Deutlich **geringere An-forderungen** an **Speicherplatz** und **schnellere Analysemöglichkeiten**. Geringere rechtliche Einschränkungen wie z.B. durch Datenschutz. Metadatenanalyse ist unabhängig davon, ob der Netzwerkverkehr verschlüsselt oder unverschlüsselt ist.	**Tiefergehende** Analysen sind **nicht möglich**, da der Inhalt des Netzwerk-pakets nicht gespeichert wird.	**½ - 1 Jahr**
Logdateien beinhalten applikations- bzw. plattform-spezifische Informationen (z.B. **Proxy Log, oder Betriebssystem-Eventlogs**).	**Tiefergehende** applikations- bzw. plattformabhängige **Analysen** sind möglich (z.B. im Rahmen eines SIEM[5] Systems).	Signifikant höherer **Aufwand,** um **Logdaten anzureichern** und aus unterschiedlichem Quellen zu **aggregieren** und zu **korrelieren**. Applikations- bzw. plattform-spezifische **Abhängigkeiten** in Bezug auf Loginhalte.	**½ - 1 Jahr**[6]

Tabelle 1: Netzwerk-Datentypen

[4] Abhängig vom Traffic und verfügbaren Speicherplatz. Für die im Anlassfall gesammelten Daten.
[5] Security Incident und Event Management
[6] z.B. Proxy Log analog zu NetFlow Daten

Bezüglich der oben erwähnten Logdatentypen ist zu erwähnen, dass von der **„reinen“ Analyseseite** (Behörden, Betrieb etc.) betrachtet, der Grundsatz „**je mehr** und umfangreicher Logdaten gesammelt werden, **desto besser**“ gilt. Dass dies natürlich in Bezug auf **Effizienz** der Logsammlung nicht immer gilt, steht außer Frage. Eventuell müssten zusätzliche Aufwände bei Speicherplatz oder personellen Ressourcen zur Analyse in Kauf genommen werden.

Ein **Minimalset an Informationen** sollte man jedoch für jeden gesammelten Logdatentyp identifizieren und zumindest auf allen Systemen implementieren **z.B**. Folgende **Systemereignisse** sollten auf **Betriebssystemebene** aufgrund Ihrer Aussagekraft bzgl. einer möglichen Malwareinfektion immer geloggt werden:

- Command/Power-Shell Befehle
- Service / CronJobs Erzeugung, Start, Stop
- Programmstarts, Autostarteinträge
- Benutzerspezifische Ereignisse (Erfolgreiche/Fehlgeschlagene Authentifizierung von lokalen und Netzwerkusern, Benutzererstellung, Änderungen von Benutzerrechten und zugewiesenen Gruppen)
- Netzwerkzugriffe

Die folgende Tabelle bietet eine Übersicht wo solche Daten innerhalb Ihres Netzwerks gesammelt werden können, bzw. welche Vor- und Nachteiles bei diesen **Sammelpunkten** existieren.

Sammelpunkt	Vorteile	Nachteile
Bei einem **Switch** können über einen **Spiegelport** Netzwerkpakete dupliziert werden, welche in weiterer Folge zu weiteren **PCAP** oder **NetFlow** Analysen weitergesandt werden.	Das Einrichten eines Spiegelports erfordert **minimale Konfigurationsanpassungen** Switches sind in fast allen **Netzwerktopologien** und -**Netzwerkebenen** im Einsatz bzw. **omnipräsent**.	**Datenverlust** durch **limitierte Bandbreite** ist möglich.
Router bieten üblicherweise die Möglichkeit **NetFlow** Daten zu exportieren	**Minimale Konfigurationsanpassungen** nötig, da Funktionalität in üblichen Netzwerktopologien bereits vorhanden ist.	Normalerweise **kein PCAP** möglich.
Layer 7 Devices wie **Web Proxies, Load Balancers, DHCP and DNS Server** etc. oder auch **Endpoint** Geräte können wertvolle Quellen zum Sammeln von PCAP, NetFlow oder auch anderen Daten und Informationen sein.	Zusätzliche Daten und Informationen können hier erfasst werden, um proaktiv und/oder im Falle eines **Vorfalls** miteinander **aggregiert**, **korreliert** und **ausgewertet werden** zu können. Siehe auch Kapitel 3.2 Datenanalyse.	Signifikant höherer **Aufwand** um **Logdaten anzureichern** und aus unterschiedlichem Quellen zu **aggregieren** und **korrelieren**. applikations- bzw. plattformspezifische **Abhängigkeiten** in Bezug auf Loginhalte.

Sammelpunkt	Vorteile	Nachteile
Ein **Netzwerk Tap** ist eine dedizierte hardwarebasierte Appliance, welche Netzwerkpakete dupliziert und diese zur weiteren **PCAP** oder **NetFlow** Analysen weitersendet.	Speziell für den Anwendungszweck des Netzwerkdatensammelns, und daher der „**Best-Case**“ in Bezug auf Sammelpunkte (auch im Hinblick auf **Performance** und **Verlässlichkeit**).	Appliances können sehr **teuer** sein und erfordern üblicherweise **kurzzeitige Unterbrechungen** des Netzwerkverkehrs für die **Installation** im Netzwerk.

Tabelle 2: Netzwerk-Sammelpunkte

Die Identifizierung geeigneter Sammelpunkte für Logdaten des Netzwerks ist der **essentielle erste Schritt**, um eine effiziente Datensammlung zum Zwecke der Überwachung bzw. des Monitoring und/oder zur Beweissicherung, zu ermöglichen. Beispielhaft wird dies in folgender Abbildung dargestellt.

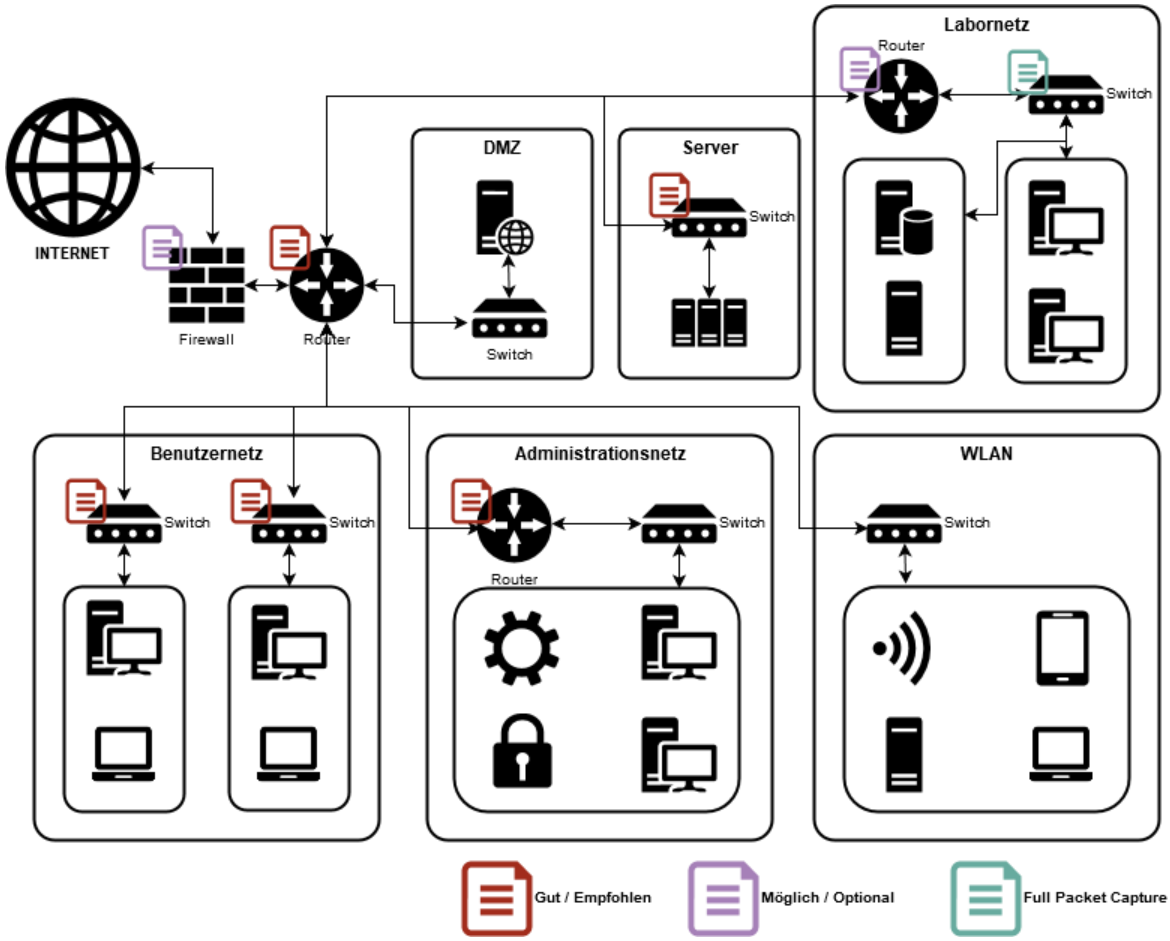

Abbildung 1: Mögliche Sammelpunkte Beispiel

Folgende **Best-Practices** können bei dieser Identifizierung helfen bzw. sollten befolgt werden:

- Identifikation **kritischer Daten / Infrastruktur**
- Erstellung / Pflege eines unternehmensweiten **Netzwerkplans(-diagramms)**

- Identifikation **zentraler** und/oder **kritischer Netzwerkpunkte** zwischen Benutzer, Daten und (wenn angebunden) Internet, z.B. Zusammenführen von VLANs
- Identifikation **kritischer** und/oder **sensibler Datenverarbeitungs-** und/oder **Datenspeicherungslokationen**, z.B.: DNS Servers, CRM System, Versionskontrollsystem, etc.
- Abstimmung bzgl. **regulatorischer** und **rechtlicher Konformität**

3.1.2 Applikations- und Datenbanklogs

Auch **Auditlogs, Zugrifflogs, Workflowlogs** etc. unterschiedlicher **Applikationen** und **Datenbanken** können sehr wertvolle Informationen zur Nachvollziehbarkeit von Vorfällen (z.B. Datenexfiltration, etc.). bieten.

Die Existenz bzw. Qualität solcher Logdaten ist natürlich **stark abhängig** von der **Umsetzung** und **Konfiguration** der **Applikation** bzw. der **Datenbank** selbst. Daher würde eine Detailauflistung aller unterschiedlicher Applikationen und Datenbanken den Umfang dieser (und vermutlich jeder anderen) Handlungsempfehlung sprengen.

3.2. Datenanalyse

Um, wie im vorherigen Kapitel beschrieben, gesammelte Daten zu verarbeiten und zu analysieren kann **folgender Arbeitsablauf** herangezogen werden.

In Bezug auf weitere (behördlichen) Ermittlungen sind im Speziellen die **Schritte eins** und **zwei** auf Seiten des **Unternehmens** von Nöten, um die **Schritte drei** und **vier** auf Seiten der **Behörden** (oder des **internen Sicherheitsteams**) zu ermöglichen.

Des Weiteren können bei einem konkreten Sicherheitsvorfall weitere Beweisobjekte wie z.B. Arbeitsspeicher und Festplatten für weitergehende Analysen von großem Wert sein.

Schritt	Ziel
1. Zusammenfassen	Vorbereitend zur Analyse werden die gesammelten **Logdaten** (im besten Falle mit Hilfe einer dafür bereits implementierten Analyseplattform) **korreliert** und **aggregiert**.
2. Fokussieren	**Reduktion** bzw. **Filterung** des gesamten Datenpools, um die Analyse auf ein oder mehrere **Subdatensets** bezüglich bestimmter **Indikatoren** (IP Adressen, Ports, Protokolle, Zeitpunkt/-spanne, Domains, Hostnamen, etc.) fokussieren zu können.
3. Analysieren	**Analyse** des im vorherigen Schrittes fokussierten Datenpools **kombiniert** mit bestehendem **Wissen** über den vermutlichen **Vorfall** und dem **normalen Verhalten** des Netzwerks auf unüblichen Netzwerkverkehr, Protokolleinsatz, Systemevents etc.
4. Erzeugen von Indikatoren (IOCs)	Das Finden von **Mustern** und/oder **Informationen,** die in weiterer Folge als **Indikatoren** für denselben oder einen ähnlichen **Vorfall** dienen können, z.B. DNS Aktivität, Malwaresamples, Zertifikate, Command & Control Netzwerkverkehr.

Schritt	Ziel
5. Verwendung von Indikatoren (IOCs)	**Suche** nach den im vorherigen Schritt neu gefundenen **Indikatoren** auf den **gesamten Datenpool** um auch hier **weitere** mögliche **Vorfälle** aufzuspüren, und/oder in weiterer Folge im Betrieb des eigenen Netzwerks zur **laufenden Überwachung**.

Tabelle 3: Datenanalyse Arbeitsschritte

Unter anderem können **folgende** (beispielhaft angeführte) **Metriken** herangezogen werden, um Anomalien in den zu analysierende Daten, oder auch bei der laufenden Überwachung im Betrieb des Netzwerks, zu erkennen:

Metrik / Lokation	DNS Server	Firewall	HTTP Proxy	HTTP Server	NetFlow	NSM	Passive DNS
Top-Kommunizierende IP Adressen					x		
HTTP User-Agent			x	x		x	
Top abgefragte DNS Domains	x					x	x
HTTP Post Größen			x	x		x	
Neu erkannte/registrierte Domänen	x					x	x
Unübliche Port und Protokoll Benutzung					x		
(Periodisches) Traffic Volumen					x		

Tabelle 4: Metriken zur Analyse - Beispiele

3.3. Personal

Alle in den vorherigen Kapiteln beschriebenen Maßnahmen, Aufgaben oder durchzuführenden Arbeitsschritte hängen in höchstem Maße von **qualifiziertem und verfügbarem Personal** ab.

Dies kann, sowohl was die vorbereitenden Maßnahmen als auch die Tätigkeiten im Anlassfall betrifft, von **eigenem Personal** als auch von **Dienstleistern** übernommen werden.

Personalressourcen für die Bearbeitung erfasster Logdaten, sowie für Wartung und Konfiguration eines SIEM Systems (bezogen auf ein mittelgroßes Unternehmen in Österreich) belaufen sich bei einem **12x5 Betrieb** auf **3 – 4** vollzeitbeschäftigte Mitarbeiter. Dies birgt allerdings ein hohes Risiko, Angriffe außerhalb der Geschäftszeiten gar nicht oder erst am nächsten Tag zu entdecken. Für einen **24x7 Betrieb** eines solchen Systems muss man bereits mit rund **7 – 8** solcher Mitarbeiter rechnen.

Diesen Überlegungen sollten auch die Ergebnisse von Analysen in der Vergangenheit aufgetretener Cyber-Angriffe (v.a. DDoS und Defacements) zu Grunde gelegt werden, die zeigen, dass entsprechende Tätergruppen oftmals den Freitagabend, das Wochenende, Ferienzeit oder auch den Vorabend von Feiertagen für solche Angriffe verwenden.

Auch sollte nicht vergessen werden, dass die entsprechenden Personen **regelmäßig weitergebildet** werden müssen, um mit neuen Angriffsszenarien umgehen zu können. Weiters sollte idealerweise ein „**Incident Response Plan**“ **angelegt** und **beübt werden**, um bei speziellen Bedrohungen schnell und richtig zu reagieren.

4. Im Anlassfall

Aus Sicht der Behörden und in Bezug auf weiterführende **Ermittlungen**, jedoch auch für die **Nachvollziehbarkeit** des Angriffes und den daraus resultierenden **Gegenmaßnahmen,** sind abhängig von der Art des Cyber-Angriffes folgende Logdaten notwendig bzw. vorteilhaft.

Logdaten / Cyber-Angriff	APT	Datenexfiltration	DDoS	Backdoors	Ransomware	(Spear) Phishing	Webapplikationsangriffe
Firewall	x	x	x				
HTTP Proxy	x	x		x	x		
HTTP Server			x[7]				x
NetFlow	x	x	x	x	x		x
NSM[8]	x	x		x	x		
Passive DNS	x	x		x	x	x	
DDoS Protection			x				
Event-Log am Host	x	x		x	x	x	
private, mitgebrachte Geräte (BYOD)	x	x					
Mailserver	x	x			x	x	
Applikations-/Datenbankserver		x	x				x

Tabelle 5: Relevante Logdaten bei Cyber-Angriffen

Weitere Beweisobjekte welche je nach Art des Angriffes gesichert werden sollten sind unter anderem:

- Arbeitsspeicher
- Festplatten
- Virtuelle Maschinen
- Embedded Devices / Appliances
- Netzlaufwerke
- Anwendungsdaten

[7] Speziell für den Zeitraum direkt vor Beginn der DDoS Attacke
[8] Network Security Monitor

- Backup
- Cloud Dienste
- Mobile Geräte
- E-Mail Verläufe

Für den Fall eines Angriffes oder Vorfalls bieten die folgenden 2 Unterkapitel eine Übersicht welche Handlungen auf KEINEN Fall bzw. auf JEDEN Fall, soweit technisch möglich, gemacht werden sollten.

4.1. Auf KEINEN Fall

Was	Warum
Herunterfahren **oder** Ausschalten **des befallenen Hosts / Rechners**[9]**.** Analog hierzu das Stoppen von virtuellen Maschinen.	Es können wichtige Daten und Informationen im Arbeitsspeicher verloren gehen.
Eigenständige Sofortanalysen **von Malware Samples mit** öffentlich verfügbaren **und für jedermann einsehbaren** Diensten **wie z.B. Virus Total**[10] **o.ä. öffentlichen Plattformen.**	• Man muss davon ausgehen, dass Hersteller von Malware auf solchen Plattformen „mithören“ und erkennen können wenn eines Ihrer Malwareprogramme zur Analyse hochgeladen wurde. • Daraus folgend kann ein Angreifer den Angriff beenden, Spuren verwischen etc.
Reine Neuinstallation des Betriebssystems**, Einspielen von Backups und Übergang zum** Tagesgeschäft.	• Manchmal wird eine tiefergehende Analyse z.B. aus Ressourcenmangel oder Angst vor öffentlichem Bekanntwerden ignoriert oder deren Behandlung stark verzögert. • Oft breitet sich der Angreifer im internen Netzwerk aus und infiziert auch andere Hosts bzw. verschafft sich alternative Zugriffsmöglichkeiten auf das System. • Der potentielle Schaden, den ein aktiver Angreifer im eigenen Netz anrichten kann, wird gerne unterbewertet. • Ohne genaue Analyse des Einfallsvektors und dem Schließen der Lücke kann der gleiche bzw. ein ähnlicher Angriff jederzeit wieder erfolgen.

Tabelle 6: Maßnahmen die auf keinen Fall zu setzen sind

[9] In speziellen Fällen, z.B. bei akutem Befall und/oder Ausbreitung von Ransomware, kann das Ausschalten des Hosts / Rechners sehr wohl die bevorzugte Option sein.
[10] https://www.virustotal.com/

4.2. Auf JEDEN Fall

Was	Warum
Isolation **des(r) befallenen Hosts / Rechner im internen Netz.**	Um „Lateral Movement“, sprich die weitere Infektion oder Übernahme von Teilen Ihres Netzwerks, zu verhindern.
Wenn möglich, Verringerung **der** Bandbreite **um C&C**[11] **Verbindungen nicht abzubrechen, jedoch zu drosseln.**	• Der Angreifer / die Malware sieht weiterhin eine Verbindung nach außen. Drosselung von Bandbreite kann mannigfaltige Gründe haben, daher wird er hier eher nicht Verdacht schöpfen entdeckt worden zu sein. • Durch die Drosselung kann Datenexfiltration im großen Stil unterbunden werden. • Eine, meist sehr aufschlussreiche, laufende Analyse der Aktivitäten des Angreifers/der Malware ist möglich.
Sicherung des Systemzustandes **vor Beginn von Analysen.**	• Analysen am System können unfreiwillig Daten zerstören / verschleiern, wie z.B. relevante Artefakte im Arbeitsspeicher oder in nicht allokierten Bereichen auf Datenträgern. • Diese Daten können jedoch bei einer tiefergehenden forensischen Analyse wertvoll sein. • Falls der Angreifer erkennt, dass er entdeckt wurde, darf er keine Möglichkeit erhalten seine Spuren zu verwischen.

Aktivierung zusätzlicher Loggingdetails**, um die Analyse zu erleichtern.**	• Dies betrifft alle Ebenen in der Systemlandschaft. (Betriebssystem-, Netzwerk-, Applikation spezifisches Logging)
	• Der Detailgrad der Loggingevents hängt stark vom Ziel der Analyse ab. Folgende Logging Informationen wären denkbar:
	  ○ Benutzerlogins
	  ○ Benutzerverwaltung
	  ○ Datenzugriffe
	  ○ Privilegierte Benutzer Aktionen
	  ○ Prozessverfolgung
	  ○ Systemevents
	  ○ Netzwerkverbindungen
	• Um ein umfassendes Bild zu erlangen, sollten sowohl Fehler- als auch erfolgreiche Ereignisse/Events mitprotokolliert werden
	• Dabei ist darauf zu achten, dass durch Aktivierung zusätzlicher Logging Informationen, der Speicherplatzverbrauch stark zunimmt.

Aktualisierung aller Softwarekomponenten **im Netzwerk.**	Um die Möglichkeit einer weitere Ausbreitung zu minimieren
Backups der **Log-Informationen.**	für Dokumentationszwecke und ggf. zur Strafverfolgung
Analyseabbild des Systems.	Wir empfehlen am betroffenen Echtsystem so wenig wie möglich bzgl. der Analyse zu agieren und wenn möglich ein Abbild in einem Standardformat zu erstellen (VM-Snapshot oder Festplattenabbild inklusive Sicherung des flüchtigen Speichers).

Tabelle 7: Maßnahmen die auf jeden Fall zu setzen sind

[11] Command & Control

5. Behördenkontakt

Bitte beachten Sie folgende Punkte in Bezug auf Behördenkontakt im Falle eines stattfindenden oder stattgefundenen Cyber-Angriffes:

- **Wen** kontaktieren?
  - Für staatsschutzrelevante Vorfälle, insbesondere den Schutz kritischer Infrastrukturen und verfassungsmäßiger Einrichtungen, ist das Cyber Security Center (CSC) des BVT zuständig und zu kontaktieren:
    → E-Mail: csc@bvt.gv.at
  - Wenn Sie einen Verdacht auf Internetkriminalität haben und Hilfe und Informationen benötigen, wenden Sie sich bitte an folgende E-Mail Adresse against-cybercrime@bmi.gv.at.
  - Wenn Sie durch eine Straftat geschädigt wurden oder konkrete Hinweise auf einen Täter haben, können Sie die Straftat natürlich auch in jeder Polizeidienststelle zur Anzeige bringen.

- **Wie** können Daten übermittelt werden?
  - Unterschiedlich je nach Art des Vorfalls, von Vorort Abholung bis via verschlüsseltes E-Mail.
  - Die genaue Art der Übermittlung wird im Anlassfall zwischen Behörde und betroffener Institution vereinbart.

Bundesamt für Verfassungsschutz und Terrorismusbekämpfung
Cyber Security Center