Bundesministerium
Inneres

Log-Daten als Grundlage für Incident Response

Sammlung, Analyse & Weiterverarbeitung

Vorbereitung auf und Empfehlungen für den Anlassfall

Impressum

Medieninhaber, Verleger und Herausgeber:
Bundesministerium für Inneres
Herrengasse 7, 1010 Wien
bmi.gv.at
Autoren: Abteilung IV/10 – Netz- und Informationssystemsicherheit
Direktion Staatsschutz und Nachrichtendienst
Druck: Digitalprintcenter des BMI

Neuauflage
Wien, Februar 2022

Rückmeldungen: Ihre Überlegungen zu vorliegender Publikation übermitteln Sie bitte an praevention@nis.gv.at | csc@dsn.gv.at

Inhalt

1 Hintergrund und Anwendungsbereich

1.1 Hintergrund

Seit mehreren Jahren kann ein stetiger Anstieg von monetär und/oder ideologisch motivierten Cyber-Angriffen unterschiedlichster Ausprägungsart beobachtet werden. Insbesondere sind in diesem Zusammenhang folgende Vorfallsarten anzuführen:

- APT-Kampagnen (Advanced Persistent Threats)[1],
- DDoS-Angriffe (Distributed Denial of Service)[2] sowie
- 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 (Cybercrime im weiteren Sinn), als auch für solche, in denen die Systeme selbst das Angriffsziel sind (Cybercrime im engeren Sinn).

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 einleiten zu können.

Bei der Analyse eines Sicherheitsvorfalls spielen die vorhandenen Log-Daten eine zentrale Rolle. Da Log-Daten meist auch personenbezogene Daten beinhalten, kommen hier auch das österreichische Datenschutzgesetz und die Datenschutzgrundverordnung zur Anwendung. Dies erfordert unter anderem sowohl eine Einschränkung auf für die Sicherheit bzw. für die Analyse von potentiellen Vorfällen relevanten Daten, als auch ein entsprechendes

[1] Hierbei handelt es sich um komplexe, zielgerichtete und aufwändige Angriffe auf Organisationen, wie Behörden, Institutionen oder Unternehmen.
[2] Siehe dazu auch CSC-Schriftenreihe: „Distributed Denial of Service (DDoS) - Hintergründe, präventive Maßnahmen und Mitigationsmaßnahmen“

Sicherungskonzept für Log-Daten, um diese vor unbefugtem Zugriff oder Manipulation zu schützen.

Das Ziel einer forensischen Untersuchung ist die Beantwortung folgender Fragestellungen:

- Was ist geschehen?
- Wo ist es passiert?
- Wann ist es passiert?
- Wie ist es passiert?

Die Beantwortung ebendieser Fragen kann durch zwei unterschiedliche Vorgehensweisen ermöglicht werden:

Post-mortem-Analyse

Bei einer Post-mortem-Analyse handelt es sich um eine Analyse eines ausgeschalteten Systems, bei der digitale Spuren auf einem forensischen Duplikat[3] 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.

Live-Response-Analyse

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

[3] Ein bitweise kopiertes 1:1-Abbild des kompromittierten Systems (z. B. HDD, RAM)

1.2 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)[4].

Der Fokus dieser Handlungsempfehlung liegt auf der Beantwortung folgender Fragestellungen:

- Was sind die wichtigsten (minimalen) Vorkehrungen und Präventivmaßnahmen, 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. **Gefahrenabwehr** und
2. **Ermittlungen**.

Aus letzterem Punkt 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 liegen im Verantwortungsbereich des Unternehmens.

[4] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf?__blob=publicationFile&v=1

2 Vorbereitungen

Der Fokus der folgenden Ausführungen liegt auf den unterschiedlichen Typen von Log-Daten und den Möglichkeiten bzw. Schritten zur Ermöglichung einer entsprechenden Analyse.

Auf infrastrukturelle und organisatorische Vorbereitungen und Regeln, wie die Sicherstellung eines erhöhten Schutzbedarfes von Log-Daten in Bezug auf Zugriffsrechte, wird im Folgenden **nicht** näher eingegangen. Nichtsdesto¬trotz muss hier auf die Wichtigkeit einer korrekten Implementierung von Schutzmaßnahmen für Log-Daten bezüglich Speicherung, Transfer und Verarbeitung hingewiesen werden.

2.1 Datensammlung

Im Zusammenhang mit der Datensammlung kann grundsätzlich zwischen (1) **Netzwerk- und Host-basierten Logs** und (2) **Applikations- und Datenbank¬Logs** unterschieden werden.

Netzwerk- und Host-basierte Logs

Die folgende Tabelle bietet Informationen über unterschiedliche Log-Daten, die geloggt werden können/sollten, inklusive deren Vor- und Nachteile sowie eine Empfehlung bzgl. des empfohlenen Aufbewahrungszeitraums.

Tabelle 1 Netzwerk-Datentypen

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 nachgelagerte Analysen der Netzwerkpakete und des 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[5]
Netflow-Daten beinhalten nicht den Inhalt der Netzwerk-Kommunikation, sondern die Metadaten jeder Netzwerkverbindung.	Deutlich geringere Anforderungen 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.	6 bis 12 Monate
Logdateien beinhalten applikations- bzw. plattformspezifische Informationen (z. B. Proxy-Log, oder Betriebssystem-Eventlogs).	Tiefergehende applikations- bzw. plattformabhängige Analysen sind möglich (z. B. im Rahmen eines SIEM[6] Systems).	Signifikant höherer Aufwand, um Log-Daten anzureichern und aus unterschiedlichen Quellen zu aggregieren und zu korrelieren. Applikations- bzw. plattformspezifische Abhängigkeiten in Bezug auf Loginhalte.	6 bis 12 Monate[7]

Bezüglich der oben erwähnten Log-Datentypen ist zu erwähnen, dass von der „reinen“ Analyseseite (Behörden, Betrieb etc.) betrachtet, der Grundsatz „je mehr und umfangreicher Log-Daten gesammelt werden, desto besser“ gilt. Dass dies natürlich in Bezug auf Effizienz

[5] Abhängig vom Traffic und vom verfügbaren Speicherplatz
[6] Security Incident und Event Management
[7] z. B. Proxy-Log analog zu Netflow-Daten

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 Log-Datentyp identifizieren und zumindest auf allen Systemen implementieren, z. B. sollten folgende Systemereignisse auf Betriebssystem¬ebene 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 Nachteile bei diesen Sammelpunkten existieren.

Tabelle 2 Netzwerk-Sammelpunkte

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 Konfigurations-anpassungen. Switches sind in fast allen Netzwerk-topologien und Netzwerk-ebenen im Einsatz bzw. omnipräsent.	Datenverlust durch limitierte Bandbreite ist möglich.
Router bieten üblicherweise die Möglichkeit NetFlow Daten zu exportieren.	Minimale Konfigurations-anpassungen nötig, da Funktionalität in üblichen Netzwerktopologien bereits vorhanden ist.	Normalerweise kein PCAP möglich.

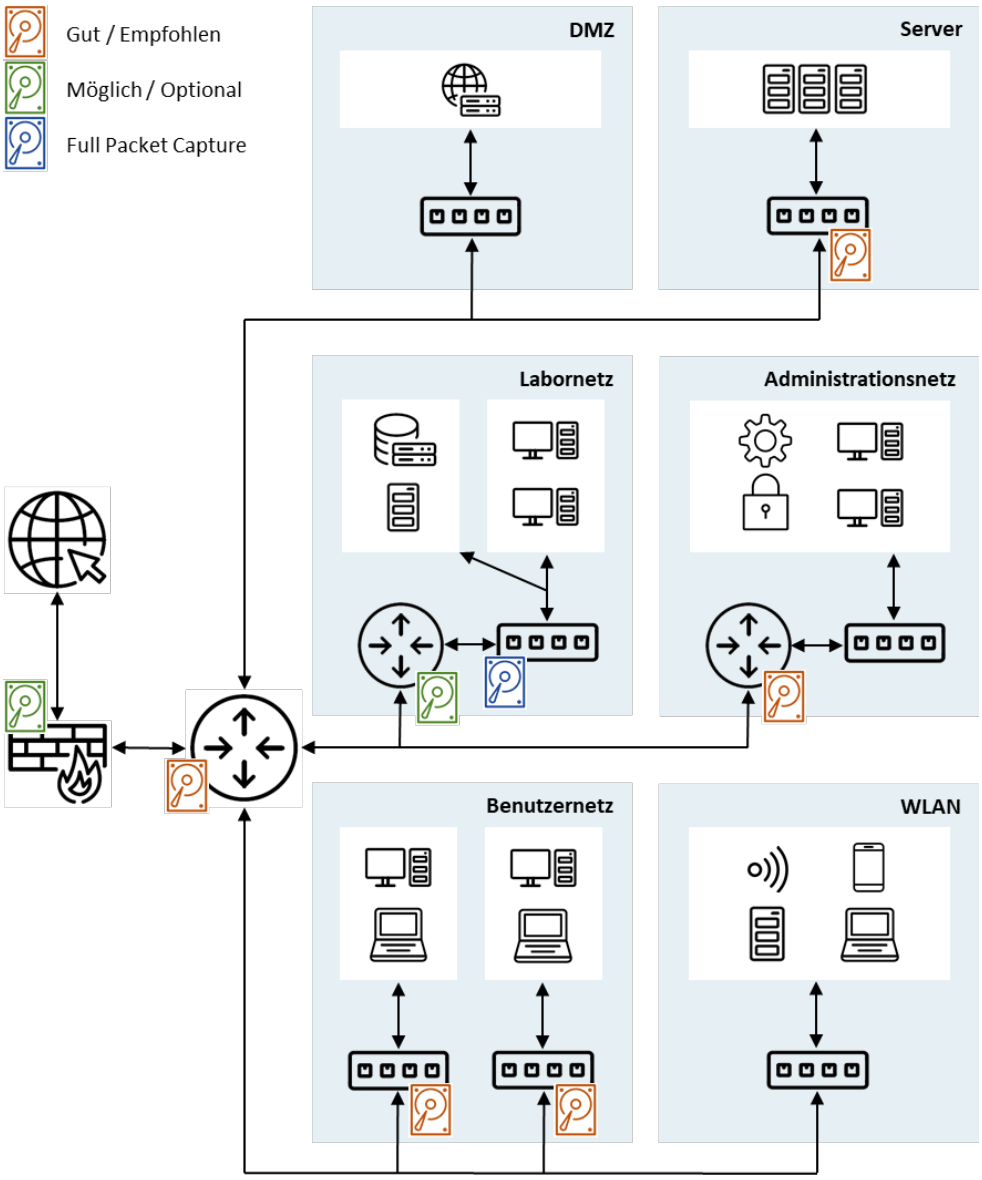
Sammelpunkt	Vorteile	Nachteile
Layer 7 Devices wie Web-Proxys, Load Balancers, DHCP und DNS Server etc. oder auch Endpoint Geräte können wertvolle Quellen zum Sammeln von PCAP, Netflow oder auch anderen Daten und Informationen sein.	Zusätzliche Daten und Informationen können hier erfasst werden, um proaktiv und/oder im Falle eines Vorfalls miteinander aggregiert, korreliert und ausgewertet werden zu können[8].	Signifikant höherer Aufwand um Log-Daten anzureichern und aus unterschiedlichen Quellen zu aggregieren und korrelieren. Applikations- bzw. plattformspezifische Abhängigkeiten in Bezug auf Loginhalte.
Ein **Netzwerk Tap** ist eine dedizierte hardwarebasierte Appliance, welche Netzwerkpakete dupliziert und diese zur weiteren PCAP oder Netflow Analyse 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.

Die Identifizierung geeigneter Sammelpunkte für Log-Daten des Netzwerks ist der essentielle erste Schritt, um eine effiziente Datensammlung zum Zwecke der Überwachung bzw. des Monitorings und/oder zur Beweissicherung zu ermöglichen.

Beispielhaft wird dies in folgender Abbildung dargestellt:

[8] Siehe auch Kapitel 2.2

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 Server, CRM System, Versionskontrollsystem usw.

- Abstimmung bzgl. regulatorischer und rechtlicher Konformität
- Speicherung von Netzwerkströmen vor der Übersetzung durch NAT/PAT/Load Balancern usw.

Applikations- und Datenbanklogs

Auch Audit-Llogs, Zugriff-Llogs, Workflowlogs etc. unterschiedlicher Applikationen und Datenbanken können sehr wertvolle Informationen zur Nachvollziehbarkeit von Vorfällen (z. B. Datenexfiltration, etc.). bieten.

Die Existenz bzw. Qualität solcher Log-Daten 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. Besonders aussagekräftig sind in diesem Zusammenhang aber Applikations-Logs von Netzwerkanwendungen, daher wurden an dieser Stelle einige praktische Hinweise zusammengefasst:

Zum Nachvollziehen des Zugriffes auf Web-Seiten sind die Logs (sowie die zwingende Verwendung) eines „http-Proxys“ entscheidend. Die relevanten Informationen hierbei sind:

- die Destination-URL,
- der Request-Type,
- die Source-IP,
- der Response Code,
- die Paketgröße,
- der Referrer und
- die Zeitstempel.

Insbesondere bei der Source-IP sollte sichergestellt sein, dass der betreffende Client eindeutig ausfindig gemacht werden kann (z. B. durch entsprechende Logs bei der Verwendung von NAT oder DHCP).

DNS-Logs geben Aufschluss darüber, welche Domain von welchem Client aufgelöst wurde. Dies hilft zum Beispiel bei der Identifikation von C2-Domains. Hilfreich hierbei ist die Verwendung einer Passive-DNS-Datenbank, um die Bearbeitung und Analyse zu erleichtern. Ebenfalls empfiehlt es sich, auch NXDOMAIN Anfragen zu loggen.

2.2 Datenanalyse

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

In Bezug auf weitere Ermittlungen sind auf Seiten des Unternehmens im Speziellen die Schritte 1 und 2 erforderlich, um den Behörden (oder einem internen Sicherheitsteam) gegebenenfalls die Möglichkeit zu bieten, die Schritte 3 und 4 durchzuführen.

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

Tabelle 3 Datenanalyse Arbeitsschritte

Schritt	Ziel
1. Zusammenfassen	Vorbereitend zur Analyse werden die gesammelten Log-Daten (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 Schritt fokussierten Datenpools, kombiniert mit bestehendem Wissen über den vermutlichen Vorfall und dem normalen Verhalten des Netzwerks auf z. B. unüblichen Netzwerkverkehr, Protokolleinsatz oder auf Systemevents.
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.
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.

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

Tabelle 4 Metriken zur Analyse - Beispiele

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		

2.3 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 die vorbereitenden Maßnahmen als auch die Tätigkeiten im Anlassfall betreffend, von eigenem Personal oder auch von Dienstleistern übernommen werden.

Personalressourcen für die Bearbeitung erfasster Log-Daten, sowie für Wartung und Konfiguration eines SIEM-Systems (bezogen auf ein mittelgroßes Unternehmen in Österreich) belaufen sich bei einem 12x5 Betrieb auf 3 bis 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 bis 8 solchen Mitarbeitern 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, die 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.

3 Im Anlassfall

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

Tabelle 5 Relevante Log-Daten bei Cyber-Angriffen

Log-Daten / Cyber-Angriff	APT	Datenexfiltration	DDoS	Backdoors	Ransomware	(Spear) Phishing	Webapplikationsangriffe
Firewall	X	X	X				
HTTP-Proxy	X	X		X	X		
HTTP-Server			X[9]				X
NetFlow	X	X	X	X	X		X
NSM[10]	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

[9] Speziell für den Zeitraum direkt vor Beginn der DDoS-Attacke
[10] Network Security Monitor

Weitere Beweisobjekte, die je nach Art des Angriffes gegebenenfalls gesichert werden sollten, sind unter anderem:

- Arbeitsspeicher
- Festplatten
- Virtuelle Maschinen
- Embedded Devices / Appliances
- Netzlaufwerke
- Anwendungsdaten
- Backup
- Daten in Cloud-Diensten
- Mobile Geräte
- E-Mail Verläufe

Für den Fall eines Angriffes oder Vorfalls bieten die folgenden zwei Unterkapitel eine Übersicht, welche Handlungen auf **keinen** Fall bzw. auf **jeden** Fall, soweit technisch möglich, gesetzt werden sollten.

3.1 Auf keinen Fall

Im Fall eines Angriffs oder Vorfalls sollten folgende Handlungen auf **keinen** Fall gesetzt werden:

Tabelle 6 Maßnahmen, die auf keinen Fall zu setzen sind

Was nicht?	Warum nicht?
Voreiliges Herunterfahren oder Ausschalten des befallenen Hosts / Rechners[11]. Analog hierzu das Herunterfahren von virtuellen Maschinen.	• Es können wichtige Daten und Informationen im Arbeitsspeicher verloren gehen.

[11] In speziellen Fällen, z. B. bei akutem Befall und/oder Ausbreitung von Ransomware, kann das Ausschalten des Rechners sehr wohl die bevorzugte Option sein. Ebenso kann es aber auch von Vorteil sein, einen Rechner nur vom Netzwerk zu trennen, um nach wie vor den Arbeitsspeicher sichern zu können.

Was nicht?	Warum nicht?
Eigenständige Sofortanalysen von Malware Samples mit öffentlich verfügbaren und für jedermann einsehbaren Diensten wie z. B. Virus Total[12] o.ä. öffentlichen Plattformen.	• Man muss davon ausgehen, dass Hersteller von Malware auf solchen Plattformen „mithören“ und erkennen können, wenn eines Ihrer Malware-Programme 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.

3.2 Auf jeden Fall

Im Fall eines Angriffs oder Vorfalls sollten folgende Handlungen auf **jeden** Fall gesetzt werden:

Tabelle 7 Maßnahmen, die auf jeden Fall zu setzen sind

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.

[12] https://www.virustotal.com/

Was?	Warum?
Wenn möglich, **Verringerung der Bandbreite**, um C&C[13] 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 Logging-Details, um die Analyse zu erleichtern.	• Dies betrifft alle Ebenen in der Systemlandschaft (Betriebssystem-, Netzwerk- und Applikations-spezifisches Logging). • Der Detailgrad der Loggingevents hängt stark vom Ziel der Analyse ab. Folgende Logging-Informationen wären denkbar: – Benutzerlogins – Benutzerverwaltung – Datenzugriffe – Privilegierte Benutzeraktionen – 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.
Schließen von kritischen Sicherheitslücken, z. B. durch Aktualisierung von Softwarekomponenten.	• 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).

[13] Command & Control

Was?	Warum?
Dokumentation aller gesetzten Maßnahmen und Handlungen	• Sicherstellung der Nachvollziehbarkeit der Vorfallsbehandlung.

4 Praktische Ratschläge für die Umsetzung

4.1 Konzeption & Konfiguration

Zur Analyse von Log-Daten, die aus den verschiedensten Datenquellen, wie zum Beispiel aus Netzwerkgeräten, Applikationen und Betriebs¬systemen von Servern oder Clients kommen können, gelten **zentrale Log-Plattformen** als State-of-the-Art. Erst im Anlassfall zu beginnen, verschiedene Datenquellen und -formate zu konsolidieren, verzögert die Analyse oft erheblich. Gleichzeitig können Log-Daten so besser gegen Manipulationen durch Angreifer oder vor Zugriff durch Unbefugte geschützt werden, als wenn diese auf einzelne verschiedene Systeme verteilt sind. Ebenfalls wird hierdurch ein aktives Monitoring des Gesamtsystems, sowohl im Hinblick auf (Spuren von) Security-Incidents, als auch bei der Fehlersuche ermöglicht bzw. erleichtert.

Zum Sammeln, Visualisieren und Analysieren der Daten existieren sowohl freie als auch kostenpflichtige Softwarelösungen. Beim Treffen einer Entscheidung, betreffend der verwendeten Technologie, sollten neben den Anschaffungskosten jedenfalls folgende Aspekte berücksichtigt werden:

- Kosten zur Mitarbeiterschulung
- Abhängigkeit der Kosten von der geloggten Datenmenge
- Kosten bei einer Anpassung der Auswahlkriterien für geloggte Daten
- Rechtliche Absicherung bei der Weitergabe von Log-Daten (welche sowohl vertrauliche unternehmensinterne als auch personenbezogene Daten beinhalten können) an Dritte bzw. Cloud-Anbieter

Bei der praktischen Analyse und Korrelation von Daten aus verschiedenen Quellen ist es zielführend, unternehmenseinheitliche Zeitangaben zu verwenden. Dies beinhaltet sowohl die Verwendung (interner oder externer) Zeitserver als auch die Verwendung einer einheitlichen Zeitzone, bzw. die Auszeichnung der verwendeten Zeitzone. Weiters empfiehlt es sich, Daten bei der Sammlung sprechend zu taggen, um auch bei einer zentralen Log-Datenanalyse die genauen Datenquellen jederzeit feststellen zu können (bzw. danach filtern zu können).

4.2 Quick-Wins

Neben einer aufwändigen Datensammlung, Korrelation und Analyse im Hinblick auf bekannte IOCs bzw. Erkennung von Anomalien, existieren auch einige Quick-Wins zur Erkennung von verdächtigem Verhalten, die auf eine bestehende Kompromittierung hinweisen können und näher untersucht werden sollten.

Auffällig können folgende Umstände sein:

- Es werden mehr Daten an einen externen Webserver hochgeladen als der Client von diesem empfängt (Upload/Download-Ratio).
- Ein- und ausgehendende E-Mails:
  - Welche Attachments kommen von außerhalb in das eigene Unternehmensnetzwerk?
  - Gibt es auffällige Datenmengen, die per E-Mail versendet werden?
  - Werden E-Mails von/zu bekannten Freemail-Providern gesendet/erhalten, obwohl dies einer internen Policy widerspricht?
  - Werden E-Mails automatisiert (z. B. über eine angelegte Regel) auf externe Adressen weitergeleitet?
  - Die Kommunikation mit IP-basierenden URLs (wie etwa Zugriffe auf z. B. https://194.12.X.X) könnte auf Schadsoftware hindeuten, da dies im Regelbetrieb nur selten vorkommt.
- Die Kommunikation mit ungewöhnlichen Ports
  - Läuft HTTP(S)-Datenverkehr über andere Ports, als über die Ports 80 und 443?
  - POST-Requests ohne Referrer: Die Abwesenheit des Referrers kann auf einen direkten Seitenaufruf hindeuten.
- Die direkte Kommunikation zwischen Workstations untereinander.
- Der Aufruf von bestimmten Programmen wie z. B. Powershell oder Windows Scripting Host.
- Kommen „interessante“ Abweichungen bei Registry Keys, Dateien im Programmordner, Services, Tasks, Plugins vor?

Diverse Abfragen lassen sich hier zum Teil mit der Windows-Powershell realisieren (z. B. Auflistung von Browserplugins oder Regeln in Outlook).

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 in der Direktion Staatsschutz und Nachrichtendienst zuständig und zu kontaktieren: **csc@dsn.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 vor Ort Abholung bis via verschlüsseltes E-Mail.
- Die genaue Art der Übermittlung wird im Anlassfall zwischen Behörde und betroffener Institution vereinbart.

Tabellenverzeichnis

Abbildungsverzeichnis

Bundesministerium für Inneres
Herrengasse 7, 1010 Wien
praevention@nis.gv.at | csc@dsn.gv.at
bmi.gv.at