forensische IT-Ermittlung

Szenario: Ein Mitarbeiter könnte heimlich Daten von einer internen Festplatte auf einen externen Datenträger kopiert haben. Möglicherweise hat er Programme oder Skripte installiert, um bestimmte Sensorwerte auf dem Mainboard oder das BIOS des Rechners zu manipulieren. Die Geschäftsführung wünscht nun eine lückenlose Dokumentation, damit eine interne IT-Forensik- Abteilung oder, falls nötig, die Strafverfolgungsbehörden den Vorfall aufklären können.



5 Phasen der Ermittlung

- Phase1 : Identifizierung
- -
- Phase2 : Abholung
- _
- Phase 3 : Analyse
- _
- Phase 4: Berichterstattung
- -
- Phase 5: Präsentation

Ermittlungen am Tatort

Identifizierungsphase

- Geräte Identifizieren
- Foto Dokumentieren
 - wie sieht der Tatort aus
 - wo lag die Hardware
 - sind geräte und steckverbindungen getrennt worden
 - gibt es physische Anzeichen für Manipulation

Katalogisieren der einzelnen Komponenten (Hardware, Ablagen und etc.)

Abholungsphase

- Datenerfassung (Image des Gerätes)
- der Ermittler muss spezielle Tools und Techniken verwenden
- der Prozess muss Dokumentiert werden

Software der Forensik

-Adepto dient zum erstellen von Datenträger-images

-Autopsy Forensic Browser Auswerten von Datenträger-Images,

Extraktion von Daten

-Captain Nemo Auslesen diverser Dateisysteme

-Chkrootkit Suche nach Spuren von gebräuchlichen

Rootkits

-Filemon, Regmon Analyse von Registry- und Filesystemzugriffen

von Applikationen

-FPort Anzeige, welche Applikationen Ports geöffnet

haben

Analyse

- werden die gesammelten Daten untersucht
- beweise identifizieren
- spezielle Techniken können gelöschte Dateien wiederherstellen
- der ermittler muss in der Lage sein, die Daten strukturiert zu analysieren, um sicherzustellen, dass alle relevanten Beweise identifiziert sind
- Analysephase kann der Ermittler mehrere Beweisstücke identifizieren
- es ist wichtig, jedes Beweisstück und die Schritte zu seiner Identifizieren und dokumentieren

Überprüfung der Schnittstellen

Durch zugriff auf dem Geräte Image:

- -überprüfen der Verlaufsdatei und Zugriffe auf dem pc
- zuletzt verwendete Dokumente, internetseiten (Browserverlauf)
- -Taskmanager App (verlauf)

IIILEII		เอษแ	CII		10	VV ?	serveriaut)			
Name	PID	Status	Benutzerna				Beschreibung	ourcenauslastung seit 13.11.20	24 für aktuelle Renutzer	- und Sustamkon	ten
AggregatorHost.exe	6756	Wird ausgeführt		00	1.020 K		Microsoft (R) Aggregator Host		24 Iui aktuelle bellutzei	- unu systemkon	ten.
amdfendrsr.exe	3368	Wird ausgeführt	SYSTEM	00	16 K		AMD Crash Defender Service	astungsverlauf löschen			
AMDRSServ.exe	12352	Wird ausgeführt	User	00	140 K		Radeon Settings: Host Service	^			
= AMDRSSrcExt.exe	9704	Wird ausgeführt	User	00	1.324 K		Radeon Settings: Source Extension	le:	CPU-Zeit	Matruark	Benachrichtigun.
AppHelperCap.exe	3808	Wird ausgeführt	SYSTEM	00	680 K		AppHelperCap	140			
ApplicationFrameHo	8872	Wird ausgeführt		00	3.600 K		Application Frame Host	 OpenWith 	0:01:43	0,1 MB	0 ME
atieclxx.exe atiesrxx.exe	3956	Wird ausgeführt	SYSTEM		980 K		AMD External Events Client Module				
	3360	Wird ausgeführt	SYSTEM	. 00	144 K 26.988 K		AMD External Events Service Module	Paint	0:00:01	0 MB	0 ME
audiodg.exe brave.exe	7684 13272	Wird ausgeführt	Lokaler Die				Windows Graphisolierung für Audiogeräte			0.000	10.000
brave.exe brave.exe	13272	Wird ausgeführt Wird ausgeführt	User	00	255.708 K		Brave Browser	pdf24	0:00:01	0 MB	0 ME
brave.exe	12468	Wird ausgeführt	User		237.956 K		Brave Browser	pdf24-Updater	0:00:00	0.1 MB	0 ME
brave.exe	12468	Wird ausgeführt	User	00	15.516 K		Brave Browser	pdf24-Updater	0.00.00	0,1 MB	UME
brave.exe brave.exe	2008	Wird ausgeführt Wird ausgeführt		00	15.516 K 2.260 K		Brave Browser Brave Browser	poqexec	0:00:03	0 MB	0 MF
brave.exe	3408	Wird ausgeführt	User		2.260 K		Brave Browser	- podence	0.00.03	0 IVID	O IVIE
brave.exe	11484	Wird ausgeführt Wird ausgeführt	User	00	284.860 K		Brave Browser	2 powershell	0:00:06	0 MB	O ME
brave.exe	9644	Wird ausgeführt	User		545,496 K		Brave Browser	powersites			
brave.exe	13256	Wird ausgeführt	User	00	6.392 K		Brave Browser	printfilterpipelinesvc	0:00:01	0 MB	0 ME
brave.exe	2964	Wird ausgeführt	User		283.656 K		Brave Browser				
brave.exe	11284	Wird ausgeführt	User	00	4.916 K		Brave Browser	provtool	0:00:01	0 MB	0 M8
brave.exe	11792	Wird ausgeführt	User	00	2.764 K		Brave Browser				
brave.exe	9436	Wird ausgeführt	User	00	41.852 K		Brave Browser	pycharm64	0:00:12	0,3 MB	0 ME
brave.exe	5208	Wird ausgeführt	User	00	16.144 K		Brave Browser				
brave.exe	11736	Wird ausgeführt	User	00	137.520 K		Brave Browser	RadeonSoftware	0:14:07	6,9 MB	0 ME
brave.exe	7060	Wird ausgeführt	User	00	4,444 K		Brave Browser	Rechner Rechner	0:00:01	0 MB	0 MF
brave.exe	9092	Wird ausgeführt	User	00	5.116 K		Brave Browser	iii Kecnner	0.00.01	0 MB	UME
brave.exe	4052	Wird ausgeführt	User	00	15,472 K		Brave Browser	RtkAudUService64	0:30:14	0 MB	0 ME
brave.exe	5960	Wird ausgeführt	User	00	6,900 K		Brave Browser	- KIMUUUSEIVICEU4	0.30.14	O IVID	O IVIE
brave.exe	7504	Wird ausgeführt	User	00	8.856 K		Brave Browser	■ RtkBtManServ	0:01:23	0 MB	0 ME
brave.exe	12828	Wird ausgeführt	User	00	30.092 K		Brave Browser	i i i i i i i i i i i i i i i i i i i			
brave.exe	9476	Wird ausgeführt	User	00	6.916 K		Brave Browser	rundli32	0:00:00	0.1 MB	0 ME
cmd.exe	7472	Wird ausgeführt		00	16 K		Windows-Befehlsprozessor				
Cncmd.exe	4768	Wird ausgeführt	User	00	16 K		AMD Software Command Line Interface	RuntimeBroker	0:11:16	0 MB	0 ME
conhost.exe	7280	Wird ausgeführt	User	00	60 K		Host für Konsolenfenster	<u></u>			
conhost.exe	3756	Wird ausgeführt	User	00		x64	Host für Konsolenfenster	sc sc	0:00:01	0 MB	0 ME
CPUMetricsServer.exe	10940	Wird ausgeführt	User	00	16 K		Radeon Settings: CPU Metrics Server	- 22 2		2000	10000
crashpad handler.exe	13940	Wird ausgeführt		00	180 K		crashpad handler	schtasks	0:00:01	0 MB	0 ME
Management beautier and	0026	taring accommendation		00	1016		hpad handler	sdbinst	0.00:01	0 MB	0 MF
		A paragraph of the					rosoft Cross Device Service	sabinst	0:00:01	0 MB	U ME
e hat deinen Bildschirm f		Control Services		Ausblenden			nt-Server-Laufzeitprozess	Sdraw	0:00:01	0 MB	0 ME
ctfmonexe	10860	Wird ausgeführt		00	4.132 K		CTF-Ladeprogramm	0.000	00100	0.110	
Cttmon.exe PDiagsCap.exe	3768		SYSTEM	00	4.132 K		CTF-Ladeprogramm DiagsCap	SearchFilterHost	0:04:29	0 MB	0 ME
DiagsCap.exe	8524	Wird ausgeführt	User	00	2.724 K			Constitutous	0:09:51	0 MB	0 MI
dlihost.exe	8524	Wird ausgeführt		00	2.724 K		COM Surrogate	A SearchIndexer	0:09:51	0 MB	0 M
dilhost.exe		Wird ausgeführt	User	00	1.376 K 49.336 K		COM Surrogate	SearchProtocolHost ■ SearchProtoc	0:24:31	0 MB	0 M
FLANFPService.exe	3728 5388	Wird ausgeführt Wird ausgeführt	DWM-1	00	49.336 K		Desktopfenster-Manager	up Searchriotocolnost	0:24:31	UMB	UM
ELANFPService.exe	5388	Wird ausgeführt	SYSTEM	00	36 K	X04	Elan Service	SECOCL64	1:15:37	0 MB	0 M

Hardware Prüfen

- Schauen ob alles internen Hardwarekomponeten funktionieren und nicht manipuliert worden.
- sind alle steckverbindungen korrekt etc.

Berichterstattung

- nach abschluss der Analysephase muss der Ermittler einen ausführlichen Bericht erstellen, ergebnisse zusammengefasst
- bericht sollte eine zusammenfassung der Untersuchung, der verwendeten Methoden, der gesammelten Beweise und der aus Analyse gezogenen Schlussfolgerungen enthalten
- bericht sollte klar und prägnant verfasst sein und keinen Fachjargon enthalten
- bericht sollte Empfehlungen für weiter Untersuchungen oder Maßnahmen enthalten

Danke Für eure Aufmerksamkeit