Technisch gerüstet: Tools für Incident Response

Incident Response und Forensik erfordern komplexe Prozesse und spezielle Werkzeuge. Welche Arten von Tools sind bei der Bewältigung von Sicherheitsvorfällen hilfreich und wofür können sie jeweils eingesetzt werden?

Von Joshua Tiago

IT-Sicherheitsvorfälle effektiv zu behandeln, erfordert viel Vorbereitung, einen klar definierten Incident-Response-Plan, erprobte Prozesse, geschultes Personal und am Ende natürlich technische Fähigkeiten und Werkzeuge. Wie in anderen Bereichen gilt auch hier: Je komplexer das Problem ist, desto spezieller sind die dafür benötigten Tools. Gängige Werkzeuge aus anderen IT-Bereichen kommen schnell an ihre Grenzen und können viele Anforderungen für die Bewältigung von Sicherheitsvorfällen und deren Analyse nicht oder nur bedingt erfüllen. Grundsätzlich unterscheidet man zwischen Tools für Incident Response (IR) und solchen der Forensik. Eine Übersicht über die wichtigsten Werkzeuge aus diesen Bereichen zeigt die Tabelle.

Die Aufgaben der Incident Response bestehen im Wesentlichen darin, Sicherheitsvorfälle schnell zu bewerten, das Ausmaß des Vorfalls zu ermitteln und entsprechende Maßnahmen zur Eindämmung einzuleiten. Werkzeuge in dieser Kategorie dienen primär dem Sammeln und schnellen Analysieren forensisch relevanter Artefakte.

EDR: Angriffe zeitnah entdecken

Ein in dieser Kategorie besonders hervorzuhebendes Werkzeug ist Endpoint Detection and Response (kurz EDR). Produkte dieser Art sollen Angriffe nach Möglichkeit sehr früh erkennen und im besten Fall vollständig unterbinden. Für Mitglieder eines Incident-Response-Teams bieten sie in der Regel aber noch viel mehr Möglichkeiten. Die Agenten der EDR-Software werden auf den zu schützenden Endgeräten installiert und dienen fortan als eine Art Sensor. Über eine zentrale Webkonsole lassen sich Informationen zu den einzelnen Endgeräten abfragen. Dadurch kann das IR-Team zum Beispiel im Rahmen eines Sicherheitsvorfalls analysieren, welche Prozesse zum Zeitpunkt des Vorfalls liefen, welche Netzwerkverbindungen bestanden und auf welche Dateien zugegriffen wurde.

Systeme isolieren, Artefakte sichern

Die meisten EDR-Tools ermöglichen Querys in einer speziellen Abfragesprache, beispielsweise KQL (Kusto Query Language). Analysten haben dadurch die Möglichkeit, sehr granular spezifische Informationen über die Webkonsole zu erhalten. Typischerweise haben IR-Teams bereits im Vorfeld Abfragen definiert und getestet, um die erforderlichen Informationen im Ernstfall schnell einzuholen. Darüber gestatten es viele EDR-Produkte, bei Bedarf Systeme zu isolieren und weitere IR-Werkzeuge oder IR-Skripte auf dem jeweiligen Host direkt auszuführen. Damit kann man beispielsweise schnell ein Abbild des Hauptspeichers erstellen oder weitere Artefakte sichern.

Eine vollständige forensische Analyse eines Systems dauert oft lange, doch bei einem Vorfall sind schnelle Erkenntnisse gefragt. Ein möglicher Ausweg besteht darin, zu Beginn eines Vorfalls nur einen kleineren Teil relevanter Artefakte zu sichern und zu analysieren. Dieses sogenannte Triage-Image enthält detaillierte Artefakte, die dem Analysten als Grundlage für ein schnelles Bild der Lage dienen.

Typischerweise enthält ein Triage-Image das Abbild des Hauptspeichers oder Teile davon, viele Artefakte aus dem Profil des betroffenen Benutzers auf dem System, Logdaten und weitere Systeminformationen. Darunter befinden sich auch Dinge wie die Browserhistorie, Informationen zu Prozessen, kryptografisches Schlüsselmaterial und vieles mehr. In vielen Fällen reichen diese Informationen für eine Erstbewertung aus. Je nach Vorfall kann das Team dann entscheiden, ob eine tiefer gehende und vollständige forensische Analyse notwendig ist.

In der Praxis werden bei Bedarf spezielle Werkzeuge auf dem betroffenen System ausgeführt, um ein solches Abbild zu erstellen. Das sind in der Regel kleine ausführbare Programme, die Teil einer Software oder Plattform für Incident Response und Forensik sind. Diese Kollektoren werden üblicherweise über die bereits vorhandene Softwareverteilung, EDR-Software oder andere Automatismen auf das Endgerät gebracht und ausgeführt. Je nach Werkzeug lässt sich detailliert auswählen, welche Artefakte im Triage-Image enthalten sein sollen.

Die Erstellung des Triage-Abbilds dauert meist nur wenige Minuten. Neben dem Hauptspeicher kann man explizit weitere Artefakte wie den Browserverlauf auswählen. Je nachdem, welche Artefakte gesichert wurden, beträgt dessen Größe wenige Hundert Megabyte bis zu einigen Gigabyte. Um die Ergebnisse auszuwerten, muss man das Image mittels der Analysesoftware des Herstellers weiterverarbeiten. Manche Werkzeuge beschränken sich darauf, die gewünschten Artefakte zu sichern. Andere gehen einen Schritt weiter und analysieren und bewerten automatisch Artefakte, die möglicherweise in Zusammenhang mit Malware stehen.

Systeme möglichst nicht verändern

Ein solches Abbild sollte man nicht auf dem Zielsystem speichern, denn es gilt der Grundsatz, im Rahmen von Incident-Response-Maßnahmen das zu untersuchende System so wenig wie möglich zu verändern. Außerdem muss das Sicherheitsteam das zu untersuchende System als bereits kompromittiert erachten. Das Abbild gehört also auf einen externen Datenträger oder auf ein Netzlaufwerk. Bei einem großen Vorfall, bei dem mehrere Systeme betroffen sind, kann das erheblichen Aufwand bedeuten. Bei einigen Tools kann man deshalb die erstellten Abbilder direkt in die Cloud des Anbieters hochladen. In manchen Szenarien ist das die schnellste und effizienteste Möglichkeit, um viele Triage-Images gleichzeitig zu erstellen und zu sichern.

Tools für Incident Response und Forensik

Produktkategorie/Anbieter	Produkt	URL
Endpoint Detection and Response (EDR)		
CrowdStrike	CrowdStrike	https://www.crowdstrike.com/
Cybereason	Cybereason EDR	https://www.cybereason.com/platform/endpoint-detection-response-edr
Microsoft	Defender for Endpoint	https://www.microsoft.com/de-de/security/business/endpoint-security/microsoft-defender-endpoint
Palo Alto Networks	Cortex XSIAM	https://www.paloaltonetworks.de/cortex
SentinelOne	SentinelOne	https://de.sentinelone.com/
Trellix	Trellix EDR	https://www.trellix.com/de-de/products/edr/
Triage/Forensiksuite		
Autopsy	Autopsy	https://www.autopsy.com/
Belkasoft	Belkasoft	https://belkasoft.com/corporate-investigation-software
Exterro	FTK Forensic Tool Kit	https://www.exterro.com/digital-forensics-software/forensic-toolkit
Magnet Forensics	Magnet Axiom Cyber	https://www.magnetforensics.com/de/products/magnet-axiom-cyber
OpenText	EnCase Forensic	https://www.opentext.com/de-de/produkte/forensic
Oxygen Forensics	Oxygen Forensic Detective	https://www.oxygenforensics.com/en/products/oxygen-forensic-detective/
X-Ways	X-Ways Forensics	https://www.x-ways.net/forensics/index-d.html
Triage		
Binalyze	Binalyze	https://www.binalyze.com/
Cyber Triage	Cyber Triage	https://www.cybertriage.com/
Case Management		
CyberCPR	CyberCPR	https://www.cybercpr.com/
DFIR-IRIS	IRIS	https://www.dfir-iris.org/
Request Tracker	RTIR	https://requesttracker.com/rtir/
StrangeBee	TheHive	https://strangebee.com/thehive/
SOAR		
IBM	IBM QRadar SOAR	https://www.ibm.com/de-de/products/qradar-soar
Palo Alto Networks	Cortex XSOAR	https://www.paloaltonetworks.de/resources/datasheets/cortex-xsoar-overview
Splunk	Splunk SOAR	https://www.splunk.com/de_de/products/splunk-security-orchestration-and-automation.html
Imaging		
Exterro	FTK Imager	https://www.exterro.com/digital-forensics-software/ftk-imager
Sumuri	Paladin	https://sumuri.com/software/paladin/
Distribution		
CAINE	Lightstream	https://www.caine-live.net/
Mandiant	FLARE-VM	https://github.com/mandiant/flare-vm
REMnux	REMnux	https://remnux.org/
SANS	SIFT Workstation	https://www.sans.org/tools/sift-workstation/
Toolsammlung		
Eric Zimmerman	Zimmerman's Tools	https://ericzimmerman.github.io/#!index.md

Eine strukturierte Herangehensweise zur Bearbeitung von Sicherheitsvorfällen erfordert eine detaillierte und vollständige Dokumentation der Erkenntnisse, Absprachen und Maßnahmen während eines Vorfalls. Anerkannte Standards wie die Norm ISO 27035 (Information Technology – Information Security Incident Management) beschreiben, welche Informationen während eines Vorfalls zu erheben und festzuhalten sind. Die Norm schreibt dafür keine spezifischen Werkzeuge oder Technologien vor.

Abgestimmtes Vorgehen mit Case Management und SOAR

Für IR-Teams, die nur sehr selten Sicherheitsvorfälle bearbeiten, eignen sich im einfachsten Fall Excel-Tabellen, einfache Datenbankanwendungen oder ein bestehendes Ticketingsystem. Für mittlere und größere IR-Teams lohnt sich allerdings ein genauer Blick auf Case-Management-Plattformen und Werkzeuge für Security Orchestration, Automation and Response (SOAR).

Eine Case-Management-Plattform für Incident Response ist eine spezialisierte Anwendung als zentrale Schaltstelle für IR- und SOC-Teams, in der sich Sicherheitsvorfälle strukturiert erfassen, dokumentieren und nachverfolgen lassen. Jeder Sicherheitsvorfall wird als eigener „Case" angelegt und enthält alle relevanten Informationen zum Vorfall – wie ermittelte Indicators of Compromise (IoCs), Absprachen, Erkenntnisse aus Analysen, umgesetzte Maßnahmen und viele Metadaten. Außerdem lassen sich in einer solchen Plattform Aufgaben an Mitglieder des IR-Teams delegieren und nachverfolgen.

Manche Plattformen dienen nicht nur der Dokumentation, sondern bieten darüber hinaus Schnittstellen zu weiteren Diensten, die die erfassten IoCs bei Bedarf überprüfen können – zum Beispiel, ob eine bestimmte Datei bei Diensten wie VirusTotal bekannt ist oder ob eine IP-Adresse, Domain oder E-Mail-Adresse im Kontext anderer Vorfälle in Erscheinung getreten ist. Die Möglichkeiten der Integration sind je nach Plattform sehr umfangreich und reichen von Anbindungen an SOAR-Produkte und MISP Threat Intelligence Feeds (Malware Information Sharing Platform) bis hin zur Integration in EDR-Software.

SOAR-Werkzeuge helfen IR-Teams dabei, automatisch festgelegte Abläufe in

Play- oder Runbooks auszuführen. Dabei können diese Werkzeuge eigenständig Informationen einholen, Systeme bereinigen oder Accounts sperren. Bei manchen IR-Plattformen ist die Unterscheidung zwischen reiner Case-Management-Plattform und SOAR-Werkzeug nicht immer möglich, da manche beide Anforderungen abdecken.

Im Open-Source-Bereich gibt es sehr spannende und bewährte Werkzeuge, die insbesondere als Case-Management-Plattform dienen, darüber hinaus aber viele Möglichkeiten zur Integration in Drittanbieterprodukte und -dienste bieten. Beispiele sind DFIR-IRIS und TheHive in der Community-Variante.

Werkzeuge für Forensik

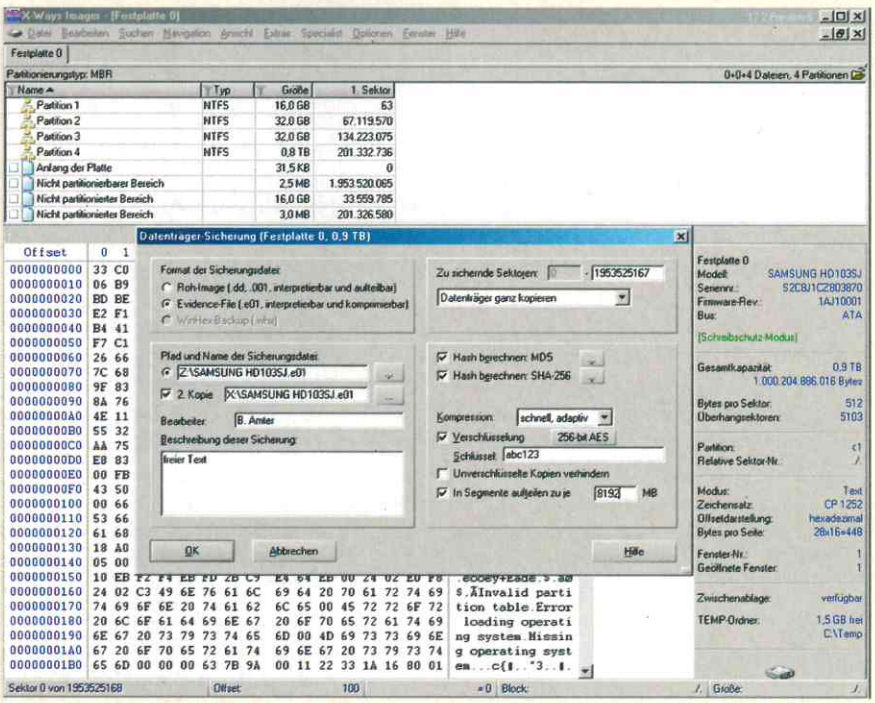
Eine weitere Aufgabe im Kontext der Vorfallsbehandlung besteht darin, zeitnah forensische Abbilder von Systemen zu erstellen, um sie später im Rahmen einer forensischen Analyse zu untersuchen. Im Wesentlichen gibt es zwei etablierte Verfahren dafür: Live Imaging und Dead Acquisition.

Die Methode Live Imaging sichert einen Datenträger im laufenden Betrieb. Aus forensischer Sicht ist das nicht die bevorzugte Variante, da während des Sicherungsvorgangs versehentlich Daten modifiziert oder gelöscht werden können. Außerdem entstehen durch das Ausführen des Werkzeugs zur Datensicherung ungewollt Spuren auf dem betroffenen System. In manchen Fällen ist diese Variante allerdings die einzig mögliche. Beispielsweise dann, wenn der zu sichernde Datenträger eine Festplattenverschlüsselung verwendet und der zugehörige Schlüssel nicht bekannt ist oder wenn die SSD fest verlötet wurde und deswegen nicht ohne Weiteres ausgebaut werden kann. Allerdings gibt es Werkzeuge, die diese Hürden beseitigen.

Für die Dead-Acquisition-Methode baut man den zu sichernden Datenträger aus dem System aus und klont ihn entweder mit einem Hardwareduplizierer oder schließt ihn mit einem Write-Blocker an eine Forensik-Workstation an und dupliziert ihn. Beide Möglichkeiten gewährleisten, dass der Originaldatenträger niemals verändert oder gelöscht werden kann. Der Hardwareduplizierer bringt alles mit, was der Forensiker benötigt. Auf der einen Seite steckt man den Originaldatenträger und auf der anderen Seite das Zielmedium ein. Eine Oberfläche auf dem Display des Duplizierers führt den Forensiker durch den Sicherungsvorgang, der nach und nach ein forensisches Abbild des Datenträgers erstellt. Sofern kein Hardwareduplizierer vorhanden ist, kann der Forensiker den Originaldatenträger an einen Write-Blocker anschließen und mit der Forensik-Workstation verbinden und dann das forensische Abbild erstellen.

Spätestens wenn es darum geht, einen Datenträger forensisch zu untersuchen, werden spezielle Werkzeuge benötigt. Andernfalls bleibt es bei der sprichwörtlichen Suche nach der Nadel im Heuhaufen. Jedes Betriebssystem speichert Informationen zu allen erdenklichen Vorgängen auf dem System an unterschiedlichen Orten. Für den Forensiker ist nicht nur entscheidend zu wissen, wo sich diese Artefakte befinden, sondern auch, wie man sie extrahiert und interpretiert. Tools helfen dabei, schnell und strukturiert einzelne für die jeweilige Untersuchung relevante Artefakte zu extrahieren und in einem lesbaren Format darzustellen. Forensiker können aus einer Fülle von Werkzeugen wählen, die dafür zur Verfügung stehen. Sie lassen sich prinzipiell in drei Kategorien einteilen: dezidierte Forensikdistributionen, komplette Forensiksuiten oder einzelne spezielle Werkzeuge, die dem Unix-Prinzip „One Tool for One Job“ folgen.

Die Distributionen enthalten eine Fülle an Werkzeugen, um direkt mit der Untersuchung zu beginnen. Der Forensiker muss sich keine Sorgen um Abhängigkeiten der einzelnen Werkzeuge machen. Die SIFT Workstation (SANS Investigative Forensic Toolkit) ist eine vom SANS Institute bereitgestellte Sammlung kostenloser und quelloffener Werkzeuge für



Quelle: X-Ways

Das Erstellen eines Festplattenabbilds – live oder bevorzugt am ausgebauten Datenträger – ist unumgänglich für eine forensische Untersuchung.

forensische Tätigkeiten. In Summe werden mehr als 150 Werkzeuge speziell für Forensik installiert.

Forensiksuiten sind Lösungen, die alle benötigten Werkzeuge für die forensische Analyse in einer integrierten Umgebung mit einheitlicher Oberfläche bereitstellen. Der Vorteil liegt auf der Hand: Der Analyst oder Forensiker muss sich nicht mit vielen unterschiedlichen Werkzeugen auseinandersetzen, sondern findet schnell an einer Stelle die Informationen, die für die Untersuchung relevant sind. Typischerweise verfügen diese Werkzeuge über Funktionen zum Erstellen von Abbildern, zur Analyse von Datenträgern und speziellen Artefakten sowie zum Anfertigen einer Zeitleiste.

Je nach Hersteller sind die Produkte teilweise sehr teuer und somit eher für größere IR-Teams, SOC-Anbieter oder Dienstleister im Bereich Incident Response und Forensik geeignet. In ihren Kernfunktionen ähneln sich die meisten Werkzeuge in dieser Kategorie. Manche Tools sind jedoch besonders leicht anzuwenden, während andere den Fokus auf die Zusammenarbeit im Team an einem Fall legen. Es lohnt sich, diverse Produkte zu evaluieren und anhand der eigenen Anforderungen und Wünsche zu vergleichen. Auch sind manche dieser Produkte vorwiegend auf die Analyse von Windows- und Linux-Systemen spezialisiert, während andere Hersteller den Fokus auf mobile Endgeräte legen.

One Tool for One Job

Unter dem bekannten Motto „One Tool for One Job" werden Tools zusammengefasst, die in der Regel nur eine einzige Aufgabe haben. Das zeigt auch schon ihre Problematik auf: Der Analyst muss wissen, in welchen Artefakten die gesuchten Informationen enthalten sind und mit welchen Werkzeugen er die gewünschten Artefakte auslesen kann. Für Forensikeinsteiger stellt das eine hohe Hürde dar. Experten hingegen können in vielen Fällen kleine spezielle Tools verwenden, um spezifische Aufgaben zu lösen. Wer sich darauf einlässt, eine der oben genannten Forensikdistributionen zu verwenden, wird automatisch viele dieser Werkzeuge kennenlernen.

In den vergangenen Jahren ist der Markt für Incident-Response- und Forensikprodukte stark gewachsen. Viele Produkte lassen sich nicht mehr so einfach in eine bestimmte Kategorie einordnen und erfüllen verschiedene Aufgaben. Wie in vielen anderen Bereichen kann ein Werkzeug nur dann gute Ergebnisse liefern, wenn der Anwender es sicher beherrscht und versteht, in welchem Fall welches Werkzeug am besten anzuwenden ist. Dies erfordert viel Erfahrung und Übung. Aktuelle Tools für Forensik erleichtern die Analyseaufgaben eines IR-Teams enorm. Mit den richtigen Werkzeugen in den richtigen Händen können Sicherheitsvorfälle schnell analysiert, bewertet und effizient behandelt werden. (ur@ix.de)

JOSHUA TIAGO

arbeitet als Leitender Berater bei der cirosec GmbH. Er leitet das IR-Team von cirosec und unterstützt Kunden bei der Bewältigung von Sicherheitsvorfällen.