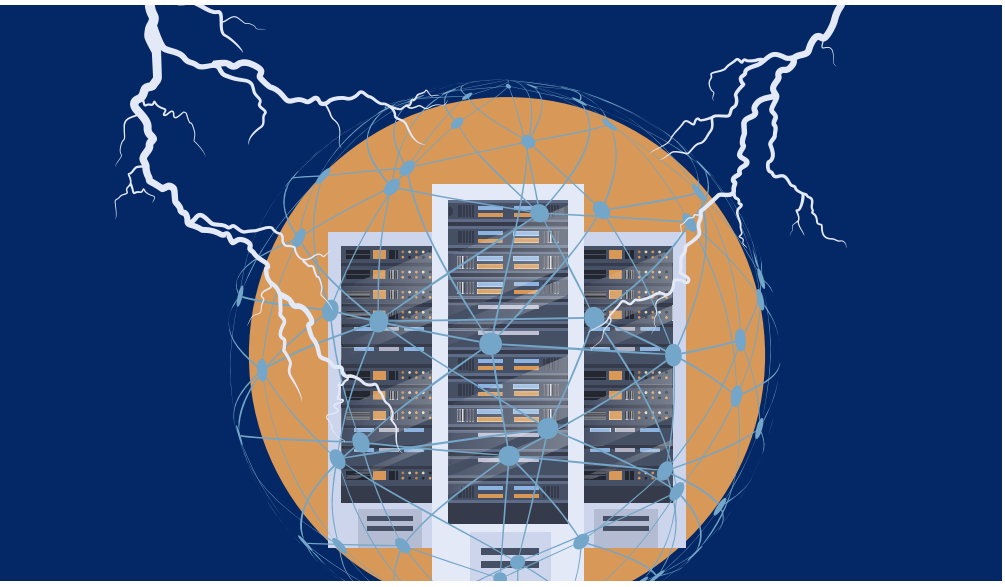


Gezielt verteidigen mit Threat-informed Defense

Um IT-Systeme besser zu schützen, müssen Unternehmen ihre Sicherheitsmaßnahmen auf die Methoden der Angreifer ausrichten. Threat-informed Defense macht die Verteidigung effizienter und die IT resilienter.

Von Timo Sablowski

Die IT-Sicherheit leidet oft an fehlender Fokussierung. Auch bei Unternehmen mit hohen Budgets für die IT- und Informationssicherheit und einem zertifizierten Information Security Management System (ISMS) kommt es immer wieder zu teilweise gravierenden Vorfällen. Das kann insbesondere bei Verantwortlichen ein Gefühl der Ohnmacht erzeugen. Häufig ignorieren sie dann das Problem oder schaffen breitflächig Produkte an, die mit Security als Schlagwort werben, in der Hoffnung, jedes erdenkliche Szenario abzusichern. Das ist nicht nur ineffizient, sondern für die meisten Unternehmen in der Praxis nicht umsetzbar. Ein sinnvollerer Ansatz beginnt mit einer realistischen Einschätzung der aktuellen Bedrohungslage und den folgenden Leitfragen:

- Für welche Angreifergruppen ist die Branche des zu schützenden Unternehmens relevant?
- Welche Angriffsvektoren setzen diese Angreifergruppen mit hoher Wahrscheinlichkeit ein?
- Wie lassen sich auf Basis dieser Erkenntnisse Abwehr- und Erkennungsmaßnahmen gezielt aufbauen?
- Wie kann das Unternehmen die vorhandenen Ressourcen möglichst effizient einsetzen?
- Sind die umgesetzten Maßnahmen effektiv?

Diese Fragen scheinen beim Blick auf die eigene IT- und Informationssicherheit selbstverständlich. Doch ist eine tiefer gehende Analyse der Branchenbedrohungen und eine Ableitung wahrscheinlicher Angriffsvektoren tatsächlich Bestandteil der Entscheidungskette, um Securitymaßnahmen umzusetzen? Das Vorgehensmodell bleibt in der Praxis aus Zeitmangel oder wegen fehlender Struktur auf der Strecke. Mit dem 2019 gegründeten Center for Threat-informed Defense hat MITRE dieses Vorgehen nicht nur formalisiert, sondern auch unterschiedlichste Werkzeuge bereitgestellt, um die einzelnen Schritte des Konzepts in beliebiger Tiefe umzusetzen.

iX-TRACT

- Der Threat-informed-Defense-Ansatz richtet die Sicherheitsmaßnahmen auf reale Bedrohungsvektoren aus.
- Er ergänzt vorhandene GRC-Prozesse (Governance, Risk, Compliance) um eine operative Ebene.
- Ein zentrales Element ist das MITRE-ATT&CK-Framework, das die Vorgehensweisen von Angreifern erfasst.

MITRE-ATT&CK-Framework gibt Überblick

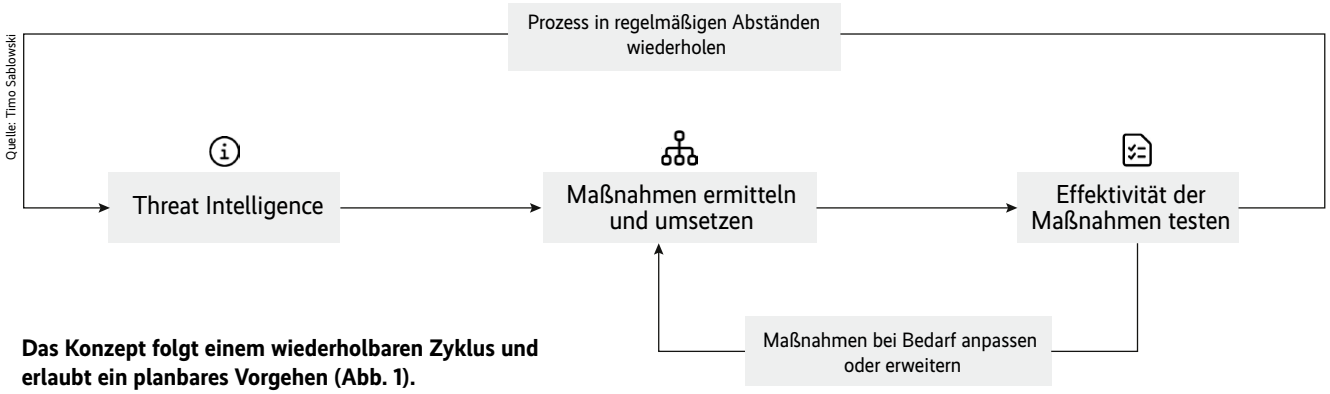
Bevor es an die Umsetzung von Threat-informed Defense geht, ist es sinnvoll, die Grundlagen für die Dokumentation und Beschreibung von Angriffsschritten zu verstehen. Hier setzt das in der IT-Sicherheitscommunity genutzte MITRE-ATT&CK-Framework an (siehe ix.de/z2vb). Es erfasst systematisch die Vorgehensweisen von Angreifern und bildet sie in TTPs (Tactics, Techniques and Procedures) ab. Ein definiertes TTP hat folgende Eigenschaften:

- Tactics beschreiben das Warum oder das Ziel einer Aktion, etwa den initialen Zugang zu einem IT-System, die Codeausführung oder die Datenexfiltration.
- Techniques beschreiben das Wie und erläutern, mit welchen Mitteln ein Ziel zu erreichen ist. Um einen initialen Zugang zu erhalten, lässt sich beispielsweise eine E-Mail mit schädlichem Anhang versenden.
- Procedures zeigen die konkrete Umsetzung der Techniken. Bei einem schädlichen Anhang kann es sich beispielsweise um einen Makrocode für ein Office-Dokument handeln.

Jedes TTP ist mit einer eindeutigen ID versehen, etwa T1059.001 für das Ausführen von PowerShell-Code. Diese Art der Kennzeichnung hat sich unter anderem in den Bereichen Red Teaming, Threat Intelligence, Incident Response und Detection Engineering zum Standard entwickelt, da sie ein gemeinsames technisches Vokabular schafft.

Die drei Schritte von Threat-informed Defense

Mit Threat-informed Defense lässt sich die IT-Sicherheit gezielt stärken. Dafür werden die notwendigen Maßnahmen an realen Bedrohungsvektoren ausgerichtet



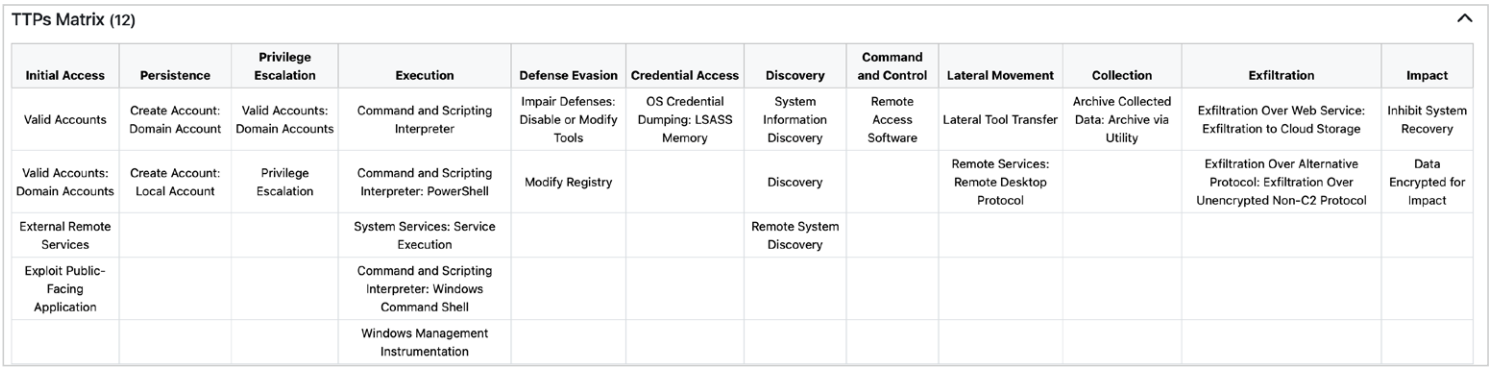
Das Konzept folgt einem wiederholbaren Zyklus und erlaubt ein planbares Vorgehen (Abb. 1).

und priorisiert. Die Vorgehensweise besteht aus drei Schritten: Threat Intelligence, Maßnahmen ermitteln und umsetzen sowie die Effektivität der umgesetzten Maßnahmen testen (Abbildung 1).

Die wichtigste Frage ist, gegen wen und was man seine Infrastruktur primär schützen möchte. Sie lässt sich auf mehreren Ebenen beantworten. Zunächst ermittelt man, was die größten Gefahren sind. Hierbei lohnt sich ein Blick auf die Lage der IT-Sicherheit auf globaler und lokaler Ebene. Publikationen wie „Die Lage der IT-Sicherheit in Deutschland“ des BSI oder der „Data Breach Investigations Report“ von Verizon zeigen gängige Bedrohungen auf (siehe ix.de/z2vb). Ransomwaregruppen oder andere offensichtlich finanziell motivierte Akteure verantworten den Großteil der bekannt gewordenen Angriffe auf IT-Infrastrukturen. Daher muss die Gefahr durch Ransomwareangriffe in der Regel immer in die weitere Betrachtung einfließen.

Dann ist zu fragen, für welche Akteure das zu schützende Unternehmen ein wahrscheinliches Ziel ist. Das ist individuell zu beantworten. Entscheidend sind folgende Aspekte: In welchen Branchen und in welchen Ländern ist das Unternehmen aktiv? Es ist ein Unterschied, ob das Unternehmen seinen Sitz und sein Geschäft in Westeuropa hat oder in Ländern wie Russland oder Nordkorea. Je nach geografischer Lage des Unternehmens und seiner Kunden haben unterschiedliche Angreifergruppen oder APTs (Advanced Persistent Threat) ein Interesse an der Kompromittierung der IT.

Weiterhin ist zu klären, ob das Unternehmen Teil einer Lieferkette für weitere Branchen ist. Üblicherweise gibt es Querverbindungen dorthin. Der Angriff auf die Südwestfalen-IT aus dem Jahr 2023 beispielsweise kompromittierte nicht nur die IT des IT-Dienstleisters, sondern hatte auch Auswirkungen auf die betreuten Kommunen. Ist ein Unternehmen Teil der Lieferkette für attraktivere Ziele, muss es diese Verbindung bei der Threat Intelligence betrachten.



TTPs Matrix (12)

Initial Access	Persistence	Privilege Escalation	Execution	Defense Evasion	Credential Access	Discovery	Command and Control	Lateral Movement	Collection	Exfiltration	Impact
Valid Accounts	Create Account: Domain Account	Valid Accounts: Domain Accounts	Command and Scripting Interpreter	Impair Defenses: Disable or Modify Tools	OS Credential Dumping: LSASS Memory	System Information Discovery	Remote Access Software	Lateral Tool Transfer	Archive Collected Data: Archive via Utility	Exfiltration Over Web Service: Exfiltration to Cloud Storage	Inhibit System Recovery
Valid Accounts: Domain Accounts	Create Account: Local Account	Privilege Escalation	Command and Scripting Interpreter: PowerShell	Modify Registry		Discovery		Remote Services: Remote Desktop Protocol		Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol	Data Encrypted for Impact
External Remote Services			System Services: Service Execution			Remote System Discovery					
Exploit Public-Facing Application			Command and Scripting Interpreter: Windows Command Shell								
			Windows Management Instrumentation								

Die von der Ransomwaregruppe Akira genutzten TTPs auf ransomware.live (Abb. 2).

Öffentlich zugängliche Quellen über Akteure und Vorgehensweisen

Liste der zehn häufigsten TTPs von Ransomwaregruppen:
center-for-threat-informed-defense.github.io/top-attack-techniques/#/top-10-lists

Gewichtung der wahrscheinlichsten TTPs anhand einer Schnelleinschätzung:
center-for-threat-informed-defense.github.io/top-attack-techniques/#/calculator

In Deutschland aktive APT-Gruppen mit Zielbranchen:
www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive_APT-Gruppen/aktive-apt-gruppen_node.html

In Deutschland aktive Cybercrimegruppen:
www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive-Crime-Gruppen/aktive-crime-gruppen_node.html

CISA-Warnungen: www.cisa.gov/news-events/cybersecurity-advisories

Beschreibung der Vorgehensweisen bekannter Cybercrimegruppen und APTs:
attack.mitre.org/groups/

Statistiken über Ransomwaregruppen und ihre Vorgehensweisen (Abbildung 2):
www.ransomware.live

Alle Links finden sich unter ix.de/z2vb.

Anhand dieser Informationen erstellt das Sicherheitsteam eine Liste von Akteuren, die für Angriffe auf IT-Infrastrukturen in diesen Bereichen bekannt sind. Zusätzlich lassen sich bei Bedarf individuelle Bedrohungen und bereits gemachte Erfahrungen mit vergangenen Angriffen auf Unternehmen in derselben Branche und auf Konkurrenten heranziehen, um das Bedrohungsprofil weiter zu individualisieren.

Diese Fragen bilden die Grundlage für die Recherche nach häufigen Angriffsvektoren, möglichen Akteuren und deren Vorgehensweisen. Hierzu lassen sich öffentlich Quellen nutzen (siehe Kasten „Öffentlich zugängliche Quellen über Akteure und Vorgehensweisen“). Hinzu kommen frei verfügbare Veröffentlichungen von Securityforschern und -firmen wie Sophos und Qualys sowie öffentliche und kostenpflichtige Threat-Intelligence-Plattformen.

Sind die Recherchen abgeschlossen, konsolidiert das Team die von den Akteuren genutzten TTPs. Für eine bessere Übersicht ist es hilfreich, mehrere Cluster zu erstellen (Ransomwaregruppen, branchenspezifische Bedrohungen et cetera).

Eine grafische Visualisierung macht das Ganze übersichtlicher. MITRE stellt hierfür das Tool MITRE ATT&CK Navigator zur Verfügung. Dabei können TTPs eine Gewichtung erhalten – beispielsweise weil besonders viele Gruppen sie verwenden – und in Abgrenzung zu anderen TTPs farbig dargestellt werden.

Abbildung 3 zeigt eine Analyse von fünf in Deutschland aktiven Ransomwaregruppen in einer Heatmap. Die TTPs sind in einem Farbverlauf von Rot über Orange nach Grün nach der Häufigkeit ihres Auftretens bei unterschiedlichen Gruppen eingefärbt. Rote Markierungen zeigen eine häufige und grüne Markierungen eine seltenere Nutzung an. Die ausgegrauten Felder beschreiben die übergeordneten, nur in ihren jeweiligen Subtechniken verwendeten TTP-Kategorien.

Maßnahmen ermitteln und umsetzen

Sind die für den Unternehmenskontext relevanten TTPs und ihre Häufigkeit bekannt, leitet man daraus Priorisierungen für Verteidigungsmaßnahmen ab. Sie unterscheiden sich je nach Infrastruktur und Geschäftsmodell. Die naheliegendste Variante ist, sich zuerst um die TTPs zu kümmern, die am häufigsten auftreten. Eine weitere und in der Praxis häufig genutzte Form besteht darin, zunächst die übergeordneten Taktiken (erste Zeile in Abbildung 3) zu gewichten und anschließend in diesen Gruppen die TTPs nach Häufigkeit zu priorisieren.

Ein Beispiel: Bei vielen Unternehmen sind am Perimeter verschiedene Securityprodukte im Einsatz, die Angriffe erkennen. Auch die Detektion der Ausführung von Schadcode und die Auswirkungen eines Angriffs (etwa durch Verschlüsselung) sind elementar. Für die ermittelten TTPs der Ransomwaregruppen setzt das Securityteam daher den Schwerpunkt auf die Taktiken Initial Access, Execution, Exfiltration und Impact (Abbildung 4).

Die Schwerpunktgruppen und die darin ermittelten TTP-Häufigkeiten bestimmen nun die Priorität der zu behandelnden TTPs (siehe Tabelle „Priorisierte TTPs“). Für jedes TTP wird ermittelt, welche vorhandenen oder potenziellen Maßnahmen die Nutzung erkennen und

wenn möglich verhindern können. Dabei ist zu beachten, dass selten eine einzelne Maßnahme ausreicht, sondern eine Schichtung mehrerer technischer und organisatorischer Maßnahmen einen höheren Sicherheitsgewinn bringt. Bei der Auswahl geeigneter Maßnahmen hilft die MITRE-D3FEND-Matrix. Das D3FEND-Projekt ist nicht nur eine Sammlung von Sicherheitsmaßnahmen, sondern unterstützt auch dabei, diese ähnlich wie das ATT&CK-Framework zu kategorisieren und mit TTPs aus dem ATT&CK-Framework zu verknüpfen. Die genannten Maßnahmen scheinen zwar abstrakt, bieten aber eine Anlaufstelle für die Recherche, um die Maßnahme in der Unternehmensumgebung umzusetzen.

Für das erste TTP der Prioritätstabelle (T1190 – Exploit Public-Facing Application) liefert D3FEND die in Abbildung 5 gezeigten Detektionsoptionen (siehe auch die MITRE-D3FEND-Seite unter ix.de/z2vb). Ein Klick auf die einzelnen Maßnahmenoptionen (blaue Kästen) führt zur Erklärung und zu möglichen Implementierungsoptionen.

Die Auflistungen aus dem D3FEND-Framework sind nicht abschließend und beschreiben in erster Linie technische Möglichkeiten. Ein Blick auf weitere gängige technische und organisatorische Securitymaßnahmen ist daher lohnenswert.

Um das Beispiel T1190 – Exploit Public-Facing Application fortzuführen, helfen auch folgende technische und organisatorische Maßnahmen:

- eine AV- oder EDR-Lösung einsetzen;
- ein Patch-Management-Konzept umsetzen;
- ein Schwachstellenmanagementkonzept verwenden;
- Attack-Surface-Management;
- exponierte Systeme und Dienste reduzieren;
- Application-Layer-Firewalls nutzen;
- IDS- und IPS-Systeme;
- Pentesting exponierter Systeme.

Für die Behandlung einer einzelnen Vorgehensweise von Angreifern kommen mehrere technische und organisatorische Konzepte infrage. In der Praxis hat eine umgesetzte Maßnahme nicht nur Einfluss auf eines, sondern wahrscheinlich auf mehrere TTPs gleichzeitig. So ist ein AV- oder EDR-Produkt nicht nur bei T1190 (Exploit Public-Facing Application), sondern auch bei TTPs wie T1059.001 (PowerShell) und T1486 (Data Encrypted for Impact) ein wichtiger Baustein. Mögliche Maßnahmen und die jeweiligen TTPs sind zur besseren Übersicht in einer Tabelle als Matrix verknüpft. Besonders wirksame Maßnahmen, die gegen mehrere TTPs wirken, werden bei der Umsetzung priorisiert.

Effektivität der umgesetzten Maßnahmen testen

Jede umgesetzte Maßnahme muss ihre Wirksamkeit unter Beweis stellen. TTPs mit einem oder mehreren implementierten Mechanismen werden gezielt simuliert und gegen die eigene Infrastruktur getestet. Solche Simulationen erfolgen je nach Intensität und Testtiefe sowohl automatisiert als auch manuell.

Priorisierte TTPs

ID	Name
T1190	Exploit Public-Facing Application
T1059.001	PowerShell
T1486	Data Encrypted for Impact
T1566	Phishing
T1047	Windows Management Instrumentation
T1567.002	Exfiltration to Cloud Storage
…	…

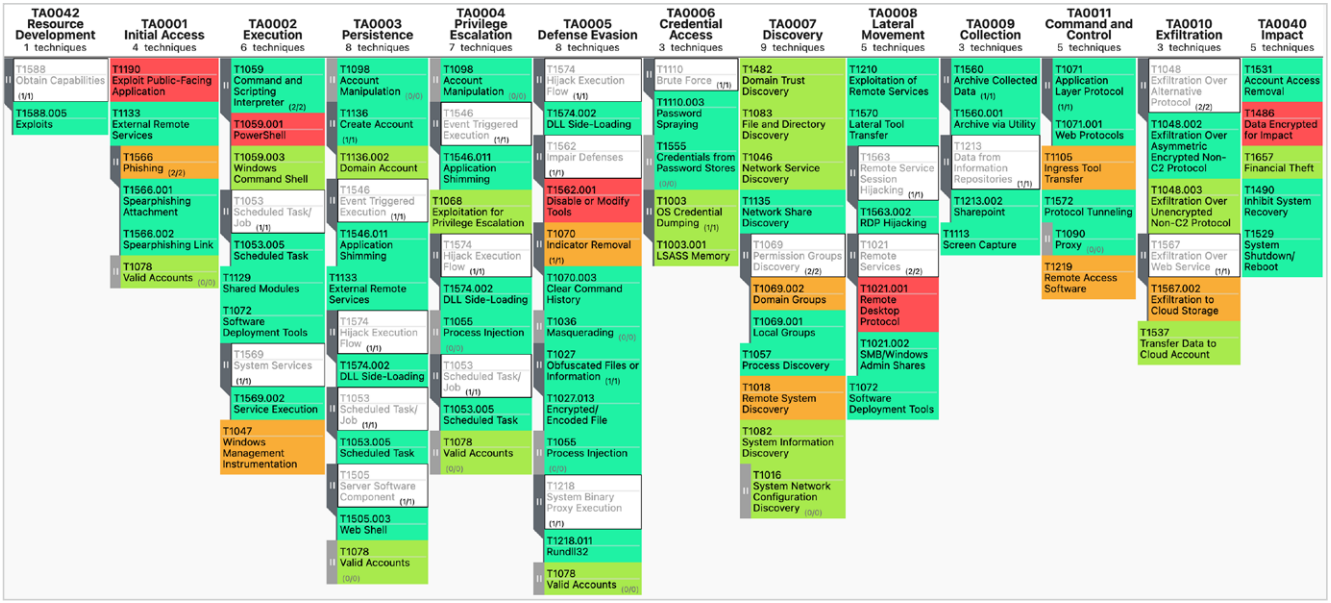
Mögliche Testmethoden können klassische Penetrationstests, Breach-and-Attack-Simulationen, Red-Team-Assessments oder Purple-Team-Übungen sein, bei denen Angreifer und Verteidiger eng zusammenarbeiten. Das Ziel ist, die Erkennungs- und Reaktionsfähigkeit möglichst realitätsnah zu testen. Für die automatisierte Simulation von TTP-Tests gibt es neben kommerziellen auch Open-Source-Produkte. Atomic Red Team von Red Canary liefert Testfälle für viele TTPs.

Als Beispiel dient ein Test, der prüft, ob das TTP T1059.001 – PowerShell wie gewünscht erkannt wird. Hierzu führt der Tester PowerShell-Code in der Kommandozeile aus (siehe Listing).

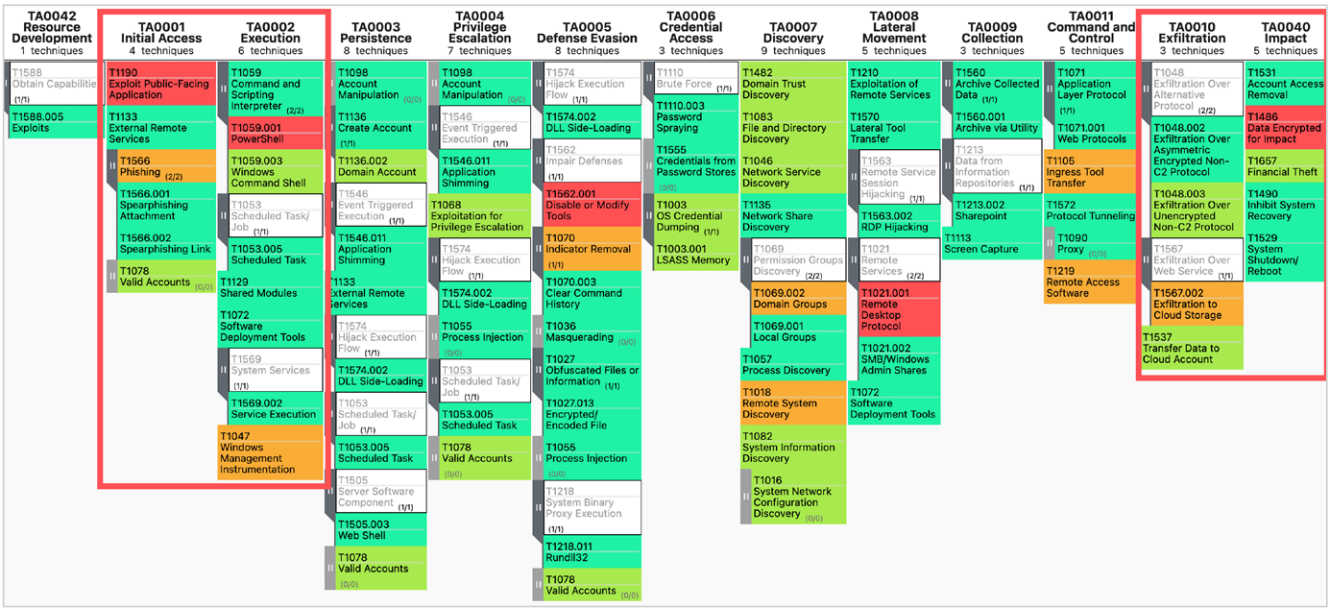
Der Base64-codierte String lautet decodiert

```
& (gcm ('ie{0}' -f 'x'))
("Wr"+"it"+"e-H"+"ost 'H"+"el"+"lo,
fr"+"om P"+"ow"+"erS"+"h"+"ell!'")
```

und gibt bei erfolgreicher Ausführung `Hello, from PowerShell!` auf der Kon-



Heatmap der genutzten TTPs: Die Farben geben die Häufigkeit des Auftretens an; Rot zeigt eine häufige Nutzung und Grün eine seltene (Abb. 3).



Die Priorisierung der Maßnahmen zur Erkennung und zum Schutz liegt auf definierten Taktiken (Abb. 4).

sole aus (Abbildung 6). Nun überprüft der Tester, ob die für dieses TTP implementierten Maßnahmen – etwa eine Weiterleitung des Logeintrags an ein SIEM – korrekt funktionieren.

Die Kombination einzelner Tests bildet eine Testkaskade, um nicht nur einzelne TTPs, sondern auch Teilschritte von Angriffsmustern zu simulieren. So kann ein PowerShell-Skript, das alle DOCX-Dateien auf einem System sucht und in Google Drive überträgt, mehrere TTPs auf einmal testen: T1059.001 – PowerShell, T1005 – Data from Local System und T1567 – Exfiltration Over Web Service.

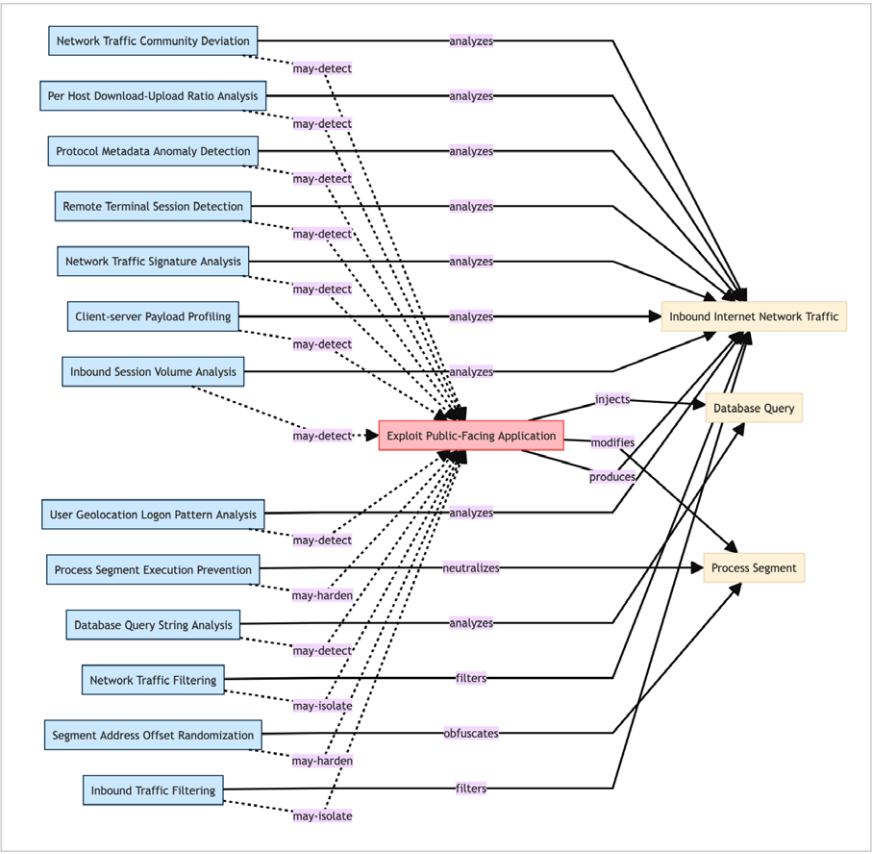
Die Tests helfen nicht nur dabei, Lücken in der Erkennung zu identifizieren, sondern offenbaren auch die operative Reife. Sie zeigen, ob das Zusammenspiel der eingesetzten Technik, der definierten Reaktionsprozesse und der verantwortlichen Personen im Ernstfall funktioniert.

Integration in GRC-Prozesse

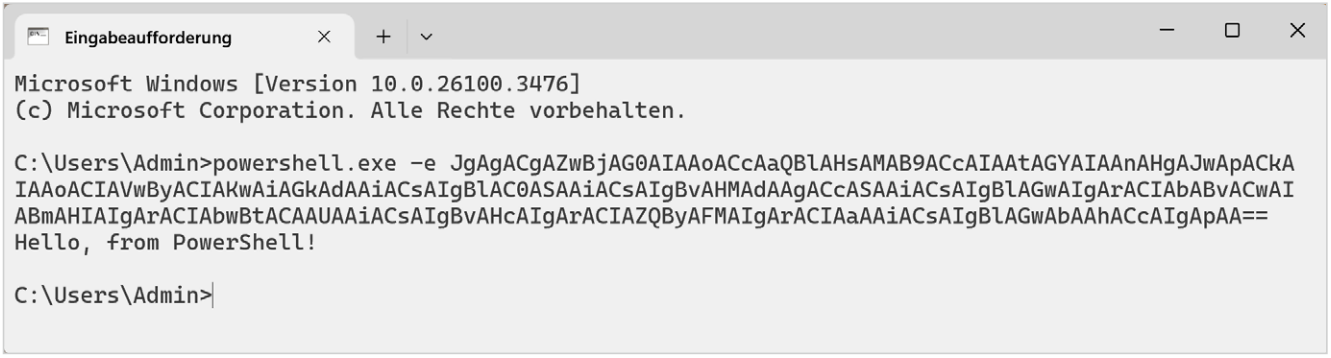
Threat-informed Defense ist mehr als nur ein technisches Konzept. Es ergänzt die üblichen und bereits etablierten GRC-Prozesse (Governance, Risk, Compliance) um eine operative und messbare Ebene und reichert Risiken und abstrakte Gefährdungen wie „Unbefugtes Eindringen in IT-Systeme“ aus dem IT-Grundschutz um konkrete Szenarien an. Die vorausgegangene Threat Intelligence hat die Eintrittswahrscheinlichkeit eines bestimmten Angriffsmusters bereits ermittelt. Zudem wird die Effektivität von Maßnahmen messbar und bestimmt dadurch eine nachvollziehbare und kontinuierliche Verbesserung im PDCA-Zyklus. Auch bei Audits entsteht dadurch ein nachvollziehbarer Nachweis über Risikoidentifikation, Maßnahmenumsetzung und deren Überprüfung.

Threat-informed Defense lädt zur Messbarkeit ein. Kennzahlen (KPIs) bieten einen Anhaltspunkt für die immer wieder auftauchende Frage der Geschäftsführung nach der Sicherheit des Unternehmens. Um diese Frage zu beantworten, sind die folgenden KPIs hilfreich:

- TTP-Abdeckungsgrad: Anteil der TTPs, für die bereits Maßnahmen existieren;
- Detektionsrate pro TTP: Anteil der durch Securitymaßnahmen erfolgreich erkannten Testfälle;



Mögliche Varianten, den Exploit-Versuch eines exponierten Systems zu erkennen (Abb. 5).



Das ausgeführte PowerShell-Kommando fungiert als Test für T1059.001 (Abb. 6).

- Mean Time to Detect (MTTD): Zeitraum zwischen Ausführen und Erkennen des TTP;
- Mean Time to Respond (MTTR): Zeitraum zwischen Erkennen einer Ausführung und einer Reaktion;
- Maßnahmenumsetzungsgrad: der Anteil der umgesetzten Maßnahmen pro TTP;
- Detektion versus Abwehr: Verhältnis zwischen erkannten und vereitelten TTP-Ausführungen.

Fazit

Threat-informed Defense ist nicht nur eine Methode zum Priorisieren technischer und organisatorischer Maßnahmen. Sie bietet auch einen strukturierten Ansatz, um Entscheidungen über Sicherheitsstrategien und -maßnahmen anhand von Wissen über reale Angriffe zu treffen und zu untermauern. Auch die Wirksamkeit der Abwehrmöglichkeiten ist dadurch messbar. Ein Mehrwert liegt darin, relevante KPIs abzuleiten.

Die Vorgehensweise ergänzt zudem das Risikomanagement durch eine realitätsnahe Ebene. Anstatt generische Risikoeinschätzungen vorzunehmen, lassen sich konkrete Angriffsszenarien modellieren und mit Verteidigungsfähigkeiten abgleichen. Diese bilden im Idealfall eine Entscheidungsgrundlage für Investitionen, Priorisierungen und Kontrollmaßnahmen.

Threat-informed Defense setzt allerdings einen gewissen organisatorischen und technischen Reifegrad voraus. Wenn bereits die grundlegende IT-Hygiene nicht gewährleistet ist, sollten Unternehmen zuerst die bekannten und offensichtlichen Probleme beheben. (nb@ix.de)

Quellen

MITRE-ATT&CK-Framework,
Data Breach Investigations Report,
Links zu Akteuren und Vorgehensweisen: ix.de/z2vb

Listing: Test zum Erkennen von TTP T1059.001 – PowerShell

```
powershell.exe -e JgAgACgAZwBjAG0AIAAoACcAaQBlAHsAMAB9ACcAIAAtAGYAIAAnAHgAJwApAC
kAIAAoACIAVwByACIAKwAiAGkAdAAiACsAIgBlAC0ASAAiACsAIgBvAHMAdAAgACcASAAiACsAIgBlAG
wAIgArACIAbABvACwAIABmAHIAIgArACIAbwBtACAAUAAiACsAIgBvAHcAIgArACIAZQByAFMAIgArAC
IAaAAiACsAIgBlAGwAbAAhACcAIgApAA==
```

TIMO SABLOWSKI

ist IT-Sicherheitsberater mit langjähriger Erfahrung in offensiver und defensiver Security. Er hilft Unternehmen bei der strategischen und technischen Weiterentwicklung ihrer Sicherheit.