Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Generalsekretariat

Nationales Zentrum für Cybersicherheit NCSC
www.ncsc.admin.ch

NCSC

Allgemeine Bedrohungsformen, Täter und Werkzeuge

Inhaltsverzeichnis

1 Vorwort

Das Dokument vermittelt eine Übersicht über die gängigen Bedrohungsformen und deren Einstufung sowie die Art der Täter, welche hinter diesen Bedrohungen stehen.

2 Bedrohungen

Die Bedrohungen, welche aus dem Internet auf Privatpersonen, private und öffentliche Organisationen wirken, sind sehr vielfältig. Eine grobe Kategorisierung kann durch eine Pyramidenform veranschaulicht werden.

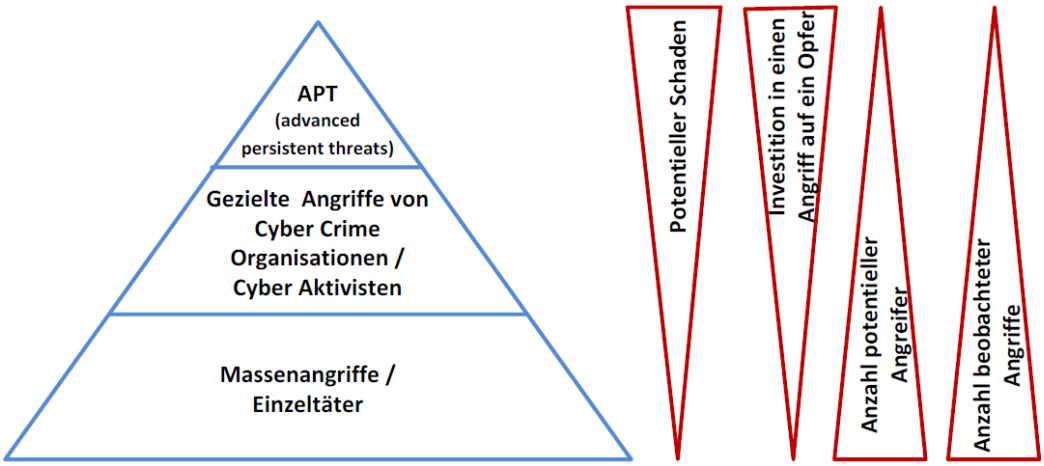

Abbildung 1: Vereinfachte Darstellung der Bedrohungspyramide nach SANS[1], RecordedFuture[2]

An der Spitze der Pyramide finden sich die APTs (Advanced Persistent Threat). Diese Bedrohung führt potentiell zu einem sehr hohen Schaden, der auf eine einzelne Organisation oder im politischen Kontext auf die Sicherheitsinteressen ganzer Staaten wirkt. Der Angreifer ist bereit, sehr viel Zeit, Geld und Wissen in den Angriff zu investieren und verfügt in der Regel über grosse Ressourcen. Das Ziel des Angreifers ist es dabei häufig, möglichst lange unentdeckt zu bleiben und sich im Netz des Opfers festzusetzen und so laufend an die für ihn interessanten Informationen zu gelangen. In seltenen Fällen kommt es auch zu Sabotage (-versuchen). Es gibt aufgrund der hohen Anforderung an die Ressourcen und Fähigkeiten eine limitierte, aber ständig wachsende Anzahl Angreifer dieser Kategorie.

In der Mitte der Pyramide liegen die Kategorien der Cyberkriminellen sowie der Cyberaktivisten. Auch wenn diese im Normalfall über geringere Ressourcen verfügen, darf die Gefährdung nicht unterschätzt werden. In der Regel sind sowohl die Zielauswahl, als auch die Hartnäckigkeit der Angreifer geringer als bei APTs . Zu beachten ist, dass die Grenzen zwischen organisierter Cyber Kriminalität und APT fliessend sind. Auch staatliche Angreifer dürften Angebote auf dem Cybercrime-Markt nutzen, um die gewünschte Ziele zu erreichen. Zudem erteilen staatliche Akteure auch Aufträge an cyberkriminelle Organisationen, um bei einer Aufdeckung ihre Beteiligung erfolgreich abstreiten zu können.

Die unterste Stufe der Pyramide wird durch opportunistische Massenangriffe sowie durch Einzeltäter gebildet. Trotz der limitierten Ressourcen, die dafür eingesetzt werden, ist diese Bedrohung alleine durch die enorme Menge an solchen Angriffen ernst zu nehmen.. Auch hier ist die Grenze zur oberen Stufe durchlässig, da insbesondere Massenangriffe häufig durch

[1] www.sans.org

[2] https://www.recordedfuture.com/assets/prioritizing-cyber-threats-1.png

cyberkriminelle Organisationen durchgeführt oder zumindest beauftragt werden. Die Durchlässigkeit zwischen den einzelnen Stufen zeigt auch, dass der Untergrundmarkt arbeitsteilig organisiert ist im Sinne eines klassischen Nachfrage- und Angebotsmarkt.

3 Typisierung von Angreifern

Im Folgenden werden Angreifer auf ihre Möglichkeiten und ihre Motivation hin eingeordnet. Diese Zusammenstellung dient der Einordnung, welche Ziele ein Angreifer mit welchen Ressourcen und welcher Hartnäckigkeit verfolgen könnte. Es handelt sich um eine grobe Annäherung ohne Anspruch auf Vollständigkeit.

3.1 Advanced Persistent Threats (APTs)

Name	Staatliche Akteure / Advanced Persistent Threats /
Beschreibung	Staaten oder Akteure mit meistens staatlichem Bezug treten als Angreifer auf oder geben den Angriff in Auftrag. In der Regel bezwecken diese Angriffe die Informationsbeschaffung im Bereich der klassischen Spionage oder der Industriespionage. In Zeiten erhöhter politischer Spannungen oder Krisen kann es auch zu Angriffen auf kritische Infrastrukturen oder zu gezielter Desinformation kommen.
Motivation	Informationsgewinnung, Störung kritischer Infrastrukturen, Beeinflussungsoperationen
Technische Ressourcen	Staaten oder Akteure mit staatlichem Bezug dürften über alle notwendigen technischen Fähigkeiten verfügen. Die Verfügbarkeit von Ressourcen ist als sehr hoch einzustufen. Gleichzeitig stehen Spezialisten für verschiedenste Arbeiten zur Verfügung bzw. können innert nützlicher Frist rekrutiert werden.
Finanzielle Ressourcen	Sehr hoch, so lange aus Sicht des Angreifers das zu erwartende Ergebnis des Angriffes den Einsatz der finanziellen Ressourcen rechtfertigt.
Rationales Vorgehen	Hoch
Hartnäckigkeit	Hoch
Ansatzpunkte für die Verteidigung	• Investitionen (auch personeller Art) in die Detektion • Erhöhung der Sichtbarkeit auf Endgeräten • Segmentierung und Überwachung der Netze und aller Systeme • Schutz des Active Directories • Einsatz von Werkzeugen wie Applocker, nur signierte Makros ausführen • Zentrale Security Gateways, über die sämtlicher Traffic fliessen muss • Blockierung von gefährlichen Dateitypen auf Gateways • Trennung von heiklen Aufgaben und Surfen / Mailen • Durchgehende ZweiFaktoren-Authentisierung • Zeitnahes und überwachtes Patchmanagement • Wirksames Backup- / Recovery-Konzept mit Offline- und Offsite-Backups in mehreren Generationen

Ansatzpunkte für die Verfolgung	Detaillierte Analyse der Angriffe, um die Attribution zu ermöglichen; international koordinierte Ermittlungen sind notwendig. Diese können von politischen Interessen beeinflusst werden.
Widerstandsfähigkeit gegen Strafverfolgung	Sehr hoch
Wahrscheinliche Angriffsziele	• Systeme mit schützenswerten Informationen • Geschäftskritische Informationen • Systeme von Schlüsselpersonen oder Entscheidungsträgern • Hintertüren in unauffälligen Systemen, die nur schwer entdeckt werden können • Gezielte Angriffe auf die Vertraulichkeit und Integrität von Systemen. • Angriffe auf die Verfügbarkeit kritischer Systeme, im Falle von erhöhten politischen Spannungen oder Krisen. • Kritische Infrastrukturen

3.2 Cyberkriminelle Organisationen – gezielte Angriffe

Name	Cyberkriminelle Organisationen – gezielte Angriffe
Beschreibung	Cyberkriminelle Organisationen können gezielte Angriffe durchführen, die nahe an einen APT heran kommen. Sie können staatliche oder private Organisationen angreifen, mit dem Ziel Informationen zu beschaffen, um diese weiterzuverkaufen oder zu ihrem Vorteil zu nutzen. Sehr häufige Ziele sind dabei Finanztransaktionssysteme. Ein gutes Beispiel sind die Angriffe auf Bankomatensteuerungen (ATM-Cashouts). Angriffe mit Verschlüsselungstrojaner sind aus Angreifersicht finanziell sehr lukrativ, weshalb sich in letzter Zeit eine Verschiebung zu solchen Angriffen beobachten lässt. Die Angreifer kopieren die Daten vor der Verschlüsselung und drohen mit dem Verkauf dieser Daten, falls das geforderte Lösegeld nicht bezahlt wird.
Motivation	Erpressung, Informationsbeschaffung und -verkauf (Industriespionage), Nutzung von Finanztransaktionssystemen für eigene Zwecke.
Technische Ressourcen	Je nach Organisation mittel bis hoch
Finanzielle Ressourcen	Je nach Organisation mittel bis joch
Rationales Vorgehen	Hoch
Hartnäckigkeit	Mittel
Ansatzpunkte für die Verteidigung	• Investitionen (auch personeller Art) in die Detektion • Erhöhung der Sichtbarkeit auf Endgeräten • Segmentierung und Überwachung der Netze und aller Systeme • Schutz des Active Directories • Einsatz von Werkzeugen wie «Applocker», nur signierte Makros ausführen • Zentrale Security Gateways, über die sämtlicher Traffic fliessen muss • Blockierung von gefährlichen Dateitypen auf Gateways • Trennung von heiklen Aufgaben und Surfen / Mailen

	• Durchgehende Zwei-Faktoren-Authentisierung. • Zeitnahes und überwachtes Patchmanagement • Wirksames Backup- / Recovery- Konzept mit Offline- und Offsite- Backups in mehreren Generationen
Ansatzpunkte für die Verfolgung	Analyse der verwendeten Angriffswerkzeuge und -Infrastruktur, enge Zusammenarbeit mit zuständigen Polizeiorganisationen und Nachrichtendiensten. Beobachten der aktuellen cyberkriminellen Organisationen.
Widerstandsfähigkeit gegen Strafverfolgung	Mittel bis hoch. Eine Strafverfolgung stört jedoch die Aktivitäten der Angreifer, weshalb diese versuchen, unter dem Radar von Strafverfolgungsbehörden zu bleiben
Wahrscheinliche Angriffsziele	• Systeme mit hohen Verfügbarkeitsanforderungen • Systeme mit vertraulichen Informationen, die einen hohen Wiederverkaufswert haben • Systeme mit Finanzinformationen

3.3 Cyberkriminelle Organisationen – opportunistische Angriffe

Name	Cyberkriminelle Organisationen, opportunistische und nicht gezielte Angriffe
Beschreibung	Dies ist Cyberkriminalität in ihrer klassischen Form. Die Angreifer versuchen, aus dem Angriff auf Endbenutzergeräte finanziellen Gewinn zu generieren. Sie versuchen beispielsweise, Zugangsdaten zu erlangen, Opfer mit DDoS- Angriffen zu erpressen oder über infizierte Geräte Spam zu verschicken. Dazu dienen häufig «Crimeware as a Service»-Dienstleistungen , welche im Schwarzmarkt gehandelt werden
Motivation	Ausschliesslich finanziell
Technische Ressourcen	Mittel, häufig werden Angriffskomponenten als «Crimeware as a Service» eingekauft
Finanzielle Ressourcen	Mittel bis hoch
Rationales Vorgehen	Hoch
Hartnäckigkeit	Tief gegen ein einzelnes Ziel
Ansatzpunkte für die Verteidigung	• Investitionen (auch personeller Art) in die Sicherheit • Einsatz von Security Gateways, Blockierung von gefährlichen Dateitypen auf Gateways • Trennung von heiklen Aufgaben und Surfen / Mailen • Zwei-Faktoren-Authentisierung für alle vom Internet her zugänglichen Ressourcen • Zeitnahes und überwachtes Patchmanagement • Wirksames Backup- / Recovery-Konzept mit Offline- und Offsite-Backups in mehreren Generationen
Ansatzpunkte für die Verfolgung	Sinkholing von entsprechenden Domains, die für cyberkriminelle Organisationen verwendet werden. Analyse der Infrastruktur sowie der verwendeten Angriffswerkzeuge. Analyse und Verhinderung der entsprechenden Geldflüsse.
Widerstandsfähigkeit gegen Strafverfolgung	Mittel bis hoch. Die internationale Anlage der meisten Vorfälle erschwert effiziente Ermittlungen

Wahrscheinliche Angriffsziele	• Schlecht geschützte Endbenutzergeräte • E-Banking-Applikationen

3.4 Hacktivisten

Name	Hacktivisten, Cyberaktivisten
Beschreibung	Cyberaktivisten protestieren mit digitalen Mitteln gegen Entscheidungen von Regierungen oder Firmen, die nicht mit ihren politischen und gesellschaftlichen Interessen übereinstimmen. Beispiele für solche Gruppierungen sind «Anonymous» oder «LULZ».
Motivation	Verbreitung eigener Aussagen und Anstossen von Diskussionen, Erlangen von Aufmerksamkeit und/oder Zufügen von Schaden.
Technische Ressourcen	Die technischen Ressourcen und Fähigkeiten variieren sehr stark. Im Falle von grossen Aktionen mit hohem Aufmerksamkeitsgrad können diese jedoch sehr beträchtliche Ausmasse annehmen.
Finanzielle Ressourcen	Limitiert, aber nicht von grosser Bedeutung für den Angreifer, weil diese Aktivitäten in der Regel auf freiwilliger Basis geschehen..
Rationales Vorgehen	Tief bis Mittel, abhängig von der Organisationform der Gruppierung.
Ausdauer	Mittel
Ansatzpunkte für die Verteidigung	• Investitionen (auch personeller Art) in die Sicherheit • Einsatz von Security Gateways, Blockierung von gefährlichen Dateitypen auf Gateways • Trennung von heiklen Aufgaben und Surfen / Mailen • Zwei-Faktoren-Authentisierung für alle vom Internet her zugänglichen Ressourcen • Zeitnahes und überwachtes Patchmanagement Wirksames Backup- / Recovery-Konzept mit Offline- und Offsite-Backups in mehreren Generationen
Ansatzpunkte für die Verfolgung	Zusammenarbeit mit Polizeiorganisationen sowie mit Nachrichtendiensten.
Widerstandsfähigkeit gegen Strafverfolgung	Mittel
Wahrscheinliche Angriffsziele	• Systeme mit hoher Sichtbarkeit/Aufmerksamkeit • Verfügbarkeit von Systemen (DDoS), Integrität (Defacements von Websites)

3.5 Einzeltäter

Name	Einzeltäter
Beschreibung	Der Einzeltäter handelt auf eigene Faust, mit limitierten Mitteln.
Motivation	individuell verschieden
Technische Ressourcen	Tief
Finanzielle Ressourcen	Tief

Rationales Vorgehen	individuell verschieden
Ausdauer	Tief bis hoch, je nach Angreifer
Ansatzpunkte für die Verteidigung	• Investitionen (auch personeller Art) in die Sicherheit • Einsatz von Security Gateways, Blockierung von gefährlichen Dateitypen auf Gateways • Trennung von heiklen Aufgaben und Surfen / Mailen • Zwei-Faktoren-Authentisierung für alle vom Internet her zugänglichen Ressourcen • Zeitnahes und überwachtes Patchmanagement • Wirksames Backup- / Recovery-Konzept mit Offline- und Offsite-Backups in mehreren Generationen
Ansatzpunkte für die Verfolgung	Normale, strafrechtliche Verfolgung
Widerstandsfähigkeit gegen Strafverfolgung	Tief
Wahrscheinliche Angriffsziele	• Schwach geschützte Systeme im Falle von «Script Kiddies» • Gut sichtbare Ziele mit hoher Aufmerksamkeit im Falle von Racheaktionen (Defacements)

4 Angriffswerkzeuge

Nebst einer Vielzahl von Werkzeugen (Portscanner, Penetration Testing Tools, etc.), die ebenso sehr legalen Zwecken dienen können, gibt es verschiedene spezifische böswillige Instrumente. Allen gemeinsam ist, dass sie ihre Verwendung auf allen Stufen der Pyramide (s. Kapitel Bedrohungen) finden.

Die Wissensdatenbank «ATT&CK» von MITRE (https://attack.mitre.org/) bietet eine Übersicht über Taktiken, Techniken und Prozeduren bei Cyberangriffen.

Zur Umsetzung dieser Taktiken, Techniken und Prozeduren kommt Schadsoftware zum Einsatz. MITRE führt eine umfangreiche Liste solcher Schädlinge(https://attack.mitre.org/software/).