Bundesamt
für Sicherheit in der
Informationstechnik

ANGRIFFSMETHODEN

Register aktueller Cyber-Gefährdungen und -Angriffsformen

Ein wirksamer Schutz vor Cyber-Angriffen ist nur möglich, wenn Gefährdungen im Cyber-Raum sowie die eigene Gefährdungslage zumindest im Überblick bekannt sind. Dieses Wissen ist Voraussetzung für die Auswahl geeigneter präventiver und reaktiver Maßnahmen gegen diese Gefährdungen und Basis für eigene Risikoanalysen.

Das vorliegende Register soll unter anderem für Anwender, Planer und Architekten von Informationstechnik, für CIOs sowie für IT-Sicherheitsberater und IT-Sicherheitsbeauftragte als Hilfsmittel dienen. Es orientiert sich an den typischen Phasen eines Cyber-Angriffs und bietet eine strukturierte Zusammenstellung mit Beispielen, welchen Cyber-Gefährdungen eine Institution in besonderer Weise ausgesetzt sein kann. Das Register unterstützt somit vom Einstieg in die Thematik „Cyber-Sicherheit“ über die Durchführung von Cyber-Risikoanalysen bis hin zur Auswahl geeigneter Sicherheitsmaßnahmen.

Ein wesentlicher Baustein der Cyber-Sicherheit ist die Abwehr von Angriffen. Aufgrund der dynamischen Entwicklung der Cyber-Sicherheitslage muss dieser Aspekt regelmäßig und gezielt neu bewertet werden. Der Fokus des vorliegenden Registers liegt demnach auf vorsätzlichen Gefährdungen (potenziellen Angriffen), die heute beobachtet werden und die mit der weltweiten Vernetzung von Informationstechnik in Zusammenhang stehen.

1 Top 6 der aktuellen Cyber-Angriffsformen

Da ein umfassender Schutz gegen die Vielzahl möglicher Cyber-Gefährdungen nicht unmittelbar erreicht werden kann, ist zunächst eine Konzentration auf die relevantesten Cyber-Gefährdungen notwendig, bevor weitere IT-Sicherheitsmaßnahmen ergriffen werden. Das BSI schätzt die folgenden Gefährdungen derzeit als besonders bedrohlich und relevant ein (ohne Rangordnung):

- Gezieltes Hacking von Webservern mit dem Ziel der Platzierung von Schadsoftware oder zur Vorbereitung der Spionage in angeschlossenen Netzen oder Datenbanken
- Drive-by-Exploits zur breitflächigen Infiltration von Rechnern mit Schadsoftware beim Surfen im Internet mit dem Ziel der Übernahme der Kontrolle des betroffenen Rechners
- Gezielte Schadsoftware-Infiltration per E-Mail und mithilfe von Social Engineering mit dem Ziel der Übernahme der Kontrolle über den betroffenen Rechner und anschließender Spionage
- Distributed Denial of Service-Angriffe mittels Botnetzen mit dem Ziel der Störung der Erreichbarkeit von Webservern oder der Störung der Funktionsfähigkeit der Netzanbindung der betroffenen Institution
- Ungezielte Verteilung von Schadsoftware mittels Spam oder Drive-by-Exploits mit Fokus auf Identitätsdiebstahl
- Mehrstufige Angriffe, bei denen z. B. zunächst zentrale Sicherheitsinfrastrukturen (wie TLS/SSL-Zertifizierungsstellen) kompromittiert werden, um dann in weiteren Schritten die eigentlichen Ziele anzugreifen

2 Phasen eines Cyber-Angriffs

Ein Cyber-Angriff setzt das vorsätzliche, unerlaubte Handeln eines Angreifers mit bestimmter Absicht voraus. Der Angreifer entscheidet in der Phase 1 zunächst über die Angriffsziele und wählt in diesem Zusammenhang auch die Angriffsreichweite: Ein gezielter Angriff richtet sich gegen wenige Ziele oder sogar nur gegen ein einzelnes System, ein Flächenangriff richtet sich gegen möglichst viele Ziele gleichzeitig.

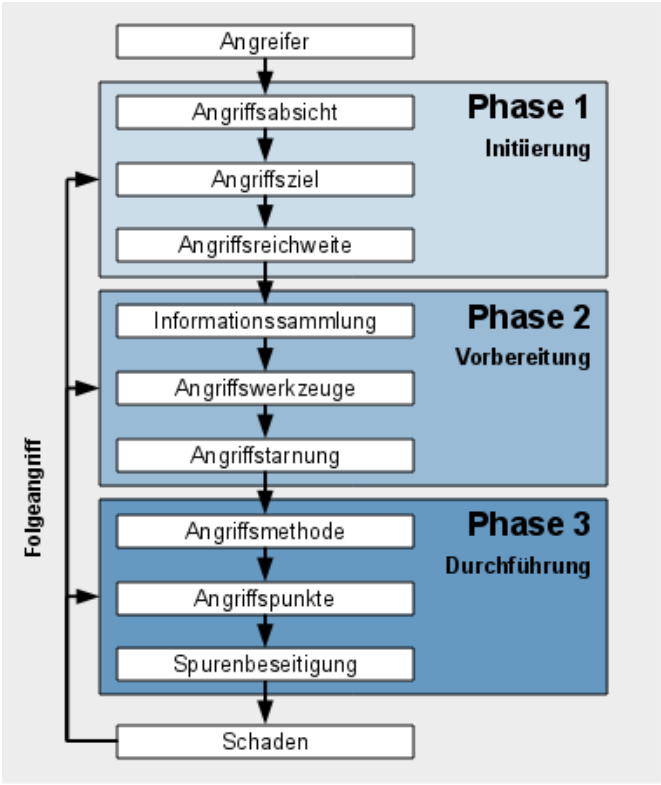

Abbildung 1: Phasen eines Cyber-Angriffs

In der Phase der Angriffsvorbereitung (Phase 2) werden Informationen über das anzugreifende Ziel erhoben. Hier werden auch die Angriffswerkzeuge konstruiert bzw. vorbereitet sowie Maßnahmen zur Angriffstarnung ergriffen.

Es folgt ein Primärangriff in Phase 3, der mithilfe bestimmter Angriffsmethoden an einem oder mehreren Angriffspunkten durchgeführt wird. Anschließend wird der Täter gegebenenfalls versuchen, die von ihm erzeugten Spuren zu beseitigen.

Falls das Angriffsziel mit einem Primärangriff nicht erreicht wurde oder dieser nur einen Zwischenschritt zum Erreichen des eigentlichen Angriffsziels darstellt, wird nach dem Primärangriff eventuell ein Folgeangriff durchgeführt.

3 Aufbau des Registers

Um die Vielzahl unterschiedlicher Cyber-Gefährdungen und Angriffsformen, die in der Praxis beobachtet werden, handhabbar zu machen, ist das Register anhand der oben beschriebenen Phasen strukturiert. Da sich Cyber-Angriffe dynamisch weiterentwickeln, wird das Register in Form von vier Anhängen (A-D) erstellt und fortgeschrieben.

- Anhang A befasst sich, außerhalb der drei Phasen eines Cyber-Angriffes, mit den unterschiedlichen Gruppen potenzieller Angreifer im Cyber-Raum und deren Motivation.
- Anhang B beschreibt die erste Phase eines Cyber-Angriffes, in der Absicht, Ziel und Reichweite eines Cyber-Angriffs eine Rolle spielen.
- Anhang C beschreibt die zweite Phase eines Cyber-Angriffs, in welcher, neben der Sammlung von Informationen über das anzugreifende Ziel, hauptsächlich die Auswahl geeigneter Angriffswerkzeuge und Möglichkeiten zur Verschleierung der Identität des Angreifers aufgegriffen werden.
- Anhang D beschreibt die dritte Phase eines Cyber-Angriffs und befasst sich, aufbauend auf dem in Anhang B und C beschriebenen Vorgehen, mit typischen Methoden zur Angriffsdurchführung, z. B. dem Einsatz von Schadprogrammen oder Identitätsdiebstahl.

Gefährdungen für die Informationssicherheit, die über den Themenbereich „Cyber-Sicherheit“ hinausgehen (wie beispielsweise Fehlbedienung, technisches Versagen oder höhere Gewalt), sind im IT-Grundschutz des BSI thematisiert und werden im vorliegenden Dokument nicht betrachtet.

4 Danksagung

Um ein möglichst vollständiges Bild über die Gefährdungen im Cyber-Raum zu gewinnen, hat das BSI Umfragen bei Verbänden, Unternehmen und Forschungseinrichtungen durchgeführt. Die Ergebnisse dieser Umfragen sind – ebenso wie die eigenen Erkenntnisse des BSI – in das vorliegende Register eingeflossen.

Das BSI dankt allen Umfrageteilnehmern und allen Multiplikatoren, die bei der Erstellung des Registers mitgewirkt haben. Besonderer Dank gilt dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) und dem Bundesverband der Deutschen Industrie e.V. (BDI) für die aktive Unterstützung des Vorhabens.

Anhang zum Register aktueller Cyber-Gefährdungen und -Angriffsformen

1 Angreifer

Trotz der großen Anzahl unterschiedlicher Angriffsziele und möglicher Angriffsmethoden kann die Motivation hinter einem Cyber-Angriff häufig auf finanzielle Interessen, Informationsbeschaffung, Sabotage, Einflussnahme oder Durchsetzung politischer Interessen zurückgeführt werden.

Die Attraktivität von Cyber-Angriffen ergibt sich vor allem durch die folgenden Merkmale:

- Die Vernetzung von Informationstechnik macht Angriffe aus der Distanz von nahezu jedem Ort der Welt und zu jedem Zeitpunkt möglich. Ein Angreifer muss sich dadurch keinen unmittelbaren Risiken vor Ort aussetzen.
- Das heutige offen gestaltete Internet bietet für Angreifer vielfältige Tarnungsmöglichkeiten, die das Entdeckungsrisiko minimieren.
- Nicht abgesicherte Informationstechnik und speziell zugeschnittene Werkzeuge ermöglichen es, eine Vielzahl unterschiedlicher Ziele parallel anzugreifen.
- Angriffswerkzeuge und -methoden sind einfach und kostengünstig verfügbar und beschaffbar. Neueste Erkenntnisse über Schwachstellen und Angriffsverfahren werden bereits nach kurzer Zeit für Cyber-Angriffe angewendet.
- Erfolgreiche Angriffe auf den elektronischen Geschäftsverkehr ermöglichen große finanzielle Gewinne für Angreifer.
- Der intensive Informationsaustausch über das Internet erleichtert den Zugriff auf schützenswerte Informationen.
- Die Komplexität der Technik und/oder fehlendes Sicherheitsbewusstsein erhöhen in vielen Fällen die Erfolgsaussichten für Cyber-Angriffe.

Die vorsätzlich handelnden Angreifer im Cyber-Raum lassen sich in folgende Gruppen einteilen:

- Cyber-Aktivisten
  Angreifer, die durch einen Cyber-Angriff auf einen politischen, gesellschaftlichen, sozialen, wirtschaftlichen oder technischen Missstand aufmerksam machen oder eine diesbezügliche Forderung durchsetzen wollen („Hacktivismus“). Die Motivation hinter dem Angriff ist Einflussnahme. Der durch einen Cyber-Angriff entstandene Schaden wird in Kauf genommen bzw. forciert, um eine höhere Aufmerksamkeit zu erlangen. Sogenannte „ethische Hacker“ begründen ihr Handeln mit gesellschaftlichen oder sozialen Themen.
- Cyber-Kriminelle
  Die Motivation von Cyber-Kriminellen ist es, mithilfe der Informationstechnik auf illegalen Wegen Geld zu verdienen. Die Bandbreite reicht von organisierter Cyber-Kriminalität bis hin zu einfacher Kriminalität mit geringen Schäden.
  - Organisierte Cyber-Kriminalität reicht vom Identitätsdiebstahl mit Warenbetrug über den Diebstahl von Geld durch Missbrauch von Bankdaten bis hin zur Erpressung. Organisierte Cyber-Kriminelle nutzen die genannten Vorteile von Cyber-Angriffen bei ihren Aktivitäten mit hoher Professionalität aus.
  - Im Gegensatz zur organisierten Kriminalität sind einfache Cyber-Kriminelle meist Einzelpersonen oder kleine Gruppen, die sich durch geringere Professionalität in ihrem Handeln auszeichnen. Dementsprechend ist auch die Auswahl der Angriffsziele eingeschränkt und der verursachte Schaden typischerweise geringer.

- Konkurrenzausspähung/Industriespionage im Cyber-Raum
  Durch die Vorteile des Internets ergeben sich für die Ausforschung eines Unternehmens durch Wettbewerber oder private Akteure neue Möglichkeiten. Konkurrenzausspähung dient finanziellen Interessen. Interne Informationen über Mitbewerber und deren Produkte bieten geldwerte Vorteile im globalen Wettbewerb.
- Staatliche Nachrichtendienste im Cyber-Raum
  Cyber-Angriffe durch staatliche Nachrichtendienste sowie staatlich gelenkte Wirtschaftsspionage dienen – im Gegensatz zur Konkurrenzausspähung – primär der Informationsbeschaffung und der Einflussnahme, auch um den eigenen nationalen Wirtschaftsunternehmen Vorteile auf den internationalen Märkten zu verschaffen.
- Staatliche Akteure im Cyber-War
  Im militärischen Sektor wird der Cyber-Raum inzwischen vielfach als weitere wichtige Domäne neben den klassischen militärischen Domänen Land, See, Luft und Weltraum angesehen.
- Cyber-Terroristen
  Terroristen können Cyber-Angriffe, wie staatliche Akteure und Kriminelle, nutzen, um unterschiedliche Ziele anzugreifen und somit ihre Ideologie zu verbreiten und ihren Einfluss auszuweiten.
- Hobbyisten/Skript-Kiddies
  Die Gruppe der Hobbyisten und Skript-Kiddies führt Cyber-Angriffe aus Neugier durch, um ihre Fähigkeiten und ihr Wissen in der Praxis zu testen. Diese Gruppe verfolgt keine finanziellen Interessen. Die Auswahl der Angriffsziele ist unspezifisch und vielfach allein vom Grad der Absicherung abhängig.
- Innentäter
  Cyber-Angriffe durch Innentäter haben größere Aussicht auf Erfolg als Angriffe von außen, da der Angreifer bereits Zugang zu internen Ressourcen einer Organisation hat und so Schutzmaßnahmen und Schwachstellen über einen langen Zeitraum analysieren kann. Zusätzliche Vorteile genießen Innentäter durch das ihnen entgegengebrachte Vertrauen einer Organisation. Externe Dienstleister, die durch ihre Tätigkeit Einfluss oder direkten Zugang zur Organisation haben, werden hier ebenfalls zu den Innentätern gezählt.
- IT-Sicherheitsforscher
  IT-Sicherheitsforscher haben ein primär akademisches Interesse an der Aufdeckung von Risiken und der Durchführung von Cyber-Angriffen. Die unkoordinierte Veröffentlichung ihrer Ergebnisse („Full Disclosure") kann reale Attacken anderer Angreifer zur Folge haben.

2 Angriffsinitiierung

2.1 Angriffsabsicht

Cyber-Angriffe stehen den klassischen Grundwerten der Informationssicherheit entgegen.

Typisch sind somit folgende Absichten hinter einem Angriff:

- Angriffe auf die Vertraulichkeit, z. B. das Ausspionieren vertraulicher Informationen:
  - durch direktes Abhören (z. B. Kabel, Funk, Netze)
  - durch Direktzugriff (z. B. Hotel, Zoll)
  - durch Diebstahl
  - durch Abfangen kompromittierender Abstrahlung
  - durch Ausspähen/Passive Reconnaissance
  - durch Wiederherstellung gelöschter Informationen
  - durch Profiling/Überwachung
- Angriffe auf die Integrität, z. B. die Manipulation:
  - von Informationen
  - von Speichermedien
  - von IT-Diensten
  - von Software
  - von Kommunikationskanälen
  - von Schnittstellen oder Zugängen
  - von zentralen/dezentralen/externen Komponenten
  - von Internet-Strukturen
  - von Spezial-IT
  - von Sicherheitskomponenten
- Angriffe auf die Verfügbarkeit, z. B. das Sabotieren von Informationen oder IT-Diensten:
  - durch Denial of Service-Angriffe
  - durch physikalische Zerstörung
  - durch Diebstahl
- Schädigung des Ansehens von Personen oder Institutionen infolge oben genannter Angriffe
- Angriffe auf die Integrität umfassen als Spezialfall auch Angriffe auf die Authentizität, beispielsweise das Vortäuschen eines falschen Absenders.

2.2 Angriffsziel

Durch Cyber-Angriffe sind vorrangig folgende Arten von Objekten innerhalb und außerhalb einer Institution bedroht:

- Informationen
- IT-Dienste
- IT-Systeme

Diese lassen sich in unterschiedliche Gruppen (B.2.1-B.2.11) weiter differenzieren.

2.2.1 Informationen

Ziel der Informationstechnik ist die einfache Nutzung, Verarbeitung und Speicherung von Informationen. Daher sind Informationen ein vorrangiges Ziel von Cyber-Angriffen. Informationen können sowohl das eigentliche Ziel eines Angriffs darstellen, aber auch als Hilfsmittel zur Durchführung von weiteren Cyber-Angriffen genutzt werden. Obwohl Informationen immateriell sind, können sie einen beachtlichen Wert besitzen und daher schützenswert sein.

Beispiele hierfür sind:

- Forschungs- und Entwicklungsdaten
- Geschäfts- und Finanzdaten
- Bankdaten und Zahlungsinformationen
- Kunden- und Rechnungsdaten
- Dokumente
- Transaktionen
- Geistiges Eigentum
- Konfigurationsdaten
- Kommunikationsdaten
- Protokollierungsdaten
- Identitätsmerkmale/Credentials
- Kryptodaten/Schlüssel/Zertifikate
- Personenbezogene/biometrische Daten
- Verhaltens- und Standortdaten
- Metadaten
- Presse- und Medieninformationen
- Verschlusssachen
- Informationen über IT-Infrastruktur und -Architektur

2.2.2 Speichermedien

Datenspeicher werden in der Informationstechnik in vielen unterschiedlichen Ausprägungen genutzt und enthalten Informationen. Jede Form von Speichermedium kann daher auch Ziel eines Cyber-Angriffs sein.

Beispiele hierfür sind:

- Datenbanken
- Dateien
- Stationäre Datenträger
- Mobile Datenträger
- Externe Datenspeicher/Cloud-Storage
- Hauptspeicher
- Zwischenspeicher (Caches)
- Cookies/Local Shared Objects
- Ausweise/Karten
- Verzeichnisse/Listen

2.2.3 IT-Dienste

Viele unterschiedliche IT-Dienste sind heute für einen reibungslosen Betrieb des Internets sowie der darauf aufbauenden Geschäftsprozesse verantwortlich. Das gilt für Basisdienste – wie beispielsweise DNS – genauso, wie für eine E-Commerce-Anwendung oder einen E-Mail-Dienst in einem Unternehmensnetzwerk. Dienste sind ein exponiertes Angriffsziel für Cyber-Angreifer und auf vielfältige Weise und mit unterschiedlicher Motivation angreifbar.

Beispiele hierfür sind:

- Elektronischer Geschäftsverkehr
- E-Government
- Web-Präsenzen/-Portale
- Web-Services
- Kommunikationsdienste
- Benutzerkonten
- Datei- und Verzeichnisdienste
- Synchronisationsdienste
- Infrastrukturdienste (z. B. DNS)
- Sicherheitsdienste (z. B. PKI)
- Authentisierungsdienste
- Administrationsdienste
- Protokollierungsdienste

2.2.4 Software und Anwendungen

Cyber-Angriffe auf Software sind gängige Wege, einen Dienst zu stören oder ein System zu infiltrieren, um anschließend z. B. Informationen auszuspähen.

Beispiele für Software als Angriffsziel sind:

- Lokale Anwendungen
- Benutzerschnittstellen/Browser/Plug-ins
- Client-Server-Anwendungen
- Internet-Anwendungen
- Mobile Anwendungen/Apps
- Aktive Inhalte
- Betriebssysteme
- Laufzeitumgebungen
- Software/Update Repositories
- Download-Plattformen/App-Stores
- Versionskontrollsysteme
- Quellcode
- Firmware
- Sicherheitssoftware

2.2.5 Kommunikationskanäle

Kommunikation läuft im Cyber-Raum über unterschiedlichste Kanäle ab. Angreifer können diese Kanäle abhören, manipulieren oder stören, um dadurch beispielsweise an die übertragenen Informationen zu gelangen oder die darüber abgewickelten Geschäftsprozesse zu beeinträchtigen.

Beispiele für Kommunikationskanäle sind:

- E-Mail
- Instant Messaging
- Web-basierte Kommunikation
- (Mobile) Telefonie (auch VoIP)
- Kurzmitteilungen
- Videokonferenzen/Webmeetings
- Fax
- Soziale Netze und Foren

2.2.6 Schnittstellen und Zugänge

Der Schutz der Schnittstellen und Zugänge zum eigenen Informationsverbund muss mit hoher Priorität erfolgen. Aus öffentlichen Netzen erreichbare Zugänge dienen häufig als Einfallstor für Cyber-Angriffe. Ein Angriff auf die Verfügbarkeit der Zugänge kann den Komplettausfall der Kommunikationsfähigkeit einer Institution zur Folge haben.

Beispiele hierfür sind:

- Provider-Anbindungen und Backbones
- Extranet-Anbindungen
- VPN-Anbindungen und -Knoten
- Kunden-/Partner-/Dienstleister-Schnittstellen
- Fernzugänge
- Drahtlose Zugänge
- Kabel
- Übertragungsprotokolle
- Infrastrukturprotokolle
- Enterprise Service Bus
- Mobilfunk-Basisstationen

2.2.7 Zentrale interne Komponenten

Zentrale Komponenten in einer Institution sind häufig Ziele eines Cyber-Angriffs, sofern Angreifer die Schutzmaßnahmen der Schnittstellen und Zugänge erfolgreich überwinden konnten. Diese Komponenten enthalten Daten oder stellen Dienste bereit, die für die Funktionsfähigkeit der Institution oft entscheidend sind.

Beispiele hierfür sind:

- Server
- Speichersysteme/Speichernetze
- Virtualisierungskomponenten
- Private Cloud-Komponenten
- Netzwerkkomponenten
- Sicherheitskomponenten
- Administrationskomponenten
- DMZ-Komponenten
- Proxies/Load Balancer
- Mobile Backend/Management

2.2.8 Dezentrale Komponenten

Dezentrale Komponenten sind oft einem großen Risiko durch Cyber-Angriffe ausgesetzt, da sie teilweise nicht von den Schutzmaßnahmen der zentralen Komponenten profitieren können. Insbesondere werden dezentrale Komponenten häufig in leicht zugänglichen Räumlichkeiten betrieben, was die Manipulationsgefahr erhöht.

Beispiele hierfür sind:

- Stationäre Clients/Endgeräte
- Mobile Clients/Endgeräte, wie Smartphones oder Tablet-PCs
- Kiosk-Systeme
- Eingabegeräte (z. B. Maus, Tastatur, Lage- und Ortssensoren)
- Ausgabegeräte (z. B. Bildschirm, Drucker)

2.2.9 Externe Komponenten

Geschäftsprozesse werden heute in der Regel nicht nur durch Komponenten der eigenen Institution abgebildet. Für bestimmte Aufgaben werden in vielen Fällen Dienstleistungen von Dritten eingekauft und in die Organisation eingebunden.

Für die Informationstechnik hat dies beispielsweise zur Folge, dass fremde Systeme an das eigene Netzwerk angebunden werden oder dass Daten zur weiteren Verarbeitung das eigene Netzwerk verlassen.

Beispiele für externe Komponenten sind:

- IT von Partnern/Kunden/Dienstleistern
- Cloud Computing
- Private IT
- Gebäude und Räume
- Versorgungsnetze (insbesondere Energie)
- Klimatisierung
- Dienstleister (nicht IT-spezifisch)

2.2.10 Internet-Strukturen

Das Internet ist für die Gesellschaft in der jüngsten Vergangenheit zu einer äußerst wichtigen Ressource geworden. Dementsprechend hoch sind auch die Anforderungen an die Versorgungssicherheit. Für die Funktionsweise des Internets sind viele unterschiedliche Basis-Dienste verantwortlich. Ein Cyber-Angriff auf einen oder mehrere dieser Fundamente des Internets kann massive Auswirkungen auf eine Vielzahl von Personen und Organisationen haben.

Beispiele für angreifbare Internet-Strukturen sind:

- Internet-Dienstleister
- Hosting-Provider
- Content Delivery Networks
- Internet-Kerninfrastruktur
- Routing-Strukturen
- Namensauflösung (DNS)
- Domain Registries
- TLS/SSL-Zertifizierungsstellen
- Suchmaschinen
- Zentrale Blacklists
- Soziale Netzwerke
- Cloud-Dienstleistungen
- Anonymisierungsdienste
- Öffentliche Internet-Zugänge

2.2.11 Spezial-IT

Mit Spezial-IT sind Systeme außerhalb der klassischen Büro-IT gemeint, die in der Vergangenheit im Hinblick auf Informationssicherheit selten angemessen berücksichtigt oder sogar komplett ausgeblendet wurden. Heute ist auch Spezial-IT vielfach mit dem Internet oder mit anderen großen Netzen gekoppelt, sodass auch sie als Ziel für Cyber-Angriffe eine Rolle spielt.

Beispiele hierfür sind:

- Zutrittskontrollsysteme
- Videoüberwachungssysteme
- Prozesssteuerung, -automatisierung, -leittechnik
- Digitale Mess-/Steuerungs-/Regelsysteme
- Medizin-IT
- Automobil-IT
- Smart Grid/Smart Metering
- Positionierungsdienste
- Geldautomaten/Zahlungsterminals

2.3 Angriffsreichweite

Cyber-Angriffe lassen sich in Bezug auf ihre Reichweite unterscheiden:

- Gezielte Angriffe auf ein Ziel oder wenige ausgesuchte Ziele
- Großflächiger Angriff auf möglichst viele beliebige Ziele gleichzeitig

Die Reichweite steht in engem Zusammenhang mit Motiv, Absicht und Ziel des Angriffs. Je nach Reichweite ist ein Angriff mit bestimmten Vor- und Nachteilen für den Täter verbunden: Ein breit gestreuter Angriff verspricht z. B. eine höhere Erfolgswahrscheinlichkeit. Andererseits fallen großflächige Angriffe meist eher auf und provozieren so rasche Gegenmaßnahmen. Weiterhin können Schäden auch bei unbeteiligten Dritten entstehen, die durch Fehler oder Fehlfunktionen unbeabsichtigt Opfer eines Cyber-Angriffs werden (Begleitschaden).

3 Angriffsvorbereitung

3.1 Informationssammlung über Angriffsziele

Um die Erfolgsaussichten für Cyber-Angriffe zu verbessern, sind Angreifer bemüht, im Vorfeld nützliche Informationen über die Angriffsziele zu beschaffen. Mittels dieser Informationen können Angriffe auf das Ziel zugeschnitten und besser getarnt werden.

Typische Informationen zur Angriffsvorbereitung sind:

- Identifikation möglicher Angriffspunkte
  - Art der IT-Systeme und IT-Architektur
  - Netzwerk-Architektur und Schnittstellen
  - Betriebssysteme, Anwendungen und Patchlevel
  - IT-Sicherheitsmaßnahmen und eingesetzte IT-Sicherheitsprodukte
- Informationen über das Angriffsziel
  - Informationen über Personen
  - Informationen über den organisatorischen Aufbau
  - Informationen über die Geschäftstätigkeit
- Abschätzung der Risiken eines Angriffs und Strategien zur Tarnung
- Abschätzung der Folgen eines Angriffs

Diese Informationen werden über verschiedene Wege eruiert, zum Beispiel:

- Social Engineering
  - Vortäuschen einer falschen Identität
  - Ausnutzen von Hilfsbereitschaft, Vertrauen oder Neugier
  - Ausnutzen von Angst, Autorität oder technischem Unverständnis
- Sammlung und Auswertung frei verfügbarer Informationen über das Ziel
  - in Veröffentlichungen
  - über Web-Inhalte
  - in Sozialen Netzen
  - im Altpapier, Restmüll und anderen Abfällen einer Organisation (Dumpster Diving)
- Sammlung und Auswertung von Informationen über Systeme und Zugänge des Angriffsziels
  - durch Network Mapping
  - durch Fingerprinting/Probing
  - Identifikation von Angriffspunkten

Einen besonders hohen Stellenwert hat die Informationssammlung, wenn ein gezielter Angriff vorbereitet wird. Bei großflächigen Angriffen stehen hingegen eher statistische Informationen im Vordergrund, beispielsweise über den Verbreitungsgrad einer bestimmten Software.

3.2 Angriffswerkzeuge

Täter bedienen sich bei Cyber-Angriffen vielfältigen Hilfsmitteln und Werkzeugen. Häufig werden unterschiedliche Typen von Schadsoftware oder Exploits zur Ausnutzung von Software-Schwachstellen genutzt, um Zugriff auf ein System zu erlangen. Hacking-Tools können beispielsweise dazu dienen, schwache Passwörter zu ermitteln oder verwundbare Systeme zu identifizieren. Datenträger werden manipuliert, Kommunikationskanäle und Software werden missbraucht. Je nach Art des Angriffs kann auch spezielle Hardware zum Einsatz kommen.

3.2.1 Schadsoftware

Schadsoftware (Malware) ist Software, die bei Ausführung auf dem Zielrechner schädliche Operationen ausführt. Dabei werden allgemein die folgenden Klassen unterschieden. Allerdings besteht moderne Schadsoftware vielfach aus einer Kombination verschiedener Funktionalitäten, ist modular aufgebaut und durch Nachladen weiterer Schadcodes dynamisch veränderbar. Entwicklung und Vertrieb von Schadsoftware werden zunehmend professionalisiert, wobei die Angreifer mit Webseiten, Support oder Hosting Verfahren der normalen Software-Entwicklung adaptieren. In diesem Zusammenhang spricht man von „Malware-as-a-Service".

- Viren
  Klassische Form von Schadsoftware, die sich selbst verbreitet und unterschiedliches Schadpotenzial in sich tragen kann (keine Schadfunktion bis hin zum Löschen der Daten auf einer Festplatte). Viren treten in Kombination mit einem Wirt auf, z. B. einem infizierten Dokument oder Programm.
- Trojanische Pferde
  Schadsoftware, die sich in scheinbar nützlichen oder interessanten Dokumenten oder Programmen versteckt. Die schädlichen Operationen werden heimlich ausgeführt. Trojanische Pferde versuchen häufig, gezielt Informationen zu sammeln (Dateien, Tasteneingaben, Bildschirmfotos) und nach außen zu übertragen – ohne dabei entdeckt zu werden – oder Hintertüren zu öffnen, um Folgeangriffe zu ermöglichen.
- Bots
  Ein Bot ist eine Schadsoftware, die einen Steuerkanal zum Angreifer aufbaut und ihm darüber die Kontrolle über das infizierte System erlaubt. Hat ein Angreifer mehrere Bots unter seiner Kontrolle, spricht man von einem Botnetz. Angreifer nutzen die Kontrolle über die Bots z. B. zur Versendung von Spam-Nachrichten, zur Durchführung von DDoS-Angriffen oder auch zur Weiterverbreitung und Vergrößerung des Botnetzes.
- Würmer
  Ein Wurm ist eine Schadsoftware, die sich selbstständig über ein Netzwerk ausbreiten kann und so binnen kürzester Zeit eine Vielzahl von Systemen infiziert. Durch die Ausbreitung kommt es häufig zur Überlastung und zum Ausfall von Systemen und/oder Netzen. Unabhängig von der Fähigkeit der Weiterverbreitung können Würmer zusätzliche Schadfunktionen enthalten.
- Rootkits
  Als Rootkit bezeichnet man eine Schadsoftware, deren Ziel es ist, sich möglichst tief im angegriffenen System zu verstecken, um eine Erkennung durch ein Virenschutzprogramm zu verhindern. Beispiele sind Rootkits, die vor dem Betriebssystem starten und durch dieses nicht während der Laufzeit erkannt werden können. Andere Schadsoftware, wie z. B. Trojanische Pferde, können ebenfalls Rootkit-Funktionen enthalten.
- Scareware
  Scareware ist eine Form von Schadsoftware, die der Nutzer selbst auf seinem System installiert. In den meisten Fällen wird dem Nutzer beim Surfen im Internet durch Täuschung oder Ausnutzen von technischem Unverständnis suggeriert, dass ein Problem mit seinem Computer besteht. Häufig wird dazu eine Infektion mit Schadsoftware gemeldet, eine angebliche Fehlfunktion des Betriebssystems erkannt oder mit einem wichtigen Sicherheits-Update geworben. Vertraut ein Anwender auf diese Meldungen und installiert die angebotene Software, hat er selbst dadurch das System im ungünstigsten Fall mit einer Schadsoftware infiziert.
- Ransomware
  Ransomware (von engl. ransom – Lösegeld) ist eine Schadsoftware, die die Verfügbarkeit des Systems oder von Daten durch Verschlüsselung, Löschung oder Aussperrung stört und ein Lösegeld vom Opfer für den Zugang zu seinen Daten fordert.
- Spyware
  Spyware ist Spionagesoftware, die beispielsweise das Verhalten des Nutzers aufzeichnet.
- Backdoors
  Backdoors sind Hintertüren, über die ein System vom Nutzer unbemerkt durch Dritte kontrolliert werden kann.

3.2.2 Datenträger und Kanäle

Vermeintlich unbedenkliche Datenträger und ungeschützte Kommunikationskanäle können zu einem Angriffswerkzeug werden, wenn ein Angreifer diese unter seine Kontrolle bringt, sie manipuliert oder Angriffstools darin versteckt. Beispiele hierfür sind:

- Mobile Datenträger
- Mobile Endgeräte
- Private Endgeräte in der Organisation („Bring Your Own Device“)
- Webseiten (infiziert oder manipuliert/gefälscht)
- E-Mails (infiziert oder manipuliert/gefälscht)
- Chats, Kurzmitteilungen, Benachrichtigungen
- Datei- und Verzeichnisfreigaben
- Netzwerkprotokolle
- Unverschlüsselte Netzwerkverbindungen

3.2.3 Software

Es existieren viele unterschiedliche Arten von Software, die Angreifer bei der Durchführung von Cyber-Angriffen unterstützen.

- Aktive Inhalte
  Die Manipulation gegebener Aktiver Inhalte, wie beispielsweise JavaScript-Code, sind häufig Ausgangsbasis für Cross-Site-Scripting oder SQL-Injection-Angriffe.
- Administrationswerkzeuge
  Schlecht abgesicherte Administrationswerkzeuge, z. B. zur Fernwartung, erlauben Angreifern u. U. einen einfachen Zugriff auf Systeme.
- Sicherheits-/Hacking-Tools
  Darunter fallen beispielsweise Programme zum automatischen Auffinden von Schwachstellen in einem Netzwerk, Tools zum Anpassen von Exploits oder Schadsoftware sowie Programme zur Durchführung von Brute-Force-Angriffen.
- Internet-Client-Software
  Browser oder andere Internet-Clients sind nicht nur Ziel von Cyber-Angriffen, sondern werden auch bei der Durchführung von Angriffen benutzt.
- Exploit
  Als Exploit bezeichnet man eine Methode oder einen Programmcode, mit dem über eine Schwachstelle in Hard- oder Software-Komponenten nicht vorgesehene Befehle oder Funktionen ausgeführt werden können. Je nach Art der Schwachstelle kann mithilfe eines Exploits z. B. ein Programm zum Absturz gebracht, Benutzerrechte ausgeweitet oder beliebiger Programmcode ausgeführt werden.

3.2.4 Internet-Strukturen

Nützliche Internet-Strukturen können als Angriffswerkzeuge missbraucht werden. Andere Internet-Dienste sind speziell für die Durchführung von Cyber-Angriffen entwickelt worden.

- Cloud-Dienstleistungen
  Flexible Cloud-Dienstleistungen können als Angriffswerkzeug missbraucht werden, wenn über sie z. B. Phishing-Seiten gehostet, DDoS-Angriffe durchgeführt oder Rechenkapazitäten für Brute-Force-Angriffe bereitgestellt werden. Abgesehen davon ist ein Missbrauch als unauffällige Steuerungsinfrastruktur möglich.
- Bulletproof-Hoster
  Bulletproof-Hoster sind Dienstleister, die Webspace, IP-Adressen oder andere Ressourcen im Internet bereitstellen und dabei den Missbrauch ihrer Dienstleistungen, z. B. auch für Cyber-Angriffe, bewusst in Kauf nehmen. Bulletproof-Hoster arbeiten nicht mit Strafverfolgungsbehörden oder anderen Autoritäten im Internet zusammen.
- Botnetze
  Große Botnetze stellen durch ihre potenziellen Ressourcen an Rechenkapazität und Bandbreite eine vielfältige Bedrohung dar. Sie werden als Angriffswerkzeug häufig für DDoS-Angriffe oder den Versand von Spam-Nachrichten verwendet. Bots werden weiterhin für Click-Betrug, für das Hosting von Phishing-Seiten oder als Dropzone missbraucht.

- Command & Control-Server
  Command & Control-Server sind zentrale Elemente eines Botnetzes und verteilen die Kommandos an die einzelnen Bots. Es existieren jedoch auch Botnetze, die Kommandos mittels Peer-to-Peer-Kommunikation weitergeben und somit auf einen zentralen Server verzichten können.
- Dropzones
  Dropzones sind Speicher im Internet, an die von Schadsoftware aufgezeichnete Daten automatisch übermittelt werden. Der Angreifer holt die Daten dann von der Dropzone ab. Ein direkter Zugriff des Angreifers auf das System des Opfers wird somit unnötig.
- Internet-Basisdienste (DNS, Routing)
  Zugriff auf und Manipulationen an Internet-Basisdiensten, wie z. B. DNS oder Routing, können für Angriffe durch Umleitung, Man-in-the-Middle oder Phishing missbraucht werden.

3.2.5 Geräte

Je nach Methode und Ziel eines Cyber-Angriffs kommen spezielle Geräte zum Einsatz oder vorhandene Geräte werden so manipuliert, dass sie zu einem Angriffswerkzeug werden. So werden z. B. Störgeräte für Angriffe auf drahtlose Netze genutzt. Von einer Organisation ausgesonderte Komponenten (z. B. Router) können ebenfalls, wenn sie nicht korrekt gelöscht und entsorgt wurden, für Angriffe auf die Organisation genutzt werden.

- Standard-IT
- Mobiltelefone
- Wanzen
- Keylogger
- Mikrokameras
- IMSI-Catcher
- Messgeräte
- Störgeräte
- Lesegeräte
- Ausgesonderte und funktionsfähige Komponenten

3.2.6 Angriffsunterstützende Informationen

Informationen sind wichtige Hilfsmittel für Cyber-Angriffe. Gestohlene Identifikationsmerkmale erlauben Zugriff auf Dienste und Dateien, Insider-Wissen erleichtert das Auffinden lohnender Ziele und die Durchführung von Angriffen.

- Gefälschte Identitätsmerkmale
- Gestohlene Identitätsmerkmale
- Gefälschte Kryptodaten
- Gestohlene Kryptodaten
- Schwachstellendatenbanken
- Insider-Wissen

3.3 Angriffstarnung

Um die Aufdeckung eines Cyber-Angriffes oder die Rückverfolgbarkeit des Angreifers zu erschweren, werden verschiedene Methoden zur Tarnung eingesetzt.

Beispiele hierfür sind:

- Anonymisierungsdienste
  Anonymisierungsdienste versuchen, bestimmte Informationen, die auf die Identität eines Internet-Nutzers hindeuten könnten, zu verschleiern.
- Fälschung von IP-Adressen, Absendern, etc.
  Einige Protokolle im Internet lassen es zu, Daten des Absenders zu manipulieren, ohne dass der Empfänger diese Manipulation erkennen kann. Ein Beispiel sind gefälschte Absender bei Spam- oder Phishing-Mails.

- Nutzung mehrerer Zwischenstationen
  Um die Rückverfolgbarkeit eines Angriffs zu erschweren, nutzen Angreifer mitunter mehrere Zwischenstationen, bevor sie ein Ziel angreifen. Diese Zwischenstationen können Anonymisierungsdienste, VPN-Dienste mit Endpunkten im Ausland oder andere Systeme sein, die unter der Kontrolle des Angreifers stehen, z. B. Bots.
- Tarnung auf dem Angriffsziel
  Um ein Ziel über einen möglichst langen Zeitraum kontrollieren oder ausspionieren zu können, muss ein Angreifer auch seine Aktivitäten auf dem Angriffsziel tarnen. Dazu werden oft Rootkit-Techniken angewendet, um eine Erkennung durch Virenschutzprogramme zu erschweren. Die Kommunikation mit dem Angreifer kann über getarnte Kommunikationskanäle laufen, die auf den ersten Blick unbedenklich erscheinen.
- Abschalten vorhandener Sicherheitsmaßnahmen
  Angreifer versuchen häufig, Sicherheitsmaßnahmen zu deaktivieren oder so zu manipulieren, dass der Angriff nicht erkannt wird, aber die Sicherheitsmaßnahme dem Anschein nach weiter ordnungsgemäß funktioniert.
- Protokollierung
  Viele IT-Systeme protokollieren die Nutzung oder die Kommunikation mit Dritten genau. Um einen Cyber-Angriff zu tarnen, muss diese Protokollierung gegebenenfalls deaktiviert, umgangen oder so manipuliert werden, dass daraus keine Rückschlüsse auf den Angriff gezogen werden können.
- Missbrauch fremder Identitäten
  Angreifer nutzen oft fremde Identitäten, wie z. B. Zugangsdaten von Dritten, damit ihre Aktivitäten nicht als Angriff, sondern als scheinbar legitimes Verhalten interpretiert werden.

4 Angriffsdurchführung

4.1 Angriffsmethode

Täter wenden bei Cyber-Angriffen eine Vielzahl unterschiedlicher Methoden an. Häufig werden diese nicht einzeln, sondern in Kombination eingesetzt, um das Angriffsziel zu erreichen.

4.1.1 Denial of Service-Angriff

Denial of Service-Angriffe (DoS, übersetzt „Angriffe auf die Betriebsfähigkeit“) richten sich gegen die Verfügbarkeit mit der Absicht, Dienste, einzelne Systeme oder ganze Netze zu stören oder vollständig betriebsunfähig zu machen. Wird ein Angriff mittels mehrerer Systeme parallel ausgeführt, spricht man von einem verteilten DoS, einem sogenannten „Distributed Denial of Service-Angriff“ (DDoS). Angriffspunkte sind häufig Webserver, Mailserver, Applikationsserver oder darauf laufende Dienste. Für Denial of Service-Angriffe können sehr unterschiedliche Methoden angewandt werden.

Beispiele sind Angriffe durch:

- Überflutung
  Ein klassisches Beispiel für einen Denial of Service-Angriff ist die Überflutung eines Webservers durch eine Vielzahl von Anfragen gleichzeitig. Sind die Ressourcen (z. B. Bandbreite oder Speicher) des Webservers durch den Angriff erschöpft, ist dieser nicht mehr oder nur noch mit sehr großen Antwortzeiten erreichbar. Durch die Überlastung eines Ziels mit einer großen Anzahl von Anfragen können DoS-Angriffe selbst dann erfolgreich sein, wenn das angegriffene System keine Software-Schwachstellen oder Konfigurationsfehler aufweist.
- Störung
  Ein Denial of Service kann auch dadurch ausgelöst werden, dass der Angreifer eine Störung herbeiführt, beispielsweise durch Ausnutzen einer bekannten Fehlfunktion einer Anwendung. Enthält eine Datenbank-Anwendung beispielsweise einen Fehler, der bei bestimmten Anfragen zu einem Ausfall der Datenbank führt, kann der Angreifer versuchen, dies für einen Denial of Service-Angriff auszunutzen.
- Abschaltung
  Angreifer können den Betrieb von Diensten auch dadurch einschränken, dass für den Betrieb des Dienstes notwendige Komponenten abgeschaltet werden, z. B. die Energieversorgung oder ein Kommunikationskanal.
- Aussperrung
  Denial of Service durch Aussperrung kann z. B. durch Manipulation der Routing-Infrastruktur realisiert werden, wodurch Datenpakete das Netz des Angriffsziels nicht mehr erreichen können. Ein weiteres wichtiges Beispiel ist das Auslösen einer Passwort-Sperre durch mehrmalige absichtliche Fehleingabe durch den Angreifer.
- Umleitung
  Eine Änderung von Verknüpfungen (z. B. ein Link auf den Warenkorb eines Online-Shops) kann dazu führen, dass Anwender eine E-Commerce-Anwendung nicht mehr nutzen können.
- Manipulation von Informationen
  Ein Denial of Service-Angriff kann durch unterschiedlichste Manipulationen erreicht werden. Ein Angreifer kann z. B. versuchen, die Konfigurationsdaten eines Dienstes zu verändern und dadurch den Dienst außer Kraft zu setzen.
- Löschen von Informationen
  Löscht ein Angreifer eine Datenbank mit Benutzerkonten, die z. B. für die Authentisierung an einer Webanwendung benötigt wird, können sich legitime Nutzer nicht mehr an der Applikation anmelden.
- Jamming
  Als „Jamming“ bezeichnet man das Überlagern von Funkwellen mit einem stärkeren Störsignal. Mittels eines solchen Störsignals können unter anderem WLAN- oder Mobilfunk-Verbindungen und somit die darüber übertragene Kommunikation (Sprache oder andere Daten) gestört werden.
- Spam
  Ein Denial of Service-Angriff mittels Spam-Nachrichten kann die Funktionsfähigkeit von Mailservern beeinträchtigen oder einen Nutzer durch Überflutung seines Postfaches in seiner Handlungsfähigkeit einschränken.

- physische Beschädigung/Zerstörung
  Durch Angriffe mit Schadsoftware auf Prozesssteuerungssysteme können unter Umständen auch ohne direkten Zugang des Angreifers physische Beschädigungen bzw. Zerstörungen hervorgerufen werden.
- Diebstahl
  Ein gezielter Diebstahl kritischer Komponenten kann auch als Denial of Service-Angriff ausgelegt werden, wenn abhängige Dienste nach dem Diebstahl nicht mehr ordnungsgemäß funktionieren. Ein Diebstahl kann außerdem dazu führen, dass Informationen in falsche Hände gelangen und/oder im eigenen Bereich nicht mehr zur Verfügung stehen.

4.1.2 Schadsoftware-Infiltration

Die in Anhang C.2.1 aufgelisteten unterschiedlichen Typen von Schadsoftware kommen je nach Zweck eines Cyber-Angriffs in unterschiedlicher Art und Weise zum Einsatz. Vor dem Einsatz der Schadsoftware muss ein Angreifer entscheiden, auf welchem Weg die Verteilung erfolgen soll.

Die Schadsoftware-Infiltration kann beispielsweise erfolgen durch:

- gezielte Verteilung
  Für gezielte Angriffe werden häufig E-Mails mit Anhängen verwendet, die aufgrund des Themas, des Absenders und der Anrede die Wahrscheinlichkeit erhöhen, dass das potenzielle Opfer den Anhang öffnet. Typische Anhänge sind Dokumente, in denen ein Schadprogramm eingebettet ist. Ein gezielter Angriff muss aber nicht auf wenige Personen beschränkt sein: Auch ein erfolgreicher Angriff auf eine einzelne Webseite, in dessen Nachgang Besucher der Webseite mit Schadsoftware infiziert werden, gilt als gezielter Angriff, wenn der Angreifer es auf die Nutzer dieser Webseite abgesehen hat. Die gezielte Verteilung von Schadsoftware mittels infizierter Datenträger kann z. B. in Form eines wertvollen Geschenks erfolgen.
- Massenverteilung
  Im Fall der Massenverteilung von Schadsoftware versuchen Angreifer z. B., hoch frequentierte Webseiten so anzugreifen, dass Besuchern der Webseite mittels Drive-by-Download Schadsoftware installiert wird. Auch Spam-Nachrichten können Schadcode im Anhang enthalten. Im Gegensatz zur gezielten Verteilung, bei denen die Opfer persönlich angesprochen werden, wird in Spam-Nachrichten z. B. mit interessanten Angeboten, Bildern, Videos, angeblichen Rechnungen oder Strafverfahren Aufmerksamkeit erzeugt, um das Opfer dazu zu bringen, den Anhang zu öffnen. Außerdem kann Schadsoftware in legitim erscheinende Programme eingebettet und so über offizielle Download-Seiten oder App-Stores verteilt werden. Eine Massenverteilung von Schadsoftware ist auch mittels Datenträgern, z. B. als Geschenk auf Messen, möglich. Massenverteilung von Schadsoftware wird unter anderem zum Auf- oder Ausbau von Botnetzen oder zum Identitätsdiebstahl mit kriminellem Hintergrund durchgeführt.
- Verteilung über Innentäter
  Die Verteilung von Schadsoftware durch Innentäter hat größere Aussicht auf Erfolg als bei Cyber-Angriffen von außen, da hierbei z. B. bestimmte Schutzmaßnamen einer Institution nicht greifen. Innentäter haben darüber hinaus häufig Zugriff auf interne Systeme und können Schadsoftware darüber in der Institution verteilen, z. B. über Dateiserver. Einem Mitarbeiter wird in der Regel ein höheres Vertrauen entgegengebracht als einem unbekannten Dritten. Dieses Vertrauen erhöht die Wahrscheinlichkeit, dass ein Angriff zum Erfolg führt.

Neben der klassischen PC-Plattform nimmt die Verbreitung von Schadsoftware für unterschiedliche mobile Plattformen über Apps und App-Stores zu.

4.1.3 Identitätsdiebstahl

Identitätsdiebstahl bzw. Identitätsmissbrauch durch Cyber-Angriffe sind heute Alltag im Internet. Angreifer versuchen, Zugriff auf Teile der Identität eines Nutzers zu erlangen, um diese für eigene Zwecke verwenden zu können. Die Bandbreite der Nutzungsszenarien ist sehr groß. Häufig ist Identitätsdiebstahl finanziell motiviert oder dient der Diskreditierung einer Person.

Ähnlich vielfältig sind die Wege, über die Identitätsdiebstahl stattfindet:

- Phishing
  Beim Phishing wird z. B. mittels gefälschter E-Mails und/oder Webseiten versucht, Zugangsdaten für einen Dienst oder eine Webseite zu erlangen. Wird diese Manipulation vom Opfer nicht erkannt und die Authentizität einer Nachricht oder Webseite nicht hinterfragt, gibt das Opfer seine Zugangsdaten u. U. selbst unwissentlich in unberechtigte Hände. Bekannte Beispiele sind Phishing-

Angriffe gegen Bankkunden, die in einer E-Mail aufgefordert werden, ihre Zugangsdaten auf der Webseite der Bank einzugeben und validieren zu lassen. Mit dem gleichen Verfahren werden aber auch Nutzer von E-Commerce-Anwendung angegriffen, z. B. Online-Shops oder Online-Dienstleister. Angreifer setzen zunehmend Schadprogramme statt klassischem Phishing als Mittel zum Identitätsdiebstahl ein. Andere Varianten des Phishings setzen auf gefälschte Near Field Communication (NFC)-Tags oder Barcodes, die vom Opfer eingelesen werden und auf eine Phishing-Seite weiterleiten.

- Spear-Phishing/Whaling
  Spear-Phishing ist eine Spezialform eines Phishing-Angriffs, bei dem nicht breitflächig, sondern nur ein kleiner Empfängerkreis (häufig Führungskräfte oder Wissensträger auf Leitungsebene) attackiert wird. Voraussetzung für einen erfolgreichen Angriff ist eine gute Vorbereitung und die Einbettung des Angriffs in einen für das Opfer glaubwürdigen Kontext. Spear-Phishing richtet sich in der Regel nicht gegen allgemein nutzbare Dienste wie Online-Banking, sondern gegen Dienste, die für Angreifer einen besonderen Wert haben.
- Maskerade
  Der Begriff „Maskerade“ beschreibt das Vortäuschen einer falschen Identität, was bei vielen Formen des Identitätsdiebstahls eine Rolle spielt.
- Man-in-the-Middle-Angriffe
  Im Allgemeinen ist ein Man-in-the-Middle-Angriff eine Angriffsmethode, bei der sich der Angreifer in die Kommunikation zwischen mindestens zwei Teilnehmern einschleust, um Daten lesen oder manipulieren zu können. In Bezug auf Identitätsdiebstahl werden Man-in-the-Middle-Angriffe heute häufig mittels Trojanischen Pferden durchgeführt, die Eingabefelder (z. B. Überweisungsempfänger und -betrag beim Online-Banking) auf dem System des Opfers (im Browser) manipulieren, bevor sie verschlüsselt an die Bank gesendet werden. Alternativ kann eine verschlüsselte Kommunikationsverbindung über einen Proxy-Server umgeleitet und aufgebrochen werden, auf dem die Daten dann unverschlüsselt vorliegen.
- Replay-Angriffe
  Replay-Angriffe beschreiben allgemein Angriffe, bei denen ein Informationsaustausch zuerst aufgezeichnet wird und die gewonnenen Informationen im Anschluss daran missbräuchlich wiederverwendet werden. Anhand eines aufgezeichneten Login-Vorgangs kann ein Angreifer beispielsweise versuchen, sich selbst unberechtigt Zugang zu dem jeweiligen System zu verschaffen.
- Nicknapping
  Personen treten im Internet mit ihrem realen Namen oder unter der Verwendung eines Pseudonyms oder Nicknames auf. Als „Nicknapping“ bezeichnet man einen Cyber-Angriff, bei dem der Angreifer unter einem bekannten Namen oder Pseudonym auftritt. Dadurch versucht der Angreifer, gegenüber Dritten den Eindruck zu erwecken, er sei der eigentliche/ursprüngliche Inhaber des Namens oder des Pseudonyms. Gelingt dies, kann der Angreifer in begrenztem Maße als der eigentliche/ursprüngliche Inhaber agieren. In der Vergangenheit wurden z. B. Twitter-Konten im Namen von Politikern erstellt, um darüber Falschmeldungen im Namen des Politikers zu verbreiten.
- Domain-Hijacking
  Mittels Domain-Hijacking wird ein Domainname unerlaubt auf einen Dritten übertragen. Dieser kann dann über die Domain verfügen, beliebige Inhalte bereitstellen und so z. B. Zugriff auf Authentisierungsmerkmale erhalten. Als „Cybersquatting“ bezeichnet man das Registrieren von Domainnamen bekannter Namen oder Marken, um diese mit Gewinn an die Rechteinhaber weiterzuverkaufen oder gegen sie zu verwenden.
- Spoofing
  Der Begriff „Spoofing“ bedeutet allgemein die Verschleierung der eigenen Identität, was für Identitätsdiebstahl in vielfältiger Weise genutzt wird. Beim klassischen Phishing, Spear-Phishing oder Spam werden z. B. E-Mails mit gefälschten Absenderadressen verschickt. Webseiten, die für Phishing- oder Pharming-Angriffe genutzt werden, geben vor, die Webseite eines vertrauenswürdigen Anbieters zu sein. IP-Spoofing wird beispielsweise bei DDoS-Angriffen verwendet, um den Ursprung des Angriffs zu verschleiern. Mittels ARP-Spoofing (ARP steht für „Address Resolution Protocol“) werden Kommunikationsverbindungen innerhalb eines Netzwerkes umgeleitet.
- Pharming
  Wie beim Phishing sind auch beim Pharming meist Zugangsdaten das Ziel eines Angriffs. Der Unterschied zum Phishing besteht darin, dass beim Pharming die Infrastruktur so manipuliert wird, dass das Opfer auch dann auf einer gefälschten Webseite landet, wenn er die korrekte Adresse des Dienstes eingeben hat. Technisch geschieht das in der Regel durch eine Manipulation der DNS-Einträge in der lokalen Hosts-Datei, an einem Zwischenspeicher oder an der zentralen DNS-Infrastruktur.
- Brute-Force-Angriff
  Wählen Nutzer ein schwaches Passwort und ist der Benutzername (z. B. die E-Mail-Adresse) bekannt, kann sich ein Angreifer unter Umständen auch durch wiederholtes Ausprobieren von Passwörtern (Brute-Force-Angriff) Zugang zu einem Benutzerkonto verschaffen. Mittels Brute-Force-Techniken kann der Angreifer auch versuchen, kryptografisch geschützte Daten, z. B. eine verschlüsselte Passwort-Datei, zu entschlüsseln.

- Missbrauch voreingestellter, schwacher oder mehrfach verwendeter Passwörter
  Hard- und Software-Komponenten können im Auslieferungszustand öffentlich bekannte oder einfach ableitbare Standard-Passwörter beinhalten. Werden diese nicht geändert, erhalten Angreifer mit geringem Aufwand Zugriff darauf. Durch die Vielzahl unterschiedlicher Benutzerkonten ist es wahrscheinlich, dass ein Nutzer identische Passwörter bei unterschiedlichen Diensten nutzt. Kommt ein Angreifer in Besitz eines gültigen Passwortes, kann dieser probieren, ob damit weitere Accounts des Nutzers übernommen werden können.
- Session-Hijacking/-Fixation
  Webapplikationen erkennen authentisierte Nutzer anhand von Session-IDs oder ähnlichen temporären Identifizierungsmerkmalen, die der Kommunikation zwischen Client und Dienst angehängt werden. Wenn ein Angreifer Zugriff auf diese Merkmale hat (Session-Hijacking) oder wenn er diese Merkmale von vornherein festlegen kann (Session-Fixation), hat er die gleichen Zugriffsrechte auf den Dienst wie der Benutzer der Zugangsdaten. Session-Hijacking und Session-Fixation sind besonders für Webanwendungen relevant, jedoch lassen sich diese Angriffsmethoden auch auf einige andere Protokolle, bei denen Session-IDs oder vergleichbare Merkmale ausgetauscht werden, anwenden.
- Diebstahl von Credentials
  Typische Beispiele für Credentials sind Passwörter, kryptografische Schlüssel und Zertifikate, sog. „Authentisierungs-Tickets“ oder auch „Session-Cookies“. Ein Diebstahl von Credentials kann z. B. Folge einer Attacke auf die Benutzerdatenbank von Webseiten oder Online-Diensten sein. Credentials können auch durch Schadsoftware-Infektionen auf Clients mitgeschnitten und so unbefugt an Dritte übermittelt werden. Es können aber auch gezielt Geräte wie Smartphones, Hardware-Tokens oder mobile Datenträger gestohlen werden, wenn ein Angreifer Zugangsdaten auf diesen Komponenten vermutet. Authentisierungs-Tickets oder Cookies können über unverschlüsselte Verbindungen mitgeschnitten werden.
- Fälschung von Credentials
  Ein Cyber-Angriff auf eine Zertifizierungsstelle (Certificate Authority) kann z. B. als Vorbereitung weiterer Angriffe durchgeführt werden. Ein Angreifer ist dadurch unter Umständen in der Lage, gefälschte Zertifikate zu erstellen und sie weitestgehend unbemerkt einzusetzen.
- Skimming
  Skimming bezeichnet das unbemerkte Auslesen von Zahlungskarten (Bank- und Kreditkarten) durch physikalische Manipulation von Geldautomaten oder Zahlungsterminals. Mit den ausgelesenen Daten werden in der Folge Karten-Kopien erstellt. Um auf das Konto des Opfers zugreifen zu können, wird meist auch die Eingabe der zugehörigen PIN aufgezeichnet, beispielsweise mithilfe einer kleinen, unauffälligen Kamera oder einer manipulierten Tastatur.

4.1.4 Hacking

In der IT-Sicherheit bezeichnet man Angreifer, die sich unbefugt Zugang zu Systemen oder Netzen verschaffen, oft als „Hacker“ oder „Cracker“.

Beispiele für deren Angriffsmethoden sind:

- Fuzzing
  Fuzzing ist eine automatisierte Testmethode für Software, bei der ein Programm eine Vielzahl automatisch generierter Eingabedaten verarbeiten muss, ohne dabei eine Fehlfunktion zu zeigen. Findet ein Hacker durch Fuzzing ein Eingabemuster, das eine Fehlfunktion erzeugt, muss überprüft werden, ob sich der gefundene Fehler als Sicherheitslücke ausnutzen lässt.
- Injection-Angriffe
  Viele Applikationen sind für Injection-Angriffe anfällig, wenn Benutzereingaben nicht ausreichend gefiltert werden. Eine SQL-Injection-Schwachstelle gibt einem Angreifer die Möglichkeit, Datenbankabfragen über eine Applikation so zu manipulieren, dass der für den Angreifer interessante Teil einer Datenbank zurückgegeben wird, anstatt des Teils, der ursprünglich für die Anwendung vorgesehen ist. Unter Umständen können durch SQL-Injection auch Änderungen an den Datenbank-Inhalten vorgenommen oder sogar Programmcode ausgeführt werden.
- Cross-Site-Scripting (XSS)
  Cross-Site-Scripting-Schwachstellen entstehen, wenn Benutzereingaben in einer Webanwendung ungefiltert durch den Server verarbeitet und an andere Clients zurückgegeben werden. Ein Angreifer hat damit unter Umständen die Möglichkeit, Programmcode wie JavaScript im Kontext des Benutzers einer Webseite auszuführen. Dies lässt sich unter anderem ausnutzen, um den Inhalt von Webseiten für einen Benutzer zu ändern oder auf Inhalte wie Cookies zugreifen zu können, um an Session-Informationen zu gelangen.
- Cross-Site-Request-Forgery (CSRF)
  Cross-Site-Request-Forgery ist eine weitere Angriffsform, die sich gegen Benutzer von Webanwendungen richtet. Mit dieser Vorgehensweise lassen sich Funktionen einer Webanwendung von einem Angreifer im Namen des Opfers nutzen. Ein Beispiel ist die Versendung einer gefälschten Statusnachricht in einem Sozialen Netzwerk: Ein Angreifer formuliert die Nachricht und schiebt sie

dem Opfer beim Abruf einer Webseite unter. Wenn der Angriff gelingt und das Opfer während des Angriffs parallel im betreffenden Sozialen Netzwerk angemeldet ist, wird die Nachricht des Angreifers im Namen des Opfers veröffentlicht.

- Poisoning
  Unter „Poisoning“ versteht man das Einschleusen von manipulierten Daten in einen Zwischenspeicher (Cache), der dann von anderen Anwendungen oder Diensten genutzt wird. Beispiele sind Angriffe mittels Poisoning auf DNS-, BGP-, oder ARP-Caches. Ein Angreifer kann so z. B. allgemein die Routen von Datenpaketen ändern oder gezielt Anfragen für Webseiten einer Bank auf eine gefälschte Seite umleiten.
- Reverse Engineering
  Mittels Reverse Engineering wird versucht, die Funktionsweise einer kompilierten Software zu analysieren, ohne dabei auf den Quelltext oder die Spezifikation der Software zugreifen zu müssen. Als Vorbereitung eines Cyber-Angriffs können z. B. Sicherheits-Updates mittels Reverse Engineering untersucht werden, um Erkenntnisse über Sicherheitslücken zu sammeln, die durch das Update geschlossen werden. Mittels dieser Informationen kann ein Angreifer Rückschlüsse ziehen, wie man diese Schwachstelle auf Systemen ausnutzen kann, die das Update nicht installiert haben.
- Missbrauch von Passwort-Zurücksetzen-Funktionen
  Anwendungen und Dienste bieten Nutzern häufig die Möglichkeit, ihr Passwort selbstständig zurückzusetzen, falls der Benutzer sein Passwort vergessen hat. Dabei werden häufig Informationen aus dem persönlichen Umfeld des Benutzers abgefragt, beispielsweise Geburtsnamen oder Namen von Haustieren. Mittels Social Engineering lassen sich solche Informationen jedoch teilweise mit geringem Aufwand ermitteln. Anstatt ein Passwort direkt anzugreifen, ist es in vielen Fällen einfacher, stattdessen die Passwort-Zurücksetzen-Funktion zu überwinden.
- Ausnutzen von Fehlkonfigurationen
  Durch den Einsatz von IT in vielen unterschiedlichen Bereichen und der daraus resultierenden hohen Gesamtkomplexität kann es schnell zu Fehlkonfigurationen kommen, die ein System für Cyber-Angriffe anfällig machen. So kann es z. B. passieren, dass die Konfiguration einer Firewall aufgrund eines neuen Produktes angepasst wird, ohne dass getestet wird, welche Auswirkungen auf die Sicherheit sich durch diese Änderung noch ergeben.
- Ausnutzen von Schwachstellen oder Implementierungsfehlern
  Implementierungsfehler und Schwachstellen können in jeder Software enthalten sein und unter Umständen als Einfallstor für Cyber-Angriffe dienen. Schwachstellen in Webbrowsern und Browser-Plugins werden z. B. häufig mittels Drive-by-Downloads zur Installation von Schadsoftware ausgenutzt. Schwachstellen im Betriebssystem selbst können in vielen Fällen dazu verwendet werden, die eigenen Benutzerrechte auszuweiten oder das System zum Absturz zu bringen.
- Ausnutzen von Design-Fehlern
  Schwachstellen durch Design-Fehler haben ihren Ursprung in fehlerhaften oder unvollständigen Spezifikationen von Anwendungen und Protokollen. Sie sind schwerer zu beheben als Implementierungsfehler und bleiben daher für Cyber-Angriffe häufig für einen längeren Zeitraum nutzbar. Konkrete Beispiele sind Angriffe auf Signaturverfahren, in denen Teile der signierten Daten ausgetauscht werden können, ohne die Signatur ungültig werden zu lassen (XML Signature Wrapping) oder die im PDF-Standard vorgesehene Möglichkeit, Programmcode außerhalb des Dokuments zu starten.

4.1.5 Menschliche und soziale Faktoren

Cyber-Angriffe sind stark durch die aktuellen Technologien der Informationsverarbeitung und des Internets geprägt. Dennoch müssen bei einer Analyse von Cyber-Angriffen auch die menschlichen und sozialen Aspekte berücksichtigt werden, da die Technik von Menschen konstruiert und genutzt wird.

Bei den folgenden potenziellen Faktoren von Cyber-Gefährdungen stehen nicht-technische Aspekte im Vordergrund:

- Diskreditierung/Rufschädigung
  Gelingt es einem Angreifer, interne bzw. vertrauliche Informationen zu veröffentlichen oder falsche Informationen in Umlauf zu bringen, kann damit die Integrität und das Ansehen von Personen oder Institutionen in der Öffentlichkeit beeinflusst werden. Eine Verunstaltung einer Webseite (Defacement) schadet dem Ansehen einer Organisation.
- Ablenkungsmanöver
  Ablenkungsmanöver können Cyber-Angriffe flankieren und die Wahrscheinlichkeit für einen Erfolg erhöhen. Beispielsweise könnte ein Angreifer einen DDoS-Angriff als Ablenkungsmanöver starten, um Ressourcen aufseiten des Angriffsziels zu binden. An anderer Stelle könnte dann parallel versucht werden, in das Netzwerk einzudringen.

- Irreführung
  Durch Verbreitung von falschen Informationen können Entscheidungen auf der Seite der Empfänger beeinflusst und so gezielt Fehlentscheidungen verursacht werden. Ein Beispiel für Irreführung ist das Vortäuschen einer Straftat.
- Erpressung/Nötigung/Korruption
  In diese Kategorie fallen beispielsweise Drohungen und Einschüchterungen per E-Mail, Erpressung zum Schutz vor DDoS-Angriffen sowie die Forderung von Lösegeld für Daten nach erfolgreicher Platzierung von Ransomware. Nach einem erfolgreichen Datendiebstahl kann das Opfer zusätzlich erpresst werden, indem mit einer Veröffentlichung von Daten oder Informationen über Sicherheitslücken gedroht wird.

4.2 Angriffspunkte

Primäre Angriffspunkte für Cyber-Angreifer sind die über Netze, insbesondere das Internet, erreichbaren IT-Komponenten der angegriffenen Ziele. Je größer diese exponierte Angriffsfläche ist, umso einfacher ist es für den Angreifer, einen Angriffspunkt zu identifizieren und die ersten Schritte eines Cyber-Angriffs erfolgreich durchzuführen. Viele der in Anhang B.2 genannten Ziele sind in gleicher Weise auch Angriffspunkte und somit das Objekt, das angegriffen wird, um das Angriffsziel zu erreichen.

Beispiele hierfür sind:

- Anwendungen mit Internetzugang
  Browser, E-Mail-Programme, mobile Endgeräte, usw. sind Angriffspunkte für die über sie verarbeiteten Informationen.
- Server
  Webserver, Kommunikationsserver, Firewalls, Remote-Wartungszugänge, usw. sind Angriffspunkte für Daten, die durch sie verarbeitet, übertragen oder geschützt werden.
- Schnittstellen und Zugänge
  ...sind Angriffspunkte, um Zugriff auf dahinterliegende Systeme und Netze zu erhalten oder diese zu stören.
- Dienste
  ...sind Angriffspunkte, um die durch sie bereitgestellte Funktion zu stören, zu manipulieren oder um Identitäten innerhalb des Dienstes zu missbrauchen.

4.3 Spurenbeseitigung

Um die Entdeckung eines Cyber-Angriffs und die Ermittlung des Täters zu erschweren, versuchen Angreifer meist, von vornherein keine Spuren zu erzeugen (siehe Anhang C.3 Angriffstarnung) oder die Spuren des Angriffs im Nachhinein zu beseitigen.

Dazu bedienen sie sich unter anderem folgender Techniken:

- Löschen oder Verbergen der auf dem Angriffspunkt genutzten Software, wie Hacking-Tools oder Schadsoftware.
- Löschen oder Verbergen der Spuren in Logdateien und Protokollen, mittels derer ein Cyber-Angriff im Nachhinein entdeckt werden könnte. Wenn es möglich ist, werden oft auch Logdateien auf den für den Angriff genutzten Zwischenstationen bereinigt.
- Löschen oder Verbergen von Dropzones, Command & Control-Servern und ähnlicher Infrastrukturen, die den Angreifern während des Angriffs als Hilfsmittel dienten.