DHBW
Duale Hochschule
Baden-Württemberg

Inwieweit eignet sich die Penetration Testing Suite Kali Linux zur systematischen Schwachstellenanalyse für mittelständische Unternehmen?

Studienarbeit

im Zusammenhang zum

Bachelor of Science

des Studiengangs Informatik

an der

Dualen Hochschule Baden-Württemberg Karlsruhe

von

Sarah Ficht

Abgabedatum 19.05.2025

Matrikelnummer	8717600
Kurs	TINF22B5
Gutachter der Studienakademie	Ralf Brune

Erklärung

Ich versichere hiermit, dass ich meine Studienarbeit mit dem Thema: *"Inwieweit eignet sich die Penetration Testing Suite Kali Linux zur systematischen Schwachstellenanalyse für mittelständische Unternehmen?"* selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Ich versichere zudem, dass die eingereichte elektronische Fassung mit der gedruckten Fassung übereinstimmt.

Ort Datum

Unterschrift

Zusammenfassung

Mittelständische Unternehmen sind zunehmend Ziel von Cyberangriffen, verfügen jedoch oft über begrenzte Ressourcen für eine umfassende IT-Sicherheit. Daher ist der Einsatz effizienter, kostengünstiger Sicherheitslösungen von hoher Relevanz.

Diese Arbeit untersucht die Eignung der Penetration Testing Suite Kali Linux zur systematischen Schwachstellenanalyse in mittelständischen Unternehmen. Dabei wird zunächst die rechtliche Grundlage des Penetration Testing in Deutschland analysiert, um den zulässigen Handlungsspielraum zu definieren.

Anschließend wird ermittelt, welche relevanten Angriffsvektoren für kleinere und mittlere Unternehmen (KMU) existieren. Darauf aufbauend wird untersucht, inwiefern Kali Linux Schwachstellen im Schutz vor diesen Angriffen aufdecken kann sowie welche Tools verwendet werden können, um die Resilienz gegenüber Cyberangriffen zu erhöhen.

Zusätzlich wird Kali Linux mit alternativen Schwachstellenanalyse-Tools verglichen, um die Effektivität und den praktischen Nutzen im Unternehmenskontext zu bewerten. Der Vergleich soll aufzeigen, inwiefern Kali Linux als eigenständige Lösung ausreicht oder durch zusätzliche Tools ergänzt werden sollte.

Aus der Bewertung der verschiedenen Tools ergibt sich zudem ein Leitfaden als Orientierungshilfe für KMU, der aufzeigt, inwiefern eine systematische Schwachstellenanalyse mit den untersuchten Werkzeugen möglich ist und wo potenzielle Lücken in der Abdeckung bestehen. Die Untersuchung erfolgt durch eine Kombination aus theoretischer Analyse und praktischem Vergleich der Tools anhand definierter Testkriterien.

Inhaltsverzeichnis

Algorithmenverzeichnis

Abkürzungsverzeichnis

Abbildungsverzeichnis

Kapitel 1

Einführung

1.1 Motivation

"Sicherheitslücken in IT-Systemen können in unserer vernetzten Welt dramatische Folgen haben. Cyberkriminelle und fremde Mächte können IT-Sicherheitslücken als Einfallstore nutzen. Krankenhäuser, Verkehrsunternehmen oder Kraftwerke können so lahmgelegt werden; persönliche Daten können ausspioniert, Unternehmen können ruiniert werden." [Buschmann 2024]

Im Zeitalter der Digitalisierung ist, wie Buschmann gesagt hat, nachhaltig wirksame IT-Sicherheit unerlässlich. So können unter anderen auch Internet of Things (IoT)-Geräte ein Einfallstor in Netzwerke bieten. IoT-Geräte verzeichnen eine immer weiter anwachsende Popularität und sind dabei im Netzwerk meist unzureichend abgeschirmt. Es existieren Websites wie Shodan, deren einzige Existenzberechtigung es ist, genau diese IoT-Geräte mit schwacher Sicherheit zu finden.

Jedoch befinden sich unter den schlecht abgesicherten Geräten auch sog. Honeypots. Das sind Geräte, die absichtlich Schwachstellen aufweisen, um Angreifer zu identifizieren. Dadurch kann das Verhalten der Angreifer auf den jeweiligen Systemen analysiert werden. Dies ermöglicht es, entsprechende Gegenmaßnahmen für reale Systeme einzuleiten.

Durch die Existenz von Honeypots wird die Anzahl der schwachen Geräte jedoch künstlich erhöht. Dadurch entsteht eine Verzerrung der Statistik. In der bezahlten Version von Shodan lassen sich die Honeypots über eine Flag filtern [achillean 2020]. Alternativ lässt sich mit dem Honeyscore auch eine Bewertung der Honeypot-Wahrscheinlichkeit einer einzelnen IP vornehmen [achillean 2025]. Dies ermöglicht es, einen realitätsnäheren Überblick über das Ausmaß der unsicheren Geräte zu erhalten.

Nichtsdestotrotz zeigt die reine Existenz von Shodan ein strukturelles Problem auf. Die Angriffsfläche für Cyberangriffe ist kolossal und wächst stetig. Angriffe auf kritische Infrastruktur kann dabei zu einer Katastrophe internationalen Ausmaßes führen. Beispielsweise kann der Angriff einer Stromkraftanlage zu einem Blackout und somit zu einem Dominoeffekt führen [Viola Kiel 2022].

Des Weiteren kann ein Denial-of-Service (DoS)-Angriff auf ein Krankenhaus zum Ausfall lebenserhaltender Geräte führen. Unter einem DoS-Angriff versteht man das Überfluten eines Systems mit Anfragen, sodass es nicht mehr in der Lage ist, auf weitere Anfragen zu reagieren bzw. den Dienst verweigert oder gar abstürzt [Bundesamt für Sicherheit in der Informationstechnik 2025a]. In 2.1.3 wird auf die verschiedenen Arten von Angriffen näher eingegangen. In jedem Fall bringen die Systemausfälle verheerende Folgen. Diese Angriffsfläche gilt es zu minimieren.

Reportagen wie *Putins Bären* zeigen auch, dass „fremde Mächte" hier nicht als eine überzogene Metapher zu verstehen sind, sondern eine reale Bedrohung darstellen [Simplicissimus 2024a]. Dabei wird deutlich gezeigt, wie mächtig und einflussreich ein Advanced Persistent Threat (APT) sein kann.

Ein APT bezeichnet einen hochentwickelten, meist staatlich unterstützten Angriff, der über einen längeren Zeitraum hinweg gezielt auf ein Netzwerk oder System ausgerichtet ist. Dabei dringt der Angreifer mit ausgefeilten Methoden in die Infrastruktur ein, bewegt sich darin unbemerkt und breitet sich möglicherweise weiter aus. Das Hauptziel besteht in der Sammlung sensibler Informationen oder der Durchführung von Manipulationen zur Spionage oder Sabotage [Bundesamt für Sicherheit in der Informationstechnik 2025b].

Dabei wird klar: Systeme können ohne Kenntnis der jeweiligen Netzwerkadministratoren infiltriert sein. So bietet auch die XZ Utils Backdoor einen Anlass zum Nachdenken. Diese Backdoor wurde in der Software XZ Utils entdeckt, die in vielen Linux-Distributionen als Standardkomponente enthalten ist. Dabei bleib diese über lange Zeit hinweg unentdeckt.

Wäre das Veröffentlichen der neuen Softwareversion mit der Backdoor nicht beinahe zufällig verhindert worden, hätte dadurch das gesamte Internet lahmgelegt werden können [Simplicissimus 2024b]. Diese Backdoor ermöglichte es, die Authentifizierung zum Fernzugriff auf Systeme zu umgehen [Bundesamt für Sicherheit in der Informationstechnik 2024c] und erlaubte Remote Code Execution [Group 2024].

Bösartiger Code wurde in den xz-Tarballs ab Version 5.6.0 entdeckt [Freund 2024]. Der liblzma-Buildprozess extrahiert dabei eine versteckte Objektdatei aus einer Testdatei, die Funktionen im liblzma-Code ändert [Group 2024]. So entsteht eine modifizierte Bibliothek, die von betroffener Software genutzt wird und Datenabfangung sowie -änderung ermöglicht [NIST 2025]. Dadurch kann die Authentifizierung via SSH umgangen werden, wenn wenn systemd für die Verwaltung der Sitzungen genutzt wird.

1.2 Hintergrund

Die voranschreitende Digitalisierung in Deutschland eröffnet Unternehmen zahlreiche Chancen und bringt durch Cyberangriffe zugleich erhebliche Risiken mit sich. Im Besonderen stehen mittelständische Unternehmen hierbei vor der Herausforderung, ihre IT-Infrastruktur gegen immer komplexere Angriffsmethoden zu schützen.

Häufig realisieren vereinzelte Personen die IT-Sicherheit eines ganzen Unternehmens, möglicherweise sogar neben vielen weiteren Zuständigkeitsbereichen. Der Spagat zwischen Ressourcenknappheit und der Notwendigkeit einer umfassenden IT-Sicherheit stellt eine Herausforderung dar, welche es mit vorliegender Arbeit zu adressieren gilt.

Diese Arbeit hat zum Ziel, eine möglichst große Aussage über einen möglichst großen Schnitt der Unternehmen in Deutschland zu treffen. Um diese Aussagekraft zu erhalten, wird sich am Mittelstand orientiert. Um Mittelständische Unternehmen von Großunternehmen abzugrenzen, wird die Definition der Bundeszentrale für politische Bildung verwendet.

"Mittelstand ist heute die gebräuchliche Bezeichnung für KMU [...]. Die Abgrenzung gegenüber Großbetrieben ist nicht immer einheitlich, wird jedoch bei öffentlichen Förderprogrammen z. B. über die Zahl der Beschäftigten (z. B. im produzierenden Gewerbe 50 bis 499 Beschäftigte) oder den Umsatz (nicht mehr als 50 Mio. € Umsatz pro Jahr) vorgenommen." [Bundeszentrale für politische Bildung 2021]

Der Mittelstand spielt eine zentrale Rolle in der deutschen Wirtschaft. Über 99% aller Unternehmen zählen zu diesem Sektor, der rund 43% der gesamten Wirtschaftsleistung erbringt. Im Mittelstand sind etwa 56% der Erwerbstätigen beschäftigt sowie rund 80% der Auszubildenden. Abb. 1.1 rechter Hand veranschaulicht diese Verteilung.

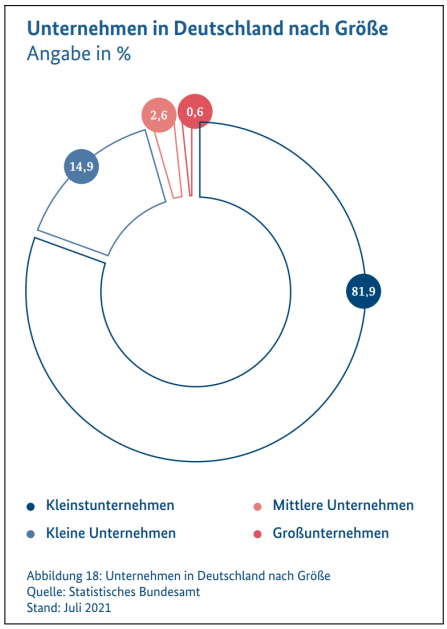

Abbildung 1.1: Die Anteilige Verteilung der Unternehmen nach Unternehmensgröße [Bundesamt für Sicherheit in der Informationstechnik 2023]

Im Jahr 2023 gaben 58% der befragten Unternehmen in Deutschland an, dass sie in den letzten 12 Monaten mindestens einmal Opfer von Cyberangriffen geworden sind. [Hiscox 2023] Deutschland belegt dabei den zweiten Platz unter den Ländern: Belgien, Frankreich, Deutschland, Irland, Niederlande, Spanien, UK und den USA. Mit 71% liegt der Anteil der betroffenen Unternehmen nur in Irland noch höher.

Innerhalb der darauffolgenden zwölf Monate gaben 80% der Unternhemen an, dass Cyberattacken auf ihr Unternehmen zugenommen haben. Im Sektor der kritischen Infrastrukturen stieg diese Zahl auf 83%, wobei hier ein größerer Anteil der Unternehmen sogar eine starke Zunahme verzeichnet. [Bitkom 2024a]

Seit 2021 stieg der prozentuale Anteil der Unternehmen, welche ihre Existenz durch Cyberangriffe bedroht sahen, von 9% auf einen Gesamtanteil von 65%. [Bitkom 2024b] Abb. 1.2 auf Seite 10 veranschaulicht diese Entwicklung.

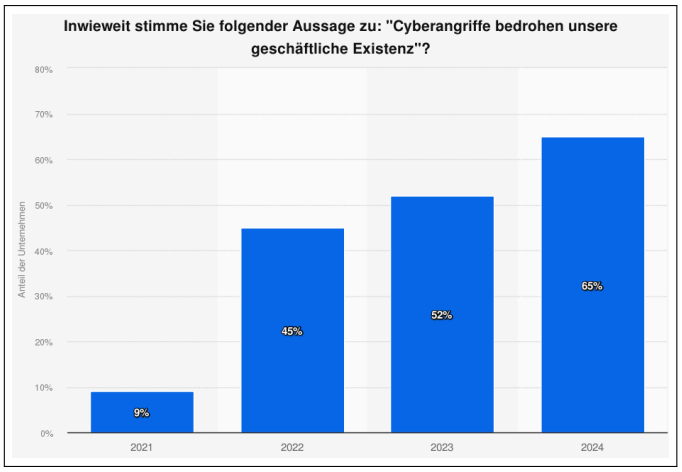

Abbildung 1.2: Die Entwicklung der wahrgenommenen Existenzbedrohung [Bitkom 2024b]

Dies scheint sich auch in den Investitionen in die Unternehmensinterne Cybersecurity widerzuspiegeln. So gaben 72% der deutschen Unternehmen an, dass sie ihre Cyber-Budgets für das Jahr 2025 erhöht haben [PwC 2024]. Nur 8% gaben eine Verringerung des Budgets an, während 15% angaben, dass das Budget gleich bleiben wird.

Obwohl die wahrgenommene Notwendigkeit für Investitionen steigt, investieren viele Unternehmen nicht ausreichend in ihre Sicherheit. Sie erkennen im besten Fall einen Teil der Bedrohungslage, jedoch seltenst in einem ausreichenden Maße. So urteilt das Bundesamt für Sicherheit in der Informationstechnik (BSI) im aktuellen Lagebericht wie folgt:

"Auch im Jahr 2024 besitzen viele Unternehmen nach Erfahrung des BSI weder eine ausreichende Kenntnis über die allgemeine Cyberbedrohungslage noch über das eigene Risikoprofil." [Bundesamt für Sicherheit in der Informationstechnik 2024b]

Die Schadensumme, welche für deutsche Unternehmen im Jahr 2024 durch Cyberattacken entstanden ist, beläuft sich auf rund 179 Milliarden Euro [Bitkom 2024c]. Damit hat nahm die Schadensumme, im Vergleich zum Vorjahr 2023, um 20% zu. Die Auswirkungen von Cyberangriffen auf die deutsche Wirtschaft sind demnach nicht zu unterschätzen.

Die Auswirkungen, welche dabei am meisten gefürchetet werden, ist auf Platz eins der Totalausfall des eigenen IT-Systems (65%). Auf Platz zwei folgt die Furcht vor Umsatzeinbußen (48,9%), dich gefolgt von der ungewollten Veröffentlichung eigener Kundendaten (48,5%) [CyberDirekt 2022].

1.3 Problemstellung

Nach Lagebericht des BSI aus dem Jahr 2024, werden selbst Elementare und kostenfreie Präventionsmaßnahmen häufig nicht ergriffen [Bundesamt für Sicherheit in der Informationstechnik 2024b]. Dennoch gibt es auch Unternehmen, die sich der Problematik bewusst sind und Personal einstellen möchten. Diese Unternehmen stellen jedoch fest, dass sie als potenzielle Arbeitgeber auf einem Angebotsmarkt nicht mit den Gehältern von Großunternehmen oder IT-Dienstleistern konkurrieren können. Zudem wird berichtet, dass Unternehmen, die ihre IT-Sicherheit an externe Dienstleister auslagern möchten, häufig feststellen müssten, dass es in ihrer Region entweder zu wenige qualifizierte Dienstleister gebe oder nur solche, die nicht zur eigenen Unternehmensgröße passen.

Die Zahl der KMUs, die bereit seien, mehr für ihre IT-Sicherheit zu tun wüssten oftmals jedoch nicht, wie sie dabei vorgehen sollten. Existierende Standardwerke seien meist zu komplex, um für KMUs geeignet zu sein. In Kooperation mit dem Bundesverband mittelständische Wirtschaft (BVMW) entstand so ein Konsortium zur Erstellung einer, für KMUs geeigneten, Spezifikation. Die Spezifikation stellt einen standardisierten Beratungsprozess zur Bestimmung des eigenen Risikoprofils bereit [Bundesverband mittelständische Wirtschaft 2023].

Mit der Erhebung des IST-Zustandes und den daraus resultierenden Handlungsempfehlungen soll ressourceneffizient eine Verbesserung der IT-Sicherheit möglich werden. Dabei wird sich auf die relevantesten Anforderungen zur Informationssicherheit beschränkt. Weiterführend bietet das BSI Hilfestellungen für KMUs in variabler Komplexität an [Bundesamt für Sicherheit in der Informationstechnik 2024a].

Daraus resultierend soll sich der Schaden durch Cyberangriffe auf mittelständische Unternehmen sukzessive verringern. Nach dem Durchlaufen des standardisierten Prüfprozesses des eigenen Risikoprofils wird empfohlen, die Handlungsempfehlungen in der Praxis umzusetzen. Dabei liegt der Fokus auf der konkreten Umsetzung von Maßnahmen zur Verbesserung der IT-Sicherheit.

Der Risiko-Check erfasst den Ist-Zustand jedoch nur rudimentär, um möglichst schnell Handlungsempfehlungen abzuleiten. Eine daraus resultierende Handlungsempfehlungen könnte etwa den Hinweis enthalten, ein Passwort zu ändern. Das ist zwar wichtig, bringt aber nur begrenzt viel und gleicht eher einer Symptombehandlung: hilfreich im Notfall, behebt langfristig jedoch nicht die Ursache des Problems.

Wenn Passwörter mehrfach verwendet werden, öffnen sie Tür und Tor für Angreifer. Ein einmal kompromittiertes Passwort kann dann gleich mehrere Dienste gefährden. Daher gilt es in diesem Fall sofort zu handeln, sprich: die Passwörter zu ändern. Das sind jedoch nur die ersten Schritte und nicht die Lösung des Problems.

Es stellt sich die Frage, wie die Absicherung umgesetzt werden kann, wenn für diese Umsetzung Budget fehlt. Unter diesem Gesichtspunkt wird in dieser Arbeit auf die kostenfreien Tools von Kali Linux zurückgegriffen. Dabei wird Kali Linux als All-in-One Toolset untersucht und bewertet, um zu prüfen, ob und in welchem Maße es sich für die Absicherung von mittelständischen Unternehmen eignet.

1.4 Zielsetzung der Arbeit

Das Ergebnis dieser Arbeit soll eine umfassende Analyse von Kali Linux ergeben, hinsichtlich der Eignung der Penetrationtesting-Suite als All-in-One Toolset. Das Toolset soll dabei Schwachstellen aufdecken können, welche für mittelständischen Unternehmen von besonderer Relevanz sind. Kali Linux wird untersucht und bewertet, um zu prüfen, ob und in welchem Maße es sich für die Absicherung von mittelständischen Unternehmen eignet.

Dabei wird zunächst auf die Angriffsvektoren bei mittelständischen Unternehmen eingegangen. Ein Angriffsvektor ist ein Weg, den Angreifer nutzen, um sich unbefugt Zugang zu einem Netzwerk oder System zu verschaffen [Cloudflare 2025b].

Es wird untersucht, welche Angriffsvektoren die größte Angriffsfläche bieten oder sich in der Vergangenheit als besonders anfällig erwiesen haben. Kali Linux wird hinsichtlich der integrierten Tools untersucht, die für die Durchführung eines Penetrationtests benötigt werden.

Es werden jene Tools im Fokus der Evaluation stehen, welche die Angriffsvektoren am besten abbilden. Die Tools werden dabei auf die jeweiligen Angriffsvektoren angewendet. Ist ein häufiger Angriffsvektor beispielsweise ein falsch konfigurierter Mailserver, so wird ein Penetrationtestingzyklus auf diesen Angriffsvektor mit den integrierten Tools von Kali Linux angewendet.

Der Penetrationtestingzyklus soll Aufschluss darüber geben, wie gut Kali Linux in der Lage ist, einen in der Praxis meist erfolgreichen Angriffsvektor, als All-In-One Toolset umzusetzen.

1.5 Aufbau der Arbeit

Zunächst erörtert Kapitel 2 die Grundlagen der IT-Sicherheit. Dabei werden Begriffe definiert und abgegrenzt, um ein einheitliches Verständnis zu schaffen. Nachdem die Terminologie geklärt ist, folgt in Kapitel 2.1.2 die Betrachtung der Rechtsgrundlagen, die für die IT-Sicherheitsforschung von Relevanz sind. Das ist für diese Arbeit von Bedeutung, da sich das Penetrationtesting in einer rechtlichen Grauzone bewegt.

Darauf aufbauend erfolgt ein Überblick über die verschiedenen Arten von Angriffen. Im Anschluss wird der Prozess des Penetrationtestings erläutert. Die verschiedenen Arten, Methoden, Typen und Phasen des Penetrationtestings werden vorgestellt, welche die Grundlage für die spätere Anwendung der Tools bilden.

Kali Linux wird in Kapitel 2.3 analysiert. Dabei erfolgt eine Betrachtung der verschiedenen Distributionen sowie der dabei integrierten Tools. Dies bietet einen Überblick über die Tools, die für die Durchführung eines Penetrationtests erforderlich sein könnten.

In Kapitel 3.1 erfolgt eine Betrachtung der Angriffsvektoren bei mittelständischen Unternehmen. Dabei wird erläutert, welche Angriffe in Deutschland auf mittelständische Unternehmen üblich sind. Es wird der Frage nachgegangen, durch welche Angriffsvektoren die meisten Erfolge der Hacker erzielt werden. Ein Angriff auf diese Vektoren gilt es dann mit Kali Linux vorzubereiten und nachzustellen.

Der Penetrationtestingzyklus wird in Kapitel 3.2 zunächst auf die größte Angriffsfläche angewendet. Dabei gilt es zu evaluieren, welche Tools von Kali am geeignetsten sind, wie diese angewendet werden und wie sie dabei abschneiden. Auf Grundlage des Ergebnisses erfolgt eine Bewertung von Kali hinsichtlich der Effektivität.

Das Ziel besteht im erfolgreichen Durchlaufen des vollständigen Penetrationtestingzyklus. Dabei gilt es Hürden zu adressieren und zu überwinden. Die Ergebnisse werden anschließend in Kapitel 4 zusammengefasst und bewertet. Abschließend wird es einen Ausblick auf mögliche zukünftige Entwicklungen gegeben.

Kapitel 2

Grundlagen

2.1 Hacking

2.1.1 Begriffsdefinition

2.1.2 Rechtsgrundlage

Bisherige Lage seit 2007

Die Rechtsgrundlage für das "Hacking" in Deutschland ist im Strafgesetzbuch (StGB) geregelt. Dabei sind die Paragrafen § 202a, § 202b und § 202c von besonderer Relevanz. § 202a StGB regelt das Ausspähen von Daten, § 202b StGB das Abfangen von Daten und §202c StGB das Vorbereiten des Ausspähens und Abfangens von Daten.

Der § 202a StGB wurde 1986 verabschiedet und im Zuge der zusätzlichen Paragrafen 2007 überarbeitet. [*Bundesgesetzblatt BGBl. Online-Archiv 1949 - 2022 | Bundesanzeiger Verlag* 1986] Das Ausspähen von Daten ist gegeben, wenn sich durch die Überwindung der Zugangssicherung, an für einen selbst unbefugte Daten, Zugang verschafft wird. Dazu zählt das Knacken eines fremden Passworts sowie das Umgehen einer Firewall. Im Folgenden einen Auszug, siehe [*Synopse_ComputerStrafR_RefE.pdf* 2024].

Strafgesetzbuch (StGB) § 202a Ausspähen von Daten
(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.
(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

Der § 202b StGB wurde zusammen mit dem § 202c StGB 2007 verabschiedet. [*Bundesgesetzblatt BGBl. Online-Archiv 1949 - 2022 | Bundesanzeiger Verlag* 2007] Daten gelten als abgefangen, wenn unbefugte auf dem Weg der Übermittlung Zugang zu den Daten gelangen. Dazu zählen die als "Man in the Middle" bekannten Angriffe. Im Folgenden einen Auszug, siehe [*Synopse_ComputerStrafR_RefE.pdf* 2024].

Strafgesetzbuch (StGB) § 202b Abfangen von Daten
Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der

elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

Das Vorbereiten des Ausspähens und Abfangens von Daten betrifft das Herstellen, Überlassen oder Verbreiten von Software oder Werkzeugen, die speziell für Hacking oder Datenmanipulation entwickelt wurden. Daher ist dieser als sog. "Hackerparagraf" bekannt. Dieser erschwert die Lage der IT-Sicherheitsforscher, da diese die Tools benötigen, um Sicherheitslücken aufzudecken. Im Folgenden einen Auszug, siehe [*Synopse_ComputerStrafR_RefE.pdf* 2024].

Strafgesetzbuch (StGB) § 202c Vorbereiten des Ausspähens und Abfangens von Daten
(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. *Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder*
2. *Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.*

(2) § 149 Abs. 2 und 3 gilt entsprechend.

Da durch den "Hackerparagraf" (§ 202c StGB) das Verbot von notwendigen Tools zur IT-Sicherheitsforschung einher geht, hat dieser hat eine Vielzahl an Kritiken geerntet. Eine Überarbeitung der Gesetzeslage wurde vermehrt eingefordert. So gehe § 202c StGB zu weit und schränke die IT-Sicherheitsforschung ein. [Meister 2024]

"Durch die rechtliche Unsicherheit für Sicherheitsforscher und Unternehmen im Umgang mit potentieller Schadsoftware ergibt sich zudem ein fallendes Sicherheitsniveau deutscher IT-Systeme." [Kurz u. a. 2008]

""Dieser Hacker-Paragraf wird auf jeden Fall die Tätigkeit von Security-Unternehmen einschränken", sagt Dirk Hochstrate [...]." [Zschunke 2007]

Die dadurch fehlende Weitsicht bezüglich Deutschland als wirtschaftlichen Industriestandort war eine durchaus laute Kritik, welche unter anderem von dem Chaos Computer Club (CCC) zum Ausdruck gebracht wurde. [Wilkens 2008] [Kurz u. a. 2008]

"Vielmehr senke die Kriminalisierung von Softwareherstellern und -benutzern das Sicherheitsniveau in Deutschland, was zu einem Standortnachteil für die deutsche Forschung und Wirtschaft werde." [Ihlenfeld 2008]

Diese, sowie viele weitere Communities, haben die Folgen für Deutschland früh absehen können. In Deutschland können Unternehmen sowie jegliche Infrastruktur somit nur auf IT-Sicherheit überprüft werden, wenn dies von der jeweiligen Frührungsriege abgesegnet wird. Wird jedoch der Stellenwert der IT-Sicherheit verkannt, bleiben notwendige Maßnahmen aus. So sind die nun vielfach in den Nachrichten genannten Cyberangriffe eine logische Konsequenz aus den ausbleibenden Sicherheitsüberprüfungen. Für den CCC schon damals äußerst klar.

"Der Gesetzgeber habe sein Ziel der Verbesserung der IT-Sicherheitslage verfehlt. Langfristig werde Deutschland zum Ziel von Kriminellen und zum Einfallstor für Wirtschaftsspionage, da die Computernetze nicht mehr wirksam verteidigt werden können, kommentiert der Sprecher des CCC, Frank Rieger." [Wilkens 2008]

Neuer Gesetzesentwurf

"Wer IT-Sicherheitslücken schließen möchte, hat Anerkennung verdient – nicht Post vom Staatsanwalt." [Buschmann 2024]

Die Pressemitteilung Nr. 97/2024 vom 04. November 2024 des Bundesministerium der Justiz (BMJ) sieht vor, dass das Aufspüren von Sicherheitslücken unter Umständen einen Tatbestandsausschluss erhält. So soll die bisher unsichere Rechtslage für IT-Sicherheitsforscher verbessert werden. Als Voraussetzung des Strafbarkeitsausschlusses gilt es, nach neuem § 202a mit Abs. 3 StGB, eine Feststellungsabsicht, Unterrichtungsabsicht und eine Erforderlichkeit kumulativ zu erfüllen. Somit soll die Strafbarkeit ausbleiben, sofern nur zur absichtlichen Feststellung der Sicherheitslücke erforderliche Praktiken angewandt werden und eine Meldung der gefundenen Lücke folgt.

Des Weiteren wird eine besondere Schwere des Strafbestandes definiert, sofern die Voraussetzungen des Tatbestandsausschlusses nicht erfüllt und zudem weitere Bedingungen erfüllt sind. Diese sind zum einen, das Auslösen eines großen Vermögensverlustes, einem gewerbsmäßigen bzw. gewinnsüchtigen Handeln, als auch dem dort näher definierten Schaden der kritischen Infrastruktur bzw. der Sicherheit in Deutschland oder dessen Ländern. [*BMJ - Pressemitteilungen - Rechtssicherheit für die Erforschung von IT-Sicherheitslücken: Bundesjustizministerium veröffentlicht Gesetzentwurf zum Computerstrafrecht* 2024]

Die potenziell neue Gesetzeslage könnte nun zulassen, dass Systeme auf IT-Sicherheit geprüft werden dürfen, selbst wenn Besitzer dieser Systeme keinen Auftrag zur Überprüfung erteilt haben. So kann nun, unabhängig des (un-)erkannten Wertes für IT-Sicherheit, jegliches IT-System in Deutschland straffrei auf die Probe gestellt werden.

Deutschland als Industriestandort kann davon profitieren, indem Systemausfälle aufgrund von Cyberangriffen präventiv entgegengewirkt werden kann. Dies kann auch als wichtigen und notwendigen Schritt für die deutsche Wirtschaft angesehen werden.

Trotz der Einsicht, die der Gesetzesentwurf mit sich bringt, gibt es auch kritische Stimmen. So auch von Lillith Wittmann, welche nach dem Aufdecken einer Sicherheitslücke in einer Wahlkampf-App der CDU eine Strafanzeige erhielt. [Hurtz 2021]

"Es ist zwar gut, dass Hackerinnen, die in positiver Absicht handeln, zukünftig nicht mehr kriminalisiert werden sollen. Es ist aber traurig, dass diese „Absicht" vermutlich nicht so einfach feststellbar ist. Denn wenn die erst vor Gericht, vielleicht nach einer Hausdurchsuchung und ähnlichen Repressionen durch den Staat festgestellt wird, dann wurde die Situation de facto nicht wirklich verbessert." [Meister 2024]

Durch die Änderungen von §202a StGB und §202b StGB wird eine Änderung von §202c StGB vom BMJ als obsolet angesehen. [*Infopapier_ComputerStrafR.pdf* 2024] Das BMJ gibt zu Papier, dass die Änderungen von §202a StGB und §202b StGB dazu führen werden, dass für die IT-Sicherheitsforscher keine Strafbarkeitsrisiken mehr bestehen. [*Infopapier_ComputerStrafR.pdf* 2024] Die betreffenden IT-Sicherheitsforscher sehen dies jedoch anders, so kommentiert der Sprecher des CCC Dirk Engeling wie folgt:

"Wir begrüßen die Einsicht des Gesetzgebers, dass Inspektionen angeblich sicherer IT-Systeme im Grundsatz legal sind. Statt jedoch durch Abschaffen des schädlichen § 202c ein Signal zu senden, Computersicherheit würde auch hierzulande endlich ernstgenommen, erlaubt der Entwurf aber nur offensichtlich harmlose Besichtigungen ausdrücklich. Berufliche Sicherheitsforscher arbeiten auch zukünftig weitestgehend in einer gefährlichen Grauzone." [Meister 2024]

Bruch der Ampel-Koalition

Auf Grundlage des Bruchs der Ampel-Koalition ist die Umsetzung des Gesetzesentwurfes vorerst hinfällig. Abzuwarten bleibt, was die nächste Regierungskoalition für die IT-Sicherheitsforschung in Deutschland bereithält.

2.1.3 Angriffstypen

Ein Cyberangriff bezeichnet eine gezielte Aktion, bei der ein Akteur versucht, digitale Systeme oder Netzwerke zu kompromittieren. Ziel eines solchen Angriffs kann der unautorisierte Zugriff auf Daten, die Manipulation von Informationen oder die Störung betrieblicher Abläufe sein. Betroffene Systeme können unter anderem Computer, Netzwerke, Server, Informationsinfrastrukturen und sicherheitskritische Systeme sein. Ein Cyberangriff verfolgt häufig das Ziel, administrative Kontrolle über ein System zu erlangen oder dessen Funktionalität zu beeinträchtigen, wodurch gespeicherte Daten zugänglich gemacht oder betroffene Prozesse gestört werden können. [Lee 2025]

Die Angriffe besitzen Ausprägungen, nach denen sich kategorisieren lässt. Im folgenden wird auf gängige Angriffstypen eingegangen, die in der Literatur und von Sicherheitsforschern häufig beschrieben werden um einen Überblick zu geben.

Man-in-the-Middle

Ein Man-in-the-Middle (MitM)-Angriff bezeichnet eine Form der Cyberattacke, bei der sich der Angreifer heimlich zwischen zwei kommunizierende Parteien schaltet. Diese Parteien könnten zum Beispiel ein Computer und ein Server oder ein Server und eine Webanwendung sein [Lee 2025] Der Angreifer kann die Kommunikation abfangen, mitlesen, manipulieren oder sogar falsche Informationen einschleusen, ohne dass die beteiligten Parteien es bemerken. Ziel eines MitM-Angriffs ist es oft, sensible Daten wie Passwörter, Kreditkarteninformationen oder vertrauliche Nachrichten zu stehlen oder die Kommunikation zu stören.

Denial-of-Service

Ein DoS bezeichnet eine Situation, in der Dienste, die eigentlich über das Internet erreichbar sein sollten, nicht verfügbar sind [Bundesamt für Sicherheit in der Informationstechnik 2025a]. Dies kann durch physische Erreichbarkeitsprobleme, ungewollte Überlastung oder gezielte Angriffe verursacht werden. Ein gezielter Angriff, überlastet das Zielsystem mit einer großen Anzahl an Anfragen, was zu einer langsamen Reaktionszeit oder Inaktivität der Dienste führt. In diesem Fall sind die Dienste für legitime Nutzer nur mit starken Verzögerungen erreichbar. Manchmal versuchen Angreifer auch, gezielt Programmfehler im Zielsystem auszunutzen, was nicht nur zu Verlangsamung, sondern auch zu Fehlverhalten oder sogar Abstürzen des Systems führen kann.

Distributed-Denial-of-Service

Um einen Distributed-Denial-of-Service (DDoS)-Angriff handelt es sich, wenn ein Angriff von mehreren Systemen gleichzeitig ausgeführt wird. Dafür wird meist ein Botnetz verwendet. Ein Botnetz ist ein Netzwerk von infizierten Computern, die von einem Angreifer kontrolliert werden. Dabei sind nicht nur klassische PCs betroffen, sondern auch alle internetfähigen Geräte wie Smart-TVs oder Kameras [Kriminalprävention der Länder und des Bundes 2025]. Diese Geräte werden dann von einem Angreifer ferngesteuert, um eine große Menge von Anfragen an das Zielsystem zu senden.

SQL-Injection

SQL-Injection ist eine Sicherheitslücke, bei der ein Angreifer schadhafter SQL-Code in eine Datenbankabfrage einschleust, was zu schwerwiegenden Folgen wie dem Diebstahl von Daten, der Veränderung oder dem Löschen von Daten sowie der Ausführung von schadhafter Software führen kann.

Um sich vor SQL-Injection zu schützen, gibt es verschiedene Maßnahmen. Eine wichtige Technik ist die Verwendung von Prepared Statements, bei denen Benutzereingaben als sichere Parameter in SQL-Abfragen eingefügt werden, wodurch schadhafter Code verhindert wird. Auch Stored Procedures bieten Schutz, indem sie vorgefertigte, sichere SQL-Abfragen definieren. Eingabevalidierung ist ebenfalls entscheidend, da so Eingaben auf gültige Formate geprüft und unsichere Eingaben herausgefiltert werden.

Zero-Day-Exploits

Ein Zero-Day-Exploit bezeichnet eine Sicherheitslücke in Hard- oder Software, die zum Zeitpunkt ihrer Entdeckung dem Hersteller noch unbekannt ist und daher nicht durch Updates oder Sicherheitspatches behoben wurde. Solche Schwachstellen können von Angreifern ausgenutzt werden, um unautorisierten Zugriff auf Systeme zu erlangen, Schadsoftware zu installieren oder sensible Daten zu stehlen. Aufgrund der fehlenden Schutzmaßnahmen stellen Zero-Day-Exploits ein besonders hohes Sicherheitsrisiko dar.

DNS-Tunneling

DNS-Tunnelling bezeichnet eine Technik zur Umgehung von Sicherheitsmechanismen. Dabei wird das Domain Name System (DNS) zweckentfremdet, um Daten in DNS-Paketen zu übertragen. Firewalls und andere Sicherheitslösungen können so konfiguriert sein, dass sie DNS-Verkehr ungefiltert zulassen, um die Namensauflösung zu ermöglichen [Attack Detect Defend 2020]. Dabei wird das eigentlich für die Namensauflösung von IP-Adressen vorgesehene DNS-Protokoll genutzt, um eine verdeckte Kommunikationsverbindung herzustellen.

Diese Technik ermöglicht es Schadsoftware zu versenden, indem DNS-Antworten manipuliert werden. Dadurch kann das kompromittierte System die DNS-Antworten als Befehle interpretieren. Zudem kann das einbetten von Daten in DNS-Anfragen dazu genutzt werden, um sensible Daten aus einem gesicherten Netzwerk auszuschleusen.

Cross-Site-Scripting

Cross-Site-Scripting (XSS) ist ein Angriff der Injektion, bei der schädlicher Code, meist in Form von JavaScript, in Webseiten einfügt wird. Von anderen Nutzern, die die Webseite besuchen, wird dieser Code daraufhin ausgeführt. Da der Browser das Skript als vertrauenswürdig einstuft, kann das schadhafte Script auf alle Cookies, Sessiontokens oder andere vertrauliche Informationen zugreifen, die vom Browser gespeichert und mit der Website verwendet werden. XSS ermöglicht es Angreifern daher, Benutzerdaten zu stehlen, Sessions zu kapern oder den Inhalt der HTML-Seite als solches zu verändern.

Diese Lücke entsteht, wenn Webanwendungen Benutzereingaben nicht ausreichend validieren oder kodieren. Es gibt drei Hauptarten von XSS: reflektiertes XSS, bei dem der Code sofort ausgeführt wird, gespeichertes XSS, bei dem der Code auf dem Server gespeichert wird, und DOM-basiertes XSS, bei dem der Code auf der Client-Seite ausgeführt wird [KirstenS 2025].

Cross-Site-Request-Forgery

Cross-Site-Request-Forgery (CSRF) ist ein Angriff, bei welchem ein authentifizierter Benutzer dazu verleitet, ungewollte Aktionen auf einer Webanwendung auszuführen. Dies geschieht durch das Einschleusen einer schadhaften Anfrage, die vom Browser des Benutzers ausgeführt wird. Dabei werden die bestehenden Authentifizierungsinformationen missbraucht [Cloudflare 2025a]. Der Angreifer kann dadurch unerwünschte Änderungen an Einstellungen, Überweisungen oder Datenmanipulationen vornehmen.

Anti-CSRF-Tokens sind kryptografisch zufällig generierte Werte, die eingesetzt werden, um sicherzustellen, dass Anfragen nur von authentifizierten Benutzern und nicht von Angreifern stammen. Diese Tokens werden in Formulare eingebettet und bei der Serververarbeitung überprüft, um die Integrität der Anfrage zu gewährleisten und CSRF-Angriffe zu verhindern.

Phishing

Phishing ist ein Versuch, Menschen dazu zu bringen, ihre persönlichen Daten wie Passwörter oder Bankinformationen preiszugeben. Angreifer tun dies, indem sie sich als vertrauenswürdige Quellen ausgeben, zum Beispiel durch gefälschte E-Mails oder Webseiten, die wie echte aussehen. Das Ziel ist es, das Opfer dazu zu bringen, auf einen Link zu klicken oder sensible Daten einzugeben. Phishing kann auch per Telefon oder Short Message Service (SMS) erfolgen. In vielen Fällen wird so versucht, Zugang zu Konten oder Geräten zu bekommen oder schadhafte Software zu installieren.

Malware

Malware bezeichnet Software, die entwickelt wurde, um Schäden an Computern oder Netzwerken zu verursachen. Sie kann verschiedene Formen annehmen, wie Viren, Würmer, Trojaner oder Ransomware. Malware wird oft unbemerkt auf ein System eingeschleust und kann Daten stehlen, das System lahmlegen oder unbefugt Zugriff auf Informationen ermöglichen. Sie wird in der Regel über unsichere Quellen wie E-Mails, Webseiten oder infizierte Software verbreitet. Das Ziel von Malware ist es, das betroffene System zu kontrollieren (siehe DDoS 2.1.3), zu beschädigen oder vertrauliche Daten zu stehlen.

Ransomware

Ransomware ist eine Form von Malware, die darauf abzielt, den Zugriff auf ein Computersystem oder dessen Daten zu blockieren. Der Angreifer verschlüsselt die Daten oder sperrt den Zugang zu wichtigen Funktionen und verlangt eine Lösegeldzahlung, um den Zugriff wieder freizugeben. Ransomware wird häufig über Phishing-E-Mails, infizierte Webseiten oder unsichere Downloads verbreitet. Sie kann sowohl Einzelpersonen als auch Unternehmen betreffen und zu erheblichen finanziellen und operativen Schäden führen. Die Zahlung des Lösegeldes garantiert jedoch nicht immer die Rückgabe der Daten oder den Wiederherstellungszugang.

Social Engineering

Social Engineering ist eine Technik, bei der Angreifer psychologische Manipulationen einsetzen, um Menschen dazu zu bringen, vertrauliche Informationen preiszugeben oder sicherheitsrelevante Handlungen auszuführen. Dabei wird das Vertrauen, die Hilfsbereitschaft oder die Angst der Zielperson ausgenutzt, um Sicherheitsmaßnahmen zu umgehen. Social Engineering kann über verschiedene Kommunikationskanäle wie E-Mails, Telefonanrufe oder auch persönliche Gespräche erfolgen. Ziel ist es, den Nutzer zu täuschen und ihn dazu zu bringen, auf schadhafte Links zu klicken, Passwörter zu verraten oder unerlaubte Aktionen durchzuführen.

typische Angriffsmuster

Seite 97 für Kategorien der Angriffe [Bartsch und Frey 2017]

DDOS: mit CaaS Cybercrime as a service mgl. S. 53-54 [Lange u. a. 2019]
[Mehta 2017]

2.2 Penetrationtesting

Penetrationtests dienen dazu, theoretische Sicherheitskonzepte in der Praxis zu überprüfen. Dabei wird versucht, die Sicherheitsmechanismen eines Systems zu durchbrechen oder zu umgehen. Dieser Vorgang wird auch als *Penetration* bezeichnet [Shimonski und Delbrueck 2023]. Dadurch, dass viele Möglichkeiten für eine erfolgreiche Penetration existieren, werden viele verschiedene Methoden und Techniken eingesetzt. Dies wird als *testing* bezeichnet.

Ist ein Pentest erfolgreich, so wird von einem *Exploit* gesprochen. Dabei wurde mindestens eine Sicherheitsbarriere penetriert und unwirksam gemacht. Ein Zugriff auf das System wurde erlangt und das Netzwerk oder Computersystem wurde erfolgreich infiltriert. Nun können Angreifer Schaden anrichten und Daten auf das eigene System exfiltrieren [Shimonski und Delbrueck 2023]. Durch ethisches Penetrationtesting können Unternehmen die Schwachstellen der IT-Systeme erkennen und beheben, bevor sie von Angreifern ausgenutzt werden können. Dadurch können Unternehmen ihre IT-Systeme besser schützen und die Sicherheit ihrer Daten gewährleisten.

2.2.1 Arten von Penetrationtestings

Innerhalb des Penetrationtestings gibt es verschiedene Arten von Tests, welche sich in dem Ausmaß der Kenntnisse über das Zielsystem unterscheiden. Durch den variablen Kenntnisstand des Angreifers können verschiedene Angriffsszenarien dargestellt werden.

Beim Black-Box-Testing bestehen vor dem Beginn des Penetrationtests keine Kenntnisse über das zu testende System. Im Gegensatz dazu bestehen beim White-Box-Testing vollständige und detaillierte Kenntnisse über das zu testende System. Das Grey-Box-Testing bildet ein Kompromiss, bei welchem teilweise Kenntnisse über das zu testende System bestehen.

Black-Box-Testing simuliert ein Angriffsszenario, welches dem eines externen Angreifers entspricht. Ein externer Angreifer hat keine Kenntnisse über das Zielsystem und muss diese erst erlangen. Diese Art des Penetrationtesting ist für die meisten KMU daher besonders realitätsnah. Dennoch ist es auch eine schon zu Beginn sehr zeitaufwändige Art des Penetrationtesting. Prinzipiell schon vorhandenes Wissen über das Zielsystem kann nicht genutzt, sondern muss erst erlangt werden.

Grey-Box-Testing simuliert ein Angriffsszenario, welches dem eines internen Angreifers entsprechen kann. Ein interner Angreifer hat teilweise Kenntnisse über das Zielsystem sowie bereits vereinzelte Rechte und Zugriffsmöglichkeiten, die direkt genutzt werden können. Aufgrund des Charakters kann diese Art des Penetrationtestings auch die Folgen eines gehackten Firmenaccounts simulieren.

White-Box-Testing bietet die Möglichkeit, das Penetrationtesting auf Basis von detaillierten Kenntnissen über das Zielsystem durchzuführen. Das kann mit Zugang zum Quellcode, zu Systemarchitekturen oder zu internen Daten realisiert werden. Der Fokus liegt darauf, gezielt tiefgehende Schwachstellen zu identifizieren, die nur schwer von außen zu entdecken wären. Diese Art des Penetrationtesting ist jedoch zeitintensiv und erfordert ein hohes Maß an Fachwissen. Besonders geeignet ist diese Art des Penetrationtestings für kleinteilige Bereiche von Produkten oder Systemen, die bereits in der Entwicklung sind bzw. am Ende der Entwicklung stehen.

2.2.2 Phasen des Penetrationtestings

Ein Penetrationtest besteht aus mehreren Phasen, die nach einer festen Reihenfolge zyklisch durchgeführt werden. Dieser strukturierte Ablauf hilft dabei, systematisch Schwachstellen zu identifizieren und zu beheben.

Planung und Reconnaissance

In der ersten Phase wird der Penetrationtest geplant. Dabei werden die Zielsysteme definiert sowie der Umfang des Tests als auch die Methoden, mit welchen aufgeklärt werden sollen, festgelegt. Des Weiteren werden in dieser Phase Informationen über das Zielsystem gesammelt. Das können IP-Adressen, Domains, Subdomains, Netzwerke, Betriebssysteme, Software sowie Mitarbeiter und Standorte sein.

Zur Informationssammlung gibt es passive und aktive Methoden. Passive Methoden umfasst die Analyse von öffentlich zugänglichen Informationen bzw. alle Informationen, die ohne Interaktion mit dem Zielsystem gesammelt werden können. Aktive Methoden hingegen sind Methoden, welche eine Interaktion mit dem Zielsystem erfordern. Das Umfasst beispielsweise das Durchführen einer DNS enumeration mit `$dig` oder `$whois` direkt beim Registrar. Das beinhaltet das Abfragen von Subdomains einer spezifischen Firmendomain über eine Datenbank mit historischen Daten.

Dafür gibt es Tools die diese Informationen sammeln und aufbereiten.

Für die passive Analyse von Subdomains gibt es beispielsweise crt.sh. Dadurch können Informationen über die Struktur des Zielsystems gesammelt werden um beispielsweise Schwachstellen in der Konfiguration zu identifizieren.

Wie bereits in Kapitel 1.1 angesprochen, kann auch Shodan, genutzt werden, um über CCTV Kameras Informationen über das Verhalten von Mitarbeitern zu sammeln. Zum einen können Informationen über die Anzahl der Mitarbeiter, die sich im Büro befinden, gesammelt werden als auch Informationen über die Arbeitszeiten. Dies setzt jedoch voraus, dass die Kameras als öffentlich zugänglich konfiguriert sind. Zur passiven Aufklärung ist auch das Erkennen des Designs von unternehmensspezifischen Werksausweisen über Social-Media-Plattformen denkbar.

Scanning & Schwachstellenbewertung

In der zweiten Phase werden Schwachstellen auf dem Zielsystem mithilfe automatisierter und manueller Test identifiziert. Diese Schwachstellen können offene Ports oder Dienste, veraltete Software, fehlerhafte Konfigurationen oder unsichere Passwörter sein. Zu den Werkzeugen, die in dieser Phase eingesetzt werden, gehören Port-Scanning, Schwachstellen-Scanning sowie Service-Versionserkennung und Analyse des Netzwerktraffics [Editor 2024].

Dabei soll herausgefunden werden, wie das Zielsystem auf Angriffe reagiert und ob es dabei Schwachstellen aufweist. Durch statische und dynamische Analyse kann das Verhalten des Systems beurteilt und Schwachstellen identifiziert werden. Statische Analyse umfasst die Beurteilung von Programmcode ohne dessen Ausführung. Dynamische Analyse im Gegenzug umfasst die Analyse von Programmcode im laufenden Betrieb für eine praxisnahe Bewertung der Sicherheitslage [Imperva 2023].

Gaining Access

In der dritten Phase werden die identifizierten Schwachstellen ausgenutzt, um Zugriff auf das Zielsystem zu erlangen. Diese Phase wird auch als *Exploitation* bezeichnet. Im günstigsten Fall können dafür bereits bekannte Exploits eingesetzt werden. Des Weiteren können in dieser Phase auch Angriffe wie Password attacks, SQL injection, Cross-Site Scripting und Social Engineering eingesetzt werden, welche in **Kapitel 2.1.3 genauer erläutert wurden**.

Maintaining Access

Die Phase *Maintaining Access* bezeichnet das Aufrechterhalten des Zugriffs auf das Zielsystem. Dazu wird geprüft, ob die initiale Schwachstelle für einen langfristigen Zugang zum Zielsystem genutzt werden kann. Dabei wird auch geprüft, ob der Zugriff auf das Zielsystem unbemerkt bleibt. Da diese Phase als Konsequenz auf die erfolgreiche Ausnutzung von Schwachstellen folgt, wird sie auch als *Post-Exploitation* bezeichnet.

Ist ein initialer Zugriff erfolgt, so folgt darauf meist die Erweiterung der Rechte, um Zugriff auf weitere Systeme zu erlangen. Dieser Prozess ist als *Escalation of Privileges* bekannt. Eine weitere Möglichkeit ist das Einrichten von Backdoors, um auch in Zukunft den Zugriff auf das Zielsystem zu behalten.

Analysis & Reporting

In der letzten Phase des Penetrationtesting werden die Ergebnisse des Tests umfassend analysiert. Dabei werden in die Schwachstellen, die während des Tests identifiziert wurden, in einem Bericht zusammenfassend aufgelistet und bewertet. Dieser enthält detaillierte Informationen über die Art der kompromittierten sensiblen Daten sowie die Dauer, in der die Tester unentdeckt im System bleiben konnten.

Die gewonnenen Erkenntnisse helfen Sicherheitsteams, effektive Gegenmaßnahmen zu ergreifen, indem sie ihre Sicherheitslösungen anpassen. Der Bericht enthält zudem eine Risikoanalyse sowie konkrete Handlungsempfehlungen zur Schließung der Sicherheitslücken und zur Stärkung der Abwehrmechanismen gegen zukünftige Angriffe.

2.2.3 Methoden des Penetrationtestings

[Imperva 2023]

2.2.4 Testtypen

[Mehta 2017]

2.3 Penetration Testing Suite Kali Linux

2.3.1 Distributionen

Mobile Kali Linux

Kali Linux NetHunter

VM

Kontainer

was ist Kali warum kali also statistik mit nutzern über die zeit, darstellen dass state of the art alternativen ParrotOS/CAINE

2.3.2 Integrierte Tools

kali linux struktur von tools mit kategorisierung der toools (Info, Network, web etc.)
zb. scanner:

Vulnerability testing/scanning

Greenbone: - keine schedule version in community edition + findet mehr schwachstellen - hat weniger false positives

Nessus: + einen schedule gleichzeitig (16 Hosts live?) + weniger überladenen output + weniger false positives (managable/machbar/nicht überfordernd) - wenige vulnerabilities werden nicht gefunden

-> erst nessus (weil abarbeitbar), dann greenbone für restliche probleme

BeyondTrust retinaCS comminity edition: - windows only

-> nur greenbone hat neuesen exploit gefunden
–> vgl. zu kali tools wie nmap, ausreichend? Grenze von Kali gefunden?

Kapitel 3

Konzeption des Leitfadens

3.1 Angriffsvektoren bei mittelständischen Unternehmen

Wo ist die Angriffsfläche am größten? Welche Angriffe sind in DE üblich auf mittelständische Unternehmen?
Kategorien der Angriffe [Bundesamt für Sicherheit in der Informationstechnik 2023]
Ausgewählte Kategorien [Bundesamt für Sicherheit in der Informationstechnik 2024b]

Durch welche Angriffsvektoren werden die meisten erfolge der Hacker erzielt? Social engineering Phishing Brute Force DDoS Ransomware etc.?

Antwort: [KPMG 2024]

3.2 Pentestingzyklus auf größte Angriffsfläche anwenden

z.b. falsche konfig von mailservern welche tools attakieren diese größte Angriffsfläche?

3.2.1 Tool für phase 1

tool aus jeweiliger Phase des Pentesting vorstellen sowie kurz wie man es bedient aka Toolname, Toolart, Toolbeschreibung, Features(Vorteile), Nachteile, Alternativen neben Kali integriert

wie gut führt dieses tool die jeweilige phase aus? alternative tools in der phase? kann dieses tool für weitere Phasen nützlich sein?

3.2.2 Tool für phase 2

gleich wie 1

3.2.3 Tool für phase 3

gleich wie 1

3.2.4 Tool für phase 4

gleich wie 1

3.2.5 Tool für phase 5

gleich wie 1

Kapitel 4

Fazit

4.1 Zusammenfassung

4.2 Bewertung der Ergebnisse

Ein Leitfaden dient als nützliche Orientierungshilfe, ist jedoch für sich genommen nicht ausreichend. Die Systemlandschaft der IT-Infrastruktur ist komplex und dynamisch. Eine Standardisierung eines einzelnen Testprozesses ist kontraproduktiv und kann aufgrund des dynamischen Charakters der IT-Systemen, sowie den daraus resultierenden Angriffsvektoren, nicht Schritt halten.

Die Bewertung von Kali-Linux hinsichtlich der Eignung zum aussagekräftigen Pentesten der eigenen IT-Systeme muss als Momentaufnahme betrachtet werden. Die Ergebnisse haben keinen Anspruch auf langfristige Gültigkeit.

4.3 Ausblick

Ein kontinuierlicher Anpassungs- und Verbesserungsprozess des Leitfadens ist notwendig, um die Aussagekraft, der Bewertung der Sicherheit der jeweilig analysierten IT-Systemen, in Zukunft beibehalten zu können.

Literaturverzeichnis

ACHILLEAN [März 2025]. *Honeyscore*. [Online; accessed 2025-03-31]. URL: https://honeyscore.shodan.io/ [siehe S. 7].

— [Sep. 2020]. *shodan - Filtering out honeypots from search results - Stack Overflow*. [Online; accessed 2025-03-31]. URL: https://stackoverflow.com/a/63943357 [siehe S. 7].

ATTACK DETECT DEFEND, (rot169) [Nov. 2020]. *Bypassing Firewalls with DNS Tunnelling (Defence Evasion, Exfiltration and Command & Control) - YouTube*. [Online; accessed 2025-04-05]. URL: https://www.youtube.com/watch?v=49F0co_VrTY [siehe S. 18].

BARTSCH, Michael und Stefanie FREY [2017]. *Cyberstrategien Für unternehmen und Behörden: Maßnahmen Zur erhöhung Der Cyberresilienz*. Springer Vieweg [siehe S. 20].

BITKOM [Aug. 2024a]. *Cyberattacken - Entwicklung 2024 | Statista*. [Online; accessed 2025-03-01]. URL: https://de.statista.com/statistik/daten/studie/1416472/umfrage/entwicklung-anzahl-cyberattacken-auf-unternehmen/ [siehe S. 10].

— [Aug. 2024b]. *Cyberattacken - Existenzbedrohung 2024 | Statista*. [Online; accessed 2025-03-01]. URL: https://de.statista.com/statistik/daten/studie/1416482/umfrage/geschaeftliche-existenzbedrohung-von-cyberattacken/ [siehe S. 10].

— [Aug. 2024c]. *Cyberattacken - Schäden 2024 | Statista*. [Online; accessed 2025-03-10]. URL: https://de.statista.com/statistik/daten/studie/1546525/umfrage/schaeden-durch-cyberattacken-nach-jahren/ [siehe S. 10].

BMJ - Pressemitteilungen - Rechtssicherheit für die Erforschung von IT-Sicherheitslücken: Bundesjustizministerium veröffentlicht Gesetzentwurf zum Computerstrafrecht [Nov. 2024]. https://www.bmj.de/SharedDocs/Pressemitteilungen/DE/2024/1104_ComputerStrafR.html. (Accessed on 24/11/2024) [siehe S. 16].

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK, (BSI) [März 2025a]. *BSI - Denial-of-Service (DoS) und Distributed Denial-of-Service (DDoS)*. [Online; accessed 2025-03-31]. URL: https://www.bsi.bund.de/dok/6599510 [siehe S. 8, 17].

— [Apr. 2024a]. *BSI - Kleine- und Mittlere Unternehmen*. [Online; accessed 2025-03-02]. URL: https://www.bsi.bund.de/dok/KMU [siehe S. 11].

— [März 2025b]. *BSI APT*. [Online; accessed 2025-03-31]. URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefaehrdungen/APT/apt_node.html [siehe S. 8].

— [Nov. 2023]. *Die Lage der IT-Sicherheit in Deutschland 2023*. [Online; accessed 2025-02-28]. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf?__blob=publicationFile&v=8 [siehe S. 9, 25].

Bundesamt für Sicherheit in der Informationstechnik, (BSI) [Nov. 2024b]. *Die Lage der IT-Sicherheit in Deutschland 2024*. [Online; accessed 2025-02-28]. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.pdf?__blob=publicationFile&v=5 [siehe S. 10, 11, 25].

— [März 2024c]. *Kritische Backdoor in XZ für Linux*. [Online; accessed 2025-03-31]. URL: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2024/2024-223608-1032.pdf?__blob=publicationFile [siehe S. 8].

Bundesgesetzblatt BGBl. Online-Archiv 1949 - 2022 | Bundesanzeiger Verlag [Mai 1986]. URL: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*%5B@attr_id=%27bgbl186s0721.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl186s0721.pdf%27%5D__1732641848164 [siehe S. 14].

Bundesgesetzblatt BGBl. Online-Archiv 1949 - 2022 | Bundesanzeiger Verlag [Aug. 2007]. URL: https://www.bgbl.de/xaver/bgbl/start.xav#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl107s1786.pdf%27%5D__1732641307137 [siehe S. 14].

Bundesverband mittelständische Wirtschaft, et. al. [Mai 2023]. *DIN SPEC 27076 - 2023-05 - DIN Media*. [Online; accessed 2025-03-02]. URL: https://www.dinmedia.de/de/technische-regel/din-spec-27076/365252629 [siehe S. 11].

Bundeszentrale für politische Bildung, bpb [Juni 2021]. *Mittelstand | bpb.de*. [Online; accessed 2025-02-27]. URL: https://www.bpb.de/kurz-knapp/lexika/lexikon-der-wirtschaft/20129/mittelstand/ [siehe S. 9].

Buschmann, Dr. Marco [Nov. 2024]. *BMJ - Pressemitteilungen - Rechtssicherheit für die Erforschung von IT-Sicherheitslücken: Bundesjustizministerium veröffentlicht Gesetzentwurf zum Computerstrafrecht*. https://www.bmj.de/SharedDocs/Pressemitteilungen/DE/2024/1104_ComputerStrafR.html. (Accessed on 24/11/2024) [siehe S. 7, 16].

Cloudflare [Apr. 2025a]. *Was ist Cross-Site Request Forgery? | Cloudflare*. [Online; accessed 2025-04-05]. URL: https://www.cloudflare.com/de-de/learning/security/threats/cross-site-request-forgery/ [siehe S. 19].

— [Jan. 2025b]. *Was ist ein Angriffsvektor? | Cloudflare*. [Online; accessed 2025-03-27]. URL: https://www.cloudflare.com/de-de/learning/security/glossary/attack-vector/ [siehe S. 12].

CyberDirekt [Apr. 2022]. *Cyberangriff - Auswirkungen für den Mittelstand | Statista*. [Online; accessed 2025-03-10]. URL: https://de.statista.com/statistik/daten/studie/1284933/umfrage/umfrage-zu-den-auswirkungen-von-cyberangriffen-im-deutschen-mittelstand/ [siehe S. 10].

Editor [Dez. 2024]. *Introduction to Penetration Testing Lifecycle - PenTesting.Org*. [Online; accessed 2025-03-20]. URL: https://www.pentesting.org/testing-process-overview/ [siehe S. 22].

Freund, Andres [März 2024]. *oss-security - backdoor in upstream xz/liblzma leading to ssh server compromise*. [Online; accessed 2025-04-03]. URL: https://www.openwall.com/lists/oss-security/2024/03/29/4 [siehe S. 8].

Group, Akamai Security Intelligence [Apr. 2024]. *Alles, was Sie über die XZ Utils Backdoor wissen müssen | Akamai*. [Online; accessed 2025-04-01]. URL: https://www.akamai.com/de/

blog/security-research/critical-linux-backdoor-xz-utils-discovered-what-to-know [siehe S. 8].

Hiscox [Okt. 2023]. *Cyberangriffe - Betroffene Unternehmen weltweit 2023 | Statista*. [Online; accessed 2025-02-28]. URL: https://de.statista.com/statistik/daten/studie/1230157/umfrage/unternehmen-die-in-den-letzten-12-monaten-eine-cyber-attacke-erlebt-haben/ [siehe S. 9].

Hurtz, Simon [Aug. 2021]. *CDU Connect: Erst die Anzeige, dann die Blamage - Politik - SZ.de*. URL: https://www.sueddeutsche.de/politik/cdu-connect-anzeige-wittmann-1.5373488 [siehe S. 16].

Ihlenfeld, Jens [Juli 2008]. *CCC: Hackerparagraph gefährdet den IT-Standort Deutschland - Golem.de*. URL: https://www.golem.de/0807/61198.html [siehe S. 15].

Imperva [Dez. 2023]. *What is Penetration Testing | Step-By-Step Process & Methods | Imperva*. [Online; accessed 2025-03-20]. URL: https://www.imperva.com/learn/application-security/penetration-testing/ [siehe S. 22, 23].

Infopapier_ComputerStrafR.pdf [Nov. 2024]. https://www.bmj.de/SharedDocs/Downloads/DE/Gesetzgebung/Dokumente/Infopapier_ComputerStrafR.pdf?__blob=publicationFile&v=4. (Accessed on 25/11/2024) [siehe S. 16].

KirstenS [Apr. 2025]. *Cross Site Scripting (XSS) | OWASP Foundation*. [Online; accessed 2025-04-05]. URL: https://owasp.org/www-community/attacks/xss/ [siehe S. 19].

KPMG [Mai 2024]. *Cyberkriminalität - Angriffsziele 2024 | Statista*. [Online; accessed 2025-04-02]. URL: https://de.statista.com/statistik/daten/studie/1482642/umfrage/angriffsziele-in-verbindung-mit-ecrime-in-deutschen-unternehmen/ [siehe S. 25].

Kriminalprävention der Länder und des Bundes, Polizeiliche [Apr. 2025]. *Bot-Netze | polizei-beratung.de*. [Online; accessed 2025-04-03]. URL: https://www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/bot-netze/ [siehe S. 18].

Kurz, Constanze, Felix Lindner, Frank Rieger und Thorsten Schröder [Juli 2008]. *Derzeitige und zukünftige Auswirkungen der Strafrechtsänderung auf die Computersicherheit*. URL: https://erdgeist.org/archive/46halbe/202output.pdf [siehe S. 15].

Lange, Hans-Jürgen, Thomas Model und Michaela Wendekamm [2019]. *Zukunft der Polizei Trends und Strategien*. Springer Fachmedien Wiesbaden [siehe S. 20].

Lee, Ivan [Jan. 2025]. *What is Cyber Attack Meaning? Types and Examples*. [Online; accessed 2025-04-02]. URL: https://www.wallarm.com/what/what-is-a-cyber-attack [siehe S. 17].

Mehta, Puneet [Juli 2017]. *Die unterschiedlichen Typen von Penetrationstests | Computer Weekly*. [Online; accessed 2025-03-21]. URL: https://www.computerweekly.com/de/ratgeber/Die-unterschiedlichen-Typen-von-Penetrationstests [siehe S. 20, 23].

Meister, Andre [Okt. 2024]. *Hacker-Paragrafen: Wir veröffentlichen den Gesetzentwurf zum Computerstrafrecht*. URL: https://netzpolitik.org/2024/hacker-paragrafen-wir-veroeffentlichen-den-gesetzentwurf-zum-computerstrafrecht/ [siehe S. 15–17].

NIST [März 2025]. *NVD - CVE-2024-3094*. [Online; accessed 2025-03-31]. URL: https://nvd.nist.gov/vuln/detail/CVE-2024-3094 [siehe S. 8].

PwC [Okt. 2024]. *Änderung des Cyber-Budgets von Unternehmen 2025 | Statista*. [Online; accessed 2025-03-02]. URL: https://de.statista.com/statistik/daten/studie/1383316/umfrage/aenderung-des-cyber-budgets-von-unternehmen-in-deutschland-und-global/ [siehe S. 10].

Shimonski, Robert und Matthias Delbrueck [2023]. *Penetration tester Werden Für dummies Robert Shimonski; übersetzung aus dem Amerikanischen von Matthias Delbrück; Fachkorrektur von Rafael Gomes Dinis und Michael Schlede*. Wiley, Wiley-VCH. ISBN: 978-3-527-71794-1 [siehe S. 20].

Simplicissimus [Feb. 2024a]. *Putins Bären – Die gefährlichsten Hacker der Welt*. [Online; accessed 2025-04-03]. URL: https://www.ardmediathek.de/film/Y3JpZDovL3N3ci5kZS9zZGIvc3RJZC8xNTg4 [siehe S. 8].

— [Sep. 2024b]. *Wie dieser Deutsche das Internet gerettet hat*. [Online; accessed 2025-03-31]. URL: https://www.youtube.com/watch?v=8p8PHeGg--U [siehe S. 8].

Synopse_ComputerStrafR_RefE.pdf [Nov. 2024]. https://www.bmj.de/SharedDocs/Downloads/DE/Gesetzgebung/Synopse/Synopse_ComputerStrafR_RefE.pdf?__blob=publicationFile&v=2. (Accessed on 25/11/2024) [siehe S. 14, 15].

Viola Kiel, DER SPIEGEL [März 2022]. *Was der Ausfall eines Satellitennetzwerks mit deutschen Windkraftanlagen zu tun hat - DER SPIEGEL*. [Online; accessed 2025-03-31]. URL: https://www.spiegel.de/wissenschaft/technik/russland-ukraine-was-der-ausfall-eines-satellitennetzwerks-mit-deutschen-windkraftanlagen-zu-tun-hat-a-22850ad5-dee2-42c4-8c5a-c2b39ac42da4 [siehe S. 7].

Wilkens, Andreas [Juli 2008]. *CCC fordert Abschaffung des "Hackerparagraphen" - heise online*. URL: https://www.heise.de/news/CCC-fordert-Abschaffung-des-Hackerparagraphen-188546.html [siehe S. 15].

Zschunke, Peter [Sep. 2007]. *Hackerparagraph: Datensicherung verboten? - DER SPIEGEL*. URL: https://www.spiegel.de/netzwelt/tech/hackerparagraph-datensicherung-verboten-a-505130.html [siehe S. 15].