Carl-Severing-Berufskolleg für Wirtschaft und Verwaltung der Stadt Bielefeld

---

FACHARBEIT

im Grundkurs Deutsch

Cybercrime

Kryptologische Abwehrmöglichkeiten zum Schutze vor Missbrauch

Vorgelegt von:	Bäumer, Marvin
	Pastor-Bangen-Weg, 40
	33758, Schloß Holte-Stukenbrock
	Jahrgangsstufe 13
	Schuljahr 2023/2024
Kurslehrerin:	Michalke, Antje
Abgabedatum:	26.02.2024

Inhaltsverzeichnis

1. Einleitung 3

2. Grundlagen der Kryptologie 3

3. Arten und Verteidigung von Cyberangriffen 4

4. Warum ist der Schutz vor Cyberangriffen von großer Bedeutung? 5

5. Fazit 7

Literaturverzeichnis 8

1. Einleitung

Die Bedeutung von Kryptologischen Abwehrmöglichkeiten zum Schutz vor Missbrauch kann kaum überschätzt werden. In einer zunehmend digitalisierten Welt, in der die Kommunikation größtenteils digital stattfindet, gewinnt das Thema Cybersecurity, dass eng mit dem Thema Kryptologie verbunden ist, immer mehr an Bedeutung. Kryptologie dient dazu, unsere Informationen sicher zu ver- und entschlüsseln, um private, wichtige und geheime Daten vor potenziellen Angreifern zu schützen. Die zunehmende Vernetzung von Geräten und die exponentiell wachsende Menge an über das Internet übertragenen Daten haben die Angriffsfläche für Cyberkriminelle erheblich vergrößert. In diesem Kontext ist es unerlässlich, effektive Schutzmechanismen zu entwickeln, um sensible Informationen zu sichern und die Integrität von Kommunikationssystemen zu gewährleisten. Hierbei spielt Kryptologie eine große Rolle da diese sich mit dem Grundsatz der Verschlüsslung beschäftigt.

Die Facharbeit behandelt zunächst die Grundlagen der Kryptologie, wie asymmetrische und symmetrische Verschlüsselung sowie Hashfunktionen. Diese dienen als Basiswissen für das Verständnis weiterer Konzepte. Im nächsten Schritt werden verschiedene Verteidigungsstrategien gegen Cyberangriffe erläutert, wobei ein besonderer Fokus auf der Rolle von Hashfunktionen, Abwehr von Man-in-the-Middle-Angriffen und Brute Force liegt. Die Facharbeit zielt darauf ab, die Bedeutung des Schutzes vor Cyberkriminalität zu erläutern und die Gründe für den erforderlichen Aufwand zu verdeutlichen. Dabei wird die zentrale Fragestellung behandelt: „Warum ist der Schutz vor Cyberkriminalität von großer Bedeutung?“.

2. Grundlagen der Kryptologie

Kryptologie ist das Feld der Wissenschaft und Technik, das sich mit der Sicherheit von Informationen befasst, insbesondere bei der Übertragung und Speicherung über unsichere Kanäle und Umgebungen. Grundlegend umfasst die Kryptologie drei Hauptprozesse: Verschlüsselung, Entschlüsselung und Schlüsselverwaltung (Informationstechnik, 2021, S. 1).

Verschlüsselung ist der Prozess, bei dem Klartext, also lesbare Daten, in Geheimtext, also unlesbare Daten, umgewandelt werden. Dies geschieht durch die Anwendung eines Verschlüsselungsalgorithmus, der auf einem Schlüssel basiert. Es gibt zwei Hauptarten von Verschlüsselungsverfahren, symmetrische und asymmetrische Verschlüsselung. Bei der symmetrischen Verschlüsselung wird derselbe Schlüssel sowohl zum Verschlüsseln als auch zum Entschlüsseln verwendet, während bei der

asymmetrischen Verschlüsselung zwei unterschiedliche Schlüssel verwendet werden, ein öffentlicher Schlüssel zum Verschlüsseln und ein privater Schlüssel zum Entschlüsseln (Informationstechnik, 2021, S. 1). „Schlüsselverwaltung“ bezieht sich auf alle Aspekte der Erzeugung, Speicherung, Verteilung und Verwaltung von Verschlüsselungsschlüsseln. Ein effektives Schlüsselverwaltungssystem ist entscheidend für die Sicherheit kryptografischer Systeme, da die Kompromittierung von Schlüsseln die Sicherheit des gesamten Systems gefährden kann. Ein Verfahren, um den sicheren Schlüsselaustausch zu gewährleisten ist das Diffie-Hellman Verfahren *„Es handelt sich um ein Verfahren, mit dem sich zwischen zwei Kommunikationspartnern über ein potenziell unsicheres Medium wie das Internet ein gemeinsamer Schlüssel sicher vereinbaren lässt.“* (Luber & Schmitz, 2019).

Zusätzlich zu Verschlüsselung und Entschlüsselung spielen Hash-Funktionen eine wichtige Rolle in der Kryptologie. Eine Hash-Funktion nimmt eine Eingabe beliebiger Länge und gibt eine feste Länge von Daten zurück, die als Hash-Wert bezeichnet wird. Hash-Funktionen sind unidirektional, was bedeutet, dass sie nicht rückgängig gemacht werden können, und werden häufig zur Integritätsprüfung von Daten verwendet (Informationstechnik, 2021)

3. Arten und Verteidigung von Cyberangriffen

Cyberangriffe stellen eine ständig wachsende Bedrohung für Unternehmen, Regierungen und Einzelpersonen dar. Sie können verschiedene Formen annehmen, von der Übernahme sensibler Daten bis hin zur Manipulation von Systemen und der Unterbrechung von Diensten. Kryptographische Techniken erweisen sich jedoch als entscheidende Verteidigungslinie gegen diese Gefahren. Der Folgende Abschnitt behandelt den Man-in-the-Middle-Angriff und die Verwendung von Hashfunktionen.

Der Man-in-the-Middle-Angriff (MITM) ist ein besonders tückischer Angriffstyp, bei dem ein Angreifer die Kommunikation zwischen zwei Parteien abfängt und möglicherweise manipuliert (Pohlmann, n.a.). Durch den Einsatz von Verschlüsselungstechnologien wie SSL/TLS kann die Vertraulichkeit und Integrität der Daten während der Übertragung gewährleistet werden. Selbst wenn ein Angreifer Zugriff auf den Kommunikationskanal hat, wird ihm der Zugriff auf die verschlüsselten Daten erschwert. „SSL“ (Secure Sockets Layer) und sein Nachfolger „TLS“ (Transport Layer Security) sind Verschlüsselungsprotokolle, die verwendet werden, um die Sicherheit von Datenübertragungen im Internet zu gewährleisten (Mierke, 2020). SSL und TLS spielen eine wichtige Rolle beim Schutz der Privatsphäre und Sicherheit im Internet,

insbesondere bei sensiblen Aktivitäten wie Online-Banking oder dem Austausch vertraulicher Informationen. Sie sind zu einem unverzichtbaren Bestandteil der modernen Internetkommunikation geworden, indem sie eine sichere Umgebung für den Austausch von Daten zwischen Benutzern und Websites bereitstellen. Sie ermöglichen eine verschlüsselte Kommunikation zwischen einem Client (z. B. ihrem Webbrowser) und einem Server (z. B. einer Website), um die Vertraulichkeit und Integrität der übertragenen Daten zu schützen. Wenn Sie eine sichere Verbindung zu einer Website herstellen, verwendet Ihr Webbrowser SSL/TLS, um die zwischen ihrem Computer und dem Server der Website übertragenen Daten zu verschlüsseln (Mierke, 2020). Dadurch können selbst abgefangene Daten nicht gelesen werden, da sie nur vom Server und ihrem Browser entschlüsselt werden können.

Ein weiteres häufiges Szenario ist der Brute-Force-Angriff. Dabei versucht ein Angreifer Zugang zu einem System zu erlangen, indem er systematisch alle möglichen Passwortkombinationen ausprobiert. Um Angriffe zu erschweren, werden kryptographische Hash-Funktionen und robuste Passwortrichtlinien eingesetzt. Durch die Verwendung von starken Hash-Algorithmen und die Implementierung von Passwortrichtlinien, die komplexe Passwörter erfordern, können Brute-Force-Angriffe erheblich erschwert werden (Luber & Schmitz, 2018).

Eine weitere Form von Cyberangriffen stellen Datenmanipulationsangriffe dar, da Angreifer versuchen können, die Integrität von Daten zu verletzen, indem sie sie während der Übertragung oder Speicherung verändern. Digitale Signaturen und kryptographische Prüfsummen bieten eine Lösung, da sie sicherstellen, dass die Daten authentisch und unverändert bleiben. Potenzielle Manipulationen können durch das Signieren von Daten mit einem privaten Schlüssel und deren Überprüfung mit einem öffentlichen Schlüssel erkannt werden (Informationstechnik, 2021).

4. Warum ist der Schutz vor Cyberangriffen von großer Bedeutung?

Der Schutz vor Cyberangriffen ist von entscheidender Relevanz, da die heutige Gesellschaft zunehmend von digitalen Technologien abhängig ist. Diese Technologien ermöglichen es uns, Informationen zu kommunizieren, zu speichern und zu verarbeiten. Allerdings bringen sie auch neue Risiken mit sich. Cyberangriffe können verheerende Auswirkungen haben, nicht nur auf Unternehmen und Organisationen, sondern auch auf Einzelpersonen. Daher stellt sich die Frage: Warum betreiben wir einen so erheblichen Aufwand, um Cyberangriffe wie Man-in-the-Middle, Brute-Force und andere abzuwehren? Dabei spielen moralische Aspekte eine zentrale Rolle.

Gemäß dem Bundesdatenschutzgesetz müssen personenbezogene Daten geschützt werden (Justiz, 2018). Dies legt nahe, dass jeder Mensch ein Recht auf Privatsphäre hat und darüber bestimmen sollte, wer Zugang zu seinen persönlichen Daten hat und wie sie verwendet werden. Cyberangriffe können die Privatsphäre verletzen, indem sie persönliche Informationen wie Identitätsdaten, Finanzinformationen und persönliche Kommunikationen offenlegen. Die Implementierung von Kryptologie ermöglicht die Verschlüsselung persönlicher Informationen, wodurch sie für Cyberangreifer nahezu unzugänglich werden. Ein anschauliches Beispiel hierfür ist die End-to-End-Verschlüsselung, die in Messaging-Anwendungen wie WhatsApp angewendet wird. Diese Verschlüsselungstechnik gewährleistet, dass die Kommunikation zwischen den Benutzern so geschützt ist, dass nur die beteiligten Parteien darauf zugreifen können. Somit bleiben private Informationen vertraulich und sind vor unbefugtem Zugriff geschützt. Des Weiteren können Unternehmen und Organisationen durch den Verlust vertraulicher Informationen, Betriebsunterbrechungen oder Erpressung finanziell geschädigt werden. Dies kann sich negativ auf die Wirtschaft und auf Arbeitsplätze auswirken und letztendlich die Lebensgrundlage vieler Menschen bedrohen. Die Nutzung verschlüsselter Daten auf einem Server sowie die Anwendung von Hashfunktionen können dazu beitragen, Sicherheitsvorfälle präventiv abzuwehren und einen finanziellen Schaden des Unternehmens vermeiden. Durch die Verschlüsselung von Daten auf einem Server werden sensible Informationen in verschlüsselter Form gespeichert, wodurch sie selbst im Falle eines Datenlecks oder unbefugten Zugriffs für Angreifer unlesbar bleiben. Dies reduziert das Risiko von Datenverlust oder -diebstahl erheblich.

Laut einer Studie von Bündnis gegen Cybermobbing e.V. vom Oktober 2022 können Cyberangriffe in Form von Cybermobbing schwerwiegende psychologische Auswirkungen haben, insbesondere bei Jugendlichen (Beitzinger, Leest, & Süss, 2022). Cybermobbing und Erpressung im Internet sind zwei Formen von Cyberangriffen, die häufig zu Depressionen, Angstzuständen und anderen psychischen Gesundheitsproblemen führen können (Beitzinger, Leest, & Süss, 2022). Daher ist es entscheidend, nicht nur die physische Sicherheit, sondern auch die psychische Gesundheit der Menschen zu schützen, indem wir gegen Cyberangriffe vorgehen, und eine sichere und unterstützende Online-Umgebung fördern unter Verwendung von Kryptologie. Jugendliche und andere Nutzer können sich sicherer fühlen, ihre Gedanken und Gefühle online auszudrücken, wenn sie wissen, dass ihre Daten verschlüsselt und vor Cyberangriffen geschützt sind. Die Verwendung von Kryptologie kann dazu

beitragen, psychische Gesundheitsprobleme zu reduzieren, indem sie eine positive und sichere Online-Erfahrung fördert.

Die Antwort auf die Frage des notwendig hohen Aufwandes für Abwehr von Cyberangriffen liegt nicht nur in der reinen technischen Sicherheit, sondern auch in moralischen und gesellschaftlichen Aspekten. Cyberangriffe, die die Privatsphäre verletzen könnten, machen den Einsatz von Kryptologie und Verschlüsselungstechniken unerlässlich. Die Implementierung von Verschlüsselungstechniken schützt persönliche Informationen vor unbefugtem Zugriff und trägt dazu bei, die Privatsphäre der Menschen zu wahren.

5. Fazit

Durch die gewonnenen Erkenntnisse über die Kryptologischen Abwehrmöglichkeiten zum Schutze vor Missbrauch stellt sich heraus, dass Verschlüsselungstechniken wie asymmetrische und symmetrische Verschlüsselung sowie Hashfunktionen entscheidende Instrumente sind, um sensible Informationen zu sichern und die Integrität von Kommunikationssystemen zu gewährleisten. Die Wahrung der Privatsphäre, die Vermeidung finanzieller Schäden und die Förderung einer sicheren Online-Umgebung tragen dazu bei, psychische Gesundheitsprobleme, die durch Cyberangriffe entstehen können, zu reduzieren. Letztendlich tragen die beschriebenen Tatsachen nicht nur zum Schutz einzelner Individuen und Organisationen bei, sondern fördern auch das Vertrauen und die Integrität unserer digitalen Gesellschaft insgesamt.

Literaturverzeichnis

Beitzinger, F., Leest, U., & Süss, D. (Oktober 2022). *buendnis-gegen-cybermobbing.de*. Abgerufen am 18. Februar 2024 von buendnis-gegen-cybermobbing.de: https://www.buendnis-gegen-cybermobbing.de/wp-content/uploads/2022/10/Cyberlife_Studie_2022_endfassung.pdf

Informationstechnik, B. f. (Hrsg.). (1. Februar 2021). *bsi.bund.de*. Abgerufen am 16. Februar 2024 von bsi.bund.de: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/03_CON_Konzepte_und_Vorgehensweisen/CON_1_Kryptokonzept_Edition_2021.pdf?__blob=publicationFile&v=2

Justiz, B. d. (Hrsg.). (2018). *gesetze-im-internet.de*. Abgerufen am 18. Februar 2024 von gesetze-im-internet.de: https://www.gesetze-im-internet.de/bdsg_2018/

Luber, S., & Schmitz, P. (17. Januar 2018). *security-insider.de*. Abgerufen am 17. Februar 2024 von security-insider.de: https://www.security-insider.de/was-ist-ein-brute-force-angriff-a-677192/

Luber, S., & Schmitz, P. (18. Februar 2019). *security-insider.de*. Abgerufen am 18. Februar 2024 von security-insider.de: https://www.security-insider.de/was-ist-der-diffie-hellman-schluesselaustausch-a-799443/

Mierke, M. (3. September 2020). *heise.de*. Abgerufen am 17. Februar 2024 von heise.de: https://www.heise.de/tipps-tricks/SSL-und-TLS-was-ist-der-Unterschied-4884686.html

Pohlmann, N. (kein Datum). *norbert-pohlmann.com*. Abgerufen am 17. Februar 2024 von norbert-pohlmann.com: https://norbert-pohlmann.com/glossar-cyber-sicherheit/man-in-the-middle-angriff-mitm/