BLOCKCHAIN® IN HEALTHCARE TODAY

NARRATIVER/SYSTEMATISCHER ÜBERBLICK/META-ANALYSE

Aufkommende Trends in der Cybersicherheit: Ein ganzheitlicher Blick auf aktuelle Bedrohungen, die Bewertung von Lösungen und die Entwicklung neuer Grenzen

Taskeen Zaid, PhD[1] und Suman Garai, MBA[(2*)]

[1]Associate Professor IT, Jain (Deemed to be University), Bengaluru, Karnataka, Indien; [2]Kalinga Institute of Industrial Technology, Bhubaneshwar, Odisha, Indien

*Korrespondierender Autor: Suman Garai, E-Mail: mr.sumangarai.3122@gmail.com DOI:

https://doi.org/10.30953/bhty.v7.302

Schlüsselwörter: vergleichende Analyse, Cyberverteidigung, Cybersicherheit, digitale Bedrohungslandschaft, innovativer Rahmen, Informationsschutz

Zusammenfassung

Im Zeitalter des digitalen Fortschritts spielt die Cybersicherheit eine zentrale Rolle beim Schutz von Informationen und Systemen vor sich entwickelnden Bedrohungen. Die zunehmende Raffinesse von Cyber-Bedrohungen macht eine kritische Prüfung der Wirksamkeit heutiger Schutzmaßnahmen erforderlich. In Anbetracht der Grenzen und Lücken aktueller Lösungen wird in dieser Forschungsarbeit ein bahnbrechender Rahmen zur Stärkung der Cyberabwehr vorgestellt. Auf der Grundlage einer umfassenden Untersuchung von Forschungsartikeln, Umfragen, Online-Medien und praktischen Studien werden in dieser Studie die Feinheiten von Cyber-Bedrohungen untersucht und die Stärken und Schwächen der bestehenden Lösungen bewertet. Die vorgeschlagenen Rahmenbedingungen sind das Ergebnis einer sorgfältigen Machbarkeits- und Praktikabilitätsstudie, in die Erkenntnisse aus verschiedenen Online-Quellen eingeflossen sind. Das "Wie" umfasst eine vergleichende Analyse, bei der das neuartige Rahmenwerk mit etablierten Lösungen verglichen wird, um deren jeweilige Vorzüge und Schwächen herauszuarbeiten. Der Anstoß für diese Forschung liegt darin, Forschern, Praktikern und politischen Entscheidungsträgern, die sich mit den vielfältigen Herausforderungen der Cybersicherheit auseinandersetzen, wertvolle Einblicke zu bieten. Durch die Navigation durch die Komplexität bestehender Lösungen und die Einführung innovativer Rahmenwerke soll dieses Papier als Leitfaden für die Stärkung der Cyberabwehr dienen. Letztendlich sieht diese Studie einen kontinuierlichen Zyklus der Verbesserung und Weiterentwicklung im Bereich der Cybersicherheit vor, da alle Beteiligten gemeinsam versuchen, sich an die sich ständig verändernde digitale Bedrohungslandschaft anzupassen.

Eingereicht: Februar 24, 2024; Angenommen: April 19, 2024; Veröffentlicht: April 30, 2024

In diesem Artikel versuchen die Autoren, die aktuelle Cyber-Bedrohungslandschaft umfassend zu untersuchen, bestehende Sicherheitslösungen zu hinterfragen und neue Rahmenbedingungen für Verbesserungen vorzuschlagen. Die primären Ziele umfassen eine gründliche Untersuchung der vorherrschenden Bedrohungslandschaft, die Analyse aktueller Sicherheitsbedrohungen, die Bewertung bestehender Lösungen und das Aufzeigen ihrer inhärenten Grenzen. Die Studie stellt zwei innovative Lösungen vor, die auf bestimmte Bereiche der Cybersicherheit abzielen, und führt detaillierte vergleichende Analysen mit etablierten Sicherheitsmaßnahmen durch, um deren jeweilige Stärken und Schwächen zu ermitteln. Zu den angewandten Methoden gehören eine umfassende Literaturrecherche, Machbarkeits- und Praktikabilitätsstudien sowie eine vergleichende Analyse, die eine solide Grundlage für die Gewinnung von Erkenntnissen, für praktische Verbesserungen und für die Festlegung künftiger Forschungsrichtungen.

Historische Perspektive

Im hektischen digitalen Zeitalter ist unser Leben nahtlos mit den unsichtbaren Fäden des Internets verwoben. Wir erledigen unsere Bankgeschäfte online, tauschen unsere Gedanken in den sozialen Medien aus und vertrauen unsere Geheimnisse einem Cloud-Speicher an. Doch hinter diesem Komfort verbirgt sich eine Schattenwelt digitaler Bedrohungen, in der böswillige Akteure versuchen, Schwachstellen auszunutzen und unsere wertvollen Daten zu gefährden. Dieser Bereich, der als Cybersicherheit bekannt ist, hat sich von der Welt der Spione und Codebrecher zu einem kritischen Schlachtfeld für Einzelpersonen, Unternehmen und Nationen gleichermaßen entwickelt. Ein Verständnis der Entwicklung - von den frühen

Verschlüsselungsbemühungen an die ausgefeilten Angriffslandschaften von heute anzupassen - ist entscheidend, um sich in diesem sich ständig verändernden Terrain zurechtzufinden.

Die Saat der Cybersicherheit wurde mitten im Chaos des Zweiten Weltkriegs gesät. In einem verzweifelten Versuch, die militärische Kommunikation zu sichern, setzten Nationen wie Deutschland fortschrittliche Verschlüsselungsmaschinen wie die Enigma ein und schufen komplexe Chiffren, die den alliierten Geheimdienst jahrelang vor ein Rätsel stellten. Die Geschichte des Knackens der Enigma, die von einem brillanten Team in Bletchley Park vorangetrieben wurde, ist ein Zeugnis für den Einfallsreichtum und die Entschlossenheit, die diesem Bereich zugrunde liegen. Noch bevor sich die Welt mit Computern beschäftigte, diente die Kryptografie als erste Verteidigungslinie gegen Gegner, die Geheimnisse stehlen und Operationen stören wollten.[1]

Nach der digitalen Revolution verlagerte sich der Schwerpunkt von physischen Codes auf den Schutz von Computersystemen und Netzwerken. In den Anfängen gab es nur vereinzelte Vorfälle wie den Morris-Wurm-Angriff von 1988, aber mit der zunehmenden Verbreitung des Internets wurden auch die Cyber-Bedrohungen immer ausgefeilter und häufiger. Hacker, motiviert durch Unfug, Spionage oder finanziellen Gewinn, nutzten Schwachstellen in Betriebssystemen, Websites und im Benutzerverhalten aus. Viren, Würmer und Malware verbreiteten sich und griffen kritische Infrastrukturen, Unternehmen und sogar Einzelpersonen an. Das Aufkommen von Cybercrime-Syndikaten fügte eine weitere Ebene organisierter Bosheit hinzu, die Angriffe wie Datenschutzverletzungen und Identitätsdiebstahl begünstigte.[2]

In dem Maße, wie sich diese digitalen Angreifer weiterentwickelt haben, hat sich auch das Arsenal der Cybersecurity-Verteidiger vergrößert. Antivirensoftware, Firewalls und Systeme zur Erkennung von Eindringlingen wurden zu unverzichtbaren Werkzeugen für den Netzwerkschutz. Die Regierungen beeilten sich, Cybersicherheitsbehörden einzurichten und Richtlinien zu formulieren. Die internationale Zusammenarbeit wurde unabdingbar und führte zu Verträgen und Vereinbarungen zur Bekämpfung der Internetkriminalität und zur Förderung eines verantwortungsvollen Online-Verhaltens. Heute ist die Cybersicherheit ein milliardenschwerer Wirtschaftszweig, der ein Heer von Fachleuten mit unterschiedlichem Hintergrund beschäftigt: ethische Hacker, Netzwerksicherheitsingenieure, Malware-Analysten und Spezialisten für die Reaktion auf Zwischenfälle.[3]

Doch das Wettrüsten geht weiter. Hacker entwickeln ständig neue Methoden und nutzen neue Technologien wie künstliche Intelligenz (KI) und Blockchain, um neue Angriffe zu starten. Ransomware, Phishing-Betrug und Angriffe auf die Lieferkette sind nur einige Beispiele für die sich entwickelnde Bedrohungslandschaft. Es steht mehr denn je auf dem Spiel: Kritische Infrastrukturen, Gesundheitssysteme und sogar demokratische Prozesse sind potenzielle Ziele. Auf dem Weg in eine zunehmend vernetzte Zukunft war der Bedarf an robusten Cybersicherheitsmaßnahmen noch nie so groß wie heute.[4]

Die Entwicklung der Cybersicherheit ist ein Zeugnis für den menschlichen Einfallsreichtum und den ständigen Kampf zwischen Angriff und Verteidigung. Von der geheimen Welt des Codeknackens zu Kriegszeiten bis zu den komplexen digitalen Schlachtfeldern von heute zeigt die Geschichte, wie wichtig Bewusstsein, Wachsamkeit und Zusammenarbeit für den Schutz unseres digitalen Lebens sind. Wenn wir uns in der sich ständig weiterentwickelnden Cyberlandschaft zurechtfinden, hilft uns das Wissen um die Geschichte und die Herausforderungen der Gegenwart, eine sicherere und widerstandsfähigere Zukunft für alle zu schaffen.

Digitale Sicherheitsrisiken in jüngster Zeit

In den letzten Jahren haben die Bedrohungen für die Cybersicherheit erheblich zugenommen, was zu erheblichen finanziellen Verlusten und zur Schädigung des Rufs vieler Unternehmen geführt hat. Bedauerlicherweise zeigen mehrere Beispiele aus der Praxis (Abbildung 1), wie ernst diese Bedrohungen sind.

Bei Angriffen auf die Lieferkette, einer ausgeklügelten Form der Cyber-Kriegsführung, werden Drittanbieter kompromittiert, um unbefugten Zugang zu den Systemen des Zielunternehmens zu erhalten. Mit dieser Methode können die Angreifer das Vertrauen ausnutzen, das zwischen

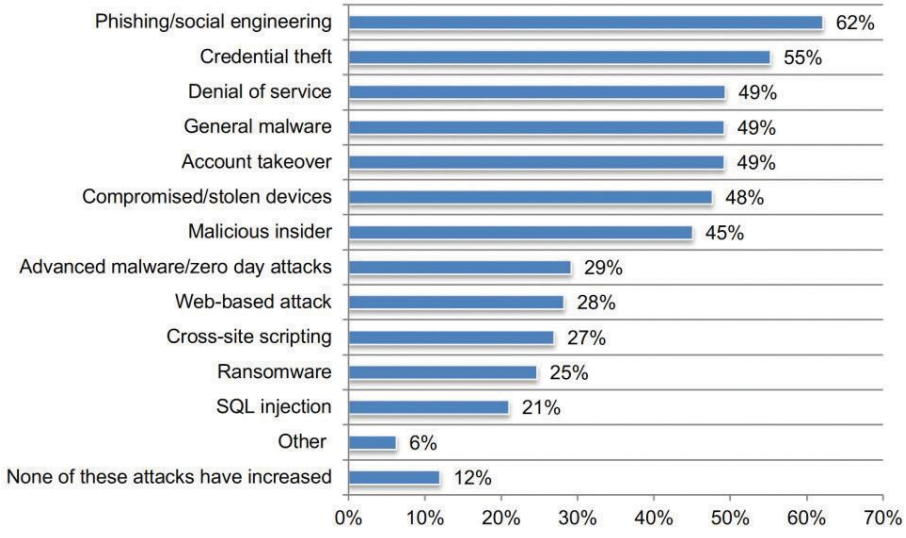

Abb. 1. Ein Umfragebericht, der die Zunahme verschiedener Arten von Cyber-Bedrohungen seit COVID-19 zeigt. SQL: strukturierte Abfragesprache

Citation: Blockchain im Gesundheitswesen heute 2024, **7**: 302 - https://doi.org/10.30953/bhty.v7.302

Organisationen und ihre Zulieferer. Der Angriff auf SolarWinds im Jahr 2020 ist ein deutliches Beispiel für diese Strategie, bei dem russische Hacker Schwachstellen im Aktualisierungsverfahren von SolarWinds ausnutzten, um in Tausende von Unternehmensnetzwerken einzudringen.[5]

Die Ausnutzung von Schwachstellen in Geräten des Internets der Dinge (IoT) ist eine weitere Facette der Cyberbedrohungen. Der Mirai-Botnet-Angriff auf Dyn im Jahr 2016 ist ein bemerkenswertes Beispiel, bei dem kompromittierte IoT-Geräte verwendet wurden, um einen massiven DDoS-Angriff (Distributed Denial of Service) zu starten, der jeden Server oder jedes Netzwerk mit einer Flut von Datenverkehr überschwemmte, was zu erheblichen Website-Ausfällen im Osten der USA führte und einen geschätzten Schaden von 110 Millionen US-Dollar verursachte.[6]

Bei fortgeschrittenen anhaltenden Bedrohungen (Advanced Persistent Threats, APTs) verschaffen sich unautorisierte Nutzer über einen längeren Zeitraum unbemerkt Zugang zu Systemen. Im Jahr 2015 führten chinesische Hacker einen groß angelegten APT gegen das U.S. Office of Personnel Management (OPM) durch und kompromittierten die persönlichen Daten von mehr als 21 Millionen Personen.[7]APTs zeichnen sich durch ihren heimlichen Charakter aus und werden oft von nationalstaatlichen Akteuren mit der Absicht betrieben, sensible Daten zu stehlen oder andere Angriffe zu verüben. Der OPM-Angriff hat deutlich gemacht, vor welch großen Herausforderungen Unternehmen bei der Erkennung und Eindämmung von APTs stehen.

Ransomware-Angriffe verschlüsseln die Daten eines Opfers und verlangen eine Zahlung für den Entschlüsselungsschlüssel. Der WannaCry-Angriff von 2017 betraf mehr als 300.000 Computer weltweit, wobei eine Schwachstelle in Microsoft Windows ausgenutzt wurde.[8]Ein weiterer bemerkenswerter Vorfall war der Angriff auf die Colonial Pipeline im Jahr 2021, bei dem ein Ransomware-Angriff die Treibstofflieferungen i m Osten der Vereinigten Staaten unterbrach, was die entscheidende Rolle der Cybersicherheit beim Schutz wichtiger Infrastrukturen unterstreicht.[9]Social Engineering ist eine Taktik, die von Cyberkriminellen angewandt wird, um Personen dazu zu bringen, sensible Informationen preiszugeben oder Handlungen vorzunehmen, die die Sicherheit gefährden. Im Jahr 2023 wurde MGM Resorts Opfer eines ausgeklügelten Social-Engineering-Angriffs, bei dem sich Hacker als legitimer Anbieter ausgaben, um sich Zugang zu verschaffen und unveröffentlichte Drehbücher, vertrauliche Finanzdokumente und Mitarbeiterdaten zu stehlen. Informationen.[10]

Deepfakes, hyperrealistische manipulierte Video- oder Audioaufnahmen, stellen eine weitere technologische Raffinesse des Social Engineering dar. Diese "synthetischen Medien" stellen eine wachsende Bedrohung dar und ermöglichen es Angreifern, sich als Führungskräfte auszugeben, Fehlinformationen zu verbreiten oder raffinierte Erpressungsversuche durchzuführen. Eine Studie der RAND Corporation aus dem Jahr 2020 warnte vor dem potenziellen Einsatz von Deepfakes bei der Störung von Wahlen, der Manipulation von Finanzmärkten und der Untergrabung des öffentlichen Vertrauens.[11]Der Deepfake-Fall von 2023, in den die Schauspielerin Rashmika Mandanna verwickelt war, zeigt die wachsende Bedrohung, die von dieser Technologie ausgeht, und verursacht Leid und Rufschädigung.[12]

Kontoübernahmen sind auf dem Vormarsch und betreffen sowohl Einzelpersonen als auch große Unternehmen. Im Jahr 2019 erlebte Capital One einen großen Kontoübernahmeangriff, bei dem sich ein Hacker Zugang zu den persönlichen Daten von Millionen von Nutzern verschaffte. Die Folgen waren schwerwiegend: Der Hacker konnte auf Sozialversicherungsnummern, Kreditwürdigkeitswerte und Bankkontonummern zugreifen, was zu einer Geldstrafe von 80 Millionen Dollar für Capital One führte.[13]

Der Diebstahl von Zugangsdaten ist eine gängige Taktik von Angreifern, um Zugang zu sensiblen Informationen oder Systemen zu erhalten. Bei der Datenpanne von Marriott International im Jahr 2018 wurden die persönlichen Daten von etwa 500 Millionen Gästen preisgegeben, da der Hacker die Anmeldedaten eines Drittanbieters gestohlen hatte. Marriott musste daraufhin eine Geldstrafe in Höhe von 123 Millionen Dollar zahlen.[14]

Böswillige Insider, also Personen mit autorisiertem Zugang zu den Systemen eines Unternehmens, können eine erhebliche Bedrohung darstellen, wenn sie diesen Zugang missbrauchen. Im Jahr 2019 wurde ein ehemaliger Tesla-Mitarbeiter angeklagt, vertrauliche Informationen und geistiges Eigentum aus dem System des Unternehmens gestohlen zu haben. Der Mitarbeiter hatte Zugang zu den Systemen des Unternehmens und kopierte mehr als 300.000 Dateien auf sein persönliches Konto.[15]Die Weitergabe von geheimen Pentagon-Dokumenten an eine Videospiel-Chatgruppe im Jahr 2023 unterstreicht die heimtückische Natur von Bedrohungen durch Insider.[16]

Der Stuxnet-Wurm ist ein bemerkenswertes Beispiel für einen Zero-Day-Angriff, bei dem ein Angreifer eine zuvor unbekannte Schwachstelle in einer Software ausnutzt.[17]Er zielte auf industrielle Kontrollsysteme ab und nutzte mehrere Zero-Day-Schwachstellen in Windows- und Siemens-Software aus, um programmierbare logische Steuerungen zu modifizieren und potenziell physischen Schaden anzurichten. Es wird vermutet, dass der Angriff von einem nationalen Akteur durchgeführt wurde, und er hatte erhebliche Auswirkungen auf die Entwicklung von Cyberwaffen und die Verwendung von Zero-Day-Schwachstellen in der Kriegsführung.

Diese Beispiele zeigen die verheerenden finanziellen und rufschädigenden Folgen, die Angriffe auf die Cybersicherheit haben können. Unternehmen können mit rechtlichen Sanktionen, dem Verlust von Kunden und einer erheblichen Schädigung ihres Rufs konfrontiert werden. Darüber hinaus kann die Gesellschaft als Ganzes unter dem Verlust sensibler Informationen, der Unterbrechung kritischer Infrastrukturen und einem erhöhten Risiko von Identitätsdiebstahl und Betrug leiden. Angesichts dieser Risiken müssen Unternehmen die Cybersicherheit ernst nehmen und in robuste Sicherheitsmaßnahmen investieren, um ihre Systeme und Daten zu schützen.

Aktuelle Maßnahmen zum Schutz vor Cyber-Bedrohungen

Im dynamischen Bereich der Cybersicherheit ist es von entscheidender Bedeutung, den sich ständig weiterentwickelnden Bedrohungen immer einen Schritt voraus zu sein. Um dies zu erreichen, müssen Unternehmen modernste Lösungen nutzen. In diesem Bericht werden sechs wichtige Entwicklungen vorgestellt und ihre Funktionen, Vorteile und praktischen Anwendungen erläutert.

Ein entscheidender Fortschritt ist die Integration von KI und maschinellem Lernen (ML) als digitale Wächter (Tabelle 1). Ihre Fähigkeiten liegen in der Echtzeitanalyse riesiger Datenströme, der Entschlüsselung von Netzwerkverkehr, Benutzerverhalten und Systemprotokollen. Dadurch können sie aus bestehenden Schwachstellen lernen und zukünftige Angriffsmuster vorhersagen. KI und ML wirken

Tabelle 1. Optionen für den Einsatz von maschinellem Lernen im Bereich der Cybersicherheit[19]

Anwendungsfall	Beschreibung
Schwachstellen-Management	Bietet IT- und Sicherheitsteams eine empfohlene Priorisierung von Schwachstellen auf der Grundlage ihrer Kritikalität.
Statische Datei-Analyse	Ermöglicht die Vorbeugung von Bedrohungen durch die Vorhersage der Schädlichkeit von Dateien auf der Grundlage ihrer Merkmale.
Verhaltensbasierte Analyse	Analysiert das Verhalten von Angreifern zur Laufzeit, um Angriffsmuster in der gesamten Cyber-Kill-Chain zu modellieren und vorherzusagen.
Statische und verhaltensbasierte Hybrid-Analyse	Kombiniert statische Dateianalyse und Verhaltensanalyse, um eine erweiterte Erkennung von Bedrohungen zu ermöglichen.
Anomalie-Erkennung	Identifiziert Anomalien in Daten, um die Risikobewertung und die Untersuchung von Bedrohungen zu unterstützen.
Forensische Analyse	Führt Spionageabwehr durch, um den Verlauf von Angriffen zu analysieren und Systemschwachstellen zu identifizieren.
Sandbox-Malware-Analyse	Analysiert Code-Samples in isolierten, sicheren Umgebungen, um bösartiges Verhalten zu identifizieren und zu klassifizieren und es bekannten Gegnern zuzuordnen.

IT: Informationstechnologie.

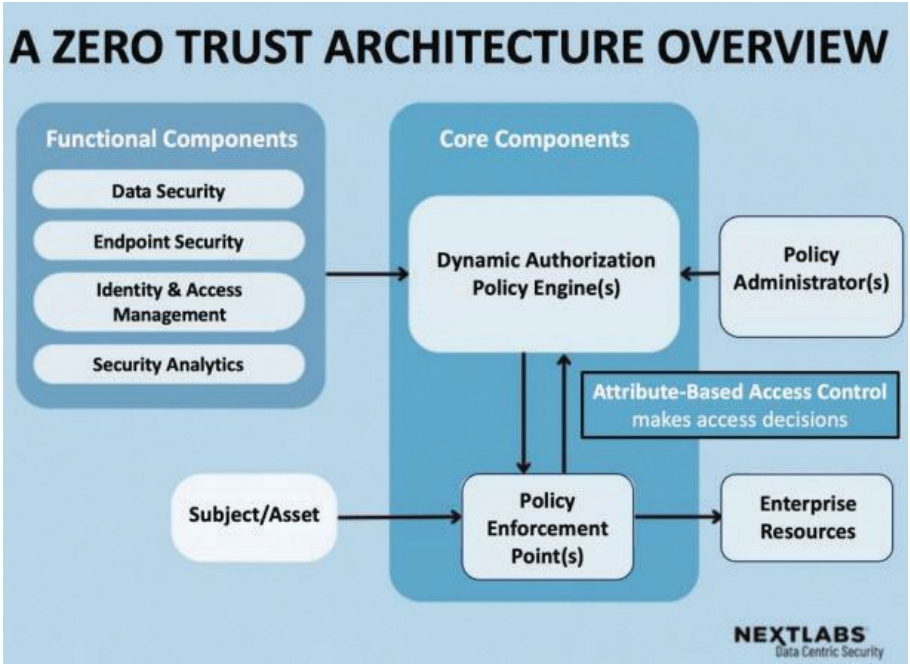

Abb. 2. Einrichtung einer ZTA-Lösung für Unternehmen. ZTA: Zero-Trust-Architektur.[21]

als übermenschliche Überwachungssysteme, die subtile Anomalien in der Netzwerkaktivität, ungewöhnliche Anmeldeversuche und verdächtige Dateiänderungen in Echtzeit erkennen. Dies ermöglicht kürzere Reaktionszeiten und versetzt Unternehmen in die Lage, Datenschutzverletzungen zu verhindern, indem sie Bedrohungen frühzeitig erkennen. Darüber hinaus sind diese Technologien hervorragend in der Lage, Zero-Day-Angriffe zu erkennen, was eine wichtige Verteidigungsschicht gegen neuartige Bedrohungen darstellt. Das Schöne an der KI-gestützten Reaktion auf Vorfälle ist die schnelle Reaktion. Diese Systeme können infizierte Systeme automatisch isolieren, Schwachstellen beseitigen und sogar Beweise sammeln und Berichte erstellen. Dadurch wird nicht nur die Ausbreitung von Bedrohungen verhindert, sondern auch der Analyseprozess gestrafft, was wertvolle Erkenntnisse für die Verbesserung künftiger Verteidigungsmaßnahmen liefert.[18]

Herkömmliche Sicherheitsansätze, die einer "Burg und Mauern" ähneln, sind in der heutigen vernetzten Welt überholt. Die Zero-Trust-Architektur (ZTA) bietet einen Paradigmenwechsel durch Mikro-Segmentierung und Zugangskontrolle, kontinuierliche Authentifizierung und Autorisierung. ZTA-Umgebungen unterteilen ein Netzwerk in kleine Festungen, die jeweils bestimmte Daten oder Anwendungen beherbergen. Die Implementierung des Least-Privilege-Zugriffs verhindert unbefugte seitliche Bewegungen innerhalb des Netzwerks (Abbildung 2). Die dynamische Vertrauensüberprüfung stellt sicher, dass das Vertrauen während einer Sitzung kontinuierlich überprüft wird und passt sich an die sich entwickelnde Risikolandschaft an. ZTA verwendet ein multifaktorielles Sicherheitssystem auf "Steroiden". Neben Passwörtern werden Faktoren wie Fingerabdrücke, biometrische Scans oder Einmalcodes zur Benutzerverifizierung eingesetzt. Bei der risikobasierten Authentifizierung werden kontextabhängige Faktoren wie die Aufenthaltsdauer des Benutzers und der Gerätetyp berücksichtigt und die Authentifizierungsanforderungen auf der Grundlage des bewerteten Risikos angepasst.[20]

Über Kryptowährungen hinaus bietet das verteilte, fälschungssichere Hauptbuch der Blockchain einzigartige Vorteile für die Cybersicherheit, einschließlich der sicheren Datenverfügbarkeit, der Fälschungssicherheit, des sicheren Identitätsmanagements und der dezentralen Verwaltung.

Citation: Blockchain im Gesundheitswesen heute 2024, **7**: 302 - https://doi.org/10.30953/bhty.v7.302

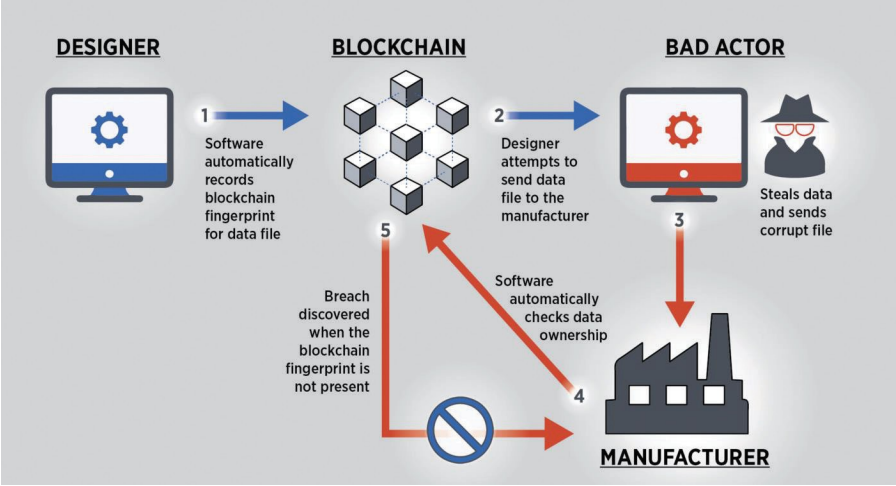

Abb. 3. Verallgemeinertes Konzept der Blockchain zum Schutz von Vermögenswerten.[22]

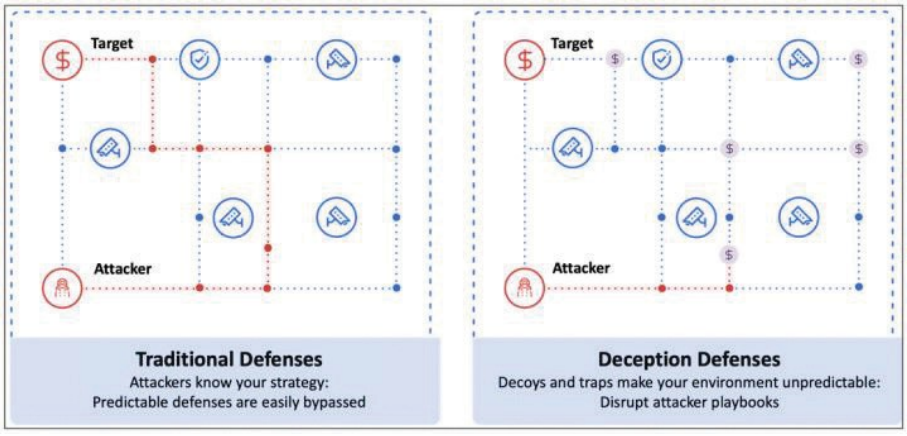

Abb. 4. Ein Beispiel für das Täuschungskonzept im Stil von Pac-Man.[24]

Identität. Blockchain verwendet kryptografisches Hashing und ein verteiltes Hauptbuch, um Datenblöcke zu sichern. Jeder Block ist mit einem eindeutigen digitalen Fingerabdruck gesichert, so dass jede Veränderung sofort erkennbar ist. Der verteilte Charakter des Hauptbuchs über ein Netzwerk macht Manipulationen praktisch unmöglich. Blockchain führt eine dezentralisierte Identität (DID) und überprüfbare Berechtigungsnachweise (VCs) ein. Die DID ermöglicht es den Nutzern, ihre Identitätsdaten zu kontrollieren, wodurch einzelne Fehlerquellen beseitigt werden. VCs ermöglichen es den Nutzern, Ausweise auszustellen und weiterzugeben, ohne auf Vermittler angewiesen zu sein, wodurch das Betrugsrisiko verringert wird (Abbildung 3).[23]

Täuschungstechnologien schaffen eine falsche digitale Realität, indem sie Honeytraps, Honeypots, Bedrohungsemulationen und Simulationen einsetzen, um Cyberkriminelle in die Irre zu führen und auszuschalten. Honeytraps und Honeypots fungieren als digitale Köder und Fallen. Honeytraps ähneln echten Systemen und verleiten Angreifer dazu, Zeit zu verschwenden. Honeypots erfassen Taktiken und Techniken von Angreifern und liefern wertvolle Informationen für Sicherheitsteams. Bedrohungsemulationen und -simulationen stellen tatsächliche Angriffsvektoren nach, Sie ermöglichen es Unternehmen, ihre Verteidigung zu testen und Schwachstellen zu erkennen. Diese Simulationen decken Schwachstellen in bestehenden Sicherheitskontrollen auf und helfen dabei, Schwachstellen vorrangig zu beheben und die Abwehr zu stärken (Abbildung 4).[25]

Solide rechtliche Rahmenbedingungen sind für die Risikominderung und die Rechenschaftspflicht von zentraler Bedeutung. Diese rechtlichen Maßnahmen bieten im Zusammenspiel mit technologischen Fortschritten eine umfassende Verteidigung gegen böswillige Akteure. Die General Data Protection Regulation, der Cybersecurity Information Sharing Act (CCPA) und andere regionale Gesetze legen Datensicherheitsstandards fest und erhöhen die branchenweite Cybersicherheit. Der Schutz kritischer Infrastrukturen schreibt spezifische Sicherheitskontrollen vor, um lebenswichtige Systeme vor Cyber-Bedrohungen zu schützen. Das CISA fördert die Zusammenarbeit zwischen dem privaten und dem öffentlichen Sektor und eine schnelle Reaktion durch den Austausch von Informationen über Bedrohungen.[26]Globale Vereinbarungen wie die Budapester Konvention fördern die Zusammenarbeit bei der Bekämpfung der Cyberkriminalität. Gesetze wie der Computer Fraud and Abuse Act in den USA stellen verschiedene cyberbezogene Straftaten unter Strafe und dienen als rechtliche Abschreckung gegen

böswillige Aktivitäten. Verordnungen wie das EU-Gesetz zur Cybersicherheit machen Unternehmen unter bestimmten Umständen für Datenschutzverletzungen haftbar, schaffen Anreize für solide Sicherheitspraktiken und fördern die Rechenschaftspflicht.[27]Initiativen wie die britische Regulatory Sandbox ermöglichen das Testen neuer Cybersicherheitstechnologien in kontrollierten Umgebungen, beschleunigen die Entwicklung und fördern Innovationen als Reaktion auf neue Bedrohungen. Regelmäßige Überprüfungen und Aktualisierungen von Gesetzen und Rahmenwerken sind von entscheidender Bedeutung, um mit der sich entwickelnden Bedrohungslandschaft Schritt zu halten. Ein offener Dialog zwischen politischen Entscheidungsträgern, Sicherheitsexperten und Interessenvertretern aus der Industrie sorgt dafür, dass die Rahmenwerke relevant bleiben.

Die Verhaltensbiometrie verleiht der Sicherheit eine neue Dimension, indem sie Benutzer anhand einzigartiger Merkmale wie Tastenanschläge, Mausbewegungen und Anmeldegewohnheiten erkennt. Die Verhaltensbiometrie überwacht kontinuierlich die Benutzeraktivität, einschließlich der Dynamik der Tastenanschläge, der Mausbewegungen und der Anmeldegewohnheiten. Auf diese Weise entsteht ein digitaler Wächter, der jede Bewegung überwacht und die Sicherheit erhöht, indem er Abweichungen von etablierten Benutzerprofilen erkennt. Diese Form der Biometrie passt die Verteidigungsmaßnahmen an das Risikoprofil des Benutzers an. Bei Szenarien mit hohem Risiko werden zusätzliche biometrische Überprüfungsschritte ausgelöst, während Aktivitäten mit geringerem Risiko weiterhin rationalisiert werden, um eine benutzerfreundliche Erfahrung zu bieten. Verhaltensbiometrie hilft auch bei der Aufdeckung von Betrug, indem sie ungewöhnliche Veränderungen im Benutzerverhalten erkennt (Abbildung 5).[29]

Während diese sechs Fortschritte einen bedeutenden Fortschritt in der Cybersicherheit darstellen, entwickelt sich die Landschaft weiter. Technologien wie Quantencomputing, sichere Mehrparteienberechnung (SMPC) und homomorphe Verschlüsselung versprechen eine weitere Stärkung der Abwehrkräfte. Für ein widerstandsfähiges und sicheres digitales Umfeld ist jedoch eine ganzheitliche Cybersicherheitsstrategie unabdingbar. Dazu müssen fortschrittliche Technologien und traditionelle Sicherheitspraktiken miteinander kombiniert und die globale Zusammenarbeit gefördert werden, um die sich entwickelnde Bedrohungslandschaft zu bekämpfen. Das Erkennen der rechtlichen Unterschiede zwischen den Regionen zu erkennen, ist für die Wirksamkeit einer solchen Strategie von entscheidender Bedeutung.

Analyse der aktuellen Cyber-Resilienzmaßnahmen gegen reale Bedrohungen

Eine eingehende Untersuchung der Verteidigungsstrategien gegen die vielfältigen digitalen Bedrohungen offenbart ein komplexes Zusammenspiel von fortschrittlichen Technologien und umfassenden Rahmenbedingungen. Dieser komplizierte Tanz beinhaltet eine symbiotische Beziehung zwischen KI, ML, ZTA, Blockchain, rechtlichen Rahmenbedingungen und robusten Cybersicherheitspraktiken, die einen vielseitigen Verteidigungsmechanismus bilden.

Sowohl KI als auch ML fungieren als wachsame Wächter, die umfangreiche Datenanalysen durchführen, um gefährdete Komponenten zu identifizieren und verdächtige IoT-Aktivitäten zu erkennen. Dies ergänzt nahtlos robuste Cybersicherheits-Frameworks, die branchenübliche Best Practices festlegen. Die ZTA stärkt die Sicherheit weiter, indem sie seitliche Bewegungen einschränkt, selbst nach einem möglichen Eindringen. Die Verwendung von Blockchain, einem unveränderlichen Ledger, gewährleistet die Nachverfolgung der Herkunft von Komponenten und geht damit auf Bedenken hinsichtlich der Authentizität in der Lieferkette ein. Die Einbeziehung von Leitlinien aus anerkannten Cybersicherheitsrahmenwerken, wie dem Cybersecurity Framework des National Institute of Standards and Technology, verbessert die sichere Implementierung von Blockchain. Es ist wichtig, das Potenzial für KI-Voreingenommenheit anzuerkennen, was die Bedeutung von ethischen Überlegungen und verschiedenen Trainingsdatensätzen unterstreicht. Auch wenn die Komplexität der ZTA spezielles Fachwissen erfordert, kann die Anwendung von Cybersicherheits-Frameworks als Implementierungsvorgaben die Herausforderungen abmildern. Die Begrenzung der Skalierbarkeit in aktuellen Blockchain-Implementierungen erfordert gemeinsame Anstrengungen und eine klare Regulierung.

Im Bereich der DDoS-Angriffe spielen KI und ML eine entscheidende Rolle bei der schnellen Reaktion auf anomale Datenverkehrsmuster und bei der Abschwächung ihrer Auswirkungen. Koordinierte Vorfälle

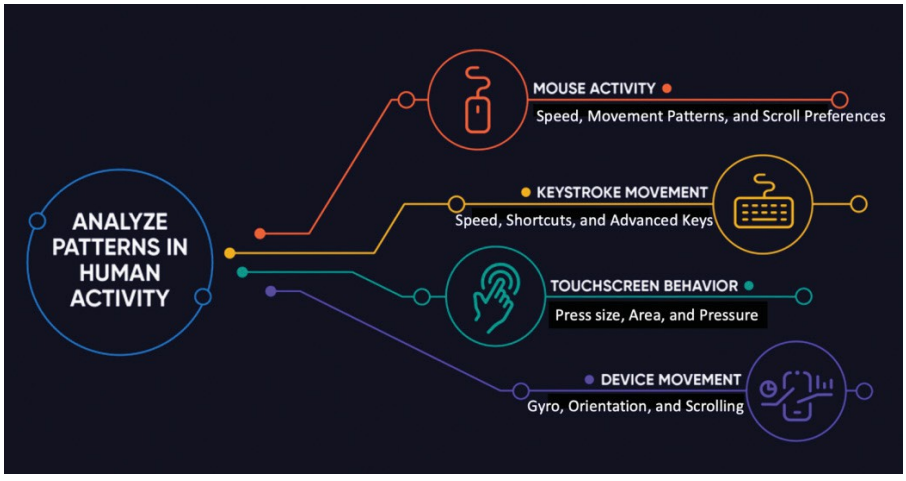

Abb. 5. Arten von Einzigartigkeit im Verhaltensmuster eines Menschen[28]

Citation: Blockchain im Gesundheitswesen heute 2024, **7**: 302 - https://doi.org/10.30953/bhty.v7.302

Reaktionspläne, wie sie in etablierten Cybersicherheitsrahmen festgelegt sind, sorgen für minimale Ausfallzeiten. Spezialisierte DDoS-Minderungsdienste dienen als Bollwerk gegen digitale Angriffe, wobei die rechtlichen Rahmenbedingungen die Dienstanbieter bei Verstößen zur Verantwortung ziehen. ZTA stärkt durch Identitätsüberprüfung und Zugangsbeschränkungen die Abwehr von DDoS-Angriffen, die von kompromittierten Konten ausgehen. Es ist jedoch wichtig zu erkennen, dass KI-basierte DDoS-Minderungssysteme unbeabsichtigt den legitimen Datenverkehr stören können, was zu Serviceunterbrechungen führt. Die Kosten, die mit spezialisierten DDoS-Abwehrdiensten verbunden sind, stellen vor allem für kleinere Unternehmen ein finanzielles Hindernis dar. Die Herausforderungen bei der Koordination während der Reaktion auf einen Vorfall, die durch Kommunikationsverzögerungen und komplexe Rechtssysteme beeinflusst werden, unterstreichen die Komplexität der DDoS-Abwehr.

Bei der Bekämpfung von APTs fungieren KI und ML als aufmerksame Analysten, die subtile Anomalien erkennen, die auf potenzielle Bedrohungen hinweisen. Rechtliche Rahmenbedingungen erleichtern den Austausch von Bedrohungsdaten und fördern eine kollektive Verteidigung gegen bekannte APT-Taktiken. ZTA verhindert durch eingeschränkten Zugang und kontinuierliche Identitätsüberprüfung die Bewegung von APT und die Datenexfiltration. Das Vorhandensein von Gesetzen zur Meldung von Datenschutzverletzungen schafft Anreize für eine rasche Offenlegung und mindert so den durch APT verursachten Schaden. KI-basierte APT-Erkennungssysteme können jedoch falsch-positive Ergebnisse liefern, was ressourcenintensive Untersuchungen erforderlich macht. Die ausgefeilten Techniken, die APTs zur Verschleierung ihrer Aktivitäten einsetzen, unterstreichen die Grenzen fortschrittlicher Überwachungsinstrumente. Datenschutzbedenken und die Notwendigkeit von Vertrauen können den gemeinsamen Austausch von sensiblen Bedrohungsdaten behindern.

Durch die Verlagerung des Schwerpunkts auf Social Engineering und die Schulung des Sicherheitsbewusstseins wird der Einzelne in die Lage versetzt, Manipulationen zu erkennen und sich dagegen zu wehren, unterstützt durch Cybersicherheitsrahmen, die eine effektive Programmumsetzung ermöglichen. Die Multi-Faktor-Authentifizierung fügt eine zusätzliche Sicherheitsebene hinzu, wobei die rechtlichen Rahmenbedingungen einen Anreiz für ihre Einführung bieten. Die Förderung einer offenen Kommunikationsumgebung begünstigt die frühzeitige Erkennung von Social-Engineering-Methoden. Die Wirksamkeit von Schulungen zum Sicherheitsbewusstsein kann jedoch von Mitarbeiter zu Mitarbeiter variieren, insbesondere bei Mitarbeitern mit begrenztem technischem Wissen. Die ständige Weiterentwicklung der Angreifer erfordert eine kontinuierliche Anpassung der Strategien, um neuen Techniken zu begegnen. Die Etablierung einer Kultur der offenen Kommunikation kann eine Herausforderung sein, insbesondere in hierarchischen Organisationen.

Verhaltensbiometrie kommt ins Spiel, wenn das Benutzerverhalten überwacht wird, um potenzielle unbefugte Zugriffsversuche aufzudecken. Starke Passwörter und Multi-Faktor-Authentifizierung bieten einen robusten Schutz, der sich an Cybersicherheits-Frameworks orientiert. Die Verhinderung von Datenverlusten minimiert das Risiko des Abflusses sensibler Daten, und die Gesetze zur Meldung von Datenschutzverletzungen schaffen Anreize für schnelle Reaktionen. Dennoch können Bedenken hinsichtlich des Datenschutzes bei der Erfassung biometrischer Daten von Mitarbeitern aufkommen, und die Ermüdung der Benutzer bei der Multifaktor-Authentifizierung kann die konsequente Einführung beeinträchtigen. Die Implementierung und Wartung effektiver Lösungen zur Verhinderung von Datenverlusten (DLP) stellt eine finanzielle Herausforderung dar.

Beim Schutz des geistigen Eigentums sorgt die Verschlüsselung der Daten für Vertraulichkeit, wobei ein unzureichender Schutz sensibler Daten durch gesetzliche Bestimmungen bestraft wird. Die Verwaltung digitaler Rechte kontrolliert den Zugriff und verhindert das unautorisierte Kopieren und Verbreiten. Die in den Rahmenwerken für Cybersicherheit vorgesehene Planung der Reaktion auf Vorfälle erleichtert ein schnelles Handeln im Falle eines vermuteten Diebstahls geistigen Eigentums. Die sichere Verwaltung von Verschlüsselungsschlüsseln ist jedoch von entscheidender Bedeutung, um die Wirksamkeit der Verschlüsselung zu gewährleisten. Probleme mit der Interoperabilität verschiedener DRM-Systeme können die Verbreitung von Inhalten behindern. Die Schnelligkeit der Reaktion auf den Diebstahl geistigen Eigentums erfordert eine umfassende Koordinierung und rechtliche Überlegungen.

Bei der Verbesserung der Zero-Day-Überwachung scannen KI und ML kontinuierlich nach Anomalien, um Zero-Day-Angriffe vor ihrer weiten Verbreitung zu bekämpfen. Täuschungstechnologien wie Honeypots und Täuschungsmanöver decken Zero-Day-Angriffe auf, wobei rechtliche Rahmenbedingungen Schutz bieten. Die Modellierung von Bedrohungen, die durch strukturierte Methoden erleichtert wird, ermöglicht proaktive Abhilfemaßnahmen. Allerdings können Probleme mit der KI-Erklärbarkeit zu falsch positiven Ergebnissen oder zur Übersehen von Bedrohungen führen. Rechtliche Überlegungen beim Einsatz von Täuschungstechnologien unterstreichen mögliche Störungen und erfordern eine sorgfältige Planung. Fachliche Lücken bei der Modellierung von Bedrohungen stellen eine Herausforderung bei der effektiven Planung und Eindämmung von Zero-Day-Bedrohungen dar.

Der Umgang mit Insider-Bedrohungen beinhaltet die Überwachung ungewöhnlichen Nutzerverhaltens durch biometrische Verhaltensdaten und die Durchführung regelmäßiger Zugriffsüberprüfungen, die von Cybersicherheitsrahmenwerken geleitet werden. Anonyme Meldemechanismen ermöglichen es den Mitarbeitern, verdächtige Aktivitäten ohne Angst vor Vergeltungsmaßnahmen zu melden. Bei der Überwachung von Mitarbeiteraktivitäten ist es wichtig, die Sicherheitsbedürfnisse mit dem Schutz der Privatsphäre der Mitarbeiter in Einklang zu bringen. Die Effizienz regelmäßiger Zugriffsüberprüfungen kann durch die ressourcenintensive Natur des Prozesses beeinträchtigt werden. Trotz des gesetzlichen Schutzes kann die Angst vor Vergeltungsmaßnahmen eine rechtzeitige Meldung von Insider-Bedrohungen behindern.

Im Zusammenhang mit der Eindämmung von Ransomware-Angriffen sorgen Datensicherungen für eine rasche Wiederherstellung, wodurch die Auswirkungen solcher Angriffe gemildert werden. Ein zeitnahes Schwachstellenmanagement verringert die Angriffsfläche, wobei die rechtlichen Rahmenbedingungen zur Offenlegung von Schwachstellen anregen. Schulungen zum Sicherheitsbewusstsein klären die Mitarbeiter über Ransomware-Risiken und Phishing-Taktiken auf. Ransomware-Angriffe können jedoch auf Backups abzielen, was selbst nach der Wiederherstellung des Primärsystems zu Datenverlusten führen kann. Die zeitnahe Behebung von Schwachstellen kann eine Herausforderung darstellen, insbesondere in komplexen IT-Umgebungen. Häufige Schulungen zum Sicherheitsbewusstsein können zur Ermüdung der Mitarbeiter beitragen.

Social-Engineering-Angriffe können durch die Überwachung sozialer Medien , geleiteter durch Daten Datenschutz entschärft werden.

Vorschriften. Kampagnen zur Sensibilisierung für Phishing und Multi-Faktor-Authentifizierung verringern die Erfolgsquote solcher Angriffe. Rechtliche Rahmenbedingungen schaffen Anreize für strenge Authentifizierungspraktiken. Die Überwachung der Social-Media-Aktivitäten von Mitarbeitern wirft jedoch Bedenken hinsichtlich des Datenschutzes auf und erfordert elternübergreifende Richtlinien. Die Entwicklung effektiver Phishing-Simulationen kann ressourcenintensiv sein. Multifaktor-Authentifizierungssysteme sind zwar effektiv, bergen aber potenzielle Schwachstellen. Die Datenklassifizierung priorisiert und kennzeichnet sensible Daten, wie in den Datenschutzbestimmungen vorgeschrieben. Die Datenzugriffskontrolle schränkt den Zugriff ein und minimiert das Risiko einer unbefugten Datenextraktion. Die DLP-Tools erkennen und verhindern unbefugte Datenübertragungen und orientieren sich dabei an Cybersicherheits-Frameworks. Allerdings kann eine zu granulare Datenklassifizierung die Betriebskosten erhöhen und den legitimen Datenzugriff behindern. Die Implementierung robuster Zugriffskontrollsysteme erfordert Fachwissen in den Bereichen Identitätsmanagement und Autorisierung. Die DLP-Tools können... Dies kann zu falsch-positiven Ergebnissen führen, die ein sorgfältiges Management erfordern.

Eine kontinuierliche Benutzerüberwachung, die durch technische und organisatorische Maßnahmen umgesetzt wird, hilft bei der Verhinderung von unbefugter Kontoübernahme. Fortschrittliche Analysetools erkennen verdächtige Muster bei Benutzeranmeldungen. Starke Authentifizierungspraktiken, einschließlich Multi-Faktor-Authentifizierung und strenge Passwortrichtlinien, verringern das Risiko einer erfolgreichen Kontoübernahme erheblich. Rechtliche Rahmenbedingungen können Anreize für Unternehmen schaffen, starke Authentifizierungsverfahren einzuführen und beizubehalten. Die Implementierung und Wartung von Systemen zur kontinuierlichen Benutzerüberwachung kann jedoch kostspielig sein, insbesondere für Unternehmen mit einer großen Benutzerbasis. Ein hohes Aufkommen an Warnmeldungen zu verdächtigen Aktivitäten kann Sicherheitsteams überfordern, was zu einer Ermüdung der Warnmeldungen und einer möglichen Übersehbarkeit echter Bedrohungen führt. Es ist eine Herausforderung, die Benutzer davon zu überzeugen, konsequent starke Authentifizierungsmethoden anzunehmen und zu verwenden, insbesondere bei technisch nicht versierten Benutzern. Bei der Navigation durch die komplizierte Landschaft der Cybersicherheit ist es unerlässlich, sowohl die Stärken als auch die Grenzen der verschiedenen Strategien zu erkennen. Die kollaborative Integration von KI, ML, ZTA, Blockchain, rechtlichen Rahmenbedingungen und umfassenden Cybersicherheitspraktiken trägt zu einer vielschichtigen Verteidigung gegen die vielfältigen und sich weiterentwickelnden Bedrohungen bei, die Schatten auf die digitale Welt werfen. Da sich die Technologien weiterentwickeln und die Bedrohungen zunehmen, ist ein ganzheitlicher Ansatz, der technologische Innovationen, ethische Überlegungen, die Einhaltung von Vorschriften und kontinuierliche Verbesserungen umfasst, für den Schutz der Integrität von entscheidender Bedeutung, Vertraulichkeit und Verfügbarkeit digitaler Daten.

Vorgeschlagene Lösungen zum Schutz der digitalen Integrität

Wir haben uns mit verschiedenen Lösungen zur Verhinderung von Bedrohungen der Cybersicherheit befasst und dabei festgestellt, dass es keine Einheitslösung gibt, die allen gerecht wird. Lassen Sie uns nun unseren Fokus auf einen anderen Aspekt des Problems richten. Wie können wir die Verbreitung von durchgesickerten vertraulichen Informationen minimieren? Welche Maßnahmen können ergriffen werden, um Datenschutzverletzungen weniger lohnend zu machen und potenzielle Angreifer davon abzuhalten, solche Aktionen zu starten? Lassen Sie uns Lösungen rund um diese Fragen untersuchen.

Konzept der Deleakifizierung

Ausgehend von der Philosophie, dass ein proaktiver Ansatz der Schlüssel zu einer effektiven Verteidigung ist, habe ich ein Konzept entwickelt, das diesem Prinzip entspricht. Bevor wir uns mit den Details befassen, sollten wir uns mit einigen grundlegenden Begriffen vertraut machen, die sich bei unserer Untersuchung als nützlich erweisen werden.

Zunächst einmal sind Hexadezimaldaten eine Darstellung von Informationen in einem numerischen System zur Basis 16. Dies ist ein grundlegendes Format für die Kodierung von Binärdaten, das häufig in der Programmierung und Informatik verwendet wird.

Beim inhaltsbasierten Fingerprinting wird der Bild- oder Toninhalt einer Datei untersucht, um einen eindeutigen Fingerabdruck zu erstellen - eine Art digitaler "Hash", der das Wesentliche des Mediums erfasst, ohne dass eine Wiedergabe erforderlich ist. Algorithmen extrahieren Merkmale wie Farben, Texturen, Formen oder Audiofrequenzen, um diesen Fingerabdruck zu erstellen. Wichtig ist, dass diese Methode bei der Identifizierung des ursprünglichen Inhalts wirksam bleibt, selbst wenn das Dateiformat geändert oder komprimiert wird.[30]Perceptual Hashing verlagert den Schwerpunkt darauf, wie Menschen Inhalte wahrnehmen. Trotz Rauschen, Komprimierungsartefakten oder Bearbeitung bleibt Perceptual Hashing bei der eindeutigen Identifizierung von Medien stabil.[31]

Ein Wurm ist eine Art von Schadsoftware, die in der Lage ist, sich unabhängig zu replizieren und sich über Netzwerke und Systeme zu verbreiten. Würmer nutzen Schwachstellen aus und stellen eine erhebliche Bedrohung für die Sicherheit von vernetzten Umgebungen dar.

Auch Trojaner-Malware tarnt sich als legitime Software und verleitet den Benutzer zur Installation der Software. Einmal infiltriert, ermöglicht sie unbefugten Zugriff und kann sensible Informationen gefährden oder andere bösartige Aktivitäten erleichtern.

Außerdem ist eine Logikbombe ein Stück Code, das absichtlich in ein Softwaresystem eingefügt wird, um schädliche Aktionen auszuführen, wenn bestimmte Bedingungen erfüllt sind. Diese Bedingungen können durch verschiedene Ereignisse ausgelöst werden, was zu Störungen oder Schäden am System führen kann.

Im Bereich der jüngsten Sicherheitslücken ist die kritische WebP-Bildschwachstelle (CVE-2023-4863) hervorzuheben.[32]Diese Schwachstelle ermöglicht es Angreifern, über manipulierte .webp-Dateien bösartigen Code auszuführen, was aufgrund der weit verbreiteten Verwendung der libwebp-Bibliothek zur Verarbeitung solcher Bilder zahlreiche Anwendungen betrifft. Um diese Sicherheitslücke zu schließen und den Schutz zu gewährleisten, sind sofortige Software-Updates erforderlich. Wir konzentrieren uns nun auf die eingebauten Schutzmechanismen: Die in das Betriebssystem integrierten Virenscanner und Suchindexer sind wichtige Werkzeuge, um Viren und Malware zu erkennen und zu neutralisieren. Diese Dienstprogramme überwachen und identifizieren aktiv potenzielle Bedrohungen und tragen damit wesentlich zum Gesamtschutz bei. Sicherheit des Systems.

Citation: Blockchain im Gesundheitswesen heute 2024, **7**: 302 - https://doi.org/10.30953/bhty.v7.302

Darüber hinaus dient ein Content Delivery Network (CDN) als verteiltes System von Servern, die zusammenarbeiten, um Webinhalte auf der Grundlage der geografischen Standorte der Nutzer effizient bereitzustellen. CDNs verbessern nicht nur die Leistung von Websites, sondern bieten auch eine zusätzliche Sicherheitsebene gegen bestimmte Cyber-Bedrohungen.

Das Verständnis dieser Begriffe ist wichtig, um die Feinheiten des Konzepts zu verstehen, bei dem es um eine proaktive Verteidigungsstrategie geht. Lassen Sie uns nun näher darauf eingehen, wie jedes dieser Elemente zum Aufbau meines robusten Cybersicherheitsansatzes beiträgt.

Dazu werden die gewünschten Medien- oder Textdateien entnommen, um sie zu "entfesseln". Diese Dateien werden dann mit Software wie Hex Dump oder Vim verarbeitet, um Hex-Daten für Textdateien und eindeutige Identifizierungsinformationen für Mediendateien zu erhalten, wobei inhaltsbasierte Fingerprinting- und Perceptual-Hashing-Methoden eingesetzt werden. Anschließend wird ein Wurmcode entwickelt, der sich über das Internet verbreitet und eine Verbindung zu CDNs herstellt, um Trojaner herunterzuladen (Abbildung 6).

Sobald der Wurm auf einem Gerät aktiv ist, ruft er das Trojaner-Paket ab, und der Trojaner wiederum lädt die zuvor generierten und über verschiedene öffentliche oder private CDNs verteilten Metadaten (Hex-Daten oder eindeutige Kennungen) herunter. Im nächsten Schritt verbindet sich der Trojaner mit den systemeigenen Virenscannern oder Suchindizes und startet einen Suchlauf, um Übereinstimmungen mit den gespeicherten Metadaten zu finden.

In Fällen, in denen dem System ein Scanner für Root-/Admin-Zugriff fehlt, kann der Wurm seinen eigenen von vorinstallierten Scannern im CDN herunterladen. Mithilfe einer Trojaner-Strategie kann der Wurm Benutzer dazu verleiten, Administratorrechte zu gewähren, indem er sich als Systemdatei ausgibt. Um auf den Scan-Prozess zurückzukommen: Wird eine Übereinstimmung festgestellt, agiert der Wurm wie eine logische Bombe und beschädigt Dateien, indem er die ursprünglichen Daten durch Mülldaten ersetzt. Diese Methode zielt darauf ab, die durchgesickerten Informationen zu entfernen, ohne zusätzliche zerstörerische Aktionen auszulösen.

In Situationen, in denen kein CDN-Zugang verfügbar ist, kann das Wurm-Skript an eine Datei angehängt und an unverdächtige Benutzer gesendet werden, was an Techniken wie Word-Makros oder die Ausnutzung von Sicherheitslücken wie .webp erinnert. Sobald der Wurm ausgeführt wird, führt er seine Aufgaben aus. Darüber hinaus ist der Wurm so programmiert, dass er das Vorhandensein vorhandener Trojaner erkennt, um eine Überlastung des Systems und eine mögliche Entdeckung durch den Benutzer zu verhindern. Dieser umfassende Ansatz gewährleistet eine strategische und nuancierte Methode zur Bekämpfung von Informationslecks.

Web3-Datenschutzmodell

Der Übergang vom Web 2.0 zum Web 3.0 markiert einen Wechsel von zentralisierten zu dezentralisierten Systemen. Das Kernprinzip des Web 3.0 ist die Dezentralisierung, die die Art und Weise, wie Daten und Anwendungen gehandhabt werden, grundlegend verändert. Dieser Wandel verbessert den Schutz der Privatsphäre, indem er die Abhängigkeit von zentralen Behörden verringert und dem Einzelnen eine größere Kontrolle über seine persönlichen Daten ermöglicht. Im Web 3.0 spielen Technologien wie Blockchain, dezentralisierte Identifikatoren und Zero-Knowledge-Proofs eine Schlüsselrolle bei der Förderung einer privateren, sichereren und benutzerfreundlicheren digitalen Umgebung. Um nun auf die Feinheiten dieses Modells einzugehen, nutzt es moderne Konzepte, die sich derzeit in der Entwicklung befinden. Bevor wir uns mit den operativen Details des Modells befassen, ist es wichtig, sich mit der zugehörigen Terminologie vertraut zu machen.

Die DIDs sind ein grundlegendes Element des Web 3.0 und spielen eine wichtige Rolle bei der Bereitstellung eines dezentralen Mechanismus zur Erstellung und Verwaltung eindeutiger Online-Identitäten. Durch die DIDs erhalten die Nutzer die Möglichkeit, ihre digitalen Persönlichkeiten selbständig zu erstellen und zu kontrollieren, wodurch der Schutz der Privatsphäre verbessert wird. Ein Beispiel hierfür ist die Fähigkeit von DIDs, Online-Identitäten zu erstellen und zu verwalten, ohne sich auf eine zentrale Behörde verlassen zu müssen, was dem übergreifenden Thema der Verbesserung der Privatsphäre der Nutzer im digitalen Bereich entspricht.[33]

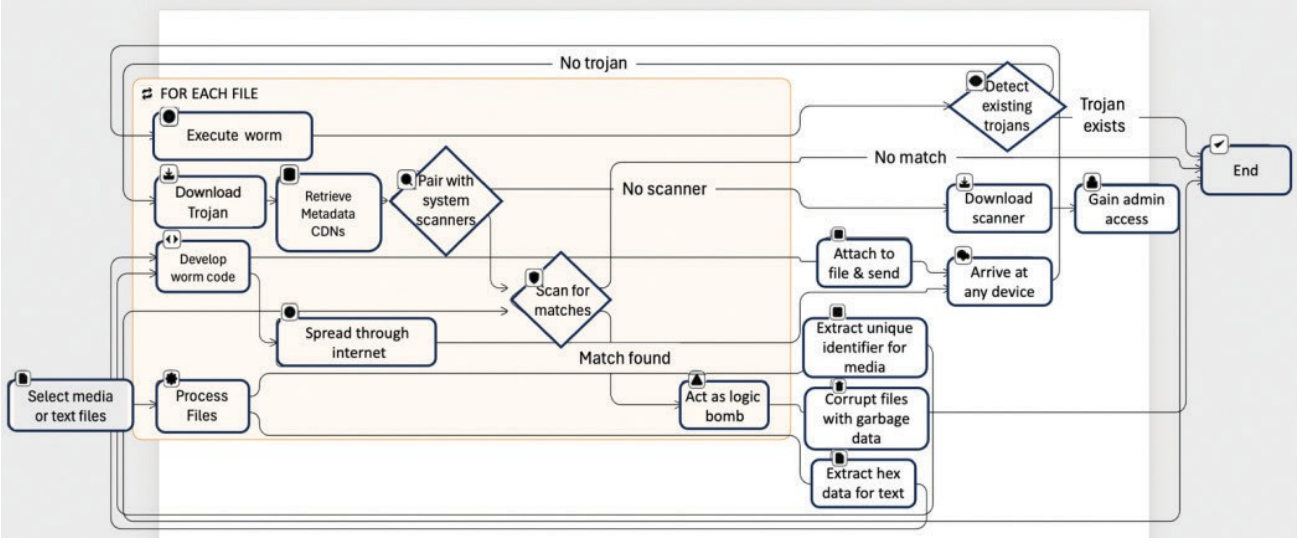

Abb. 6. Flussdiagramm zur Erklärung des Funktionsmechanismus.

VCs sind ein zentraler Aspekt des Web 3.0, da sie die Ausstellung und Präsentation von fälschungssicheren, digital überprüfbaren Berechtigungsnachweisen erleichtern. In der Praxis können Einzelpersonen digital signierte Ausweise, wie z. B. Diplome, weitergeben, ohne unnötige persönliche Informationen preiszugeben. Dies ist ein Beispiel für die Rolle der VCs bei der Stärkung der Privatsphäre und der Sicherheit und ein konkretes Beispiel dafür, wie sie die Nutzer in der digitalen Landschaft unterstützen.[34]

Zero-knowledge proofs (ZKPs) sind eine wichtige kryptografische Technik innerhalb des Web 3.0-Paradigmas, die es Parteien ermöglicht, die Authentizität von Informationen zu beweisen, ohne die eigentlichen Daten offenzulegen. Die ZKPs leisten einen wichtigen Beitrag zum Schutz der Privatsphäre, indem sie Informationen verifizieren, ohne die zugrunde liegenden Details preiszugeben. Ein Beispiel, das dieses Konzept veranschaulicht, ist die Tatsache, dass ZKPs es jemandem ermöglichen, die Kenntnis eines Geheimnisses zu beweisen, ohne das Geheimnis selbst offenzulegen, wodurch die Privatsphäre bei digitalen Transaktionen gewährleistet wird.[35]

Föderiertes Lernen (FL) verändert die ML-Landschaft im Web 3.0, indem es das gemeinsame Trainieren von Modellen auf dezentralen Geräten erleichtert. Ein Beispiel für den datenschutzfreundlichen Ansatz von FL ist die Möglichkeit, dass mobile Geräte gemeinsam ein Vorhersagemodell trainieren können, ohne Rohdaten auszutauschen. Auf diese Weise wird die Privatsphäre der Nutzer gewahrt, während gleichzeitig das gesammelte Wissen zum Nutzen des gesamten Systems genutzt wird.[36]

SMPC spielt eine entscheidende Rolle im Web 3.0, da es sichere Berechnungen zwischen mehreren Parteien ermöglicht, ohne dass die einzelnen Eingaben offengelegt werden. Ein anschauliches Beispiel ist, wenn SMPC es mehreren Parteien ermöglicht, gemeinsam ein Ergebnis zu berechnen, ohne ihre individuellen Eingaben preiszugeben. Diese Funktionalität erweist sich als wertvoll für die Analyse vertraulicher Daten und unterstreicht ihre Bedeutung für den Schutz der Privatsphäre.[37]

Persönliche Datenspeicher (PDS) ermöglichen es dem Einzelnen, seine persönlichen Daten sicher in einem privaten Speicher zu verwalten. PDS ermöglichen es den Nutzern beispielsweise, den Zugriff auf ihre gespeicherten Informationen zu kontrollieren, wodurch die Kontrolle der Nutzer über ihre digitale Identität gestärkt und die Privatsphäre bei der Verwaltung persönlicher Daten verbessert wird.[38]

Blockchain-basierte Datenspeicherung (BBDS) ist ein revolutionäres Konzept im Web 3.0, das die Informationsspeicherung über ein Netzwerk von Knotenpunkten dezentralisiert. Dieser transparente und fälschungssichere Ansatz gewährleistet die Datenintegrität und minimiert das Risiko unbefugter Änderungen. Ein Beispiel zur Veranschaulichung dieses Konzepts ist die Speicherung von Daten in der Blockchain, die sie fälschungssicher macht und eine transparente, sichere und datenschutzfreundliche Datenspeicherung gewährleistet.[39]

Vertrauenswürdige Ausführungsumgebungen (Trusted Execution Environments, TEEs) leisten einen wichtigen Beitrag zum Web 3.0, indem sie sichere Bereiche auf Geräten für die Verarbeitung sensibler Informationen bereitstellen. TEEs sind in der Lage, Verschlüsselungsschlüssel zu sichern und die Privatsphäre der Nutzer zu schützen, indem sie sicherstellen, dass bestimmte Prozesse in einem vertrauenswürdigen und geschützten Bereich auf einem Gerät stattfinden.[40]

Derzeit ist die Terminologie vielleicht nicht ganz klar (Abbildung 7). Verschaffen wir uns ein umfassendes Verständnis von

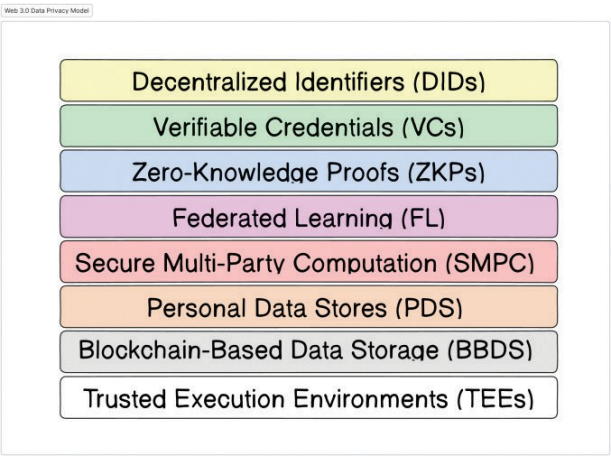

Abb. 7. Web3-Datenschutzmodell (W3DPM).

all dieser Konzepte, indem wir das Modell verwenden und ein Beispiel erkunden, das die Funktionalität jedes Modells demonstriert.

In diesem futuristischen Wahlszenario, das auf Web 3.0-Technologien basiert, erlebt der Einzelne einen transformativen und datenschutzgerechten Wahlprozess. Jeder Wähler ist mit einer DID ausgestattet, die auf seinem Mobilgerät gespeichert ist und ihm das Eigentum und die Kontrolle über seine digitale Identität verleiht, unabhängig von einer zentralen Behörde. Anstelle eines herkömmlichen physischen Ausweises stellen die Wähler über ihre DIDs direkt aus den Datenbanken der Regierung sichere Wahlscheine aus, mit denen sie ihre Wahlberechtigung nachweisen können, ohne ihre persönlichen Daten preiszugeben, und die somit ihre Privatsphäre verbessern.

Um den Datenschutz weiter zu gewährleisten, setzt die Wahlbehörde ZKPs ein, um die Wahlberechtigung zu überprüfen, ohne auf individuelle Datensätze zuzugreifen, und um die Wahlberechtigung zu bestätigen, ohne spezifische Details preiszugeben. Die kollaborative prädiktive Modellierung wird durch FL erreicht, wobei ML-Modelle auf verschlüsselten Wählerdaten trainiert werden, die sicher auf einzelnen Geräten gespeichert sind. Dadurch wird nicht nur die Vorhersagegenauigkeit erhöht, sondern auch die Privatsphäre während des gesamten Prozesses gewahrt.

Die Integrität der Wahlergebnisse wird durch den Einsatz von SMPC bei der Berechnung der Ergebnisse sichergestellt. Wahlhelfer und unabhängige Prüfer analysieren gemeinsam die Wahldaten, ohne sensible Informationen direkt auszutauschen, wodurch die Vertraulichkeit der einzelnen Stimmen gewahrt bleibt. Die Wähler behalten die Kontrolle über ihr Wahlverhalten und ihre Präferenzen durch die PDS, auf die die Wahlkommission nur mit ausdrücklicher Zustimmung der Wähler über DIDs und VCs zugreifen kann, wodurch die Datenexposition minimiert wird und die Nutzer in die Lage versetzt werden, ihre Informationen sicher zu verwalten (Abbildung 8).

Eine transparente und fälschungssichere Speicherung wird durch BBDS erreicht, bei der die Wahlergebnisse und Wahlprotokolle sicher auf einer genehmigten Blockchain gespeichert werden. Dies gewährleistet die Integrität des Wahlprozesses und beschränkt den Zugang auf autorisierte Stellen. Zusätzlich,

Citation: Blockchain im Gesundheitswesen heute 2024, **7**: 302 - https://doi.org/10.30953/bhty.v7.302

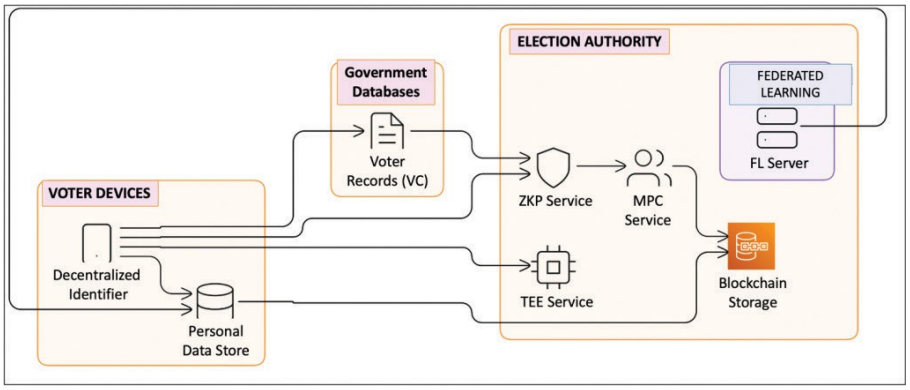

Abb. 8. Beispiel für ein Wahlszenario. FL: föderiertes Lernen; TEE: vertrauenswürdige Ausführungsumgebung; ZKP: Zero-Knowledge-Proofs.

TEEs tragen zu einer zusätzlichen Sicherheitsebene bei, indem sie sensible Berechnungen, wie Betrugserkennung und Ergebnisüberprüfung, innerhalb vertrauenswürdiger Enklaven auf den Geräten der Wähler isolieren.

Dieses umfassende Beispiel zeigt, wie Web 3.0-Prinzipien reale Anwendungen revolutionieren. Es bietet ein sicheres, transparentes und datenschutzfreundliches Wahlerlebnis, bei dem der Einzelne während des gesamten Wahlvorgangs die Kontrolle über seine Identität und persönlichen Daten behält.

Vergleichende und kritische Analyse

Wie bereits erwähnt, weichen meine Cybersicherheitslösungen und mein Ansatz erheblich von den gängigen Praktiken auf diesem Gebiet ab. Folglich stellt ein direkter Vergleich mit bestehenden Methoden eine besondere Herausforderung dar. Das Konzept der Deleakifizierung erweist sich als umstritten und potenziell gefährlich, da es sowohl Vor- als auch Nachteile aufweist.

Ein gut konzipierter Virus, der integraler Bestandteil des Deleakifizierungskonzepts ist, birgt das Potenzial, zielgerichtete Daten effizient zu scannen und zu entfernen und damit manuelle oder herkömmliche Methoden zu übertreffen - besonders vorteilhaft bei umfangreichen Datensätzen. Dieser Vorteil ist vor allem in zeitkritischen Situationen von entscheidender Bedeutung, in denen die rasche Beseitigung von Datenlecks von größter Wichtigkeit ist.

Ein zusätzlicher Vorteil liegt in der Fähigkeit des Virus, auf Daten zuzugreifen und sie von infizierten Systemen zu entfernen, die mit herkömmlichen Mitteln nur schwer zu erreichen sind, wie z. B. Offline-Geräte oder versteckte Speicherorte. Obwohl dies in bestimmten Szenarien von Vorteil ist, ergeben sich naturgemäß Bedenken hinsichtlich unbeabsichtigter Folgen und möglicher Verletzungen der Privatsphäre.

Die Vision eines sich selbst replizierenden Virus im Rahmen dieses Konzepts eröffnet die Aussicht auf eine Automatisierung des Datenentfernungsprozesses, wodurch die Abhängigkeit von menschlichen Eingriffen verringert und das Risiko menschlicher Fehler potenziell minimiert wird. Diese Automatisierung wirft jedoch berechtigte Bedenken hinsichtlich der Kontrollierbarkeit und der Möglichkeit einer unbeabsichtigten Verbreitung oder Schädigung auf.

Es muss unbedingt anerkannt werden, dass die praktische Umsetzung eines solchen Virus mit erheblichen Herausforderungen verbunden wäre. Es ist eine schwierige Aufgabe, die durchgesickerten Daten zielgenau zu entfernen, ohne legitime Online-Inhalte zu beeinträchtigen. Angesichts der schnellen und unkontrollierbaren Verbreitung von Viren besteht ein erhebliches Risiko, dass auch Daten betroffen sind, die in keinem Zusammenhang mit dem Virus stehen, was zu Kollateralschäden führen kann. Erschwerend kommt hinzu, dass die durchgesickerten Daten oft in fragmentierter Form auf verschiedenen Websites und Plattformen vorliegen. Der Virus würde ein außergewöhnlich ausgeklügeltes Design erfordern, um alle Instanzen der durchgesickerten Informationen zu lokalisieren und zu entfernen. zu finden und zu entfernen, was in den meisten Fällen ein Ding der Unmöglichkeit ist. Hinzu kommt, dass die Technologie, die einem solchen Virus zugrunde liegt, obwohl sie für ethische Zwecke im Rahmen der Enttarnung entwickelt wurden, für böswillige Zwecke missbraucht werden könnten. Dies stellt einen besorgniserregenden Präzedenzfall für potenzielle künftige Cyberangriffe dar und unterstreicht die erheblichen ethischen und sicherheitstechnischen Bedenken.

Datenschutzlösungen im Web 3.0 bringen einen Paradigmenwechsel in der Art und Weise mit sich, wie Einzelpersonen ihre Identitäten verwalten, und dabei spielen DIDs eine entscheidende Rolle. Indem sie es dem Einzelnen ermöglichen, seine Identität selbst zu besitzen und zu verwalten, verringern DIDs den Einfluss zentraler Behörden und minimieren so die Anfälligkeit von Daten. Die Komplexität der Verwaltung von DIDs und VCs könnte jedoch einer breiten Akzeptanz entgegenstehen, insbesondere bei technisch nicht versierten Nutzern. Um eine nahtlose Zusammenarbeit über verschiedene Plattformen hinweg zu gewährleisten, ist eine kontinuierliche Verbesserung der Standards und der Interoperabilität unabdingbar.

Die VCs bieten eine sichere Möglichkeit, spezifische Datenattribute auszutauschen und so die Risiken von Datenmanipulation und Identitätsdiebstahl zu verringern. Die Integration von VCs in verschiedenen Sektoren erfordert jedoch eine breite Akzeptanz und einheitliche Formate, um eine nahtlose Überprüfung und Nutzung zu ermöglichen. Die ethische Umsetzung ist entscheidend, um die potenziell diskriminierende Verwendung von VCs zu verhindern.

Die ZKPs bieten eine innovative Lösung, indem sie den Besitz von Informationen nachweisen, ohne Details preiszugeben, wodurch die Datenexposition verringert wird. Die Implementierung und das Verständnis von

ZKPs stellen jedoch sowohl für Entwickler als auch für Nutzer eine Herausforderung dar und erfordern technisches Fachwissen. Die Rechenkosten komplexer ZKPs könnten sich auf die Verarbeitungsressourcen auswirken, was eine sorgfältige Abwägung bei der Integration erforderlich macht.

Der FL minimiert die gemeinsame Nutzung von Daten, indem er Modelle auf lokalen Geräten trainiert und so den Datenschutz verbessert. Die Zusammenführung und Verwaltung dezentraler Daten kann jedoch zu langsameren Prozessen führen. Robuste Sicherheitsprotokolle sind unerlässlich, um die Datensicherheit über verschiedene Geräte und Netze hinweg zu gewährleisten, und gut konzipierte Anreize sind entscheidend, um die Beteiligung der Nutzer zu fördern.

Der SMPC ermöglicht die gemeinsame Datenanalyse ohne Offenlegung der individuellen Beiträge und fördert so die sichere Zusammenarbeit. Der Rechenaufwand für komplexe Protokolle und die Herausforderungen bei der Skalierung für große Datenmengen erfordern jedoch leistungsfähige Hardware. Eine effektive Implementierung erfordert spezielles technisches Wissen und Fachkenntnisse.

Die PDS ermöglichen es dem Einzelnen, seine Daten zu besitzen und zu verwalten, was die Anfälligkeit für zentralisierte Verstöße verringert. Allerdings sind einheitliche Datenformate und Zugriffsprotokolle für eine nahtlose gemeinsame Nutzung unerlässlich. Robuste Sicherungs- und Wiederherstellungsmechanismen sind unerlässlich, um Datenverluste zu vermeiden, und die Schulung der Benutzer ist der Schlüssel für eine breite Akzeptanz.

Das BBDS gewährleistet die Unveränderlichkeit und Transparenz der Daten, aber es gibt Herausforderungen bei der Skalierung für große Mengen und Umweltprobleme mit einigen Konsensmechanismen. Techniken zur Wahrung der Privatsphäre sind entscheidend, um die Vorteile der Transparenz mit der Privatsphäre der Nutzer in Einklang zu bringen.

Die TEEs bieten sichere Enklaven für sensible Berechnungen und erhöhen so die Datensicherheit. Die begrenzte Verfügbarkeit auf allen Geräten und der potenzielle Ausführungsaufwand müssen jedoch berücksichtigt werden. Kontinuierliche Forschung ist unerlässlich, um potenzielle Schwachstellen zu beseitigen und robuste Sicherheit zu gewährleisten.

Insgesamt bietet das Konzept der Deleakifizierung und der Datenschutzlösungen des Web 3.0 ein großes Potenzial, dem Einzelnen mehr Kontrolle über seine Daten zu geben und die Privatsphäre in der digitalen Welt zu schützen. Jede Technologie bringt jedoch eine Reihe von Vor- und Nachteilen mit sich, und ihre erfolgreiche Umsetzung erfordert eine sorgfältige Abwägung dieser Faktoren sowie die Zusammenarbeit verschiedener Interessengruppen, um die bestehenden Herausforderungen zu bewältigen und eine ethische und verantwortungsvolle Entwicklung zu gewährleisten.

Schlussfolgerung und zukünftige Möglichkeiten

Die derzeitige Landschaft der Unleakification- und Web3-Datenschutzmodelle stößt auf Grenzen, da sich diese Technologien noch in einem frühen Stadium befinden. Dieses Anfangsstadium bietet jedoch die Möglichkeit, sie zu verbessern, um sie praktikabler, benutzerfreundlicher und breiter einsetzbar zu machen und damit letztlich ihre Stabilität zu erhöhen. Herausforderungen wie technische Komplexität, Nutzerakzeptanz und Skalierbarkeit müssen angegangen werden, aber die Möglichkeiten, die sich durch Dezentralisierung und Daten im Besitz der Nutzer ergeben, versprechen eine sichere und nutzerorientierte Zukunft.

Im Bereich der KI und der Cybersicherheit sind die größeren Angriffsflächen, die sich aus der Integration von KI ergeben, besorgniserregend. Rahmenwerke und Vorschriften wie ISO 42001 und europäische KI-Gesetze sind Schritte in die richtige Richtung für eine verantwortungsvolle Entwicklung und robuste Sicherheit. Auch wenn neue Lösungen wie die Quantenkryptografie vielversprechend sind, ist die Wachsamkeit gegenüber potenziellen Bedrohungen, insbesondere durch künstliche Intelligenz (AGI), von entscheidender Bedeutung. Neben technischen Erwägungen ist die Auseinandersetzung mit den sozialen und ethischen Auswirkungen der KI und des Datenschutzes von entscheidender Bedeutung. Offene Diskussionen über Dateneigentum, algorithmische Verzerrungen und KI-gesteuerte Manipulationen sind für eine verantwortungsvolle Entwicklung notwendig. Die Betonung der Zusammenarbeit zwischen Mensch und KI und die Sichtweise, dass KI eher ein Werkzeug zur Befähigung als ein Ersatz ist, kann zu einer ethischen und nützlichen Entwicklung beitragen. Die fortschreitende KI-Revolution bringt sowohl Fortschritte als auch Herausforderungen mit sich. Die weit verbreitete Implementierung von KI in verschiedenen Sektoren vergrößert die Angriffsfläche und stellt Cybersecurity-Experten vor Herausforderungen, die sie meistern müssen. Trotz bestehender Rahmenwerke gibt es noch viel zu schützen. Die Rechenleistung der KI könnte derzeit sichere Technologien überflüssig machen. Während neue Lösungen wie die Quantenkryptografie vielversprechend sind, unterstreichen die potenziellen Bedrohungen durch künstliche Intelligenz die Notwendigkeit vorsichtiger Forschung, robuster Sicherheitsmaßnahmen und ethischer Überlegungen.[41] Fortgesetzte Forschung, Zusammenarbeit und sorgfältige Abwägung der Herausforderungen und ethischen Implikationen können dazu beitragen, das Potenzial dieser Technologien für eine sichere, gerechte und bereichernde Zukunft zu nutzen.

Finanzierung

Für die Erstellung dieses Artikels wurden keine Mittel bereitgestellt.

Finanzielle und nicht-finanzielle Beziehungen und Aktivitäten

Keine von den Autoren angegeben.

Mitwirkende

Alle Autoren dieser Forschungsarbeit haben direkt an der Planung, Durchführung oder Analyse dieser Studie mitgewirkt. Alle Autoren dieser Arbeit haben die eingereichte Endfassung gelesen und genehmigt.

Erklärung zur Datenverfügbarkeit (Das), gemeinsame Nutzung von Daten, Reproduzierbarkeit und Datenrepositorien

Die Originaldaten wurden bei der Erstellung des Artikels nicht verwendet.

Anwendung von KI-generiertem Text oder verwandter Technologie

KI und verwandte Technologien wurden bei der Erstellung dieses Artikels nicht verwendet.

Citation: Blockchain im Gesundheitswesen heute 2024, **7**: 302 - https://doi.org/10.30953/bhty.v7.302

Danksagungen

Keine.

Referenzen

1. Enigma. Bletchley Park. [zitiert 2024 Jan 13]. Verfügbar unter: https://bletchleypark.org.uk/our-story/enigma/
2. Zeitleiste der Computerviren und Würmer. Wikipedia; 2024 [zitiert 2024 Jan 13]. Verfügbar unter: https://en.wikipedia.org/w/index.php?title=Zeitleiste_von_Computerviren_und_Würmern&oldid=1194773804
3. cybercrimemag. Globale Ausgaben für Cybersicherheit werden von 2017 bis 2021 voraussichtlich 1 Billion Dollar übersteigen. Cybercrime Magazine. 2024 [zitiert 2024 Jan 13]. Verfügbar unter: https://cybersecurityven-tures.com/cybersecurity-market-report/
4. Die größten Bedrohungen für die Cybersicherheit im Jahr 2023. Cisco. [zitiert 2024 Jan 13]. Verfügbar unter: https://www.cisco.com/c/en/us/products/secu-rity/top-cybersecurity-threats-2023.html
5. M. C. D. O. C. (CDOC) Intelligence Microsoft Threat. Tiefes Eintauchen in die Solorigate-Aktivierung der zweiten Stufe: von SUNBURST zu TEARDROP und raindrop. Microsoft Security Blog. [zitiert 2024 Jan 15]. Verfügbar unter: https://www.microsoft.com/en-us/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/
6. Was ist das Mirai-Botnetz? Cloudflare. [zitiert 2024 Jan 12]. Abrufbar unter: https://www.cloudflare.com/learning/ddos/glossary/ mirai-botnet/
7. Der OPM-Hack erklärt: Schlechte Sicherheitspraktiken treffen auf Chinas Captain America. CSO Online. [zitiert 2024 Jan 12]. Verfügbar unter: https://www.csoonline.com/article/566509/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america. html
8. Was ist der WannaCry-Ransomware-Angriff? | UpGuard. [zitiert am 2024 Jan 12]. Verfügbar unter: https://www.upguard.com/blog/wannacry
9. Colonial Pipeline Ransomware-Angriff. Wikipedia; 2023 [zitiert 2024 Jan 12]. Verfügbar unter: https://en.wikipedia.org/w/index.php?title=Colonial_Pipeline_ransomware_attack&oldid=1189897140
10. Times F. Ein Anruf beim Helpdesk war wahrscheinlich alles, was nötig war, um MGM zu hacken. Ars Technica. [zitiert 2024 Jan 12]. Verfügbar unter: https://arstechnica.com/security/2023/09/a-phone-call-to-help-desk-was-likely-all-it-took-to-hack-mgm/
11. Helmus TC. Künstliche Intelligenz, Deepfakes und Desinfor-mation: eine Fibel. RAND Corporation; 2022 [zitiert 2024 Jan 12]. Abrufbar unter: https://www.rand.org/pubs/perspectives/ PEA1043-1.html
12. Rashmika Mandanna deepfake Fall: Delhi Polizei 4 Verdächtige aufgespürt, Jagd auf Hauptverschwörer läuft. Hindustan Times. [zitiert 2024 Jan 12]. Verfügbar unter: https://www.hindustantimes.com/india-news/rashmika-mandanna-deepfake-case-delhi-police-track-down-4-suspects-hunt-for-key-conspirator-on-101703043714888.html
13. 2019 Capital One Cybervorfall | Was geschah. Capital One. [zitiert 2024 Jan 12]. Verfügbar unter: https://www.capitalone.com/ digital/facts2019/
14. Marriott Data Breach FAQ: Was ist wirklich passiert? Hotel Tech Report. [zitiert 2024 Jan 12]. Verfügbar unter: https://hoteltechre-port.com/news/marriott-data-breach
15. Seite C. Tesla sagt, dass die Datenpanne, von der 75.000 Mitarbeiter betroffen waren, ein Insiderjob war. TechCrunch. [zitiert 2024 Jan 12]. Verfügbar unter: h t t p s : / / techcrunch.com/2023/08/21/tesla-breach-employee-insider/
16. Hern A, A. H. U. Technologie-Redakteur. Pentagon-Leck auf Videospiel-Chatgruppen-Nutzer zurückgeführt, die sich über Krieg in der Ukraine streiten. *The Guardian*; 2023 Apr 11 [zitiert 2024 Jan 12]. Verfügbar unter: https://www.theguardian.com/world/2023/apr/11/pentagon-leak-traced-to-video-game-chat-group-users-arguing-over-war-in-ukraine
17. Stuxnet. *Wikipedia*; 2024 Jan 10 [zitiert 2024 Jan 12]. Verfügbar unter: https://en.wikipedia.org/w/index.php?title=Stuxnet&oldid=119468 7512
18. KI in der Cybersicherheit: Verteidigen Sie Ihre digitale Welt. [zitiert 2024 Jan 13]. Verfügbar unter: https://www.veritis.com/blog/ai-in-cybersecurity-defending-against-evolving-threats/
19. Maschinelles Lernen (ML) in der Cybersicherheit: Anwendungsfälle-Crowd-Strike.crowdstrike.com;[zitiert2024Jan15]. Verfügbar unter:https://www.crowdstrike.com/cybersecurity-101/machine-learning-cybersecurity/
20. Chandramouli R, Butcher Z. A zero trust architecture model for access control in cloud-native applications in multi-cloud environments. National Institute of Standards and Technology, NIST Special Publication (SP) 800-207A; 2023.
21. Zhou L. Was ist eine Zero Trust Architektur (ZTA)? | NextLabs Data-CentricSecurity.NextLabs.[cited2024Jan13].Availablefrom: https://www.nextlabs.com/what-is-zero-trust-architecture-zta/
22. NIST: blockchain provides security, traceability for smart man-ufacturing. NIST; 2019 [cited 2024 Jan 13]. Available from: https://www.nist.gov/news-events/news/2019/02/nist-block-chain-provides-security-traceability-smart-manufacturing
23. Innovationseinblick für dezentralisierte Identität und überprüfbare Ansprüche. Gartner. [zitiert 2024 Jan 13]. Verfügbar unter: https://www.gartner.com/en/documents/4004851
24. Was ist Täuschungstechnologie? Bedeutung und Vorteile| Zscaler. [zitiert 2024 Jan 13]. Verfügbar unter: https://www.zscaler.com/resources/security-terms-glossary/what-is-deception-technology
25. Han X, Kheir N, Balzarotti D. Deception techniques in com-puter security: a research perspective. ACM Comput. Surv. 2018;51(4):80:1–36. https://doi.org/10.1145/3214305
26. Home Page| CISA. [cited 2024 Jan 13]. Verfügbar unter: https://.www.cisa.gov/
27. Der Europarat: Hüter der Menschenrechte, der Demokratie und der Rechtsstaatlichkeit für 700 Millionen Bürger - Portal-www.coe.int. Portal. [zitiert 2024 Jan 13]. Verfügbar unter: https://www.coe.int/en/web/portal
28. Was ist verhaltensbiometrische Daten? [zitiert 2024 Jan 13]. Verfügbar unter: https://www.biocatch.com/blog/what-is-behavioral-biometrics
29. Liang Y, Samtani S, Guo B, Yu Z. Behavioral biometrics for continuous authentication in the internet-of-things era: an artificial intelligence perspective. IEEE Internet Things J. 2020;7(9):9128-43. https://doi.org/10.1109/JIOT.2020.3004077
30. Du L, Shang Q, Wang Z, Wang X. Robust image hashing based on multi-view dimension reduction. J Inf Secur Appl. 2023;77:103578. https://doi.org/10.1016/j.jisa.2023.103578
31. Qin C, Liu E, Feng G, Zhang X. Perceptual image hashing for content authentication based on convolutional neural network with multiple constraints. IEEE Trans Circuits Syst Video Technol. 2021;31(11):4523–37. https://doi.org/10.1109/ TCSVT.2020.3047142
32. Uncovering the Hidden WebP vulnerability: a tale of a CVE with muchbiggerimplicationsdhanitoriallyseedallyst. The Cloudflare Blog. [zitiert 2024 Jan 14]. Verfügbar unter: https://blog.cloudflare.com/uncovering-the-hidden-webp-vulnerability-cve-2023-4863
33. Dezentralisierte Identifikatoren (DIDs) v1.0. [zitiert 2024 Jan 14]. Verfügbar unter: https://www.w3.org/TR/did-core/

34. Barker E. Recommendation for key management: part 1-gen-eral. Gaithersburg, MD: National Institute of Standards and Technology; 2020.
35. Fenzi G. Zero knowledge proofs theory and applications. Uni-versity of St. Andrews. September 2019. [zitiert n.d.]. Verfügbar unter: https://info.cs.st-andrews.ac.uk/student-handbook/files/ project-library/cs4796/gf45-Final_Report.pdf
36. Mahlool DH, Abed MH. Eine umfassende Übersicht über föderiertes Lernen: Konzept und Anwendungen. arXiv. 2022. https://doi.org/10.48550/arXiv.2201.09384
37. Merino L-H, Cabrero-Holgueras J. Secure multi-party compu-tation. In: V Mulder, A Mermoud, V Lenders, B Tellenbach, editors. Trends in Datenschutz und Verschlüsselungstechnologien. Cham: Springer Nature Schweiz, 2023; S. 89-92.
38. Arewa O. Data Collection, Privacy, and Children in the Digital Economy. George Mason Legal Studies Research Paper No. LS 23-22, Kapitel in FAMILIEN UND NEUE MEDIEN (Springer Link 2023). 2023. [zitiert n.d.]. Verfügbar unter: https://ssrn.com/ abstract=4617953 oder https://doi.org/10.2139/ssrn.4617953
39. Weltwirtschaftsforum. [zitiert 2024 Jan 14]. Abrufbar unter: https://www.weforum.org/publications/realizing-the-potent ial-of-blockchain/
40. Lee D, Kohlbrenner D, Shinde S, Asanovi K, Song D. Key-stone: an open framework for architecting trusted execution environments. In Proceedings of the fifteenth European con-ference on computer systems, in EuroSys '20. New York, NY: Association for Computing Machinery, 2020; S. 1-16.
41. Kaur R, GabrijelčičD, Klobučar T. Artificial intelligence for cyber-security: literature review and future research directions. Inf Fusion. 2023;97:101804. https://doi.org/10.1016/j.inffus.2023.101804

Citation: Blockchain im Gesundheitswesen heute 2024, **7**: 302 - https://doi.org/10.30953/bhty.v7.302