# MONTHLY SECURITY SUMMARY

AUSGABE APRIL 2023
CHATBOTS UND SECURITY FRAMEWORKS

## RISIKEN MODERNER CHATBOTS

Lösungen wie ChatGPT haben die Wahrnehmung von KI in der breiten Öffentlichkeit revolutioniert. Mit der Nutzung entsprechender Lösungen gehen jedoch Gefahren und Risiken einher, die wir in unserem Beitrag beleuchten werden.

## ERFAHRUNGEN MIT SECURITY FRAMEWORKS

Es gibt verschiedene Security Frameworks, die bei der Umsetzung von Sicherheitsmassnahmen unterstützen können. Wir besprechen die wichtigsten von ihnen.

# April 2023: Ransomware tut weh

In der heutigen digitalen Welt wird Cybersecurity immer wichtiger, da Cyberkriminelle ständig nach neuen Wegen suchen, um Zugang zu sensiblen Informationen zu erlangen. Ein aktuelles Thema, das für Unternehmen und Verbraucher gleichermassen von Bedeutung ist, ist die Bedrohung durch Ransomware-Angriffe.

Ransomware ist eine Art von Malware, die den Zugriff auf den Computer oder die Daten des Opfers sperrt und dann Lösegeld für die Freigabe verlangt. Die Angriffe haben in den letzten Jahren stark zugenommen und die Kosten für Unternehmen und Verbraucher können enorm sein.

Um sich vor Ransomware-Angriffen zu schützen, sollten Unternehmen und Verbraucher mehrere Massnahmen ergreifen. Eine wichtige Massnahme ist die regelmässige Sicherung von Daten auf einem externen Speichergerät oder in der Cloud. Auf diese Weise können wichtige Daten im Falle eines Angriffs wiederhergestellt werden, ohne dass das Lösegeld gezahlt werden muss.

Weitere wichtige Massnahmen sind die Verwendung von Antivirus- und Antimalware-Software sowie die Durchführung regelmässiger Software-Updates, um Schwachstellen zu schliessen. Auch die Schulung von Mitarbeitern und die Sensibilisierung für die Risiken von Phishing-Angriffen und anderen Bedrohungen ist entscheidend.

Es ist wichtig, sich proaktiv zu schützen, indem man die oben genannten Massnahmen ergreift und sich bewusst macht, wie man Ransomware-Angriffe erkennt und darauf reagiert. Nur so können wir uns gegen diese Bedrohung verteidigen und unsere Daten und Systeme sicher halten.

Marc Ruef
Head of Research

NEWS

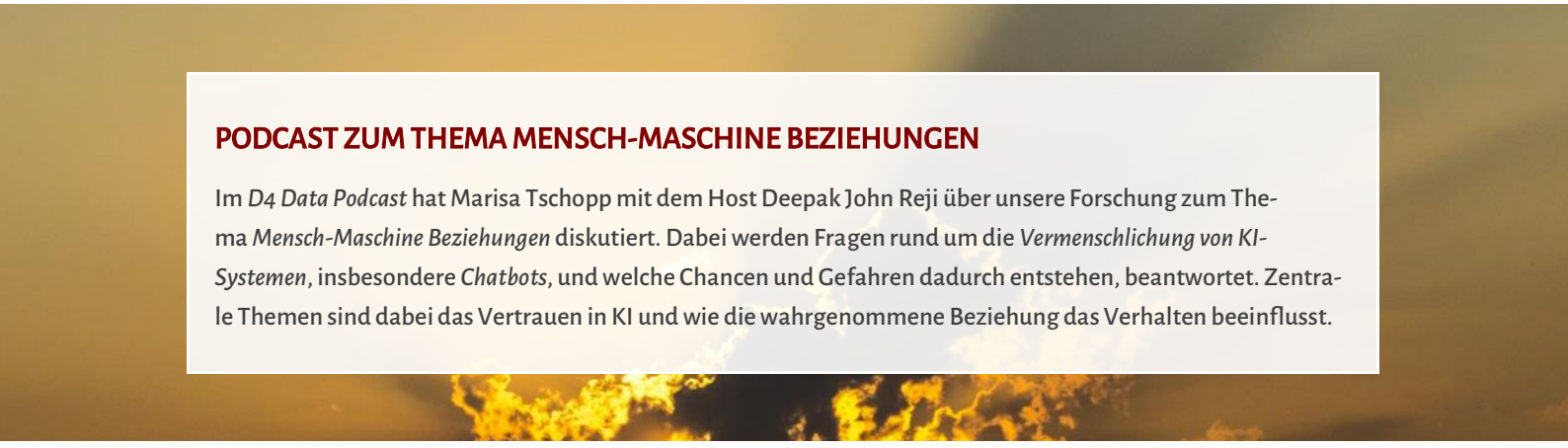
# WAS IST BEI UNS PASSIERT?

## INTERVIEW ZU RANSOMWARE-ANGRIFF GEGEN NZZ

Das Medienunternehmen *NZZ* (Neue Zürcher Zeitung) ist seit zwei Wochen von einer *Ransomware-Attacke* betroffen. Diese hat die Geschäftsabläufe massgeblich beeinflusst, so dass die letzten Tage sogar Teile der Produktion und Verfügbarkeit von Inhalten heruntergefahren werden musste. In einem Interview mit dem Journalisten Pascal Lago für *Echo der Zeit* von *SRF* äussert sich Marc Ruef zum Thema.

## PUBLIKATION ZUM UMGANG VON KINDERN MIT ROBOTERN IN INTERACTION STUDIES

Der Artikel *Exploring space for robot mistakes in child robot interactions*, bei dem Marisa Tschopp als Co-Autorin mitgewirkt hat, steht im Journal *Interaction Studies* (Social Behaviour and Communication in Biological and Artificial Systems) zur Verfügung. Die experimentellen Studie untersucht die Frage, wie Kinder in einer Lernaufgabe mit einem Roboter auf fehlerhaftes Verhalten des Roboters reagieren.



## PODCAST ZUM THEMA MENSCH-MASCHINE BEZIEHUNGEN

Im *D4 Data Podcast* hat Marisa Tschopp mit dem Host Deepak John Reji über unsere Forschung zum Thema *Mensch-Maschine Beziehungen* diskutiert. Dabei werden Fragen rund um die *Vermenschlichung von KI-Systemen*, insbesondere *Chatbots*, und welche Chancen und Gefahren dadurch entstehen, beantwortet. Zentrale Themen sind dabei das Vertrauen in KI und wie die wahrgenommene Beziehung das Verhalten beeinflusst.

Weitere News zu unserem Unternehmen finden Sie auf unserer Webseite.

SCIP BUCHREIHE

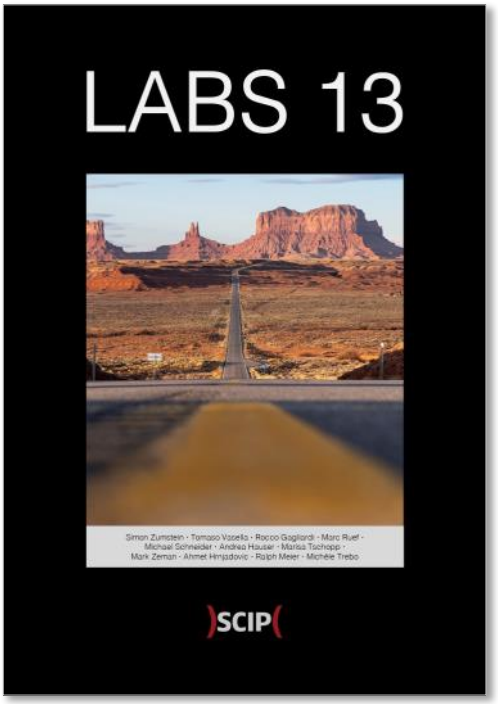
# UNSER AKTUELLES JAHRBUCH

Erneut veröffentlichen wir die aktuelle Ausgabe unseres Jahrbuchs. Bereits zum 13ten Mal fassen wir in diesem die Fachbeiträge von einem Jahr Forschung im Bereich Cybersecurity zusammen.

Das Buch ist wiederum sowohl in deutscher (ISBN 978-3-907109-30-4) als auch in englischer Sprache (ISBN 978-3-907109-31-1) verfügbar. Das Vorwort wurde von Dr. iur. David Vasella verfasst und setzt sich mit den rechtlichen Rahmenbedingungen der Informationssicherheit auseinander.

In unserem Katalog finden sich ebenfalls themenspezifische Bücher zu Künstlicher Intelligenz (ISBN 978-3-907109-14-4) und Sicherheit in der Hotellerie (978-3-907109-16-8).

Weitere Informationen auf unserer Webseite.




Bildquelle: https://pixabay.com/images/id-7885675/

MARC RUEF

# GEFAHREN UND RISIKEN VON MODERNEN CHATBOTS

Wahrscheinlich keine andere technische Entwicklung hatte in den letzten Jahren so eine gesellschaftliche Diskussion entfacht, wie ChatGPT. Der Chatbot vermag mit einem sehr hohen Sprachverständnis und einer weitreichenden Wissensdatenbank zu überzeugen. Es ist absehbar, dass durch solche Systeme viele Berufszweige in Bedrängnis geraten werden. Doch durch derartige Lösungen werden zusätzliche Risiken für Betreiber und Benutzer eingeführt. Dieser Beitrag zeigt auf, welche Gefahren es zu beachten gilt und wie diesen entgegnet werden kann.

ChatGPT basiert auf GPT, das mit grossen Datenmengen trainiert wird, um Sprachkompetenz zu erwerben. Die Fähigkeit, menschenähnliche Antworten zu geben, beruht auf dem Einsatz von Deep Learning, die es ermöglichen, Sprache und Bedeutung von Sätzen einzuordnen. Anschliessend wird maschinelles Lernen verwendet, um eine passende Antwort zu generieren, die auf den Daten und Informationen basiert, die während des Trainingsprozesses gesammelt wurden. Das System kann also nicht im menschlichen Sinne verstehen oder denken, sondern nähert sich an Texte an, die es einmal gelernt hat. Aus diesem Grund können Antworten je nach Komplexität der Frage und Verfügbarkeit von relevanten Informationen variieren.

## VERLETZUNG VON GEHEIMHALTUNG UND PRIVATSPHÄRE

Chatbots interagieren mit Menschen. Im Dialog kann es gegeben sein, dass der Benutzer sensitive und sensible Daten preisgibt. Zum Beispiel, wenn eine KI-gestützte Offerte erstellt werden soll und zu diesem Zweck kundenspezifische Details eingegeben werden. Diese Daten werden für den KI-Betreiber zugänglich und könnten missbraucht werden.

Selbstlernende Systeme können diese Eingaben aber auch für weitere Verarbeitungen nutzen. Wenn also Benutzer A Details zu einem Kunden X eingibt, könnte Benutzer B bei einer ähnlichen Anfrage eben diese Details als Antwort erhalten.

Der mögliche Missbrauch reicht von Urheberrechtsverletzungen über Social Engineering-Angriffe bis hin Identitätsdiebstahl und Erpressungen. Aus diesem Grund ist es empfohlen, sehr vorsichtig mit sen-

siblen Anfragen umzugehen. Auf persönliche, sensible und kundenspezifische Angaben sollte weitestgehend verzichtet werden. Firmen sollten Richtlinien erlassen, wie mit solchen Systemen umgegangen werden darf. Dabei kann sich an den Vorgaben orientiert werden, die zum Beispiel schon bezüglich Online-Übersetzungsdienste erlassen wurden.

## FEHLERHAFTES ANTWORTVERHALTEN

Moderne Chatbots werden anhand bestehender Datensätze trainiert. So können sie sich das entsprechende Wissen aneignen und auf Fragen kohärent reagieren – oder zumindest so tun, als ob sie sich ihrer Antworten sicher sind. Die Qualität und Quantität des Ursprungsmaterials ist massgeblich dafür verantwortlich, wie die Qualität der Reaktionen aussehen kann. Fehlerhaftes oder manipuliertes Material kann zu unliebsamen Effekten führen. Zum Beispiel können Unwahrheiten verbreitet werden und so das Konzept von Fake News befeuern.

Eine langfristige Gefahr, die stetig wachsen wird, ist durch Feedback-Loops gegeben. Was passiert, wenn Chatbots auf Daten trainiert werden, die durch Chatbots generiert wurden? Fehlerhafte Daten werden so verstärkt und werden durch Systeme als absolute Wahrheiten etabliert.

Die durch Chatbots generierte Antworten sind deshalb immer auf ihre inhaltliche Richtigkeit hin zu prüfen. Dabei spielt es keine Rolle, ob eine Kurzbiogarphie, eine Zusammenfassung einer Newsmeldung oder einer Grobofferte erstellt wurde. Eine Plausibilitisierung dieser Art setzt natürlich voraus, dass der Benutzer des Systems die Inhalte verstehen und einordnen kann. Das Generieren von Resultaten ist jeweils einfach. Das Einordnen und Gewährleisten der Qualität setzt hingegen ein weitreichendes Verständnis voraus.

Ein Chatbot-Anbieter sollte eine unkomplizierte Möglichkeit zur Verfügung stellen, fehlerhafte Dialoge als solche markieren und Änderungsvorschläge einreichen zu können. Durch die rege Mitarbeit der Nutzer kann so die Qualität der Lösung erhöht werden.

## VERSTÄRKEN VON PROBLEMATISCHEN NARRATIVEN

Beim Training von Chatbots wird durch die Betreiber der Datensatz definiert und mit ihm die Gewichtung der einzelnen Aussagen. Dies ist unweigerlich mit einer gewissen tendenziösen Subjektivität verknüpft. Durch diese kann es gegeben sein, dass gewisse Narrative sehr ausgrepägt zur Geltung kommen, andere hingegen marginalisiert werden. Problematische, beleidigende und diskriminierende Effekte können verstärkt werden.

Beim Trainieren von Chatbots muss auf die Qualität des Datensatzes Wert gelegt werden. Die Gewichtung einzelner Aussagen muss sorgfältig ausarbeitet werden, wobei gewisse Tendenzen markiert oder rigoros verhindert werden müssen. Ungefilterte frauenfeindliche und rassistische Aussagen sowie das Verbreiten von skurrilen Verschwörungstheorien können keinen Nutzen mitbringen.

Auch hier sollten Anbieter entsprechende Funktionen bereitstellen, um problematische Inhalte unkompliziert melden zu können. In einem Moderationsverfahren sollten diese dann geprüft, angepasst oder verhindert werden.

Grosse Hersteller wie Microsoft und Google sind durch ChatGPT unter Druck gekommen und wollen den lohnenswerten Markt nicht ohne Kampf dem Mitbewerber überlassen. Dabei ist zu beobachten, dass man durch das partielle Reduzieren oder gänzliche Abschaffen der Ethik-Teams einen Vorteil erlangen will. Dies mag auf kommerzieller Ebene kurzfristig der Fall sein. Langfristig wird sich diese Entscheidung jedoch rächen. Denn mit jeder problematischen Aussage verliert ein System an Vertrauen und Akzeptanz. Diese lässt sich nicht ohne weiteres zurückgewinnen wie Forschung aus dem Bereich Mensch-Maschine Vertrauen und Vertrauensherstellung gezeigt hat.

## VERBREITUNG VON MALWARE

Die Manipulation oder Kompromittierung eines Chatbots kann dazu führen, dass er Malware verbreitet. Dies kann, wie bei anderen Anwendungen auch, über Schwachstellen wie Cross Site Scripting oder SQL-Incjetion geschehen. Ein derartiger Angriff kann

aber auch auf den Datenbestand stattfinden. Falls zum Beispiel ein Chatbot für das Genieren von Programmcode genutzt wird, könnte eine Manipulation dazu führen, dass bösartiger Code eingeschleust und in harmlos erscheinenden Dialogen ausgegeben werden kann.

Antworten von Chatbots müssen daher immer kontrolliert werden. Die Inhaltskontrolle ist auch bei Codebeispielen sorgfältig umzusetzen, um Sicherheitslücken in generiertem Code oder bösartige Codeteile nicht in produktiven Umgebungen auszuführen.

## FEHLENDE TRANSPARENZ

Nicht selten kommt es vor, dass ein Chatbot mit einer Antwort aufwarten kann, die verblüffend sinnvoll daherkommt. Manchmal ist aber auch das Gegenteil der Fall. Wie dem auch sei, kann sich durch Nutzer das Bedürfnis manifestieren zu verstehen, wieso nun genau diese konkrete Antwort ausgewählt wurde. Doch die meisten Systeme lassen eine Transparenz dieser Art vermissen. Stattdessen liegt es an einem selbst, einen Dialog richtig einzuordnen und zu akzeptieren. Diese fehlende Möglichkeit von Einsichten kann zu einer gewissen Hörigkeit führen. Vor allem dann, wenn über Themen diskutiert wird, deren Inhalte und Tragweite durch Nutzer nicht oder nur eingeschränkt abgeschätzt werden können.

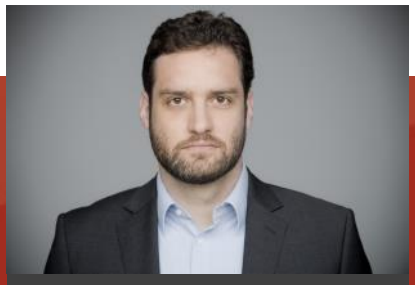
Es muss als erklärtes Ziel für Entwickler von KI-Lösungen gelten, dass ihre Produkte mit einem sogenannten Verbose-Modus daherkommen. Der Nutzer muss immer die Möglichkeit haben, eine Erklärung für ein Resultat zu verlangen. Bei Chatbots besteht eine simple Lösung darin, dass der Nutzer eine Warum-Frage stellen kann: Warum hast Du diese Antwort gegeben? Es liegt dann am Chatbot die Herleitung für das Resultat aufzuzeigen, um der eigenen Vorgehensweise ein gewisses Mass an Vertrauen mitgeben zu können. Bisher sind wir leider weiter davon entfernt, dass gegenwärtige Lösungen Mechanismen dieser Art anbieten können.

## FAZIT

Wie bei jeder Technologie gibt es Risiken im Zusammenhang mit ihrer Anwendung. Es ist daher entscheidend, dass Entwickler und Nutzer sich dieser Risiken bewusst sind und angemessene Massnahmen anstreben, um die Sicherheit und den Schutz der Chatbots geteilten Daten und Informationen zu gewährleisten.

Insgesamt bieten KI-basierte Chatbots in der Masse nun aufregende Möglichkeiten für die Mensch-Maschine-Interaktion. Aber es bleibt wichtig, mit skeptischem Optimismus heranzugehen und die Sicherheit des Systems und seiner Benutzer zu priorisieren.

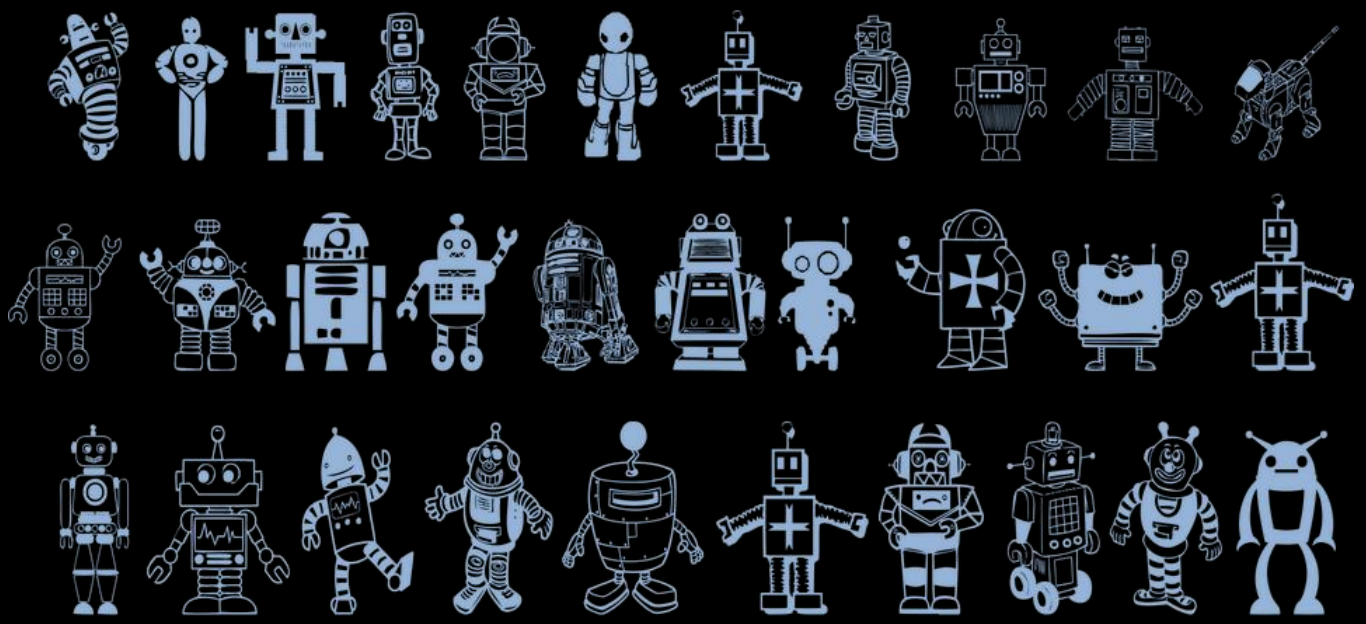
Um Risiken zu minimieren, ist es wichtig, bewährte Verfahren in der Cybersicherheit zu befolgen. Es ist deshalb von entscheidender Bedeutung, Transparenz und Rechenschaftspflicht bei der Entwicklung und Bereitstellung von Chatbots zu wahren, einerseits in Bezug auf ethische Aspekte. Dabei müssen die gesetzlichen Verpflichtungen in Bezug auf den AI Act der EU beachtet werden. Die Regulierung von KI-Systemen in der EU (betrifft auch alle, die mit der EU Handel treiben wollen) kann unter Umständen eine generelles Verbot von textgenerierenden Systemen bewirken oder es werden sehr hohe Anforderungen an Betreiber gestellt, welche teils auch aus finanziellen Gründen schwer zu erfüllen sein werden.



Marc Ruef

know your vulnerabilities

# VulDB



## Automatisieren Sie Ihr Vulnerability Management

Tägliche Dokumentation neuer Schwachstellen, detaillierte Analyse der technischen Hintergründe, exklusive Details zu Exploiting und Gegenmassnahmen. Mit **vuldb.com** erhalten Sie ein durchschlagskräftiges Werkzeug, um den Bedrohungen im Cyberspace entgegnen zu können.

)SCIP(
official data provider

> https://vuldb.com

ROCCO GAGLIARDI

# UNSERE ERFAHRUNGEN MIT SECURITY FRAMEWORKS

Cybersecurity-Frameworks bestehen aus sicherheitsfördernden Regeln, Praktiken und Vorgehensweisen. Diese Frameworks unterstützen Cybersecurity-Teams bei der Absicherung wichtiger Vermögenswerte durch die Bewertung von Sicherheitsprozessen und die Härtung von Systemen. Die Wahl des Frameworks hängt vom IT-Modell, der Einhaltung von Vorschriften, der Erfahrung mit der Implementierung und den individuellen Vorlieben ab. Es mag zwar verlockend sein, ein Framework zu verwenden, indem man einfach alle Fragen durchgeht, vielleicht mit Hilfe von ChatGTP, aber die Dinge sind etwas komplizierter.

Ein Sicherheits-Framework liefert das Gerüst, auf dem wir die Sicherheit aufbauen können, oder zeigt uns, worauf wir uns bei unserer Bewertung konzentrieren müssen, aber sie erfordern eine Fülle von Kenntnissen und beträchtliche Erfahrung. Wenn im letzten Jahr die Überprüfung der Einhaltung der NIST CSF PR.AC-3 Kenntnisse über verschiedene Technologien erforderte, ist es jetzt mit ChatGPT einfacher (siehe Screenshot).

Oder zumindest scheint es einfacher zu sein. Wenn die von ChatGTP generierte Liste auf den ersten Blick wie ein gültiges Bewertungsmuster aussieht, wird schnell klar, dass es sich um eine Umdeutung mehrerer bereits im CSF vorhandener Punkte handelt, die auf unterschiedliche Weise angeordnet sind. ChatGPT ist ein gültiges Hilfsmittel, aber ein Hilfsmittel. Es ersetzt – vorläufig – keinen Auditor.

## SECURE CONTROL FRAMEWORK

Wir bei der scip AG verwenden seit einem Jahrzehnt das NIST-CSF als Grundlage für die Sicherheitsbewertung, obwohl wir mittlerweile für die meisten unserer Kunden das CIS CSC V8 bevorzugen. Aufgrund der Komplexität und der sich ständig weiterentwickelnden Natur von Cyber-Bedrohungen sowie des Bedarfs an standardisierten Best Practices und Richtlinien, die Unternehmen dabei helfen, diese Risiken effektiv zu verwalten und zu mindern, gibt es jedoch zahlreiche Cybersicherheits-Frameworks.

Neben den Klassikern ISO27k, PCI-DSS und COBIT gibt es weitere Modelle, die auf die Cloud (CSA-CCM), das Gesundheitswesen (HITRUST) und das

NIST CSF PR.AC-3 is a standard that focuses on the technical assessment of systems to ensure they comply with the security requirements of an organization. To comply with this standard as a revisor, you should consider the following technical assessment tasks:

1. Identify and document the hardware, software, and data assets that are part of the organization's system.
2. Identify the vulnerabilities and threats to the system and assess the likelihood and potential impact of each one.
3. Evaluate the effectiveness of the existing security controls, such as access controls, intrusion detection systems, and firewalls.
4. Test the security controls to ensure they are operating as intended and identify any gaps or weaknesses.
5. Review the system configuration and identify any misconfigurations that could lead to security issues.
6. Assess the effectiveness of the organization's incident response plan and procedures for detecting, investigating, and responding to security incidents.
7. Evaluate the effectiveness of the organization's security awareness training program to ensure that all employees understand their roles and responsibilities in maintaining the security of the system.
8. Document the assessment findings and recommend remediation measures to address any identified vulnerabilities or weaknesses.

By completing these technical assessment tasks, you can ensure that the organization's system meets the security requirements of the NIST CSF PR.AC-3 standard.

allgemeine NIST (CSF oder 800-53) ausgerichtet sind, und viele andere, die in fast allen der am häufigsten verwendeten Framework-Rankings zu finden sind.

Das Secure Control Framework (SCF) ist jedoch überraschenderweise in diesen Listen nicht enthalten.

> Hackers share information on attack methods with other hackers, so why shouldn't the good guys share information on how to best protect an organization?

Freiwillige mit unterschiedlichem Hintergrund in der Cybersicherheitsbranche arbeiteten und arbeiten weiterhin zusammen, um Probleme im Zusammenhang mit Datenschutz und Governance, Risiko und Compliance (GRC) zu lösen. Fachleute aus den Bereichen Audit, Technik, Architektur, Reaktion auf Vorfälle, Beratung und anderen verwandten Bereichen. Das Endergebnis sind von Experten abgeleitete Inhalte, aus denen sich das SCF zusammensetzt. Ein riesiger Satz von Kontrollen, der der Öffentlichkeit kostenlos zur Verfügung gestellt wird.

Ich habe mich von der ersten Version an in das SCF verliebt und setze es seit 2019 in unseren Projekten ein. SCF ist komplex: Heute, in der Version 2023.1, gibt es 1168 Steuerelemente in 33 Domänen. Die Kontrollen werden mindestens einmal im Jahr aktualisiert. Aber wenn es 2019 nur eine große Checkliste mit 900 Kontrollen gab, sind heute zusätzliche Definitionen hinzugekommen, die die meisten der Bereiche abdecken, die von anderen Frameworks nicht abgedeckt werden.

So finden wir die Sicherheits- und Datenschutzgrundsätze das Integrierte Kontrollmanagement das Capability Maturity Model das Risk Management Model und die Datenschutzgrundsätze.

Um das SCF zu nutzen, wird auf den 16 Seiten des Integrierten Kontrollmanagements die Herangehensweise skizziert, mit der das Rahmenwerk am besten genutzt werden kann; allerdings ist Erfahrung erforderlich. Hier wollen wir die Stärken des SCF zusammenfassen:

- **Abstimmung mit anderen Standards**: Das SCF ist auf andere Standards und Richtlinien abge-

stimmt, wie z.B. das NIST CSF und die ISO/IEC 27001:2013. Dies erleichtert es Unternehmen, die SCF in ihre bestehenden Sicherheitsprogramme zu integrieren und die Einhaltung verschiedener Vorschriften und Gesetze zu erreichen.

- **Flexibilität**: Das SCF ist so konzipiert, dass es flexibel und anpassungsfähig ist, so dass Unternehmen ihre Sicherheitskontrollen an ihre spezifischen Bedürfnisse und Risikoprofile anpassen können. So können Unternehmen ein maßgeschneidertes Sicherheitsprogramm implementieren, das effektiver und effizienter ist.

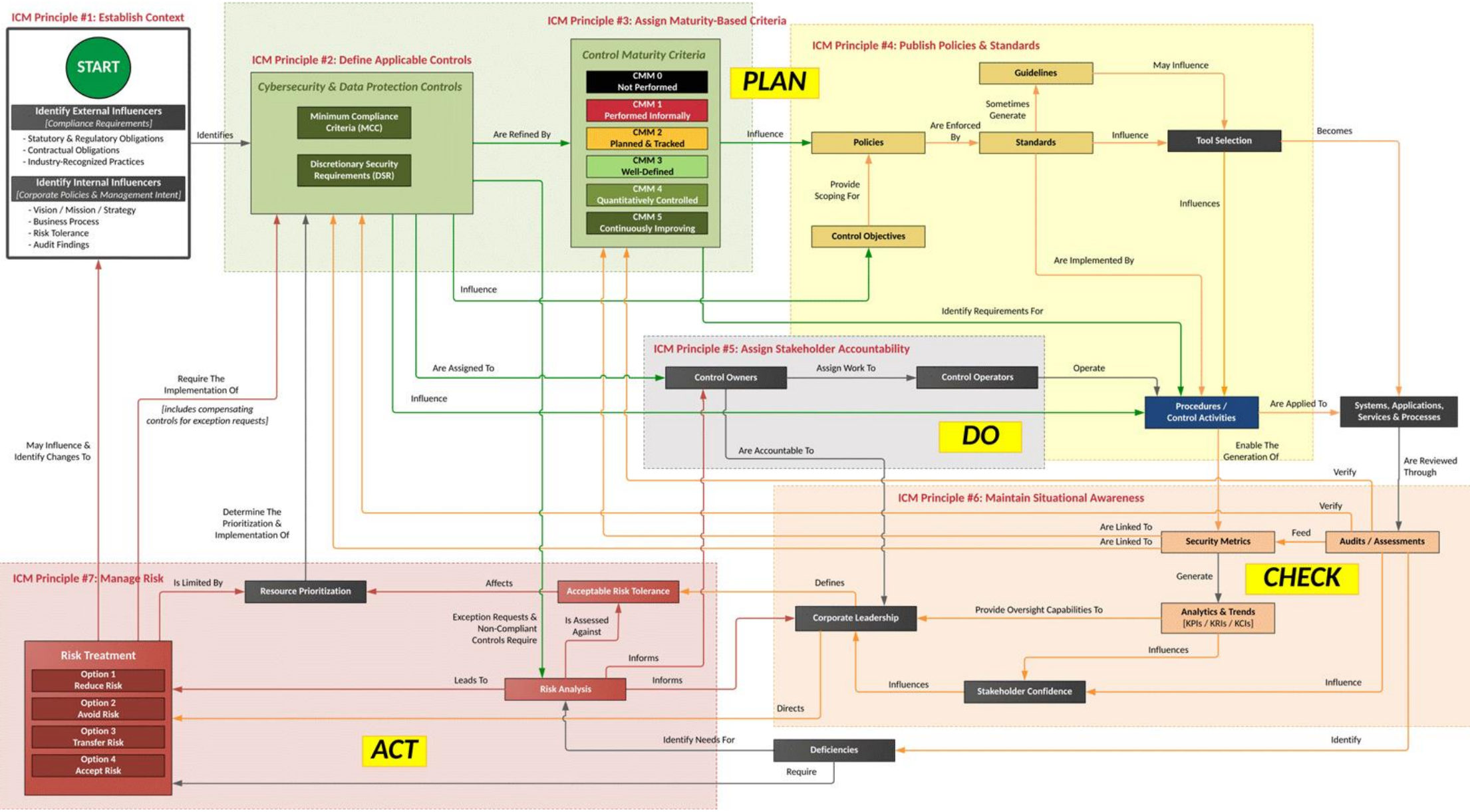
- **Kontinuierliche Verbesserung**: Der SCF ermutigt Unternehmen dazu, ihre Sicherheitslage kontinuierlich zu überwachen und zu verbessern. Dadurch wird sichergestellt, dass die Sicherheitsmaßnahmen im Laufe der Zeit wirksam bleiben und an sich ändernde Bedrohungen und Technologien angepasst werden.

- **Verwendung von Best Practices der Branche**: Der SCF basiert auf bewährten Praktiken der Branche und auf Anleitungen von führenden Sicherheitsorganisationen und -spezialisten aus verschiedenen Bereichen. Dadurch wird sichergestellt, dass der SCF auf dem neuesten Stand ist und die neuesten Überlegungen zur Cybersicherheit einbezieht.

Neben den zahlreichen Bereichen und Kontrollen, die ein breites Spektrum von Cybersicherheitsthemen abdecken, wird vor allem die Fähigkeit, sie zu filtern, geschätzt. Die Zuordnung von Kontrollen zu anderen Standards (insgesamt 198), die nach Ländern, Sektoren oder Fachgebieten geordnet sind, ermöglicht es, schnell zu erkennen, ob eine Organisation diesen spezifischen Standard einhält oder nicht, oder nur eine Teilmenge von besonderem Interesse auszuwählen.

Dasselbe gilt für die Bedrohungs- und Risikozuordnung. Jeder Kontrolle ist zugeordnet, welcher Bedrohung/welchem Risiko sie ausgesetzt ist, wodurch der Risikomanagementprozess effektiver wird.

SCF ist gut strukturiert und kann durch die Einbeziehung von Mappings zu anderen Systemen wie


ICM Principle #1: Establish Context
START
Identify External Influencers
[Compliance Requirements]
- Statutory & Regulatory Obligations
- Contractual Obligations
- Industry-Recognized Practices
Identify Internal Influencers
[Corporate Policies & Management Intent]
- Vision / Mission / Strategy
- Business Process
- Risk Tolerance
- Audit Findings
Identifies
ICM Principle #2: Define Applicable Controls
Cybersecurity & Data Protection Controls
Minimum Compliance Criteria (MCC)
Discretionary Security Requirements (DSR)
Are Refined By
ICM Principle #3: Assign Maturity-Based Criteria
Control Maturity Criteria
CMM 0 Not Performed
CMM 1 Performed Informally
CMM 2 Planned & Tracked
CMM 3 Well-Defined
CMM 4 Quantitatively Controlled
CMM 5 Continuously Improving
PLAN
Influence
ICM Principle #4: Publish Policies & Standards
Guidelines
May Influence
Sometimes Generate
Policies
Are Enforced By
Standards
Influence
Tool Selection
Becomes
Provide Scoping For
Influences
Control Objectives
Are Implemented By
Influence
Identify Requirements For
ICM Principle #5: Assign Stakeholder Accountability
Are Assigned To
Control Owners
Assign Work To
Control Operators
Operate
Require The Implementation Of
[includes compensating controls for exception requests]
Influence
Procedures / Control Activities
Are Applied To
Systems, Applications, Services & Processes
DO
May Influence & Identify Changes To
Are Accountable To
Enable The Generation Of
Are Reviewed Through
Verify
ICM Principle #6: Maintain Situational Awareness
Determine The Prioritization & Implementation Of
Verify
Are Linked To
Are Linked To
Security Metrics
Feed
Audits / Assessments
Generate
CHECK
ICM Principle #7: Manage Risk
Is Limited By
Resource Prioritization
Affects
Acceptable Risk Tolerance
Defines
Corporate Leadership
Provide Oversight Capabilities To
Analytics & Trends
[KPIs / KRIs / KCIs]
Exception Requests & Non-Compliant Controls Require
Is Assessed Against
Informs
Influences
Risk Treatment
Option 1 Reduce Risk
Option 2 Avoid Risk
Option 3 Transfer Risk
Option 4 Accept Risk
Leads To
Risk Analysis
Informs
Influences
Stakeholder Confidence
Influence
Directs
ACT
Identify Needs For
Deficiencies
Identify
Require

ATT&CK als Brücke zwischen den zahlreichen Standards im Bereich der Cybersicherheit dienen.

## WELCHES SYSTEM SIE VERWENDEN SOLLTEN

Die Auswahl des zu verwendenden Sicherheits-Frameworks hängt, wie bereits erwähnt, von einer Reihe von Kriterien ab. Es wird immer eines dieser drei ausgewählt. Dies sind einige Kriterien, die Ihnen bei Ihrer Entscheidung helfen können.

### CIS CSC v8

CIS Controls v8 ist ein taktischer Rahmen mit konkreten Aktivitäten zur Verbesserung der Cybersicherheit. Es enthält eine nach Prioritäten geordnete Liste von Sicherheitsmaßnahmen, die auf tatsächlichen Angriffen und Vorfällen basieren und in 18 bewährte Praktiken für die Cybersicherheit gegliedert sind, um Unternehmen dabei zu helfen, ihre Sicherheitslage zu verbessern und Cyberrisiken zu verringern.

CIS Controls v8 ist branchenspezifisch und richtet sich an kleine und mittlere Unternehmen. CIS CSC v8 deckt ein breites Spektrum an Sicherheitskontrollen ab, z. B. Asset Management, Schwachstellenmanagement, Zugriffskontrolle, Reaktion auf Vorfälle und Datenschutz.

CIS CSC v8 ist ein präskriptives Rahmenwerk, das präzise Verfahren zur Verbesserung der Cybersicherheit auf der Grundlage tatsächlicher Risiken und Angriffe beschreibt und praktische Hilfestellung bei der Erstellung effektiver, verständlicher Sicherheitsmaßnahmen gibt. Es handelt sich um ein umfassendes Rahmenwerk, das Unternehmen einen gründlichen Fahrplan zur Verbesserung ihrer Cybersicherheitslage bietet.

CIS CSC v8 ist möglicherweise nicht so umfassend wie andere Rahmenwerke und deckt nicht alle Bereiche der Sicherheit ab, da es sich in erster Linie auf technische Kontrollen konzentriert und Governance, Risikomanagement und Compliance nicht sehr detailliert behandelt.

### NIST CSF

Das Cybersecurity Framework (CSF) des National Institute of Standards and Technology (NIST) ist eine

Reihe von Richtlinien zur Verbesserung der Cybersicherheit in allen Bereichen kritischer Infrastrukturen. Es handelt sich um ein übergeordnetes Rahmenwerk, das Cyber-Bedrohungen identifiziert, schützt, erkennt, auf sie reagiert und sich von ihnen erholt und eine gemeinsame Sprache und Methodik für die Verwaltung und Reduzierung von Cyber-Sicherheitsrisiken bereitstellt.

Das NIST CSF kann von jeder Organisation verwendet werden, unabhängig von ihrer Größe oder Branche. Deckt fünf Kernfunktionen ab: Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen, die Organisationen dabei helfen sollen, ihr Cybersecurity-Risiko zu verstehen und zu verwalten.

NIST CSF ist ein Rahmenwerk, das Unternehmen beim Umgang mit Cybersicherheitsrisiken berät. Es handelt sich um ein flexibles Rahmenwerk, das an die individuellen Bedürfnisse verschiedener Unternehmen angepasst werden kann. Es bietet eine gemeinsame Sprache und einen standardisierten Ansatz für die Cybersicherheit, der es Unternehmen erleichtert, über ihre Sicherheitslage zu kommunizieren.

Die Umsetzung des NIST-CSF kann erhebliche Ressourcen und Fachkenntnisse erfordern, insbesondere für kleine Unternehmen. Der NIST-CSF ist nicht präskriptiv, was bedeutet, dass Unternehmen die Richtlinien so interpretieren und anwenden müssen, wie es für ihren spezifischen Kontext sinnvoll ist. Dies kann es für Unternehmen schwierig machen, zu erkennen, ob sie das Rahmenwerk richtig umsetzen.

**SCF**

Das Secure Controls Framework (SCF) konzentriert sich auf interne Kontrollen. Dabei handelt es sich um die Richtlinien, Standards, Verfahren, Technologien und zugehörigen Prozesse im Bereich der Cybersicherheit und des Datenschutzes, die so konzipiert sind, dass sie mit hinreichender Sicherheit gewährleisten, dass die Geschäftsziele erreicht und unerwünschte Ereignisse verhindert, entdeckt und korrigiert werden.

Das SCF kann von jeder Organisation verwendet werden, unabhängig von ihrer Größe oder Branche. Der SCF deckt 33 Hauptbereiche ab. Zusammen mit den Domänen gibt es Listen von Prinzipien, Risiken,

Bedrohungen und anderen, die zusammen mit einem Modell und einer Gebrauchsanweisung Organisationen dabei helfen sollen, ihre Cybersicherheitsrisiken zu verstehen und zu verwalten.

SCF bietet einen vollständigen Satz von Sicherheitskontrollen, die sowohl technische als auch organisatorische Sicherheitsfragen umfassen. Wichtig ist die Zuordnung der Kontrollen zu mehreren Standards, was eine einfache Filterung und eine Prüfung auf Konformität mit anderen Standards ermöglicht.

SCF ist komplex und schwierig zu implementieren und kann erhebliche Ressourcen und Fachkenntnisse erfordern.

## ZUSAMMENFASSUNG

Zusammenfassend lässt sich sagen, dass jedes Rahmenwerk seine eigenen Stärken und Schwächen hat. Unternehmen sollten bei der Auswahl eines Frameworks für die Implementierung ihre spezifischen Bedürfnisse und Ressourcen berücksichtigen. Wenn das Unternehmen nicht besonders einfallsreich ist und sich auf das Wesentliche konzentrieren möchte, um eine angemessene IT-Hygiene zu gewährleisten, ist CIS-CSC eine gute Option. SCF kann in der Zukunft eingesetzt werden, um die IT-Haltung zu verbessern, oder in Unternehmen, die über die Mittel und das Fachwissen verfügen, um den aktuellen Stand der meisten Kontrollen auf dem Markt zu bewerten.

Rocco Gagliardi


)SCIP(
EIN NEUANFANG
IST IMMER EINE
GUTE CHANCE

SCIP MONTHLY SECURITY SUMMARY

# IMPRESSUM

## ÜBER DEN SMSS

Das *scip Monthly Security Summary* erscheint monatlich und ist kostenlos.

Anmeldung: smss-subscribe@scip.ch
Abmeldung: smss-unsubscribe@scip.ch

Informationen zum Datenschutz.

Verantwortlich für diese Ausgabe:
Marc Ruef

Eine Haftung für die Richtigkeit der Veröffentlichungen kann trotz sorgfältiger Prüfung durch die Redaktion des Herausgebers, den Redaktoren und Autoren nicht übernommen werden. Die geltenden gesetzlichen und postalischen Bestimmungen bei Erwerb, Errichtung und Inbetriebnahme von elektronischen Geräten sowie Sende- und Empfangseinrichtungen sind zu beachten.

## ÜBER SCIP AG

Wir überzeugen durch unsere Leistungen. Die scip AG wurde im Jahr 2002 gegründet. Innovation, Nachhaltigkeit, Transparenz und Freude am Themengebiet sind unsere treibenden Faktoren. Dank der vollständigen Eigenfinanzierung sehen wir uns in der sehr komfortablen Lage, vollumfänglich herstellerunabhängig und neutral agieren zu können und setzen dies auch gewissenhaft um. Durch die Fokussierung auf den Bereich Information Security und die stetige Weiterbildung vermögen unsere Mitarbeiter mit hochspezialisiertem Expertenwissen aufzuwarten.

Weder Unternehmen noch Redaktion erwähnen Namen von Personen und Firmen sowie Marken von fremden Produkten zu Werbezwecken. Werbung wird explizit als solche gekennzeichnet.

scip AG
Badenerstrasse 623
8048 Zürich
Schweiz

+41 44 404 13 13
www.scip.ch