WIK CONSULT

Cybersicherheit

Mittelstand-Digital Magazin
WISSENSCHAFT TRIFFT PRAXIS
Ausgabe 23

Impressum

Herausgeber/Redaktion:
Begleitforschung Mittelstand-Digital
WIK-Consult GmbH
Rhöndorfer Straße 68
53604 Bad Honnef
HRB: Amtsgericht Siegburg, 7043
Tel. +49 (0)2224-9225-0, Fax +49 (0)2224-9225-68
E-Mail: mittelstand-digital@wik.org
www.mittelstand-digital.de

Eine Publikation der Mittelstand-Digital Begleitforschung im Auftrag des Bundesministeriums für Wirtschaft und Klimaschutz (BMWK)

Verantwortlich: WIK-Consult, Martin Lundborg
Redaktion: WIK-Consult, Malte Roloff
Satz und Layout: WIK-Consult, Karin Wagner

Bildnachweis:
Titelseite: Adobe Stock – onephoto
Seite 5: Adobe Stock – TechTonic
Seite 9: Jonas Blöhbaum; Mittelstand-Digital Zentrum Darmstadt
Seite 11: Freepik – Starline/ Freepik
Seite 14: Porträtfoto Dickmann: Raimar von Wienskowski
Seite 15: Adobe Stock – Robert Kneschke
Seite 17: Porträtfotos: Susann Gerstäcker / © Zentralverband des Deutschen Handwerks
Seite 18: Adobe Stock – Patrick P. Palej
Seite 23: Eigene Darstellung Jan Fischer
Seite 29: Hintergrundbild: Freepik

Stand: Oktober 2024

Druck:
Plump Druck & Medien GmbH
Rolandsecker Weg 33, 53619 Rheinbreitbach

ISSN (Print) 2198-8544
ISSN (Online) 2198-9362

Aus Gründen der besseren Lesbarkeit wird möglicherweise auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Mittelstand-Digital ist ein Förderschwerpunkt des

Bundesministerium für Wirtschaft und Klimaschutz

Mittelstand-Digital

Der Förderschwerpunkt Mittelstand-Digital wird im Auftrag des Bundesministeriums für Wirtschaft und Klimaschutz durchgeführt von

DLR Projektträger

WIK CONSULT

Mittelstand-Digital Magazin WISSENSCHAFT TRIFFT PRAXIS – Ausgabe 23

Cybersicherheit

Inhalt

Editorial

Liebe Leserinnen und Leser,

Der Mittelstand steht in Zeiten zunehmender Digitalisierung vor großen Herausforderungen – und Cybersicherheit ist eine der dringendsten. Kleine und mittlere Unternehmen sehen sich immer komplexeren Bedrohungen gegenüber, gleichzeitig sind Ressourcen oft knapp. Die Beiträge dieser Ausgabe zeigen praxisnahe Lösungsansätze und innovative Tools, um die Unternehmen bestmöglich zu unterstützen.

Unser erster Beitrag widmet sich der Rolle von KI-Chatbots und beleuchtet, wie Unternehmen mithilfe von „Security by Design" Cybersicherheit schon im Entwicklungsprozess verankern können. Im Handel zeigt sich die Notwendigkeit eines umfassenden Schutzes für Kundendaten und Finanztransaktionen, was Cybersicherheit im Handel zu einem zentralen Erfolgsfaktor macht. Handwerksbetriebe profitieren ebenfalls von sicheren digitalen Strukturen – hier hilft ein starkes Netzwerk, um Cybersicherheit zu verankern.

Für viele kleine und mittlere Unternehmen ist der pragmatische Muddling-Through-Ansatz eine flexible Möglichkeit, erste Schritte im Bereich der IT-Sicherheit zu gehen, ohne gleich hohe Budgets zu investieren. Doch wie lassen sich innovative Sicherheitsmaßnahmen trotzdem strukturiert angehen? Im Beitrag zu generativer KI und Cybersicherheit werfen wir einen Blick auf Chancen und Risiken neuer KI-Entwicklungen für Unternehmen. Schließlich zeigt predictive Cybersecurity, wie durch KI-gestützte Bedrohungsanalysen potenzielle Angriffe frühzeitig erkannt und abgewehrt werden können.

Wir wünschen Ihnen eine inspirierende Lektüre und viele wertvolle Anregungen, um Ihr Unternehmen gegen digitale Bedrohungen zu wappnen!

Malte Roloff
Begleitforschung Mittelstand-Digital

Justus Rein, Alexander Schlicher

Security by Design: Relevanz für einen KI-Chatbot

Angesichts des Fachkräftemangels in Deutschland wird die Automatisierung von Prozessen immer wichtiger, um Kosten zu senken und Effizienz zu steigern. Künstliche Intelligenz (KI) spielt dabei eine entscheidende Rolle in der Digitalisierung. Sie ermöglicht die Analyse großer Datenmengen und erweist sich als wertvolles Werkzeug zur Unterstützung von Mitarbeitern bei vielfältigen Aufgaben. Besonders im Kundensupport, als Wissensdatenbank oder als Copilot für unternehmensinterne Prozesse sind KI-Chatbots eine ideale Ergänzung zu bestehenden Systemen. Sie tragen dazu bei, Aufgaben effizienter und mit geringerer Fehlerquote zu erledigen.

Dieser Leitfaden des Mittelstand-Digital Zentrums Darmstadt hilft Ihnen, die IT-Sicherheit Ihres Chatbots schon während der Entwicklung fest im Blick zu behalten und somit ein sicheres, vertrauenswürdiges System zu schaffen. Anhand eines Beispiels zeigen wir auf wie man mit passgenauer Anwendung von künstlicher Intelligenz für den Kundensupport den persönlichen Kontakt zu seinem Kundenstamm bewahren, während man gleichzeitig den Arbeitsaufwand für das Personal reduzieren kann.

Gefahrenanalyse

Da in der Ära der künstlichen Intelligenz neue Sicherheitsrisiken für die Nutzenden entstehen, gewinnt der Schutz von Chatbots zunehmend an Bedeutung. Deshalb ist ein sicherheitsorientierter Entwicklungsansatz bereits in der frühen Phase der Entwicklung eines KI-Chatbots unerlässlich. Security by Design bedeutet, dass Schutzaspekte von Beginn an in den Entwicklungsprozess integriert werden, anstatt sie nachträglich hinzuzufügen. Dieser Ansatz gewährleistet ein besonders hohes Sicherheitsniveau und ist in Zusammenhang mit KI aus den folgenden Gründen besonders wichtig:

- **Vertrauen und Datenschutz**: Nutzer teilen Chatbots häufig persönliche und sensible Informationen mit. Eine Sicherheitsverletzung kann nicht nur den Datenschutz gefährden, sondern auch das Vertrauen in

Abbildung 1: Gefahrenanalyse

die gesamte Organisation erheblich schädigen. Ein sicher gestalteter Chatbot minimiert das Risiko von Datenlecks und Missbrauch, was zur Stärkung des Vertrauens der Nutzer beiträgt.

- **Schutz vor Cyberangriffen**: Chatbots sind potenzielle Ziele für Cyberangriffe wie Prompt Injections, Data Poisoning und andere bösartige Techniken. Durch die Anwendung von Security by Design werden solche Schwachstellen bereits in der Entwicklungsphase identifiziert und behoben, was das Risiko von Angriffen erheblich reduziert.
- **Regulatorische Compliance**: Viele Branchen unterliegen strengen Datenschutzgesetzen und Richtlinien, wie etwa der DSGVO. Ein sicher gestalteter Chatbot trägt dazu bei, diese gesetzlichen Anforderungen zu erfüllen und hohe Bußgelder sowie Reputationsschäden zu vermeiden.

Die Integration von Sicherheitsmaßnahmen in die Entwicklung von Chatbots stellt sicher, dass sowohl die rechtlichen Vorgaben eingehalten als auch die Interessen und das Vertrauen der Nutzer geschützt werden.

Welche Art von Chatbot erfüllt meine Anforderungen – Muss es immer KI sein?

Viele KI-gestützte Chatbots verwenden ein Large Language Model (LLM), um Anfragen zu beantworten. Oftmals sind jedoch auch einfache Lösungen ohne künstliche Intelligenz ausreichend, insbesondere bei wenigen und sich häufig wiederholenden Anfragen. Der Einsatz von KI bringt immer ein zusätzliches Risiko mit sich, da im Gegensatz zu herkömmlichen Programmen, oft nicht nachvollziehbar ist, wie die Antworten generiert werden. Solche "Black-Box"-Systeme sind schwerer gegen Hackerangriffe oder Systemfehler zu schützen, weil die Funktionsweise für Entwickler weitgehend undurchsichtig bleibt. Daher gilt auch für Chatbots: KI sollte nur dann eingesetzt werden, wenn sie tatsächlich einen Mehrwert bietet und keine einfachere Lösung ähnlich gute Ergebnisse liefert. Weniger komplexe Systeme sind weniger anfällig für Angriffe und benötigen deshalb auch weniger Schutzmaßnahmen.

Die drei wichtigsten Arten von Chatbots sind: Regelbasierte Systeme (ohne KI), spezialisierte KI-Modelle (fine-getunte LLMs) und KI-Modelle mit Retrieval Augmented Generation (RAG), die das LLM mit einer maschinenlesbaren Datenbasis kombinieren. Ein LLM ist in der Regel auf allgemeinen Daten trainiert und kann Texte verstehen und sinnvolle Antworten liefern, benötigt aber für spezifischere Aufgaben zusätzliche Informationen.

- **Regelbasierte Systeme** arbeiten auf Basis festgelegter Entscheidungsbäume und reagieren mit vordefinierten Regeln auf Benutzereingaben. Sie sind sicher und effizient bei der Bearbeitung standardisierter Fragen, bieten jedoch wenig Flexibilität gegenüber unerwarteten Anfragen, da jede Regel und jede Antwort einzeln programmiert werden müssen.
- **KI-Chatbots mit einem fine-getunten LLM** nutzen ein vortrainiertes LLM, das durch zusätzliche Trainingsdaten auf eine bestimmte Aufgabe oder ein Fachgebiet spezialisiert wird. Dieses Fine-Tuning ist nicht nur kostenintensiv, sondern erfordert bei jeder Aktualisierung des Wissens auch ein erneutes Training des Modells. Zudem besteht die Gefahr, dass die Qualität der Antworten nach einem (erneuten) Fine-Tuning abnimmt, da das Modell eventuell unvorhersehbare Veränderungen im Verhalten zeigt oder vorheriges Wissen überschrieben wird.
- **KI-Chatbots mit LLM und RAG** kombinieren ein vortrainiertes LLM mit einer aktuellen Faktenbasis. Bei jeder Nutzeranfrage greift der Chatbot auf diese Faktenbasis zu und integriert die aktuellen Informationen in die Antwort. Um die Antworten zu aktualisieren, muss lediglich die zugrunde liegende Datenbasis aktualisiert werden.

Diese verschiedenen Ansätze verdeutlichen, dass der Einsatz komplexer KI-Modelle nicht immer erforderlich ist – die Wahl des passenden Chatbot-Typs sollte stets an den spezifischen Anforderungen und den gewünschten Anwendungsfall ausgerichtet sein. Auch Kombinationen der verschiedenen Chatbot-Typen sind möglich, sollten jedoch nur dann in Betracht gezogen werden, wenn sie einen klaren Mehrwert für das Projekt bieten und die jeweiligen Stärken optimal genutzt werden können.

Abbildung 2: Arten von Chatbots

Sicherheit bei der Beantwortung von Fragen

Neben der IT-Sicherheit spielt auch die Zuverlässigkeit und Genauigkeit der Antworten eines Chatbots eine zentrale Rolle. Es ist wichtig, zu reflektieren, wie hoch der Wahrheitsgehalt der Aussagen ist und wie gut der Chatbot in der Lage ist, effektiv zu kommunizieren. Es ist unmöglich, einen Chatbot zu nutzen, der auf allgemeinem Wissen trainiert wurde, um spezifische Fragen zu beantworten. Ein spezialisierter Chatbot, der durch gezieltes Fine-Tuning oder durch ein RAG mit Fachwissen ausgestattet ist, bietet, in seinem Fachbereich, deutlich präzisere und konsistentere Antworten als beispielsweise bei Fragen zum Produktportfolio eines bestimmten Unternehmens. Ein Chatbot kann sogar aus mehreren Sprachmodellen bestehen, die jeweils Experten auf ihrem Gebiet sind. Ein übergeordnetes Modell übernimmt dann die Aufgabe, Anfragen an die passenden Expertensysteme weiterzuleiten. Expertensysteme sind nicht nur bei KI-Chatbots von Bedeutung, sondern finden in vielen weiteren KI-Systemen Anwendung.

(Indirect) Prompt Injection

Prompt Injection ist eine Angriffstechnik, bei der Hacker versuchen, einen Chatbot durch gezielte Texteingaben (Prompts) zu manipulieren. KI-basierte Chatbots sind besonders anfällig dafür, da sie jede Nutzereingabe verarbeiten und darauf reagieren. Wenn ein solcher Chatbot Zugriff auf firmeninterne Daten, das Internet oder andere Programme (z. B. PDM-Systeme) hat, könnten Hacker potenziell auf diese Ressourcen zugreifen.

Ein hundertprozentiger Schutz vor solchen Angriffen ist oft schwer oder gar nicht zu gewährleisten. Daher sollte ein Chatbot keinen direkten Zugriff auf kritische Systeme haben, und die Datenübertragungen zu und von ihm sollten sorgfältig überwacht werden. Besonders gefährlich wird es, wenn Hacker über angeschlossene Systeme auf den Chatbot zugreifen und dadurch fehlerhafte Antworten generiert werden, ohne dass die Nutzer dies bemerken. Um solche Risiken zu minimieren, sollten Nutzer regelmäßig über die potenziellen Gefahren von KI-Chatbots informiert werden und die Antworten stets kritisch hinterfragen.

Architektur eines eigenen KI-Chatbots zum Beantworten von Mails

Im Folgenden ist eine mögliche Architektur für einen KI-Chatbot mit LLM und RAG zur Beantwortung von Mails aus mehreren Bausteinen vorgestellt. Dabei wird die Kompatibilität durch web- bzw. protokollbasierte Schnittstellen sichergestellt. Es stehen neben kommerziellen Lösungen auch solide entwickelte, kostenlose Open-Source-Komponenten zur Umsetzung der genannten Funktionen bereit.

- **Mail-Client**: Es sollte ein Mail-Client verwendet werden, der Verschlüsselung und Authentifizierung unterstützt, um sichere Kommunikation zu gewährleisten.
- **LLM**: Es sollte ein LLM, z.B. „Mixtral 7B“, ausgewählt und die Ein- und Ausgabeverarbeitung des Modells so abgesichert werden, dass keine Code Injections möglich sind.
- **RAG**: Verwendet werden sollte ein robuster RAG-Mechanismus, der sicherstellt, dass nur relevante und aktuelle Daten abgerufen und verwendet werden.
- **Faktenbasis**: Fakten sollen sich nicht widersprechen, damit das LLM bessere Entscheidungen treffen kann.

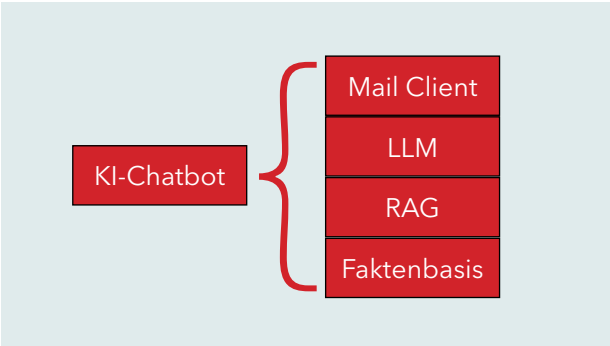


Abbildung 3: Architektur KI-Chatbot

Alignment

Das Alignment eines eigenen KI-Chatbots bedeutet, ihn so zu trainieren oder anzupassen, dass er den spezifischen Anforderungen und ethischen Richtlinien eines Unternehmens entspricht. Dies umfasst die Abstimmung auf die gewünschten Kommunikationsstile sowie Sicherheitsprotokolle und die Vermeidung schädlicher oder irreführender Inhalte. Dabei kann der Chatbot sowohl dazu gebracht werden, bestimmte Floskeln in der Kommunikation zu verwenden, als auch darauf angepasst werden, nur Fragen zu Themen zu beantworten, für deren Beantwortung er vorgesehen ist. Für die IT-Sicherheit ist dies besonders relevant, da ein gut ausgerichteter Chatbot potenzielle Sicherheitslücken minimieren kann, indem er beispielsweise vertrauliche Informationen schützt und nur auf sichere Weise kommuniziert. Ein gutes Alignment ist eine erste erfolgsversprechende Schutzmaßnahme gegen Prompt Injection.

Entwicklungsleitfaden für einen sicheren Chatbot nach dem Security by Design Prinzip

Um die IT-Sicherheit bei der Entwicklung eines Chatbots von Anfang an zu gewährleisten, empfiehlt es sich, einen strukturierten Entwicklungsprozess zu verfolgen. Hierbei können die folgenden Schritte Orientierung bieten:

1. **Anforderungsanalyse:** Definieren Sie klar die Funktionen, die der Chatbot ausführen soll. Welche Aufgaben soll der Chatbot übernehmen und wie soll er mit den Nutzern interagieren? Muss der Chatbot mit dem Internet agieren oder Programme ausführen können? Achtung: Solche Funktionen können ein großes Angriffspotential für Prompt Injection bieten.

2. **Risikobewertung**: Identifizieren Sie potenzielle Risiken im Zusammenhang mit den festgelegten Funktionen. Überlegen Sie, wie diese Risiken minimiert oder ganz vermieden werden können. Dabei sollte auch eine Abwägung von Nutzen und Risiko erfolgen.

3. **Datenschutz und Datenminimierung**: Analysieren Sie, welche Daten für die Erfüllung der Chatbot-Funktionen wirklich notwendig sind. Wo immer möglich, sollten anonymisierte oder pseudonymisierte Daten verwendet werden. Ein Chatbot benötigt in der Regel keine langfristige Datenspeicherung. Idealerweise werden Daten unmittelbar nach der Verarbeitung gelöscht. Sollten Daten gespeichert werden müssen, sollten diese auf getrennten Systemen mit einer für den jeweiligen Anwendungsfall sinnvollen Authentifizierungsstrategie erfolgen, um den Missbrauch des Chatbots als Trojanisches Pferd zu verhindern. Wichtig ist, dass Sie jederzeit die Kontrolle darüber behalten, ob und wo Daten langfristig gespeichert werden.

4. **Sichere Authentifizierung und Autorisierung**: Stellen Sie sicher, dass nur autorisierte Nutzer Zugriff auf den Chatbot haben. Ist der Chatbot für jeden zugänglich oder nur für bestimmte Nutzergruppen, wie beispielsweise Abteilungen innerhalb eines Unternehmens?

5. **Sichere Kommunikation**: Der Chatbot sollte stets über sichere, verschlüsselte Kommunikationskanäle mit anderen Systemen interagieren, um Man-in-the-Middle-Angriffe zu verhindern und die Integrität der übermittelten Daten zu gewährleisten.

6. **Logging und Monitoring**: Implementieren Sie Überwachungsmechanismen, um ungewöhnliche Aktivitäten frühzeitig zu erkennen. Auffälligkeiten im Systemverhalten können auf potenzielle Angriffe hinweisen und sollten umgehend analysiert werden.

7. **Schulungen**: Der Mensch bleibt die größte Schwachstelle in jedem IT-System. Schulen Sie Ihre Mitarbeiter umfassend, damit sie den Chatbot sicher und bewusst nutzen können. Regelmäßige Schulungen tragen dazu bei, Sicherheitslücken zu vermeiden.

8. **Regelmäßiges Update- und Patch-Management**: Um die IT-Sicherheit langfristig zu gewährleisten, sollten alle sicherheitsrelevanten Systemkomponenten regelmäßig aktualisiert werden. Dies umfasst sowohl Software-Updates als auch Patches, um bekannte Schwachstellen zu schließen.

Hardware

Überlegen Sie, auf welcher Hardware der Chatbot betrieben werden soll. Ein selbst entwickelter Chatbot kann sowohl auf eigener Hardware als auch auf der eines Cloud-Dienstleisters laufen. Während eigene Hardware die volle Kontrolle bietet, verfügen externe Cloud-Dienstleister in der Regel über eine sichere Infrastruktur und Experten, die sich um die Sicherheitsaspekte kümmern.

Praxisbeispiel: Implementierung eines KI-gestützten Kundensupports

Das Dienstleistungsunternehmen BENSO, eine kommerzielle Sportschule für ostasiatische Kampfkunst, wurde im Jahr 2019 gegründet und beschäftigt zehn Mitarbeiter. Anfang 2024 startete das Mittelstand-Digital Zentrum Darmstadt gemeinsam mit dem Unternehmen das Umsetzungsprojekt „Einführung eines KI-Chatbots zur Automatisierung des Kundensupports".

Die Entscheidung, ein Digitalisierungsprojekt mit dem Mittelstand-Digital Zentrum Darmstadt zu beginnen, entstand aus dem Wunsch heraus, Routineaufgaben durch Automatisierung effizienter erledigen zu können und damit dem Personal zu ermöglichen, sich vermehrt auf komplexe Anfragen der Kunden konzentrieren zu können.

Im Rahmen des Projektes wurde ein Chatbot, mit der hier beschriebenen Sicherheitsstruktur, implementiert. Dabei hat das Mittelstand-Digital Zentrum Darmstadt, im regelmäßigen Austausch mit dem Unternehmen, ein Konzept entwickelt und die Kampfkunstschule über einen Zeitraum von fünf Monaten bei der Entwicklung und Implementierung des KI-Chatbots mit fachlicher Expertise unterstützt.

Durch den Einsatz des KI-Chatbots können häufig gestellte Fragen nun schnell beantwortet und Probleme unmittelbar gelöst werden. So können Wartezeiten reduziert und die Kundenzufriedenheit gesteigert werden. Die Mitarbeitenden des Unternehmens beschreiben es als entlastend, im täglichen Schriftverkehr Hilfe zu bekommen und zugleich die Gewissheit zu haben, dass das System sicher ist und Kundendaten nicht gefährdet werden. Obwohl kein internes IT-Team vorhanden ist, kann der sichere Betrieb auch in Zukunft durch die, während der Entwicklung eingeführten Schutzmaßnahmen, gewährleistet werden. Dank der klaren Struktur und der Kontrolle über den Quellcode ist zudem eine zukünftige Weiterentwicklung und Wartung durch einen externen IT-Dienstleister möglich.

Abbildung 4: MDZ-Team bei der Kampfkunstschule BENSO

Autoren

Justus Rein, M.Sc. ist Maschinenbau-Ingenieur und seit Oktober 2023 wissenschaftlicher Mitarbeiter an der Technischen Universität Darmstadt (TUDa) im Fachgebiet Product Lifecycle Management (PLCM). Er beschäftigt sich mit der Automatisierung von Produktionsprozessen. Neben seiner wissenschaftlichen Forschung arbeitet er im Mittelstand-Digital Zentrum Darmstadt und ist dort für die Information und Qualifizierung von kleinen und mittelständischen Unternehmen (KMU) zur Verbesserung ihrer IT-Sicherheit zuständig.

Dipl.-Ing. **Alexander Schlicher** studierte bis April 2023 Elektrotechnik an der Rheinland-Pfälzischen Technischen Universität Kaiserslautern-Landau (RPTU). In seiner Diplomarbeit entwickelte er eine Methode zur automatisierten Rekonstruktion topologieoptimierter Netzgeometrien in einer parametrischen Modellierungsumgebung. Seit Oktober 2023 ist Alexander Schlicher als wissenschaftlicher Mitarbeiter am Fachgebiet Product Life Cycle Management an der Technischen Universität Darmstadt tätig und beschäftigt sich im Rahmen des Mittelstand-Digital Zentrum Darmstadt mit IT-Sicherheit und automatisierter Konstruktion.

Das **Mittelstand-Digital Zentrum Darmstadt** besteht aus einem Zusammenschluss von vier Forschungsinstituten der TU Darmstadt, zwei Fraunhofer Instituten und der IHK Darmstadt Rhein-Main-Neckar.

Das Zentrum unterstützt mit seinem kostenlosen Angebot kleine und mittlere Unternehmen (KMU) bei der Digitalisierung. Zur Wissensvermittlung bietet es eine Mischung aus Präsenz- und Online-Formaten an, die je nach Bedarf eingesetzt werden können. Dazu zählen Online-Seminare für eine erste Orientierung, Videotelefonate oder Gespräche, um sich persönlich über eine Fragestellung auszutauschen oder Workshops vor Ort, wenn es um die konkrete Umsetzung von Ideen geht. Weiterhin sind spezialisierte Lernfabriken zentraler Bestandteil der Wissensvermittlung. Unternehmen können hier eine einzigartige Praxisnähe erleben.

In den kommenden beiden Jahren konzentriert sich das Zentrum auf die Vermittlung der notwendigen Kompetenzen zum Erreichen der KI-Readiness in fünf Feldern des produzierenden Gewerbes:

- KI-getriebene Produktion
- KI-basierte Geschäftsmodelle und datenbasierte Services
- Arbeitswelt und KI
- IT-Sicherheit und KI
- Nachhaltigkeit durch KI

Wenden Sie sich gern direkt an uns, falls auch Sie in Ihrem Unternehmen einen IT-sicheren KI-Chatbot einsetzen wollen oder sich für die Arbeit des Zentrums interessieren.

https://digitalzentrum-darmstadt.de/

Mittelstand-Digital Zentrum Darmstadt

Franziska Dickmann

Auf dem Weg zur Cybersicherheit im Handel

Vom Warenwirtschaftssystem über die Kundenbetreuung bis hin zur Zahlungsabwicklung: Die Digitalisierung hat den Handel verändert. Die Digitalisierung dieser Prozesse bringt zahlreiche Vorteile mit sich, öffnet aber auch Cyberkriminellen einige Türen. Insbesondere für mittelständische Handelsunternehmen stellt die eigene Cybersicherheit eine große Herausforderung dar.

Cybersicherheit im Handel bedeutet vielfachen Schutz auf verschiedenen Ebenen, der nicht durch einen einzigen, verantwortlichen Mitarbeiter abgedeckt werden kann. Doch wo beginnt der Weg? Und gibt es ein (vorläufiges) Ziel?

Cybersicherheit als Grundstein?

Die Angriffsfläche von Cyberkriminellen vergrößert sich ständig: Jede Online-Transaktion, E-Mail sowie gespeicherte Kundendaten stellen potenzielle Ziele dar. Ein erfolgreicher Cyberangriff kann weitreichende Konsequenzen haben. Dabei geht es nicht nur um die finanziellen Verluste und gestohlenen Daten: Ein derartiger Vorfall kann auch den Ruf eines Unternehmens nachhaltig schädigen. Für Handelsunternehmen gehört das Vertrauen der Kund:innen daher zu ihrem Fundament. Wenn diese ihre Zahlungsinformationen oder persönlichen Daten an ein Unternehmen übermitteln, erwarten sie, dass sie geschützt sind. Befragt zur Sicherheit beim Onlineshopping, gaben über 80 Prozent bei einer Erhebung des Bundesamts für Sicherheit in der Informationstechnik an, dass der Schutz der eigenen Zahlungsdaten und damit der Schutz vor finanziellen Risiken für sie im Vordergrund steht. Rund die Hälfte der Befragten hat sich schon einmal über das Thema „Datensicherheit beim Online-Shopping" informiert. 85 Prozent der Verbraucher:innen sind zudem der Meinung, dass Onlineshops dazu verpflichtet sind, die Sicherheit ihrer persönlichen Daten zu gewährleisten.[1]

Damit sind sie durchaus im Recht: Händler:innen haben eine rechtliche Verantwortung zum Schutz der Daten ihrer Kundschaft. Die Datenschutz-Grundversorgung (DSGVO) stellt strenge Anforderungen an den Umgang

1 IT-Sicherheit auf dem digitalen Verbrauchermarkt: Fokus Onlineshopping-Plattformen – Bundesamt für Sicherheit in der Informationstechnik, *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/onlineshopping-plattformen.pdf?__blob=publicationFile&v=21*

mit personenbezogenen Daten. Händler:innen, die auf Cyberangriffe vorbereitet sind, können zudem schneller auf neue Bedrohungen reagieren und so potenzielle Schäden minimieren. Unternehmen können ihre Cybersicherheit daher auch als Wettbewerbsvorteil nutzen. Denn Datenschutz und -sicherheit rücken immer mehr in den Fokus und können ein entscheidender Faktor bei Kundenentscheidungen sein.

Digitale Bedrohungen, reale Gefahr

Die Bedrohungen in der digitalen Welt entwickeln sich stetig weiter, Cyberkriminelle haben in den letzten Jahren immer neue Wege gefunden, um anzugreifen. Daher ist es für Händler:innen im ersten Schritt entscheidend, die verschiedenen Bedrohungen zu kennen, um sich entsprechend wappnen zu können:

Phishing gehört zu den häufigsten Methoden unter den Cyberangriffen. Es handelt sich um eine betrügerische Methode, bei der Kriminelle sich, oft durch E-Mails oder Anrufe, als vertrauenswürdige Quellen wie Bankinstituten etc. ausgeben, um sensible Daten wie Passwörter oder Kreditkartennummern zu erhalten. Oft sind Phishing-Mails so gestaltet, dass sie legitimen Nachrichten stark ähneln, zudem können sie gefälschte Logos, ähnliche Absenderadressen und überzeugende Inhalte enthalten. Diese Ähnlichkeiten sollen die Empfänger:innen dazu verleiten, auf einen Link zu klicken oder einen Anhang zu öffnen, wodurch Malware installiert werden kann, oder zu einer gefälschten Webseite weitergeleitet wird, die darauf angelegt ist, Daten zu stehlen.
Onlinehändler:innen können beispielsweise Phishing-E-Mails erhalten, die angeblich vom eigenen Zahlungsdienstleister stammen und dazu auffordern, Kontodaten zu bestätigen. Die E-Mails enthalten einen Link zu einer Webseite, die der echten Webseite des Dienstleisters stark ähnelt. Vertrauen Händler:innen den E-Mails, werden ihre Daten direkt an Cyberkriminelle geleitet.

Quishing ist eine Form des Phishings. Dabei nutzen Cyberkriminelle QR-Codes, um E-Mail-Sicherheitslösungen zu umgehen. Während klassische Anti-Viren-Programme und Sicherheitslösungen Anhänge und URLs in E-Mails scannen, erkennen sie QR-Codes lediglich als Bilddateien und sehen in ihnen kein Risiko.

Malware ist eine Schadsoftware, die dazu entwickelt wurde, Computer oder Netzwerke unbemerkt im Hintergrund zu beschädigen oder Unbefugten Zugriff zu ermöglichen. Dazu gehören Viren, Würmer, Trojaner und Ransomware. Malware kann sich zum Beispiel über Anhänge in einer Phishing-E-Mail verbreiten.
Händler:innen laufen Gefahr, sich eine vermeintlich nützliche Software herunterzuladen, die sich jedoch als Trojaner entpuppt. Der Trojaner öffnet den Cyberkriminellen dann Zugang zum internen Netzwerk des Unternehmens, wo sie unbemerkt Daten stehlen können.

Ransomware, eine besonders bedrohliche Form von Malware, verschlüsselt Daten mit dem Ziel, diese nur gegen Erpressung eines Lösegeldes wieder freizugeben. Ransomware-Angriffe können verheerend sein, da sie den gesamten Betrieb eines Unternehmens zum Stillstand bringen können. Selbst wenn Unternehmen das Lösegeld zahlen, haben sie keine Garantie, dass die Daten tatsächlich wiederhergestellt werden. Ransomware wird oft über Phishing-E-Mails verbreitet, kann aber auch durch Schwachstellen in der Netzwerksicherheit in das System gelangen. Die verschlüsselten Daten sind für das betroffene Unternehmen meist wertlos, was den Druck erhöht, das geforderte Lösegeld zu zahlen.
Wird ein mittelständisches Modeunternehmen beispielsweise Opfer eines Ransomware-Angriffs, können sämtliche Kundendaten und Geschäftsunterlagen verschlüsselt werden. Die Angreifer:innen fordern eine hohe Summe in Bitcoin. Das Unternehmen steht vor der Wahl, das Lösegeld zu zahlen oder den Verlust der Daten zu riskieren.

DDoS-Angriffe (Distributed Denial of Service) zielen darauf ab, bei einem Webdienst durch Anfragen eine Überlastung auszulösen. Dabei werden zahlreiche Computer oder andere internetfähige Geräte genutzt, um gleichzeitig eine Masse an Anfragen an den Zielserver zu senden. Diese Überlastung kann dazu führen, dass der Server abstürzt oder so stark verlangsamt wird, dass legitime Benutzer:innen keinen Zugriff mehr auf die Website oder den Dienst haben.
DDoS-Angriffe sind besonders für Onlinehändler:innen gefährlich, da sie während eines Angriffs keine Geschäfte abwickeln können. Dies kann zu erheblichen Einnahmeverlusten führen, insbesondere wenn der Angriff in einer umsatzstarken Zeit, wie dem Weihnachtsgeschäft, erfolgt. So kann ein Onlineshop für Elektronikartikel während des Black Fridays von einem DDoS-Angriff getroffen werden. Ist der Server überlastet und die Website für mehrere Stunden nicht erreichbar, verliert der Onlineshop in dieser Zeit Tausende potenzieller Verkäufe.

Keylogger sind spezialisierte Programme, die Tastenanschläge aufzeichnen, um Passwörter und andere sensible Daten zu stehlen. Keylogger sind besonders gefährlich, da sie oft unbemerkt bleiben und über einen längeren Zeitraum Daten sammeln können. Unternehmen, die Online-Zahlungen abwickeln, sind ein bevorzugtes Ziel, da die gesammelten Daten direkt für finanzielle Betrüge verwendet werden können.
Installiert ein Angestellter eines Handelsunternehmens unwissentlich einen Keylogger, kann dieser über einen längeren Zeitraum seine Eingaben überwachen. Die Angreifer:innen sammeln so Passwörter und sensible Unternehmensinformationen, die sie später für einen gezielten Angriff nutzen.

Der „Faktor Mensch" darf nicht vergessen werden

Diese Auswahl zeigt: Cyberangriffe sind vielfältig und oft nicht sofort erkennbar. Besonders mittelständischen Unternehmen fehlt es oftmals an den notwendigen Ressourcen und dem Wissen, um sich effektiv vor Cyberangriffen zu schützen oder sich gegen diese zu wehren. Viele kleine und mittlere Händler:innen gehen zudem davon aus, dass sie für Cyberkriminelle gar nicht attraktiv genug sind. Dies führt häufig dazu, dass die Sicherheitsanliegen vernachlässigt werden. Sicherheitslücken werden nicht rechtzeitig erkannt und geschlossen, es mangelt an einer Sicherheitsstrategie. Viele Mitarbeiter:innen sind sich der Gefahr eines Cyberangriffes nicht bewusst und sind nicht ausreichend geschult. Phishing-E-Mails, unsichere Passwörter und der unbedachte Umgang mit vertraulichen Daten sind nur einige der Risiken, die so durch den „Faktor Mensch" entstehen.

Kleine und mittlere Unternehmen gelten daher als leichter angreifbar und sind so bevorzugte Ziele von Cyberkriminellen. Aufgrund der knapperen finanziellen Ressourcen kann ein erfolgreicher Angriff jedoch erhebliche Folgen für das Unternehmen mit sich bringen, die bis zur Existenzbedrohung reichen können. Damit alle Mitarbeiter:innen, unabhängig von ihrer Position im Unternehmen, ein grundlegendes Verständnis für Cybersicherheit entwickeln und wissen, wie in Krisensituationen zu handeln ist, sind daher regelmäßigen Schulungen notwendig, um ihnen die Gefahren näherzubringen.

Schritt für Schritt auf dem Weg zur Cybersicherheit

Angesichts der vielfältigen Bedrohungen und Herausforderungen müssen Handelsunternehmen im zweiten Schritt konkrete Maßnahmen ergreifen. Doch was ist damit gemeint und welche Maßnahmen sind auch mit weniger Ressourcen umsetzbar?

Ein grundlegender und wenig aufwendiger Schritt zur Verbesserung der Cybersicherheit ist die *regelmäßige Durchführung von Updates*, denn veraltete Software stelle eine der größten Schwachstellen dar. Händler:innen sollten sicherstellen, dass all ihre Systeme, Anwendungen und Geräte stets auf dem aktuellen Stand sind. Hierbei handelt es sich nicht nur um die Betriebssysteme und Server, sondern auch um Endgeräte wie Smartphone und Laptops, die im Arbeitsalltag genutzt werden.

Ein weiteres Werkzeug im Kampf gegen Cyberbedrohungen ist *Sicherheitssoftware*. Zu den grundlegenden Komponenten einer Sicherheitsstrategie gehören Antivirus-Programme, Firewalls und Intrusion-Detection-Systeme (IDS). Durch die Systeme wird der Netzwerkverkehr überwacht, wodurch verdächtige Aktivitäten und potenzielle Angriffe entdeckt und geblockt werden können. Händler:innen können sich außerdem über Software-Lösung informieren, die auf ihre spezifischen Bedürfnisse zugeschnitten sind. Für Onlinehändler:innen kann beispielsweise die Installation einer Web Application Firewall (WAF) sinnvoll sein, dass diese Cyberangriffe auf Webanwendungen erkennen und abwehren kann.

Auch die Implementierung von *Zwei-Faktor-Authentifizierungen (2FA)* ist eine wirksame Maßnahme, um den Zugriff auf die sensiblen Systeme und Daten zu verhindern. Bei 2FA ist neben des Passworts ein zweiter Identitätsnachweis erforderlich, zum Beispiel in Form eines Einmalcodes, der an das Mobiltelefon gesendet wird. Diese zusätzliche Sicherheitsebene erschwert es Cyberkriminellen, unbefugt auf Systeme zuzugreifen, selbst wenn sie in den Besitz eines Passworts gelangen sollten. Händler:innen sollten 2FA für alle kritischen Systeme und Anwendungen einführen und die Nutzung durch die Mitarbeiter:innen fördern. Auch alternative Authentifizierungsmethoden wie biometrische Verfahren sollten in Erwägung gezogen werden.

Ein weiterer Baustein auf dem Weg zur Cybersicherheitsstrategie sind *regelmäßige Backups*. Im Falle eines Ransomware-Angriffs oder eines anderen schwerwiegenden Vorfalls stellen Backups sicher, dass aktuelle Daten schnell wiederhergestellt werden können. Backups sollten daher automatisiert und regelmäßig durchgeführt werden. Die gesicherten Daten sollten dabei an einem sicheren Ort gespeichert werden, der nicht direkt mit dem Hauptsystem verbunden ist. Cloudbasierte Backup-Lösungen können beispielsweise eine sinnvolle Ergänzung sein, um sicherzustellen, dass die Daten auch bei Diebstahl geschützt sind.

Für Unternehmen ist auch die *Etablierung eines Notfallplans oder einer Notfallkarte* unerlässlich. Dieser sollte nicht nur digital, sondern auch ausgedruckt zur Verfügung stehen. Ein derartiger Plan enthält Anweisungen für alle Mitarbeiter:innen zu den wichtigsten Schritten im Falle eines Cyberangriffs. Durch regelmäßige Überprüfungen sollte außerdem sichergestellt werden, dass alle Mitarbeiter:innen wissen, wie im Ernstfall zu handeln ist. Zu den wichtigsten Elementen des Notfallplans gehören (falls notwendig) die Benachrichtigung der zuständigen Behörden, die Isolation betroffener Systeme, die Kommunikation mit Kund:innen und Geschäftspartner:innen und die Wiederherstellung von Daten aus Backups. Unternehmen sollten auch sicherstellen, ob sie über eine ausreichende Cyber-Versicherung verfügen, um mögliche finanzielle Verluste abzufedern.

Nicht zu vergessen ist schließlich: Neben den technischen Herausforderungen ist Cybersicherheit auch eine

Managementaufgabe. Denn die Verantwortung für die Sicherheit eines Unternehmens darf nicht allein der IT-Abteilung überlassen werden. Die Führungsebene sollte aktiv in die Entwicklung und Umsetzung einer umfassenden Sicherheitsstrategie eingebunden sein, um diese aus ihrer Position heraus (unter anderem durch die Bereitstellung von notwendigen Ressourcen) voranzutreiben.

Am Ziel angekommen?

Alle möglichen Sicherheitsrisiken sind bekannt, alle notwendigen Maßnahmen getroffen – Ist das Ziel des Weges nun erreicht? Leider nein, denn Cyberkriminelle schlafen nicht. Die Konsequenz für Unternehmen lautet entsprechend: „wachsam bleiben". Dazu gehört, regelmäßig die eigenen Maßnahmen zu überprüfen und Systeme aktuell zu halten, sowie Mitarbeitende regelmäßig zu informieren. Unter anderem Künstliche Intelligenz wird immer stärker dabei unterstützen können, das eigene Unternehmen zu schützen. KI kann dabei vor allem mit Blick auf den Onlinehandel eine Hilfe sein, zum Beispiel bei der Verbesserung der Betrugs- und Risikoerkennung. Mithilfe von Machine Learning können beispielsweise bestimmte Muster wie bei Phishing-E-Mails erkannt werden. Bereits bekannte, aber auch unbekannte Bedrohungen können so in Echtzeit identifiziert und blockiert werden, verdächtige Aktivitäten können gezielter überwacht werden. Darüber hinaus kann Künstliche Intelligenz dazu genutzt werden, um synthetische Inhalte zu identifizieren und vertrauenswürdige von nicht vertrauenswürdigen Inhalten zu unterscheiden. Andererseits wird der Einsatz Künstlicher Intelligenz auch dazu führen, dass Cyberangriffe immer schwieriger auszumachen ist, da sich die Anschreiben via E-Mail etc. immer weiter verbessern.

Fazit

Der Einblick zeigt: Für Handelsunternehmen stellt Cybersicherheit einen kontinuierlichen Prozess dar, bei dem Händler:innen wachsam bleiben müssen, um sensiblen (Kunden-) Daten als auch ihren Geschäftsbetrieb zu schützen. Der Ausbau der eigenen Cybersicherheit ist für Händler:innen ein entscheidender Punkt, um das Vertrauen der Kund:innen zu erhalten, finanzielle Verluste zu vermeiden und so langfristig wettbewerbsfähig zu sein. Um ein cybersicheres Unternehmen zu führen, muss dieses in die notwendigen Technologien und auch das Personal investieren und so eine Sicherheitskultur etablieren.

Händler:innen finden beim Mittelstand-Digital Zentrum Handel verschiedene Informationen und Angebote, u.a. Checklisten und Infoblätter zu den Themen

- **IT-Sicherheit im Online-Handel**
  https://digitalzentrumhandel.de/wp-content/uploads/2021/12/it_check_kompetenzzentrum.pdf
- **IT-Sicherheit im Handel**
  https://digitalzentrumhandel.de/infoblaetter-und-checklisten/infoblatt-it-sicherheit-im-handel/
- **Sicherheitsmaßnahmen für Shop-Systeme**
  https://digitalzentrumhandel.de/infoblaetter-und-checklisten/infoblatt-sicherheitsmassnahmen-fuer-shop-systeme/
- **NIS-2-Richtlinie**
  https://digitalzentrumhandel.de/wp-content/uploads/2024/07/infoblatt-nis-richtlinie-mdzh-19-06-2024.pdf
- **Podcastfolge zur Frage „Wie lässt sich IT-Sicherheit im Handel umsetzen?"**
  https://digitalzentrumhandel.de/it-sicherheit-im-handel-umsetzen/

Autorin

Franziska Dickmann ist Projektleiterin im Mittelstand-Digital Zentrum Handel und zuständig für die Presse- und Kommunikationsaktivitäten.

Das **Mittelstand-Digital Zentrum Handel** ist die branchenspezifische Anlaufstelle für kleine und mittlere Unternehmen des Einzel- und Großhandels in Deutschland. Es unterstützt mittelständische Unternehmen dabei, ihre Geschäftsmodelle mithilfe digitaler Anwendungen und Technologien nachhaltig zukunftssicher zu machen. Gefördert durch die Initiative Mittelstand-Digital des Bundesministeriums für Wirtschaft und Klimaschutz, setzt sich das Zentrum aus dem Handelsverband Deutschland e.V. (HDE), ibi research, EHI Retail Institute, IFH Köln und dem Deutschen Forschungszentrum für Künstliche Intelligenz (DFKI) zusammen.

https://digitalzentrumhandel.de/

Mittelstand-Digital Zentrum Handel

Juliane Haase, Stephan Blank

Ein starkes Netzwerk für ein sicheres Handwerk

Die digitale Transformation eröffnet auch dem Handwerk viele Chancen: neue Geschäftsmodelle, vereinfachte Arbeitsprozesse, effizienterer Einsatz von Ressourcen und Einsparpotenziale. Aber mit vielen Chancen kommt meist auch viel Verantwortung. Und daher sollte auch Cybersicherheit von Anfang an mitgedacht werden, wenn man sich entscheidet, digitale Prozesse oder Technologien im Unternehmen einzubinden.

Viele Betriebe vermeiden dieses Thema jedoch noch häufig. Fehlendes Knowhow oder Verständnis für die Wichtigkeit aber auch fehlende Greifbarkeit sorgen für Berührungsängste. Dabei kann man bereits mit wenigen, einfachen und häufig sogar kostenfreien Maßnahmen eine gewisse Grundsicherung gewährleisten.

Wer digitalisiert, muss Cybersicherheit von Anfang an mitdenken

Denn, wer lässt schon seine Haustür offenstehen? Und Gleiches gilt in der digitalen Welt. Auch hier muss man die digitale Haustür verriegeln, um den Zugriff von Unbefugten zu vermeiden. Ganz logisch eigentlich, oder?

Dennoch ist es zugegebenermaßen in der Praxis nicht ganz so einfach, wie den Schlüssel im Haustürschloss umzudrehen. Cybersicherheit ist unsichtbar, für haptisch veranlagte Menschen schwer greifbar aber vor allem auch sind Erfolge nicht unmittelbar sicht- oder messbar – den Anschein hat es.

Darüber hinaus besteht häufig noch die Annahme, Handwerksbetriebe wären zu klein und uninteressant für Hakker. Leider trifft es aber eben genau diese Betriebe, wenn sie einfach gar keine Schutzmaßnahmen ergriffen haben. Denn Angriffe erfolgen längst nicht mehr durch einzelne Personen, die gezielt einem Unternehmen schaden wollen. Nein, es sind automatisierte Softwareprogramme,

die im Hintergrund laufen und gezielt nach Schwachstellen suchen. **Das heißt: Die Frage ist längst nicht mehr, ob der eigene Betrieb angegriffen wird, sondern wann er angegriffen wird bzw. wann ein Angriff erfolgreich ist.** Und in diesem Fall, sollte jeder Betriebsinhaber oder Geschäftsführer vorbereitet sein. Denn ein Angriff kann verheerende Folgen haben, dem Image schaden oder sogar existenzbedrohend sein.

Doch wie kann man als kleiner Betrieb diesem Thema begegnen?

Cybersicherheit ist für viele – besonders Handwerksbetriebe – ein schwer greifbares Thema. Denn ihre Kompetenzen liegen in ihrer handwerklichen Tätigkeit. Dies bestätigt auch die Digitalisierungsumfrage von ZDH und Bitkom aus 2022. Demnach empfinden 61 Prozent der befragten Betriebe Cybersicherheit als Herausforderung und haben Schwierigkeiten bei der Umsetzung von entsprechenden Maßnahmen. Auch wenn sie sich der Wichtigkeit inzwischen bewusst sind (67 Prozent), sehen sich jedoch viele Unternehmen vor dem Hintergrund der eigenen Betriebsgröße, hoher Auslastung aber auch aufgrund fehlenden Knowhows aber auch fehlender zeitlicher und personeller Ressourcen nicht in der Lage, sich intensiv genug mit dem Thema zu befassen.

Dabei lohnt es sich, sich einmal richtig damit auseinanderzusetzen, entsprechende Vorkehrungen zu treffen und so eine solide Basis zu schaffen. Ernüchternd aber beruhigend zugleich: Es wird keinen 100-prozentigen Schutz geben und Angriffe werden sich nicht vermeiden lassen. Daher ist das Beste, was man tun kann, es dem Angreifer so schwer wie möglich zu machen, die wichtigen Betriebs- und Personendaten bestmöglich zu schützen und vor allem regelmäßig Updates und Backups zu erstellen, um sich vor Erpressung zu schützen und schnellstmöglich wieder einsatzfähig zu sein.

Cybersicherheit ist, genau wie Digitalisierung, ein Prozess und keine einmalige Maßnahme. Mit einfachen ersten Schritten kann sich jeder gut aufstellen, ohne große Vorkenntnisse zu besitzen. Einige der wichtigsten Maßnahmen sind eine Firewall einzurichten, regelmäßige Backups zu ziehen, eine Zwei-Faktor-Authentifizierung einrichten und – vermutlich eine der wichtigsten Maßnahmen – die Mitarbeiter entsprechend zu sensibilisieren und zu schulen, um Berührungsängste abzubauen und eine Atmosphäre des Vertrauens zu schaffen. Denn im Ernstfall kann es entscheidend sein, möglichst schnell die Schwachstelle zu identifizieren und somit unverzüglich handeln zu können.

Es ist hilfreich, wenn die Mitarbeiter des Unternehmens wissen, welche Angriffsmöglichkeiten es gibt und in welchen Situationen sie skeptisch und besonders aufmerksam sein sollten – aber eben auch, was zu tun ist, wenn sie beispielsweise doch mal einen falschen Link angeklickt haben sollten.

Sinn und Zweck der Schutzmaßnahmen ist es, in der digitalen Welt, die Kronjuwelen des Unternehmens zu schützen – also wichtige Informationen und Geschäftsgeheimnisse. Dementsprechend ist es essenziell die Daten zu verschlüsseln und Backups zu ziehen.

Betriebe müssen sich dem Thema nicht allein stellen

Bevor sie sich dem Thema widmen, stehen viele Betriebe erst einmal vor einigen Fragen:

- Welche Maßnahmen sind für den eigenen Betrieb sinnvoll und notwendig?
- Wie und womit können sie anfangen?
- Wie teuer ist Cybersicherheit?
- Wo finden sie Unterstützung?

Es gibt verschiedene Anlaufstellen, die Handwerksbetriebe und mittelständische Unternehmen bei der Identifizierung und Umsetzung von Cybersicherheit in ihrem Betrieb helfen – kostenfrei und anbieterneutral. Zum einen sind hier die Unterstützungsangebote des Bundesamts für Sicherheit in der Informationstechnik zu nennen. Mit der Allianz für Cybersicherheit bietet das BSI Unternehmen und Privatpersonen Ansprechpartner, Checklisten, Veranstaltungen, Informationen und vieles mehr, um sich mit dem Thema auseinanderzusetzen.

Außerdem bietet das Mittelstand-Digital-Netzwerk viel Unterstützung und stellt mit den Mittelstand-Digital Zentren aber auch der Transferstelle für IT-Sicherheit viele verschiedene – ebenfalls kostenfreie Angebote zur Verfügung.

Speziell für das Handwerk hat das Mittelstand-Digital Zentrum Handwerk eine Initiative gegründet, um ihnen den Zugang zu Informationen rund um dieses Thema zu vereinfachen. Die dazugehörige Onlineinformationsplattform ist eine Anlaufstelle, bei der Handwerksbetriebe alles gebündelt finden, was sie benötigen, um ihren Betrieb cybersicher zu machen. Auf *https://cybersicherheit-handwerk.de* finden Betriebe zahlreiche Informationsmaterialien, Leitfäden, geeignete Ansprechpartner und Cybersicherheitsberatende aus der Handwerksorganisation, Hinweise auf die konkret fürs Handwerk passenden Hilfsmittel des BSIs, sowie auch die Angebote aus dem Mittelstand-Digital Kosmos.

Cybersicherheit ist für das Mittelstand-Digital Zentrum Handwerk schon viele Jahre eine Herzensangelegenheit

– stellt sie doch eine wesentliche Grundvoraussetzung dar, wenn Betriebe digitalisieren wollen.

Da bei den mehrheitlich kleinen und Kleinstbetrieben ein enormer Informationsbedarf besteht und damit auch gewisse Berührungsängste mit dem Thema Cybersicherheit einhergehen, wollte das Zentrum ein Angebot schaffen, dass den Betrieben tatsächlich hilft, ihre Fragen beantwortet und ihnen ihre Unsicherheiten nimmt.

Das starke Netzwerk der Initiative besteht aus Cybersicherheitsexperten, die in der Handwerksorganisation angesiedelt sind und Betrieben jeden Gewerks für Fragen und unterstützend zur Verfügung stehen. Bisher verfügt leider nicht jede Handwerkskammer über einen Sicherheitsbotschafter. Aber jeder Betrieb kann sich jederzeit an die bestehenden Berater wenden. Eine Übersicht über die IT-Sicherheitsbotschafter finden Sie auf der Website der Initiative Cybersicherheit Handwerk (*https://cybersicherheit-handwerk.de/Sicherheitsbotschafter*).

Ein wichtiges Ziel der Initiative ist darüber hinaus die Hilfe zur Selbsthilfe. Über verschiedene Weiterbildungen können Betriebe beispielsweise Mitarbeitende zu Digitalen Ersthelfern oder IT-Vorfall-Praktikern qualifizieren lassen. Auf Cybersicherheitstagen haben Betriebe die Gelegenheit, in Workshops Tools, Unterstützungsangebote oder Leitfäden kennenzulernen sowie mit Cybersicherheitsexperten in den direkten Austausch zu treten.

Wie ist die Initiative aufgebaut?

Eine hilfreiche Online-Plattform.
Alles Wichtige auf einen Blick: Hilfe im Notfall, Kontaktmöglichkeiten für alle Sicherheitsfragen, Tipps und Anleitungen zur Prävention und Analyse, Leitfäden, Tools und Unterstützung für die Umsetzung.

Ein starkes Netzwerk.
Ein Netzwerk aus Cybersicherheitsexpertinnen und -experten steht zum Erfahrungsaustausch, Beratung und Wissenstransfer zur Verfügung. Hier können alle voneinander lernen.

Attraktive Netzwerkveranstaltungen.
Auf Cybersicherheitstagen, in Workshops und Schulungen können Sie sich umfassend zum Thema IT-Sicherheit im Handwerk informieren und weiterbilden.

Kollaboration und Wissenstransfer.
In unserer Community können Sie mögliche Hemmnisse rund um die Cybersicherheit abbauen und sich direkt an Expertinnen und Experten aus dem Handwerk wenden.

Schließen Sie sich dem Netzwerk an und profitieren Sie von dem Expertenwissen, Ansprechpartnern und den vielen kostenfreien Angeboten, die Ihnen bei der Umsetzung von Cybersicherheitsmaßnahmen im eigenen Betrieb Unterstützung bieten. Weiterführende Infos zur Initiative: *https://cybersicherheit-handwerk.de*

Das **Mittelstand-Digital Zentrum Handwerk** unterstützt Handwerksbetriebe und Handwerksorganisationen seit 2016 dabei, die Chancen digitaler Technologien, Prozesse und Geschäftsmodelle zu nutzen – kostenfrei, anbieterneutral und deutschlandweit. Es bietet praxisnahe Ratgeber und Seminare, zahlreiche interaktive Tools sowie einen Digitalisierungscheck, der zur digitalen (Weiter-) Entwicklung des eigenen Betriebs dient. Regionale Technologie-Erlebniswelten laden zum Ausprobieren ein, Experten und Expertinnen unterstützen Betriebe mit vielfältigen Innovations- und Umsetzungsformaten und stehen für Fragen bereit. Mit dem monatlichen Newsletter bleiben Handwerksbetriebe informiert.

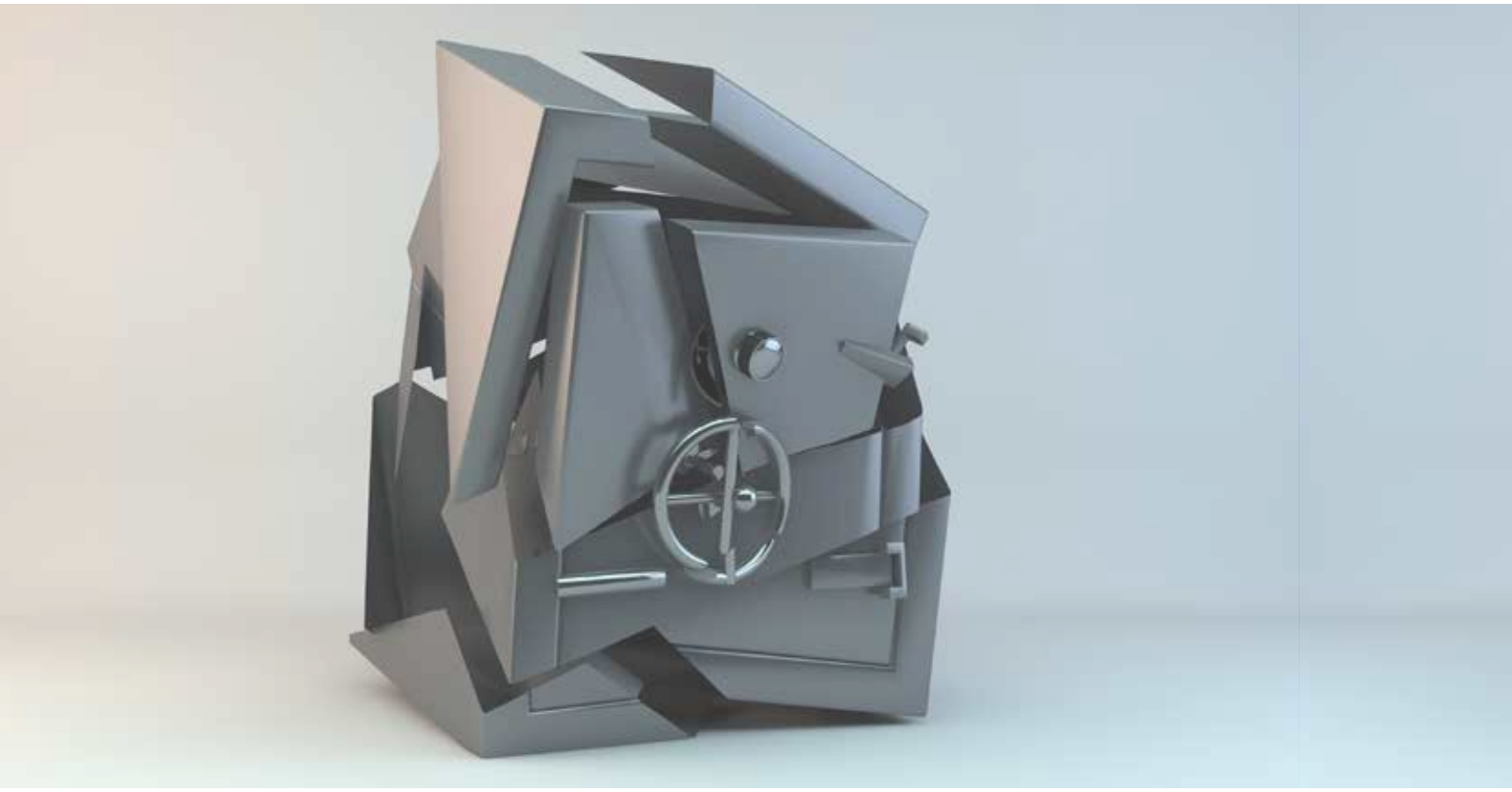
www.handwerkdigital.de

Mittelstand-Digital Zentrum Handwerk

Autorin und Autor

Juliane Haase, Master of Business Communication, studierte Kommunikations- und Wirtschaftswissenschaften an der Hochschule für Technik und Wirtschaft in Berlin und setzt sich seit 2018 beim Zentralverband des Deutschen Handwerks und in ihrer Funktion als stellvertretende Geschäftsleiterin des Mittelstand-Digital Zentrums Handwerk für die Unterstützung von Handwerksbetrieben bei der digitalen Transformation und der Steigerung des Cybersicherheitsniveaus in Deutschland ein.

Stephan Blank, Diplom-Wirtschaftsingenieur und Master of Business Administration (MBA) studierte an der HTW Berlin, der RWTH Aachen und der University of St. Gallen Wirtschaftsingenieurswesen, General Management und Innovationsmanagement. Er ist Referatsleiter für Digitalisierung im Zentralverband des Deutschen Handwerks (ZDH) und Vorsitzender des Fachbeirats der Allianz für Cyber-Sicherheit des BSI. Der Digitalisierungs- und Innovationsexperte gestaltet in seiner Funktion als Geschäftsleiters im Mittelstand-Digital Zentrum Handwerk die digitale Transformation im Handwerk aktiv mit.



Martin Dukek

Bewusst aber unvorbereitet: KMU zwischen IT-Sicherheitsbedarf und Ressourcenmangel – Ein Muddling-Through-Ansatz

In unserer zunehmend vernetzten Welt stehen kleine und mittlere Unternehmen (KMU) vor der Herausforderung, ihre IT-Infrastrukturen gegen immer komplexere Bedrohungen zu schützen. Trotz eines wachsenden Bewusstseins für IT-Sicherheit fehlen oft die notwendigen Ressourcen und Strukturen, um effektive Maßnahmen umzusetzen. Wir am FZI Forschungszentrum Informatik haben in verschiedenen Projekten mit KMU die Erfahrung gemacht, dass KMU deshalb einen „muddling through"-Ansatz verfolgen, bei dem Entscheidungen inkrementell und reaktiv getroffen werden. Dieser Artikel untersucht, wie dieser Ansatz zu fragwürdigen Sicherheitsstrukturen führt, und zeigt auf, wie die Einführung von Informationssicherheitsmanagementsystemen (ISMS) zur Verbesserung beitragen kann. In der Arbeitsgruppe IT-Sicherheit haben wir daher auch einen besonderen Schwerpunkt auf die Einführung von ISMS gelegt, z.B. durch regelmäßige Treffen zu verschiedenen Themen rund um ISMS. Zusätzlich bieten wir über Klima.Neutral.Digital im Rahmen von Klima-Coachings oder ISMS-Coachings Informationen zu den ersten Schritten hin zu einem ISMS an.

Der Muddling-Through-Ansatz: Verständnis und Anwendung in KMU

Der Ausdruck „Muddling Through" wurde vom amerikanischen Politikwissenschaftler Charles E. Lindblom in den 1950er Jahren geprägt. In seinem Aufsatz „The Science of 'Muddling Through'" beschreibt er einen inkrementellen Entscheidungsfindungsprozess, bei dem Organisationen kleine, schrittweise Veränderungen vornehmen, anstatt umfassende strategische Planungen durchzuführen – sie „wurschteln sich durch". Dieser Ansatz ist besonders in Situationen von Unsicherheit und Ressourcenbeschränkungen prävalent.

Kernelemente des „Muddling-Through“:

- **Inkrementelle Entscheidungen**: Anstatt radikale Veränderungen anzustreben, werden kleine Anpassungen vorgenommen.
- **Begrenzte Analyse**: Ressourcen für umfassende Analysen fehlen, daher konzentriert man sich auf unmittelbar relevante Faktoren.
- **Pragmatisches Vorgehen**: Entscheidungen basieren auf praktischer Erfahrung und kurzfristigen Lösungen.

In der Praxis bedeutet dies, dass KMU oft auf akute Probleme reagieren, anstatt proaktiv Strategien zu entwickeln. Sicherheitsmaßnahmen werden implementiert, wenn ein konkreter Bedarf erkannt wird, beispielsweise nach einem Sicherheitsvorfall oder aufgrund externer Anforderungen.

Fragwürdige Sicherheitsstrukturen durch Muddling-Through

Die Anwendung des Muddling-Through-Ansatzes auf die IT-Sicherheitsstrategie eines Unternehmens führt zu fragmentierten, oft unzureichenden Lösungen, die potenziell gefährliche Sicherheitslücken offenbaren. Mehrere Beispiele verdeutlichen, wie sich dieses Vorgehen in KMU manifestiert.

Ein Bereich, in dem Muddling-Through deutlich zu sehen ist, ist das Passwortmanagement. Viele KMU sind sich bewusst, dass sichere Passwörter entscheidend sind, haben jedoch keine durchdachte Strategie, um dieses Wissen in die Praxis umzusetzen. Der Einsatz eines Passwortmanagers, der diese Herausforderung effektiv lösen könnte, wird oft vernachlässigt. Infolgedessen entwickeln Mitarbeitende eigene, nicht immer sichere Lösungen. Sie verwenden zum Beispiel für alle Konten ähnliche Passwörter oder verwenden alte Passwörter mit minimalen Veränderungen wieder. So entsteht das Gefühl von Sicherheit, obwohl die Passwörter jedoch leicht angreifbar sind.

Ein weiteres Problem besteht darin, dass sich die gängige Alltagsweisheit oft auf die Komplexität von Passwörtern konzentriert, z.B. auf die Verwendung von Sonderzeichen. Diese Passwörter sind jedoch aufgrund ihrer unzureichenden Länge leicht zu brechen.

Ein weiteres Beispiel sehen wir in Backups: Viele Unternehmen wissen, dass sie regelmäßige Backups ihrer Daten erstellen müssen, und tun dies auch. Allerdings wird oft übersehen, dass Backups regelmäßig überprüft und getestet werden sollten. In der Praxis kommt es nicht selten vor, dass Unternehmen zwar Backups erstellen, diese aber nie darauf überprüfen, ob sie im Ernstfall tatsächlich funktionsfähig sind. Ein Backup ist jedoch praktisch wertlos, wenn es im Ernstfall versagt. Dabei geben regelmäßige Wiederherstellungstests nicht nur Sicherheit, sondern auch ein Gefühl dafür, wie lange ein Wiederherstellungsvorgang im Ernstfall dauert.

Darüber hinaus fehlt es vielen KMU an klaren Notfallplänen. Das Wissen, dass Phishing-Angriffe eine Bedrohung darstellen, ist weit verbreitet, und einige Unternehmen schulen ihre Mitarbeitenden sogar in diesem Bereich. Doch mangelt es oft an Ansprechpersonen oder klaren Prozessen, wenn ein solcher Angriff tatsächlich stattfindet. Der Notfallplan bleibt fragmentarisch oder nicht existent, was im Ernstfall zu Verzögerungen und Unsicherheiten führen kann.

Ein weiterer kritischer Bereich betrifft die technischen Aspekte der IT-Sicherheit, die häufig nicht ernsthaft behandelt werden, weil sie komplex oder wenig sichtbar sind. Beispielsweise wird die Segmentierung des Netzwerks oft vernachlässigt, obwohl sie ein entscheidender Faktor für die Sicherheit sein kann. Der Grund für diese Versäumnisse liegt oft in der Ressourcenknappheit. Während Schulungen für Mitarbeitende relativ einfach zu organisieren sind, erfordern technische Maßnahmen wie die Netzwerksegmentierung oder die Implementierung von Zwei-Faktor-Authentifizierung spezialisierte Kenntnisse und zusätzliche Investitionen. Auch hier zeigt sich das typische Muddling-Through: Es werden zwar Maßnahmen ergriffen, aber oft nicht in der Tiefe, die notwendig wäre, um echte Sicherheit zu gewährleisten. Abwägungsentscheidungen zu Investitionen werden zugunsten naheliegender Erfolge getroffen.

Der Einfluss des Muddling-Through-Ansatzes auf die IT-Sicherheit in KMU

Der Muddling-Through-Ansatz in der IT-Sicherheit von KMU spiegelt aber nicht ein fahrlässiges oder unorganisiertes Vorgehen wider. Vielmehr zeigt er, wie Unternehmen pragmatisch und effizient versuchen, mit den vorhandenen Mitteln und Kompetenzen das Beste herauszuholen. Es geht darum, im Alltag zurechtzukommen – oft ohne dediziertes IT-Sicherheitspersonal oder ausgiebige Budgets. In vielen Fällen ist es eine Person, die sich IT-Sicherheit „zur Mission“ gemacht hat und damit beginnt, das Thema im Rahmen des Möglichen anzugehen.

Vorteile des Muddling-Through-Ansatzes: Pragmatismus und Notwendigkeit

Effektive Nutzung begrenzter Ressourcen: Viele KMU stehen vor der Herausforderung, dass sie schlicht nicht die Ressourcen für eine umfassende, professionelle

IT-Sicherheitsstrategie haben. Stattdessen greifen sie auf das zurück, was verfügbar ist: vorhandenes Personal, Werkzeuge und Zeit. Der Muddling-Through-Ansatz ermöglicht es ihnen, trotz dieser Einschränkungen handlungsfähig zu bleiben. Sie treffen schrittweise Entscheidungen und ergreifen Maßnahmen, die sofort umgesetzt werden können.

Flexibilität im Geschäftsalltag: Im hektischen Alltag von KMU, wo IT-Sicherheit nicht immer die höchste Priorität hat, erlaubt der Muddling-Through-Ansatz schnelle, bedarfsorientierte Lösungen. Häufig wird erst gehandelt, wenn ein konkretes Problem auftaucht – sei es ein Sicherheitsvorfall oder eine Anforderung durch Kundschaft oder Ähnliche. In solchen Momenten müssen Entscheidungen getroffen werden, ohne dass Zeit für tiefgehende Analysen oder komplexe Planungen bleibt. Der Ansatz passt sich diesen Realitäten des Geschäftsbetriebs an und ermöglicht es Unternehmen, sofort zu reagieren und Lösungen zu finden, die im Alltag funktionieren.

Personalisierte IT-Sicherheitsansätze: In KMU gibt es öfters jemanden, der sich freiwillig der IT-Sicherheit annimmt, auch wenn dies nicht offiziell zu seinem Aufgabenbereich gehört. Diese Person beginnt oft mit kleinen Schritten – etwa indem sie auf einfache Probleme wie Passwortrichtlinien oder regelmäßige Backups aufmerksam macht. Diese individuelle Initiative führt dazu, dass KMU oft eine Basisabsicherung erreichen, auch wenn die Maßnahmen nicht perfekt sind.

Pragmatischer Nutzen kurzfristiger Lösungen: In vielen Fällen führen KMU nur Sicherheitsmaßnahmen ein, die gerade notwendig sind, um konkrete Probleme zu lösen. Diese reaktiven Maßnahmen – ob es das Einführen von Zwei-Faktor-Authentifizierung nach einem Sicherheitsvorfall oder das Schließen einer konkreten Sicherheitslücke ist – wirken direkt und vermeiden unnötige Komplexität.

Nachteile des Muddling-Through-Ansatzes: Langfristige Risiken und Unsicherheit

Fehlende Langfristigkeit und Strategie: Der größte Nachteil des Muddling-Through-Ansatzes ist, dass es oft an einer strategischen Ausrichtung fehlt. Maßnahmen werden kurzfristig und punktuell getroffen, aber es gibt keinen umfassenden Plan, der sicherstellt, dass diese Lösungen auf lange Sicht ineinandergreifen und die Sicherheit des Unternehmens nachhaltig verbessern. Dadurch entstehen oft fragmentierte Strukturen, in denen einzelne Maßnahmen zwar für sich genommen sinnvoll sind, aber nicht systematisch koordiniert werden.

Gefahr von Sicherheitslücken: Weil KMU im Muddling-Through-Ansatz häufig reaktiv und ohne umfassende Analysen agieren, übersehen sie möglicherweise kritische Sicherheitsbereiche. Oft werden nur die Probleme adressiert, die sichtbar oder dringend sind, während weniger offensichtliche, aber potenziell gefährliche Lücken bestehen bleiben.

- **Ineffiziente Ressourcennutzung**: Trotz der pragmatischen Vorteile kann es passieren, dass Unternehmen durch diesen Ansatz Ressourcen nicht optimal nutzen. KMU investieren möglicherweise in Lösungen, die kurzfristig das Problem lösen, aber langfristig ineffizient sind. Ein klassisches Beispiel ist die Einführung neuer Technologien oder Software, die nicht in die bestehende IT-Infrastruktur integriert werden kann, oder die Investition in teure Tools, die nicht effektiv genutzt werden, weil das Fachwissen fehlt.
- **Falsches Sicherheitsgefühl**: Der Muddling-Through-Ansatz kann KMU ein falsches Gefühl der Sicherheit geben. Unternehmen glauben möglicherweise, ausreichend geschützt zu sein, weil sie reaktiv Maßnahmen ergriffen haben. Dabei werden oft grundlegende Sicherheitsaspekte übersehen oder Maßnahmen nur unvollständig umgesetzt.
- **Fehlende Fachexpertise**: Diejenigen, die sich dem Thema IT-Sicherheit widmen, tun dies häufig ohne tiefere Expertise und verlassen sich dabei auf Alltagsweisheiten oder das, was allgemein als gute Praxis gilt. Ein häufiges Beispiel ist der Umgang mit Passwörtern.

Der Muddling-Through-Ansatz ist kein Zeichen von Nachlässigkeit, sondern ein pragmatischer Versuch von KMU, mit den ihnen zur Verfügung stehenden Mitteln das Beste in Sachen IT-Sicherheit zu erreichen. Er erlaubt es Unternehmen, trotz begrenzter Ressourcen handlungsfähig zu bleiben und auf akute Probleme schnell zu reagieren. Allerdings bringt dieser Ansatz auch langfristige Risiken mit sich. Der Schlüssel liegt darin, diesen pragmatischen Ansatz mit strategischen Elementen zu ergänzen – etwa durch ein einfaches, aber wirksames IT-Risikomanagement oder die schrittweise Implementierung eines ISMS das eine gewisse Struktur und Richtung bietet, ohne die Flexibilität und den Pragmatismus des Muddling-Through-Ansatzes aufzugeben.

ISMS als strukturierende Lösung: Mehr Ordnung im Muddling-Through

Ein ISMS kann dabei helfen, den Muddling-Through-Ansatz zu strukturieren, ohne ihn vollständig zu ersetzen. KMU stehen oft vor der Realität, dass sie nicht die Ressourcen haben, um sofort umfassende IT-Sicherheitsstrategien umzusetzen. Ein ISMS bietet jedoch eine Möglichkeit, schrittweise Verbesserungen auf eine strukturierte und nachvollziehbare Weise umzusetzen.

ISMS als Rahmenwerk für IT-Sicherheit

Ein ISMS stellt sicher, dass IT-Sicherheitsmaßnahmen nicht nur inkrementell, sondern auch systematisch und kohärent eingeführt werden. Es bietet klare Vorgaben, welche Maßnahmen in welcher Reihenfolge umgesetzt werden sollten, und ermöglicht es KMU. Damit gibt es dem Muddling-Through-Ansatz einen Rahmen, der dazu beiträgt, dass jede schrittweise Verbesserung Teil einer größeren Sicherheitsstrategie wird.

Vorteile eines ISMS für KMU

Ein ISMS strukturiert den Prozess der IT-Sicherheit in mehreren wichtigen Bereichen:

- **Verantwortlichkeiten**: Ein ISMS legt klar fest, wer für welche Sicherheitsmaßnahmen verantwortlich ist. Das bedeutet, dass nicht mehr ad-hoc oder nebenbei Entscheidungen getroffen werden, sondern klare Zuständigkeiten definiert sind.
- **Risikomanagement**: Durch die systematische Bewertung von Risiken hilft ein ISMS dabei, die drängendsten Sicherheitslücken zu identifizieren und Prioritäten zu setzen. Anstatt nur reaktiv zu handeln, können KMU gezielt in die Bereiche investieren, die das größte Sicherheitsrisiko darstellen.
- **Kontinuierliche Verbesserung**: Ein ISMS verlangt regelmäßige Überprüfungen und Anpassungen der Sicherheitsmaßnahmen. Dies bedeutet, dass KMU nicht nur auf aktuelle Bedrohungen reagieren, sondern auch proaktiv Sicherheitslücken schließen und ihre IT-Sicherheit langfristig verbessern können.

Leitfäden, Best Practices und technische Richtlinien als unterstützende Elemente

Neben einem ISMS sind einfach zugängliche Leitfäden und Best Practices entscheidend, um KMU den Einstieg in die IT-Sicherheit zu erleichtern. Solche Leitfäden bieten praxisnahe, umsetzbare Schritte, die an den Muddling-Through-Ansatz anknüpfen und ihn gleichzeitig auf eine fundiertere Basis stellen. Diese Leitfäden sind speziell für Unternehmen nützlich, die nicht über die tiefere Fachexpertise verfügen und ihre IT-Sicherheit schrittweise und ohne Überforderung verbessern wollen.

- **Umsetzung praxisnaher Sicherheitsmaßnahmen**: Sie bieten einfach verständliche, umsetzbare Lösungen für konkrete Probleme wie Passwortmanagement, Netzwerksegmentierung oder Backups und greifen dabei bestehende Alltagspraktiken auf. Dadurch werden gängige Missverständnisse – wie der übermäßige Fokus auf Passwortkomplexität ohne Berücksichtigung der Länge – korrigiert.
- **Handlungsorientierte Tipps**: Gerade im IT-Sicherheitsbereich sind konkrete Handlungsempfehlungen essenziell. Leitfäden, die Schritt-für-Schritt-Lösungen bieten, wie zum Beispiel die Implementierung einer Zwei-Faktor-Authentifizierung oder das Testen von Backups, machen es KMU einfacher, sofortige und sinnvolle Sicherheitsmaßnahmen zu ergreifen, ohne dass umfassende IT-Kenntnisse notwendig sind.

Leitfäden und Best Practices bieten zwar wertvolle Hilfestellung, reichen jedoch oft nicht aus, um die komplexen Anforderungen der IT-Sicherheit vollständig abzudecken. KMU stehen vor Herausforderungen, die über einfache Anleitungen hinausgehen. Zum einen fehlt oft die Fähigkeit, spezifische Bedrohungen richtig einzuschätzen und die richtigen Maßnahmen aus den allgemeinen Empfehlungen auszuwählen. Zum anderen können Leitfäden nur begrenzt auf individuelle Bedürfnisse eingehen, die je nach Unternehmensstruktur und IT-Landschaft stark variieren. Ohne fachkundige Unterstützung bleiben viele Unternehmen bei der Implementierung oft stecken oder setzen Maßnahmen unvollständig um. Deshalb bieten wir über Klima.Neutral.Digital eine Begleitung durch unser Fachpersonal an.

Im Rahmen des ISMS-Coachings unterstützen wir KMU bei der Auswahl der passenden Leitfäden und beantworten erste Fragen zu einem ISMS, um den Einstieg zu erleichtern. Die Klima-Coaches des Mittelstand-Digital Zentrums Klima.Neutral.Digital begleiten Unternehmen zusätzlich auf ihrem Weg zur Klimaneutralität und informieren unabhängig sowie anbieterneutral über Digitalisierungslösungen, die sowohl Nachhaltigkeits- als auch IT-Sicherheitsaspekte berücksichtigen. Dabei wird besonderer Wert auf den Schutz digitaler Infrastrukturen gelegt.

Zusätzlich bieten wir spezialisierte KI-Trainer mit IT-Sicherheitsfachkenntnissen, die KMU bei der Bewältigung von Unsicherheiten und Unklarheiten in Bezug auf Künstliche Intelligenz und IT-Sicherheit unterstützen. Sie helfen dabei, die Potenziale von KI sicher zu nutzen und gleichzeitig Sicherheitsrisiken zu minimieren.

Die Herausforderung: Muddling-Through und zunehmende Digitalisierung

Mit der fortschreitenden Digitalisierung steigen auch die Anforderungen an die IT-Sicherheit. Digitale Projekte – sei es die Einführung neuer Softwarelösungen, die Nutzung von Cloud-Diensten oder die Automatisierung von Geschäftsprozessen – schaffen zusätzliche Angriffsflächen und erhöhen die Komplexität der Sicherheitsanforderungen.

Hier wird der Muddling-Through-Ansatz zu einer noch größeren Gefahr, da Sicherheitslücken, die in einer weniger digitalisierten Umgebung vielleicht weniger gravierend waren, nun ernste Konsequenzen haben können. Ein Unternehmen, das sich im Rahmen eines Digitalisierungsprojekts stärker auf cloudbasierte Lösungen verlässt, riskiert ohne ein klares ISMS, dass Sicherheitsfragen wie die Zugriffssteuerung oder die Verschlüsselung nicht ausreichend bedacht werden. Dies kann zu gravierenden Sicherheitsvorfällen führen, die das Unternehmen sowohl finanziell als auch in ihrer Reputation schwer schädigen können.

Autor

Martin Dukek ist seit 2023 wissenschaftlicher Mitarbeiter am FZI Forschungszentrum Informatik und arbeitet dort im Themenfeld Angewandte Sicherheit. Im Rahmen von Klima.Neutral.Digital ist er für das Themenfeld IT-Sicherheit verantwortlich und koordiniert die AG IT-Sicherheit.
Seine Interessens- und Forschungsschwerpunkte liegen in den Bereichen Penetration Testing und Epistemologie der IT-Sicherheit.

Das **Mittelstand-Digital Zentrum Klima.Neutral.Digital** unterstützt kleine und mittlere Unternehmen sowie das Handwerk dabei, die ersten Schritte in die Klimaneutralität zu gehen. Die Digitalisierung spielt dabei eine entscheidende Rolle, um Ressourcen zu schonen, Prozesse zu optimieren und zukunftsfähig zu sein. Klima.Neutral.Digital bietet dafür ein breites Spektrum an Informationsveranstaltungen, von Laborführungen und Demonstratorpräsentationen über Webinare und Barcamps bis hin zu vertiefenden Workshops. Zudem bietet das Zentrum den KMU die Möglichkeit, unterstützt durch die KI-Trainer und Klima-Coaches Maßnahmen in Digitalisierungsprojekten umzusetzen.

Die Themenschwerpunkte des Zentrums sind:

- Nachhaltigkeit
- Sensorik, Smarte Systeme und Digitale Prozesse für ressourcenschonende Produktion
- Nachhaltige Energiesysteme
- Digitale Geschäftsmodelle
- Digitale Produktentwicklung
- KI
- IT-Sicherheit

www.klima-neutral-digital.de

Mittelstand-Digital Zentrum Klima.Neutral.Digital

Jan Fischer, Axel Wagenitz

Generative KI und Cybersecurity: Wissenschaft trifft Praxis

Generative KI und Deepfake-Technologien bringen neue Herausforderungen für die Cybersicherheit mit sich. Durch täuschend echte Video- und Audiofälschungen können Angreifer in die Identität von Führungskräften oder Mitarbeitern schlüpfen und unerlaubte Transaktionen auslösen oder sensible Daten abgreifen. Die Weiterentwicklung dieser Technologien macht es notwendig, durch gezielte Mitarbeiterschulungen und Sicherheitsprozesse ein Bewusstsein für diese Risiken zu schaffen.

Einleitung

Das Telefon klingelt, und der Buchhaltungsmitarbeiter seufzt – ein Anruf kurz vor Feierabend. Zögernd nimmt er ab; auf dem Bildschirm erscheint ein Video: Die Geschäftsführerin, ernst und gestresst. Sie sei im Ausland, es gebe ein Problem. Ein wichtiger Deal drohe zu platzen. „Wir müssen heute noch eine Überweisung machen."

Die Verbindung knistert, das Bild flackert, aber die Stimme ist unverkennbar. Kein Zweifel, es ist die Chefin. Der Mitarbeiter nickt, versucht zu begreifen, was auf dem Spiel steht. „Wir reden hier von Millionen", fügt die Geschäftsführerin hinzu, ihr Blick durchdringend. Alles hänge davon ab.

Das Gespräch endet abrupt, und sofort erscheint eine E-Mail. Der Mitarbeiter öffnet sie, seine Hände zittern leicht. Kontodaten, Betrag – alles ist klar und präzise aufgelistet. Es bleibt keine Zeit für Fragen, keine Zeit, das Gesagte zu hinterfragen. Die Stimme war authentisch, die Dringlichkeit echt – die Geschäftsführerin hat es angeordnet, und es gibt keine Zeit zu verlieren.

Was der Mitarbeiter nicht weiß: Am anderen Ende der Leitung saß nicht die Geschäftsführerin. Es war eine Künstliche Intelligenz (KI), ein Deepfake, der mit erschreckender Präzision Stimme und Gesicht imitiert hat. Ein perfekt orchestrierter Betrug, der in wenigen Minuten Millionen aus dem Unternehmen schleust.

Diese Geschichte ist fiktiv, doch genau so oder ähnlich kann es in der Realität passieren. Anfang 2024 wurde ein internationaler Konzern Opfer eines solchen Deepfake-Betrugs. Kriminelle inszenierten eine täuschend echte Videokonferenz, in der sie Stimmen und Gesichter von Führungskräften nachahmten. Der Druck war groß, die Situation schien dringend, und so gelang es ihnen, 24 Millionen Euro zu erbeuten. Der Mitarbeiter, der die Überweisung vornahm, hatte keine Chance, den Betrug zu erkennen.[1]

Doch nicht immer sind solche Angriffe erfolgreich. Im Frühjahr 2024 geriet Ferrari ins Visier von Betrügern. Ein Topmanager erhielt WhatsApp-Nachrichten und sogar einen Anruf von einer KI, die Stimme und Akzent des Ferrari-CEOs Benedetto Vigna perfekt imitierte. Doch der Manager war misstrauisch. Kleine Unstimmigkeiten in der Sprechweise ließen ihn aufhorchen, und er stellte eine Fangfrage. Der Betrug flog auf, bevor Schaden angerichtet werden konnte. Dieser Fall zeigt, wie täuschend echt solche Deepfake-Angriffe inzwischen sein können und wie knapp Unternehmen oft an einem Desaster vorbeischrammen.[2] Für kleine und mittlere Unternehmen (KMU) ist es daher entscheidend, sich der Risiken bewusst zu sein und geeignete Sicherheitsmaßnahmen zu ergreifen.[3]

Das „Business Innovation Lab" (BIL) der HAW Hamburg, als Teil des Mittelstand-Digital Zentrums Hamburg, untersucht und testet die Potenziale und Gefahren von Technologien wie Deepfakes und anderen generativen KI-Anwendungen. Ziel ist es, Unternehmen fundierte Einschätzungen zu möglichen Risiken und Nutzen dieser Technologien zu geben. Neben den Gefahren durch Missbrauch gibt es aber auch positive Einsatzszenarien. So können KMU generative KI nutzen, um beispielsweise automatisierte Produktvideos oder multilinguale Onboarding-Videos zu entwickeln. Durch praxisnahe Forschung und realitätsnahe Szenarien bietet das BIL KMU wertvolle Einblicke und unterstützt sie dabei, sich besser gegen Bedrohungen zu schützen und gleichzeitig innovative Anwendungen gewinnbringend zu nutzen.

Deepfakes: Die Kunst der digitalen Täuschung

Ursprünglich beschrieb der Begriff Deepfakes lediglich der Erstellung von KI-generierten Bildern. Mittlerweile sind damit jedoch auch täuschend echte Audio- und Videoaufnahmen gemeint. Deepfakes basieren auf Deep-Learning-Algorithmen, die Mimik, Gestik oder die Stimme einer Person analysieren und verblüffend realistisch reproduzieren können.[4] Kriminelle nutzen diese Fortschritte, um in die Rolle von Geschäftsleitung, Mitarbeitern oder anderen Vertrauenspersonen zu schlüpfen. So können sie unbemerkt unbefugte Transaktionen durchführen oder auf sensible Daten zugreifen. Die Auswirkungen sind gravierend: Identitätsbetrug, Industriespionage und finanzieller Schaden sind nur einige der möglichen Konsequenzen.[5]

Früher waren minutenlanges Videomaterial und stundenweise Audioaufnahmen erforderlich, um realistische Fälschungen zu erstellen. Heute sind moderne Deep-Learning-Modelle in der Lage, mit nur einem oder wenigen Bildern einen einigermaßen realistischen Deepfake zu erzeugen. Ebenso können sie innerhalb weniger Sekunden die Stimme einer Person klonen. Die Erstellung hochwertiger Deepfakes war einst mit großem technischem Aufwand und hohen Kosten verbunden, die erhebliche Rechenleistung erforderten. Mittlerweile sind benutzerfreundliche Tools frei verfügbar, und kommerzielle Dienste bieten Deepfake-Software an, die auch auf normaler Verbraucher-Hardware läuft. Dadurch ist es nun auch technisch weniger versierten Personen möglich, täuschend echte Fälschungen zu erstellen.[6]

Automatisierte Phishing-Angriffe: Massenhafte Täuschung

Generative KI eröffnet Cyberkriminellen neue Möglichkeiten bei klassischen Phishing- und Spear-Phishing-Angriffen. Sie können personalisierte Phishing-Angriffe in großem Maßstab automatisieren und so massenhaft täuschen. Die durch Large Language Models (LLMs) generierten E-Mails wirken täuschend echt, weil sie individuell auf die jeweiligen Empfänger zugeschnitten werden können.[7] Ein alarmierendes Beispiel ist der 135%ige Anstieg von Spam-Mails mit verbesserter Grammatik und Syntax, der auf den Einsatz generativer KI zurückzuführen ist.[8]

Neben E-Mails setzen Kriminelle auch automatisierte Telefonanrufe ein. Dabei verwenden sie synthetische Stimmen, um sensible Informationen zu erlangen – ein Vorgehen, das als Voice Phishing (Vishing) bezeichnet wird.[9]

WormGPT: Large Language Models für schnelle Malware-Entwicklung

Die Produktivitätsgewinne durch Large Language Models wie ChatGPT kommen nicht nur Unternehmen zugute, sondern auch Cyberkriminellen. Bereits 2021

1 Hurtz (2024).
2 Brien (2024).
3 Bundesamt für Sicherheit in der Informationstechnik (2022).
4 Perov et al. (2022); Mirsky et al. (2021); Bovenschulte (2019).
5 Bundesamt für Sicherheit in der Informationstechnik (2022); Mirsky et al. (2021); Dash und Sharma (2023).
6 Bovenschulte (2019).
7 Falade (2023); Mirsky et al. (2021); Neupane et al. (2023).
8 Neupane et al. (2023).
9 Falade (2023); Neupane et al. (2023).

tauchte WormGPT in Darknet-Foren auf; es soll speziell für die Entwicklung von Schadsoftware entwickelt worden sein. Im Gegensatz zu ethisch ausgerichteten Modellen bietet es uneingeschränkte Möglichkeiten zur Erstellung schädlicher Inhalte.[10] Mit der Weiterentwicklung immer besserer freiverfügbarer Modelle ist davon auszugehen, dass auch die Qualität und Vielfalt der Malware steigen wird.

Visuelle Deepfakes: Funktionsweise und Technologien

Die Erstellung visueller Deepfakes basiert auf verschiedenen KI-Technologien, darunter Autoencoder, Generative Adversarial Networks (GANs) und Diffusionsmodelle.

Autoencoder

Autoencoder sind neuronale Netze, die darauf trainiert werden, Daten zu komprimieren und wiederherzustellen. Für Deepfakes werden zwei Autoencoder eingesetzt: einer mit Bildern der Zielperson, also der Person, deren Gesicht im Video erscheinen soll, und einer mit Bildern der Originalperson aus dem ursprünglichen Video.

Der Prozess funktioniert folgendermaßen: Der Encoder wandelt das Gesicht der Originalperson in eine komprimierte Darstellung um. Anstatt diese Daten mit dem eigenen Decoder zu rekonstruieren, wird der Decoder der Zielperson verwendet. So entsteht ein Gesichtstausch, bei dem das Gesicht der Originalperson durch das der Zielperson ersetzt wird. Das Ergebnis ist ein Video, in dem die Zielperson scheinbar die Mimik und Lippenbewegungen der Originalperson ausführt, was den täuschend echten Effekt des Deepfakes erzeugt.[11] Möchte man hochqualitative Deepfakes wie in der Filmindustrie erzeugen, benötigt man in der Regel eine große Menge an Trainingsdaten. Tausende von Bildern oder Stunden an Rohvideomaterial sind nötig, damit die KI die Mimik, Gestik und andere Details einer Person präzise erlernen kann. Zusätzlich ist eine Trainingszeit von mehreren Tagen bis Wochen erforderlich, um diese hochauflösenden Deepfakes zu erstellen. Aufgrund des enormen Rechenaufwands sind solche Deepfakes oft nicht in Echtzeit nutzbar.[12]

Für eine Online-Videokonferenz mit begrenzter Qualität ist der Aufwand jedoch geringer. Hier können oft nur wenige Minuten Videomaterial oder sogar ein einzelnes Bild ausreichen. Das Training eines solchen Modells kann in wenigen Stunden bis zu einem Tag abgeschlossen sein.

Generative Adversarial Networks (GANs)

Es gibt auch Systeme, die kein spezielles weiterführendes Training benötigen. Einmal auf eine Vielzahl von Gesichtern trainiert, können diese Modelle in Echtzeit ein Deepfake eines bisher ungesehenen Gesichts erstellen. GANs bestehen aus zwei neuronalen Netzen: dem Generator und dem Diskriminator. Der Generator versucht, realistische Daten zu erzeugen, während der Diskriminator echte von gefälschten Daten zu unterscheiden versucht. Dieser Wettbewerb führt dazu, dass der

10 Falade (2023).

11 Perov et al. (2022).
12 Perov et al. (2022).

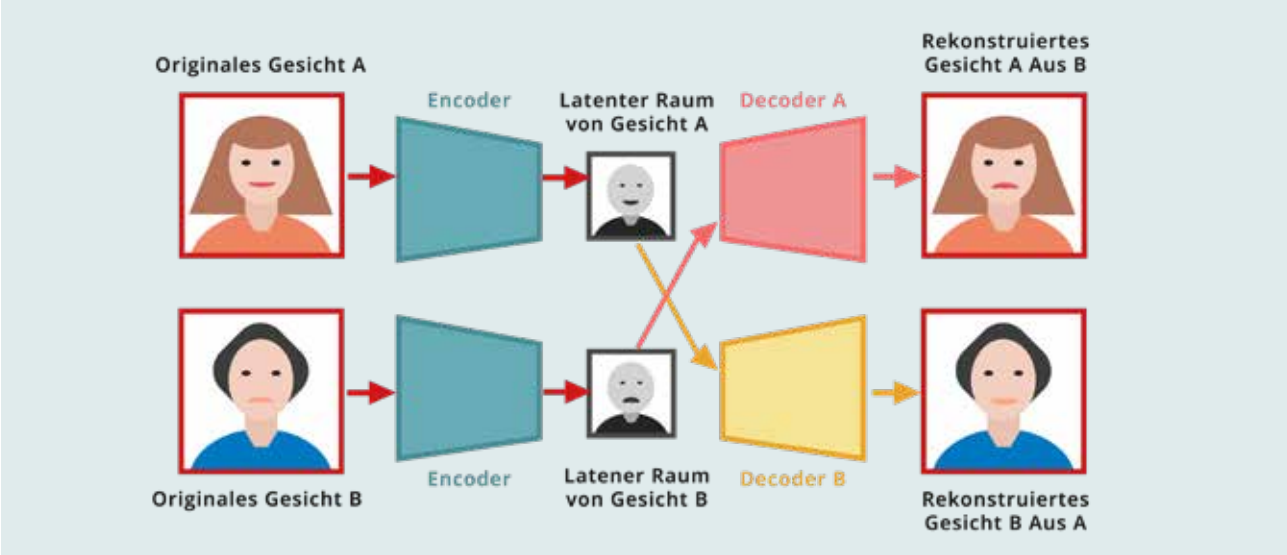


Abbildung 1: Deepfake mittels Autoencoder

Generator immer bessere und realistischere Deepfakes erstellt.[13] Aufgrund des fehlenden speziellen Trainings weist das erzeugte Bild meist weniger Ähnlichkeit zum Original auf. Um Echtzeit-Fakes erstellen zu können, ist die Auflösung dieser Modelle oft zu gering.

Diffusionsmodelle

Diffusionsmodelle sind eine neuere Technologie, die hochrealistische Bilder erzeugen kann, indem sie den Prozess der Datenzerstörung umkehrt. Sie fügen zunächst Rauschen zu den Daten hinzu und trainieren dann ein neuronales Netzwerk, dieses Rauschen wieder in klare, realistische Bilder zu verwandeln. Diese Modelle sind in der Lage, äußerst komplexe und detailreiche Bild-Deepfakes zu erzeugen.[14] Allerdings ist der Prozess derzeit noch recht aufwendig, und es gibt bisher keine praktikablen, frei verfügbaren Echtzeit-Anwendungen für Videos. Es ist jedoch zu erwarten, dass sich diese Technologie weiterentwickeln wird und in Zukunft realistische Echtzeit-Videoanwendungen möglich sein könnten – ähnlich wie wir es bereits von Video-Generatoren wie OpenAI's Sora sehen.

Funktionsweise von Voice Deepfakes

Voice Deepfakes oder genauer gesagt Voice Cloning nutzen KI-Modelle, die Sprachaufnahmen analysieren, um die einzigartigen Merkmale einer Stimme zu erlernen – wie Tonhöhe, Sprachmelodie und Rhythmus. Mit diesen Informationen erzeugen sie neue Sprachdaten, die der Originalstimme sehr ähnlich sind. Die meisten modernen Voice-Cloning-Systeme basieren auf einer speziellen Art von Autoencoder.

Variational Autoencoder (VAE)

Variational Autoencoder bestehen ebenfalls aus einem Encoder-Decoder-Paar. Der Encoder nimmt die Sprachaufnahme und extrahiert daraus die charakteristischen Merkmale der Stimme. Diese Merkmale werden in einem komprimierten Code, dem sogenannten latenten Raum, gespeichert. Der Decoder nutzt diesen Code, um eine neue Audioausgabe zu erzeugen, die der Originalstimme entspricht. Der Encoder des VAE strukturiert den latenten Raum so, dass er nicht nur die Stimme klonen, sondern auch neue Variationen der Stimme erzeugen kann. Dadurch kann der VAE die Originalstimme nicht nur imitieren, sondern sie auch in verschiedenen Stilen und Nuancen reproduzieren, was ihm eine größere Flexibilität verleiht.[15]

13 Dash und Sharma (2023).
14 Bhattacharyyaet al. (2024).
15 Casanova et al. (2024); Bird und Lotfi (2023); Kim et al. (2021).

Früher benötigten solche Systeme viel Rechenzeit und Stunden an Aufnahmen, um eine Stimme realistisch zu klonen. Die Ausgaben klangen oft noch "mechanisch" oder verzerrt. Heute genügen bereits Minuten oder sogar wenige Sekunden, um täuschend echte Stimmklone zu erzeugen. Neben kommerziellen Anbietern, die Voice Cloning als kostengünstige Dienstleistung für automatische Voice-Overs oder Videoübersetzungen anbieten, gibt es auch frei verfügbare Software. Die synthetischen Stimmen können in Echtzeit erzeugt werden, direkt während eines Gesprächs in Telefonaten oder Videokonferenzen.[16]

KI-gestützte Phishing-Angriffe: Funktionsweise

KI-gestützte Phishing-Angriffe nutzen Large Language Models wie ChatGPT, um personalisierte und überzeugende Phishing-Nachrichten zu erstellen. Automatisierte Systeme durchsuchen das Internet und soziale Netzwerke nach Informationen über Unternehmen und deren Mitarbeiter – wie Namen, Positionen und E-Mail-Adressen. Selbst scheinbar unwichtige Details werden verwendet, um spätere Phishing-Nachrichten authentischer zu gestalten.[17] Mit diesen Daten erstellen LLMs personalisierte E-Mails und Nachrichten, die täuschend echt wirken und mit passenden Ansprachen und Themen versehen sind.[18] Dadurch können Cyberkriminelle in Echtzeit massenhafte Phishing-Kampagnen durchführen, was die Effizienz und den potenziellen Schaden solcher Angriffe steigert.[19]

Gegenmaßnahmen – Praktische Ansätze für KMU

Um sich vor den Gefahren von KI-unterstützten Cyberangriffen wie Deepfakes und Phishing zu schützen, müssen Unternehmen proaktiv handeln. Diese Bedrohungen lassen sich nicht allein durch technische Lösungen abwehren; sie erfordern gezielte Mitarbeiterschulungen und Sensibilisierung.

Es gibt zwar Softwarelösungen, die speziell zur Erkennung von Deepfakes entwickelt wurden.[20] Doch dies ist ein ständiges Katz-und-Maus-Spiel zwischen Angreifern und Detektoren, und die Wirksamkeit dieser Systeme ist in der Praxis oft unzuverlässig. Daher ist es ratsam, die öffentliche Verfügbarkeit von Bildern und Videos von Mitarbeitern und Führungskräften zu minimieren, um weniger Angriffsfläche für Deepfakes zu bieten. Unternehmenswebseiten und soziale Netzwerke sollten regelmäßig

16 Bird und Lotfi (2023).
17 Neupane et al. (2023).
18 Neupane et al. (2023); Dash und Sharma (2023).
19 Mirsky et al. (2021).
20 Pei et al. (2024).

überprüft werden, um sensible Materialien zu entfernen oder den Zugang zu beschränken. Sensible Informationen sollten nicht öffentlich zugänglich sein, und der Zugriff auf solche Daten sollte streng kontrolliert und nur autorisierten Personen gewährt werden.[21] Ein bewusster Umgang mit Daten kann potenzielle Deepfake- oder Spear-Phishing-Angriffe bereits im Vorfeld erschweren.

Der wichtigste Schutz ist die Schulung der Mitarbeiter: Sie sollten über die Existenz, Funktionsweise und Risiken von Deepfakes und Phishing aufgeklärt werden. Durch regelmäßige Sensibilisierung sind sie besser darauf vorbereitet, verdächtige Inhalte zu erkennen. Ungewöhnliches Verhalten – wie ein abweichendes Profilbild, mangelnde Interaktion oder ein abruptes Beenden des Gesprächs – sollte als potenzielles Warnsignal erkannt werden. Im Zweifelsfall ist es ratsam, gezielte Fragen zu stellen, die nur die echte Person beantworten kann. E-Mails und Anrufe, vor allem aus unbekannten Quellen, sollten kritisch betrachtet und nicht sofort vertraut werden. KMU sollten klare Prozesse zur Identitätsprüfung von Anrufern und Videokonferenzteilnehmern etablieren, um sich vor KI-unterstützten Angriffen zu schützen. Besonders bei sensiblen Themen oder finanziellen Transaktionen ist es wichtig, eine zusätzliche Sicherheitsebene einzuführen.[22] Beispielsweise können festgelegte Sicherheitsfragen oder Codewörter genutzt werden, um die Identität des Gesprächspartners zu verifizieren. Zusätzlich können einfache Methoden angewendet werden, um Deepfake-Systeme zu stören. Viele dieser Systeme nutzen Gesichtserkennung, bei der die Software die Position des Gesichts im Bild erkennt, um es anschließend manipulieren zu können. Sie funktionieren oft nicht richtig, wenn das Gesicht verdeckt wird oder man die gespreizten Finger langsam vor dem Gesicht vorbeiführt, im Zweifel müssen Mitarbeiter ihre Gesprächspartner dazu auffordern, um den Deepfake zu entlarven. Diese Methode, die auch bei Online-Identifizierungsverfahren von Banken eingesetzt wird, bietet jedoch keinen vollständigen Schutz, da fortgeschrittene Deepfake-Modelle solche Störungen umgehen könnten.

Fazit

Die rasante Entwicklung von generativer KI und Deepfake-Technologien stellt eine erhebliche Gefahr für die Cybersicherheit dar. Von täuschend echten Video- und Audioaufnahmen bis hin zu KI-gestützten Phishing-Angriffen – die Möglichkeiten für Cyberkriminelle, Unternehmen zu schädigen, nehmen stetig zu. Diese Technologien haben nicht nur die Qualität von Angriffen verbessert, sondern auch die Eintrittsbarriere für weniger versierte Täter gesenkt.

Die Bedrohung durch Deepfakes und automatisierte Phishing-Angriffe zeigt, dass technische Lösungen allein nicht ausreichen. Besonders KMU müssen auf Mitarbeiterschulungen und ein erhöhtes Bewusstsein setzen. Nur durch gezielte Sensibilisierung und die Einführung klarer Sicherheitsprozesse kann man sich effektiv gegen diese Art von Angriffen schützen.

Obwohl spezialisierte Softwarelösungen zur Erkennung von Deepfakes existieren, bleibt der Kampf zwischen Angreifern und Verteidigern ein fortwährendes Katz-und-Maus-Spiel. Deshalb ist es entscheidend, proaktiv zu handeln – sei es durch die Kontrolle öffentlich verfügbarer Informationen oder durch die Entwicklung eines gesunden Misstrauens gegenüber ungewöhnlichen Anfragen. Letztlich liegt der Fokus darauf, die menschlichen Faktoren zu stärken. Geschulte und aufmerksame Mitarbeiter machen den entscheidenden Unterschied im Kampf gegen KI-gestützte Cyberangriffe aus.

Das Mittelstand-Digital Zentrum Hamburg bietet KMU Unterstützungsangebote zu generativen KI-Technologien. Diese umfassen Beratungen zur Identifikation von Risiken und Entwicklung von Schutzstrategien, aber auch Schulungen, um die Potenziale der Technologien im Bereich Kundenkommunikation und Marketing zu nutzen.

21 Neupane et al. (2023).
22 Bundesamt für Sicherheit in der Informationstechnik (2022).

Literatur

Bhattacharyya C, Wang H, Zhang F, Kim S, Zhu X. Diffusion Deepfake [Internet]. arXiv.org. 2024 [cited 2024 Sep 19]. Available from: https://arxiv.org/abs/2404.01579v1

Bird JJ, Lotfi A. Real-time Detection of AI-Generated Speech for DeepFake Voice Conversion [Internet]. arXiv.org. 2023 [cited 2024 Sep 19]. Available from: https://arxiv.org/abs/2308.12734v1

Bovenschulte M. Deepfakes – Manipulation von Filmsequenzen. 2019 Jan 1 [cited 2024 Sep 19]; Available from: https://publikationen.bibliothek.kit.edu/1000133910

Brien J. KI-Deepfake-Betrug gescheitert: Ferrari-Manager stellt entscheidende Frage [Internet]. t3n Magazin. t3n Magazin; 2024 [cited 2024 Sep 19]. Available from: https://t3n.de/news/ki-deepfake-betrug-ferrari-manager-entscheidene-frage-1638005/

Bundesamt für Sicherheit in der Informationstechnik [Internet]. Bundesamt für Sicherheit in der Informationstechnik. BSIWEB; 2022 [cited 2024 Sep 19]. Available from: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html

Casanova E, Davis K, Gölge E, Göknar G, Gulea I, Hart L, et al. XTTS: a Massively Multilingual Zero-Shot Text-to-Speech Model [Internet]. arXiv.org. 2024. Available from: https://arxiv.org/abs/2406.04904

Dash B, Sharma P. Are ChatGPT and Deepfake Algorithms Endangering the Cybersecurity Industry? A Review. IJEAS. 2023;10(1). doi: 10.31873/IJEAS.10.1.01.

Falade P. Decoding the Threat Landscape : ChatGPT, FraudGPT, and WormGPT in Social Engineering Attacks. J Sci Res Comput Sci Eng Inf Technol [Internet]. 2023;9(5):185–98. Available from: https://arxiv.org/ftp/arxiv/papers/2310/2310.05595.pdf

Hurtz S. Deepfake-Betrug: Angestellter überweist 24 Millionen Euro ins Nichts [Internet]. Süddeutsche.de. Süddeutsche Zeitung; 2024 [cited 2024 Sep 19]. Available from: https://www.sueddeutsche.de/wirtschaft/deepfake-betrug-videokonferenz-hong-kong-1.6344209

Kim J, Kong J, Son J. Conditional Variational Autoencoder with Adversarial Learning for End-to-End Text-to-Speech [Internet]. arXiv.org. 2021 [cited 2024 Sep 19]. Available from: https://arxiv.org/abs/2106.06103v1

Mirsky Y, Demontis A, Kotak J, Shankar R, Gelei D, Yang L, et al. The Threat of Offensive AI to Organizations [Internet]. arXiv.org. 2021 [cited 2024 Sep 19]. Available from: https://arxiv.org/abs/2106.15764

Neupane S, Fernandez IA, Mittal S, Rahimi S. Impacts and Risk of Generative AI Technology on Cyber Defense [Internet]. arXiv.org. 2023 [cited 2024 Sep 19]. Available from: https://arxiv.org/abs/2306.13033v1

Pei G, Zhang J, Hu M, Zhang Z, Wang C, Wu Y, et al. Deepfake Generation and Detection: A Benchmark and Survey [Internet]. arXiv.org. 2024 [cited 2024 Sep 19]. Available from: https://arxiv.org/abs/2403.17881v4

Perov I, Gao D, Chervoniy N, Liu K, Marangonda S, Umé C, et al. DeepFaceLab: A simple, flexible and extensible face swapping framework. arXiv:200505535 [cs, eess] [Internet]. 2020 May 20; Available from: https://arxiv.org/abs/2005.05535

Autoren

Jan Fischer M.Sc. ist wissenschaftlicher Mitarbeiter am Forschungs- und Transferzentrum „Business Innovation Lab (BIL)" der HAW Hamburg. Nach seinem Studium der Wirtschaftsinformatik (M.Sc.) an der Universität Oldenburg arbeitet er seit 2017 intensiv an der Digitalisierung von kleinen und mittleren Unternehmen, mit Fokus auf Produktionsplanung, Supply Chain Management und den Einsatz künstlicher Intelligenz. Er ist an verschiedenen Projekten beteiligt, darunter das "Mittelstand-Digital Zentrum Hamburg" und der "European Digital Innovation Hub Hamburg". Im Rahmen seiner Tätigkeiten beschäftigt er sich zudem intensiv mit der praktischen Anwendung von (generativer) KI sowie deren Auswirkungen u.A. auch auf die Cybersicherheit.

Prof. Dr.-Ing. Axel Wagenitz ist Professor für Wirtschaftsinformatik an der HAW Hamburg und leitet das "Business Information Lab". Als Informatiker mit Promotion im Bereich Ingenieurwesen entwickelte er am Fraunhofer IML Ansätze zur Planung von Logistiknetzwerken. Dort war er auch an der Umsetzung von über 50 Forschungs- und Industrieprojekten beteiligt. Als Projektleiter am Mittelstand-Digital Zentrum Hamburg und Mitbegründer des Forschungs- und Transferzentrums berät er Unternehmen in den Bereichen Digitalisierung, Künstliche Intelligenz und Logistik. Zudem ist er weiterhin als wissenschaftlicher Berater im Supply Chain Engineering tätig.

Nico Piepenstock, Erich Behrendt, Werner Krause

Predictive Cybersecurity mit KI im Mittelstand

In der heutigen digitalen Ära sind kleine und mittlere Unternehmen (KMU) einem stetig wachsenden Risiko von Cyberangriffen ausgesetzt. Während Cyberkriminelle zunehmend raffinierte Methoden entwickeln, stoßen traditionelle, reaktive Sicherheitsmaßnahmen immer häufiger an ihre Grenzen. Die Notwendigkeit, nicht nur auf Bedrohungen zu reagieren, sondern sie proaktiv zu verhindern, wird immer dringlicher. Hier kommt die Künstliche Intelligenz (KI) ins Spiel, die eine entscheidende Rolle in der prädiktiven Cybersicherheit übernimmt.

Künstliche Intelligenz ermöglicht es, potenzielle Bedrohungen frühzeitig zu erkennen, indem sie große Mengen an Daten analysiert, Muster identifiziert und darauf basierend Vorhersagen trifft. So können Sicherheitslücken geschlossen und Angriffe verhindert werden, bevor sie Schaden anrichten können. Dieser Artikel untersucht, wie prädiktive Sicherheitslösungen auf KI-Basis speziell für KMU von Vorteil sein können und welche Herausforderungen bei der Implementierung zu bewältigen sind. Das Interview wird von Nico Piepenstock vom Mittelstand-Digital Zentrum WertNetzWerke geführt, der mit zwei Experten auf diesem Gebiet – Prof. Dr. Erich Behrendt und Werner Krause – praxisnahe Einblicke und wertvolle Empfehlungen für KMU gibt, um ihre Cybersicherheit zukunftssicher zu gestalten.

Also was versteht man nun unter prädiktiver Cybersicherheit und wie unterscheidet sie sich von traditionellen reaktiven Ansätzen?

Prof. Dr. Erich Behrendt:
Prädiktive Cybersicherheit markiert einen grundlegenden Wandel in der Bedrohungsabwehr, indem sie auf vorausschauende statt reaktiver Prinzipien setzt. Traditionelle Sicherheitsstrategien greifen oft erst dann, wenn ein Angriff bereits stattgefunden hat. Prädiktive Cybersicherheit ermöglicht hingegen die frühzeitige Erkennung und Neutralisierung potenzieller Bedrohungen, bevor diese in Angriffe münden.
Dieser Ansatz stützt sich auf den Einsatz fortschrittlicher Künstlicher Intelligenz (KI) und maschinellen Lernens (ML), die großen Datenmengen analysieren, um Muster und Anomalien zu identifizieren. Durch die Kombination historischer Daten mit Echtzeitinformationen entwickeln diese Technologien die Fähigkeit, Bedrohungen zu antizipieren und präventive Maßnahmen zu ergreifen. Diese

Proaktivität ermöglicht es Unternehmen, Schwachstellen frühzeitig zu schließen und gezielte Abwehrstrategien zu implementieren, bevor ein Angriff Schaden anrichten kann.
Ein wesentlicher Vorteil dieser Systeme liegt in ihrer Fähigkeit, kontinuierlich zu lernen und sich an das sich ständig verändernde Bedrohungsspektrum anzupassen. Während traditionelle, reaktive Sicherheitsansätze oft auf bekannte Angriffsmuster beschränkt sind, ein bisschen wie in unserem Digitalisierungsprojekt „Fernwartung und Condition Monitoring" nur nicht mit Maschinendaten, sondern Datenmustern, Verhaltensanalysen und Netzwerktraffic.
Für kleine und mittlere Unternehmen, die oft nicht über die Ressourcen verfügen, um nach einem Cyberangriff entstandene Schäden zu beheben, bietet diese Form der Sicherheit einen entscheidenden Vorteil. Die Möglichkeit, proaktiv zu handeln und durch vorausschauende Maßnahmen Bedrohungen abzuwehren, kann für diese Unternehmen den entscheidenden Unterschied ausmachen.

Welche konkreten Anwendungen und Tools für prädiktive Cybersicherheit gibt es denn derzeit und wie können diese von KMU implementiert werden?

Werner Krause:
Die Integration von Künstlicher Intelligenz in Sicherheitsstrategien eröffnet die Möglichkeit, Bedrohungen nicht nur zu erkennen, sondern diese auch proaktiv abzuwehren, bevor sie Schaden anrichten. Ein zentraler Anwendungsbereich hierbei ist die Verhaltensanalyse, bei der Benutzer- und Systemaktivitäten kontinuierlich überwacht werden, um Anomalien zu identifizieren. Solche Abweichungen, wie etwa ein plötzlicher Anstieg des Netzwerkverkehrs außerhalb der regulären Arbeitszeiten, können auf potenzielle Angriffe hinweisen, vielleicht ist aber auch nur eine Deadline unbedingt einzuhalten und es müssen Überstunden gemacht werden. Die frühzeitige Erkennung solcher Anomalien und die automatisierte Interpretation, ermöglicht es Unternehmen, umgehend gezielte Sicherheitsmaßnahmen zu ergreifen.
Ein weiteres wichtiges Element ist die Netzwerküberwachung. KI-basierte Systeme analysieren den gesamten Datenverkehr in Echtzeit und können ungewöhnliche Muster in Datenströmen erkennen. Sollten z.B. Daten an verdächtige IPs gesendet werden, können sie automatisch Gegenmaßnahmen einleiten oder das IT-Sicherheitsteam alarmieren. Die Anomalieerkennung kann so auch neue, bisher unbekannte Bedrohungen identifizieren.
Die allgemeine Fähigkeit von Machine-Learning-Systemen zu lernen und sich kontinuierlich zu verbessern, ist ein entscheidender Vorteil, um komplexe Muster aufzudecken, die herkömmlichen Sicherheitslösungen entgehen könnten.

Natürlich bringt die Implementierung solcher Technologien auch Herausforderungen mit sich, wie etwa die Komplexität der Technik, der Bedarf an spezialisierten Kenntnissen und die damit verbundenen Kosten. KMU sollten sich zunächst auf einfache, skalierbare Lösungen konzentrieren, die sich leicht in ihre bestehende Infrastruktur integrieren lassen. Viele gängige Anbieter bieten mittlerweile Cloud-basierte Sicherheitslösungen an, die speziell für kleinere Unternehmen entwickelt wurden und sich flexibel an die Bedürfnisse des Unternehmens anpassen und auch in bestehende Systeme integriert werden können. Diese Lösungen sind in der Regel kostengünstiger und einfacher zu implementieren als umfangreiche On-Premise-Systeme.

Welche Herausforderungen sehen Sie beide, bei der Integration von KI in bestehende Cybersicherheitsinfrastrukturen von KMU, und wie können diese überwunden werden?

Prof. Dr. Erich Behrendt:
Eine der größten Herausforderungen bei der Integration von Künstlicher Intelligenz in die Cybersicherheit ist die hohe technologische Komplexität. KI-Systeme benötigen nicht nur umfangreiche Datenmengen für eine effektive Funktion, sondern erfordern auch eine kontinuierliche Analyse und Verwaltung dieser Daten. Für kleine und mittlere Unternehmen mit begrenzten IT-Ressourcen kann dies eine erhebliche Belastung darstellen. Darüber hinaus setzt die Implementierung solcher Systeme fundierte Kenntnisse im maschinellen Lernen und in der Datenanalyse voraus – Fähigkeiten, die in vielen KMU oft nicht ausreichend vorhanden sind. Dies führt häufig dazu, dass entweder intern entsprechendes Know-how aufgebaut oder externe Expertise eingekauft werden muss, was zusätzliche Kosten verursacht.
Ein weiteres zentrales Risiko besteht im Umgang mit sensiblen Unternehmensdaten innerhalb der KI-Systeme. Datenschutzverletzungen können schwerwiegende Folgen haben, weshalb KMU sicherstellen müssen, dass alle Datenschutzrichtlinien nicht nur den gesetzlichen Vorgaben entsprechen, sondern auch die Sicherheit der verarbeiteten Daten gewährleisten.
Um diese Herausforderungen zu meistern, kann eine schrittweise Einführung von KI eine sinnvolle Strategie sein. Hierbei könnten zunächst kleinere Pilotprojekte gestartet werden, um das System in der Praxis zu testen und gegebenenfalls anzupassen.

Werner Krause:
Neben den technischen und datenschutzrechtlichen Herausforderungen sind die finanziellen Hürden für KMU bei der Einführung von KI-basierten Sicherheitslösungen auch nicht außer Acht zu lassen. Die Anschaffung, Implementierung und fortlaufende Wartung solcher Systeme stellen eine erhebliche Investition dar, die sorgfältig geplant werden muss. Diese Kosten können

schnell ansteigen, insbesondere wenn spezialisierte Hardware und zusätzliche Schulungen erforderlich sind.
Trotzdem bieten KI-Systeme große Chancen. Insbesondere durch die Automatisierung von Sicherheitsprozessen. Mit Hilfe von KI können Bedrohungen nicht nur schneller erkannt, sondern auch automatisch abgewehrt werden. Sowie die Anpassungsfähigkeit von diesen Systemen, die sich kontinuierlich weiterentwickeln und neuen Bedrohungen flexibel begegnen können. Dadurch bleibt die Sicherheitsinfrastruktur dynamisch und widerstandsfähig.
Um die Integration von KI trotz der Herausforderungen erfolgreich zu meistern, empfiehlt es sich, mit Pilotprojekten zu beginnen. Diese ermöglichen es, die Technologie in einem begrenzten Umfang zu testen und dabei wertvolle Erkenntnisse für eine umfassendere Implementierung zu gewinnen. Als ein guter Anlaufpunkt sind dort sicher die Mittelstand-Digital Zentren oder auch die extra dafür eingerichtete Initiative IT-Sicherheit in der Wirtschaft zu nennen.

Welche zukünftigen Entwicklungen erwarten Sie im Bereich prädiktiver Cybersicherheit und welche Schritte sollten KMU unternehmen, um vorbereitet zu sein?

Prof. Dr. Erich Behrendt:
Die Zukunft der prädiktiven Cybersicherheit wird maßgeblich durch die Weiterentwicklung der Künstlichen Intelligenz und verwandter Technologien gestaltet. Wir können erwarten, dass KI-Modelle zunehmend spezialisierter und präziser werden, wodurch sie in der Lage sein werden, Bedrohungen noch genauer vorherzusagen und immer komplexere Angriffsmuster zu erkennen. Ein entscheidender Fortschritt wird die Integration von verhaltensbasierten und generativen KI-Modellen sein. Diese Modelle arbeiten nicht nur mit historischen Daten, sondern sind auch in der Lage, neue Bedrohungen in Echtzeit zu identifizieren. Sie können Angriffe simulieren, potenzielle Schwachstellen aufdecken und präventive Maßnahmen vorschlagen, noch bevor ein tatsächlicher Angriff erfolgt.
Gleichzeitig wird die Automatisierung in der Bedrohungsabwehr weiter zunehmen, was insbesondere für KMU von großem Vorteil sein wird. Diese Automatisierung reduziert die Reaktionszeiten bei Sicherheitsvorfällen erheblich. Die regelmäßige Aktualisierung der Sicherheitsstrategien und die Integration neuer KI-basierter Tools werden unerlässlich sein, um die eigene Cybersicherheitslage zu stärken und sich für zukünftige Herausforderungen zu wappnen.

Werner Krause:
Ein weiterer wichtiger Trend wird die stärkere Vernetzung von Sicherheitslösungen sein. Verschiedene Systeme und Tools werden zunehmend miteinander kommunizieren, um ein umfassendes Sicherheitsnetzwerk zu schaffen, das sämtliche Bereiche eines Unternehmens abdeckt. KMU sollten daher sicherstellen, dass ihre Infrastruktur flexibel genug ist, um neue Technologien problemlos integrieren zu können, und dass ihre Sicherheitslösungen miteinander kompatibel sind.
Eine langfristige Planung und die Investition in skalierbare Technologien, die mit den wachsenden Anforderungen Schritt halten können, sind unerlässlich. Es reicht nicht aus, kurzfristige Lösungen zu implementieren; vielmehr ist eine nachhaltige Cybersicherheitsstrategie notwendig, die den Herausforderungen der Zukunft gewachsen ist. KMU müssen sich bewusst sein, dass Cybersicherheit ein fortlaufender Prozess ist, der kontinuierliche Anpassung und Weiterentwicklung erfordert. Durch regelmäßige Überprüfung und Anpassung ihrer Sicherheitsstrategien sowie den Einsatz der neuesten, am besten cloudbasierten, Technologien können sie sich besser gegen zukünftige Bedrohungen wappnen und ihre Position in der digitalen Welt stärken.

Wie kann prädiktive Cybersicherheit dabei helfen den Cyber Resilience Act (CRA) und die NIS2-Richtlinie zu erfüllen?

Prof. Dr. Erich Behrendt:
Der Cyber Resilience Act (CRA) setzt voraus, dass digitale Produkte von Beginn an ohne bekannte Sicherheitslücken entwickelt und regelmäßig mit Sicherheitsupdates versorgt werden. Unternehmen müssen daher das "Security by Design"-Prinzip befolgen, was bedeutet, dass Sicherheitsaspekte schon frühzeitig in den Entwicklungsprozess integriert werden. Die NIS2-Richtlinie geht sogar noch weiter, indem sie den Fokus auf die Sicherheit von Netzwerken und Informationssystemen legt, besonders für Betreiber kritischer Infrastrukturen. Diese Richtlinie verlangt nicht nur strenge Meldepflichten bei Sicherheitsvorfällen, sondern auch regelmäßige Risikobewertungen und die Einhaltung spezifischer Sicherheitsstandards.
Hier kann prädiktive Cybersicherheit KMU entscheidend unterstützen. Neben generativen KIs die den Programm-Code auf Schwachstellen analysieren, können diese Systeme kontinuierlich das Verhalten von Netzwerken und Systemen überwachen, identifizieren Anomalien und weisen sofort auf mögliche Schwachstellen hin. Dadurch wird es für Unternehmen einfacher, rechtzeitig Sicherheitsupdates bereitzustellen und sicherzustellen, dass ihre Produkte den Anforderungen des CRA entsprechen.
Zudem bietet prädiktive Cybersicherheit die Möglichkeit, automatisierte und regelmäßige Sicherheitsüberprüfungen durchzuführen, die den gesamten Lebenszyklus eines Produkts abdecken. Diese automatisierten Prozesse reduzieren den manuellen Aufwand und gewährleisten, dass alle notwendigen Sicherheitsmaßnahmen kontinuierlich umgesetzt werden.
Ein weiterer wesentlicher Vorteil prädiktiver Cybersicherheit ist die Fähigkeit, umfangreiche Datenanalysen durchzuführen, um potenzielle Bedrohungen zu bewerten und

präventive Maßnahmen vorzuschlagen. Solche Risikobewertungen sind für die Einhaltung der NIS2-Richtlinie von zentraler Bedeutung, da sie KMU dazu verpflichten, ihre Sicherheitsstrategien ständig an neue Bedrohungen anzupassen. KI-gestützte Systeme ermöglichen nicht nur die Vorhersage von Bedrohungen, sondern auch die Erstellung detaillierter Berichte, die für die Erfüllung der Meldepflichten gemäß NIS2 notwendig sind.

Schlussfazit

Die prädiktive Cybersicherheit stellt für kleine und mittlere Unternehmen eine vielversprechende Möglichkeit dar, ihre Sicherheitsstrategien zukunftssicher zu gestalten. In einer Zeit, in der Cyberbedrohungen immer raffinierter werden und gesetzliche Anforderungen wie der **Cyber Resilience Act** und die **NIS2-Richtlinie** zunehmend strenger werden, bietet die Integration von Künstlicher Intelligenz (KI) einen klaren Vorteil. KI-basierte prädiktive Sicherheitssysteme ermöglichen es KMU, potenzielle Bedrohungen frühzeitig zu erkennen und präventive Maßnahmen zu ergreifen, wodurch nicht nur gesetzliche Vorgaben erfüllt, sondern auch die operative Effizienz gesteigert wird.

Für den Einstieg in die prädiktive Cybersicherheit können KMU auf zahlreiche Unterstützungsangebote des **Mittelstand-Digital Netzwerks** zurückgreifen. Diese bieten praxisnahe Informationen, wie z.B. die Broschüre „Sichere Digitalisierung im Mittelstand" in der bereits 2020 auf das Thema der Prädiktiven Analyse eingegangen wurde. Sowie Schulungen und spezifische Programme, die Unternehmen helfen, ihre Cybersicherheitsmaßnahmen zu optimieren und die neuen gesetzlichen Anforderungen zu erfüllen. Hervorzuheben ist hier die extra dafür ins Leben gerufene Initiative **IT-Sicherheit in der Wirtschaft**. Durch die aktive Nutzung dieser Ressourcen und die Investition in prädiktive Cybersicherheit können KMU nicht nur ihre Resilienz gegenüber Cyberangriffen stärken, sondern auch ihre Wettbewerbsfähigkeit im digitalen Zeitalter sichern.

Autor und Interviewpartner

Als Referent und Projektmitarbeiter im Projekt Mittelstand-Digital Kompetenzzentrum eStandards gestartet, ist **Nico Piepenstock** nun für die Öffentlichkeitsarbeit und Medienproduktion für das Mittelstand-Digital Zentrum WertNetzWerke Standort Hagen und das wisnet innovation research institut e.V. verantwortlich. Darüber hinaus ist er als Fotograf tätig und bringt großes Verständnis im Bereich IT, KI und Medien Design mit.

Mit seiner langjährigen Erfahrung im Bereich IT-Consulting mit dem Schwerpunkt auf Cybersicherheit ist **Werner Krause** eine kompetente Anlaufstelle für Themen rund um IT-Sicherheit in kleinen und mittelständischen Unternehmen. Er unterstützt das Mittelstand-Digital Zentrum WertNetzWerke immer wieder mit seiner Expertise zu Themen rund um Cybersicherheit.

Prof. Dr. Erich Behrendt lehrte Soziologie mit einem Fokus auf empirische Methoden und Statistik an der Universität Duisburg-Essen. Seit 2019 hat er eine Honorarprofessur für Digital Transformation and Leadership an der University of Applied Sciences Europe inne und leitet das wisnet innovation research institute e.V. Zudem ist er KI-Trainer des Mittelstand-Digital Zentrums WertNetzWerke.

Das **Mittelstand-Digital Zentrum WertNetzWerke** ist Teil der Förderinitiative Mittelstand-Digital des BMWK. Es unterstützt kleine und mittlere Unternehmen bei der digitalen Transformation, indem es ihnen innovative Konzepte und praxisnahe Lösungen aufzeigt, um digitale Technologien effektiv einzusetzen. Ein Schwerpunkt liegt auf der Förderung digitaler und nachhaltiger Zusammenarbeit in Wertschöpfungsnetzwerken. Hierzu werde z.B. sichere Vertrauensumgebungen geschaffen, die eine Kollaboration und Selbstqualifizierung ermöglicht, etwa durch die Nutzung eines Enterprise Metaversums oder KI-Technologien. Unternehmen profitieren so von neuen Formen der überbetrieblichen Vernetzung und können Wissen, Ressourcen und Technologien effizienter teilen und anwenden.

https://www.mittelstand-digital-wertnetzwerke.de/

Mittelstand-Digital Zentrum WertNetzWerke

Tobias Diemer

Die CYBERDialoge

Ein erfolgreicher Einstieg für Unternehmen in die Cybersicherheit

"Ich würde ja gerne was für meine Cybersicherheit tun, ich weiß nur nicht, wo ich anfangen soll." – Solche Aussagen hören wir in den letzten Monaten häufig, besonders in persönlichen Gesprächen mit mittelständischen Unternehmen. Und das nicht ohne Grund: Das Thema Cybersicherheit wirkt auf viele kleine und mittlere Betriebe nach wie vor abschreckend und komplex. Unser Auftrag ist es, genau diesen Unternehmen die Berührungsängste zu nehmen und sie bei den ersten Schritten zu unterstützen.

Zu diesem Zweck hat die Transferstelle Cybersicherheit im Mittelstand die **CYBERDialoge** entwickelt. In einstündigen, persönlichen Gesprächen bieten wir einen unkomplizierten und praxisnahen Einstieg in die Cybersicherheit an. Durch standardisierte Fragen ermitteln wir zunächst den aktuellen Stand der Cybersicherheit im Unternehmen. Anschließend geben wir konkrete Handlungsempfehlungen und bieten gezielte Hilfestellungen.

Ergänzend dazu haben wir den CYBERsicher Check entwickelt. Ein online basiertes Tool, mit dem Unternehmen selbständig schnell und einfach erfahren können, wie es um die Lage der Cybersicherheit im Betrieb bestellt ist. Auch hier helfen wir mit personalisierten Handlungsempfehlungen und präzise ausgesuchten Materialien aus unserer eigenen Plattform.

Eine Firma, die bereits von unseren Angeboten profitieren konnte, ist die Völpker Spezialprodukte GmbH, ein internationaler Hersteller und Lieferant von Wachsadditiven und Gerbstoffen. Der Kontakt begann mit einem Gespräch auf einer unserer Veranstaltungen. Über den CYBERDialog mit unserem Experten Mike Wäsche bis hin zur Teilnahme an verschiedenen Workshops der Transferstelle konnten sowohl das Wissen zur IT-Sicherheit als auch das Sicherheitsniveau im Unternehmen durch gezielte Maßnahmen gesteigert werden. Dazu zählen vor allem unternehmensinterne Regelungen sowie Schulungs- und Sensibilisierungsmaßnahmen.

Nutzen Sie jetzt die Gelegenheit, Ihre Cybersicherheit voranzubringen!

Buchen Sie jetzt einen CYBERDialog mit unseren Expert*innen und packen Sie die Cybersicherheit in Ihrem Unternehmen an. Wir verschaffen Ihnen einen Überblick über den aktuellen Stand Ihrer Cybersicherheit und zeigen Ihnen anschließend konkrete nächste Schritte auf. Profitieren Sie von der Erfahrung unserer Expert*innen und lassen Sie sich praxisnah und unkompliziert auf dem Weg zur sicheren IT begleiten. Starten Sie noch heute und schützen Sie Ihr Unternehmen nachhaltig vor Bedrohungen aus dem Netz. Wir freuen uns auf Sie!

Die **Transferstelle Cybersicherheit im Mittelstand** unterstützt kleine und mittlere Unternehmen, Handwerksbetriebe und Start-Ups kostenfrei bei der Prävention, Detektion und Reaktion auf Cyberangriffe.

Über zahlreiche Veranstaltungen bundesweit, die CYBERDialoge, den CYBERsicher Check und die CYBERsicher Notfallhilfe wollen wir das Cybersicherheitsniveau im Mittelstand erhöhen und den deutschen Mittelstand so resilienter machen.

https://transferstelle-cybersicherheit.de/

Autor

Tobias Diemer ist innerhalb der Transferstelle für die Presse- und Öffentlichkeitsarbeit sowie das Netzwerkmanagement zuständig. Er studierte Politikwissenschaften in Bamberg und Birmingham und gelangte über Stationen im Europäischen Parlament und im politischen Berlin zum Bundesverband mittelständische Wirtschaft (BVMW), welcher der Transferstelle als Konsortialführer vorsteht. Innerhalb der Transferstelle widmet er sich nun vor allem der Aufbereitung und Darstellung der Inhalte im öffentlichen Raum.

Glossar

Alignment	Anpassung von KI-Modellen an ethische, rechtliche oder organisatorische Richtlinien, um sicheres und verantwortungsvolles Verhalten sicherzustellen.
Autoencoder	Neuronale Netze, die darauf trainiert sind, Daten zu komprimieren und wiederherzustellen. In Deepfake-Technologien genutzt, um Gesichter zu tauschen.
Cyber Resilience Act	Gesetzesrahmen zur Verbesserung der Cybersicherheitsresilienz in der EU.
Darknet	Teil des Internets, der nicht durch Standard-Suchmaschinen erfasst wird und oft für anonyme Kommunikation genutzt wird.
DDoS-Angriff (Distributed Denial of Service)	Überlastungsangriff, der den Zugriff auf Online-Dienste durch massenhafte Anfragen blockiert.
Deep Learning	Ein Bereich des maschinellen Lernens, der auf tiefen (vielschichtigen) neuronalen Netzen basiert und es Computern ermöglicht, komplexe Muster in Daten zu erkennen.
Deepfake	Digital erstellte Fälschungen, realistische Audio- oder Videoinhalte, die mit KI-Technologien wie Deep Learning generiert wurden.
Diffusionsmodelle	KI-Technologie, die hochrealistische Bilder erzeugt, indem sie den Prozess der Datenzerstörung umkehrt und aus verrauschten Daten klare Bilder rekonstruiert.
Fine-getunte LLM	Ein vortrainiertes LLM, das durch zusätzliche Daten auf eine spezifische Aufgabe oder ein Fachgebiet spezialisiert wird.
Generative Adversarial Networks (GANs)	Ein neuronales Netzwerkmodell, bestehend aus einem Generator, der neue Daten erzeugt, und einem Diskriminator, der authentische Daten von den generierten unterscheidet, was zu stetig verbesserten und realistischeren Ausgaben führt.
Generative KI	KI-Systeme, die neue Inhalte wie Texte, Bilder oder Musik selbstständig erzeugen können. Sie nutzen fortgeschrittene Algorithmen, um Muster in Daten zu lernen und kreativ anzuwenden.
Informationssicherheits-Managementsystem (ISMS)	Rahmenwerk zur systematischen Festlegung und kontinuierlichen Verbesserung von IT-Sicherheitsmaßnahmen.
Intrusion Detection System (IDS)	Systeme zur Überwachung und Erkennung potenzieller Angriffe im Netzwerkverkehr.
Keylogger	Schadsoftware zur Überwachung und Aufzeichnung von Tastatureingaben, oft zur Erbeutung von Passwörtern.
Künstliche Intelligenz (KI)	Technologie, die es Computern ermöglicht, menschenähnliche Aufgaben zu erledigen und aus Erfahrungen zu lernen.
Large Language Models (LLMs)	Große neuronale Netzwerke, die darauf spezialisiert sind, menschenähnliche Texte zu generieren. Sie verstehen und produzieren Sprache basierend auf umfangreichen Trainingsdaten.
LLM	Abkürzung für Large Language Models, große neuronale Netze, die menschenähnliche Sprache generieren.
Machine Learning	Ein Teilgebiet der KI, das auf Algorithmen basiert, die aus Daten lernen und Entscheidungen treffen.
Malware	Oberbegriff für Schadsoftware wie Viren, Würmer und Ransomware, die Systeme oder Daten unbefugt manipulieren.
Muddling-Through-Ansatz	Inkrementeller Entscheidungsprozess, der besonders bei Unsicherheit und Ressourcenmangel genutzt wird.
NIS2-Richtlinie	EU-Richtlinie zur Harmonisierung der Cybersicherheitsanforderungen und zur Erhöhung der Widerstandsfähigkeit kritischer Infrastrukturen
Phishing	Betrügerische Versuche, durch gefälschte E-Mails oder Nachrichten vertrauliche Informationen zu erlangen.

Prädiktive Cybersicherheit	Cybersicherheitsansatz, der zukünftige Bedrohungen und Schwachstellen durch Datenanalyse vorhersagt.
Prompt Injection	Angriffstechnik, bei der KI-Systeme durch gezielte Nutzereingaben manipuliert werden.
Quishing	Phishing-Variante, die QR-Codes zur Umgehung von E-Mail-Sicherheitslösungen verwendet.
RAG (Retrieval-Augmented Generation)	Kombiniert vortrainierte Sprachmodelle mit einer Datenbank für aktuelle Fakten, um auf neueste Informationen zuzugreifen.
Regelbasierte Systeme	Systeme, die auf festgelegten Entscheidungsbäumen basieren und vordefinierte Regeln für Benutzeranfragen anwenden.
Security by Design	Prinzip, bei dem Sicherheitsaspekte von Beginn an in das Systemdesign integriert werden.
Spear-Phishing	Eine zielgerichtete Form des Phishings, bei der die Angriffe auf spezifische Individuen oder Unternehmen zugeschnitten sind.
Two-Factor Authentication (2FA)	Authentifizierungsverfahren, das einen zusätzlichen Identitätsnachweis zur Passwortabsicherung erfordert.
Variational Autoencoder (VAE)	Eine spezielle Art von Autoencoder, der für generative Aufgaben verwendet wird. Der VAE modelliert die zugrunde liegenden Wahrscheinlichkeitsverteilungen der Eingabedaten, um neue Datenpunkte zu generieren, die den Originaldaten ähnlich sind.
Vishing	Phishing durch Einsatz von Telefonanrufen, wobei oft synthetische Stimmen verwendet werden, um sensible Informationen zu erschleichen.
Voice Cloning	Prozess des Nachbildens einer menschlichen Stimme mithilfe von KI, um täuschend echte Audioinhalte zu erzeugen.
Voice Deepfakes	Anwendung von Deepfake-Technologie auf menschliche Stimmen, oft für betrügerische Zwecke.
WormGPT	Eine spezielle Version von Large Language Models, die zur schnellen Entwicklung von Schadsoftware im Darknet eingesetzt wird.

Mittelstand-Digital
Zentren
Deutschlandweit

Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Kompetenzzentren helfen vor Ort dem kleinen Einzelhändler genauso wie dem größeren Produktionsbetrieb mit Expertenwissen, Demonstrationszentren, Netzwerken zum Erfahrungsaustausch und praktischen Beispielen. Das Bundesministerium für Wirtschaft und Klimaschutz ermöglicht die kostenlose Nutzung aller Angebote von Mittelstand-Digital.

Weitere Informationen finden Sie unter *www.mittelstand-digital.de*.

www.mittelstand-digital.de

ISSN (Print) 2198-8544
ISSN (Online) 2198-9362