Schieb Report

Ausgabe 2023.39

Die Bedeutung von Datenanalysen und Künstlicher Intelligenz im Businessplan

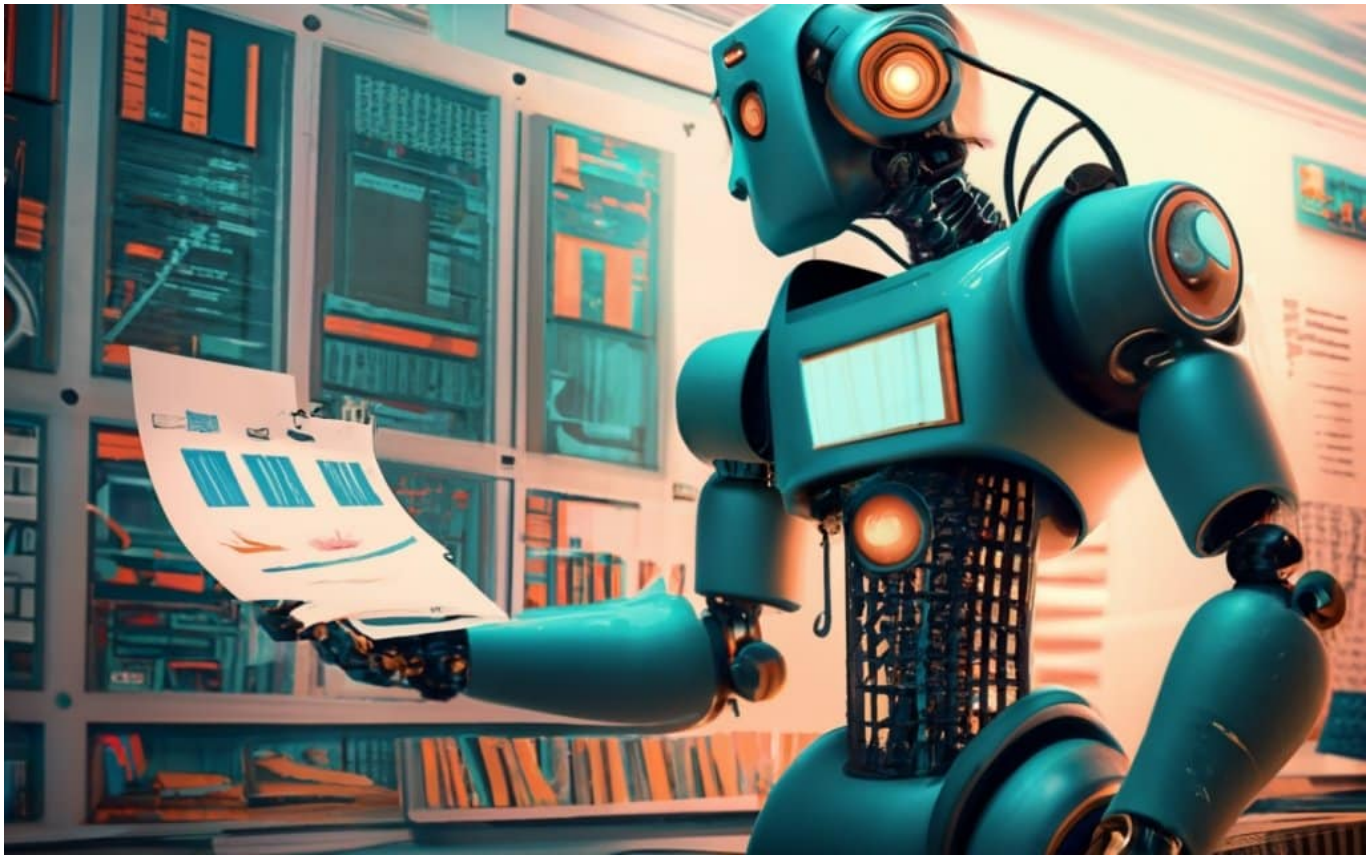
KI kann längst mehr als nur Texte erstellen oder Fotos erzeugen. Die eigentliche Stärke von KI ist das Erkennen von Mustern - und vor allem die Datenanalyse. Genau das kann man sich auch im Business zunutze machen.

In der heutigen Geschäftswelt sind Datenanalysen und Künstliche Intelligenz (KI) nicht mehr bloße Buzzwörter, sondern entscheidende Elemente für den Erfolg eines Unternehmens. Die Integration dieser Technologien in den Businessplan kann einen tiefgreifenden Einfluss auf die Effizienz, Wettbewerbsfähigkeit und Innovationskraft haben. Dieser Artikel erkundet, wie Datenanalysen und KI in Geschäftsstrategien eingebunden werden können, um Geschäftsmodelle zu optimieren und den Weg in die Zukunft zu ebnen.

Datenanalysen und Künstliche Intelligenz

Datenanalysen und Künstliche Intelligenz (KI) haben sich zu unverzichtbaren Instrumenten in der Unternehmenswelt entwickelt. Datenanalysen ermöglichen die Aufbereitung und Interpretation von Informationen, während KI Algorithmen und maschinelles Lernen nutzt, um Muster zu erkennen und Vorhersagen zu treffen.

Diese beiden Technologien, gemeinsam angewendet, bieten ein leistungsfähiges Werkzeug zur Optimierung von Geschäftsmodellen und zur Steigerung der Wettbewerbsfähigkeit.



Eine Stärke von KI ist die Analyse großer Datenmengen

Synergie zwischen Datenanalysen und KI

Die Synergie zwischen Datenanalysen und Künstlicher Intelligenz (KI) bildet das Herzstück innovativer Geschäftsstrategien. Datenanalysen extrahieren wertvolle Erkenntnisse aus Daten, während KI mithilfe von Algorithmen und maschinellem Lernen Muster und Trends erkennt.

Gemeinsam ermöglichen sie eine datengesteuerte Entscheidungsfindung in

Echtzeit, automatisierte Prozesse und die Vorhersage von Kundenverhalten. Dieses Zusammenspiel führt zu einem tieferen Verständnis des Marktes, erhöhter Effizienz und der Fähigkeit, schnell auf sich ändernde Bedingungen zu reagieren.

Die Künstliche Intelligenz in der Datenanalyse

In der modernen Datenanalyse spielt Künstliche Intelligenz (KI) eine transformative Rolle. KI-Algorithmen ermöglichen eine tiefgehende und schnelle Analyse großer Datenmengen, was traditionelle Methoden bei Weitem übertrifft. Sie erkennen Muster und Abweichungen in Echtzeit und bieten präzise Vorhersagen.

Eine Revolution in der Datenanalyse?

Die Integration von KI in die Datenanalyse markiert zweifellos eine Revolution in diesem Bereich. KI automatisiert nicht nur repetitive Analyseaufgaben, sondern ermöglicht auch eine tiefere Analyse von komplexen Datensätzen. Machine-Learning-Algorithmen erlauben es der KI, Muster und Trends zu erkennen, die für menschliche Analysten schwer zu identifizieren wären. Dies führt zu genaueren Vorhersagen und einem besseren Verständnis von Kundenverhalten, Markttrends und operativen Abläufen.

Weitere Einsatzbereiche von KI in Unternehmen

Weitere Einsatzbereiche von KI in Unternehmen sind vielfältig und tragen maßgeblich zur Verbesserung verschiedener Geschäftsprozesse bei:

- **Kundenserviceoptimierung**: KI-basierte Chatbots bieten schnelle und effiziente Lösungen für Kundenanfragen rund um die Uhr.
- **Personalisierte Marketingkampagnen**: KI analysiert das Verhalten der Kunden und ermöglicht die Erstellung individueller Marketingstrategien, was die Kundenbindung erhöht.
- **Automatisierung der Produktion**: Durch die Integration von Robotern und intelligenten Automatisierungssystemen in Fertigungsprozesse steigt die Effizienz und Qualität der Produktion.
- **Verbesserte Lieferkettenplanung**: KI optimiert die Bestandsverwaltung und Lieferkettenprozesse, was zu Kostenersparnissen und reibungsloseren Lieferungen führt.

- **Erhöhung der Cybersicherheit**: KI erkennt und bekämpft proaktiv Cyberbedrohungen, wodurch Unternehmen geschützt werden.
- **Medizinische Diagnoseunterstützung**: In der Gesundheitsbranche hilft KI bei der schnelleren und genaueren Diagnose von Krankheiten.
- **Autonomes Fahren**: Die Automobilindustrie profitiert von KI, um selbstfahrende Fahrzeuge sicherer und effizienter zu gestalten.
- **Erleichterung der Finanzanalyse**: KI analysiert riesige Datenmengen in Echtzeit und unterstützt so Finanzexperten bei fundierten Entscheidungen.

Der obige Auszug aus der breiten Palette der Einsatzmöglichkeiten zeigt, wie KI die Effizienz und Wettbewerbsfähigkeit von Unternehmen in verschiedenen Sektoren steigert, was sie zu einem unverzichtbaren Werkzeug für die moderne Geschäftswelt macht.

Schritt-für-Schritt-Anleitung zur Integration von Datenanalysen und KI

Die Integration von Datenanalysen und Künstlicher Intelligenz (KI) in den Businessplan erfordert eine durchdachte Herangehensweise. Hier sind fünf wesentliche Schritte, die dabei helfen, Daten optimal zu nutzen und KI erfolgreich in das Geschäftsmodell zu integrieren.

Schritt 1: Datensammlung und -speicherung

Die Grundlage jeder Datenanalyse und KI-Anwendung ist die Datensammlung. Es gilt, relevante Datenquellen zu identifizieren und Daten systematisch zu sammeln und zu speichern, unter Beachtung aller Datenschutzrichtlinien.

Schritt 2: Datenverarbeitung und -analyse

Nach der Datensammlung folgt die Verarbeitung und Analyse. Hier können leistungsfähige Analysetools genutzt werden, um Muster und Erkenntnisse aus den Daten zu gewinnen.

Schritt 3: Identifikation von Geschäftsmöglichkeiten

Basierend auf den Analyseergebnissen werden Geschäftsmöglichkeiten

identifiziert. Welche Potenziale und Chancen bieten sich an?

Schritt 4: Integration von KI in den Businessplan

Als nächstes erfolgt die Integration von KI in die Geschäftsstrategie, um datengesteuerte Entscheidungen zu fördern. Dabei sollten konkrete Bereiche ermittelt werden, in denen KI einen Mehrwert bietet.

Schritt 5: Kontinuierliche Optimierung mit KI

Der letzte Schritt beinhaltet die kontinuierliche Optimierung. KI-Systeme müssen überwacht und an sich verändernde Daten und Geschäftsanforderungen angepasst werden, um kontinuierlichen Erfolg sicherzustellen.

Die Zukunft von Datenanalysen und KI im Businessplan

Die Welt der Datenanalysen und Künstlichen Intelligenz (KI) entwickelt sich rasant weiter, und Unternehmen müssen sich auf zukünftige Trends und Entwicklungen vorbereiten, um wettbewerbsfähig zu bleiben. Im Folgenden werfen wir einen Blick auf aktuelle Trends und wie Unternehmen von den Fortschritten in Datenanalysen und KI profitieren können.

Trends und Entwicklungen in der Welt der Datenanalysen und KI

Datenanalysen und die KI-Branche verzeichnen eine zunehmende Integration von Explainable AI, um Entscheidungen transparenter zu gestalten. Außerdem gewinnen Edge Computing und Quantencomputing an Bedeutung, um datenintensive Aufgaben effizienter zu bewältigen.

Wie Unternehmen von den Fortschritten in Datenanalysen und KI profitieren

Unternehmen können von diesen Fortschritten profitieren, indem sie ihre Datenstrategie weiterentwickeln und in Schulungen für ihre Mitarbeiter investieren. Die Integration von KI in Geschäftsprozesse ermöglicht präzisere

Prognosen, effizientere Abläufe und eine bessere Kundenbindung.

#Dontsendit: Wo bei Kinderpornografie das Gesetz übers Ziel hinausschießt

#dontsendit: Das BKA warnt aktuell in einer Kampagne davor, eigene Nacktbilder zu versenden. Die Verbreitung von Nacktbildern von Kindern und Jugendlichen kann strafrechtliche Folgen haben. Allerdings schießt das Gesetz aus Sicht des deutschen Richterbunds über das Ziel hinaus.

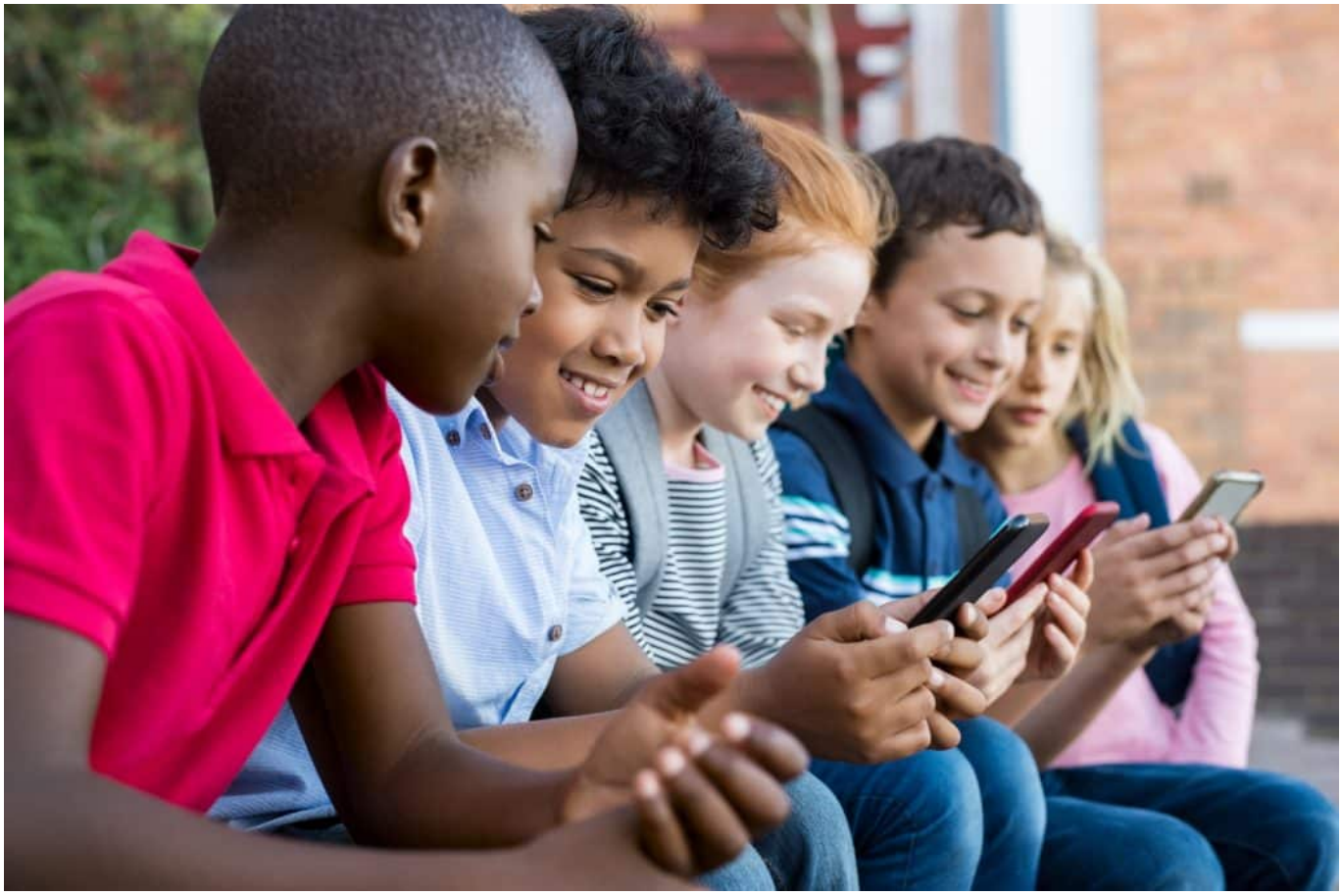
Das Handy: immer griffbereit. Das gilt für die meisten Erwachsenen, aber erst recht für Jugendliche.

Das Handy ist das mit Abstand wichtigste Kommunikationsmedium. Nicht zum Telefonieren, das nur im Notfall. Aber für Chats und Social Media. Wenn Jugendliche ihre Sexualität entdecken, kann es vorkommen, dass sie Nacktbilder von sich machen und mit Freund oder Freundin austauschen.

Strafbarkeit bei Nackbildern

Für Erwachsene manchmal schwer vorstellbar. Aber die heutige Jugend wächst halt mit Smartphones auf. Doch das ist alles andere als harmlos.

Nicht aus moralischen Gründen, sondern aus juristischen. Denn Nacktbilder von Jugendlichen unter 18 Jahren sind strafrechtlich gesehen „Jugendpornografie“ – und da gerät man schnell in den Bereich der Strafbarkeit.



Wenn Kids ein Smartphone nutzen, haben Eltern jede Kontrolle verloren

Strafbar, wenn Jugendliche Bilder von sich verschicken

Der Laie ist da schnell verwirrt: Wieso soll es strafbar sein, wenn Jugendliche von sich selbst Fotos schießen?

Darauf kommt man in der Tat nicht, wenn man sich mit der Thematik nicht näher befasst.

Aber es ist so: Die große Koalition hatte am Ende ihrer Legislaturperiode noch ein Gesetz, das die Verbreitung pornografischer Aufnahmen mit Kindern und Jugendlichen unter Strafe stellt, deutlich verschärft.

Wenn **Kinder**, also Personen unter 14 Jahren, Nacktbilder oder -videos

> von sich fertigen, handelt es sich hierbei um sog. kinderpornografische Inhalte. Wer solche Nacktbilder oder -videos herstellt, versendet, empfängt, weiterleitet oder speichert, macht sich gemäß § 184b StGB strafbar. Seit dem Sommer 2021 handelt es sich dabei um ein Verbrechen. Das heißt, dass die Straftat mit mindestens einem Jahr Freiheitsstrafe bedroht ist. Eine Verfahrenseinstellung durch die Justiz ist daher kaum noch möglich. Personen sind ab dem vollendeten 14. Lebensjahr gemäß § 19 StGB strafmündig, sodass sie strafrechtlich zur Verantwortung gezogen werden können. Kinder bleiben daher straflos.

Laut Paragraf 184b ist es auf jeden Fall ein Verbrechen, solches Material überhaupt im Handy zu haben.

Dabei seien auch Aufnahmen von "ganz oder teilweise unbekleideten" Minderjährigen als "sexuell aufreizend" einzustufen, "wenn aus Sicht eines Durchschnittsbetrachters eine Stimulierungstendenz hervorgerufen wird.

Und das schließt auch Aufnahmen ein, die Jugendliche von sich selbst machen – mit wenigen Ausnahmen. Und diese Verschärfungen haben Konsequenzen: 41,3% der Tatverdächtigen waren im letzten Jahr unter 18 Jahren alt. Und weil es sich durch die Verschärfung um ein Verbrechen handelt, können Staatsanwaltschaften Verfahren nicht einfach so wieder einstellen.

Safer Sexting: Es gibt einiges zu beachten, wenn Jugendliche aus Unwissenheit Nacktbilder austauschen

Vorsicht: Screenshots können strabar sein

Das erklärt dann auch – zumindest teilweise – den hohen Anteil an minderjährigen Straftätern. Die hatte der Gesetzgeber doch wohl eher nicht im Sinn, als das Gesetz verschärft wurde.

Aber jetzt sind wir in einer Situation, in der jede Nacktaufnahme auf dem Handy eines Jugendlichen zu einem strafrechtlichen Problem werden kann. Mehr als das: Wenn Eltern oder Lehrer in einem Chat eine Nacktaufnahme sehen und beispielsweise einen Screenshot davon machen, um etwas gegen unerlaubt verteilte Nacktaufnahmen zu unternehmen, machen sie sich strafbar!

Und weil es sich nach dem neuen Gesetz um ein Verbrechen handelt, das sogar mit Haftstrafen belegt ist, müssen Polizei und Staatsanwaltschaft der Sache nachgehen. Der Richterbund warnte unjüngst vor dieser überschießenden Strafverfolgung gegen Kinderpornografie. Hier muss unbedingt nachgebessert

werden, damit das Gesetz nicht ständig die Falschen trifft.

Aktion #dontsendit vom BKA

Nun hat das Bundeskriminalamt (BKA) eine Kampagne gestartet, um Jugendliche vor der Problematik und der Gefahr zu warnen, durch die Verbreitung von Nacktbildern/Nudes strafbare Handlungen zu begehen.

Das BKA hat zwei Videos gemacht und verteilt sie auf Social Media. Eins mit einem Jungen, eins mit einem Mädchen – beide chatten gerade im Messenger und werden aufgefordert, doch mal Nacktbilder zu machen. Was sie dann auch tun, wie angedeutet wird. Dann hören wir eine strenge Stimme: „Ist dir das eine Straftat wert? Dontsendit."

Finde ich ehrlich gesagt nicht so gelungen. Denn hier wird den Jugendlichen lediglich mitgeteilt: Du könntest eine Straftat begehen... Was prinzipiell stimmt, aber nicht in jedem Fall. Das Video erzeugt Druck, anstatt Hilfe anzubieten. Es vermittelt den Eindruck: „Die Polizei sieht dich – und dann gibt's Ärger". Dabei ist eine Nachtaufnahme, die Jugendliche von sich selbst freiwillig machen, erst mal straffrei.

Safer Sexting: Eine gute Aufklärungsseite der LfM NRW

Kompliziertes Regelwerk

Die Regeln sind ja auch kompliziert. Wie soll man da nur durchblicken?

Die Regeln sind schwierig, genau – besonders für Jugendliche. Und da hilft ein drohendes „Ist es das wert?“ von der Bundesinnenministerin nicht wirklich weiter, finde ich.

Sehr viel besser macht es da die Landesanstalt für Medien NRW. Die haben nämlich eine gut gemachte Info-Webeseite gebaut, die sich unter safer-sexting.de erreichen lässt.

Hier können sich Jugendliche, aber auch Eltern und Lehrer informieren, wie das alles mit der rechtlichen Situation genau aussieht, was man machen darf – und was eben nicht. Es gibt auch parallel Informationskampagnen an und für Schulen. Und die drei wichtigen Regeln für Jugendliche lauten:

- Möchte die andere Person die Fotos überhaupt sehen?
- Schickt Ihr Euch auch wirklich nur Fotos, die euch selbst zeigen?
- Vertraust Du der anderen Person?

Das ist in meinen Augen viel hilfreicher, als wenn die Jugendlichen dank BKA-Video nur die Handschellen klicken hören.

Lükex: Behörden problen Cyber-Ernstfall - aber nicht so richtig

Cyberangriffe nehmen zu - gleichzeitig sind wir alle, auch als Gesellschaft immer mehr abhängig von funktionierender IT-Infrastruktur. Doch was, wenn öffentliche IT-Systeme ausfallen? Eine groß angelegt Übung soll die richtigen Reaktionen trainieren. Es gibt aber noch Luft nach oben.

Das Szenario ist alles andere als unrealistisch: Hackergruppen aus dem Ausland haben IT-Infrastruktur in Deutschland ins Visier genommen. Sie versuchen, in die Systeme kritischer Infrastruktur einzudringen, um die Kommunikation oder das öffentliche Leben lahmzulegen. Es droht ein umfangreicher Cyber-Angriff.

Was tun in einer solchen Situation? Bund, Länder und Gemeinden müssen dann zusammenarbeiten – ebenso die unterschiedlichsten Behörden. Wie wappnen sich Bund und Länder dafür? Das wird vom 25. Bis 29. September in mehreren Bundesländern in einer großangelegten Übung durchgespielt.

Deutschland muss sich besser schützen gegen Cyberangriffe jeder Art

Cyberangriffe nehmen stetig zu

Die Zahl der Angriffe auf IT-Infrastruktur nimmt bekanntlich zu, vor allem seit dem Angriffskrieg auf die Ukraine.

Laut dem Bundesamt für Sicherheit in der Informationstechnik (BSI) gab es im Jahr 2022 insgesamt 1.428 Fälle von Cyberangriffen auf Bund, Länder und Behörden in Deutschland. Davon waren 1.201 Fälle von sogenannten Ransomware-Angriffen.

Bei solchen Angriffen verschlüsseln die Angreifer nach dem Eindringen in PCs oder Netzwerke der Behörden oder Institutionen die gespeicherten Daten. Rechner und Netzwerke lassen sich dann oft überhaupt nicht mehr benutzen – und es wird ein Lösegeld verlangt. Solche Angriffe sind derzeit besonders weit verbreiten.

Jüngste Cyberangriffe, die erfolgreich waren

Noch im August 2023 wurde die IT-Infrastruktur des Bundesinnenministeriums lahmgelegt: Kriminellen verschlüsselten Daten von rund 1.000 Rechnern und

Servern, darunter auch Daten des Verfassungsschutzes. Die vollständige Wiederherstellung der IT-Systeme dauerte mehrere Wochen.

Es gab Dutzende solcher Angriffe in diesem Jahr. Auch auf Behörden im Land. Am 2. Mai 2023 wurde zB die IT-Infrastruktur des Kreisgesundheitsamts in Dortmund durch einen Ransomware-Angriff lahmgelegt, betroffen auch das Impfregister. Die vollständige Wiederherstellung der IT-Systeme dauerte mehrere Wochen.

Gespräch mit Manuel Atug

Das wird geübt - und auch nicht

Was aber wird nun genau geübt: Ein fiktiver Cyberangriff auf das Regierungshandeln – was muss man sich darunter vorstellen?

Diesmal geht es ausschließlich um IT-Sicherheit. Ziel der Übung ist es, während eines fiktiven bundesweiten Angriffs auf die IT-Infrastruktur von Behörden des Bundes die Staats- und Regierungsfunktionen aufrecht zu erhalten. Was passiert, wenn Server ausfallen, wenn die Kommunikation des Regierungsapparats erschwer und unmöglich gemacht wird? Funktioniert die Kommunikation noch?

Bei der Übung kommen bis zu 1.000 Leute aus den unterschiedlichsten Behörden zusammen. Klappt die Kommunikation trotz Einschränkung der IT? Wie wird entschieden? Kernübungstage sind der 27. und 28. September 2023 – da soll es also richtig zur Sache gehen. Allerdings ist die gesamte Übung fiktiv. Es erfolgen keine tatsächlichen Angriffe auf die IT-Infrastruktur, um zu prüfen, ob die belastbar ist. Es wird also nur so getan als ob.

Hacker hacken - doch die Behörden müssen gewappnet sein

Keine echten Belastungstests

Bei einer Wehrübung müssen Soldaten in den Panzer und in den Matsch – aber bei dieser Übung treffen sich nur Angehörige der Entscheiderebene.

Das ist auch einer der Hauptkritikpunkte der AG Kritis. Eine Arbeitsgemeinschaft, die sich intensiv mit der Kritischen Infrastruktur beschäftigt und das Ziel hat, dass unsere kritische Infrastruktur geschützt ist. Ich habe mit Manuel Atug von der AG Kritis gesprochen, die auch die Bundesregierung berät.

Die Kritik ist eindeutig: Gut, dass es eine Übung gibt. Aber nicht gut, dass sie so stattfindet. Wer die tatsächlich vorhandene IT-Infrastruktur nicht auf die Probe stellt – und alle Menschen, die mit ihr arbeiten und sie bereitstellen und pflegen –,

der übt nicht wirklich und richtig.

Vor allem bestehe offensichtlich kein ernsthaftes Interesse daran, Fehler und Schwachstellen zu finden. Das wäre aber zwingend nötig, um daraus zu lernen und die Fehler zu beseitigen. Denn wir haben in Deutschland eine IT der Monokultur: Windows, Office, SAP – Standardprogramme, die jeder Hacker kennt – und für die es auch reichlich bekannte Sicherheitslecks gibt.

Da einzudringen, ist vergleichsweise einfach. Doch die Übung dient nur dem Zweck, Fehler in der Struktur der Behörden aufzudecken.

Keiner denkt an die Bevölkerung

Ein weiteres Problem, meint die AG Kritis: Die Katastrophenschutzübungen in Deutschland hätten vornehmlich das Ziel, den Staats- und Regierungsbetrieb sicherzustellen. Das ist zweifellos erstes Ziel nicht falsch, greife aber zu kurz.

Genau so wichtig und eng verknüpft ist aus Sicht der AG Kritis die Sicherstellung oder Wiederherstellung der Versorgung der Bevölkerung. Denn das wäre in aller Regel die unvermeidbare Folge eines großflächigen Cyberangriffs auf IT-Infrastruktur: Behörden würden möglicherweise nicht funktionieren, vielleicht sogar andere Infrastruktur.

Das hätte Folgen für die Bevölkerung. Doch es ist nicht Ziel der LÜKEX - weder jetzt, noch in der Vergangenheit –, darauf einen Blick zu werfen und sich Gedanken zu machen, wie die Bevölkerung schnellstmöglich wieder versorgt wird. Aus Sicht der Kritiker ein immenser Mangel und Fehler.

Verwenden von Datenträgerkopien (ISO, VDHX)

Bei vielen Anbietern findet ihr ganze Datenträger zum Download. Nein, keine Raubkopien, sondern Installationsmedien wie DVDs in einer einzigen Datei. Zum Beispiel Windows 11. Was könnt ihr damit tun?

Was sind ISO und VHDX-Dateien?

Komplexere Programme und Betriebssysteme wurden früher über CDs und DVDs ausgeliefert. Das ist mittlerweile viel zu teuer und dazu noch wenig sinnvoll: schon wenige Tage nach der Produktion dieser physischen Datenträger ist der Inhalt veraltet, weil es Updates gibt. Aus diesem Grund werden stattdessen oft die Datenträger als Image-Dateien zum Download bereitgestellt.

Weit verbreitet ist immer noch das ISO-Format, das den Datenträger als Abbild enthält. Die Vielzahl der Dateien, die ein Windows 11 beispielsweise beinhaltet, sind so in einer Datei gebündelt. Neuer ist das von Microsoft eingeführte VHDX-Format, das einen virtuellen Datenträger darstellt.

Was tun mit einer ISO/VDHX?

Für beide Formate gilt: Zur Installation braucht ihr die Dateien in dem Image in ihrer ursprünglichen Verzeichnisstruktur. Andernfalls können die Installationsroutinen nicht fehlerfrei ausgeführt werden.

- Um das zu erreichen, öffnet den Windows Explorer und navigiert zu der entsprechenden Datei. Wenn ihr diese heruntergeladen habt, dann liegt die im **Download**-Verzeichnis.
- Klickt dann mit der **rechten Maustaste** auf die ISO oder VHDX und dann auf **Bereitstellen**.
- Windows verbindet sich nun mit der Datei und stellt sie euch als virtuelles DVD-Laufwerk zur Verfügung.
- Über dieses Laufwerk könnt ihr auf alle Dateien zugreifen und die Installation starten, als wäre es eine echte DVD.
- Seid euch bewusst, dass Teile der Dateien auf dem virtuellen Datenträger komprimiert sind. Ihr könnt sie nur nach der Installation nutzen, das Kopieren einzelner Dateien ist meist nicht möglich.

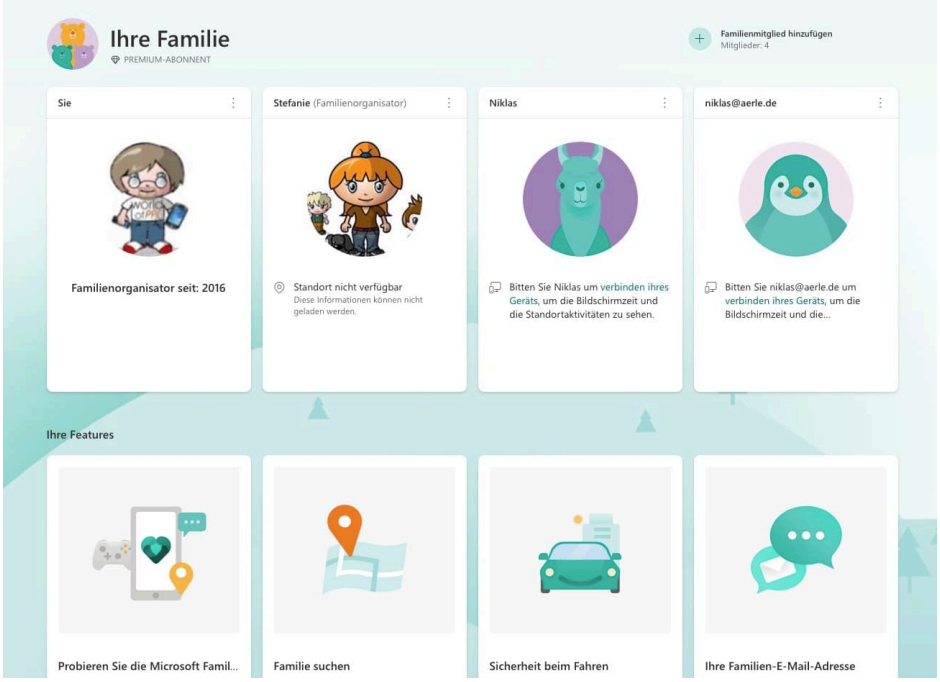
Familieneinstellung bei Microsoft 365 Konten vornehmen

Windows ist das Standard-Betriebssystem, das auf den meisten im Handel vertriebenen PCs vorinstalliert ist. Auch für Kinder und Jugendliche bleibt also keine Alternative. Wem dies Sorge bereitet, der sollte sich die Familieneinstellungen anschauen.

Die Familie - auch unter Windows

Familie ist allgemein ein wichtiges Gut. Das kennt Ihr aus dem normalen Leben, und warum sollte es am PC anders sein? Oft ist es so, dass ihr in der Familie eine Person habt, die IT-affiner ist als die anderen. Die euch regelmäßig damit nervt,

dass ihr ja Dinge anders machen könntet, Sicherheitsrisiken eingeht und vieles mehr. Ärgert euch nicht, sondern macht einfach den einfach zum Familienmanager. Das macht vor allem Sinn, wenn ihr einen Jugendlichen oder ein Kind an einen PC lassen wollt.



Die Voraussetzung: Alle zugehörigen Microsoft-Konten müssen bereits angelegt sein, dann erst können sie in das Familienkonstrukt aufgenommen werden.

Festlegen der Rechte der Kinder/Jugendlichen

Der Ausgangspunkt für alle Familieneinstellungen ist das Family-Portal, das ihr unter diesem Link erreicht. Meldet euch mit dem Microsoft Account des Familienverwalters an, dieser bekommt dann automatisch die Administratorenrolle zugewiesen.

- Klickt auf das Plus neben **Familienmitglied hinzufügen**, um ein bestehendes Kontos hinzuzufügen.
- Gebt die E-Mail-Adresse des hinzuzufügenden Kontos ein, dann wählt aus, ob dieses Konto ein (verwaltetes) Mitglied sein soll oder ein weiterer Administrator.
- Folgt den Anweisungen auf dem Bildschirm.

Um nun die Berechtigungen und Kontrollmöglichkeiten einzurichten, klickt auf die drei Punkte oben rechts in der Kachel des zu verwaltenden Kontos, dann

- Klickt auf Zustimmung verwalten. Diese Option ist eigentlich nur für das Entfernen der Zustimmung des Elternteils zu dem Kinderkonto an sich, darunter verbergen sich aber auch die anderen Optionen.
- Klickt auf **Jugendschutz anzeigen**. Wichtig ist hier, dass mindestens ein Gerät (PC oder Notebook) mit dem Microsoft-Account angemeldet ist).
- Unter **Computerzeit** könnt ihr einstellen, wie lange der PC am Tag benutzt werden darf.
- Unter **Inhaltsfilter** könnt ihr festlegen, welche Inhalte aus welchen Kategorien verwendet werden dürfen. Das funktioniert mit Microsoft Edge, der ja der Standardbrowser in Windows ist.
- Unter **Ausgaben** gebt ihr ein Limit fest für die monatlichen Ausgaben im Windows Store und anderen Microsoft zugeordneten kostenpflichtigen Quellen an.