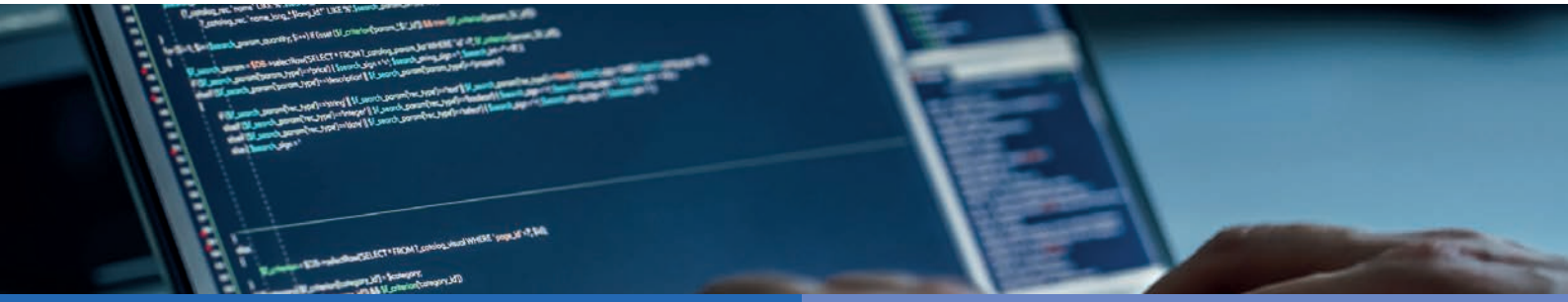
September 2023

ComConsult GmbH
Beratung + Planung + Schulung

# Der Netzwerk Insider



## Software entwickeln: nichts für Softies

**von Diplom-Inform. Univ. Stefan Hable**

Der Computer-Nerd in Hollywood-Filmen ist ein stark verkürztes Klischee: Komplexe und komplizierte Software zu entwickeln erfordert ausgeprägte Kreativität und Virtuosität, die man als Persönlichkeitsmerkmale sicher eher Musikern oder Schauspielern zuschreiben würde. Dennoch: Wenn Sie Programme entwickeln, sind Sie Welten-Erschaffer, Drehbuchautor, Schauspieler, Regisseur und Cutter in einer Person! − Na, wenn das mal keinen Spaß macht!

Seite 9

## Cybersecurity-Awareness-Trainings: Notwendiges Übel oder sinnvolle Investition?

**von Prof. Dr. Stefan Sütterlin**

Die starke Nachfrage nach IT-Sicherheits-Awareness-Trainings führt zu längeren Wartezeiten und steigenden Preisen. Bei niedrigem Qualitäts- und Weiterentwicklungsdruck ist die kritische Bewertung von Angeboten entscheidend. Der Artikel beleuchtet Schwächen, Erfolgskriterien, Risiken und innovative Ansätze solcher Trainings.

Seite 20

## Zum Entwurf des KI-Gesetzes der EU

**von Dr. Behrooz Moayeri**

Die Organe der Europäischen Union (EU), hauptsächlich der EU-Rat, die EU-Kommission und das Europäische Parlament, befassen sich mit dem Entwurf eines KI-Gesetzes (Artificial Intelligence Act, AIA). Der vorliegende Beitrag geht auf einige Aspekte des bisherigen Entwurfs ein.

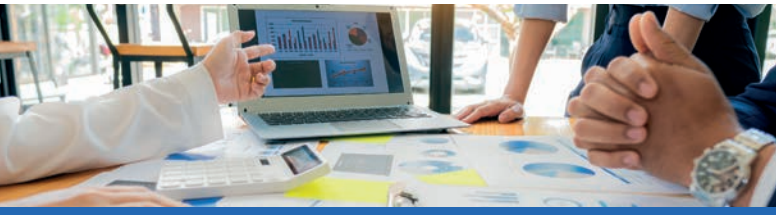
Seite 2

## Warum der IT-Support so oft einen schlechten Ruf hat – und was Sie tun können!

**von Peter Rach**

Einer meiner häufigsten Aufträge als Kommunikationstrainer ist die verzweifelte Bitte von IT-Bereichsleitern: Bringen Sie meinen Leuten bitte bei, wie man mit Kunden spricht.

Seite 36



Webinar der Woche

## Aufbau einer IT-Dokumentation

Seite 35

## Neue, schwerwiegende Sicherheitsvorfälle in der Microsoft-Welt

**von Dr. Markus Ermes**

Schwachstellen in IT-Systemen sind für uns alle alltäglich. Kaum ein Tag, an dem nicht irgendein Artikel zu Sicherheitslücken oder ein Hinweis auf ein Sicherheitsupdate ankommen. Diesmal in der Azure-Cloud von Microsoft.

Seite 33

# Zum Entwurf des KI-Gesetzes der EU

von Dr. Behrooz Moayeri

Die Organe der Europäischen Union (EU), hauptsächlich der EU-Rat, die EU-Kommission und das Europäische Parlament, befassen sich mit dem Entwurf eines KI-Gesetzes (Artificial Intelligence Act, AIA). Der vorliegende Beitrag geht auf einige Aspekte des bisherigen Entwurfs ein. Die damit verbundenen gesetzlichen und regulatorischen Entwicklungen werden höchstwahrscheinlich gravierende Auswirkungen auf die Arbeit aller Menschen haben, die Künstliche Intelligenz (KI) nutzen oder nutzen werden.

## Gesetzliche Definition von KI

Zunächst etwas aus meiner Sicht Positives: Im Anhang I des Vorschlags für eine „Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union“ (so der sperrige Titel des Entwurfs) ist eine gesetzliche Definition von KI enthalten. Demnach weist KI die folgenden Hauptmerkmale und Konzepte auf:

- Konzepte des maschinellen Lernens, mit beaufsichtigtem, unbeaufsichtigtem und bestärkendem Lernen unter Verwendung einer breiten Palette von Methoden, einschließlich des tiefen Lernens (Deep Learning),
- Durch Logik und Wissen gestützte Konzepte, einschließlich Wissensrepräsentation, induktiver (logischer) Programmierung, Wissensgrundlagen, Inferenz- und Deduktionsmaschinen, (symbolischer) Schlussfolgerungs- und Expertensysteme, sowie
- statistische Ansätze, Bayessche Schätz-, Such- und Optimierungsmethoden.

Um weltweit eindeutige Begriffe zu verwenden, kann man bei einem System von KI sprechen, wenn es Machine Learning (ML), Reasoning und Modelling anwendet.

## Gegenstand des KI-Gesetzes

Laut Artikel 1 des vorliegenden Entwurfs ist der Gegenstand des vorliegenden Entwurfs wie folgt:

- Vorschriften für das Inverkehrbringen, die Inbetriebnahme und die Verwendung von KI
- Verbote bestimmter Praktiken im KI-Bereich
- Anforderungen an Hochrisiko-KI-Systeme und Verpflichtungen für Betreiber solcher Systeme
- Transparenzvorschriften für KI-Systeme, die mit natürlichen Personen interagieren sollen, für KI-Systeme zur Emotionserkennung und zur biometrischen Kategorisierung sowie für KI-Systeme, die zum Erzeugen oder Manipulieren von Bild-, Ton- oder Videoinhalten verwendet werden
- Vorschriften für die Marktbeobachtung und Marktüberwachung

Unter Hochrisiko-KI-Systemen werden Systeme für folgende Zwecke verstanden:

- Biometrische Echtzeit-Fernidentifizierung und nachträgliche biometrische Fernidentifizierung natürlicher Personen
- Betrieb des Verkehrswesens sowie der Wasser-, Gas-, Wärme- und Elektrizitätsversorgung
- Entscheidungen über den Zugang oder die Zuweisung natürlicher Personen zu Einrichtungen der allgemeinen und beruflichen Bildung
- Bewertung von Schülern in Bildungseinrichtungen und für die Bewertung der Teilnehmer an Tests für die Zulassung zu Bildungseinrichtungen
- Einstellung oder Auswahl natürlicher Personen für freie Stellen, Sichten oder Filtern von Bewerbungen und das Bewerten von Bewerbern in Vorstellungsgesprächen oder Tests

# Software entwickeln: nichts für Softies

von Diplom-Inform. Univ. Stefan Hable

Der Computer-Nerd in Hollywood-Filmen ist ein stark verkürztes Klischee: Komplexe und komplizierte Software zu entwickeln erfordert ausgeprägte Kreativität und Virtuosität, die man als Persönlichkeitsmerkmale sicher eher Musikern oder Schauspielern zuschreiben würde. Dennoch: Wenn Sie Programme entwickeln, sind Sie Welten-Erschaffer, Drehbuchautor, Schauspieler, Regisseur und Cutter in einer Person! − Na, wenn das mal keinen Spaß macht!

## Ausräumung eines hartnäckigen Missverständnisses

Heute ist die ganze Welt computergesteuert – und das ist erst der Anfang. Ohne Software jedoch sind Computer lediglich tote, nutzlose Materie. Die Geschichte der Programmierung ist spannend, Software-Erstellung selbst allerdings komplex, anspruchsvoll und, insbesondere von außen betrachtet, mehr als verwirrend. Tatsächlich?

Was wohl kaum ein User glauben mag: Auch der Prozess der Software-Entwicklung selbst ist heute tatsächlich eine extrem spannende, faszinierende und persönlich herausfordernde Tätigkeit, die höchste Anforderungen an die Fähigkeiten und das in gewisser Weise doch sehr "spezielle" Wissen und Wesen der Entwickler stellt. Ja, ich weiß: "spannend" ist relativ, doch glauben Sie mir: Mit "spannend" meine ich auch "spannend". Und ich bin seit jeher ein extrem interdisziplinärer Mensch, der weit über IT-Horizonte hinausblickt und hinausblicken kann. IT ist schließlich kein Selbstzweck!

Bild: notebook-1071775_1280 [1]

Hinzu kommen geradezu die Eigenschaften solider Olympioniken: Hartnäckigkeit, Ausdauer, Frustrationstoleranz, Experimentierfreude, Selbstüberwindung und leider auch ganz viel Selbstdisziplin. Diese sind in fast allen Prozessphasen der Software-Entwicklung erforderlich und müssen stets abrufbar sein.

## Heutige IT ist zu 50 % Psychologie – wirklich?

Die unerfreuliche Nachricht vorneweg, gerade auch aus User-Sicht: Die Komplexität heutiger Softwareprojekte ist parallel zu der von Software selbst enorm gestiegen, nicht zuletzt durch die riesige Auswahl an Plattformen, Endgeräten, Tools und Frameworks, den für User unsichtbaren Entwickler-Werkzeugkasten,

# Cybersecurity-Awareness-Trainings: Notwendiges Übel oder sinnvolle Investition?

von Prof. Dr. Stefan Sütterlin

Die starke Nachfrage nach IT-Sicherheits-Awareness-Trainings führt zu längeren Wartezeiten und steigenden Preisen. Bei niedrigem Qualitäts- und Weiterentwicklungsdruck ist die kritische Bewertung von Angeboten entscheidend. Der Artikel beleuchtet Schwächen, Erfolgskriterien, Risiken und innovative Ansätze solcher Trainings.

## Der Boom der Awareness-Trainings

*"A company can spend hundreds of thousands of dollars on firewalls, intrusion detection systems and encryption and other security technologies, but if an attacker can call one trusted person within the company, and that person complies, and if the attacker gets in, then all that money spent on technology is essentially wasted." (Kevin Mitnick, 1963-2023)*

Die Beobachtung, dass Cyberangriffe zu einem überwiegenden Teil durch Ausnutzung menschlicher Schwächen, nämlich durch Social Engineering, durchgeführt werden, ist ein seit Langem anerkannter Fakt. Verschiedene Berichte von Purplesec, IBM Security, Verizon und anderen weisen konstant darauf hin, dass bis zu 98 % aller erfolgreichen bzw. bekannten Cyberangriffe auf diese Weise erfolgen. Trotz dieser eindrucksvollen Statistiken gibt es nach wie vor eine verbreitete Meinung, dass Cybersicherheit ausschließlich ein technisches Problem sei und dementsprechend nur technische Lösungen erfordere („einer klickt doch immer"). Diese Sichtweise verkennt jedoch das nachgewiesene Potenzial von IT-Security-Awareness-Schulungen, die sich als rasch wachsender Markt einer überproportional rasch wachsenden Nachfrage gegenübersehen. Diese Schulungen zielen darauf ab, bei den Nutzern ein Bewusstsein für grundlegende IT-Sicherheitskompetenzen zu schaffen und risikominimierende Verhaltensweisen zu vermitteln.

Die Notwendigkeit dieser Schulungen wird angesichts der steigenden Anzahl von Cyberangriffen, die Social Engineering nutzen, immer deutlicher. Die Verbesserung technischer Schutzmaßnahmen gegen Netzwerk-Kompromittierungen als Teil eines Wettrüstens zwischen Cyberkriminellen und ihren potenziellen Opfern, wie etwa durchdachte Authentifizierungsverfahren oder KI-gestützte Phishing-Filter, führt paradoxerweise dazu, dass alternative Social-Engineering-Techniken zunehmend attraktiver werden. So kann beispielsweise eine gezielte Spearphishing-Mail an einen Chief Information Security Officer (CISO) viele Schwierigkeiten und Herausforderungen bei der Durchdringung technischer Sicherheitsvorkehrungen „ressourcenschonend" umgehen.

Ein anschauliches Beispiel für die Sicherheitskonzepte komplementierende Rolle des „human factor" ist eine Studie des MIT zum sogenannten Prevalence Paradox. Die Studie zeigte, dass technische Verbesserungen von Phishing-Filtern, die zu einer spürbaren Reduktion von Phishing-Mails führten, paradoxerwei-

# Warum der IT-Support so oft einen schlechten Ruf hat – und was Sie tun können!

von Peter Rach

Einer meiner häufigsten Aufträge als Kommunikationstrainer ist die verzweifelte Bitte von IT-Bereichsleitern: Bringen Sie meinen Leuten bitte bei, wie man mit Kunden spricht. Mit Kunden sind hier nicht nur die Käufer und Nutzer einer Softwarelösung gemeint, die einen bezahlten Support gebucht haben. Auch der Inhouse-Support, z. B. der IT-Support eines Universitätskli-nikums, hat „Kunden“. Denn alle Chefärzte, Assistenzärzte, Pfleger und die Verwaltung brauchen bei Hard- und Software-Problemen schnelle Lösungen. Keiner dieser Nutzer möchte als Bittsteller abgefertigt werden. Jeder Bereichsleiter sieht seine Leute als „interne Kunden“.

Jetzt leistet ein Großteil aller IT-Support-Teams ohne Zweifel großartige Arbeit. Sie planen, installieren und administrieren komplexe Netzwerke, betreuen eine überwältigende Anzahl von Softwaresystemen, arbeiten mit hunderten oder vielleicht tausenden unterschiedlichster Hardware-Komponenten. Jeder einzelne Supportfall ist dringend und muss umgehend gelöst werden. Hinzu kommt eine täglich größer werdende Anzahl an Herausforderungen, was die IT-Sicherheit angeht. Das alles stellt höchste Ansprüche an jedes Support-Team. Und wie auch immer, sie sorgen dafür, dass alles weiterläuft.

Dennoch leiden sehr viele Support-Teams unter einem extrem schlechten Ruf. Statt der zu erwartenden Dankbarkeit und verdienten Wertschätzung schlägt Ihnen permanent eine Welle von Beschwerden entgegen. Die Ursachen dafür liegen nur teilweise in der Natur der Sache. Es kann vorkommen, dass die Technik nicht funktioniert, was den Nutzer ärgerlich stimmt. Und wenn dann nicht sofort eine Lösung möglich ist – man kann ja nicht überall gleichzeitig sein – ist der Schuldige schnell gefunden.

Im Gegenzug findet der IT-Support den Schuldigen gern auf der Gegenseite. Die (internen) Kunden sind undankbar. Oder die Nutzer stellen sich teilweise einfach dumm an: Da wird nur der Monitor eingeschaltet, jedoch nicht der PC. Doch anstatt die eigene Unfähigkeit einzugestehen, wird es lieber der IT-Abteilung angelastet. Hinzu kommt ein oft rüder Umgangston. Viele Vorstände, Chefärzte, Professoren und Bereichsleiter neigen in Ihrer Kommunikation eher zu zackigen Anweisungen als zu freundlichen Bitten. Und wenn das „Fußvolk“ dann nicht das Problem sofort beseitigt, wird mit der eigenen Wichtigkeit gedroht.

Doch mit „Schuldige suchen“ wurde noch nie ein Problem gelöst. Und auch im Strauß der Ursachen für den schlechten Ruf von IT-Bereichen gibt es noch ein paar verborgene Hebel. So ist ganz oft ein Anruf beim IT-Support für den Mitarbeiter, der gerade ein Problem hat, eine unangenehme Erfahrung. Es gibt Menschen, die ihren Mitmenschen mit Empathie, Ver-ständnis und Diplomatie begegnen. Es gibt allerdings auch Menschen, die das nicht tun – es vielleicht noch nicht einmal wollen. Die Erfahrung zeigt, dass letztere im IT-Bereich weit öfter vorzufinden sind als im Bevölkerungsdurchschnitt. Das könnte daran liegen, dass sich jene Menschen lieber mit technischen Geräten auseinandersetzen als mit anderen Menschen. Das führt dazu, dass sie einen Beruf ergreifen, bei dessen Ausübung erst einmal wenig Empathie und Diplo-