März 2023

ComConsult GmbH
Beratung + Planung + Schulung

Der Netzwerk Insider

Sicherheitskonzeption in agilen Projekten

von Oliver Flüs
Agile Entwicklung von IT-Lösungen und kontrollierte bedarfsgerechte Informationssicherheit müssen kein Widerspruch sein. Ohne feste Phasen klassischer Vorgehensmodelle muss man hierzu jedoch effizientes Vorgehen neu lernen.

Der Verzicht auf starre Phasenabfolgen und ausführliche, umfassende und detaillierte Planungsdokumentation hat seinen Preis. Die Ermittlung maßgeblicher Sicherheitsanforderungen und die Erarbeitung eines geeigneten Satzes an Sicherheitsmaßnahmen, als wirksames Sicherheitskonzept, müssen flexibel gestaltet werden.

Seite 7

Der nächste Cloud-Ausfall kommt bestimmt

von Dr. Behrooz Moayeri
Als im Oktober 2021 die wichtigsten Dienste des Facebook-Konzerns (Facebook, WhatsApp und Instagram) aufgrund einer fehlerhaften Netzkonfiguration stundenlang ausfielen, habe ich in einem kurzen Beitrag auf das Risiko von Konfiguration als Single Point of Failure hingewiesen. Vielleicht haben sich damals einige IT-Manager in Unternehmen gesagt, dass man einem geschenkten Gaul nicht ins Maul schauen dürfe.

Seite 2

Was kann ChatGPT??

von Nils Wantia und ChatGPT
Als IT-Profis wissen Sie, wie wichtig es ist, immer auf dem neuesten Stand der Technologie zu bleiben. Dabei spielt Künstliche Intelligenz eine immer größere Rolle. OpenAI hat mit ChatGPT ein KI-Modell entwickelt, das die Art und Weise, wie wir Konversationen führen, für immer verändern wird.

Seite 28

Webinar der Woche

IEC 62443:
Die perfekte Ergänzung der ISO 27001

Seite 26

Sicherheitslücke in KeyPass – und eine alte Diskussion kommt wieder auf

von Dr. Markus Ermes
Vor Kurzem ist eine Sicherheitslücke im Passwort-Manager KeyPass aufgetaucht und nach einiger Diskussion auch geschlossen worden. Doch mit einer Lücke in einem der am weitesten verbreiteten Passwort-Manager kommt wieder die Frage auf: Wie sinnvoll sind Passwort-Manager?

Seite 24

Der nächste Cloud-Ausfall kommt bestimmt

von Dr. Behrooz Moayeri

Als im Oktober 2021 die wichtigsten Dienste des Facebook-Konzerns (Facebook, WhatsApp und Instagram) aufgrund einer fehlerhaften Netzkonfiguration stundenlang ausfielen, habe ich in einem kurzen Beitrag auf das Risiko von Konfiguration als Single Point of Failure hingewiesen. Vielleicht haben sich damals einige IT-Manager in Unternehmen gesagt, dass man einem geschenkten Gaul nicht ins Maul schauen dürfe. Schließlich handelte es sich bei den allermeisten Usern der ausgefallenen Dienste um Menschen, die diese Dienste privat nutzten und nichts dafür bezahlten. Allerdings wage ich zu behaupten, dass weder die zahlenden Werbekunden von Facebook noch die vielen Firmen, die zum Beispiel Facebook und Instagram für Marketing nutzen, den Ausfall so entspannt wahrgenommen haben.

Am 25. Januar 2023 passierte Microsoft etwas ganz Ähnliches wie Facebook ca. 14 Monate vorher. Auch beim stundenlangen Ausfall wichtiger Microsoft-Cloud-Dienste wie Teams, Exchange Online, SharePoint Online und OneDrive for Business handelte es sich um ein Problem wegen einer wohl nicht ganz durchdachten Netzkonfiguration.

Anders als beim Facebook-Ausfall in 2021 verursachten die Microsoft-Cloud-Probleme im Januar 2023 Produktivitätsverluste bei hunderten Millionen Menschen, die die Microsoft-Dienste geschäftlich nutzen. Die dienstliche Nutzung von Microsoft Teams ist zum Beispiel sehr verbreitet. Ein Großteil der 270 Millionen Teams-User nutzt die UCC-Plattform von Microsoft für die Arbeit und nicht privat.

Was kostet ein Cloud-Ausfall?

Um sich ein Bild von den wirtschaftlichen Auswirkungen eines Cloud-Ausfalls zu machen, nehmen wir das Beispiel Teams. Nehmen wir an, die Produktivität eines Arbeitsplatzes, an dem Teams genutzt wird, sinke während des Ausfalls von Teams durchschnittlich um 20%. Unrealistisch ist eine solche Annahme nicht, denn an dem besagten Donnerstag mussten viele Besprechungen abgesagt werden, was sicher Auswirkungen auf Geschäftsabläufe hatte. Ferner nehmen wir an, dass sich der Ausfall überwiegend in den Zeitzonen der östlichen Hemisphäre bemerkbar machte und bis zum Dienstbeginn der User in Amerika die Probleme behoben waren. So können wir vielleicht von 100 Millionen betroffener dienstlicher User ausgehen. Als Mittelwert für den Wert einer Arbeitsstunde für den Arbeitgeber nehmen wir 100 Euro an (nicht zu verwechseln mit dem Lohnanteil allein, denn zum Lohn kommen noch die ganzen anderen Kosten für Gebäude etc. hinzu). Bei einem fünfstündigen Ausfall kommen wir also auf 100 Millionen X 5 Stunden X 100 Euro / Stunde X 20 % = 10 Milliarden Euro!

Die volkswirtschaftlichen Ausmaße eines Cloud-Ausfalls sind also immens. Wer kommt dafür auf? Der Cloud-Betreiber bestimmt nicht, denn die in solchen Fällen gutgeschriebenen Beträge berechnen sich aus den Gebühren, die der Kunde pro Arbeitsplatz für die Dienste zahlt. Die Gutschrift pro Arbeitsplatz wird also nur einen sehr kleinen Bruchteil der 100 € ausmachen, die wir oben berechnet haben. Die Kunden bleiben fast auf den ganzen Schadenskosten sitzen.

Ausfälle sind nicht nur auf die Cloud beschränkt

Zur Ehrenrettung von Microsoft und auch der anderen großen Cloud-Betreiber sei gesagt, dass Ausfälle auch außerhalb von großen Clouds passieren, und das vielleicht sogar häufiger. Den

Sicherheitskonzeption in agilen Projekten

von Oliver Flüs

Agile Entwicklung von IT-Lösungen und kontrollierte bedarfsgerechte Informationssicherheit müssen kein Widerspruch sein. Ohne feste Phasen klassischer Vorgehensmodelle muss man hierzu jedoch effizientes Vorgehen neu lernen.

Der Verzicht auf starre Phasenabfolgen und ausführliche, umfassende und detaillierte Planungsdokumentation hat seinen Preis. Die Ermittlung maßgeblicher Sicherheitsanforderungen und die Erarbeitung eines geeigneten Satzes an Sicherheitsmaßnahmen, als wirksames Sicherheitskonzept, müssen flexibel gestaltet werden. Neben dem konkreten Schutzbedarf muss fallspezifisch auf den Entstehungsverlauf der abzusichernden Lösung und auf Rahmenbedingungen für das Projektteam reagiert werden. Entsprechende Geschicklichkeit und Optionen zum Miteinander der verschiedenen Spezialisten bei agilem Vorgehen müssen erlernt und eingeübt werden.

Im Vergleich zum Einsatz klassischer Vorgehensmodelle ist der Schatz an nachlesbaren „good and best practices“ zur Einbindung des Sicherheitsmanagements und der Sicherheits-Expertise im agilen Vorgehen noch gering. Dem Lernen aus Erfahrungen durchlaufener agiler Projekte kommt hier besondere Bedeutung zu. Der vorliegende Artikel versucht, über Beobachtungen und Hinweise aus der ComConsult-Projektpraxis ein paar Beiträge zu leisten.

Agilität – Strategieanpassung auch unter Sicherheitsgesichtspunkten

Die Erstellung und Weiterentwicklung umfangreicherer Software- und IT-Lösungen erfordert eine koordinierte und planvolle Vorgehensweise. Nur so können konkrete Anforderungen gezielt erfüllt, die Ergebnisse notwendiger Arbeitsteilung effizient zusammengeführt und die Lösung geeignet in eine bestehende Umgebung eingefügt werden.

Wer Software-Entwicklung nach einer klassischen Methodik gelernt hat, ist ein Top-Down-artiges Vorgehen in Form einer mehr oder weniger formalen Anwendung eines Wasserfall-Modells gewohnt. Der Weg von Anforderungsanalyse zum erfolgreich realisierten und getesteten Ergebnis, das in einen Routinebetrieb übergeben werden kann, folgt einem Phasenmodell. Am Ende jeder Phase steht ein definiertes Ergebnis mit vorgegebener Dokumentation, die als Ausgangspunkt der Folgephase erwartet wird. Bei strenger Anwendung dieser Strategie ist eine Rückkehr in eine vorherige Phase, also ein iteratives Vorgehen bei der Lösungsentwicklung, nicht vorgesehen.

Kommt eine Rückkehr in eine eigentlich abgeschlossene Phase der Methodik und eine Anpassung an einer zum Phasenabschluss abgenommenen Dokumentation dennoch vor, sieht dies nach notwendiger Korrektur von Schwächen in der eigentlich abgeschlossenen Phase aus. Aus Sicht eines streng angewendeten Wasserfallmodell-Ansatzes musste offenbar qualitativ nachgebessert werden.

Funktioniert eine solche Vorgehensweise im konkreten Fall gut, fallen Ressourcenmanagement sowie Aufgaben der Termin- und Ressourcenplanung vergleichsweise leicht, sobald die maßgeblichen Anforderungen feststehen. Kontrollen zu den Zwischenständen und Endergebnissen einer Phase können sich gut auf Festlegungen und die Dokumentation aus den jeweils vorangegangenen Phasen stützen. Projektmanagement und strukturierte Qualitätssicherung werden so vom Vorgehensmodell der Lö-

Generationenwechsel bei ComConsult

Mit Thomas Simon sprach Christiane Zweipfennig

Jedes Jahr wollen sich nach Schätzungen der KfW mehr als 75.000 Firmeninhaber in Deutschland aus ihren Unternehmen zurückziehen. Fachkräftemangel und demografischer Wandel sind Ursachen dafür, dass ein Nachfolger immer schwerer zu finden ist. Jedes Unternehmen sollte sich daher frühzeitig mit der Planung der eigenen Nachfolgeregelung beschäftigen. Wichtige Prozessschritte werden nur oberflächlich behandelt, wenn das Thema zu spät angegangen wird.

Thomas Simon ist seit 1995 Geschäftsführer der ComConsult GmbH. 2025 wird er nach dreißig Jahren seine Position als Geschäftsführer abgeben. In diesem Gespräch erzählt er davon, wie er seine Nachfolger auf ihre neue Führungsrolle vorbereitet hat.

Thomas, kannst du bitte kurz zusammenfassen, wie sich ComConsult entwickelt hat und deine Karriere verlaufen ist?

Von der Garagenfirma zur ComConsult

Angefangen hat alles im Jahr 1986 mit einer Garagenfirma, die sich mit Softwareentwicklung beschäftigte. Als ich von der Uni kam, bin ich in diese Firma als Teilhaber eingestiegen. Es folgten zwei Umzüge innerhalb des Aachener Stadtgebietes. Mein Geschäftspartner hatte währenddessen mit dem Bau eines Bürogebäudes im Aachener Industriegebiet auf der Pascalstraße begonnen, in das wir 1991 einzogen. Vom Leiter Systemprogrammierung bin ich 1995 zum Geschäftsführer aufgestiegen, indem ich ein neues Unternehmen gründete. Ich hatte meine eigenen Vorstellungen, wie man mit dem Unternehmen umgehen sollte und habe den Bereich der Beratung ausgegliedert. Es entstand die ComConsult Beratung und Planung GmbH. 1996 kam Dr. Moayeri als technischer Direktor mit an Bord, der bis heute Miteigentümer und Gesellschafter ist. 2019 habe ich die ComConsult Akademie, die mein damaliger Geschäftspartner zwischenzeitlich gegründet hatte, erworben. Im gleichen Jahr wurde das Unternehmen in die heutige ComConsult GmbH umbenannt.

Wie hat sich die Mitarbeiterstruktur im Laufe der Zeit geändert?

Mit 20 Mitarbeitern begonnen - heute sind wir knapp 90

Gestartet haben wir vor fast dreißig Jahren mit rund 20 Mitarbeitern. Das Unternehmen ist organisch gewachsen. Heute sind es rund 90 Mitarbeiter, angefangen vom Fuhrparkleiter bis zum Doktor-Ingenieur.

Es hat sich in der Praxis eine Faustregel bewährt: Spätestens mit 55 Jahren sollte sich ein Geschäftsführer Gedanken über seine Nachfolge machen. Wie war das bei dir?

Ich war 60, als ich anfing, mich konkret mit dem Thema auseinanderzusetzen. Ein Anlass war die Nachfrage einer Bank in Zusammenhang mit einem Kredit. Wenn die Nachfolgeregelung nicht schriftlich formuliert ist, werden die Kredite teuer, weil das Risiko höher ist.

Sicherheitslücke in KeyPass – und eine alte Diskussion kommt wieder auf

von Dr. Markus Ermes

Vor Kurzem ist eine Sicherheitslücke im Passwort-Manager KeyPass aufgetaucht und nach einiger Diskussion auch geschlossen worden. Doch mit einer Lücke in einem der am weitesten verbreiteten Passwort-Manager kommt wieder die Frage auf: Wie sinnvoll sind Passwort-Manager?

Die Sicherheitslücke

Die Sicherheitslücke in KeyPass (CVE-2023-24055) ermöglichte einem Angreifer mit Nutzerrechten, eine Passwort-Datenbank in Klartext zu exportieren, da die Software eine entsprechende Richtlinie unterstützte. Selbst wenn diese vom Nutzer manuell deaktiviert wurde, war es für einen Angreifer mit Nutzerrechten natürlich wieder möglich, diese Richtlinie zu aktivieren. Daher war ein reines Deaktivieren der Richtlinie wenig hilfreich.

Die gute Nachricht: Der Entwickler hat reagiert und diese Richtlinie in der neuesten Version von Keypass nicht nur deaktiviert, sondern ganz aus der Software entfernt. Damit ist diese Sicherheitslücke definitiv geschlossen; man kann keine Funktion ausnutzen, die es nicht gibt.

Die schlechte Nachricht: Die Lücke wurde erst nach einiger Diskussion entfernt, da der Entwickler zunächst nicht wirklich einen Sinn dahinter sah, diese Sicherheitslücke zu schließen.

Um besser zu verstehen, warum diese Lücke erst einmal nicht geschlossen werden sollte, ist es sinnvoll, sich die Argumente des Entwicklers etwas genauer anzuschauen. Denn ganz unrecht hatte er nicht.

Die Argumente des Entwicklers

Wie kommt ein Entwickler auf die Idee, eine Sicherheitslücke nicht zu schließen, obwohl damit alle Passwörter eines Nutzers kompromittiert werden können?

Um diesen Standpunkt zu verstehen, muss man die Rahmenbedingungen betrachten, die ein Ausnutzen überhaupt möglich machen. Denn ein Angreifer musste die Rechte des Nutzers erlangen, der die jeweilige Passwortdatenbank erstellt hat und verwaltet. Und wenn ein Angreifer schon die Rechte dieses Nutzers hat, gibt es viele Möglichkeiten, auch anderweitig an die Passwörter zu kommen. Dazu gehören beispielsweise:

- Öffnen eines Browserfensters und Zugriff auf die Passwörter durch entsprechende Plug-Ins
- Nutzen eines Keyloggers, um die Eingabe des Master-Passworts für die Passwort-Datei mitzuschneiden
- Installation sonstiger Malware im Kontext des jeweiligen Nutzers

Der Entwickler hat es dabei recht passend ausgedrückt: Eine so wichtige Software in einer unsicheren Umgebung abzusichern, ist

Was kann ChatGPT??

von Nils Wantia und ChatGPT

Als IT-Profis wissen Sie, wie wichtig es ist, immer auf dem neuesten Stand der Technologie zu bleiben. Dabei spielt Künstliche Intelligenz eine immer größere Rolle. OpenAI hat mit ChatGPT ein KI-Modell entwickelt, das die Art und Weise, wie wir Konversationen führen, für immer verändern wird.

ChatGPT ist ein language-based KI-Modell, das auf einer enormen Menge an Texten trainiert wurde. Dies ermöglicht es dem Modell, menschenähnliche Antworten auf eine Vielzahl von Fragen und Anfragen zu geben. Seine fortschrittliche Technologie ermöglicht es ChatGPT, seine Antworten auf eine Weise zu formulieren, die für Menschen nachvollziehbar und authentisch wirkt.

Eines der stärksten Merkmale von ChatGPT ist seine Fähigkeit, auf den Kontext einer Konversation einzugehen. Es kann Verständnis für die Bedeutung von Wörtern und Phrasen in einem Gespräch entwickeln und auf dieser Basis seine Antworten formulieren. Dies gibt ChatGPT eine unvergleichliche Flexibilität und macht es zu einem wertvollen Werkzeug für eine Vielzahl von Anwendungen.

Als IT-Profis können Sie ChatGPT nutzen, um innovative Anwendungen zu entwickeln, die auf Konversationen basieren. Ob es sich um Kundenservice-Chatbots, virtuelle Assistenten oder Spiele handelt – die Möglichkeiten sind endlos. ChatGPT ist ein leistungsstarkes Werkzeug, das Ihnen dabei hilft, Ihre Ziele zu erreichen und Ihre Visionen Wirklichkeit werden zu lassen.

Und wenn Sie nicht glauben, dass ChatGPT tatsächlich recht überzeugend daherkommt, dann haben Sie mit Sicherheit längst bemerkt, dass sämtliche vorherigen Absätze vollständig von ChatGPT selbst stammen. Mit wenigen ergänzenden Angaben über das Chatfenster lässt sich ein recht allgemeiner Text aus initialem Entwurf deutlich spezifizieren. Dazu gehört in diesem Fall natürlich auch die Sprache und das ist bereits der erste bemerkenswerte Punkt. Denn natürlich ist OpenAI kein deutsches Unternehmen und ChatGPT ist kein deutsches Produkt, ansonsten würde die Torschlusspanik-Diskussion über den KI-Standort Deutschland nicht geführt werden.

Weiterhin ist die genannte Flexibilität tatsächlich beeindruckend. Ein recht allgemeiner Text im Format eines Wikipedia-Artikels (oder Teilen davon) lässt sich zu vielen Themen problemlos finden. Dass dieser bei Bedarf jedoch plausibel angepasst werden kann, macht die Sache interessant, denn dazu ist eine nicht triviale Transferleistung notwendig. Die Betonung liegt dabei jedoch auf ‚plausibel', denn nicht immer ist der Inhalt der Texte tatsächlich zu 100 Prozent sinnvoll und teilweise sind Aussagen schlichtweg falsch. Das System ist ziemlich gut darin Banalitäten oder gar Falschaussagen so zu formulieren, dass man es auf den ersten Blick nicht mitbekommt. Immerhin beschreibt sich ChatGPT sogar selbst so: „Antworten auf eine Weise zu formulieren, die für Menschen nachvollziehbar und authentisch wirkt" (siehe oben). Insofern muss man sich manchmal schon fragen was genau man mit dem Werkzeug eigentlich erreichen möchte. Wenn es um die Schwächen von ChatGPT geht, kann das System sich wiederum ganz gut selbst beschreiben:

ChatGPT hat als Sprachmodell einige Schwächen, die es verbessern kann, um seine Leistung zu verbessern. Eine der größten Schwächen ist, dass es oft Schwierigkeiten hat, die Kontextualität einer Frage richtig zu verstehen und dementsprechend eine relevante Antwort zu geben. Ein weiteres Problem ist, dass es manchmal fehlerhafte oder unangemessene Antworten gibt, insbesondere auf Fragen, die moralische oder ethische Aspekte betreffen. Es ist auch noch nicht in der Lage, emotionale Intelligenz auszudrücken, wie sie von Menschen erwartet werden könnte. Es ist wichtig zu beachten, dass ChatGPT ein maschinelles Lernmodell ist und daher nur so gut ist wie die Daten, die es trainiert wurden. Um seine Schwächen zu überwinden, muss es mit besseren und vielfältigeren Daten trainiert werden, um ein besseres Verständnis für den Kontext und die Bedeutung von Fragen und Antworten zu entwickeln.

Abschließend kann gesagt werden, dass ChatGPT ein fortschrittliches Sprachmodell ist, dass jedoch noch Verbesserungen benötigt, um eine bessere Leistung zu erreichen. Es ist wichtig, dass es ständig weiterentwickelt und verbessert wird, um eine höhere Genauigkeit und Zuverlässigkeit in seinen Antworten zu erreichen.