Januar 2025

ComConsult GmbH
Beratung + Planung + Schulung

Der Netzwerk Insider

Schon wieder Security-Awareness-Schulungen…

von Maren Poppe
Für viele Beschäftigte sind Schulungen zur Informationssicherheit ein notwendiges Übel, das sich in die jährlichen Durchklick-Marathons zu Datenschutz und Arbeitssicherheit einreiht. Meist zählt weniger der Lernerfolg für die Teilnehmenden, als möglichst schnell damit fertig zu sein. Aufgabe des Informationssicherheitsbeauftragten ist es, das zu ändern – aber wie?

Seite 7

Hitliste der IT-Projekte

von Dr. Behrooz Moayeri
ComConsult-Mitarbeiter haben in 2024 in ungefähr 300 Projekten gearbeitet. Da unser Leistungsspektrum die Schwerpunkte der Tätigkeit der IT-Abteilungen unserer Kunden widerspiegelt, lässt sich anhand der bei ComConsult obligatorischen Zeiterfassung in Projekten gut ablesen, womit sich die IT in verschiedenen Organisationen beschäftigt. Die Betrachtung einer dreistelligen Anzahl von Organisationen verschiedener Branchen ermöglicht dabei eine Analyse mit einem hohen Grad an statistischer Signifikanz.

Seite 2

Der Strukturwandel, immer größere Rechenzentren und hohe Standortanforderungen

von Dr. Johannes Dams
Nicht weit vom Standort der ComConsult in Aachen entfernt im Rheinischen Braunkohle-Revier findet ein Strukturwandel statt, wie es ihn in der Vergangenheit selten gegeben hat. Die Stilllegung der Braunkohle-Tagebaue und die Abschaltung der Braunkohlekraftwerke stellen eine besondere Herausforderung für Politik und Wirtschaft dar.

Seite 14

Webinar der Woche

Java – Ihr Einstieg in die Softwareentwicklung

Seite 19

Finanzieller Betrug per Man-in-the-Middle und Quishing

von Dr. Markus Ermes
Immer wieder liest und hört man in einschlägigen Medien, dass per Ransomware signifikante Geldbeträge erpresst werden können, oder dass sensible Daten nach einem erfolgreichen Einbruch in Systeme im Darknet verkauft werden.

Seite 20

Hitliste der IT-Projekte

von Dr. Behrooz Moayeri

ComConsult-Mitarbeiter haben in 2024 in ungefähr 300 Projekten gearbeitet. Da unser Leistungsspektrum die Schwerpunkte der Tätigkeit der IT-Abteilungen unserer Kunden widerspiegelt, lässt sich anhand der bei ComConsult obligatorischen Zeiterfassung in Projekten gut ablesen, womit sich die IT in verschiedenen Organisationen beschäftigt. Die Betrachtung einer dreistelligen Anzahl von Organisationen verschiedener Branchen ermöglicht dabei eine Analyse mit einem hohen Grad an statistischer Signifikanz.

Welcher Bereich nimmt den Spitzenplatz ein?

Bevor Sie weiterlesen, können Sie raten, welcher Bereich den Spitzenplatz in der Hitliste der Projekte belegt. Und Ihre Vermutung wird sehr wahrscheinlich richtig sein: Es ist die Informationssicherheit, für die wir in Projekten im Vergleich zu anderen Schwerpunkten am meisten tätig werden.

Das Themenfeld Informationssicherheit ist in unseren Projekten breit gefächert. Für eine zunehmende Anzahl von Organisationen werden wir tätig, weil diese Organisationen aus regulatorischen Gründen ihre IT-Sicherheitslösungen und die zugehörigen Prozesse dokumentieren müssen. Dieser Dokumentationsaufwand nimmt aufgrund der steigenden Anzahl von Regularien wie KRITIS und NIS2-Richtlinie zu. Auch Regularien, die einen abweichenden Fokus von der Informationssicherheit im engeren Sinne haben, sind zu berücksichtigen, wie DSGVO und sicher auch die jetzt einzuhaltende KI-Verordnung der Europäischen Union.

Neben der Dokumentation zu Zwecken der Einhaltung der Regularien und der Vorbereitung auf Audits verursacht die Umsetzung von Maßnahmen, die in den vergangenen Jahren nicht im großen Stil implementiert wurden, einen signifikanten Aufwand. Besonders zu nennen sind hier die Projekte rund um das Security Information and Event Management (SIEM) und den Aufbau von Einrichtungen namens Security Operations Center (SOC).

Einige spezielle Technik-Gebiete tragen ebenfalls zur Grundlast im Bereich IT-Sicherheit bei, zum Beispiel Network Access Control (NAC).

Netze und Infrastrukturen sind regelmäßig zu modernisieren

Bevor ich auf weitere Schwerpunkte in IT-Projekten eingehe, muss ich einschränken, dass die ComConsult-Sicht auf das Tätigkeitsfeld der IT-Abteilungen den selbstverständlich großen Bereich der Fachapplikationen weitgehend ausklammert. Unter Fachapplikationen meine ich hauptsächlich sogenannte branchenspezifische Lösungen mit zugehöriger Software. ComConsult befasst sich in Projekten hauptsächlich mit branchenunabhängigen Technologien und Lösungen. Jede IT-Abteilung muss sich jedoch neben den nichtbranchenspezifischen Lösungen auch mit Fachanwendungen befassen, die für die betreffende Organisation relevant sind.

Diese Einschränkung vorweggeschickt, komme ich auf zwei Tätigkeitsschwerpunkte, die – getrennt betrachtet – in der Hitliste der Projekte direkt auf die Informationssicherheit folgen. Zusammen genommen übertreffen sie sogar die Tätigkeit im Bereich der Informationssicherheit. Ich meine die Disziplin „Netze und Infrastrukturen“. Wir haben bei ComConsult seit Jahrzehnten die diesbezüglichen Spezialisierungen arbeitsteilig in zwei Bereiche aufgeteilt: passive und aktive Infrastrukturen. Ersteres ist in der Regel fest mit Gebäuden verbunden und hat einen längeren Lebens- und Abschreibungszyklus. Als ich vor über 35 Jahren angefangen habe, Organisationen beim Aufbau von Netzen und Infrastrukturen zu beraten, gab es ein wichtiges Ziel: Die informationstechnische Verkabelung muss mindestens 10 Jahre nutzbar sein. Mit ein bisschen Stolz kann ich nun sagen, dass wir dieses Ziel weit übertroffen haben. Beispiel ist unser eigenes Bürogebäude: Die IT-Verkabelung darin wurde vor ungefähr einem Vierteljahrhundert aufgebaut und hat sich seitdem nicht geändert.

Einen derart langen Lebenszyklus kann man beim aktiven Netz

Schon wieder Security-Awareness-Schulungen…

von Maren Poppe

Für viele Beschäftigte sind Schulungen zur Informationssicherheit ein notwendiges Übel, das sich in die jährlichen Durchklick-Marathons zu Datenschutz und Arbeitssicherheit einreiht. Meist zählt weniger der Lernerfolg für die Teilnehmenden, als möglichst schnell damit fertig zu sein. Aufgabe des Informationssicherheitsbeauftragten ist es, das zu ändern – aber wie?

Um die Mitarbeitenden für wichtige Themen zu begeistern und ihr Mitwirken zu garantieren, gibt es viele Ansätze. Vielleicht fragen sich einige Leser, weshalb ich Mitarbeiter für Regelungen begeistern muss, an die man sich schlicht und ergreifend halten muss. Für andere Themen wie zum Beispiel Arbeitszeiterfassung ist schließlich auch kein extra Aufwand nötig: Es gibt Regelungen innerhalb des Unternehmens, und hält sich jemand nicht daran, werden entsprechende Disziplinarmaßnahmen eingeleitet. Dafür braucht es keine Begeisterung.

Beim Thema Informationssicherheit ist das leider nicht so einfach: Es gibt viele Maßnahmen, deren Einhaltung nicht direkt nachvollziehbar ist. Beispielsweise kann ich nicht messen, ob ein Mitarbeiter E-Mails bei der Bearbeitung gewissenhaft prüft, die Absenderadresse mit dem angezeigten Namen vergleicht, bei Hyperlinks die URL vor dem Klicken prüft und Dateianhänge durch einen Virenscan absichert. Auch wenn ich keinen Sicherheitsvorfall erlebe, kann ich als Informationssicherheitsbeauftragte nicht davon ausgehen, dass alle meine Kollegen die Maßnahmen durchführen. Spätestens bei einem Sicherheitsvorfall merke ich dann jedoch, dass diese offenbar nicht eingehalten wurden – vielleicht auch nur dieses eine Mal, weil der betreffende Kollege, der sonst sehr gewissenhaft ist, bloß einen schlechten Tag hatte. Außerdem ist der potenzielle Schaden bei Verletzung von Regelungen der Informationssicherheit signifikant höher als, wie beim Beispiel oben, bei falsch oder nicht eingetragenen Arbeitszeiten. Sie betreffen nicht nur eben jenen Kollegen, sondern das ganze Unternehmen, wenn nicht sogar deren Kunden und Lieferanten.

Security-Awareness-Kampagnen

Gerade im Bereich der Informationssicherheit haben sich daher Security-Awareness-Kampagnen durchgesetzt. Wie der Name schon sagt, geht es um Aktionen, die das Bewusstsein für Informationssicherheit bei der Belegschaft steigern sollen. Ein Bewusstsein oder auch eine persönliche Motivation für dieses Thema greift die gerade beschriebene Begeisterung auf: Für ein erfolgreiches Informationssicherheitsmanagement ist es notwendig, dass zumindest ein Großteil der Mitarbeiter verstanden hat, was auf dem Spiel steht und gleichzeitig bereit ist, einen Teil dazu beizutragen. Nach meiner Erfahrung ist genau das, was nicht messbar ist, der wichtigste Teil: die tatsächliche Anteilnahme bzw. das Sich-Verantwortlich-Fühlen auch über die eigenen konkreten Aufgaben hinaus.

Informiert man sich über Angebote zu Awareness-Maßnahmen, stolpert man schnell über Phishing-Kampagnen. Ein Anbieter sendet in Absprache mit dem Unternehmen gutartige Phishing-Mails an alle Mitarbeiter. Überprüft wird, ob und wenn ja wie viele Mitarbeiter auf die in den Mails platzierten Links klicken. Anhand der Ergebnisse kann ein Schulungsbedarf festgestellt werden, auch bezogen auf eine spezielle Abteilung. Der Lerneffekt geht über die bloße Information in einer Schulung, nicht auf potenziell bösartige Links zu klicken, hinaus. Denn ein Mitarbeiter, der den betreffenden Link klickt, ist auf einmal persönlich involviert. Einen Fehler, den man einmal gemacht hat, sei es auch in einem simulierten

Der Strukturwandel, immer größere Rechenzentren und hohe Standortanforderungen

von Dr. Johannes Dams

Nicht weit vom Standort der ComConsult in Aachen entfernt im Rheinischen Braunkohle-Revier findet ein Strukturwandel statt, wie es ihn in der Vergangenheit selten gegeben hat. Die Stilllegung der Braunkohle-Tagebaue und die Abschaltung der Braunkohlekraftwerke stellen eine besondere Herausforderung für Politik und Wirtschaft dar. Hierbei hat die NRW-Landesregierung die Umsetzung der fortschreitenden Digitalisierung zu einem der Eckpfeiler dieses Umbaus gemacht. Tatsächlich haben die aktuelle Debatte um KI und der damit verbundene Bedarf an Rechenzentrumskapazität diesen Strukturwandel und die Planung von Rechenzentrumsflächen zusätzlich befeuert. Die Dateninfrastruktur wird damit Grundlage des Strukturwandels.

Abbildung 1: So tief muss natürlich keine Baugrube für ein RZ sein

Dies bietet uns als Planer und Berater die Gelegenheit, weiterführende Einblicke in RZ-Dimensionen zu gewinnen, die wir bei unseren üblichen Kunden eher selten erhalten. Die verschiedenen Projekte überbieten sich hierbei hinsichtlich Projektgröße und Umfang – beginnend mit der Ansiedlung von Microsoft als Hyperscaler, die durch die Presse ging (Pressemitteilung der Stadt Bedburg, https://www.bedburg.de/Aktuelles/Doppelpack-fuer-die-Region-Weltkonzern-Microsoft-kommt-nach-Bedburg-und-Bergheim.html). In der Tat stehen wir als ComConsult in einem ähnlichen Projekt einem Kunden mit einer Grobkonzeption bzgl. der Netzwerkinfrastruktur zur Seite.

Anforderungen an moderne IT-Standorte

Die Standort-Werbung durch das Land NRW und die Ansiedlung von Microsoft haben den Bedarf an entsprechenden Flächen in der Region weiter erhöht. Um Anforderungen und Bedarfe klar zu definieren, wurde dabei vonseiten des Landes mit verschiedenen Partnern eine Machbarkeitsstudie für solche Digitalpark- und RZ-Flächen erstellt (Studie des Landers NRW, https://www.wirtschaft.nrw/pressemitteilung/dateninfrastruktur-rheinisches-revier).

Hieraus lassen sich einige spannende Anforderungen ablesen, die aufzeigen, welche Aspekte im Bereich der Hyperscaler-Planung und vielleicht auch der Planung von IT-Standorten im Allgemeinen zu berücksichtigen sind.

Konkret befasst sich die Studie mit Standorten für Hyperscaler-

Finanzieller Betrug per Man-in-the-Middle und Quishing

von Dr. Markus Ermes

Immer wieder liest und hört man in einschlägigen Medien, dass per Ransomware signifikante Geldbeträge erpresst werden können, oder dass sensible Daten nach einem erfolgreichen Einbruch in Systeme im Darknet verkauft werden. Und ja, die potentiellen Schäden für einzelne Betroffene können enorm sein. Und selbst wenn nur ein kleiner Teil der Betroffenen das geforderte Lösegeld zahlt oder die erbeuteten Daten nur in wenigen Fällen zu hohen Preisen verkauft werden, sind die Gesamtschäden enorm. Es wird geschätzt, dass 2023 über 1 Milliarde US-Dollar an Lösegeldern geflossen sind.

Doch es gibt noch andere Möglichkeiten für Cyberkriminelle, Leute um ihr Geld zu bringen. Jede Einzelne von diesen aufzuzählen würde den Rahmen dieses Standpunkts sprengen, daher möchte ich hier auf zwei Angriffsformen eingehen, die in den letzten Monaten häufiger vorkommen: Man-in-the-Middle-Angriffe für Rechnungen sowie „Quishing“.

Erstere Angriffsform nutzt dabei klassische Ansätze des Social Engineering, Quishing nutzt die Bequemlichkeit, jedoch auch die schlechte bis nicht vorhandene Lesbarkeit von QR-Codes aus. Was genau steckt dahinter?

Man-in-the-Middle und Rechnungen

Auch wenn wir in der Informationssicherheit viele Formen des „Man-in-the-Middle“-Angriffs kennen, vom Abhören von Kommunikation bis hin zur Manipulation von Daten, sind diese meistens mit verschiedenen technischen Ansätzen auf Netzwerkebene verbunden.

Seit einigen Monaten gibt es eine neue Form von „Man-in-the-Middle“, die auch in den allgemeinen Medien zu finden ist: Hier werden E-Mail-Accounts von Dienstleistern und Handwerkern geknackt, meistens per Social Engineering oder Phishing.

Der Clou bei der Sache: Hat ein Angreifer Zugriff auf das E-Mail-Postfach einer Firma, werden bereits an Kunden versandte Rechnungen manipuliert und erneut verschickt. Die Manipulation betrifft dabei insbesondere die aufgeführte Bankverbindung. Natürlich ist es verdächtig, wenn ein Kunde zweimal die gleiche Rechnung mit einer anderen IBAN erhält. Daher wird (vom Angreifer) zusätzlich darauf hingewiesen, dass sich die Bankverbindung geändert hat und daher die Rechnungssumme auf das „neue“ Konto zu überweisen ist. Dieses Konto gehört natürlich nicht der kompromittierten Firma, sondern dem Angreifer oder einem Strohmann. Und hat das Opfer, dem die Rechnung zugeschickt wird, erst einmal bezahlt, kommt irgendwann die Mahnung mit den korrekten Bankdaten. Zu diesem Zeitpunkt ist das auf das falsche Konto überwiesene Geld schon weg.

Der Begriff „Man-in-the-Middle“ trifft es also schon recht gut, und es gibt viele Parallelen zu Man-in-the-Middle-Angriffen z.B. auf Webseiten, bei denen ein Angreifer die Daten, die ein Client von einem Server erhält, manipuliert. Hier haben sich allerdings Mechanismen wie TLS durchgesetzt und machen die Angriffe speziell im Internet deutlich schwieriger.

Bei der neuen Angriffsform spielt, wie so häufig, der menschliche Faktor eine große Rolle. Bei der kompromittierten Firma ist es ein eventuell schlecht abgesichertes E-Mail-Postfach, beim zahlen-