Nummer des Beitrages	Titel des Beitrages	Name Beiratsmitglied	Entspricht der Beitrag den		Ist der Beitrag übersichtlich				Aktualität in		Originalità		Fachlich		Welchem Thema lässt sich der Beitrag zuordnen?																				möchte den Beitrag in das Programm aufnehm					Durchschnittsbewertung	Gesamturteil des Beitrages
			Ja	Nein	1	2	3	4	Ja	Nein	Ja	Nein	Ja	Nein	5G / NESAS	Aktuelle Entwicklungen in der Kryptographie	Automotive und vertrauenswürdige Lieferketten	(Basis-)Technologien für sichere IT-Systeme (Secure Elements, TPMs, Virtualisierung, OS, ...)	Cloud Computing	Cyber-Sicherheit in der Wirtschaft	Digitaler Verbraucherschutz	Incident Response	IoT-Sicherheit	IT-Sicherheit und Recht	Management von Informationssicherheit	Maschinelles Lernen, Künstliche Intelligenz (KI)	Mediale Identitäten	Messenger	Nicht-Standard-IT-Systeme: Operationelle Technologien, Produktions- und Steuerungssysteme, Embedded Systeme, ...	SecOps	Sichere Digitalisierung der Verwaltung (z.B. digitale Zusammenarbeit)	Sicherheit Kritischer Infrastrukturen	Sichere VS-IT Systeme	Threat Intelligence	Usable Security - Faktor Mensch in der IT-Sicherheit	Zertifizierung	1	2	3	4	5		
2			1	0	0	0	1	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0		Der Beitrag fÃ¼hrt zwar eine Bedrohungslage (Social Engineering) mit PrÃventionsmaÃ¶nahmen zusammen. Allerdings erschÃ¶pft sich der Beitrag in der etwas ermÃ¼denden Systematik "Angst machen" und dann "mehr Sicherheit einfÃ¼hren". Die vorgeschlagenen MaÃ¶nahmen lassen dabei eine AbwÃ¤gung verschiedener SicherheitsmaÃ¶nahmen sowie ein Ris komanagement vermissen. Insgesamt kein ungeeigneter Beitrag aber nicht in den besten 25%.
2			**1**	**0**	**0**	**0**	**0**	**1**	**1**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**1**	**0**	**3**	**Gut strukturierter und fachlich korrekt aufbereiteter Beitrag. Inhaltlich fÃ¼r Expertenkreise keine Neuigkeit, fÃ¼r Interessierte und Neulinge im Thema / auf dem Kongress aber sicherlich spannend und bereichernd. Der Vortrag verspricht unter hinzunehmende von Praxisbeispielen einen spannenden Slot.**
2			**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**1**	**0**	**0**	**0**		**Der Beitrag stellt einen hypothetische Angriff vor, in dem ein C-Level-Entscheidungsträger mit Hilfe von OSINT und KI nachgeahmt wird, um dem Opfer im Unternehmen Anweisungen zu geben. Die Opfer werden mit Hilfe von NLP (Neurolinguistisches Programmieren) untersucht. Es werden keine Details zu den o.g. Verfahren genannt, auch die Machbarkeit ist unklar. NLP ist eine relativ zweifelhafte Technik, deren Wirksamkeit wissenschaftlich vÃ¶llig unklar ist. Insgesamt ist der Beitrag nicht glaubwÃ¼rdig.**
5			**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**2,7**	**Studentischer Vortrag - positiv zu wÃ¼rdigen. Inhaltlich keine wirklich neuen DenkanstÃ¶Ãe, vielmehr ein Ãœberblicksartikel. Angesichts der Tatsache, dass viele Unternehmen an den grundlegenden Sicherheitsmaßnahmen scheitern, dennoch ein nicht zu vernachlÃ¤ssigender Beitrag. Von der FlughÃ¶he her ein Vortrag, der in wenigen Minuten viel Grundlagenwissen vermitteln kann. Vor allem die Betrachtung der Risiken von (Passwort-)Richtlinien ist ein erfrischender Blickwinkel, der nicht allzu hÃ¤ufig eingenommen wird. Aufnahme wird empfohlen.**
5			1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0		Thema Passwortrichtlinie erscheint in den Nachteilen zu negativ die VorschlÃ¤ge zur Verbesserung sind einseitig. Die Handhabung und Vorgehensweise erscheint wenig innovativ.
5			**1**	**0**	**0**	**1**	**0**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**		**Im Beitrag werden Passwortrichtlinien genannt, die sehr unsicher und gefÃ¤hrlich sind, wie z.B. "Richtlinien, die Wochentage, Monate, Jahre etc. mit Buchstaben und Sonderzeichen verknÃ¼pfen (Samstag, 2021 = Passwort: S2a0m2%1g". Ein Unternehmen, das solche Richtlinie aufstellt, kann es hoffentlich nicht geben. Der Beitrag besteht aus offensichtlichen Behauptungen, z.B. "Die Passwortrichtlinie vereinfacht Prozesse im Betrieb"., die niemanden helfen. Als Abhilfe gegen "durchsichtige" Richtlinien wird "HÃ¤ufiges Ã„ndern der gesamten Richtlinie" vorgeschlagen, was von der Usability-Perspektive ein Horror ist.**
6			**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**		**Abstract ist gut formuliert und stellt eine gute Ãœbersicht Ã¼ber die aktuelle Situation und die gegebenen Herausforderungen vor. OriginÃ¤re BeitrÃ¤ge zur LÃ¶sung dieser Herausforderungen sind aber nicht zu erkennen.**
6			**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**		**Der Beitrag bringt zwar keine neuen wissenschaftlichen Erkenntnisse macht aber klar, dass aufgrund der neuen TechnologieansÃ¤tze Handlungsbedarf herrscht und zeigt auch die wesentlichen Unterschiede zur bisherigen Situation auf. Im Sinne eines Ãœberblickes wÃ¤re der Beitrag daher anzunehmen.**
6			1	0	0	0	0	1	1	0	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	**3,7**	Der Beitrag behandelt das Thema Kryptoag itÃ¤t vor dem Hintergrund der Migration auf Post-Quanten Kryptografie. Er beschreibt dabei die Herausforderungen dieses komplexen Themas. Dabei wird auf die Unterschiede von klassischer und Post-Quanten Kryptografie eingegangen und welche Herausforderungen sich im Bezug auf Kryptoagilität daraus fÃ¼r Hardware PKIen Protokolle und in der Praxis ergeben. Es werden ebenfalls ausgewÃ¤hlte Forschungsprojekte zu einzelnen Themen genannt. Der Beitrag liefert damit wichtige Erkenntnisse und zeigt auf was bei der Migration zu quantencomputerresistenter Kryptografie zu beachten ist. Ich empfehle daher den Beitrag anzunehmen. Ein Kommentar zu Abbildung 1: Diese ist stark vereinfacht und zeigt nicht wie moderne Gitter-basierte VerschlÃ¼sselung tatsÃ¤ch ich funktioniert (wÃ¼rde man so verschlÃ¼sseln wÃ¤re das Verfahren unsicher). Ich empfehle daher die Grafik zu entfernen bzw durch eine Grafik die Gitter-Probleme wie SVP oder BDD zeigt zu ersetzen.
7			**1**	**0**	**0**	**0**	**0**	**1**	**1**	**0**	**0**	**1**	**1**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**		**Der Beitrag ist nicht neu, sondern wurde in der vor iegenden/Ã¤hnlichen Form schon auf verschiedenen Veranstaltungen gehalten. Die Darstellung der Verfahren mittels Cartoos ist recht originell, ein wesent icher Beitrag zum tieferen VerstÃ¤ndnis der Verfahren oder der aktuellen Herausforderungen ergibt sich allerdings nicht.**
7			1	0	0	0	1	0	1	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0		Die I lustrationen geben den Sachverhalt der einzelnen Verfahren so stark simplifiziert wieder dass der eigentliche Bezug zu den genannten PQ-Verfahren kaum oder nicht erkennbar ist. Die Simplifizierungen sind te lweise auch nicht korrekt. Zum Beispiel ist die Veranschaulichung von multivariaten Verfahren mit dem Leiterproblem nicht adÃ¤quat gewÃ¤hlt da das Leiterproblem nur ein univariates Problem ist das grundsÃ¤tzlich leicht zu lÃ¶sen ist. Bei der Einreichung besteht daher das Problem dass die Sachverhalte falsch wiedergegeben werden. Insgesamt empfehlen wir den Beitrag abzulehnen.
7			**1**	**0**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**		**2**	**Die Einreichung kÃ¼ndigt einen didaktisch aufbereiteten Satz von Cartoons an, um PQ-Verfahren zu erklÃ¤ren. Leider wird weder der theoretische Ansatz (welche didaktischen Ideen stecken hinter den Cartoons) noch deren praktischer Einsatz (z.B. der erwartete Vorkenntnis-Stand der Zielgruppe beleuchtet), stattdessen werden im Beitrag die PQ-Verfahren erklÃ¤rt, die die Leser bereits kennen. Genauso wir angekÃ¼ndigt, bei Akzeptanz den Vortrag ausschließlich aus Cartoons zu gestalten â€“ auch hier scheint mir der Sinn fragwÃ¼rdig, die ZuhÃ¶rer wollen ja nicht die PQ-Verfahren verstehen, sondern die Cartoons und wie sie einzusetzen sind. Es ist auch nicht klar, wem die Cartoons zur VerfÃ¼gung gestellt werden: Werden sie frei im Internet verÃ¶ffentlicht, ist die Herausgabe eines Buches damit geplant, sind Begleitmaterialien vorgesehen? Die drei Beispiel-Cartoons folgen keinem erkennbaren didaktischen Konzept (inkonsistente â€žErklÃ¤rgestaltâ€œe, unklare Begriffe). CRYSTALS-DILITHIUM 2x CRYPTALS geschrieben.**
8			**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**		**Gute Argumentation fÃ¼r Security by Design in der Anlagenplanung, ergÃ¤nzt mit einem Vorgehensmodell**
8			1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	**3,7**	Heutzutage wird die IT-Sicherheit am Ende oder nachtrÃ¤glich berÃ¼cksichtigt was i. d. R. eine schlechtere Absicherung oder Kostensteigerungen zur Folge hat. Insofern ist der Beitrag aktuell. Er stellt die Lage und Entwicklungen im betrachteten Pharma und IT-Sicherheit dar und deutet das SpannungsverhÃ¤ltnis zwischen IT-Sicherheit und der regulativen Anforderungen an. Relevante Standards werden in der Gliederung benannt und im Text teilweise erwÃ¤hnt. CCE wird nicht erwÃ¤hnt. Insbesondere der B3S Pharma und der Zusammenhang mit KRITIS erscheinen hier besonders relevant. Der Beitrag weiÃŸt keine besonderen fach ichen MÃ¤ngel auf jedoch gibt es sprach iche MÃ¤ngel (Wortwahl Zeichensetzung). DarÃ¼ber hinaus ist die Auswahl der Beispiele zur Lagedarste lung suboptimal und untermauert die Aussagen wenngleich diese aber richtig sind nicht in vollem Umfang. Insgesamt bleibt der Abstract leider hinter dem aus der Gliederung zu erwartenden Inhalt zurÃ¼ck. Daher gehÃ¶rt der Beitrag trotz des relevanten Themas nicht zu den besten 25%.
8			**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**		**Thema ist relevant und der Beitrag will Problematik und LÃ¶sungsansatz fÃ¼r Security by Design in Pharma- und Biotechnologie aufzeigen; sicherlich ein konstruktiver Beitrag zur notwendigen Umsetzung von Sicherheit.**
9			1	0	0	0	0	1	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	**4,7**	Der Beitrag so lte unbedingt angenommen werden. Der Beitrag ist gut geschrieben und Ã¼bersichtlich geg iedert. Die Fragestellung wurde in der Ausgangslage benannt und gut erlÃ¤utert. Der zur LÃ¶sung des Problems gewÃ¤hlte Ansatz (Atomisierung von Anforderungen und toolgestÃ¼tzte Erfassung von Meta-Informationen Ã¼ber Anforderungen auf Einzelanforderungsebene) ist aus unserer Sicht sehr vielversprechend. Als nachteilig ist jedoch zu bewerten dass die Auseinandersetzung mit der Literatur und den Werkzeugen (Tools) im Themenbereich des Beitrags fehlt bzw. unzureichend erfolgte. Auch bleibt es unklar ob der hier dargeste lte Ansatz in der Praxis tatsÃ¤ch ich funktioniert da der produktive Einsatz erst fÃ¼r 2022 geplant ist. Nichtsdestotrotz sollte das Paper unbedingt angenommen werden weil es ein Problem mÃ¶glicherweise lÃ¶st das in der Praxis von groÃŸer Relevanz ist.
9			**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**			**Beitrag stellt einen interessanten Ansatz fÃ¼r die Praxis dar. Der LÃ¶sungsansatz bedarf weiterer ErlÃ¤uterungen.**
9			**1**	**0**	**0**	**0**	**0**	**1**	**1**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**		**Der Ansatz ist dringend nÃ¶tig. TatsÃ¤chlich kann er noch weiter ausgedehnt werden, Einbindung von SOPs (Standard Operating Procedures) etc. mÃ¼ssen noch kommen, als agilerer Ansatz zum PapiergestÃ¼tzten Prozess unbedingt zu empfehlen. Bin mir nicht ganz sicher, ob ich den zahlreichen Case Studies oder Use Cases glaube, aber trotzdem sehr wichtig das mal rauszustellen!**
10			1	0	0	0	0	1	1	0	0	1	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	**3,7**	Der Beitrag hat einen starken datenschutzrechtlichen Einschlag. Er ist aber durchaus gut strukturiert und fÃ¼hrt anhand eines gut nachvollziehbaren Szenarios in die Haftungsfragen nach einem IT-Sicherheitsvorfalles ein.
10			**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**		**Der Beitrag beschÃ¤ftig sich mit den rechtlichen Impl kationen bezogen auf Datenschutz und IT-Sicherheit, die sich aus Sicherheitsvorfällen fÃ¼r einen IT-Dienstleister ergeben. Die AusfÃ¼hrungen machen insgesamt einen sehr guten Eindruck - allerdings bin ich kein Jurist und kann dies insofern auch nur eingeschrÃ¤nkt einschÃ¤tzen. Die behandelten Fragestellungen sind jedenfalls sehr relevant. Die AusfÃ¼hrungen wirken fundiert.**
10			**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**		**Beitrag bezieht sich auf eine in 2021 aufgetretene SicherheitslÃ¼cke und Folgen hieraus, Ergebnisse kÃ¶nnen ggf. aber auch auf andere FÃ¤lle Ã¼bertragen werden.**
11			1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	**3,3**	Der Beitrag behandelt ein aktuell relevantes Thema ("Zero Trust Networking") in einem konzeptionellen Ansatz. Das Paper verspricht unterschiedliche Modelle zu beleuchten und MÃ¶glichkeiten einer Kombination dieser zu prÃ¤sentieren. Dabei beschrÃ¤nkt sich das Paper nicht auf den hÃ¤ufig zitierten "Cloud"-Anwendungsfall sondern beschreibt den allgemeinen Ansatz von dem auch Unternehmen / BehÃ¶rden ohne starke Cloud-Nutzung profitieren kÃ¶nnen. Der Beitrag selbst gibt eine Ãœbersicht der bestehenden Zero Trust Konzepte (mit Fokus auf Networking) er erarbeitet dabei nichts eigenstÃ¤ndiges innovatives. Das Thema wird aber auch ohne eigene Innovation durch den Vortragenden als relevant (insbesondere fÃ¼r alle Infrastrukturbetreiber) angesehen.
11			**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**		**Basis-Ãœberblick Ã¼ber Trustless Networks, keine neuen Erkenntnisse, nur interessant fÃ¼r jemand, der noch nie von dem Konzept gehÃ¶rt hat.**
11			**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**			**Eine gelungene Vorstellung des Zero-Trust-Networking-Konzepts. Offensichtlich aus Berater-Ecke und damit Herstellerneutral. Viel Neues gibt es in diesem Beitrag aber nicht. Der Beitrag ist eher ein Tutorial vermutlich auch in Bezug auf NIST SP 800-207 und damit eine gute EinfÃ¼hrung fÃ¼r Nicht-Experten. Passt m.E. in das Programm. Es wÃ¤re gut, wenn der Beitrag nicht nur den Ort der Durchsetzung diskutiert, sondern auch die Art und Weise. Die Authentisierungsfaktoren sind nur ein wenig relevantes Beispiel. Es fehlt die Klarheit, welche Angriffe abgefangen werden.**
12			**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**		**Der Beitrag schildert zum einen die aktuelle Situation hinsichtlich Quantum Computing und den Standardisierungsaktivitäten zu PQC - der Fokus liegt allerdings auf Projekterfahrungen aus ersten Migrationsprojekten/Tests. Dies ist insbesondere fÃ¼r Anwender/Organisationen hilfreich, die sich auf eine solche Migration frÃ¼hzeitig vorbereiten wollen. Insbesondere aufgrund dieses Aspektes wird der Beitrag zur Aufnahme empfohlen.**
12			0	1	0	1	0	0	1	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	**2,3**	Im Beitrag werden einige sehr allgemeine Fragen u a. zur Entwicklung von Quantencomputern und der Migration zu Post-Quanten-Kryptografie aufgeworfen. Es bleibt aber trotz der LÃ¤nge des Textes (die Kurzfassung ist zu lang) leider vÃ¶l lig unklar welche AnsÃ¤tze oder Ergebnisse in der Langversion Ã¼berhaupt zu erwarten sind. Ich empfehle deshalb auch die Einreichung nicht zu verÃ¶ffentlichen.
12			**0**	**1**	**0**	**1**	**0**	**0**	**1**	**0**	**0**	**1**	**1**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**		**Der Titel legt nahe, dass im Beitrag die Ankunft von QC thematisiert wird, was nicht zutrifft. Es wurde mir nicht klar, welchen Standpunkt die Autoren vertreten wollen. Sie schreiben, dass aktuelle PQ Verfahren â€žnur eingeschÃ¤nkt praxistauglichâ€œ seien (begrÃ¼nden das aber nicht) und proponieren stattdessen â€žAlternativen, die man einigermaÃŸen gut als mÃ¶glichst direkten Ersatz nehmen kÃ¶nnte. Welche sind das denn? Worin sind sie besser, worin schlechter als z.B. die NIST-Finalisten? Wie viel Risiko geht man ein, wenn man sie nimmt? Was soll der Leser, der der Argumentation der Autoren folgen mÃ¶chte, genau tun? Ein sehr großer Teil der Einreichung wird mit der a lgemeinen BegrÃ¼ndung, warum man Ã¼berhaupt Kryptografie braucht, und mit Deta ls der Umsetzung bekannter Mechanismen; so wird die Message des Beitrags nicht deutlich.**
13			0	1	0	0	1	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	**2,7**	Das im Beitrag geschilderte â€žStore now decrypt laterâ€œ-Szenario ist ein sehr relevantes Thema. Hier wird letztlich die Schlussfolgerung gezogen dass nur der One Time Pad den Ã¤ngerfristigen Schutzbedarf vertraulicher Daten garantiert - insbesondere im Hinb ick auf die mÃ¶g iche Entwicklung eines Quantencomputers. Das entspricht nicht der EinschÃ¤tzung der internationalen Fachgemeinschaft gemÃ¤Ã¤ der symmetrische Algorithmen mit ausreichenden SchlÃ¼ssse lÃ¤ngen sowie Post-Quanten-Algorithmen nach aktuellem Kenntnisstand einen hinreichenden Schutz geben. Dagegen werden die Probleme die eine Umsetzung des One Time Pads in der Praxis mit sich bringt im Beitrag weitestgehend ignoriert. Hinweise auf neue Ideen fehlen vollstÃ¤ndig. Der Entwicklungsstand eines Quantencomputers wird auch tendenzie l Ã¼bertrieben und damit unsachlich dargestellt. Insgesamt finden sich im Beitrag zu viele Unstimmigkeiten und falsche Aussage und auch keine neuen Ideen als das eine Annahme gerechtfertigt wÃ¤re.
13			**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**1**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**			**Aufbauend auf der Google Sycamore Anekdote wurde ein spannender Beitrag geschrieben. SchÃ¶n zu lesen. Formal: Warum ist das Bild 1 nicht zu sehen? (ich habe zwei verschiedene Programme getestet) Was mir im Beitrag fehlt: Wann kÃ¶nnen Quanten Computer bei Normaltemperaturen betrieben werden (solange wie by Sycamore -273 Grad erforderlich sind, bleibt der Angriff sehr theoretisch) Es fehlt auch in diesem Beitrag die Innovation. Aber der Beitrag passt in das Programm.**
13			**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**1**	**0**	**0**			**Der vorliegende Beitrag rekapituliert im Wesentlichen bekanntes Wissen Ã¼ber PQ-Verfahren und weist auf den laufenden Standardisierungsprozess hin. Die ErklÃ¤rungen sind korrekt. Allerdings vermisse ich in der vorliegenden Kurzfassung den zentralen Beitrag des Papers, nÃ¤mlich die Empfehlungen des BSI in diesem Kontext. Ich gehe davon aus, dass diese relevant und ein hohes Interesse fÃ¼r die Kongress-Teilnehmer darstellen. Im Sinne einer Begutachtung ist das, was derzeit vorliegt, bisher sehr spÃ¤rlich, geht kaum Ã¼ber die Grundlagen hinaus und lÃ¤sst sich kaum einordnen. Es wÃ¤re aus meiner Sicht eine Zusammenlegung mit 0079 (Quantum Leitfaden) Ã¼berlegenswert.**
14			**1**	**0**	**0**	**0**	**0**	**1**	**1**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**		**Der Beitrag widmet sich dem hochaktuellen Thema SSI und hoheitliches IdentitÃ¤tsmanagement. Die Darlegung der Potentiale aus der Verbindung der bestehenden Technologien ist schlÃ¼ssig, ebenso die realistische EinschÃ¤tzung hinsichtlich Standardisierung und "Reifung" der SSI Technologien. Insbesondere vor dem Hintergrund der aktuellen eIDAS Revision der EU Kommission ist der Beitrag aktuell und gibt interessante DenkanstÃ¶Ãe und wird daher zur Aufnahme in das Programm empfohlen.**

14	[redacted]	1	0	0	0	1	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	2,7	Der Artikel befasst sich mit Self-Sovereign Identities (SSI) und der MÃ¶glichkeit einer Kombination von SSI mit eID-Dokumenten. Inhalt ich geht der Beitrag kaum Ã¼ber altbekannte SSI-AnsÃ¤tze hinaus. Das Zusammenspiel von SSI und eID bedeutet im wesentlichen dass der Nutzer das eID-Dokument zur Authentisierung gegenÃ¼ber dem SSI-System verwenden kann. Dieser Ansatz ist nicht neu. Angaben zur technischen Umsetzung z.B. zur Ableitung von Attributen aus einem eID-Dokument fehlen. Das Dokument weist eine recht groÃŸe Zahl fachlicher MÃ¤ngel und unsauberer Formulierungen auf ("Authentisierung" vs. "Authentifizierung" "AttributsbestÃ¤tigung durch digitale Signatur oder durch Blockchain" GegenÃ¼berstellung eID vs. Passwort). FÃ¼r die Umsetzung von SSI wird ohne BegrÃ¼ndung und ohne Notwendigkeit rein auf Blockchain gesetzt. Die wesentlichen Herausforderungen der IT-Sicherheit bei der Nutzung von SSI (Identifizierung der Nutzer Personenbindung AuthentizitÃ¤t der Daten) werden nicht angesprochen.
14	[redacted]	**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**1**	**0**	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0		**WÃ¼rde zwar thematisch passen, liefert aber wenig Neues oder Innovatives.**
15	[redacted]	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**1**	**0**	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	2,3	**Beitrag richtet sich primÃ¤r an eine Zielgruppe die typischer Weise nicht auf dem BSI Kongress vertreten sein wird.**
15	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0		Beitrag behandelt ein interessantes Thema: Die zwei verschiedenen Ebenen beim Vorfall Arbeitsebene und Entscheiderebene laufen teilweise parallel haben andere Fragestellungen setzen unterschiedliche Schwerpunkte und es gibt oftmals Kommunikationsdefizite. Beitrag will dazu sensibilisieren und Wege zu einer effizienteren Zusammenarbeit aufzeigen.
15	[redacted]	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0		**Nicht wirklich was neues**
16	[redacted]	**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**1**	**0**	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	3,7	**Neben den technischen Informationen zur Wiederherstellung der Vertrauensanker in einem DomÃ¤nen Controllen / Active Directory zeigt der Votrag auch die Notwenigkeit von NotfallmaÃŸnehmen und -Ãœbungen (=> Awareness in Unternehmen und Organisationen)**
16	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1		Der Beschre bung nach ein sehr technisch tiefgehender Vortrag zum Vorgehen eines Vorfallsteams nach einem Angriff. Neben der Beschreibung einer Triage nennt der Beitrag viele Faktoren auf die man bei einem Vorfa l trifft und an die man auch denken muss. Der Vortrag behandelt aber nur das Vorgehen (Analyse Wiederherste lung) am "System" und nicht die sonstigen IR-MaÃŸnahmen.
16	[redacted]	**1**	**0**	**0**	**1**	**0**	**0**	**1**	**0**	**0**	**1**	**1**	**0**	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0		**Der Beitrag beschreibt anekdotenhaft die BekÃ¤mpfung eines laufenden Angriffs im AD-Umfeld, also die ergriffenen MaÃŸnahmen um eine weitere Ausbreitung zu verhindern. Der Beitrag verspricht spezifische Praxistips zu geben. Eine Gliederung des geplanen Beitrags ist nicht enthalten und bleibt daher unklar. Etwas irritierend ist, dass der Titel von [redacted] ".**
17	[redacted]	1	0	0	1	0	0	1	0	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	2	Ich tue mich schwer diesen Beitrag zu bewerten. Hier wurde vermutlich ein technischer Beitrag (s. Gliederung) in einem Abstract juristisch aufgeladen. Die Gliederung und der Text passen daher te lweise nicht zueinander. Es wird te lweise zwischen technischen AusfÃ¼hrungen (wie kann man Google Analytics sicher einstellen) und rechtlichen AusfÃ¼hrungen zur allgemeinen datenschutzrecht ichen ZulÃ¤ssigkeit geschwankt. Das wirkt in sich nicht sauber. Daher wÃ¼rde ich den Beitrag auch nicht bei IT-Sicherheit und Recht sehen. Vie leicht passt er fÃ¼r ein anderes Themenfeld. Das mÃ¼sste dann aber jmd. anderes bewerten.
17	[redacted]	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**0**	**1**	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0		**Die Kernaussage des Beitrages bleibt absolut unklar. Welche Ro le Google Analytics im Beitrags insbesondere in Zusammehnag mit Angriffen spielt wird nicht klar. Zitat: [redacted] " Wenn ich als Angreifer volle Kontro le Ã¼ber die Web-Seite habe - wozu brauche ich dann noch Google Analytics?**
17	[redacted]	**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0		**Nicht besonders innovativ, aber vor dem Hintergrund der oft unbekannten Rechtslage wird ein allgemeines und verbreitetes Problem angesprochen.**
18	[redacted]	1	0	0	0	0	1	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	1,3	Der Beitrag befasst sich mit dem PhÃ¤nomen "Cybermobbing" sowie den Verantwortlichkeiten im Unternehmen um gegen dieses wirksam vorzugehen. Es besteht kein Bezug zum Thema Cyber-Sicherheit.
18	[redacted]	**1**	**0**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**1**	**1**	**0**	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0		**"Cybermobbing" am Arbeitsplatz hat wenig bis nichts mit der den BSI-Aufgaben zugrundeliegenden Definition von IT- und Cybersicherheit zu tun. DarÃ¼ber hinaus bietet der Beitrag keine interessanten Empfehlungen.**
18	[redacted]	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**0**	**1**	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0		**wie definiert sich [redacted] also woher wissen die Autoren was sich bewÃ¤hrt hat? Unklar was der Fokus ist. Neu weil Cybermobbing im Unternehmen? Am Rande: Es fehlen die Quellen**
19	[redacted]	1	0	0	0	1	0	1	0	0	1	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	3	Der Vortrag sollte aus folgenden GrÃ¼nden abgelehnt werden: 1. Das Thema Quanten-/Postquantenkryptographie betr fft alle Anwendungsbereiche von IT. KMU sind durch Quantencomputer weder stÃ¤rker bedroht als andere Bereiche noch unterscheiden sich die "GegenmaÃŸnahmen" bei KMU von denen anderer Bereiche. Das sehen auch die Autoren des Abstracts so: [redacted] Das Abstract geht auf diesen Umstand in ke ner Weise ein. 2. Auf das Thema Quantenkryptographie wird im Vortrag nur sehr knapp eingegangen. 3. Das Buzzword Quantenkryptographie wird lediglich als AufhÃ¤nger verwendet um einen Standardvortrag Ã¼ber die IT-Sicherheit von KMU im Vortragsprogramm unterzubringen. 4. Der Vortrag bietet in der Kombination der Themen fÃ¼r KMU keinen Mehrwert.
19	[redacted]	**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0		**Nicht aufnahmewÃ¼rdig, da die von Quantencomputern ausgehende Gefahr nicht KMU-spezifisch ist und auf dem Kongress kein irrefÃ¼hrendes Narrativ bemÃ¼ht werden sollte. Anstatt sich mit der abstrakten Gefahr durch Quantencomputern zu beschÃ¤ftigen, sollten sich KMU vor allem auf grundlegende SicherheitsmaÃŸnahmen konzentrieren (HÃ¤rtung von Systemen, ISMS, etc.).**
19	[redacted]	**1**	**0**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0		**Das Thema ist zwar sehr interessant, kann aber in dem zeitlichen Rahmen des BSI IT-Sicherheitskongress nicht ausfÃ¼hrlich genug erÃ¶rtert werden**
20	[redacted]	1	0	0	1	0	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	3,3	Bei der Bewertung des Abstracts fallen zwei Sachverhalte schnell ins Auge. Der Autor des Papiers verwendet legacy Produkte des BSI welche bereits in 2017 abgekÃ¼ndigt wurden. Falls der Vortrag berÃ¼cksichtigt wird muss noch eine QS erfolgen. Zweitens lassen sich manche Schlussfolgerungen der Studie nicht gut nachvollziehen wirken im Abstract nicht Ã¼bergreifend genug. Es mag sein dass sich dieser Eindruck bei der Studie des Forschungsberichts nicht bestÃ¤tigt.
20	[redacted]	**1**	**0**	**0**	**1**	**0**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0		**Durchaus interessante Resultate, die vorstellungswÃ¼rdig sind. E-Ma l-Sicherheit und die kommunale Ebene sind zwei Schwerpunktbereiche, die medial und fachlich verstÃ¤rkt im Fokus liegen. NatÃ¼rlich ist der Abstract nicht ausfÃ¼hrlich genug, um eine verlÃ¤ssliche EinschÃ¤tzung zur QualitÃ¤t der empirischen Analyse abgeben zu kÃ¶nnen.**
20	[redacted]	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**1**	**0**	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0		**Die empirische Studie des Beitrags bringt einige Aspekte, die allerdings bei einer Annahme deutlich besser mit der Schlussfolgerung verkoppelt werden sollten. So wie es aus dem Abstract erscheint ist die Schlussfolgerung vorab vermutet und die Studie wird herangezogen um die Schlussfolgerung zu untermauern. Daher ist die Robustheit der Schlussfolgerung nicht offensichtlich.**
21	[redacted]	**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**1**	**0**	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	3	**Der Abstract hebt die Relevanz von IdentitÃ¤ts- und Berechtigungsmanagement (IAM) in KMU hervor und fokussiert auf einen open source-basierten Ansatz. Vor dem Hintergrund des sich stÃ¤ndig weiterentwickelnden Bedrohungsszenariums durch die MÃ¶glichkeit der Ãœbernahme von IdentitÃ¤ten im Unternehmenskontext sieht der Abstrakt IAM als zentrale LÃ¶sung, um Berechtigungen fÃ¼r den Zugriff auf Dateien etc. durch IdentitÃ¤ten regelbasiert zu managen. Das Thema ist insbesondere fÃ¼r KMU von hoher Relevanz. Der Beitrag wirkt jedoch eher deskriptiv. Wenn mit dem BSI-Kongress 2022 explizit KMU adressiert werden sollen und zudem konkrete LÃ¶sungen zur StÃ¤rkung der Cyberresilienz in KMU vorgestellt werden sollen, wÃ¤re die Aufnahme des Themas zu empfehlen.**
21	[redacted]	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0		**welche alternativen LÃ¶sungen gibt es? Was sind die Limitations dieser? Was ist das Ziel des Beitrags? Was bedeutet "deutlich gesteigerten Sicherheit"?**
21	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0		IdentitÃ¤ts- und Berechtigungsmanagement ist ein wichtiges Thema das leider von vielen BehÃ¶rden und Unternehmen (nicht nur KMU) vernachlÃ¤ssigt wird - auch wenn es keine Innovation mehr darstellt. Im Vortrag wird der Fokus auf Open-Source-LÃ¶sungen gelegt eine einseitige Produktbewerbung ist somit nicht zu befÃ¼rchten. Der Beitrag so lte daher angenommen werden.
22	[redacted]	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**1**	**1**	**0**	**1**	**0**	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	2,7	**Sicher fachlich sehr gute Darstellung, geringe direkte praktische Anwendung, eher Forschungscharakter**
22	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0		Der Beitrag klingt interessant ich kenne solche Spiele aus anderen Bereichen z.B. UnternehmensfÃ¼hrung IT-Service Management oder auch CTFs usw. Spiele kÃ¶nnen trotz oder wegen einer verminderten KomplexitÃ¤t kausale ZusammenhÃ¤nge bewusst machen und auf Probleme hinweisen bzw. Sensibi isieren. Es gibt einen Bezug zu MITRE ATT&CK fÃ¼r Cloud das ist gut. Der Umfang des Spiels kann im Abstract nicht vollends abgeschÃ¤tzt werden. Der Beitrag kann angenommen werden.
22	[redacted]	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**0**	**1**	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0		**FÃ¼r mich ist die initiale Motivation, warum man Games einsetzen sollte nicht erkennbar. Was soll denn erreicht werden? Auch verstehe ich das Flowchart in Figure 1 und die umgebende Beschreibung nicht.**
23	[redacted]	**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	2,7	**Beitrag bring neue DenkansÃ¤tze als Alternative zu einem reinen Microsoft Produktstack, ggf interessant fÃ¼r Digitalisierung in Verwaltung und Wirtschaft**
23	[redacted]	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**0**	**0**	**1**	**1**	**0**	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0		**Beitrag zeigt ein aktuelles Thema an, jedoch werden die InnovativitÃ¤t und der Mehrwert des Ansatzes, auch als Beitrag im Kongress, nicht deutlich. Es bedarf Strukturierung und weiterer AusfÃ¼hrungen.**
23	[redacted]	0	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0		Der vorliegende 1 1/2-Seiten Abstrakt erlÃ¤utert einen Ansatz Exchange Hybrid zu betreiben und nimmt Bezug auf die HAFNIUM-Exploits von Anfang 2021 die on-premise Exchange-Server betrafen. Aus dem Abstrakt wird leider nicht klar wie die vorgeschlagene Architektur durch Begrenzung auf einzelne Exchange-Webservices in Kombination mit anderen (vorgeschalteten) Diensten realisiert wird. Auch wird der direkte Zusammenhang zu "Teams" im Abstrakt nicht verstÃ¤ndlich erlÃ¤utert. Insgesamt fÃ¤llt es auf Grundlage des vorliegenden knappen Abstrakt schwer eine fundierte Bewertung vorzunehmen da er diverse technische RÃ¼ckfragen zur angedachten Umsetzung insbesondere zum Sicherheitsmehrwert aufwirft.
25	[redacted]	**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**1**	**0**	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	3,3	**Das Thema ist sicherlich relevant, die Darstellung ist aber "it-security as usual", eigentlich geht es nur um die Vorstellung einer BSI-Handreichung, wichtig, aber eben "nur" das ...**
25	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0		Der Beitrag weiÃŸt auf einen wichtigen Aspekt zum Management von Informationssicherheit hin der in der Praxis viel zu selten beachtet wird. AuÃŸerdem werden direkt Hilfeste lung gegeben wie dieser Aspekt umgesetzt werden kann. Das Thema sollte auf jeden Fall auf dem BSI Kongress adressiert werden da es fÃ¼r viele Institution Firmen und BehÃ¶rden eine wichtige Rolle spielt. Der Beitrag ist gut formuliert und verstÃ¤ndlich. Eine eher editorielle Anmerkung: Vielleicht kÃ¶nnten die Autoren das Schaubild noch nÃ¤her erklÃ¤ren insbesondere die Bedeutung der Buchstaben in der Grafik werden im Text nicht aufgegriffen und weshalb im Reaktiv-BCMS 1x in der Mitte eingetragen ist.
25	[redacted]	**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0		**Beitrag verdeutlich die Problemstellung und zeigt anhaltende Risiken auf. Jedoch wird die Zielsetzung des Beitrags zu Beginn nicht deutlich. Die InnovativitÃ¤t lÃ¤sst sich schwer beurteilen.**
26	[redacted]	**0**	**1**	**0**	**0**	**0**	**1**	**1**	**0**	**1**	**0**	**1**	**0**	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	5	**Auch wenn der Beitrag nicht vollstÃ¤ndig anonymisiert ist stellt er doch einen ganz erheblichen Beitrag fÃ¼r die offene Frage der Sicherheitszertifizierung der 5G Netze da und sollte daher unbeding angenommen werden.**
26	[redacted]	**1**	**0**	**0**	**0**	**0**	**1**	**1**	**0**	**1**	**0**	**1**	**0**	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1		**Thematisiert sehr gut die SchwÃ¤chen von Zertifizierungsprozessen und bietet auch LÃ¶sungsansÃ¤tze**
27	[redacted]	**1**	**0**	**0**	**0**	**0**	**1**	**1**	**0**	**1**	**0**	**1**	**0**	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	4	**Vor dem Hintergrund der aktuell diskutierten Aufnahme von an Hersteller gestellte Anforderungen an die Cybersicherheit, Datenschutz und BetrugsprÃ¤vention in die europÃ¤ische Radio Equipment Richtlinie soll der Beitrag die neuen Verpflichtungen der Hersteller einordnen und konkrete Handlungsempfehlungen formulieren. Da bereits 2023 laut CISCO jede(r) Deutsche knapp 10 vernetzbare GerÃ¤te besitzen wird, gewinnt die Wahrung der Cyberresilienz sowie der Schutz personenbezogener Daten bei vernetzbaren GerÃ¤ten an Bedeutung. Die Darstellung dieser Anforderungen sowie das Aufzeigen von Empfehlungen zur rechtskonformen Umsetzung sind vor dem Hintergrund des Awareness-Raisings von zentraler Bedeutung fÃ¼r produzierende Unternehmen. Der Beitrag ist sehr logisch strukturiert und bietet â€“ nicht zuletzt aufgrund seiner AktualitÃ¤t â€“ einen signifikanten Mehrwert. Eine Aufnahme in das Tagungsprogramm erscheint zielfÃ¼hrend â€“ auch um eine europÃ¤isch-regulatorische Komponente darin zu integrieren.**
27	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0		1) Gliederung im Kopfbereich ist nicht im Text ersichtlich 2) Bspw. Quelle / FuÃŸnote 4 und 5 identisch. Evtl. kann dieser Beitrag vor VerÃ¶ffentlichung lektoriert werden.
27	[redacted]	**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**1**	**0**	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0		**Sinnvoller Beitrag zur Diskussion der Radio Equipment Directive. GrÃ¼ndlich und seriÃ¶s aufbereitet.**
28	[redacted]	1	0	0	1	0	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	2	Votum: Der Vortrag sollte nur ZWEITRANIGIG berÃ¼cksichtigt werden also nur dann wenn ein Slot letztendlich nicht besetzt werden kÃ¶nnte. EntscheidungsgrÃ¼nde: a) Das Hauptthema erscheint mit dem AufhÃ¤nger [redacted] " "an den Haaren herbeigezogen" zu sein und kaschiert einen Vortrag mit einem "Rundumschlag" mit Kritik an der Gesetzgebung de [redacted] und am Krankenhausmanagement. Dass "die Chefin es richten muss" ist keine Forderung die sich aus dem BSI-Lagebericht 2020 ableiten lÃ¤sst. b) Dass IT-Sicherheit in der Verantwortung des Top-Level-Managements liegt ist eine Binsenweisheit - die im Ãœbrigen nicht nur speziell auf KrankenhÃ¤user zutrifft. c) Vor dem allgemeinen Pub ikum des BSI-Kongresses hat der Vortrag eher die Funktion eines Sachstandberichts und weniger der Sensibi isierung von Krankenhaus-Fachpersonal. Bis auf die verkÃ¼rzten Verweise auf SGB V und den B3S beinhaltet er jedoch zu wenig sektorspez fische Informationen als dass er insbes. den sektorfremden Kongressteilnehemern einen Mehrwert wird bieten kÃ¶nnen.
28	[redacted]	**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0		**Die Herangehensweise ist behauptend und beschreibend. Die faktisch nachvollziehbare BegrÃ¼ndung hinkt dem nach und daher wirkt der Beitrag eher als eine politisch motivierte Aufforderung. Sollte der Beitrag angenommen werden, sind die Aussagen deutlicher durch Fakten und nachvollziehbare Schlussfolgerungen zu untermauern.**
28	[redacted]	**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**1**	**0**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0		**Der Vortrag so lte abgelehnt werden, da er keine neuen DenkanstÃ¶ÃŸe aufzeigt**

29	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	4,3	Die Autoren stellen ein Tool vor das mithilfe von Methoden aus dem Bereich des maschinellen Lernens die AnfÃ¤lligkeit einer TLS-Implementierung fÃ¼r eine spezielle Art von Seitenkanalangriffen (sog. Padding Orakel-Angriffe) feststellen kann. Die Zusammenfassung geht nicht nÃ¤her auf die Deta ls des verwendeten ML-Verfahrens ein dies soll ebenso wie eine mÃ¶gliche Erweiterung auf andere Seitenkanalangriffe im Vortrag nÃ¤her erlÃ¤utert werden. Das Tool das in einer Live-Demo anhand des Bleichenbacher-Angriffs vorgefÃ¼hrt werden soll ist wÃ¤hrend eines Projekts entstanden und prototypisch in eine Testsuite einer der Projektpartner integriert der diese als Produkt vertreibt. Die gesamte Implementierung soll auch kostenlos und quelloffen zur VerfÃ¼gung gestellt werden (eine kurze Recherche ergab dass dies aktue l nicht der Fa l ist). Das grundsÃ¤tzliche Verfahren kÃ¶nnte sich als interessant erweisen insbesondere wenn es sich auf andere Arten von Seitenkanalangriffen und/oder andere Implementierungen/Algorithmen verallgemeinern lÃ¤sst. Dies ist aus dem Abstract jedoch nicht ersichtlich.
29	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1		**Der Beitrag ist auf technische Sicherheit und Angriffe auf VerschlÃ¼sselung orientiert und passt daher gut in das Portfo io des BSI. Die AbstÃ¼tzung durch Hintergrundliteratur und damit die Sicherstellung der OriginalitÃ¤t so lte in der finalen Version unbedingt verbessert werden.**
29	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0		**Die Einreichung beschre bt die praktischen Aspekte der Umstellung der VPN-LÃ¶sungen auf KryptoagilitÃ¤t im Allgemeinen und PQ-Verfahren im Besonderen. Der Neuigkeitsgehalt ist nicht besonders hoch, die Geschichte wird jedoch durchaus interessant erzÃ¤hlt, sie ist aus meiner Sicht korrekt beschrieben und bleibt auf einer angemessenen Abstraktionsebene. Der Beitrag ist meiner Meinung nach fÃ¼r Entscheider und fÃ¼r interessierte Ã–ffent ichkeit durchaus interessant, und ich wÃ¼rde nach der Form der Kurzfassung eine gelungene Ausarbeitung erwarten. Schreibfehler: Laboroсаtorien.**
30	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	4,3	**Beitrag beschÃ¤ftigt sich mit der kontinuierlichen VerÃ¤nderung von IT durch Updates und der Wechselwirkungen mit Zertifizierungen bzw. der Frage wie diese vermieden werden kÃ¶nnen. Sehr zukunftsorientierter Ansatz zur Weiterentwicklung der klassischen ZertifizierungsansÃ¤tze.**
30	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0		**Grenzen der Zertifizierung werden aufgezeigt und LÃ¶sungsvarianten aufgezeigt. Zeigt auf, wie die Zertifizierungslandschaft unter BerÃ¼cksichtigung des Patchmanagements in Zukunft aussehen sollte**
30	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0		Das eingereichte Abstract mit dem Tite [redacted] adressiert ein Thema das aktuell wieder vermehrt diskutiert wird und insgesamt fÃ¼r den Bereich der Produktzertifizierung hÃ¶chst relevant ist. Der Beitrag ist gut gegliedert fÃ¼hrt in die Thematik ein und diskutiert aktuelle LÃ¶sungsansÃ¤tze. Aus Wissenschaftlicher Sicht wÃ¤re es schÃ¶n gewesen den Beitrag noch mit Referenzen zu unterfÃ¼ttern. Da es sich jedoch um einen Beitrag mit hoher Praxisrelevanz handelt ist dieser Punkt zu vernachlÃ¤ssigen. Votum: Beitrag kann gut angenommen werden.
31	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	3,7	Der Wert des Papers besteht vor allem darin aufzuzeigen dass BCM ein aktuelles Thema ist das seinen Beitrag nicht nur bei den "klassischen" VerfÃ¼gbarkeitsthemen (Stromausfall Feuer Einbruch etc.) leistet sondern auch bei aktuellen IT-gestÃ¼tzten Angriffen. Dies ist zwar nicht besonders innovativ aber fÃ¼r die Anwender dennoch relevant und wichtig. Trotz der leichten SchwÃ¤chen bei Rechtschreibung/Grammatik ist das Paper sehr gut strukturiert und sehr gut verstÃ¤ndlich in der Darstellung. Dadurch dass die Schnittstelle zwischen BCM und IR betrachtet wird ist die OriginalitÃ¤t/Innovation zwar gegeben sie ist aber sicherlich nicht besonders hoch. Dies ste lt das grÃ¶ÃŸte Defizit des Papers dar. Insgesamt gehÃ¶rt das Paper somit zwar nicht zu den besten 10% sollte aber durchaus in Betracht gezogen werden wenn andere Papers im Themenbereich "Incident Response" nicht angenommen werden kÃ¶nnen.
31	[redacted]	1	0	0	0	0	1	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0		**Ersteindruck war, dass der Beitrag konkrete Hilfestellung bei Ransomwareangriffen geben sollte, im Script lieÃŸt es sich dann aber doch eher wie ein klassischer Notfa lplan der mit dem Bergriff "Ransom Ware Angriff" modern angestrichen wird.**
31	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0		**Das Thema ist sicherlich relevant und wichtig. Es kÃ¶nnte im schriftlichen Beitrag zu kurz ausfallen, weil doch weit ausgeholt wird und gleichzeitig eine Fallstudie gezeigt werden soll ... es ist auch wichtig zu verstehen, dass hier eine besondere Vorfallsart herausgegriffen wird, ohne jedoch - zumindest im Abstrakt - alle relevanten Szenarienvarianten zu erfassen ....**
32	[redacted]	1	0	0	0	0	1	1	0	0	1	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1,7	**Keine Neuigkeiten oder Besonderheiten, reine Darstellung eines Lice-Hacks mit Standard-Vorgehen und dann noch unrealstischem Vorgehen (zu frÃ¼he Se bst-Bekanntmachung) des Hackers. Sollte allen, die sich fÃ¼r Cybersicherheit interessieren, bekannt sein.**
32	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0		Gehe davon aus dass dies ein Beitrag des BSI ist [redacted] . Jedoch ist der Vortrag zu trivial. -> Erste 10 Minuten -> Beschreibung wie Phishing funktioniert (mit e nem Live-Deepfake Exkurs) -> dann wird der Rechner "gehacked" -> Ersthelfer kommt findet raus was passiert da nur lokaler Angriff kein Schaden. Zu einfach aber ggf. will man damit die Digitalen Ersthelfer auf dem BSI Kongress vorstellen dann wÃ¤re der Beitrag vertretbar.
32	[redacted]	1	0	1	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0		**Der Abstract skizziert das Drehbuch fÃ¼r einen Live-Hack. Da keine Gliederung angegeben wird bleibt vÃ¶llig unklar wie der Beitrag aussehen soll.**
33	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	2,7	Der Abstract hat HÃ¶hen und Tiefen. Die vorangestellte Gliederung und deren Themen wÃ¤re sehr gut. Der Abstract folgt dieser Struktur jedoch bisher nicht. Statt der Darstellung der Haftung von Unternehmen Vorstand und Aufsichtsrat wird vorwiegend Ã¼ber das ISMS geschrieben. Das spiegelt den Vortragstitel nicht wirk ich wider. Wenn der endgÃ¼ltige Beitrag wirklich die G iederung sauber abb ldet kann er gut werden. im Hinblick auf die Bewertung von Cyberversicherungen kÃ¶nnte dieser Beitrag im Wechselspiel zum Beitrag [redacted] sein der zu einer anderen EinschÃ¤tzung kommt. Wenn beide BeitrÃ¤ge auf einem Panel laufen kÃ¶nnte das Diskussionen anregen.
33	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0		**Ausgehend vom kontinuierlichen Anstieg an CybersicherheitsvorfÃ¤llen und den damit verbundenen Schadensvolumina fÃ¼r Unternehmen zielt der Beitrag darauf ab, die Haftung durch VorstÃ¤nde und AufsichtsrÃ¤te fÃ¼r diese SchÃ¤den zu beleuchten. Zudem intendiert der Beitrag darzulegen, dass ein wirksames ISMS einen essenziellen Beitrag zur StÃ¤rkung der Cyberresi ienz von Unternehmen leisten kann. Der Abstract ist nachvo lziehbar strukturiert und adressiert ein relevantes Thema (Cybersicherheit = Chefinnen-(Chefsache). Vor dem Hintergrund der aktuell auf europÃ¤ischer Ebene laufenden Beratungen fÃ¼r eine NIS 2-Richtlinie und der damit verbundenen (etwaigen) EinfÃ¼hrung von zusÃ¤tzlichen regulatorischen Anforderungen an die Leitungsorgane eines Unternehmens, empfiehlt sich die Aufnahme dieses Themas eher ins BSI-Programm 2023 oder 2024, sodass der aktuellste Gesetzstand rechtssicher berÃ¼cksichtigt werden kann.**
33	[redacted]	1	0	0	1	0	0	1	0	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0		**Der Beitrag spricht zwar ein sehr wichtiges Thema an es wird dieses Thema im vorliegenden Abstract allerdings relativ oberflÃ¤chlich behandelt und geht kaum Ã¼ber allgemein Bekanntes hinaus. Daher ist der Beitrag in der vorliegenden Form eigentlich nicht annehmbar.**
34	[redacted]	1	0	0	0	1	0	1	0	1	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	3,7	**Der Beitrag schildert einen Ansatz zur grundlegenden Bewertung von IT Security Massnahmen im KMU Umfeld nach einer geeigneten Bewertungsmethode. Der Ansatz ist grundsÃ¤tzlich interessant, ein Nachweis einer echten Wirksamkeit kann nicht Ã¼berzeugend dargelegt werden, auch da die Anzahl der Interviewpartner (5) sehr niedrig ist. Trotzdem zeigt der Beitrag einen mÃ¶glichen neuen Ansatz zur objektiveren Bewertung der Wirksamkeit von IT Security MaÃŸnahmen in Organisationen auf und wird daher zur Aufnahme in das Programm empfohlen.**
34	[redacted]	1	0	0	0	1	0	1	0	1	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0		**Wichtiges Thema, wissenschaftlicher Beitrag, interessante Herangehensweise, aber kleines n bei den Interviews. Die Vorstellung des Ansatzes wÃ¤re durchaus vorstellungswÃ¼rdig. Vielleicht kann ein neuer Impuls in die Breite gegeben werden, um den Ansatz verstÃ¤rkt in den Blick zu nehmen. Die Ergebnisse sind allerdings mit Vorsicht zu genieÃŸen.**
34	[redacted]	1	0	0	0	1	0	1	0	1	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0		Das Thema wird sehr strukturiert angegangen. Allerdings lÃ¤sst sich die Eignung der entwickelten Taxonomie durch Auswertung von lediglich fÃ¼nf Interviews nicht wirklich belegen. Und "Der GroÃŸte l der Teilnehmer hielt es auch fÃ¼r sinnvo l die Taxonomie fÃ¼r die Auswahl von Rahmenwerken bei der Entwicklung der Strategie einzusetzen." kÃ¶nnte auch bedeuten dass es sich hier um drei von fÃ¼nf Teilnehmern handelte. Dennoch eine interessante Ausarbeitung die im Vergleich zu anderen Einreichungen zumindest wissenschaftlich anmutet (mehr lÃ¤sst sich - verstÃ¤nd icherweise - aus dem Abstract nicht erkennen).
35	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	4,3	Das Thema Deepfake ist vor dem Hintergrund dass in verschiedenen Bereichen von Ã¶ffent icher Verwaltung und Privatwirtschaft immer noch VideoIdent-Verfahren zur Nutzerregistrierung zugelassen oder zumindest diskutiert werden hochaktuell.
35	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0		**In der Langfassung wird dieser Beitrag sicherlich eine gute Ãœbersicht Ã¼ber und EinfÃ¼hrung in die Problematik, sowie die technisch-organisatorisch-rechtlichen LÃ¶sungsansÃ¤tze anbieten. Das Thema ist aktuell.**
35	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0		**Beitrag zeigt aktuelle Entwicklungen auf die auch in die Zukunft gerichtet sind.**
36	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	4	**Der Beitrag schildert den konkreten Umbau eines gÃ¤ngigen Mailclients zur Aufnahme von PQC Algorithmen/Mechanismen. Er leistet damit einen wesentlichen Beitrag zur EinschÃ¤tzung der PraktikabilitÃ¤t von derzeit betrachteten PQC Mechanismen fÃ¼r das Thema MailverschlÃ¼sselung. Aufgrund er groÃŸen Praxisrelevanz wird der Beitrag uneingeschrÃ¤nkt zur Aufnahme in das Konferenzprogramm empfohlen.**
36	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1		Der vorliegende Beitrag beschre bt ein Implementierungsprojekt zur Integration von Post-Quanten Kryptografie in den Email-Client Thunderbird. Dabei wird auf Kernkonzepte wie hybride Signaturen und VerschlÃ¼sselung Kryptoagi itÃ¤t AbwÃ¤rtskompat bilitÃ¤t und Herausforderungen bei der Migration eingegangen. Die gewonnenen praktischen Erkenntnisse und die Beschreibung der Umsetzung stellen einen wertvollen Beitrag dar. Ich empfehle daher die Annahme des Beitrags. In der Langversion kÃ¶nnten folgende Aspekte ergÃ¤nzt werden: Unterschiede zwischen PKE und KEM und Auswirkungen Details zu Datenformaten Aspekte zur Anwendersicht.
36	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0		**Hier wird Postquantum-sichere Kryptographie in den EMail-Client Thunderbird eingebaut. Die Verfahrensauswahl wird diskutiert. Das Thema Migration zu PQ-Verfahren wird grundsÃ¤tzlich thematisiert. Der entsprechende Leitfaden des BSI wird genannt, ob dieser befolgt wurde oder ob es Kritik an diesem gibt, bleibt leider offen. Da die PQ-Standardisierung noch lÃ¤uft wird hier weit vorgegriffen - keiner weiss heute welche PQ-Verfahren am Ende standardisiert werden. Es ist nicht ganz klar, was Ziel und Ergebnis der Arbeit/Ãœbung sind. Es wird gezeigt dass es geht, aber das ist wenig Ã¼berraschend.**
37	[redacted]	1	0	1	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	2	**Ein an sich spannendes Thema, aber es wirkt mehr, als wolle man hier ein Produkt oder eine Dienstleistung fÃ¼r [redacted] (?) platzieren, als einen Beitrag zu Cyber- und IT-Sicherheit leisten. NatÃ¼rlich wird hier an Stellen auf die Relevanz von Informationssicherheit fÃ¼r das Thema hingewiesen, es wirkt aber eher wie ein nachgeordnete Gedanke.**
37	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0		**Der Beitrag Ã¼berzeugt insbesondere durch seine Problemstellung und Analyseebenen.**
38	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	2,3	**Am Ende geht es in dem Vortrag um Prozessautomatisierung, die ausnahmelos positiv fÃ¼r die Cyber-Sicherheit dargestellt wird. Die Herleitung ist langatmig und greift nur a legemein Bekanntes (GrÃ¼nde fÃ¼r den Aufbau eines ISMS â€¦) auf.**
38	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0		Gliederung sehr gut und praxisbezogen auf die Herausforderungen einer Kommune im Hinblick auf die zunehmende Digitalisierung. FÃ¼r [redacted] ein sehr relevantes Thema. Die Herleitung der Problematik erscheint folgerichtig.
38	[redacted]	0	1	0	1	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0		**Der Vortrag so lte abgelehnt werden, da der Bezug zur IT-Sicherheit nicht aufgezeigt wurde**
39	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	3,7	**VerstÃ¤ndlich, aber sehr aufwÃ¤ndig zu lesen. Ich sehe aktuell nur eine geringe direkte praktische Anwendung, eher Forschungscharakter mit Zielgruppe Security Research**
39	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0		Das Thema ist ein Dauerbrenner. Es soll die Ergebnisse einer Dissertation prÃ¤sentiert werden. Daher ist von einem fachlich fundierten Vortrag auszugehen. Der Abstract bleibt jedoch sehr oberflÃ¤chlich und die Bilder sind (bewusst) in schlechter QualitÃ¤t erstellt. Daher keine TOP Bewertung aber eine Empfehlung zur Annahme.
39	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0		**Forschungsbeitrag mit unklarer Relevanz fÃ¼r praktische Umsetzung. WÃ¼rde fachlich qualitÃ¤tsvolle PrÃ¤sentation erwarten. Empfehlung zur Aufnahme ist 3-4.**
40	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	3,7	**Der Beitrag schildert das Vorgehensmodell zur sicheren Ãœbertragung von Lichtbilddaten fÃ¼r hoheitliche Dokumente gemÃ¤ÃŸ BSI TR-03170. Aufgrund der aktuell vorliegenden Morphing Attacken ist die sichere Ãœbertragung der Lichtbilddaten ein wesentlicher prozeduraler Sicherheitsanker bei der Beantragung von hoheitlichen Dokumenten. Der Beitrag wird daher fÃ¼r die Aufnahme in das Programm empfohlen.**
40	[redacted]	1	0	0	0	0	1	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0		Das Paper [redacted] gibt einen Ãœberblick Ã¼ber die BSI-seitigen Vorbereitungen im Kontext Morphing-Verhinderung bei der Beantragung von deutschen Ausweisdokumenten. Auf Basis des Gesetzes zur â€žStÃ¤rkung der Sicherheit im Pass-Ausweis- und auslÃ¤nderrecht ichen Dokumentenwesenâ€œ soll es ab Mai 2025 Dienstleistern mÃ¶glich sein elektronisch Lichtbilder Ã¼ber eine CloudlÃ¶sung in die Pass- und AusweisbehÃ¶rden zu transportieren. Das Paper gibt einen guten Ãœberblick Ã¼ber die rechtlichen HintergrÃ¼nde dieses Vorhabens und stellt im weiteren Verlauf den Aufbau der zugehÃ¶rigen TR-03170 dar wobei die Autoren explizit auf die zukÃ¼nftigen Prozesse eingehen und die informationstechnischen Sicherheitsanforderungen beleuchten. Die Darstellung ist vo lstÃ¤ndig und bietet einen guten Ãœberblick zum Thema welches selbst aktuell und wichtig ist. Das Paper sollte daher fÃ¼r den BSI-Kongress 2022 aufgenommen werden.
40	[redacted]	0	1	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0		**Keine Innovation und nur allgemeine AusfÃ¼hrungen mit Bezug auf bestehende TRs.**
41	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	4	**Ausgehend von der These, dass die Aufrechterhaltung einer stÃ¶rungsfreien Versorgungssicherheit in der Energiewirtschaft maÃŸgeblich von einer stÃ¶rungsfreien und resilienten IKT abhÃ¤ngig ist und zugleich Verteilnetzbetreiber (VNB) vielfach nicht ausreichende persone le Ressourcen zur Umsetzung der Anforderungen aus dem IT-SiG 2.0 haben, wird die Etablierung einer OT CERT-Einheit als Shared Services Center fÃ¼r mehrere VNB vorgeschlagen. Dieser Ansatz basiert auf einer Forschungskooperation in NRW, im Rahmen derer bereits ein Prototyp entwickelt wurde, der ab Oktober 2021 im Feld getestet wird. Die Arbeit ist sehr wissenschaftlich verfasst und richtet sich primÃ¤r an eine sehr begrenzte, jedoch sehr relevante Zielgruppe (VNB). Es wÃ¤re seitens des [redacted] zu prÃ¼fen, inwiefern VNB in der Vergangenheit am Kongress teilgenommen haben.**
41	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0		Vorstellung eines Forschungsvorhabens fÃ¼r die Systematisierung des Managements von IT-Sicherheitsanforderungen im KRITIS-Umfeld. Sinnvo ler Programmbeitrag um mehr Aufmerksamkeit fÃ¼r den Ansatz bei KRITIS-Betreibern zu erzeugen.
41	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1		Durch die Neuerung des IT-SiG kommen auf Betre ber Kritischer Infrastrukturen sowie Verteilnetzbetreiber der Branchen Gas und Strom neue Herausforderungen bei der Absicherung ihrer IT und OT gegenÃ¼ber Cyberangriffen zu. Teil der Neuerungen ist eine verbindliche Forderung im BSIG sogenannte Angriffserkennungssysteme in eigenen Systemen einzusetzen. Gegenstand des Papers ist die fachliche Konzeption und die spÃ¤tere Operationalisierung eines OT CERT als Shared Service Center (SSC) fÃ¼r Verteilnetzbetreiber (VNB). Ein Prototyp eines solchen SSC wird bereits versuchsweise bei VNBs eingesetzt. Da gerade unter den VNBs eine Vielzahl kleiner und mittelstÃ¤ndischer Unternehmen ist kann mit dem Ansatz eines SSCs ein realer Mehrwert fÃ¼r die Branchen Strom und Gas bei der ErhÃ¶hung ihrer IT-Sicherheit erreicht werden.

42	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	2,3	Der Beitrag befasst sich mit dem Thema Digitale SouverÃ¤nitÃ¤t und dessen Auswirkungen auf die IT-Sicherheit auf EU-Ebene. Dazu wird zunÃ¤chst methodisch der Begriff Digitale SouverÃ¤nitÃ¤t und seine Dimensionen definiert. Im Ausb ick auf die Langversion sollen die gefundenen SchlagwÃ¶rter dann in Bezug auf ihre Auswirkungen auf die IT-Sicherheit diskutiert werden. Meiner Meinung nach ein wichtiges und aktuelles Thema allerdings liefert die eingereichte Kurzform keinen Ausblick auf die Diskussion und eventuelle Ergebnisse. Es fehlt eine prÃ¤gnante Zusammenfassung von daher fÃ¤llt meine Bewertung "Neutral" aus.
42	[redacted]	**1**	**0**	**0**	**1**	**0**	**0**	**1**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**		**Leider wurden lediglich die ersten Seiten der Gesamteinreichung als Abstract deklariert. AusfÃ¼hrungen zu den Definitionen sind wenig aussagekrÃ¤ftig, Ergebnisse fehlen dagegen. GrundsÃ¤tzlich aber ein interessantes und politisch relevantes Thema. Zuordnung zu einem Oberthema fÃ¼r den Kongress allerdings schwierig. Vorstellung dieses komplexen Themas in wenigen Minuten eher schwierig. Gesamturteil daher nur neutral.**
42	[redacted]	**1**	**0**	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**		**Es handelt sich hierbei lediglich um die ersten Seiten aus einer lÃ¤ngeren Studie. Es ist nicht ersichtlich, was im Endeffekt gemacht wurde und welche Ergebnisse und Empfehlungen sich daraus ergeben.**
43	[redacted]	**1**	**0**	**0**	**0**	**0**	**1**	**1**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**3,7**	**Der Beitrag stellt vor dem Hintergrund des zunehmenden Grads an Cyberbedrohungen und den Ã¼berschaubaren personellen und finanziellen Ressourcen von KMU das Konzept des Smart Matchings, welches Grundlage des sec-o-mats von TISiM ist, vor. Beim Smart Matching handelt es sich um ein Expertensystem, das die individuellen Bedarfe eines Unternehmens an IT-Sicherheit ermittelt und darauf aufbauend entsprechende Handlungsempfehlungen generiert, die wiederum mit hierzu passenden UmsetzungsvorschlÃ¤gen verknÃ¼pft sind. Der Beitrag hebt dabei insbesondere auf den dahinterliegenden Klass fikation- und Selektionsprozess sowie die Angebotsauswahl ab. Der Beitrag stellt konzise und in sehr guter sprachlicher QualitÃ¤t das dem [redacted] zugrundeliegende Konzept des Smart Matchings vor. Das von [redacted] vorgestellt Tool ist ohne Frage von hohem Wert fÃ¼r KMU. Da der [redacted] bereits verÃ¶ffentlicht ist, der Neuigkeitswert des Vortrags fÃ¼r IT-Security-Experten jedoch begrenzt.**
43	[redacted]	**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**		**Bewertung erfolgt neutral,da das Themengebiet/Vortrag aus dem [redacted] kommt.**
43	[redacted]	0	1	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0		Der Beitrag wurde zwar nicht ausreichend anonymisiert (er stammt vermutlich von [redacted]) und de [redacted] ist auch bereits ein Jahr alt und damit nicht mehr neu. GrundsÃ¤tzlich ist der verfolgte Ansatz jedoch innovativ und kann fÃ¼r KMU wertvolle Hilfeste lungen liefern.
44	[redacted]	1	0	0	0	0	1	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	2,3	GrundsÃ¤tzlich behandelt das Paper ein nach wie vor aktuelles Thema wobei der Ansatz im ISMS und DMS auf ein gemeinsames Tool und damit einen gemeinsamen Datenbestand zurÃ¼ckzugreifen nicht gÃ¤nz ich neu ist. Allerdings wird dadurch noch nicht automatisch ein integriertes Managementsysteme erzeugt wie es das Paper nahelegt da hier einfach auch noch weitergehende Fragen zu beantworten sind. Diese werden jedoch nur oberflÃ¤ch ich aufgegriffen. DarÃ¼ber hinaus werden die Vorteile eines Tooleinsatzes plakativ hervorgehoben wÃ¤hrend die Nachteile nicht behandelt werden. Hier fehlt es dem Paper an der erforderlichen NeutralitÃ¤t. Daher nur ein insgesamt neutrales Votum.
44	[redacted]	**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**		**Der Beitrag hat zwei wesentliche Aussagen: a) Informationssicherheitsmanagement und Datenschutz-Management sollten zusammen betrachtet werden b) WerkzeugunterstÃ¼tzung ist bei der Umsetzung hilfreich Beides sind sicher absolut richtige Feststellungen - nur aus meiner Sicht auch absolut nicht neu. Es ist nicht erkennbar, welche neuen Erkenntnisse der Beitrag bringt.**
44	[redacted]	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**		**Beitrag nicht besonders innovativ und unklar, worum es inhaltlich genauer gehen soll. Nur allgemeine AusfÃ¼hrungen. Ã„hn iche Thematik wurde bereits letztes Jahr eingereicht.**
45	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	4	Der Beitrag greift Frageste lungen auf die innerhalb der Branche als auch vonseiten der Ministerien und BehÃ¶rden diskutiert werden. Insbesondere zwei thematische Bereiche sind im [redacted] als Aufgabenbereiche verankert: Die Aufgaben im Rahmen von KRITIS sowie die der Digitalisierung der Energiewirtschaft. [redacted] Davon sind Gas- und Stromverteilnetze betroffen da eine Nutzung von intelligenten Messsystemen verpflichtend wird. Die im Beitrag beschriebene Notwendigkeit auch in der OT Mechanismen zur Angr ffserkennung zu implementieren zeichnete sich bereits in der Vergangenheit ab und spiegelt sich in den neuen Anforderungen zur Angriffserkennung im IT-Sicherheitsgesetz 2.0 wieder. Daher sind die Ergebnisse des Beitrags von sehr hohem Interesse fÃ¼r mehrere Bereiche des [redacted] und kann wichtige Impuls fÃ¼r deren zukÃ¼nftige Arbeit geben.
45	[redacted]	**1**	**0**	**0**	**0**	**0**	**1**	**1**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**		**Es so l basierend auf der Erfahrung aus konkreten VorfÃ¤llen die praktische Umsetzung eines Defense-In-Depth-Ansatzes in der OT von Energieversorgungsunternehmen aufgezeigt werden. Sicherlich ein interessanter Beitrag zur aktuellen Diskussion.**
45	[redacted]	**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**		**Der Vortrag gehÃ¶rt zu den 25% der Besten, da er einen ausfÃ¼hrlichen LÃ¶sungsansatz zeigt.**
46	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	2,7	Behandelt wird das Thema "Webanwendungen" unter dem irrefÃ¼hrenden Titel "Penetrationstests". Bedauerlicherweise wird versucht verschiedene Aspekte der "Bewertung" eines Webauftrittes in ein Schema "Priorisierung" zu pressen. Grundwerte (VVI) Techniken etc. werden dabei nicht herangezogen um eine Priorisierung zu begrÃ¼nden. Ebenso wird das Ergebnis einer "Priorisierung" nicht anderen "Bewertungsmatrizen" bzw. "BewertungsmÃ¶glichkeiten" gegenÃ¼bergestellt Die Argumentation ist schwach und wenig einleuchtend
46	[redacted]	**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**		**[redacted] Beitrag zur Entwicklung einer Methodik fÃ¼r die Priorisierung von [redacted] Ressourcen bei komplexen Webanwendungen. Die Selektion auf der Basis von Ã„hnlichkeiten in Funktionspunkten kÃ¶nnte in der Praxis tatsÃ¤chlich sinnvoll sein.**
46	[redacted]	**1**	**0**	**0**	**1**	**0**	**0**	**0**	**1**	**0**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**		**Das Thema ist weder neu noch besonders eindrucksvoll dargestellt. Ich habe Zweifel, dass die Value-Oriented Prioritization nutzbringend ist.**
47	[redacted]	**1**	**0**	**0**	**0**	**0**	**1**	**1**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**3,3**	**Metr ken in der IT-Sichehreit sind zwar nicht neu, werden aber noch zu wenig eingesetzt, um Handlungsbedarf aufzuzeigen. Da Transparenz bei immer komplexeren Systemen wichtig ist, kann der Vortrag hier wertvoll sein.**
47	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0		Die KPI-basierte Bewertung der Resilienz von Organisationen in Wirtschaft Gesellschaft und Verwaltung ist Voraussetzung fÃ¼r viele Bereiche: IT-Budgets Cyber-Versicherungen Lagebewertung Risikomanagement Benchmarking um nur einige zu nennen. Sollte der in dem Beitrag skizzierte Ansatz verbreiteten Einsatz finden kÃ¶nnten wesentliche Probleme der Messung von Cyber-Sicherheit adressiert werden - sowohl auf Ebene der einzelnen Organisation wie auch auf der Ebene der gesamtgesellschaftlichen sicheren Digita isierung. Die Erfahrungen und Ergebnisse aus der Studie sollten daher der FachÃ¶ffentlichkeit zugÃ¤nglich gemacht werden.
47	[redacted]	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**		**Ein Firmenlogo prankt Ã¼ber dem Abstract. Leider leistet der Beitrag nicht was er verspricht - [redacted] . Die Vorgehensweise zum Scoring ist folgende: mit einem bestimmten technischen System werden exponierte IT-Systeme/Komponenten der betrachteten Organsiation ermittelt. Dieser werden einer Art Pentest unterzogen, die Testergebnisse fliessen in die Bewertung ein. Wie genau die Bewertung und die Bildung eines Scores erfolgt bleibt leider unklar. Damit ist nicht klar welchen neuen Beitrag der Abstract haben soll. ErwÃ¤hnte wird die beispielhafte Bewertung von hessischen Gemeinden. Welchen Score haben diese denn? Leider wird keine Antwort gegeben oder in AUssicht gestellt.**
48	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	3,7	Da Ransomware eine herausragende Bedrohung fÃ¼r Staat Wirtschaft und Gesellschaft darstellt und wiederholt beobachtet werden kann dass auch grundlegende IT-SicherheitsmaÃŸnahmen nur unzureichend umgesetzt werden befÃ¼rworte ich die Aufnahme dieses Beitrags auf den Kongress. Inhalt ich wird das Thema umfassend abgedeckt und fachlich korrekt wiedergegeben. Hierbei werden auch aktuelle Entwicklungen berÃ¼cksichtigt was fÃ¼r einen tiefgreifendes VerstÃ¤ndnis des Autors spricht. Zwar werden seitens das [redacted] und der IT-Sicherheitscommunity einige Begriffe nicht so verwendet wie der Autor sie verwendet aber die Begriffe in der IT-Sicherheit unterliegen mitunter einer fluiden Def nition. Da die verwendeten Begriffe wie "Wasserbetteffekt" nicht mit anderen PhÃ¤nomen missverstanden werden kÃ¶nnen erkenne ich dies nicht als Mangel an. Die abgeleitete Empfehlung fÃ¼r das Ris komanagement in Unternehmen ist der entscheidende Appell weshalb der Beitrag meiner Meinung nach unbedingt aufgenommen werden sollte.
48	[redacted]	**1**	**0**	**0**	**0**	**0**	**1**	**1**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**		**Ãœberblick Ã¼ber die Angreifer-Vorgehensweisen bei Ransomware-Attacken. Keine besonders neuen Erkenntnisse, da jedoch das Wissen Ã¼ber die Vorgehensweisen und Methoden im Detail noch ungenÃ¼gend verbreitet ist eine sinnvolle ErgÃ¤nzung des Programms insb. fÃ¼r Teilnehmende aus der Wirtschaft.**
48	[redacted]	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**		**Diskutiert wird der Stand der Technik bzw. Modus Operandi auf seiten der TÃ¤ter im Ransomware Umfeld. Allerdings gehen die Informationen des Beitrags nicht Ã¼ber das hinaus, was aus dem BSI-Lagebericht zur SIcherheit zum Thema entnommen werden kann.**
49	[redacted]	1	0	0	1	0	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	2,3	Die inhaltliche Gliederung wurde im Abstract nicht ausreichend dargestellt. Die Kernaussagen des Beitrags sind nicht erkennbar. Entsprechend lÃ¤sst sich aus dem Abstract keine konkrete Relevanz des Beitrags ableiten. Das Abstract ist sehr allgemein gehalten und listet in erster Linie Grundlagen auf. Der innovative fachliche Mehrwert zum Thema ist in den vorliegenden Informationen nicht erkennbar. Daher kÃ¶nnen wir keine Empfehlung zur Aufnahme ins Programm des BSI-Kongresses aussprechen obgleich das Thema im Grundsatz der Zielstellung des Kongresses entspricht.
49	[redacted]	**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**		**Der Beitrag wÃ¤rmt Sensibilisierung, Awareness und Stakeholdermanagement unter dem Begriff "Security Marketing" neu auf. Dauerthema, das sicherlich bei vielen "technischen" CISOs auch zu kurz kommt.**
49	[redacted]	**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**1**	**0**	**0**	**0**		**Der Beitrag geht Ã¼ber eine Darstellung nicht hinaus und bringt auch keine konkreten AnsÃ¤tze. Aufgrund der OberflÃ¤chlichkeit des Beitrages sollte dieser eher abgelehnt werden.**
50	[redacted]	**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**3,7**	**Zukunftsorientierter Beitrag mit vielen wichtigen Bezugspunkten zur Bedrohungslage von morgen. Inhaltlich bleibt der Abstract an der OberflÃ¤che, sodass die fachliche Eignung nur bedingt beurteilt werden kann. Insgesamt konnte aber ein guter Ersteindruck gewonnen werden. Sicherlich ein interessanter Vortragsslot fÃ¼r den Kongress und ein Beitrag, der sich - zumindest von den von mir evaluierten Einreichungen - abhebt. Aufnahme in das Programm wird empfohlen.**
50	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0		Etwa 2/3 des Beitrags beschÃ¤ftigt sich mit standardisierten Verfahren. Im letzten drittel erwÃ¤hnen die Autoren eine [redacted] sowie das Thema (Teil-)Automatisierung im lokalen Incident Handling. Diese Themen haben durchaus Potenzial. Ob Sie neues oder nnovatives bieten bleibt aber offen.
50	[redacted]	**1**	**0**	**0**	**0**	**0**	**1**	**1**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**		**Die Bewertung erfolgt neutral; es wurden zu wenig neue DenkansÃ¤tze eingebracht**
51	[redacted]	**1**	**0**	**0**	**0**	**0**	**1**	**1**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**4**	**Der Beitrag schildert den Einsatz sog. digitaler Siegel in Form von Barcodes zur Sicherung der IntegritÃ¤t und AuthentizitÃ¤t von Papierdokumenten oder Nachweisen in mobilen Apps. Diese Technologie ist hervorragend geeignet um eine BrÃ¼cke zwischen analogen Prozessen und Dokumenten und einer digitalen (mobilen) Nutzung zu schaffen. Eine prototypische Anwendung wird ebenfalls erlÃ¤utert und Schritte zur Umsetzung im Produktivbetrieb aufgezeigt. Die Arbeit wird daher zur Aufnahme in das Programm empfohlen.**
51	[redacted]	1	0	0	0	1	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0		Thema K51 [redacted] . Ã¼bernommen//Was ist neu in K51?//MÃ¤ngel bzgl. K51 TR-03171:)Inkompatible Ablage des neuen â€žDocument Type Category 200â€œ zu TR-03137-1/ICAO daher in Siegel-Message-Bereich ablegen da Siegel-Generate/Verify unabhÃ¤ngig von Nutzdatendarstellung 2)Rechtssicherheit/Interop: Statt Anforderungsaufhebung von Zertifikatseigenschaften (K0051 S.3 Abs.3) Anforderungen bzgl. Verwaltungs-PKI/TrustServices gemÃ¤ÃŸ Trusted List (eIDAS-VO) spezifizieren/referenzieren 3)Keine DEZV <Zertifikatsnr>: â€žDocument Signer a. Certificate Referenceâ€œ gem. Standards TR-03137-1 ICAO ETSI Zertifikats-Profilen EN319412/ TS119412 belegen 4)â€žMenschen lesbare Nutzdaten-Dar-stellungâ€œ: â€žDoc. Type Category 200â€œ nicht genug. Besser XDOMEA als Metadatenstandard IT-gestÃ¼tzter Ãœbermittlung von Akten-VorgÃ¤ngen-Dokumenten zwischen BehÃ¶rden
51	[redacted]	**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**		**Der Inhalt des Papers ist durchaus interessant, da es eine neue praktisch relevante und standardisierte Technologie beschreibt und auf ein konkretes Umsetzungsprojekt verweist. Die Menge der Informationen ist nicht sehr hoch, eigentlich passt das komplette Paper in die 4-Seitenbegrenzung. Ich wÃ¼rde anregen, diese Einreichung mit [redacted] zusammenzulegen, das im Prinzip die gleiche Technologie von einer etwas anderen Seite beleuchtet.**
52	[redacted]	**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**4**	**Mit der Sicherheit von C-ITS-Systemen greift der Beitrag ein aktuelles Thema auf und operationalisiert dieses schlÃ¼ssig (1. Analyse bestehender Herausforderungen in Bezug auf die ITS; 2. Analyse des LÃ¶sungsbeitrags der TR-03164). Insgesamt leistet der Beitrag dadurch einen Erkenntnisgewinn, der eine Annahme grundsÃ¤tzlich rechtfertigt.**
52	[redacted]	**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**		**Der Beitrag spricht ein sehr wichtiges Thema an und ordnet die LÃ¶sungen auch in die technischen Normen und rechtlichen Notwendigkeiten ein. Daher wÃ¤re der Beitrag anzunehmen.**
52	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0		Die Einreichung befasst sich mit der Technischen Richtlinie TR-03164 des BSI die Vorgaben fÃ¼r Public-Key-Infrastrukturen und Komponenten fÃ¼r kooperative intel igente Transportsysteme formu iert. Im Abstract wird schlÃ¼ssig dargelegt dass die bisher bestehenden Vorgaben und Standards InterpretationsspielrÃ¤ume bei der Umsetzung lassen die zu einem uneinheitlichen IT-Sicherheitsniveau fÃ¼hren kÃ¶nnten. Diese LÃ¼cken sollen durch die TR gefÃ¼llt werden. Der Beitrag befasst sich mit einem aktuell in der Umsetzung befindlichen Vorhaben. Er ist gut strukturiert und formu iert. Ich empfehle eine Aufnahme in das Konferenzprogramm. Transparenzhinweis: An der Einreichung sind [redacted] beteiligt.
54	[redacted]	**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**3**	**Beitrag soll neben einem Ãœberblick zur Aktuellen Situation vertiefend auf die Rolle des Incident Managers eingehen und sieht neben den technischen Aspekten auch den Erfolgsfaktor Mensch als wichtigen Teil im Incident Prozess.**
54	[redacted]	1	0	0	0	0	1	1	0	0	1	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0		Einreicher hat sich MÃ¼he mit dem Layout gegeben und reichlich Text geschrieben. Dabei ist aber die HÃ¤ fte Einleitung und dann wird nicht ganz klar wo der Schwerpunkt liegt. SOC oder Incident Response Management wobei beim letzteren auch noch die Vorbereitung und psychologische Aspekte erwÃ¤hnt werden. Die Themen werden nebeneinander erwÃ¤hnt ohne das ein roter Faden fÃ¼r den Vortrag zu erkennen wÃ¤re auch wenn das Thema an sich sicher ich spanned wÃ¤re.
54	[redacted]	**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**		**Es gibt kein Ziel, das im Abstrakt formuliert wird, so ist unklar, was das Ziel Ã¼berhaupt ist. Etwas Ã¼ber viele Daten und Notwendigkeit eines SOCs sowie den Ãœbergang zum Incident Response zu schreiben reicht sicherlich nicht aus.**
55	[redacted]	1	0	0	1	0	0	1	0	0	1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0		Der Abstact weist auf bekannte Best-Practices hin jedoch nicht auf eine Vorgehensweise. Zum Aufzeigen von verfÃ¼gbaren Sammlungen wie Bausteinen im Grundschutz bzw. NIST und CSA Papern wÃ¤re das fÃ¼r KMUs oder Einzelanwender okay. AuffÃ¤llig ist dass der [redacted] nicht erwÃ¤hnt wird dieser sollte in einer Recherche zur Auditierung von sicheren Clouds auch auffindbar sein. Der Beitrag sollte abgelehnt werden.

55	[redacted]	0	1	0	1	0	0	1	0	0	1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1,7	AusfÃ¼hrungen leider viel zu kurz. Mehrwert des Ansatzes kann kaum beurteilt werden.
55	[redacted]	1	0	0	1	0	0	1	0	0	1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0		Bei dem Beitrag handelt es sich um eine Art Tutorial (oder best practice Beispiel? - das bleibt etwas unklar) bzgl. der zu berÃ¼cksichtigenden Richtlinien und Standards bei der Verlagerung einer Anwendung in die Cloud. Dabei wird mehr oder weniger unmotiviert eine Menge an Richtlinien und Standards herangezogen und dargelegt, wie diese in der Praxis anzuwenden sind. Das kann vielleicht ein nettes Tutorial werden - als Beitrag aber sicher ungeeignet, da insbesondere nicht erkennbar ist, auf welchen empirischen Erhebungen sich die ValiditÃ¤t des Vorgehens stÃ¼tzt.
56	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1		Qualitative EinschÃ¤tzung im Vergleich mit anderen wie oben angeregt kann ich nicht geben. Aber wegen Zukunftsthema bzw. neuer zukÃ¼nftige [redacted] wichtige und sinnvolle Gelegenheit [redacted] beim Kongress vorzustellen. Die Zielgruppe des Kongresses (u.a. deutsche Unternehmen und Forschung) sind wichtig fÃ¼ [redacted]
56	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	4,3	Beitrag zeigt eine Zusammenfassung zur Einrichtung des EuropÃ¤ischen Kompetenzzentrums fÃ¼r Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren (NCCs). Eine andere Zielsetzung ist nicht ersichtlich. Da der Informationswert hoch ist und ein allgemeines Interesse an dieser Thematik angenommen werden kann, wÃ¤re der Beitrag interessant fÃ¼r den Kongress.
56	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0		Der Beitrag betont die EU-Zusammenarbeit in der Cybersicherheitsforschung und ist damit relevant für den Aufbau einer europäischen digitalen Souveränität. Der Beitrag scheint bisher wenig auf die Herausforderungen und Probleme bei der Zusammenarbeit einzugehen. Dies sollte bei der weiteren Ausarbeitung nachgeholt werden.
57	[redacted]	0	1	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0		Fasst bekannte Methoden zur Detektion zusammen und liefert so einen Ãœberblick zur Gefahr und Erkennung. Nicht neu, kann aber einen Ãœberblick geben.
57	[redacted]	1	0	0	0	0	1	1	0	0	1	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	2,7	Der Beitrag veranschaulicht diverse DetektionsmÃ¶glichkeiten von einschlÃ¤gigen Webshells mittels bekannter forensischer Instrumente. Die Quellenangaben deuten auf eine Webrecherche ohne BerÃ¼cksichtigung wissenschaftlicher Studien hin. FÃ¼r das geneigte Publikum kÃ¶nnte die Vorstellung des Beitrags hinreichenden Mehrwert haben.
57	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0		Webshells sind kein neues PhÃ¤nomen sondern gehÃ¶ren seit Jahren zum Angreiferwerkzeugkasten. Der Beitrag stellt bekannte AnsÃ¤tze zur Erkennung/Auffindung von dieser speziellen Form von HintertÃ¼ren dar. Es werden jedoch nur wohl bekannte Verfahren und Werkzeuge thematisiert.
58	[redacted]	1	0	0	0	1	0	0	1	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0		Der Vortrag ist zwar innovativ (als Drehbuch fÃ¼r einen F lm) gestaltet behandelt jedoch einen recht alten Sachverhalt (ca. 5 Jahre alt) der schon im Umfeld der IT-Sicherheit im Finanzwesen bekannt ist. Er bietet keinen Mehrwert fÃ¼r den Kongress. Der beschriebene Angriff den der Einreichende im Abstract darste lt wird offensichtlich Ã¤hn ich bzw. umfangreicher beim Kongress vorgestellt. Der Vorfall wurde jedoch sogar schon in einem BSI-Lagebericht vor Jahren behandelt. Insgesamt halte ich den Beitrag fÃ¼r ungeeignet; insbesondere sehe ich keinen Mehrwert und denke nicht ob das Niveau [redacted] angemessen ist.
58	[redacted]	1	0	0	1	0	0	0	1	0	1	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1,3	Der Beitrag beschreibt als eine Art Zeitungsartikel den Cyber-Bankraub bzgl. der Bank of Bangladesh aus dem Jahre 2016. Nett aufgeschrieben - sicher gut fÃ¼r Spiegel oder Heise (wo ein vergleichbarer Bericht aber vermutlich schon erschienen ist). Ansonsten findet man darÃ¼ber auch sonst viele interessante Berichte - jedenfalls defintiv nichts fÃ¼r den BSI-Kongress.
58	[redacted]	1	0	1	0	0	0	0	1	0	1	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0		Der Beitrag stellt einen digitalen Bankraub vor, der 2016 passierte und sehr ausfÃ¼hrlich in vielen Medien beschrieben wurde, u.a. auch auf Wikipedia: https://en.wikipedia.org/wiki/Bangladesh_Bank_robbery Der Beitrag hat damit keinen Neuwert.
59	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1		Der Beitrag schildert eine Umsetzung eines Mailclients, der sowohl PGP als auch S/MIME unterstÃ¼tzt und damit eine "BrÃ¼cke" zwischen den beiden zur Zeit gÃ¤ngigen VerschlÃ¼sselungsverfahren schafft. Die "RivalitÃ¤t" dieser beiden Verfahren ist sicherlich ein Grund fÃ¼r die schwer durchsetzbare Akzeptanz von MailverschlÃ¼sselung zum derzeitigen Zeitpunkt. Insofern hat der Beitrag eine hohe praktische Relevant, weniger eine akademische. Trotzdem wird der Beitrag zur Aufnahme in das Programm empfohlen, da er einen guten Impuls zur Weiterentwicklung von gÃ¤ngigen Mailc ients setzt.
59	[redacted]	1	0	0	0	0	1	1	0	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	4,3	Im Rahmen der derzeitigen AblÃ¶se von Chiasmus im Verschlusssachenumfeld ist das Thema EmailverschlÃ¼sselung relevant und aktue l. Auch wenn keine vÃ¶llig neuen DenkansÃ¤tze vorgeste lt werden (es g bt bereits LÃ¶sungen die sowohl Smime als auch gpg unterstÃ¼tzen) so ist dennoch eine Darstellung der Herausforderungen Probleme und LÃ¶sungsansÃ¤tze im Kontext einer gleichzeitigen UnterstÃ¼tzung beider Standards interessant. Daher sollte der Vortrag angenommen werden.
59	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0		Bei der Einreichung handelt es sich um einen Erfahrungsbericht ohne groÃŸe methodische Neuigkeit. Die betrachtete Fragestellung ist durchaus praktisch relevant und die erarbeitete LÃ¶sung kann als eine gelungene Fallstudie gewertet werden. FÃ¼r die Endversion wÃ¼rde ich es mir wÃ¼nschen, etwas besser zwischen prinzipiellen Schwierigkeiten und Implementierungsanforderungen, die FleiÃŸarbeit erfordern, zu unterscheiden. Schreibfehler: â€žBenutzerfreunlichkeitâ€œ, â€ž-Mailâ€œ.
60	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1		Der Beitrag schildert Erfahrungen aus der Umsetzung eines Projekts zur gemeinschaftlichen Umsetzung von MailverschlÃ¼sselung im Umfeld von VS- und Nicht-VS Kommunikation in einem System. Er geht insbesondere auf technische Erfahrungen und Konsequenzen fÃ¼r die zugrundeliegende Systemarchitektur ein und ist insofern auch von hoher praktischer Relevanz, da ein solcher "hybrider" Betrieb ein wesent icher Beitrag zur Steigerung der Akzeptanz des Einsatzes von MailverschlÃ¼sselung ist. Der Beitrag wird insbesondere aufgrund der hohen praktischen Relevanz zur Aufnahme in das Programm empfohlen.
60	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	4	Der Beitrag sollte im Falle einer Annahme grÃ¼ndlich bearbeitet werden. Beispiele: S/MIME VerschlÃ¼sselung ohne Hinweis auf Betreffszeile, VS-NfD konforme Signaturen anstelle der Terminologie qualifizierte Signatur (das Thema der qualifizierten Signatur und damit das erfÃ¼llen der Unterschriftsanforderung wird gÃ¤nzlich ausgespart) etc.
60	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0		Im Rahmen der derzeitigen AblÃ¶se von Chiasmus fÃ¼r VS-NfD-Verschlusssachen ist das Thema Ema lverschlÃ¼sselung relevant und aktuell. Durch die Chiasmus-AblÃ¶se wird voraussichtlich ein Mischbetrieb von VS/NonVS â€“EmailverschlÃ¼sselung ein immer relevanterer Anwendungsfall. Eine solche Case-Study mit Beschreibung von typischen Problemen samt LÃ¶sungsansÃ¤tzen wird fÃ¼r Ã¤hnliche zukÃ¼nftige Projekte interessant und hilfreich sein. Daher sollte der Vortrag angenommen werden.
61	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1,7	[redacted] Kurze EinschÃ¤tzung: - In dem Abstract ist wenig wissenschaft iche QualitÃ¤t erkennbar. Es kann jedoch als Praxisleitfaden sinnvoll sein. - Eine kurze Recherche ergab dass das selbe Thema mit der gleichen Detektionstechnik bereits 2020 in einem Paper von Forschern der TU Prag vorgestellt und diskutiert wurde (https://www.scitepress.org/Papers/2020/89550/89550.pdf) Ist das behandelte Thema fÃ¼r 2022 relevant - Ja Kerberoasting ist in Mitre Att&ck neben Golden Ticket gelistet (https://attack.mitre.org/techniques/T1558/003/) Ist das Abstract innovativ - Nein Ist das Abstract frei von handwerklichen Fehlern - Auf den ersten Blick ja jedoch ist nicht klar in wie weit die Honeypot-Technik in grÃ¶ÃŸeren Umgebungen funktioniert wenn EntitÃ¤ten legitim angefragt werden. Hier greift der Personalengpass Aufgrund der zwei anfangs genannten GrÃ¼nden raten wir das Abstract fÃ¼r den BSI-Kongress abzulehnen
61	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0		Der Beitrag diskutiert technisch, wie durch Einrichtung von KÃ¶der-Accounts und Beobachtung der Interaktion mit diesen sogenannte Kerberoasting-AktivitÃ¤ten frÃ¼hzeitig erkannt werden kÃ¶nnen. Sowohl Angriff als auch KÃ¶dertechnik sind zwar aktuell praxisrelevant, aber nicht neu.
61	[redacted]	0	1	0	1	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0		Der Beitrag ist nicht sonderlich spannend geschrieben. Ich glaube kaum, dass er viele Besucher anziehen wird. Das Paper ist mit 6 Seiten zu lang und entspricht nicht den formalen Aspekten.
62	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0		Der Beitrag fokussiert auf die Chance von Siegeln als SicherheitsqualitÃ¤tskennzeichen und adressiert auch die heutigen Probleme in dem Zusammenhang
62	[redacted]	1	0	0	0	1	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0		Ein wirklicher fachlicher Bezug ist fÃ¼r mich nicht erkennbar. ISO 27k-Zertifikate und z.B TISAX sind heute schon etablierte Mittel, es erschlieÃŸt sich mir nicht, was das Erfolgsmodell Fairtrade-Siegel hier beitragen soll
62	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	3,3	Der Artikel adressiert die Problematik von Informationsasymmetrien bei der Beschaffung von informationstechnisch sicheren Produkten zwischen den Produktanbietern Vertrauensanbietern fÃ¼r GÃ¼tesiegel/Zertifikate und KMU als Produktverbrauchern die zu mangelnder Akzeptanz und Nutzung von GÃ¼tesiegeln bzw. Zertifikaten fÃ¼hren. Er geht das Problem mit einer vergleichenden Untersuchung bestehender Zertifikate und Siegel und alternativer AnsÃ¤tze an identifiziert die wesentlichen Faktoren fÃ¼r deren Akzeptanz und leitet daraus Handlungsempfehlungen fÃ¼r die Akteure ab. Die Problemstellung ist relevant und der LÃ¶sungsansatz erscheint zielfÃ¼hrend. Die Ãœbertragbarkeit der Analyseergebnisse von Fair-Trade auf IT-Siegel bleibt zu belegen erscheint aber zumindest aussichtsreich. Die Ergebnisse versprechen einen konkreten handlungsleitenden Mehrwert fÃ¼r die benannten Akteure einschl. dem BSI. Der Artikel ist einwandfrei art kuliert und stringent organisiert. Die Annahme wird daher befÃ¼rwortet.
63	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1		Der Beitrag fÃ¼hrt eine Vorgehensweise zur nachhaltigen PrÃ¤vention im Unternehmen vor. Dabei wird insbesondere kritisiert dass Unternehmen oftmals LÃ¶sungen von der Stange kaufen und dann bei der Umsetzung / im Change Management Fehler machen. Hierdurch wird die IT-Sicherheit nicht gefÃ¶rdert aber Ressourcen verschwendet. Der Ansatz ist sehr gut dargestellt und weckt Interesse an der konkreten Umsetzung.
63	[redacted]	0	1	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	4,5	Der Beitrag stellt ein Modell zum Erlernen sicherheitsbewussten Verhaltens in Unternehmen vor. Dabei wird insbesondere folgender Beitrag zitiert: [redacted] [redacted]
64	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1		Der Vortrag gehÃ¶rt zu den 10% der Besten und sollte auf jeden Fall angenommen werden. AktualitÃ¤t erhÃ¤lt der Beitrag, da durch den Vermehrten Einsatz von Online-Meetings die Gefahr eines Angriffs in diesem Bereich gewachsen ist.
64	[redacted]	1	0	0	1	0	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	4,7	Der Beitrag beleuchtet ein aktuelles und von wenigen europÃ¤ischen Arbeitsgruppen behandeltes Thema. Die Kombination von Stimm- und Videomanipulation ist von besonderer Relevanz. Jedoch lÃ¤sst die Kurzbeschreibung keine RÃ¼ckschlÃ¼sse auf die QualitÃ¤t und Nutzung von besonders innovativen Verfahren zu. Bei Annahme des Beitrags muss die QualitÃ¤t der genutzten Verfahren detaillierter evaluiert werden. Weiterhin sollte die Struktur des Beitrags verbessert werden und Literaturangaben hinzugefÃ¼gt werden.
64	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1		Praktische Vorstellung des Stands der Technik bei Phishing in Messengern und Video/Audioconferencing mit Hilfe von aktueller ML-gestÃ¼tzter Simulation echter Personen. Als Ausb ick auf die Zukunft sehr sinnvoller Beitrag.
65	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0		UnterstÃ¼tzung und Teil-Automatisierung der ÃœberprÃ¼fung der Rechner-Konfigurationen sind nicht neu, es mangelt eher an der Umsetzung, hier kÃ¶nnte der Beitrag zur Awareness beitragen.
65	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	3,7	Der im Beitrag vorgestellte Ansatz zur Wartung und Umsetzung von Sicherheitsrichtlinien (wie beispielsweise aus dem SiSyPHuS Win 10-Projekt bzw. des Center for Information Security) soll im Wesentlichen die verschiedenen Herausforderungen bei der Umsetzung berÃ¼cksichtigen. Die Vorgehensweise des beschriebenen Ansatzes orientiert sich dabei an gÃ¤ngigen Prozessen des IT-Sicherheitsmanagements. Besonderes Interesse wecken die entwickelten Werkzeuge sowie die technische Umsetzung des Imports der Richtlinien hrer Verarbeitung und Anpassung sowie die Skript-basierte automatische ÃœberfÃ¼hrung in die zu hÃ¤rtenden Zielsysteme. Hier kÃ¶nnte fÃ¼r die Zielgruppe ein Mehrwert entstehen in dem sie bei der Anpassung und Umsetzung von Sicherheitsrichtlinien durch die Werkzeuge entsprechend unterstÃ¼tzt werden. Positiv ist anzumerken dass der Beitrag praxisorientiert am Fal beispiel gestaltet werden soll und eine Demo der Evaluation zur Veranschaulichung gezeigt wird.
65	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0		Beitrag ist gut und enthÃ¤lt auch im Hinblick auf Innovation gute und zukunftsorientierte AnsÃ¤tze.
66	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0		Zeigt eine LÃ¶sung auf, wie die (eigentliche) SelbstverstÃ¤ndlichkeit Asset-Management auch mal wirklich implementiert werden kann. KÃ¶nnte Mut machen, es doch im eigenen Unternehmen /in der eigenen Organisation mal zu versuchen und nicht an der befÃ¼rchteten KomplexitÃ¤t zu scheitern.
66	[redacted]	0	1	0	0	1	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	2,3	Der Beitrag fÃ¤llt bereits in der Einleitung durch die Nennung eines Produktes in dem der vorgestellte Ansatz umgesetzt sei negativ auf. Durch die Produktnennung ist das formale Kriterium der AnonymitÃ¤t nicht erfÃ¼llt. Prinzipiell ist eine Kontextdatenbank sinnvoll und interessant vor allem wenn Kontextinformationen aus verschiedenen Quellen automatisch gesammelt konsolidiert gepflegt und bereitgestellt werden. Leider reiÃŸt das Abstract das Thema nur an und nennt Te le der LÃ¶sung wie SIEM-Regeln Graph-Datenbank ESPER (eine Java Bibliothek mit SQL Ã¤hn icher Syntax). Es ist dem Dokument nicht zu entnehmen wie diese Automatisierung praktisch funktionieren soll. Die Autoren vergleichen ihren Ansatz nicht mit denen anderer Arbeiten und kÃ¶nnen daher seine Einzigartigkeit und seinen Innovationscharakter nicht belegen.
66	[redacted]	1	0	0	0	1	0	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0		Der Beitrag thematisiert den Umstand, dass die Hinzuziehung von Kontextinformationen von Vorteil fÃ¼r Erkennung, Analyse und Incident Response sein kÃ¶nnen und nennt ein konkretes Produkt, welches dies realisiert. Er enthÃ¤lt weder neue noch besonders Ã¼berraschende/interessante Einsichten.
67	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1		Der Beitrag schildert den Einsatz eines neuartigen Konzepts zur farbigen Kodierung von 2d Barcodes im Kontext von digitalen Siegeln auf analogen (hoheitlichen) Dokumenten. Die neuartige Kodierung ermÃ¶glicht den einfacheren Einsatz insbesondere auf hoheit ichen Dokumenten mit entsprechendem Sicherheitspapier sowie erweiterte Kodierungs- und Speicheroptionen. Es wird auch auf die bereits laufende nationale und internationale Standardisierung eingegangen. Digitale Siegel schaffen eine wichtige BrÃ¼cke bei der sicheren Digitalisierung bestehender analoger Prozesse und Nachweise. Der Beitrag wird daher zur Akzeptanz fÃ¼r das Konferenzprogramm empfohlen.
67	[redacted]	1	0	0	0	0	1	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	5	Der Beitrag ist gut strukturiert und verstÃ¤nd ich geschrieben. Die Autoren liefern einen relevanten Beitrag fÃ¼r die praktikable und internationale Nutzung Digitaler Siegel. Im vollstÃ¤ndigen Beitrag wÃ¤re es wÃ¼nschenswert wenn die folgenden Aspekte berÃ¼cksichtigt werden wÃ¼rden: 1) Technische Details zur SpeichergrÃ¶ÃŸe der Barcodes. Welche Faktoren beeinflussen diese? 2) Detaillierte AusfÃ¼hrung der Sicherheitseigenschaften der Anwendung Digitaler Siegel mittels JAB-Codes.

67	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1		**Diese Einreichung ist mit [redacted] eng verwandt und kann aus meiner Sicht mit dieser zusammengelegt werden. Hier geht es um Farbe als weiteres Merkmal, um die Informationsdichte von QR-Codes zu erhÃ¶hen, und die Umsetzung dieses Prinzips in einem neuen Standard. Der Beitrag ist gut verstÃ¤ndlich beschrieben und behandelt, Ã¤hnlich wie [redacted], die Thematik innerhalb der 4 Seiten weitgehend abschlieÃŸend, so dass fÃ¼r die finale Version eigentlich keine groÃŸe Erweiterung notwendig wÃ¤re. Aus technischer Sicht hÃ¤tte mich interessiert, welche Anforderungen auf die Medien (Papier usw.) sowie an die Farbmittel gestellt werden, damit die QR-Codes auch bei entsprechender Alterung (VerfÃ¤rbung durch Sonneneinstrahlung, Radiationseinwirkung usw.) langfristig zuverlÃ¤ssig funktionieren.**
68	[redacted]	0	1	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	**3,5**	**Gute Darstellung der aktuellen Situation in der OT und er Notwendigkeit zur ganzheitlichen Integration Auseinandersetzung mit den Herausforderungen sowohl seitens der Technik als auch der Organisation und Prozesse**
68	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0		Das wird kein theoretischer Vortrag. In dem Abstract wird der Praxisanteil nicht explizit beschrieben man kann aber zwischen den Ze len sehr gut die Praxiserfahrung lesen die dem Vortrag zugrunde liegen wird. Es wÃ¤re somit ein guter Vortrag in OT und die Herausforderungen von OT Monitoring LÃ¶sungen die Teil der Angriffserkennungssysteme sind die IT-SiG 2.0 fordert und fÃ¼r die ZuhÃ¶rer interessant sein wird die nicht aus dem klassischen IT- oder BehÃ¶rdenumfeld stammen.
68	[redacted]	0	1	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0		Das Thema ist aufgrund der geforderten Angriffserkennungssysteme nach IT-SiG 2.0 aktuell. Der Abstract beschrÃ¤nkt sich leider darauf die Herausforderungen/Anforderungen zu beschreiben ohne die im Titel genannten Erfahrungen einflieÃŸen zu lassen. FÃ¼r den Fall dass dies beim Vortrag so wÃ¤re ist es sicherlich fÃ¼r die ZuhÃ¶rer ein interessanter Vortrag. Da dies nicht klar erkennbar ist folgt eine neutrale Bewertung des Beitrags.
68	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0		**Hochaktuelles Thema. Integration und Betrieb von Security Monitoring im OT Umfeld, wobei explizit die Diskussion von Praxiserfahrungen angekÃ¼ndigt wird.. Daher die Empfehlung zur Aufnahme.**
69	[redacted]	1	0	0	0	1	0	0	1	0	1	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1,6	Der Beitrag enthÃ¤lt eine Sammlung aus subjektivem Eindruck erfasster Wahrnehmungen zur IT-Sicherheit in Arztpraxen. Der Beitrag hat keine logische Struktur (z.B. Problemdarste lung Problemaufarbeitung LÃ¶sung) verfolgt kein erkennbares Ziel (z.B. Simplifizierung Vertiefung oder Optimierungsansatz) und prÃ¤sentiert keine LÃ¶sungen. Letztlich bleibt der Leser mit vielen offenen Fragen im Raum zurÃ¼ck. Der fachliche Ante l an IT-Sicherheit und BSI-Themen ist eher gering. Da die inhaltlich angerissenen Problemstellungen derzeit alle Arztpraxen haben und keine LÃ¶sungen prÃ¤sentiert werden wÃ¤re eine VerÃ¶ffent ichung kontraproduktiv.
69	[redacted]	1	0	0	1	0	0	1	0	0	1	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0		**Der Beitrag behandelt Probleme/Fragen bzgl. IT-Sicherheit/Datenschutz in Zusammenhang mit der Digitalisierung im Gesundheitswesen aus der Perspektive einer Arztpraxis. Es ble bt insgesamt unklar, was die Aussage des Beitrages sein soll. Es handelt sich um ein Sammelsurium an Aussagen/Fragen, wobei jeweils unklar ist, was damit bezweckt wird bzw. was Ã¼berhaupt der Inhalt ist. Manches scheint inhaltlich auch fraglich. Insgesamt wirkt der Beitrag so, als habe sich jemand den "Frust von der Seele geschrieben" bzgl Digitalisierung. Insgesamt ist das Thema sicher relevant und der Frust in Teilen nachvollziehbar - aber so wie der Beitrag das Problem angeht, ist es nicht hilfreich.**
69	[redacted]	1	0	0	1	0	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0		**Der Beitrag ist ein sehr persönlicher Erfahrugsbericht aus dem Alltag der IT-Sicherheit in einer kleinen Arztpraxis. Empirische Beobachtungen sind zwar durchaus interessant, können aber nur bedingt vera lgemeinert werden. Es fehlt der wissenschaftliche Zugang, die analytische Tiefe ist gering.**
70	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	**4**	**Qualitativ deutlich fortgeschritten im Vergleich zu den restlichen von mir bewerteten Einreichungen. Aufnahme wird stark befÃ¼rwortet - auch wenn das Thema beim Kongress mehr Zeit in Anspruch nehmen mÃ¼sste, um es adÃ¤quat darstellen zu kÃ¶nnen. Aufnahme sollte davon abhÃ¤ngen, wie viele weitere qualitativ hochwertige Einreichungen im Bereich Post-Quantum Migration vorliegen.**
70	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1		Der Beitrag adressiert ein sehr wichtiges und aktuelles Problem die Umstellung von Public-Key-Infrastrukturen auf quantensichere Verfahren. Hierzu haben die Autor:innen des Beitrags verschiedene LÃ¶sungsansÃ¤tze betrachtet und aus Sicht verschiedener Industrieanwendungen bewertet. Daraus haben sie eine prÃ¤ferierte LÃ¶sung abgeleitet (Mixed-PKI) und zu dieser Untersuchungen hinsichtlich der Prakt kabilitÃ¤t durchgefÃ¼hrt. Die Kurzversion verspricht interessante Erkenntnisse aus diesen Untersuchungen. Die inhaltliche und editorische QualitÃ¤t des Beitrags ist sehr gut und er passt sehr gut in das Kongressthema "Aktuelle Entwicklungen in der Kryptografie". Der Beitrag so lte auf jeden Fall ins Programm aufgenommen werden gerade auch im Vergleich mit anderen BeitrÃ¤gen zu Ã¤hnlichen Themen.
70	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0		**Der Vortrag so lte abgelehnt werden, da er zu theoretisch mit wenig Praxisbezug ist.**
71	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	**3**	**Der Beitrag stellt ein System zum ÃœberprÃ¼fen der Office-Makros in einer Organisation vor. Die Makros werden zuerst automatisch vorsortiert. die ungefÃ¤hrlichen werden signiert und durchgelassen, die gefÃ¤hrlichen werden gesperrt, die Signaturen der Makros werden zum spÃ¤teren Abgleich gespeichert. Der Rest wird manuell sortiert. Ich kann das Neuwert des System nicht einschÃ¤tzen. AuÃŸerdem wird im Beitrag folgendes in der Gliederung versprochen: 4 Evaluation des Tools 4.1 Statistische Analyse zur Erkennungsgenauigkeit 4.2 User Experience zum Webservice Dazu steht aber absolut nichts im Absract, so dass ich nicht ienschÃ¤tzen kann, wie die EffektivitÃ¤t, Effizienz und die User Experience methodisch evaluiert wurden, und ob sie gut sind. Es lÃ¤sst sich nicht erkennen, ob diese Evaluation Ã¼berhaupt passiert ist. Deswegen erscheint mir der Beitrag nicht fundiert genug.**
71	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0		Da meine letzte Bewertung verloren gegangen ist hier nur eine Kurzzusammenfassung: * Interessantes Thema das immer noch aktuell ist * Einleitung etwas lang geraten * Fokussierung auf die Methodik wÃ¤re wÃ¼nschenswert * Zitate der Verwendeten Werkzeuge so lte erfolgen (lege artis)
71	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0		**Ich kann mir vorstellen, dass diese Ansatz fÃ¼r einige Anwender von Interesse ist. (Es gab bereits eine LÃ¶sung fÃ¼r E-Mail-AnhÃ¤nge mit Macros. Das Problem welches zusÃ¤tzlich gelÃ¶st werden sollte ist, das Klicken auf Links zum Download von Dateien mit Macros; Hier wÃ¼rde ich empfehlen im Rahmen der Awareness darauf hinzuweisen, wie man Ã¼berprÃ¼fen kann, ob der Link von einer vertrauenswÃ¼rdeigen Quelle kommt oder nicht) Was ich in dem Beitrag vermisse, ist eine Limitation Section. Der Fokus liegt auf Schadsoftware durch Macros und nicht anderen. Die Evaluation des Tools kann nicht bewertet werden, weil hierzu im Abstract nichts gesagt wird**
72	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	**4**	Der Titel des Abstracts legt einen Schwerpunkt nahe der sich in der G iederung des Abstracts nur mit sehr viel "Anlauf" wiederfindet. Teilweise ble ben die AusfÃ¼hrungen sehr abstrakt was jedoch vermutlich auf die Begrenzung des Abstract-Umfangs zurÃ¼ckzufÃ¼hren ist. Sehr schÃ¶n sind die AusfÃ¼hrung zum Problem der Dauer der Update-Pflicht. Der LÃ¶sungsansatz ist spannend. WÃ¼rde ich gerne hÃ¶ren - auch wenn es nicht der beste Abstract ist.
72	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0		UÌˆberblick der zu erwartenden Neuerung durch das Gesetz uÌˆber digitale Inhalte unter besonderer BeruÌˆcksichtigung der Updatepflicht fuÌˆr digitale Produkte. Da die Ã„nderungen fÃ¼r alle Unternehmen die digitale Produkte anbieten und betreiben relevant sind sinnvolle Awareness-Steigerung.
72	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0		**Der Titel macht Lust auf den Beitrag, allerdings wird ein sehr weiter Bogen geschlagen und nicht wirklich ersichtlich, wie genau der Zusammenhang zwischen Updatepflicht und Leitungsebene aussieht bzw. aussehen soll. Hierauf wÃ¤re die ausfÃ¼hrliche Einreichung nochmal zu Ã¼berprÃ¼fen. Insgesamt aber ein interessantes Thema, das durchaus potenzial fÃ¼r eine Vorstellung im Rahmen des Kongresses mitbringt.**
73	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	**3,7**	Interessanter und durchaus innovativer Ansatz fÃ¼r den Aufbau eines integrierten Managementsystems fÃ¼r Informationssicherheit und Datenschutz. Der Ansatz wirkt dabei vielversprechend sofern eine solche Bewertung anhand der Kurzfassung mÃ¶g ich ist. Leider sind im Deta l noch nicht alle Aspekte/Punkte 100% rund herausgearbeitet was allerdings natÃ¼rlich auch zu einem gewissen Grad an der Kurzfassung liegen kÃ¶nnte. Daher eine Empfehlung dazu dass der Beitrag angenommen werden kann.
73	[redacted]	1	0	0	1	0	0	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0		**Beitrag zeigt zwar grundsÃ¤tzlich ein wichtiges Thema, aber der Ansatz scheint wenig innovativ.**
73	[redacted]	0	1	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1		**Die Referenz ist wahrschein ich das, was die Anonymisierung des Papiers aufhebt, aber darauf habe ich jetzt nicht besonders geachtet. Der - naheliegenden und immer mehr in die KÃ¶pfe kommende - Ansatz bedarf auf jeden Fall der weiteren Verbreitung und Motivation, we l es nicht nur um die wichtigen Einsparungen geht, sondern auch die Konfliktvermeidung zwischen unterschiedlichen Anforderungen, die nicht gemeinsam ausgeprÃ¤gt werden - sondern mÃ¼hselig erst spÃ¤ter zusammengeflickt werden mÃ¼ssen.**
74	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	**2,7**	Das Thema (Security Awareness im hybriden Arbeiten) ist insbesondere fÃ¼r FÃ¼hrungskrÃ¤fte wichtig zur Entscheidung entsprechender MitteleinsÃ¤tze - insofern passt es genau zum Kongressthema. Die Besonderheiten der IT-Sicherheit im Home Office werden gut dar gestellt und LÃ¶sungsansÃ¤tze prÃ¤sentiert. Dabei werden sowohl AutomationsmÃ¶glichkeiten als auch neue AnsÃ¤tze der Mitarbeiterweiterb ldung dargestellt. K ingt also vielversprechend und innovativ.
74	[redacted]	0	1	1	0	0	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0		**Der Beitrag argumentiert, dass im hybriden Arbeiten, wie es seit der Pandemie Ã¼blich ist, die Ã¼bliche Security Awareness MaÃŸnahmen nicht ausreichen. Diese Argumentation ist gut und logisch. Leider schlÃ¤gt der beitrag folgende Methoden vor, um mehr Awareness zu erreichen (Zitat) [redacted] Leider ist es in der Forschung bekannt, dass weder "Bespielen" als auch das Simulieren der Angriffen bisher keine Wirksamkeit gezeigt hat. Wenn dieser Beitrag die Wirksamkeit untersucht hÃ¤tte, wÃ¤re es eine sehr spannende Untersuchung. Aber im jetzigen Zustand ist der Neuwert des Beitrages sehr gering.**
74	[redacted]	0	1	1	0	0	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0		**Der Beitrag ist: Folgendes bei security Awareness zu beachten: 1. Modularisierung der Inhalte 2. Einbeziehen weiterer KanÃ¤le (Messenger, Anrufe, SMS, etc.) 3. Proaktives Lernen (â€žNudgingâ€œ) 1-2 sind nichts neues und 3 ist sehr umstritten, siehe: https://publikationen.bibliothek.kit.edu/1000119662/74582106 (Phishing-Kampagnen zur Mitarbeiter-Awareness : Analyse aus verschiedenen Blickwinkeln: Security, Recht und Faktor Mensch) Es wird keine Limitation des Beitrags diskutiert Kleinigkeit: Es fehlen Quellen zu den Aussagen, wie dass Soc.Eng. deutlich zugenommen hat.**
75	[redacted]	1	0	0	0	1	0	0	1	1	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	**3**	Der eingereichte Beitrag skizziert ein Verfahren um Mikrocontroller fÃ¤lschungssicher zu machen d h. ein Austauschen durch einen gleichwertigen Mikrocontroller zu erkennen. Dabei wird der M krocontroller bei der Produktion mit einer unverÃ¤nderbaren gerÃ¤temodellspezifischen ID versehen. Die Authentifizierung eines M krocontrollers erfolgt dann Ã¼ber ein Challenge-Response Verfahren bei dem nur der originale Mikrocontroller mit der entsprechenden gerÃ¤temodellspezifischen ID in der Lage ist die fÃ¼r die Challenge korrekte Response zu erzeugen. Trotz vier Seiten Abstract bleibt die konkrete Umsetzung offen. Es wird lediglich skizziert dass gerÃ¤temodellspezifische Eigenschaften ausgenutzt werden. Eine Authentifizierung scheint dabei recht aufwendig zu sein. Der echte Nutzen - im Abstract wird einzig der Preis erwÃ¤hnt - gegenÃ¼ber einem kryptografischen Cha lenge-Response Verfahren mit entsprechend sicher gespeichertem SchlÃ¼ssel auf dem Controller ble bt unklar. Das resultierende Sicherheitsniveau bleibt unklar.
75	[redacted]	1	0	0	0	1	0	1	0	1	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0		**Unklar, ob der geschilderte Ansatz zielfÃ¼hrend ist im Vergleich zu herkÃ¶mmlichen PUFs bzw. embedded Sicherheitsmerkmalen; erreichbares Sicherheitsniveau und Robustheit gegen Angriffe unklar im Rahmen des Abstracts.**
75	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0		**Der Beitrag betrachtet die Frage, wie gefÃ¤lsche Komponenten erkannt werden kÃ¶nnen. In diesem Kontext werden physikalisch nicht-klonbare Funktionen (PUFs) seit einigen Jahren diskutiert. Der Beitrag thematisiert alternativ die Nutzung "schwer simulierbarer Eigenschaften" und stellt die Unterschiede/Vorteile dieses Ansatzes heraus. Nach meinem Kenntnisstand (dies ist nicht mein Gebiet) sind das relativ neuartige Ideen/Betrachtungen.**
76	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	**3,7**	**Der Beitrag schildert einen prototypischen Einsatz von PQC Technologien im Umfeld von VS Layer 1 VerschlÃ¼sselung. Es wird auf die Integration der neuen Mechanismen eingegangen, zusÃ¤tzlich werden aber auch Auswirkungen auf Protokollebene im Sinne der Kodierung geschildert. Der Beitrag liefert daher einen Beitrag zur praktischen Umsetzung von PQC Migrationsprojekten und wird prinzipiell zur Aufnahme empfohlen.**
76	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0		Im Beitrag wird eine Implementation eines quantensicheren hybriden VerschlÃ¼sselungsmechanismus im OSI Layer 1 beschrieben. Als quantensicherer Anteil kommt hier Classic McEliece zum Einsatz ein Verfahren zum SchlÃ¼sselaustausch (Ã¼ber Key encapsulation) das in der laufenden 3. Runde des NIST-Prozesses zu den Finalisten gehÃ¶rt und vom BSI als konservatives Verfahren auch in den vorlÃ¤ufigen Handlungsempfehlungen (https://www.bsi.bund.de/pq-Migration.html) empfohlen wird. Ein interessanter Aspekt an der Layer 1-VerschlÃ¼sselung ist dass diese hochperformant umgesetzt werden kann. In der Langfassung des Beitrages soll es konkrete Testdaten zu einem Einsatz in einem Glasfasernetz geben. Die theoretischen und praktischen Erkenntnisse der Arbeit halte ich fÃ¼r sehr interessant und besonders fÃ¼r die VS-Verarbeitung relevant weshalb ich den Beitrag zur VerÃ¶ffentlichung empfehle.

76	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0		Die Einreichung thematisiert die Anwendung des NIST-Kandidaten Classic McElliece in einer praktischen Applikation, in der seine hohe Anforderungen an den SchlÃ¼sselspeicher nicht besonders kritisch sind. Es ist ein sehr anwendungsorientierter Beitrag, methodische Neuigkeit ist nicht zu erwarten. Die Zusammenfassung behandelt im Wesentlichen die Motivation der Arbeit (die aus meiner Sicht die Problematik korrekt einordnet); die eigentlich LÃ¶sung wird aber kaum beschrieben. Deswegen ist es etwas schwierig, die QualitÃ¤t des zu erwartenden endgÃ¼ltigen Beitrags zu antizipieren, obwohl eigentlich noch Seiten verfÃ¼gbar gewesen wÃ¤ren. Deswegen wÃ¼rde ich eher keine klare Empfehlung abgeben wollen; der Beitrag kann interessant vorgetragen werden, kann aber auch eine â€žKatze im Sackâ€œ sein. FÃ¼r â€žNicht-Insiderâ€œ wÃ¤re eine frÃ¼hzeitige AufschlÃ¼sselung der AbkÃ¼rzungen â€žVSâ€œ und â€žNfDâ€œ hilfreich, die auch nicht unbedingt im Titel verwendet werden mÃ¼ssten.
77	[redacted]	1	0	0	0	1	0	1	0	0	1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	2,3	Thema DDoS Schutz ist generell nicht neu, fraglich ob das vor dem zu erwartenden Fachpublikum ein hoch relevantes Thema sein wird aber der Ansatz des Vortrages gerade kleineren Unternehmen einen Methodenkoffer an die Hand zu geben ist gut.
77	[redacted]	1	0	0	0	1	0	1	0	0	1	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0		Der Beitrag so l im Wesentlichen eine Zusammenfassung einer Literaturrecherche zum Thema DDoS sein. Daraus sollen prÃ¤ventive reaktive und nachbereitende MaÃŸnahmen abgeleitet werden. Zu allen genannten Punkten existieren bereits zahlreiche Papiere - unter anderem vom BSI. Aus dem Abstract lÃ¤sst sich nicht erkennen welchen Mehrwert das Papier bieten kann/soll.
77	[redacted]	1	0	0	0	1	0	0	1	0	1	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0		Der Beitrag gibt einen Ãœberblick Ã¼ber wohlbekannte Anti-DDOS-AnsÃ¤tze.
78	[redacted]	1	0	0	0	0	1	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	4	Der Beitrag ist nicht Ã¼bermÃ¤ÃŸig innovativ beleuchtet das Thema aber sehr gut und strukturiert. Insgesamt definitiv das rundeste Gesamtbild der Abstracts zu IT-Sicherheit und Recht.
78	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0		Das Beispiel eines vernetzten Medizinproduktes erscheint mir hier nicht sinnvoll, zumal Medizinprodukte heute schon regulatorischen Rahmenbedingungen fÃ¼r Cybersecurity unterliegen. UnabhÃ¤ngig davon werden in dem Verlauf die rechtlichen Anforderungen und die sich daraus ergebenden Pflichten fÃ¼r die Organisation thematisiert. Guter Beitrag zur ErhÃ¶hung der Awareness fÃ¼r Cybersicherheit mit Verweis auf mÃ¶g iche Rechtsfolgen
79	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	4,7	Die Inhalte im Beitrag sind valide. Es wird allerdings dringend geraten, die Aspekte der Quantenkryptographie und der Quanten Key Distribution besser zu differenzieren, da deutlich unterschiedliche Mechanismen angesprochen werden. Zudem wÃ¤re das Thema der HeranfÃ¼hrung von EndgerÃ¤ten an QKD anzusprechen, da die Quantenorientierten Terminatoren in aller Regel nicht im EndgerÃ¤t stattfinden werden kÃ¶nnen.
79	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1		Die Einreichung behandelt ein sehr aktuelles Thema mit akutem Handlungsbedarf. Empfehlungen [redacted] sind fÃ¼r die Kongressteilnehmer von groÃŸem Interesse da sich viele daran orientieren wo len oder sogar mÃ¼ssen. Die vorgestellten Empfehlungen zu Post-Quanten-Kryptografie (PQC) und Quantum-Key-Distr bution (QKD) aktua isieren und erweitern bestehende Empfehlungen des BSI. Das Thema ist gut aufbereitet und fÃ¼r ein breites Publikum zugÃ¤nglich beschrieben insbesondere werden die Konzepte PQC und QKD erklÃ¤rt. Wir erhalten eine Einordnung der Bedrohungslage durch Quantencomputer Handlungsempfehlungen um der Bedrohung jetzt entgegenzuwirken sowie einen Ausb ick was noch zu tun ist um weiterhin fundierte Sicherheitsaussagen tÃ¤tigen zu kÃ¶nnen.[redacted] Ich empfehle den Vortrag in die engere Auswahl zu nehmen.
79	[redacted]	1	0	0	1	0	0	1	0	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0		Im Beitrag wird ein demnÃ¤chst erscheinender Leitfaden zu PQ und QKD thematisiert. Vermutlich wÃ¤re es schon sinnvoll, diesen Leitfaden beim Kongress vorzustellen. So richtig klar werden die intendierte Rolle, Zielgruppe, Umfang und Detailgrad des Leitfadens aus der Beschre bung nicht; stattdessen werden offenbar einige Punkte daraus widergegeben. Diese sind zweifelsohne technisch einwandfrei, ich hÃ¤tte mir aber mehr Angaben Ã¼ber und nicht aus dem Leitfaden gewÃ¼nscht. Es wÃ¤re eine Zusammenlegung mit Beitrag [redacted] denkbar, in dem ebenfalls Empfehlungen [redacted] zu PQ vorgestellt werden. â€žDie Sicherheit â€¦ kann zusÃ¤tzliche Sicherheit liefernâ€œ klingt nach einem Zirkelschluss; â€žfÃ¼r konservative Wahlen entschiedenâ€œ kÃ¶nnte im Sinne von politischen Wahlen missverstanden werden.
80	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	3	Beitrag ist thematisch nicht sonderlich originell, bietet aufgrund seines Designs als qualitiative Fallstudie jedoch recht praxisnahe Einblicke in das IT-Sicherheitsmanagement von KMU.
80	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0		Der Vortrag wurde neutral bewertet, da er im Vergleich zu den anderen Themen im Bereich Cyber-Sicherheit bei KMUs nicht so gut abschneidet.
80	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0		Die Gliederung auf Seite 1 des Abstracs vermittelt ein klareres Bild des zu erwartenden Vortrages als der aus recht vielen A lgemeinplÃ¤tzen bestehende Textteil auf den Seiten 2 und 3. FÃ¼r die ZuhÃ¶rer aus dem KMU-Umfeld spannend wird vor allem der Praxisbericht am Ende des Vortrages sein. FÃ¼r KMU die auf einem geringen Wissensniveau abgeholt werden mÃ¼ssen sicher ein guter Einstieg in die Thematik.
81	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	3	Abstract ste lt die Absicherung von Daten als neues Paradigma in einem erweiterten nicht vertrauenswÃ¼rdigen "Cloud"-Perimeter in den Fokus. Nimmt auch VS und Cloud als AufhÃ¤nger hier insbesondere fÃ¼r Microsoft Produkte wie Sharepoint Office 365 etc. Eine Komponente mit zwei Modulen wird per API zwischen Client und Cloud geschaltet um mittels Filter und VerschlÃ¼sselungsfunktionen kontrollierbar zu machen was ein Cloud Provider sehen kann. Im Fokus steht allerdings die Ablage von Daten Ã¼ber Trusted Storage Module d.h. ein wirk iches Trusted Computing findet hier wohl nicht statt. Der Vortrag nimm [redacted] als "Beispiel". Es kann also davon ausgegangen werden dass dieses Produkt damit auch indirekt beworben wird. Wenn dies i.O. ist dann wÃ¼rden wir aufgrund der aktuellen Relevanz des Themas empfehlen dass der Beitrag angenommen wird.
81	[redacted]	1	0	0	1	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0		Beitrag ist leider stark Produktbezogen und sollte deshalb abgelehnt werden.
81	[redacted]	1	0	0	0	1	0	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0		Ein schÃ¶ner konstruktiver Beitrag und mit dem Fokus auf VS-NfD Zulassung gewiss fÃ¼r viele Teilnehmer relevant. Mir fehlt der Bezug zur aktuellen Forschung. Wenn Volltextsuche in verschlÃ¼sselten Daten gewÃ¼nscht wird, dann sollte auch homomorphic encryption diskutiert werden. Die implizite Werbung fÃ¼r ein Produkt der [redacted] ist unpassend.
82	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	3	Wesentliche neue Inhalte Ã¼ber den State of the Art hinaus sind im Beitrag nicht erkennbar. Die Bearbeitung des durchaus nicht neuen Themas ist auch etwas oberflÃ¤chlich â€“ als Beispiel sein hier das erwÃ¤hnte Nachsignieren im Kontext von eIDAS angesprochen.
82	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0		Die in der Kurzfassung vorgestellten Intelligent Composed Algorithms (ICAs) fÃ¼hren eine zusÃ¤tzliche Verwaltungsschicht von Algorithmen ein. Dies soll der einfachen Kombination und flexiblen EinfÃ¼hrung von Algorithmen dienen insbesondere vor dem gerade aktuellen Hintergrund einer notwendigen Migration zu Post-Quanten-Kryptografie. Dies ist grundsÃ¤tz ich ein wichtiger Aspekt (Stichwort Kryptoagi itÃ¤t) und dementsprechend ein sehr interessanter Ansatz. Da aber beispielsweise alle Produkte/Anwendungen die die Endnutzerzertifikate prÃ¼fen mÃ¼ssen diesen Ansatz umsetzen mÃ¼ssen erscheint dieser nur sinnvoll und praktikabel wenn er international anerkannt und standardisiert ist. Zurzeit gibt es international viele Bestrebungen kryptografische Protokolle an die PQ-Verfahren anzupassen aber gleichzeitig auch ag ler zu gestalten. Hier mÃ¼sste man sich mit einem komplett neuen Ansatz wie er im Beitrag beschrieben wird rechtzeitig in den entsprechenden Gremien aktiv einbringen und diesen bewerben. Im Beitrag wird nicht ersichtlich dass die Autor:innen diesen Aspekt im Blick haben.
82	[redacted]	1	0	0	1	0	0	1	0	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0		Der Beitrag ist fÃ¼r einen AuÃŸenstehenden sehr schwer im Detail zu verstehen, weil er von nicht aufgeschlÃ¼sselten AbkÃ¼rzungen wimmelt, unter anderem gleich im Titel [redacted] ist offenbar eine PrÃ¤gung der Autoren und wird erst auf S. 3 diskutiert (und wenn man nach [redacted] googelt kommt eine abweichende AufschlÃ¼sselung â€žIntermediate Certificate Authorityâ€œ heraus). Ich bin aus ErklÃ¤rungen nicht klug geworden, was Controlling- und Component-Algorithmen genau sein sollen und wie sich ICA von normaler Schachtelung hervorhebt. Eine Beschreibung oder eine Illustration ihrer Wirkweise (und wie sie zu den guten Eigenschaften aus dem letzten Abschnitt fÃ¼hren) wÃ¤re sinnvoll gewesen, und fÃ¼r sie wÃ¤re auch Platz vorhanden. Der Text ist durchaus holprig (â€žseien es unsere Kunden â€¦ oder direkt bei unsâ€œ).
83	[redacted]	1	0	0	1	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	3,3	Der Beitrag ist etwas konfus und versucht zu viele Themen abzudecken. Titelgebend sind die Haftungsfragen aber im Folgenden so len laut dem Abstract dann auch einzelne andere Fragen angesprochen werden - etwa die ZulÃ¤ssigkeit von Software-Untersuchungen. Das kann man machen muss es dann aber besser in das Gesamtkonstrukt einbinden. Zudem werden wichtige Begrenzungen der Untersuchungsrechte nicht gesehen sondern alleine das GeschGehG und das UrhG thematisiert. Kann man aber nehmen wenn noch BeitrÃ¤ge fehlen.
83	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0		Das Thema ist nicht sonderlich originell, allerdings berÃ¼cksichtigt der Autor die rechtlichen Entwicklungen der jÃ¼ngeren Vergangenheit (u.a. im Kaufrecht), deren Implikationen einen Mehrwert fÃ¼r das Publikum bieten kÃ¶nnten.
83	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0		Der Beitrag beschÃ¤ftigt sich mit aktuellen rechtlichen Entwicklungen bzgl. der Haftung bei mangelhafter IT-Sicherheit. Insofern wird ein sehr relevantes Thema in dem Beitrag adressiert. Er macht insgesamt einen soliden Eindruck - allerdings fÃ¤llt mir als Nicht-Jurist eine wirkliche EinschÃ¤tzung schwer. Ich denke aber, dass der Beitrag angenommen werden sollte - insbesondere auch, um die Diskussion dieses sehr wichtigen Themas weiter zu fÃ¶rdern.
84	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	3	Wertvoller Beitrag im Kontext von Multicloud-Umgebungen ZeroTrust Architektur und Umsetzung ist sehr aktuell
84	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0		Die Einreichung thematisiert (Ã¤hn ich wie Einreichung [redacted] das Thema "Zero Trust" und legt dabei den Fokus des Einsatzzweckes ausschlieÃŸlich auf Cloud-Nutzung. Die im Paper erlÃ¤uterten AnsÃ¤tze sind fachlich richtig und v.a. auch auf dem aktuellen Stand. Das Paper wirkt an einigen Stellen leicht "Buzzword"-lastig indem neben Zero Trust weitere Begr ffe als relevante AnsÃ¤tze herangezogen werden die nicht zwingend mit Zero Trust in Verbindung stehen mÃ¼ssen (bspw. 5G oder KI). Sollte ein Themenbereich (hier: Zero Trust) inhaltlich nur einmal auf dem BSI-Kongress prÃ¤sentiert werden so wird die Einreichung [redacted] im Vergleich zu dieser als grundlegenderer konzeptionellerer Ansatz (mit Fokus auf Networking) fÃ¼r die EinfÃ¼hrung in das Themengebiet gesehen da es potentiell auch Unternehmen oder BehÃ¶rde ohne Cloudnutzung adressiert.
84	[redacted]	1	0	0	1	0	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0		Der Beitrag ist im Prinzip ganz gut geschrieben. Aber was die eigene Leistung sein soll, das wird mir nicht klar. Es werden eigentlich nur Anwendungsfelder unter dem Aspekt "Zero-Trust" beleuchtet. Zudem, wenn der Author nicht weiss, wofÃ¼r NIST steht, dann habe ich Sorge um seine wirkliche Fachkenntnis.
85	[redacted]	0	1	0	1	0	0	1	0	0	1	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1,7	Wenig Neuigkeitswert, viele AllgemeinplÃ¤tze, die nicht unbedingt von Expertise und Erfahrung in dem Kontext sprechen. Ich teile nicht die EinschÃ¤tzung des Autors, dass eine Inventarisierung mit geringem Ressourceneinsatz durch den Betreiber umgesetzt werden kann und dass keine weiteren organisatorischen Anpassungen erforderlich seien, wie neue Rollen oder Prozesse. Genau das Gegenteil ist der Fall
85	[redacted]	1	0	0	1	0	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0		Das im Beitrag prÃ¤sentierte Reifegradmodell ist nicht konsistent und nicht allgemeingÃ¼ltig. Die in Stufe 3 propagierte risikobasierte Vorgehensweise lÃ¤sst Parallelen zu Consequence-driven Cyber-informed Engineering (CCE) erkennen - hat aber zunÃ¤chst keinen direkten Bezug zum Kernthema "Angriffserkennung". Aufgrund der aktuellen Marktsituation (hoher Aquisedruck seitens der Hersteller) sollte der Kongress nicht als Marketing-Plattform missbraucht werden.
85	[redacted]	0	1	0	1	0	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0		Keine neuen Aspekte, eher AllgemeinplÃ¤tze. Die Diskussion Ã¼ber AufwÃ¤nde und Risikomanagement lÃ¤sst fehlende Praxiserfahrung vermuten.
86	[redacted]	1	0	0	1	0	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	2,3	Insgesamt ist das Ziel der Beitrags nicht klar, die Autoren sind im Abstract eher thematisch sprunghaft
86	[redacted]	0	1	0	1	0	0	1	0	0	1	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0		Generischer Beitrag, keine innovativen AnsÃ¤tze, wiederholt nur altbekannte Problemstellungen und LÃ¶sungen.
86	[redacted]	1	0	0	1	0	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0		- Motivation/Struktur: Bedrohung GefÃ¤hrdung Risiko und SchutzmaÃŸnahme fÃ¼r Domains gehen durcheinander. - Inhalt: Sowohl konkrete GefÃ¤hrdungen (z.B. beobachtete VorfÃ¤lle) als auch konkrete MaÃŸnahmen fehlen. Im Detail: - Welche konkreten Szenarien
87	[redacted]	0	1	0	0	1	0	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	3	Die Autoren scheinen sich selbst in den Referenzen genannt zu haben der Beitrag wÃ¤re also nicht anonym. Das Abstract erweckt Eindruck als hÃ¤tten die Autoren lediglich ein bekanntes Thema aufgegriffen und in einen anderen Kontext gestellt. Es handelt sich also um keinen neuen Angriffsvektor da lediglich der bekannte Angriffsvektor Ã¼ber SSF im Kontext von WiFi Netzwerken herausgestellt wird. Es handelt sich eher um eine Vorbereitungshandlung fÃ¼r einen Angriff. Um den Angriff durchfÃ¼hren zu kÃ¶nnen muss einem Angre fer das nutzerspezifisches Muster des Zielnutzers bereits bekannt sein was am ehesten vorstellbar ist wenn der Rechner des Opfers bereits kompromittiert ist was den Angriff Ã¼berflÃ¼ssig macht. Alternativ kommen andere Que len wie z.B. Ã¶ffentlich zugÃ¤ng iche Rechner oder ein kompromittiertes ZweitgerÃ¤t des Nutzers in Betracht. Es ist natÃ¼r ich mÃ¶glich dass in der vollstÃ¤ndigen Arbeit noch weitere Deta ls vorhanden sind die den Angriffsvektor interessanter machen.
87	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0		Der Beitrag thematisiert das Problem der Nutzeridentifikation an Hand von Verkehrsmustern, die im Zuge der DatenÃ¼bermittlung im Rahmen von SuchvorschlÃ¤gen bei Suchmaschinen entstehen. Dabei wird gezeigt, dass auch bei verschlÃ¼sselter Kommunikation (WPA2, VPN) erfolgreich Angriffe durchgefÃ¼hrt werden kÃ¶nnen. Es wird ein Browser-Plugin vorgestellt, dass die Erkennungswahrscheinlichkeit zumindest senkt. Der Beitrag baut auf bekannten Erkenntnisse auf und bestÃ¤tigt diese insofern. Er macht einen soliden Eindruck und kann angenommen werden, falls Platz ist.
87	[redacted]	1	0	0	0	1	0	0	1	0	1	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0		Es ist nicht ganz klar wie relevant das Problem in der Praxis ist. "Padd zeigt sich als sehr nutzerfreundliche und effektive GegenmaÃŸnahme." woher wissen die Autoren das es nutzerfreundlich ist?
88	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	4	Der Beitrag liefert eine Ãœbersicht Ã¼ber momentan laufende eID Projekte und Massnahmen. Hierbei wird insbesondere auch auf die mobile Umsetzung der eID eingangen. Als Ãœbersichtsartikel wird die Aufnahme in das Programm empfohlen.
88	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0		Das Abstract beschÃ¤ftigt sich mit einer aktuellen Entwicklung in der Politik und auch auf europÃ¤ischer Ebene. Zum Zeitpunkt des Kongresses besteht durchaus die MÃ¶glichkeit dass sich Teile im Hinblick Smart eID und ID Wallet bereits aufgelÃ¶st haben die Frage der Aktua itÃ¤t ist also zumindest in dem Bereich nicht klar mÃ¶glicherweise veraltet. Die BerÃ¼cksichtigung der EU Arbeitsgruppen bleibt wiederum voraussichtlich auch noch das ganze Jahr 2022 Ã¼ber aktuell ist aber noch in Entstehung und daher ist eine Idee zur Integration eines Konzeptes welches mÃ¶glicherweise ein halbes Jahr spÃ¤ter schon anders aussieht vielleicht nicht zielfÃ¼hrend. Leichte Anpassungen kÃ¶nnten daher fÃ¼r die AktualitÃ¤t spÃ¤ter notwendig sein abhÃ¤ngig auch von politischen Entscheidungen die schwer vorherzusagen sind.
88	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0		Der Artikel gehÃ¶rt zu den 25% Besten und kann angenommen werden. Es werden verschiedene Arten der digitalen IdentitÃ¤t sehr verstÃ¤ndlich erklÃ¤rt und ein Ausblick auf eine starke eID-Made in Germany gegeben.
89	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1		Beitrag stellt die Technische Basis fÃ¼r die Nutzung des digitalen Personalausweises auf dem Smartphone da. Wichtiges Thema wenn ein Massenrollout mit unterschiedlichten Nutzungsszenarien erreicht werden soll.
89	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1		Der Beitrag schildert den Einsatz des TSMS im Kontext der laufenden eID Initiativen des Bundes (Smart eID etc.) Es wird insbesondere auf TR KonformitÃ¤t und die umgesetzte Architektur eingegangen. Der Beitrag wird zur Aufnahme empfohlen, eventuell kann eine Zusammenlegung mit [redacted] erfolgen?

89	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	1	5	Der Beitrag geht auf das Trusted Service Management System (TSMS) ein welches in Optimos2.0 erprobt und derzeit mit einer ersten Anwendung "Smart-eID" im Auftrag des Bundes und unter Begleitung durch BMI/BSI umgesetzt wird. Hier wird das System aus sich des Trusted Service Managers einer zentralen Rolle im TSMS betrachtet. Neben Systemkonzept und Bedeutung fÃ¼r die Smart-eID soll auch auf den Nutzen fÃ¼r weitere Anwendungen eingegangen werden. Durch den Bezug zur Smart-eID und weitere AnwendungsfÃ¤lle ist das Thema grundsÃ¤tzlich fÃ¼r ein relativ breites Publikum interessant. Das technische System selbst ist zwar eher fÃ¼r einen eingeschrÃ¤nkten Fachkreis relevant a lerdings ist hier die Ã¶ffentliche Informationslage etwas mager was den Beitrag wertvoll macht. Daher so lte der Beitrag "unbedingt" angenommen werden.
90	[redacted]	0	1	0	0	1	0	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	2,3	Der Beitrag ist nicht anonymisiert der Autor ist den PDF-Eigenschaften hinterlegt. Inhalt ich ist die grundsÃ¤tzliche Idee an dem Thema interessant aber leider sehr schlecht umgesetzt. Die Analogien zwischen StraÃŸenverkehr und Informationssicherheit sind oberflÃ¤chlich betrachtet erst mal nett aber fÃ¼r ein Paper fÃ¼r den IT-Sicherheitskongress dass ausschlieÃŸlich auf oberflÃ¤chliche Analogien aufbaut und keinen Schluss daraus zieht oder eine Erkenntnis ist es zu dÃ¼nn. Fachlich wird an vielen Stellen deut ich dass der Autor nicht zwischen safety und security unterscheidet wodurch diese Analogien schlichtweg nicht haltbar sind. Andere Vergleiche sind sehr fragwÃ¼rdig so wird eine Fahrschule mit einem Awareness-Training gleichgesetzt hier ist schon ein deutlicher Unterschied.
90	[redacted]	1	0	0	0	1	0	0	1	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0		**Beitrag zeigt grundsÃ¤tzlich wichtiges Thema auf. Jedoch wird das Thema IT-Sicherheit in der Wirtschaft sehr unterkomplex behandelt.**
90	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0		**Die Kombination ist interessant verpackt, der Fokus auf KMU (eigentlich geht es nur um Unternehmen) ist natÃ¼rlich zu kurz gegriffen, warum so lte ein TÃœV fÃ¼r Autos bei den BehÃ¶rden nicht nÃ¶tig sein, oder brauchen Angestellt*e im Ã¶ffentlichen Dienst keinen FÃ¼hrerschein??? Also interessante Analogie, bisschen mehr generalisieren (und die darin liegenden Probleme auch lÃ¶sen/ansprechen), aber nur ins Programm, wenn es keine besseren gibt**
91	[redacted]	0	1	0	0	0	1	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	3,5	Das Dokument ste lt gut dar dass aktuell kein datenschutzkonformer Einsatz von Microsoft 365 mÃ¶g ich ist der Anwenderwunsch aber hoch ist die SoftwarelÃ¶sung einzusetzen. Um dem BedÃ¼rfnis der Anwender als auch dem des Datenschutzes gerecht zu werden skizziert das Dokument eine techn. LÃ¶sungsmÃ¶glichkeit von [redacted] . Die Grundidee sieht vor dass der Client nicht mehr direkt mit der Cloud von Microsoft kommuniziert sondern die Daten vorher an ein Security Gateway umgeleitet werden. Hier werden die Daten im Sinne des Datenschutzes gefiltert die Originaldaten verschlÃ¼sselt und in einem deutschen/europÃ¤ischen Rechenzentrum gespeichert. FÃ¼r eine fachliche Bewertung reicht das Abstract nicht aus. Es bleiben Fragen offen wie: Wieso werden Daten zusÃ¤tzlich in der Microsoft Cloud abgelegt? Wieso kann innerhalb von verschlÃ¼sselten Dokumenten eine Volltextsuche stattfinden? Wer kontrolliert und aktualisiert den fest definierten Datenverkehr der an das Security Gateway umgelenkt wird?
91	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0		**Beitrag beleuchtet ein aktuelles Thema und zeigt einen LÃ¶sungsweg auf. Sollte aufgenommen werden.**
93	[redacted]	1	0	0	1	0	0	1	0	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	2,3	Der Beitrag wiederholt die Bedrohungslage bleibt aber eine Darstellung der LÃ¶sung im Wesentlichen schuldig. Einzig eine "zentrale Datenhaltung" wird als MaÃŸnahme vorgeschlagen diese ist aber nicht wirklich erlÃ¤utert und auch nicht in Relation zu Bedrohungsszenarien diskutiert (Ransomware?). Der Problemaufriss ist richtig aber im Fa le der Annahme des Papers mÃ¼sste bei der LÃ¶sung noch nachgelegt werden.
93	[redacted]	1	0	0	0	0	1	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0		**Laut PDF-Titel will der:die Autor:in durch [redacted] Im Abstract kommt dieser Gedanke aber erst ganz am Ende rÃ¼ber. Auch die BegrÃ¼ndung ist schwierig, denn lediglich die Verlagerung von Daten in die Cloud schÃ¼tzt nicht, wie der:die Autor:in argumentiert, vor Ransomware, zum Beispiel. Es ist unklar, ob dieser Beitrag einen innovativen oder intellektuellen Mehrwert hat, da er das offensichtliche beschreibt und eine etwas holzschnittartige LÃ¶sung vorschlÃ¤gt.**
93	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0		**Der Beitrag sollte abgelehnt werde, da er zwar aktuell ist, aber keinen neuen Ideen prÃ¤sentiert.**
94	[redacted]	1	0	0	1	0	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	3	**Abstrakt ist sehr Kurz und oberflÃ¤ch ich, das Thema ansich ist aber wichtig und unterstÃ¼tz einen Grundpfeiler unserer Demokratie - die Wahlen - im digitalen Raum.**
94	[redacted]	1	0	0	1	0	0	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0		**Der Abstrakt ist sehr kann knapp gehalten. Der Beitrag hat durchaus Relevanz, aber aber aus meiner Sicht nicht fÃ¼r die Zielgruppe des Kongresses.**
94	[redacted]	0	1	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0		Das eingereichte Abstract mit dem Tite [redacted] gibt leider in nur ca. einer halben Din A4-Seite einen Ãœberblick Ã¼ber den Beitrag. Hier ist jedoch zu sehen dass sich die Autorinnen und Autoren mit der Themat k beschÃ¤ftigt haben. Leider wird durch das kurze Abstract nicht 100%ig klar in welche Richtung der Beitrag ausgerichtet ist. Daher ein neutrales Votum.
95	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	4,3	**Der Beitrag schildert Anforderungen und Vorgehensmodelle zur Umsetzung und zum Test von kryptoagilen Mechanismen in SW Systemen. Insbesondere der Fokus auf Testmethodologien und Best Practices liefert einen wichtigen Beitrag in der aktuellen Diskussion zu KryptoagilitÃ¤t. Der Beitrag wird daher zur Annahme empfohlen.**
95	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0		The submission proposes a survey of research regarding crypto-agility i.e. the ab lity update and exchange cryptographic components of larger IT-systems. The survey finds that there is no consistent definition of crypto-agi ity as there are issues and inconsistencies in the understanding of crypto-agi ity between the reviewed research articles. Therefore they propose a broader notion and categorization of the desired functionalities. The survey highlights research questions and directions however the open nature of the overview leads to a less focussed core message. Since the survey appears to present more questions and research directions than answers and takeaways it is unclear whether this is an ideal venue for this submission.
95	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1		**Der Beitrag gibt einen sehr brauchbaren Ãœberb ick Ã¼ber das Thema der ag len Kryptographie und spart auch die Probleme nicht aus. Umfassende Referenzen ordnen die Aussagen auch gut in andere Arbeiten im betroffenen Umfeld ein.**
96	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	4,3	**Der Beitrag schildert eine Umsetzung eines zulassungsfÃ¤higem Mikrohypervisor, der in der Folge zur Umsetzung einer zulassungsfÃ¤higen vertrauenswÃ¼rdigen Netzwerkanbindung im Cloud Kontext eingesetzt werden kann.Verschiedene virtuelle Netzwerktopologien werden vorgestellt und deren Vor-und Nachteile diskutiert. Im Kontext der "Cloudifizierung" von VS Infrastrukturen ist dies ein wertvoller Diskussionsbeitrag. Der Beitrag wird zur Annahme empfohlen. Die Referenzierung von konkreten Produkten sollte a lerdings mÃ¶glichst unterbleiben.**
96	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0		**Der Beitrag stellt zu stark auf ein Produkt [redacted] ab. Gleichzeitig wird eine inhaltliche Abgrenzung zu anderen vergleichbaren Produkten nicht vorgenommen und damit ist die Hilfestellung im Entscheidungsprozess fÃ¼r den angesprochenen behÃ¶rdlichen Bereich kaum gegeben.**
96	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1		Im Hinblick auf die zahlreichen Cloud-Projekte in der Bundesverwaltung in denen eingestuften Informationen verarbeitet und gespeichert werden sollen bildet der Beitrag einen wichtigen Ansatz beim Aufbau der notwendigen Cloud-Infrastrukturen.
97	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	3,3	**KomplexitÃ¤t in Netzen ist bereits jetzt schon ein kritischer Faktor, hier kann der Ansatz helfen, wieder VerstÃ¤ndlichkeit in die Netze zu bekommen, um Besonderheiten zu erkenen.**
97	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0		Der Abstract bleibt an manchen Stellen vage. Es bleiben Zweifel ob der Vorschlag bereits in der Praxis umgesetzt wurde oder erfolgreich umgesetzt werden kann. Bei erfolgreicher Umsetzung handelt es sich aber um ein interessantes Ergebnis.
97	[redacted]	1	0	0	1	0	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0		**Der Beitrag thematisiert die KomplexitÃ¤t der Konfiguration von Firewall-Systemen/Mikrosegmentierung und schlÃ¤gt Maschinelles Lernen zur KomplexitÃ¤tsreduktion vor. Konkret werden Cluster-Verfahren zur Abstraktion (Zusammenfassung von Einzelelementen zu Clustern) betrachtet. Es wird nicht klar, ob nur die Bedienbarkeit verbessert oder auch die Sicherheit erhalten/verbessert wird. Auswirkungen von Fehlern in der ML werden nicht diskutiert. Damit fehlt eine Diskussion der eigentlich spannenden Fragen zum Thema.**
98	[redacted]	1	0	1	0	0	0	1	0	1	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	2,7	**Mangelnde Strukturierung des Beitrags lÃ¤sst vermuten, dass das Thema auf dem BSI-Kongress nicht sonderlich verstÃ¤ndlich prÃ¤sentiert werden wÃ¼rde.**
98	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1		Der Beitrag betrachtet aktuelle Herausforderungen der Automobil-Lieferkette. Er diskutiert LÃ¶sungsstrategien die fÃ¼r KMU bedeutend sind. FÃ¼r das BSI ist diese Betrachtung wichtig um die Digitalisierung der Lieferkette praxisnah mitgestalten zu kÃ¶nnen.
98	[redacted]	0	1	0	0	1	0	0	1	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0		**Werbebeitrag fÃ¼r Beratungsunternehmer; frehlende AnonymitÃ¤t; wiederholt grob fehlerhafte Zahlen genannt; keinerlei neue Aspekte.**
99	[redacted]	1	0	0	0	1	0	0	1	0	1	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	2,3	Wie im Beitrag genannt ist die Cold Boot Attacke seit 2008 bekannt. Als Neuerung wird bei dem vorgefÃ¼hrten Angriff die Firmware manipuliert das Ãœberschreiben des Speichers verhindert und so der Angriff wieder ermÃ¶glicht. Durch geeignete GrundschutzmaÃŸnahmen wird dies jedoch bereits extrem erschwert. Bedingt durch die starke individuelle HardwareabhÃ¤ngigkeit dÃ¼rfte dieser Angriff in der Praxis - wie bisher auch - keine groÃŸe Bedeutung haben.
99	[redacted]	1	0	0	0	1	0	0	1	0	1	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0		**Kein Neuigkeitswert erkennbar.**
99	[redacted]	1	0	0	0	1	0	0	1	0	1	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0		**Keine wirklich neue Erkenntnis. Eher auf dem Niveau eines Seminars im Studium. Sehr begrenzte Relevanz fÃ¼r die heutige Praxis.**
100	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	4,3	Getrieben aus den populÃ¤ren Supply-Chain Attacks in 2021 schlÃ¤gt das Paper vor einen Hypervisor nach Micro-Kernel Ansatz in der Programmiersprache RUST zu implementieren. Durch die Typsicherheit von RUST kann eine formale Verifikation des Hypervisors erheblich vereinfacht werden da die teils extrem komplexe Modellierung des Speicherverhaltens entfallen kann. Gleichzeitig schlagen die Autoren reprozierbare Software Builds sowie synchrones Testen neuen Codes vor um Vertrauen und Transparenz in den gesamten Entwicklungsprozess zu etablieren bzw. weiter zu steigern. Virtualisierung ist eine wichtige Basistechnik. Ein formal verifizierbarer Hypervisor wÃ¼rde groÃŸes Vertrauen in die Isolationseigenschaft des Hypervisors herste len wodurch verschiedene Anwendungen beweisbar voneinander isoliert werden kÃ¶nnten. Ein sehr transparenter Entwicklungsprozess kÃ¶nnte auch sinnvoll und Vorbild fÃ¼r andere DomÃ¤nen sein.
100	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0		**Interessanter Vorschlag fÃ¼r einen Hypervisor in RUST zur Vereinfachung formaler VerifikationsaufwÃ¤nde.**
100	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0		**Vor dem Hintergrund aktueller Software Supply Chain Angriffe thematisiert der Beitrag Ansatzpunkte in der Softwareentwicklung, die zu besserer VertrauenswÃ¼rdigkeit von Software fÃ¼hren kÃ¶nnen, nÃ¤mlich u.a. Formale Verifikation, Memory-Safe Programmiersprachen (Rust)... In der Softwareentwicklung liegt die Ursache vieler Sicherheitsprobleme; der Beitrag diskutiert aktuelle Vorgehensweisen zur Verbesserung - was leider zu selten passiert. Echte Neuheiten sind dem Beitrag aber nicht zu entnehmen.**
101	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	2,7	**Security-Metriken auch auf die FÃ¤higkeiten eiens SOC zu beziehen, ist nicht wirklich neu. Da es aber fÃ¼r einige Organisationen/Unternehmen ein AnstoÃŸ zur EinfÃ¼hrung von Metriken sein kann, ist das Gesamturteil zumindest neutral.**
101	[redacted]	0	1	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0		Der Beitrag wurde nicht anonymisiert eingereicht und entspricht somit nicht den o.g. formalen Kriterien. Der Beitrag besteht aus 12 Zeilen einfÃ¼hrendem Text und ca. 1 5 Seiten Gliederungspunkten. Somit ist der im wesentlichen aus Gliederungspunkten bestehende Beitrag naturgemÃ¤ÃŸ Ã¼bersichtlich und gut geg iedert. Ebenfalls naturgemÃ¤ÃŸ sind bei dieser Form des Beitrags keine "besonderen handwerklichen Fehler" zu erwarten. Eine inhaltliche Bewertung ist bei dieser Form nur sehr eingeschrÃ¤nkt mÃ¶glich. Dazu hÃ¤tte es jeweils einer genaueren ErlÃ¤uterung des geplanten Inhalts zum G iederungspunkt bedurft was auf 3 Seiten durchaus mÃ¶glich gewesen wÃ¤re. Ausgehend von den aufgefÃ¼hrten Gliederungspunkten und den wenigen zusÃ¤tz ichen Informationen kÃ¶nnte der Beitrag aber prinzipiell interessant sein.
101	[redacted]	0	1	0	1	0	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0		**Reifegradmessung und -steigerung ist immer eine gute Idee. Hier wird in Stichpunkten ein Beitrag skizziert, der diese Botschaft fÃ¼r SOCs aufgreift. Das Thema soll im Beitrag motiviert werden und verschiedene Reifegradmodelle vorgestellt werden. Ob und wie vergleich diese sind bleibt unklar. Bei dem Beitrag lÃ¤uft es vermutlich auf einen Ãœberblick zum Stand von Verfahren zur Reifegraderhebung hinaus. Es bleibt unklar, welchen Wert der Beitrag fÃ¼r den Leser haben kann.**
102	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	3,7	**Beitrag fokussiert nicht auf die 5G Technik als solches aber auf eine Anwendung der 5G am Beispiel einer kritischen Infrastruktur (Gesundheitswesen) mit sehr kritischen Daten (Patientendaten).**
102	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0		**Gute EinfÃ¼hrung in das Thema und Verbindung mit 5G, hoffentlich gepaart mit einer guten Darstellung anhand eines Beispielkrankenhauses**
102	[redacted]	1	0	0	0	0	1	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0		**Thema nicht neu, aber noch aktuell. Beitrag kann angenommen werden.**
103	[redacted]	1	0	0	0	1	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	2,3	**Der Beitrag versucht einen Einsatz einer Selbstauskunft auf Basis des Personalausweises darzustellen. Die Einsatzszenarien und der Nutzen des Personalausweises im Kontext der dargeste lten AnwendungsfÃ¤lle ist allerdings unklar. Der Beitrag sollter nicht aufgenommen werden.**
103	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0		Der Artikel merkt korrekterweise an dass mit Verlassen der Daten aus der Selbstauskunft vom LesegerÃ¤t/Smartphone kein Vertrauen in diese Daten mehr bestehen kann. Was mit diesen Daten passiert wird im Abstract nicht erklÃ¤rt wie diese gegen VerfÃ¤lschung oder Kopieren geschÃ¼tzt werden ebenfalls nicht. Das Verfahren hat daher die MÃ¶glichkeit dem Anwender ein falsches SicherheitsgefÃ¼hl zu vermitteln und dann insbesondere auch keine grÃ¶ÃŸere Sicherheit zu bringen. Den Mehrwert sehe ich persÃ¶nlich daher eher als gering an. Zum Punkt der Origina itÃ¤t ist anzumerken dass das beschriebene Verfahren durchaus neu ist und ein eine gewisse OriginalitÃ¤t mitbringt aber voraussichtlich bessere MÃ¶glichkeiten fÃ¼r die Umsetzung existieren wÃ¼rden.
103	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0		**Beitrag beschreibt ein altes Problem.**
104	[redacted]	1	0	0	1	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	2,7	(I) Das Paper liefert zwar eine Gliederung des Vortrags hÃ¤lt diese in sich selbst jedoch nicht ein sondern besteht im Wesent ichen aus einem langen Textblock. Es ist nicht zu erkennen wie die Gliederungspunkte im Vortrag umgesetzt werden. (II) OriginalitÃ¤t/AktualitÃ¤t Das Vortragsthema (IT-GefÃ¤hrdungslage der dt. KrankenhÃ¤user) ist zwar aktue l jedoch nicht (mehr) (besonders) origine l da bereits mehrfach zu vielen Gelegenheiten kolportiert. (III) AblehnungsgrÃ¼nde Die Herangehensweise der Alpha Str ke Labs birgt so wie das BSI sie verstanden hat das Risiko von False-Positives in den gesammelten Daten sodass die Ableitung einer grundsÃ¤tzlichen GefÃ¤hrdungslage aus Sicht des BSI nicht zweifelsfrei zulÃ¤ssig ist. Insofern wÃ¼rde der Vortrag ein verfÃ¤lschtes/Ã¼berzeichnetes B ld der tatsÃ¤chlichen Lage zeichnen welches insbes. in einer mÃ¶glichen medialen Aufbereitung im Rahmen der Berichtserstattung zum Kongress zu einer Fehlinformation der Ã–ffentlichkeit fÃ¼hren kann.
104	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0		**Update eines Ã¤lteren Talks zur Sicherheitslage im deutschen Krankenhausbereich. Sinnvoll.**
104	[redacted]	0	1	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0		**Ein sehr spannendes Thema und gute Methode, aber: 1. der Beitrag ist das Gegenteil von anonymisiert 2. die Einreichenden haben sich absolut keine MÃ¼he bei dem Abstract gegeben, denn der Beitrag besteht fast nur aus Zitaten und Grafiken aus der Studie und ist nicht anonymisiert.**

105	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	3,3	Das Thema Sensibilisierung von FÃ¼hrungskrÃ¤ften fÃ¼r IT-Sicherheit ist nicht neue. Auch eine Studie die auf 17 Interviews basiert ich nicht sehr reprÃ¤sentativ. Die 10 vorgeschlagen Security-Themengebiete findet mach auch im IT-Grundschutz-Baustein. Der Bezug zur Rolle der FÃ¼hrungskrÃ¤fte allgemein und der Ro le der FÃ¼hrungskrÃ¤fte in der sicheren Softwareentwicklung wird nicht deutlich. Interessant wÃ¤ren die Inhalte der 2-tÃ¤gigen Schulung fÃ¼r FÃ¼hrungskrÃ¤fte im Themenbereich Softwareentwicklung.
105	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0		**Die Einreichung bemÃ¼ht sich um den BrÃ¼ckenschlag zwischen "Cybersicherheit ist FÃ¼hrungsaufgabe" und sicherer Softwareentwicklung. Dabei wird viel Bekanntes reproduziert und wenig neue Gedanken aufgeworfen, die dem zu untersuchenden BrÃ¼ckenschlag gerecht werden. Die MaÃŸnahmen werden zwar gut zusammengefasst, sind aber hinlÃ¤nglich bekannt. Tendenz auf Basis des Abstracts: eher nicht vorstellungswÃ¼rdig.**
105	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0		**Der Beitrag stellt eine Interviewstudie mit 17 FÃ¼hrungskrÃ¤ften (FK) und Product Owner (PO) vor zum Thema "Sichere Softwareentwicklung". Das Fazit der Studie ist, dass die FK und PO unzureichende Kompetenzen in diesem Bereich besitzen, und die erforderlichen MaÃŸnahmen nicht implementiert werden. Die Autoren stellen eine allgemein Checkliste vor, die sie zur Verbesserung der Lage vorschlagen. Diese Liste wÃ¤re meiner Meinung nach fÃ¼r Leute mit niedrigeren IT-Sicherheitkompetenzen nicht verstÃ¤ndlich. Die Autoren versprechen aber, dass sie auch einen 2-TÃ¤gigen Workshop entwickelt haben, um diese Kompetenzen zu vermitteln. Die vorgestellten Ergebnisse sind in der internationalen Forshcung bekannt, passen jedoch ganz gut zum Kongressthema. Ich denke, dass sie fÃ¼r die Kongressbesucher interessant sein kÃ¶nnten. leider wurden die Empfehlungen des Beitrags nicht evaluiert, so dass ihre EffektivitÃ¤t unklar ist.**
106	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	4	**Sicherheit von Lieferketten und das Vertrauen in Liefer-- und Produktionsketten wird immer wichtiger. Der Vortrag versucht dies zu operationalisieren. Leider wird im Abstract eher nur die Problembeschreibung dokumentiert, die versprochenen LÃ¶sungsansÃ¤tze waren zumindest in der Kurzfassung nicht aufgefÃ¼hrt. In der Hoffnung, dass dies in der Langfassung erfolgt, kann der Vortrag angenommen werden.**
106	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0		Der Beitrag stellt die Problematik mit Lieferketten in Bezug auf Digitale SouverÃ¤nitÃ¤t gut und praxisorientiert dar. Es wird ein kurzer Einblick in mÃ¶g iche LÃ¶sungsansÃ¤tze gegeben und weist auf weitere Probleme der Thematik in der Langfassung hin. Generell sind BeitrÃ¤ge zur Digitalen SouverÃ¤nitÃ¤t ein aktuelles und wichtiges Thema.
106	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0		**Wichtiges Thema und gute Herangehensweise.**
107	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	3	Das Thema hat durch seinen Sicherheitsbezug (Anwendungsgebiet TI) eine Relevanz fÃ¼r den BSI Kongress. Durch die Entwicklung in einer Docker Umgebung wird eine ÃœberprÃ¼fung durch Dritte ermÃ¶glicht. Die verwendeten Methoden im Bereich NLP sind alt bekannt und eine gute Wahl fÃ¼r eine erste Auseinandersetzung mit dem Thema im Rahmen einer Bachelorarbeit. Aktuellere Methoden wie z.B. Word Embeddings werden nicht diskutiert. Zur Bewertung der Verfahren nutzen die Autoren lediglich einen ML Classifier. Durch diese EinschrÃ¤nkung entgehen den Autoren potentiell wertvolle Erkenntnisse zur QualitÃ¤t der ausgewÃ¤hlten Merkmale. Die Ergebnisse zeigen dass die Arbeit von TI Analysten durch ML und NLP vereinfacht werden kann. Allerdings gehen bei dem entwickelten Ansatz mÃ¶glicherweise wichtige Informationen verloren die als nicht relevant eingestuft werden und somit nicht ihren Weg bis zum Analysten schaffen. Aufgrund dieser recht ausgeglichenen Beurteilung ist mein Votum zur VerÃ¶ffentlichung neutral.
107	[redacted]	1	0	0	1	0	0	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0		**Analyse von Nachrichtenartikeln fÃ¼r Threat Intelligence ist wenig zielfÃ¼hrend, da Trends eher spÃ¤t sichtbar werden und eine Gewichtung anhand der Anzahl von Artikeln durch die Mechanismen der Medienproduktion nicht aussagekrÃ¤ftig ist.**
107	[redacted]	1	0	0	0	1	0	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0		**Der Beitrag ist nicht Ã¼bermÃ¤ÃŸig klar geschrieben. Auch in Hinsicht auf die technische Beschreibung habe ich einige Bedenken (Beispiel: was ist das MaÃŸ tf-idf und wofÃ¼r steht es?). Aber fÃ¼r einen [redacted] sehr gut. Kandidat fÃ¼ [redacted]**
108	[redacted]	0	1	0	0	0	1	1	0	1	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	2,25	Der Beitrag lÃ¤sst die Urheber erkennen (Podcast [redacted]). Eher keine Empfehlung als Paper anzunehmen wohl aber zur BerÃ¼cksichtigung im Kongress insgesamt (siehe Vorschlag im Paper selbst). Das kÃ¶nnte eine gute Darstellung des Darknet werden.
108	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0		Die Autorinnen schlagen ihre virtuelle Reise durch das Darknet se bst als â€žShowactâ€œ fÃ¼r zwischendurch vor. In ihrem Beitrag wo len sie zugÃ¤ng ich fÃ¼r Laien und andere Akteure die sich vor dem Darknet scheuen als dramaturgisch aufbereitete Live-Demonstration die Ambivalenz des Darknet zwischen "Dystopie und Demokratie" veranschaulichen. Die Autorinnen sind [redacted] die den prÃ¤mierten Podcast [redacted] mit dem Themenschwerpunkt Cybercrime betreiben. (Die Anonymisierung des Beitrags wird durch die Namensnennung teils aufgehoben.) Durch die Einreichung wird kein Wissensbeitrag vorgeschlagen sondern es wird Ã¼ber ein innovatives und ansprechendes Konzept ein Thema mit BerÃ¼hrungsÃ¤ngsten anschaulich und differenziert nÃ¤hergebracht. Die OriginalitÃ¤t des Beitrages ist durch die dramaturgische Aufbereitung der begrÃ¼ndet. Aus Verbrauchersicht ist eine AufklÃ¤rung Ã¼ber des Darknets interessant. Der Beitrag selbst zielt jedoch nicht primÃ¤r auf Verbraucher:innen ab. Insgesamt macht der Beitrag Sinn sofern das Thema als solch eine Showeinlage ins Programm passt.
108	[redacted]	0	1	0	0	1	0	0	1	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0		**Kein inhaltlich origneller Beitrag, quasi eine "gefÃ¼hrte Tour" durch das "Darknet". Fachliche Relevanz nicht erkennbar.**
108	[redacted]	0	1	1	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0		**Anforderungen sind nicht erfÃ¼llt, klingt nach Werbeveranstaltung**
109	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	4,5	**Beitrag betrachtet die 5G Sicherheit sehr akademisch, will auch einen Ausblick auf die notwendigen Lehren fÃ¼r die 6G Standardisierung geben, insofern trotz sehr theoretischem Ansatz sehr wertvoll und Zukunftsweisend.**
109	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0		**Hoch, sehr gute Darstellung der unterschiedlichen Angriffsstrategien, den Bedrohungen und daraus abgeleiteten LÃ¶sungsansÃ¤tzen**
111	[redacted]	1	0	0	0	1	0	0	1	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	2,3	Der Beitrag stellt die bestehenden Herausforderungen und LÃ¶sungen im Kontext der Passwortverwaltung und -verwendung fachlich korrekt dar. Ich habe jedoch keine neuen AnsÃ¤tze oder Ideen gesehen. Es bleibt bei der Beschre bung des seit Jahren nicht wesentlich verÃ¤nderten Standes. Der Titel verspricht zwar eine AuflÃ¶sung der aktuellen Schwierigkeiten und entsprechende Entwicklung auf dem Gebiet es ist im Abstract aber nicht erkennbar dass der Beitrag dieses Versprechen einlÃ¶sen wÃ¼rde. Ein echter KRITIS-Bezug besteht nur insofern dass auf alte und schwer ablÃ¶sbare ICS-LÃ¶sungen verwiesen wird die hÃ¤ufig ausschlieÃŸ ich passwortbasierte Authentikation anbieten. Der Beitrag ist insofern sicherlich nicht "peinlich" bringt aber auch kaum Mehrwert. Sollten nach Abschluss der Bewertungsrunden Bedarf fÃ¼r weitere BeitrÃ¤ge bestehen kÃ¶nnte er aber ein Kandidat sein.
111	[redacted]	1	0	0	0	1	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0		**Beitrag erlÃ¤utert ein andauerndes Risiko, welches ausfÃ¼hrlich geschildert wird. Leider wird der LÃ¶sungsansatz in dieser Kurzfassung nicht deutlich und die InnovativitÃ¤t kann kaum beurte lt werden.**
111	[redacted]	1	0	1	0	0	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0		**Der beitrag argumentiert zuerst auf zwei Seiten, warum PasswÃ¶rter unsicher und nicht nutzerfreundlich sind, und wie sie angegriffen werden. Dann wird folgendes System angesprochen (Zitat): [redacted] So ein System wÃ¤re in der tat wÃ¼nschenswert und sehr relevant. Leider wird im Beitrag Ã¼berhaupt nicht erklÃ¤rt, wie das System funktioniert. Der Informationsgehalt dieser Einreichung ist deswegen leider sehr nah an Null.**
112	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	3,7	**Mit der Entwicklung eines speziell auf KMU zugeschnittenen Security-Reifegradmodells leistet die Untersuchung einen innovativen Beitrag zur Frage, wie die IT-Sicherheit von KMU verbessert werden kann.**
112	[redacted]	1	0	0	0	0	1	1	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0		**Der Artikel wurde neutral bewertet, da kein Bezug zur Praxis aufgefÃ¼hrt wurde.**
112	[redacted]	1	0	0	0	1	0	1	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0		Ein Beitrag der eines der groÃŸen Probleme aus dem KMU-Umfeld aufgreift. WÃ¼nschenswert wÃ¤re wenn im Vortrag auch eine BrÃ¼cke in die Praxis geschlagen wÃ¼rde da dies erfahrungsgemÃ¤ÃŸ gerade bei KMU fÃ¼r die "Management Attention" wesentlich ist.