digiVolution
Prepare for the next

dVNews

Les billets de digiVolution / digiVolution's Newsletters
[28.08.2024 – Édition / Ausgabe Nr. 104]

Sorry for the BSoD?

Chers Lectrices et Lecteurs,

Nous avons le plaisir de vous adresser la 104ème dVNews (13-2024) et sa sélection d'articles et liens. Vous nous avez manqué… mais nous avions aussi besoin de vacances et les JO de Paris nous ont beaucoup occupés.

La tech sera un des enjeux majeurs de l'élection américaine, avec des intérêts divergents, entre une tendance régulatrice du côté des Démocrates et libérale chez les Républicains. Trop réguler ou peu réguler, telle est la question ! Depuis sa création, digiVolution ne cesse d'attirer l'attention sur les conséquences des cyberpannes potentiellement systémiques. Qu'elles soient intentionnelles ou pas n'est pas le plus important. **Le BSoD (Blue Screen of Death) provoqué par la mise à jour ratée de CrowdStrike le 19 juillet et la panne du 30 juillet lorsque Microsoft s'est loupé dans la défense contre une attaque DDoS doivent nous interpeller.**

Liebe Leserinnen und Leser,

Wir freuen uns, Ihnen unsere 104. dVNews (13-2024) mit einer Auswahl an Artikeln und Links zukommen zu lassen. Wir haben euch vermisst... wir brauchten auch eine kleine Auszeit und die Olympischen Spiele in Paris haben uns sehr beschäftigt.

Technologie sind bei den US-Wahlen eine der grössten Themen, mit divergierenden Interessen, von einer regulatorischen Tendenz der Demokraten zu einer liberalen seitens der Republikaner. Zu viel oder wenig Regulierung– das ist die Frage! Seit seiner Gründung, hat digiVolution immer wieder auf die Folgen von potenziell systemischen Cyberpannen hingewiesen. Ob absichtlich oder nicht, ist nicht die Frage. **Der BSoD (Blue Screen of Death), der durch das fehlgeschlagene CrowdStrike-Update am 19. Juli ausgelöst wurde, und der Ausfall am 30. Juli, als Microsoft bei der Abwehr eines**

Dear readers,

We are pleased to send you our 104th dVNews (13-2024) with a selection of articles and links. We missed you... but we also needed a vacation, and the Paris Olympics kept us busy.

Technology is one of the biggest issues in the US elections, with competing interests from a regulatory tendency on the part of the Democrats and a liberal one on the part of the Republicans. Too much or few regulation - that is the question! Since the beginning, digiVolution has repeatedly highlighted the consequences of potentially systemic cyber mishaps. Whether intentional or not is not the question here. **The BSoD (Blue Screen of Death) triggered by the failed CrowdStrike update on July 19 and the outage on July 30, when Microsoft failed to defend against a DDoS attack, should challenge us.**

How can such a situation be accepted in which a small

Comment peut-on tolérer une situation où, à l'échelle mondiale, un petit bout de code et un processus de développement mal gérés interrompent des services bancaires, cloue au sol près de 6'000 vols, met hors ligne un nombre incalculable de services d'information, rende inopérants des centres d'appels d'urgences pour ne nommer que quelques conséquences. Les 8.5 millions de systèmes considérés comme touchés ne sont que ceux qui ont annoncé une panne à Microsoft. Combien ne l'ont pas fait et ainsi quel est le véritable impact de cette crise ? Un producteur de software peut-il se cacher derrière un article dans des conditions générales (ont-elles été lues ?) disant « ne doit pas être engagé dans des processus critiques » ? Une entreprise / infrastructure critique peut-elle être tenue responsable d'avoir mis des personnes / des intérêts / provoqué des pertes et des dégâts divers pour n'avoir pas tenu compte de cette condition? Peut-on accepter que des services essentiels intègrent en leur cœur des processus automatisés qui, en cas de panne, peuvent les mettre à terre ? Pourquoi tout ça ? Parce que l'on continue à économiser sur le dos de la sécurité. Quelle catastrophe faudra-t-il pour qu'enfin les standards de sécurité soient effectivement et intelligemment mis en œuvre ? Il y a un moment où le libéralisme doit s'effacer et où l'irresponsabilité et la

DDoS versagte, sollten uns herausfordern.

Wie kann eine Situation toleriert werden, in der ein kleines Stück Code und ein schlecht geführter Entwicklungsprozess weltweit Bankdienstleistungen lahmlegt, fast 6'000 Flüge am Boden hält, eine unkalkulierbare Anzahl von Informationsdienste offline stellt und Notrufzentralen lahmlegt, um nur einige der Folgen zu nennen? Die 8,5 Millionen Systeme, die als betroffen gelten, sind nur diejenigen, die einen Ausfall an Microsoft gemeldet haben. Wie viele haben es nicht getan, und wie gross sind die Auswirkungen dieser Krise wirklich? Kann sich ein Softwarehersteller hinter einem Artikel in den Allgemeinen Geschäftsbedingungen (wurden sie gelesen?) verstecken, der besagt, «darf nicht in kritischen Prozessen eingesetzt werden»? Kann ein Unternehmen oder eine kritische Infrastruktur dafür verantwortlich gemacht werden für Verluste und Schäden für Menschen oder Organisationen und Unternehmen, weil diese Bedingung nicht beachtet wurde? Können wir akzeptieren, dass wesentliche Dienste in ihrem Kern automatisierte Prozesse dulden, die sie bei einem Ausfall zum Erliegen bringen können? Warum ist das alles so? Weil auf dem Rücken der Sicherheit weiter gespart wird. Wie gross muss die Katastrophe sein, bis Sicherheitsstandards tatsächlich und intelligent umgesetzt werden? Es

piece of code disrupts banking services worldwide, grounding almost 6,000 flights, taking an incalculable number of information services and paralyzing emergency call centers, to name just a few of the consequences? The 8.5 million systems that are considered affected are only those that have reported an outage to Microsoft. How many did not, and how big is the real impact of this crisis? Can a software vendor hide behind an article in the General Terms and Conditions (have they been read?) that says, "must not be used in critical processes"? Can a company Can a company or critical infrastructure be held responsible for loss and damage to people or organizations and businesses because this condition was not observed? Can we accept that essential services tolerate automated processes at their core that can bring them to a standstill in the event of a failure? Why all this? Because we're still saving money at the expense of security. How big does the catastrophe have to be before security standards are actually and intelligently implemented? There is a point at which liberalism must step back and irresponsibility and negligence must be punished, as required by the Swiss Criminal Code (Art. 12 para. 3 SCC).

Apart from the unavailability of services and the opportunity for certain criminals to take advantage of the

négligence doivent être sanctionnées, comme l'exigence le code pénal (art. 12 al. 3 CP).

Au-delà de l'indisponibilité des services et de l'opportunité pour certains criminels de profiter de l'aubaine, il faut maintenant aussi considérer cette situation comme le révélateur d'une violation ou d'un abandon graves de la souveraineté des acteurs touchés. Ont-ils connaissance de leur dépendance réelle par rapport à leurs fournisseurs IT ? À l'évidence, non. Conséquences ?

Le coup de semonce doit être entendu et une analyse de cette situation est IMPERATIVE en fonction de la criticité du service délivré. Espérons que le Parlement passera dès que possible une motion pour imposer une analyse nationale de ce risque et qu'il en découle des responsabilités et obligations claires à l'adresse de l'ensemble des acteurs de la chaîne de valeur / d'approvisionnement.

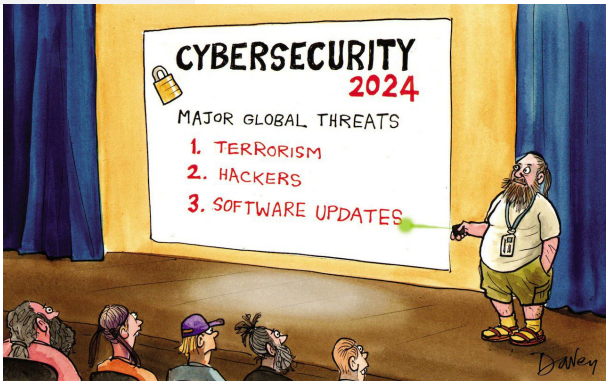
gibt einen Punkt, an dem der Liberalismus zurücktreten muss und Verantwortungslosigkeit und Nachlässigkeit bestraft werden müssen, wie es das Strafgesetzbuch verlangt (Art. 12 Abs. 3 StGB).

Abgesehen von der Nichtverfügbarkeit der Dienste und der Möglichkeit für Kriminelle, die Gunst der Stunde zu nutzen, muss diese Lage mindestens auch als Hinweis auf eine schwerwiegende Verletzung oder Verlust der Souveränität der Betroffenen betrachtet werden. Sind sie sich ihrer tatsächlichen Abhängigkeit von ihren IT-Anbietern bewusst? Offensichtlich nicht. Was sind die Folgen?

Der Warnschuss muss gehört werden. Eine Analyse dieser Situation ist ZWINGEND erforderlich und hängt vom Gefährdungspotential des Dienstes ab. Es ist zu hoffen, dass das Parlament so bald wie möglich eine Motion verabschiedet, um eine nationale Analyse dieses Risikos zu erzwingen und daraus klare Verantwortlichkeiten und Verpflichtungen für alle Akteure der Wertschöpfungs- und Lieferkette zu bestimmen.

moment, this situation must at least also be regarded as an indication of a serious violation or loss of the sovereignty of the affectied actors. Are they aware of their actual dependence on their IT providers? Obviously not. What are the consequences?

The warning shot must be heard, and an analysis of this situation is IMPERATIVE and depends on the criticality of the service. Hopefully, Parliament will pass a motion as soon as possible to force a national analysis of this risk and derive clear responsibilities and obligations for all actors in the value and supply chain.



BOOKS & REPORTS

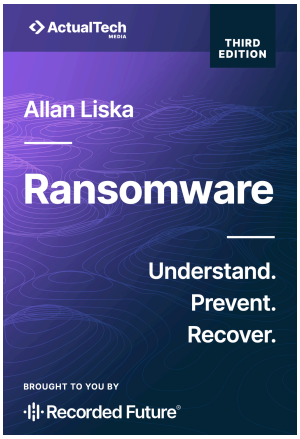
Voici la liste des livres et publications d'intérêt découverts lors de nos recherches, disponibles avec force détails sur dVPedia à la rubrique dVLibrary.

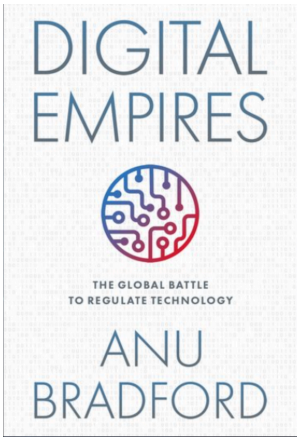
BOOKS & REPORTS

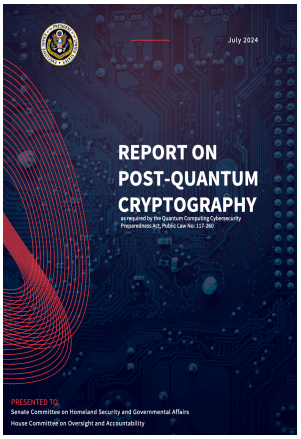
Dies ist eine Liste relevanter Bücher und Publikationen, auf die wir bei unseren Recherchen gestossen sind, mit vielen Details auf dVPedia unter dVLibrary verfügbar.

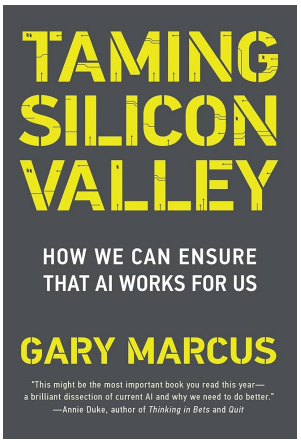
BOOKS & REPORTS

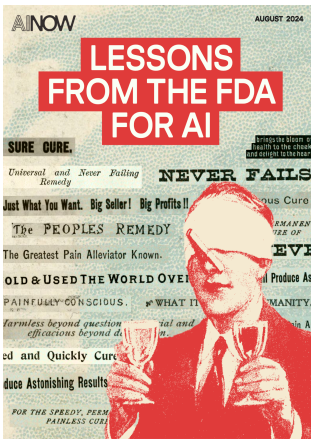
Here's a list of books and publications of interest discovered over the last few weeks, available with a lot of details in the dVLibrary section of dVPedia.

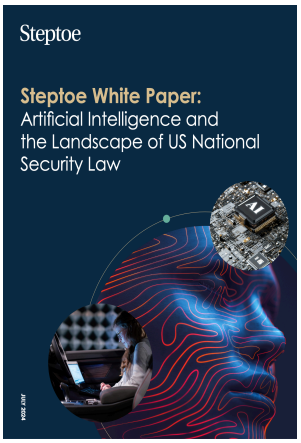


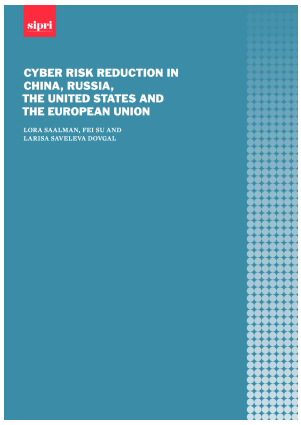


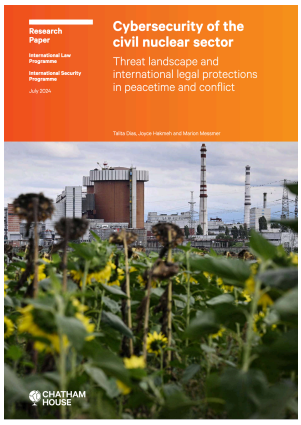


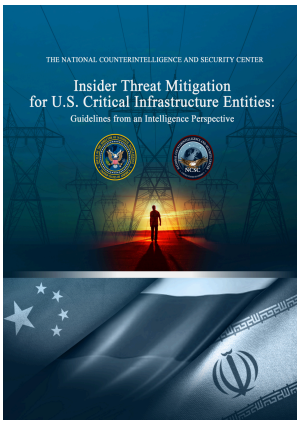












ACTUALITES

▶ **PQC ou Post Quantum Cryptography** – Depuis la création de *digi*Volution, nous ne cessons d'alarmer sur l'avènement des ordinateurs quantiques qui disposeront prochainement (2, 4, 10 ans ? les experts ne sont pas d'accord) d'une telle capacité de calcul, qu'ils pourront casser tous les algorithmes de chiffrage actuellement utilisés. Sont menacés non seulement les contenus / fichiers (y.c. ceux volés hier et aujourd'hui), mais également les réseaux, notamment le petit « s » du « https ». Quiconque disposera d'un ordinateur quantique pourra se balader librement et faire des dégâts dans toute infrastructure IT non protégée avec un PQC (ou plutôt une QRC – quantum resistant cryptography). Aux USA, le National Institute of Standards and Technology (NIST) vient de publier trois normes de chiffrement post-quantique. Le 21 décembre 2022, le Président Biden a promulgué la Loi sur la préparation à la cybersécurité de l'informatique quantique. Aux USA la migration démarre. Et en Suisse ? Avons-nous au moins une analyse des risques ? Et qui sait que nous avons une entreprise à la pointe et dont les solutions opérationnelles vont au-delà des exigences du NIST sans impacter les performances ?

▶ **Désinformation** – Dans notre société de la data et de la communication, la tentative

AKTUELLES

▶ **PQC oder Post Quantum Cryptography** – Seit der Gründung von *digi*Volution warnen wir immer wieder vor dem Einsatz von Quantencomputern, die bald (in 2, 4 oder 10 Jahren? die Experten sind sich nicht einig) über eine so grosse Rechenkapazität verfügen werden, dass sie alle derzeit angewendeten Verschlüsselungsalgorithmen knacken können. Bedroht sind nicht nur Inhalte / Dateien (auch solche, die gestern und heute gestohlen wurden), sondern auch Netzwerke u.a. das kleine „s" in „https". Wer einen Quantencomputer hat, kann sich frei bewegen und in jeder IT-Infrastruktur Schaden anrichten, die nicht mit einer PQC (oder eher einer QRC - quantum resistant crypto-graphy) geschützt ist. In den USA hat das National Institute of Standards and Technology (NIST) gerade drei Standards für Post-Quantum-Chiffrierung veröffentlicht. Am 21. Dezember 2022 hat Präsident Biden das Gesetz zur Vorbereitung auf die Cybersicherheit von Quantencomputern verabschiedet. In den USA beginnt nun die entsprechende Migration. Was ist mit der Schweiz? Haben wir mindestens eine Risikoanalyse? Und wer weiss, dass wir hier bereits ein Unternehmen haben, das die NIST-Anforderungen übertrifft, ohne die Leistung zu beeinträchtigen?

NEWS

▶ **PQC or Post Quantum Cryptography** – Ever since *digi*Volution was founded, we've been sounding the alarm about the use of quantum computers, which will soon (2, 4, 10 years from now? experts disagree) have such computing power that they can crack all encryption algorithms currently in use. At risk are not only contents / data (including those stolen yesterday and today), but also networks, including the little "s" in "https". Anyone with a quantum computer will be able to roam freely and wreak havoc on any IT infrastructure unprotected by a PQC (or rather a QRC - quantum resistant cryptography). In the USA, the National Institute of Standards and Technology (NIST) has just published three post-quantum encryption standards. On December 21, 2022, President Biden signed into law the Quantum Computing Cybersecurity Preparedness Act. The corresponding migration is beginning in the USA. What about Switzerland? Do we even have a risk analysis? And who knows that we have a cutting-edge company whose operational solutions going beyond NIST requirements without impacting performance?

▶ **Disinformation** – In our society of data and communication, the assassination attempt on Donald Trump has produced this iconic image,

d'assassinat contre Donald Trump a produit cette image désormais iconique, déjà comparée à celle d'Ivo Jima lors de la Guerre du Pacifique.

▶ **Desinformation** – In unserer Daten- und Kommunikationsgesellschaft hat der Attentatsversuch auf Donald Trump ein Bild hervorgebracht, das bereits mit dem von Ivo Jima während des Pazifikkriegs verglichen wird.

already compared to that of Ivo Jima during the Pacific War.

Quasiment annoncé comme facile vainqueur en novembre prochain, un mois plus tard, le candidat Trump mesure certainement déjà amèrement les effets de la campagne des Démocrates sur le thème « weird ». Quelles leçons tirer ? La volatilité des opinions qui reposent sur des bases toujours plus émotionnelles et simplistes et plus élevée que jamais. La course à l'élection risque fort d'être tumultueuse et marquée par de nombreux dérapages qu'attisent déjà certains acteurs étrangers. Et comme on vient de le voir avec les émeutes en Grande-Bretagne, manipuler les foules déjà chauffées à blanc par des années de frustration est facile.

Fast schon als sicherer Sieger im November gefühlt, sieht sich der Kandidat Trump einen Monat später sicherlich verbittert der „weird" Kampagne der Demokraten gegenüber. Welche Lehren lassen sich daraus ziehen? Die Volatilität von Entscheidungen, die auf immer emotionaleren und populistischen Grundlagen beruhen, ist grösser denn je. Die Zeit vor der Wahl wird turbulent und einige ausländische Akteure haben bereits Aktionen in Richtung USA initiiert. Und wie wir gerade bei den Unruhen in Grossbritannien gesehen haben, ist es leicht, Menschenmassen zu manipulieren, die durch jahrelange Frustration aufgeheizt sind.

Almost announced as an easy winner in November, a month later, the candidate Trump is certainly already bitterly measuring the effects of the Democrats' "weird" campaign. What lessons can be drawn? The volatility of opinions, based on ever more emotional and populistic fundamentals, is higher than ever. The run-up to the election is likely to be a tumultuous one, marked by a number of skids already being stirred up by certain foreign players. And as we've just seen with the riots in Great Britain, manipulating crowds already fired up by years of frustration is easy.

▶ **Budget 2025 de l'OFCS** – Avec son budget de 16.1 Mio CHF (1.5 Mio de plus qu'en 2024), l'Office fédéral de la cybersécurité pèsera… 18 fois moins que le sport et ses 303 mio CHF. On parle pourtant ici de la sécurité du pays et de toutes nos activités totalement dépendantes du numérique ! Comment sont établies les priorités ?

▶ **Budget 2025 des BACS** – Mit einem Budget von 16,1 Mio. CHF (1,5 Mio. mehr als 2024) wird das Bundesamt für Cybersicherheit 18 Mal weniger Gewicht haben als der Sport mit seinen 303 Mio. CHF. Wir reden hier über die Sicherheit des Landes und all unsere Aktivitäten, die von der Digitalisierung abhängen! Wie werden die Prioritäten gesetzt?

▶ **NCSC 2025 budget** – With a budget of CHF 16.1 million (CHF 1.5 million more than in 2024), the Federal Office for Cybersecurity will have 18 times less weight than sport with its CHF 303 million. But we're talking about the country's security and all our activities that are totally dependent on digital technology! How are the priorities set?

▶ **NIS2 - Network and Information Security** – Le 25 juin, nous avons eu le privilège de participer à Vienne chez *Die Presse*, l'équivalent autrichien de notre *NZZ,* à un débat autour de la nouvelle loi européenne sur la sécurité des systèmes d'information. En résumé : maintenant on ne rigole plus et il est plus que l'heure pour les entreprises suisses, que cela plaise ou non, de prendre connaissance de ces nouvelles règles qui les concernent aussi dès lors qu'elles interagissent avec des partenaires et clients européens.

▶ **NIS2 - Network and Information Security** – Am 25. Juni hatten wir das Privileg, in Wien bei *Die Presse*, dem österreichischen Pendant zu unserer *NZZ*, an einer Debatte über das neue europäische Gesetz über die Sicherheit von Informationssystemen teilzunehmen. Kurz gesagt: Jetzt ist Schluss mit lustig und es ist höchste Zeit, dass sich Schweizer Unternehmen, ob sie wollen oder nicht, mit den neuen Regeln vertraut machen, die auch sie betreffen, wenn sie mit europäischen Partnern und Kunden interagieren.

▶ **NIS2 - Network and Information Security** – On June 25, we had the opportunity of taking part in a debate on the new European law on information systems security at *Die Presse*, the Austrian equivalent of our *NZZ* in Vienna. In a nutshell : now is the time for Swiss companies, like it or not, to take note of these new rules, which also affect them when interacting with European partners and consumers.

La prochaine fois, nous vous parlerons des JO de Paris auxquels nous avons contribué. Sans trahir de secrets d'affaires, il s'agira de tirer les enseignements de cette méga-manifestation. Nous aurions pu le faire à chaud, mais voulons rester au niveau stratégique sans nous laisser influencer par les manchettes de la presse. Prenons le recul nécessaire.

Voilà pour cette 104ème édition. Nous espérons qu'elle vous a, une fois encore, inspiré et vous souhaitons aussi une enrichissante découverte des articles et liens sélectionnés.

Merci également de souscrire à *d*VPedia et ainsi de soutenir son développement au profit de tous.

Das nächste Mal werden wir über die Olympischen Spiele in Paris berichten, zu denen wir einen Beitrag geleistet haben. Ohne Geschäftsgeheimnisse zu verraten, wird es darum gehen, die Lehren aus dieser Mega-Veranstaltung zu ziehen. Wir hätten das auch aus dem Stegreif tun können, aber wir wollen auf der strategischen Ebene bleiben und uns nicht von den medialen Schlagzeilen beeinflussen lassen. Lass uns einen Schritt zurücktreten.

Das war's für diese 104. Ausgabe. Wir hoffen, dass sie Sie einmal mehr inspiriert hat und wünschen Ihnen viel Spass beim Entdecken der ausgewählten Artikel und Links.

Bitte registrieren Sie sich ebenfalls für *d*VPedia und unterstützen Sie damit seine Entwicklung zum Nutzen aller.

Next time, we'll tell you about the Paris Olympics, to which we contributed. Without betraying any business secrets, we'll be drawing lessons from this event. We could have done so in the heat of the moment, but let's stay at the strategic level, not allowing ourselves to be influenced by press headlines. Let's take a step back.

That's all for this 104th edition. We hope you enjoyed it again and wish you an enriching discovery of the selected articles and links.

Thank you for subscribing to *d*VPedia and supporting its development for the benefit of all.

Merci de penser à soutenir *digi*Volution.

Bitte denken Sie daran, *digi*Volution zu unterstützen.

Please consider supporting *digi*Volution.

digiVolution

TWINT

Depuis le 8 janvier 2021, digiVolution publie un billet de réflexion (newsletter) qui accompagne une sélection d'articles « hand picked » pour illustrer la complexité des défis liés à la mutation digitale ; ils sont disponibles à l'adresse https://www.digivolution.swiss/dv-blog.
Ce billet est rédigé par des individus et non par de l'IA. Nous employons des moyens techniques utilisant de l'IA pour soutenir nos recherches, mais ne lui confions aucune tâche rédactionnelle ou de réflexion.

Seit dem 8. Januar 2021 veröffentlicht digiVolution regelmässig Newsletter, die von einer Auswahl «handverlesener» Artikel begleitet wird, die die Komplexität, der mit der digitalen Mutation einhergehenden Herausforderungen veranschaulichen; Sie finden diese unter https://www.digivolution.swiss/dv-blog.
Dieser Beitrag wird von Menschen und nicht von KI geschrieben. Wir setzen technische Mittel ein, die KI verwenden, um unsere Forschung zu unterstützen, übertragen KI jedoch keine redaktionellen oder gedanklichen Aufgaben.

Since January 8, 2021, digiVolution has been publishing a newsletter that accompanies a selection of «hand picked» articles to illustrate the complexity of the challenges linked to digital mutation; they are available at https://www.digivolution.swiss/dv-blog. This newsletter is written by individuals, not by AI. We employ technical means using AI to support our research, but do not entrust it with any editorial or reflective tasks