Les billets[i] de *digi*Volution / *digi*Volution's Newsletters
[14.02.2022 – 45ème édition]

February 24, 2022

Chers Lectrices et Lecteurs

Voici les ***d*V-News 05-2022** et leur sélection d'articles et de liens pour illustrer l'actualité de la dernière quinzaine. Dans cette édition, nous avons décidé de nous concentrer sur les **cybermenaces en lien avec la guerre déclenchée par la Russie contre l'Ukraine et choisi pour titre une date qui restera désormais dans l'histoire.**

"*Yesterday, December 7, 1941 - a date which will live in infamy - the United States of America was suddenly and deliberately attacked by naval and air forces of the Empire of Japan*." Ainsi commença le discours du Président Roosevelt devant le Congrès le 8 décembre 1941. Comment, le 24 février 2022, en est-on arrivé à cette situation qui risque de nous précipiter dans un nouveau conflit généralisé aux conséquences dévastatrices? Comment en est-on arrivé au point où ce gouvernement russe se met à menacer le monde du feu nucléaire? Nous laisserons ici les commentateurs – tous plus avisés les uns que les autres – déterminer qui porte quelles responsabilités dans le chemin qui a amené l'humanité à ce point de bascule, mais nous voulons, haut et fort, affirmer **notre profonde conviction qu'aucune raison ne justifie cette escalade de violence et qu'elle doit être condamnée dans les termes les plus durs**.

Quels sont les développements possibles de cette guerre dans les sphères cybernétique et informationnelle pour la Suisse? Toute action dépend de trois critères: savoir, pouvoir, vouloir. Le savoir, soit le "où et comment frapper", est largement disponible. Le pouvoir, soit les moyens opération-

Liebe Leserinnen und Leser

Dies sind die ***d*V-News 05-2022** und unsere Auswahl von Artikeln und Links, die die Nachrichten der letzten zwei Wochen aufzeigen. In dieser Ausgabe haben wir beschlossen, uns auf die **Cyberbedrohungen im Zusammenhang mit dem von Russland gegen die Ukraine entfesselten Krieg zu konzentrieren, und als Titel ein Datum gewählt, das nun in die Geschichte eingehen wird.**

"*Yesterday, December 7, 1941 - a date which will live in infamy - the United States of America was suddenly and deliberately attacked by naval and air forces of the Empire of Japan.*" So begann die Rede von Präsident Roosevelt vor dem Kongress am 8. Dezember 1941. Wie konnte es am 24. Februar 2022 zu dieser Situation kommen, die uns in einen neuen, umfassenden Konflikt mit verheerenden Folgen stürzen könnte? Wie konnte es so weit kommen, dass die russische Regierung der Welt mit nuklearem Feuer droht? Wir überlassen es den klugen Kommentatoren, zu entscheiden, wer welche Verantwortungen für den Weg trägt, der die Menschheit an diesen Wendepunkt gebracht hat. Wir wollen allerdings **laut und deutlich unsere tiefe Überzeugung bekräftigen, dass es keinen Grund gibt, diese Eskalation der Gewalt zu rechtfertigen, und dass sie auf das Schärfste verurteilt werden muss**.

Welche Auswirkungen könnte dieser Krieg auf die Cyber- und Informationssphären für die Schweiz haben? Jede Handlung hängt von drei Kriterien ab: Wissen, Können und Wollen. Das Wissen, d.h. "wo und wie man zuschlägt", ist weitgehend verfügbar. Das Können, d.h. die operativen Mittel,

nels, ils sont déjà largement engagés au quotidien. Le vouloir, ou la décision de passer à l'acte; Poutine a balayé lui-même les derniers doutes et ses dernières déclarations sur l'emploi de l'arme nucléaire ne laissent rien augurer de bon.

Nous avons donc décrit ci-après les risques qui, sur la base des faits passés et actuels, pourraient se matérialiser dans un futur proche contre la Suisse et ses intérêts.

Dans l'immédiat

- **Cyberharcèlement** - Les soutiens criminels habituels du Kremlin peuvent, à l'instar des actions des Anonymous qui ont annoncé vouloir cibler la Russie, arroser la société de multiples cyberattaques peu sophistiquées, mais suffisantes pour provoquer d'importantes perturbations qui ne manqueraient pas de toucher directement la vie quotidienne de la population et impacteraient les activités de nos entreprises. Nos moyens de lutte atteindront ici déjà rapidement leurs limites.
- **Propagande et désinformation** - Ces actions sont déjà largement en cours. Les réseaux sociaux sont inondés de fake news et la rhétorique utilisée est extrêmement agressive avec des allusions hallucinantes au nazisme et à un génocide en cours. À part la diffusion de consignes au moyen de ses services de communication, notre gouvernement n'a pas de moyens. Elle ne peut que se réfugier derrière la liberté de l'information et espérer que cette situation n'aille pas plus diviser une population déjà éprouvée par deux ans de dégâts informationnels infligés par le COVID.
- **Cybercriminalité** – Le vacarme de la guerre est une aubaine pour ceux qui veulent profiter d'un "effet tunnel". Il faut donc s'attendre à une recrudescence de cyberattaques opportunistes des "petits voleurs", comme ce fut le cas dès le début de la crise du COVID.

Ensuite, si le conflit dure et s'étend à d'autres théâtres (les poudrières ne manquent pas).

diese gehören bereits dem Alltag. Das Wollen oder die Entscheidung, zur Tat zu schreiten; da hat Putin selbst die letzten Zweifel beseitigt und seine jüngsten Äusserungen über den Einsatz von Atomwaffen verheissen nichts Gutes.

Im Folgenden zeigen wir bedeutende Risiken auf, die sich auf der Grundlage der vergangenen und aktuellen Fakten in naher Zukunft für die Schweiz und ihre Interessen ergeben könnten.

In unmittelbarer Zukunft

- **Cybermobbing** – Die üblichen kriminellen Unterstützer des Kremls können - wie die Akteure von Anonymous, die angekündigt haben, Russland ins Visier zu nehmen - die Gesellschaft mit zahlreichen wenig raffinierten Cyberangriffen überziehen, die jedoch ausreichen, um erhebliche Störungen zu verursachen, die das tägliche Leben der Bevölkerung und die Aktivitäten unserer Unternehmen direkt betreffen. Unsere Gegenmassnahmen werden hier schnell an ihre Grenzen stossen.
- **Propaganda und Desinformation** – Diese Massnahmen sind bereits weitgehend im Gange. Die sozialen Netzwerke werden mit Fake News und Bots überschwemmt und die verwendete Rhetorik ist extrem aggressiv mit halluzinierenden Anspielungen auf den Nationalsozialismus und einen stattfindenden Genozid. Abgesehen von der Verbreitung von Anweisungen über ihre Kommunikationsdienste verfügt unsere Regierung kaum über Mittel. Sie kann sich nur hinter der Informationsfreiheit verstecken und hoffen, dass diese Situation nicht zu einer weiteren Spaltung der Bevölkerung führt, die bereits durch den zweijährigen Informationsschaden, der ihr durch COVID zugefügt wurde, geschädigt wurde.
- **Cyberkriminalität** – Der Kriegslärm ist ein gefundenes Fressen für diejenigen, die von einem "Tunneleffekt" profitieren wollen. Daher ist mit einem Anstieg der opportunistischen Cyberangriffe der "kleinen Diebe" zu rechnen,

- **Cybersabotages** – La préparation de cyberattaques sophistiquées prendra quelques semaines ou mois, sauf si les préparatifs ont déjà été réalisés. Des actions à des fins stratégiques visant des infrastructures et services vitaux dans le but de paralyser la société sont ainsi probables avec pour cibles primaires l'électricité et les câbles sous-marins pour le transport des données dont nous sommes totalement dépendants. Dans ce cas, des attaques contre l'UE impacteront aussi la Suisse en raison de l'interconnexion des réseaux. Ces dernières années, la Russie s'est déjà "exercée" contre l'Ukraine, les USA et le réseau de distribution européen et divers alliés de la Russie pourraient intensifier les efforts de celle-ci et compliquer l'attribution de ces cyberattaques, entravant ainsi notre propre défense. Car sans identification claire de l'auteur, pas de contre-mesure possible.
- **Chaînes d'approvisionnement** – La perturbation croissante des flux complexes de l'économie mondiale conduira à un manque de ressources de base (métaux, pétrole, etc.) et de composants, entraînant une perturbation croissante de notre économie. Seront notamment impactés le remplacement ou la réparation de systèmes en panne ou ayant subi divers types d'attaques, dont celles cyber. Le fragile équilibre de notre économie "en flux tendu" sera fortement perturbé pendant une durée inconnue à ce stade.
- **Atteinte contre la société et la démocratie** – Rappelons-nous les élections aux USA avec des mouvements de type Q-Anon, aussi présents en Suisse. Rappelons-nous aussi la votation sur la loi COVID à fin 2021. Nous l'avons déjà écrit, la Suisse n'est pas à l'abri et personne ne sait ce que le cocktail "hausse des prix / privations + peur + désinformation" pourrait entraîner chez nous aussi. Dans ce contexte, il faut aussi craindre un possible effet boule de neige qui pourrait affecter d'autres régions du monde.

wie es bereits seit Beginn der COVID-Krise der Fall war.

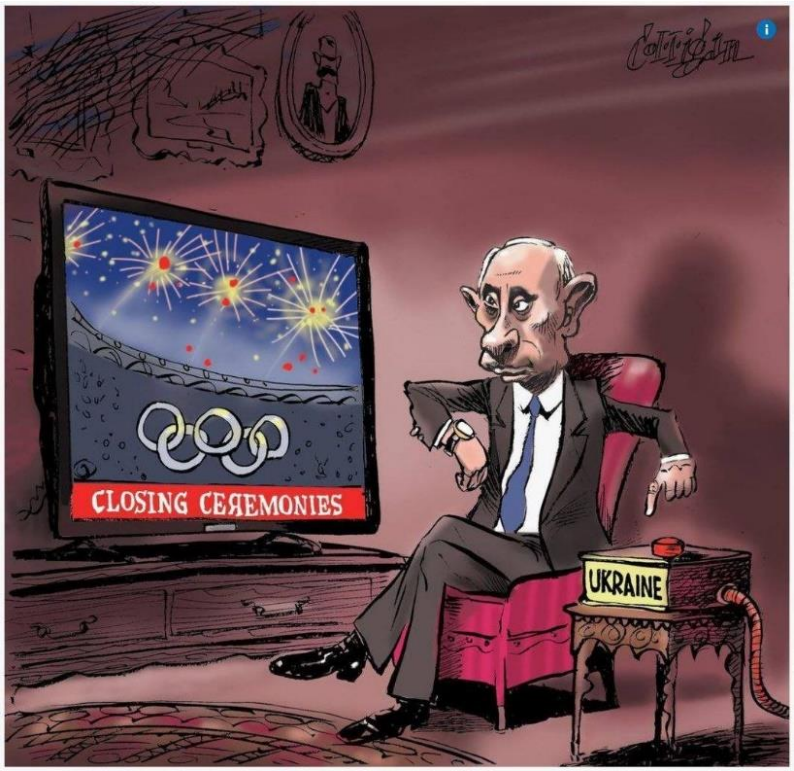
Später, wenn der Konflikt anhält und sich auf andere Schauplätze ausweitet (an Pulverfässern mangelt es nicht).

- **Cybersabotage** – Die Vorbereitung ausgeklügelter Cyberangriffe wird einige Wochen oder Monate in Anspruch nehmen, sofern sie nicht bereits abgeschlossen sind. Strategisch motivierte Aktionen, die auf lebenswichtige Infrastrukturen und Dienste abzielen, um die Gesellschaft lahmzulegen, sind somit wahrscheinlich, wobei die primären Ziele die Stromversorgung und die Unterseekabel für den Datentransport sind, von denen wir völlig abhängig sind. In diesem Fall würden Angriffe auf die EU auch die Schweiz betreffen, da die Netze miteinander verbunden sind. Russland hat in den letzten Jahren bereits gegen die Ukraine, die USA und das europäische Verteilungsnetz "geübt", und verschiedene Verbündete Russlands könnten ihre Bemühungen verstärken und die Zuweisung solcher Cyberangriffe erschweren und damit unsere eigene Verteidigung behindern. Denn ohne eindeutige Identifizierung des Urhebers (Attribution) sind keine Gegenmassnahmen möglich.
- **Lieferketten** – Die zunehmende Störung der komplexen Abläufe in der Weltwirtschaft wird zu einem Mangel an grundlegenden Ressourcen (Metalle, Öl, usw.) und Komponenten führen, was eine zunehmende Beeinträchtigung unserer Wirtschaft zur Folge hat. Dies betrifft u.a. den Ersatz oder die Reparatur von Systemen, die ausgefallen sind oder die verschiedenen Arten von Angriffen, einschliesslich Cyberangriffen, ausgesetzt waren. Das sensible Gleichgewicht unserer "just-in-time"-Wirtschaft wird für eine derzeit noch nicht absehbare Zeit stark gestört sein.
- **Angriff auf die Gesellschaft und die Demokratie** – Erinnern wir uns an die Wahlen in den USA mit den Q-Anon-Bewegungen, die auch in der Schweiz präsent sind. Erinnern wir uns

Que l'on ne vienne pas nous dire que ces développements ne sont pas réalistes! Depuis 1991, ceux qui ont désarmé notre Pays ont eu tort: **la guerre et ses conséquences n'ont pas disparu du paysage de la politique européenne et mondiale et doivent demeurer partie intégrante de notre vocabulaire**. La culture suisse en matière de politique de sécurité doit revenir à la réalité: le monde n'est pas une grande colonie de gentils Bisounours! Il y aura toujours des intérêts de puissance utilisés abusivement par des criminels prêts à presser sur le bouton…

auch an die Abstimmung über das COVID-Gesetz Ende 2021. Wir haben bereits geschrieben, dass die Schweiz nicht immun ist und niemand weiss, was der Cocktail "steigende Preise / Entbehrungen + Angst + Desinformation" auch bei uns bewirken könnte. In diesem Zusammenhang ist auch ein möglicher Schneeballeffekt zu befürchten, der andere Regionen der Welt betreffen könnte.

Man kann uns nicht weismachen, dass diese Entwicklungen unrealistisch sind! Diejenigen, die unser Land seit 1991 entwaffnet haben, haben sich geirrt: **Krieg und seine Folgen sind nicht aus der Landschaft der europäischen und globalen Politik verschwunden und müssen Teil unseres Vokabulars bleiben.** Die sicherheitspolitische Kultur der Schweiz muss sich auf die Realität besinnen: Die Welt ist keine grosse Kolonie freundlicher Teddybären! Es wird immer Machtinteressen geben, die von Kriminellen missbraucht werden, die bereit sind, auf den Knopf zu drücken...



Nous non plus ne savions pas ce qui allait se passer le 24 février 2022, mais chez *digi*Volution nous cultivons un **sens profond de précaution** et les recommandations de notre billet du 14 février étaient ainsi en phase avec la situation devenue entre-temps réelle. S'il n'est pas honteux de subir une attaque, quelle qu'elle soit, il est en revanche inacceptable de subir des dégâts qui auraient pu être évités par des mesures préconisées et répétées depuis longtemps par de nombreux professionnels. Rappelons que la négligence est un acte criminel puni pénalement par notre code pénal.

La Suisse est-elle prête aux développements probables exposés ci-dessus? La réponse est clairement non! Alors, en fonction de l'évolution de la situation, voici une mise à jour de nos recommandations:

- Les mesures préconisées dans notre billet du 14 février doivent être mises en œuvre sans plus attendre: ◆ vérifier la **liste des cyberrisques** susceptibles d'impacter la marche des affaires et adapter les **mesures de cybersécurité** en conséquence; ◆ former le **personnel** à détecter et à réagir face à des actes cybermalveillants et aux perturbations qui pourraient s'ensuivre; ◆ vérifier et entraîner le **dispositif de gestion de crise.** Au besoin *digi*Volution peut prêter main forte.
- Dans le cyberespace, un suivi permanent de l'évolution de la situation doit être réalisé et le renseignement ainsi gagné doit être distribué sans attendre à tous les décideurs. *digi*Volution construit en ce moment une solution qui sera annoncée lors des prochains SCSD.
- Les enseignements de cette première guerre de haute intensité au temps de l'hyperconnectivité doivent être tirés et concrétisés en continu. Se donner des années pour mettre en place un projet? C'est terminé. L'agilité doit être un fait et non plus un slogan vide. Chez *digi*Volution nous assurons une veille stratégique et partagerons volontiers nos observations pour aider les organisations à prendre les bonnes décisions.

Auch wir wussten nicht, was am 24. Februar 2022 passieren würde, aber bei *digi*Volution pflegen wir einen **ausgeprägten Sinn für Vorsicht**, und so entsprachen die Empfehlungen in unserem Newsletter vom 14. Februar der mittlerweile realen Situation. Es ist zwar nicht schändlich, einen wie auch immer gearteten Angriff zu erleiden, aber es ist inakzeptabel, Schäden zu erleiden, die durch Massnahmen hätten vermieden werden können, die von vielen Fachleuten seit langem empfohlen und wiederholt werden. Es sei daran erinnert, dass Fahrlässigkeit eine kriminelle Handlung ist, die in unserem Strafgesetzbuch entsprechend geahndet wird.

Ist die Schweiz auf die oben beschriebenen wahrscheinlichen Entwicklungen vorbereitet? Die Antwort ist eindeutig Nein! Je nachdem, wie sich die Situation entwickelt, werden unsere Empfehlungen hier aktualisiert:

- Die in unserem Newsletter vom 14. Februar empfohlenen Massnahmen sollten umgehend umgesetzt werden: ◆ Überprüfung der Liste der Cyberrisiken, die sich auf den Geschäftsbetrieb auswirken könnten, und entsprechende Anpassung der Cybersicherheitsmassnahmen; ◆ Schulung der Mitarbeiter in der Erkennung und Reaktion auf bösartige Cyberattacken und die daraus resultierenden Störungen; ◆ Überprüfung und Training des eigenen Krisenmanagementdispositivs. Bei Bedarf kann *digi*Volution Unterstützung leisten.
- Im Cyberspace muss die Entwicklung der Lage ständig verfolgt werden, und die so gewonnenen Erkenntnisse müssen unverzüglich an alle Entscheidungsträger verteilt werden. *digi*Volution baut derzeit an einer Lösung, die bei den nächsten SCSD angekündigt werden soll.
- Die Lehren aus diesem ersten hochintensiven Krieg in Zeiten der Hyperkonnektivität müssen laufend gezogen und konkretisiert werden. Jahrelang an der Umsetzung eines Projekts arbeiten? Das ist vorbei. Agilität muss eine Tatsache und kein leeres Schlagwort

- La milice est un moyen unique pour créer sans délai un successeur à feu le Régiment d'information 1 disparu à fin 2003. La Suisse doit enfin se donner les moyens d'analyser et de combattre en continu la propagande et la désinformation. Là aussi, *digi*Volution dispose dans ses cartons d'une solution qui devrait pouvoir être prochainement communiquée.
- Il faut d'urgence prendre acte des transformations profondes qu'entraînent la digitalisation et l'hyperconnexion. Quand on lit "*Ueli Maurer will eine starke Armee*", de laquelle s'agit-il? Nous doutons que dans l'immédiat *plus de blindés et d'artillerie* soient la bonne réponse. Il est par ailleurs urgent d'adapter les mécanismes politiques qui, année après année, empêchent l'armée de se développer. L'initiative contre le F35 en étant le dernier avatar. On peut réduire les droits abusifs de recours contre le déploiement d'éoliennes et pas en matière de défense nationale? Et quid de notre base industrielle de défense?

Chers Lectrices et Lecteurs, nous aspirons tous à la paix et à un bonheur légitime, mais l'actualité nous a brutalement réveillés et montré un visage que beaucoup avaient voulu oublier. Il n'est plus l'heure de tergiverser et de remettre à demain ce que nous aurions dû faire depuis longtemps pour notre cybersécurité. Si nous avons pu mettre des milliards pour défendre les salaires durant le COVID, pourquoi ne pourrions pas mettre des moyens enfin à la hauteur des défis pour défendre nos entreprises et infrastructures menacées par d'autres virus…! Cela est urgent.

Nous nous permettons, une fois encore, de revenir sur nos remarques sur le Rapport de politique de sécurité du Conseil fédéral. Nous en sommes convaincus, les enjeux de la mutation digitale n'ont pas été compris.

Dans les années '80, on disait de la Suisse qu'elle n'avait pas d'armée, mais quelle était une armée. Et si nous adaptions cette image aux nouveaux défis? **Dans le cyberespace seule une société solide en profondeur, où toutes les mains, petites**

sein. Wir bei *digi*Volution beobachten die Lage und teilen gerne unsere Erkenntnisse, um Organisationen dabei zu helfen, die richtigen Entscheidungen zu treffen.

- Die Miliz ist ein einzigartiges Mittel, um ohne Verzögerung einen Ersatz für das Ende 2003 verschwundene Informationsregiment 1 zu schaffen. Die Schweiz muss sich endlich die Mittel verschaffen, um Propaganda und Desinformation kontinuierlich zu analysieren und zu bekämpfen. Auch hier hat *digi*Volution eine Lösung in petto, die demnächst bekannt gegeben wird.
- Die tiefgreifenden Veränderungen, die die Digitalisierung und Hypervernetzung mit sich bringen, müssen dringend zur Kenntnis genommen werden. Wenn man liest "*Ueli Maurer will eine starke Armee*", welche ist das? Wir bezweifeln, dass *mehr Panzer und Artillerie* im Moment die richtige Antwort ist. Ausserdem ist es dringend notwendig, die politischen Mechanismen anzupassen, die die Armee Jahr für Jahr daran hindern, sich weiterzuentwickeln. Die Initiative gegen den F35 ist das jüngste Beispiel dafür. Man kann die missbräuchlichen Einspruchsrechte gegen die Errichtung von Windkraftanlagen einschränken, aber nicht im Bereich der Landesverteidigung? Und was ist mit unserer industriellen Verteidigungsbasis?

Liebe Leserinnen und Leser, wir alle sehnen uns nach Frieden und legitimem Glück, aber die Nachrichten haben uns unsanft geweckt und ein Gesicht gezeigt, das viele vergessen wollten. Es ist nicht mehr an der Zeit, zu zögern und auf morgen zu verschieben, was wir für unsere Cybersicherheit schon längst hätten tun sollen. Wenn wir während der COVID-Krise Milliarden für die Verteidigung der Löhne aufbringen konnten, warum sollten wir dann nicht endlich die Mittel aufbringen, die den Herausforderungen entsprechen, um unsere Unternehmen und Infrastrukturen zu verteidigen, die von anderen Viren bedroht werden...? Das ist dringend notwendig.

et grandes, font leur part, sera en mesure d'assurer sa protection et sa résilience, de maintenir la confiance et l'unité de ses citoyens et d'assumer sa souveraineté. Une "défense générale" – bien sûr revisitée – est l'affaire de tous.

Chez *digi*Volution nous militons, comme d'autres pour penser et construire une cybersécurité globale qui ne soit pas un simple accessoire de notre temps, mais la clé d'une mutation digitale réussie de notre société et pour passer d'une logique de réaction à celle de l'anticipation.

Nous vous souhaitons une enrichissante découverte des articles et liens sélectionnés, nous réjouissons de vous retrouver dans 15 jours.

Wir erlauben uns, noch einmal auf unsere Bemerkungen zum Sicherheitspolitischen Bericht des Bundesrates zurückzukommen. Wir sind überzeugt, dass die Herausforderungen des digitalen Wandels nicht verstanden wurden.

In den 1980er Jahren sagte man über die Schweiz, dass sie keine Armee habe, sondern eine Armee sei. Wie wäre es, wenn wir dieses Bild an die neuen Herausforderungen anpassen würden? **Im Cyberraum wird nur eine in der Tiefe solide Gesellschaft, in der alle, ob gross oder klein, ihren Teil beitragen, in der Lage sein, sich zu schützen und resilient zu sein, das Vertrauen und die Einheit ihrer Bürger aufrechtzuerhalten und ihre Souveränität wahrzunehmen**. Eine "Gesamtverteidigung" – natürlich in neuem Gewand – geht uns alle an.

Bei *digi*Volution setzen wir uns, wie andere auch, dafür ein, eine globale Cybersicherheit zu denken und aufzubauen, die nicht einfach ein Add-On unserer Zeit ist, sondern der Schlüssel zu einer erfolgreichen digitalen Mutation unserer Gesellschaft und um von einer Logik der Reaktion zu einer Logik der Antizipation überzugehen.

Wir wünschen Ihnen eine bereichernde Entdeckung der ausgewählten Artikel und Links und freuen uns darauf, Sie in zwei Wochen wieder zu informieren.

---

[i] *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. Ces articles sont disponibles à l'adresse https://www.digivolution.swiss/news/. Les personnes intéressées trouveront sur cette même page le lien pour s'y inscrire. /// Seit dem 8. Januar 2021 veröffentlicht digiVolution regelmässig einen Newsletter, der von einer Auswahl «handverlesener» Artikel begleitet wird, die die Komplexität, der mit der digitalen Mutation verbundenen Herausforderungen veranschaulichen. Diese Artikel finden Sie unter https://www.digivolution.swiss/news/. Interessierte finden auf dieser Seite auch den Link zur Anmeldung.*