

Les billetsⁱ de *digiVolution* / *digiVolution's* Newsletters
[20.06.2023 – Édition / Ausgabe Nr. 78]

Awake now?

Chers Lectrices et Lecteurs

Voici les **dV-News 12-2023** et leur sélection d'[articles et liens](#).

La Suisse assiégée - Place enfin au réveil et au réalisme

Il y a quelque chose que nous détestons faire chez *digiVolution*, c'est de dire: «*nous avions prévenu*» ! Dans le cadre de l'attaque contre la société XPLAIN, nous écrivions il y a 15 jours, en réaction aux affirmations qu'aucune donnée opérationnelle n'avait été exposée, «*on mesurera l'ampleur réelle plus tard*». Et quelle surprise... de [telles données se retrouvent dans la nature](#) ! Il incombe maintenant au [NCSC](#) de défaire l'imbroglio, de réparer et de faire oublier la communication précipitée et peu professionnelle de certains offices.

Dans la même veine, la firme Bobst annonçait en avril avoir subi une cyberattaque, tout en restant optimiste. «*Nos défenses ont été très efficaces*» et «*à notre connaissance, nous n'avons subi aucune fuite de données*». Pourtant le 9 juin, plusieurs médias rapportaient que des [données sensibles](#) ont bel et bien été dérobées et sont désormais disponibles dans le dark web. Espérons que la [commune de Bex](#) aura eu plus de chance...!

Cette semaine, très vraisemblablement en lien avec le conflit russo-ukrainien et l'intervention du Président Zelensky au Parlement, plusieurs attaques DDoS, des «*dénis de service distribués*» pour les non-initiés, ont rendu temporairement indisponibles divers services, notamment dans les villes de Lausanne, Zürich,

Liebe Leserinnen und Leser

Dies sind die **dV-News 12-2023** und eine Auswahl an [Artikel und Links](#).

Belagerte Schweiz - Endlich wach werden und auf Realismus setzen

Es gibt etwas, das wir bei *digiVolution* nicht gerne tun, nämlich zu sagen: «*Wir haben gewarnt*»! Im Zusammenhang mit dem Angriff auf die Firma XPLAIN schrieben wir vor zwei Wochen als Reaktion auf die Behauptung, dass keine Betriebsdaten offengelegt worden seien: «*Das wahre Ausmass wird sich später zeigen*». Und was für eine Überraschung... [solche Daten sind in die freie Wildbahn gelangt](#). Es ist nun die Aufgabe des [NCSC](#), den Schlammassel zu lösen, die übereilte und aufgrund unprofessioneller Kommunikation Richtigstellungen und Korrekturen zu veranlassen.

Die Firma Bobst gab im April bekannt, dass sie von einem Cyberangriff betroffen war, blieb aber optimistisch. «*Unsere Verteidigung war sehr effektiv*» und «*soweit wir wissen, haben wir keinen Datenverlust erlitten*». Am 9. Juni berichteten jedoch mehrere Medien, dass [sensible Daten](#) tatsächlich entwendet wurden und nun im Dark Web verfügbar sind. Hoffen wir, dass die [Gemeinde Bex](#) mehr Glück hatte...!

In dieser Woche, höchstwahrscheinlich im Zusammenhang mit dem russisch-ukrainischen Konflikt und der Rede von Präsident Zelensky im Parlament, führten mehrere DDoS-Angriffe, für Laien «*Distributed Denial of Service*» genannt, zu einer vorübergehenden



St-Gall, Fribourg et Bâle-Ville, ainsi que l'aéroport de Genève. Même la vénérable [Association Suisse des Banquiers](#) a été victime de la vague qui a déferlé sur la Suisse. Les conséquences sont apparemment limitées au dégât d'image et à la confiance dans nos institutions à assurer leur cybersécurité. Aurons-nous toujours autant de chance?

Une situation frustrante, car au moins une solution aurait drastiquement réduit l'impact de ces attaques. Il s'agit de [SCION](#) et du [Anapaya GATE](#), une solution suisse née à l'EPFZ, disponible depuis le début de l'année et qui protège notamment contre les DDoS en rendant les services invisibles pour les cybercriminels. Oui, la Suisse est le premier pays à disposer – pour autant qu'elle en fasse bon usage – d'une infrastructure Internet nationale capable d'augmenter massivement sa sécurité.

Si on considère le verre à moitié vide, oui les nombreux incidents du mois de juin font mal. Il est rageant de constater, après tout ce qui a été dit sur les cybermenaces, que des entités publiques et des entreprises importantes se fassent à ce point malmener et montrent même qu'elles ne savent pas où se trouvent leurs données et comment elles sont gérées... Et cela à 2 mois et demi de l'entrée en vigueur de la nouvelle loi?

Si on regarde au contraire le verre à moitié plein, les dégâts ont été heureusement limités et on ne peut qu'espérer qu'ils fassent office de *last wake up call* pour les dirigeants suisses. Malgré les critiques récurrentes et faciles, [l'administration fédérale](#) fait le boulot et s'améliore graduellement sous les impulsions d'un NCSC courageux, mais dont les moyens sont encore bien trop faibles. Cela devrait aller beaucoup plus vite, mais qui connaît la complexité des services de la Confédération et ses nombreux éléments hérités (les *legacy*) sait aussi le temps nécessaire pour opérer des changements de fond.

Alors oui il y aura toujours et encore des incidents et notre slogan chez [digiVolution](#) est

Nichtverfügbarkeit verschiedener Online-Dienste, insbesondere in den Städten Lausanne, Zürich, St-Gallen, Freiburg und Basel-Stadt, sowie am Genfer Flughafen. Sogar die ehrwürdige Schweizerische [Bankiervereinigung](#) wurde Opfer der Angriffswelle, die gegen die Schweiz schwappte. Die Folgen scheinen sich auf den Imageschaden und das Vertrauen in unsere Institutionen zu beschränken, ihre Cybersicherheit gewährleisten zu können. Werden wir weiterhin Glück haben?

Eine frustrierende Situation, denn zumindest eine bewährte Lösung hätte die Auswirkungen dieser Angriffe drastisch reduziert. Es ist [SCION](#) und das [Anapaya GATE](#), eine Schweizer Lösung, die an der ETH Zürich entwickelt wurde und die seit Anfang des Jahres verfügbar ist und insbesondere gegen DDoS schützt, indem es die Dienste für Cyberkriminelle unsichtbar macht. Ja, die Schweiz ist das erste Land, das – sofern es sie richtig nutzt – über eine nationale Internetinfrastruktur verfügt, die in der Lage ist, die Sicherheit massiv zu erhöhen.

Betrachtet man das Glas halb leer, so schmerzen die vielen Vorfälle im Juni. Es ist ärgerlich, dass nach allem, was über die Cyberbedrohung gesagt wurde, wichtige öffentliche Einrichtungen und Firmen immer noch so schlecht reagieren und sogar bewusst machen, dass sie nicht wissen, wo ihre Daten liegen und wie sie verwaltet werden... Und das zweieinhalb Monate vor dem Inkrafttreten des neuen Datenschutzgesetzes?

Wenn man das halbvolle Glas betrachtet, wurde der Schaden glücklicherweise begrenzt und man kann nur hoffen, dass es *the last wake up call* für die Schweizer Führungskräfte war. Trotz andauernder und stark vereinfachter Kritik macht die [Bundesverwaltung den Job](#) und verbessert sich laufend über Inputs eines mutigen NCSC, dessen Mittel wohl gemerkt immer noch viel zu gering sind. Es sollte viel schneller gehen, aber wer die Komplexität der Bundesdienste und ihre zahlreichen Legacy-Elemente kennt, weiss auch, wie



«Être cyberattaqué n'est pas honteux. C'est de ne pas s'y être préparé qui l'est !».

Nos recommandations sont simples. Il faut:

- enfin mettre en place PARTOUT les mesures connues et disponibles,
- PUNIR ceux qui ne mettent pas en place ces mesures dans des délais raisonnables (pour rappel, la négligence constitue un délit pénal),
- FORMER les décideurs et leurs états-majors à la gestion de crise et cesser de communiquer des informations qui s'avéreront fausses une fois les informations réelles disponibles. Il faut avoir le courage de dire «*je ne sais pas encore*».

À l'issue de ces deux semaines maudites, la Suisse se sent un peu comme le pont George Washington à New York dans la fumée des incendies qui ravagent le Canada. Ce serait bien d'agir avant que ce soit plus grave. Non?

lange es dauert, grundlegende Änderungen vorzunehmen.

Ja, es wird immer und immer wieder Zwischenfälle geben und unser Motto bei *digiVolution* lautet: **«Ein Cyberangriff zu erleiden ist keine Schande. Es ist eine Schande, nicht darauf vorbereitet zu sein!»**

Unsere Empfehlungen sind einfach. Es geht darum:

- endlich ÜBERALL die bekannten und verfügbaren Massnahmen umsetzen,
- diejenigen BESTRAFEN, die diese Massnahmen nicht innerhalb einer angemessenen Frist umsetzen (zur Erinnerung ist Fahrlässigkeit ein strafrechtliches Vergehen),
- Entscheidungsträger und ihre Stäbe in Krisenmanagement AUSBILDEN und keine Informationen mehr weitergeben, die sich als falsch erweisen, sobald die tatsächliche Realität vorliegt; man muss den Mut haben, «*Ich weiss es noch nicht*» zu sagen.

Am Ende dieser zwei verflixten Wochen fühlt sich die Schweiz ein wenig wie kürzlich die George-Washington-Brücke in New York während der Brandkatastrophe in Kanada an. Es wäre gut zu handeln, bevor es noch schlimmer wird. Nicht?



Pour ceux qui ne savent pas par où commencer, *digiVolution* disposent de compétences stratégiques de premier plan pour les accompagner.

Für diejenigen, die nicht wissen, wo sie anfangen sollen, verfügt *digiVolution* über erstklassige strategische Kompetenzen, um sie zu begleiten.



Avenir de la sécurité de la société numérique

Nous l'avons déjà écrit dans de précédents billets, si les prévisions sur la cybercriminalité se réalisent, en 2025 déjà les [dégâts à l'échelle mondiale atteindront près de 10'500 milliards \\$](#), soit 10% du produit mondial brut. Ramené à la Suisse, c'est comme si celle-ci jetait par la fenêtre 16 fois le budget de son armée et tout indique que la descente aux enfers n'est pas terminée. Tout simplement insupportable! Les USA semblent les seuls à avoir identifié et à vouloir briser cette spirale infernale [dont on connaît l'issue fatale depuis 50 ans](#). Même si les USA parviennent à leurs fins (en gros, il s'agit de *tordre les pouces* à toute une industrie de l'IT qui sort d'un demi-siècle de libéralisme), quand, ou et quel effet se fera-t-il sentir? Chez *digiVolution* nous réfléchissons à des solutions sociétales innovantes qui répondront à cette urgence et aux nombreux défis de la mutation numérique, notamment celle de [l'évolution démographique](#) dont les conséquences sont encore largement inconnues.

Pour cela **NOUS AVONS BESOIN D'AIDE MATÉRIELLE**. [Contactez-nous svp.](#)

Petit cyber-digest

Les sujets qui ont retenu notre attention durant les deux semaines écoulées.

- **Duplicité** - Peut-on encore croire les patrons des *géants de la tech*? La planète s'est émue parce que des industriels de renom se sont soudainement vu pousser des ailes d'éthique. Apparemment dépassés par leurs inventions ils ont appelé à une pause dans le développement de l'IA, alors que [dans les coulisses](#) certains poursuivaient de plus belle la fuite en avant. Un autre a témoigné [devant le Congrès américain](#) sur le danger absolu que représente l'IA et la nécessité de la réglementer. Mais 4 mois auparavant, il [prétendait l'exact contraire](#)

Zukunft der Sicherheit in der digitalen Gesellschaft

Wir haben es bereits in früheren Ausgaben vermerkt: Wenn die Prognosen zur Cyberkriminalität eintreffen, [wird sich der Schaden weltweit bereits 2025 auf fast 10,5 Billionen \\$](#) oder 10% des Bruttoweltprodukts belaufen. Auf die Schweiz bezogen ist das so, als ob sie das 16-fache ihres Armeebudgets aus dem Fenster werfen würde und alles deutet darauf hin, dass die Höllenfahrt noch nicht zu Ende ist. Einfach unerträglich! Die USA scheinen die einzigen zu sein, die diese Abwärtsspirale erkannt haben und sie durchbrechen wollen, [deren letale Auswirkung seit 50 Jahren bekannt ist](#). Selbst wenn die USA ihr Ziel erreichen (im Wesentlichen geht es darum, der gesamten IT-Industrie, die ein halbes Jahrhundert des Liberalismus hinter sich hat, an die Kandare zu nehmen), wann wird wo welcher Effekt spürbar sein? Bei *digiVolution* denken wir über innovative gesellschaftliche Lösungen nach, die dieser Dringlichkeit und den zahlreichen Herausforderungen der digitalen Mutation gerecht werden, insbesondere auch der [demographischen Entwicklung](#), deren Folgen noch weitgehend unbekannt sind.

Hierfür **BENÖTIGEN WIR MATERIELLE UNTERSTÜTZUNG**. [Bitte kontaktieren Sie uns.](#)

Kleines Cyberdigest

Die Themen, die uns in den vergangenen zwei Wochen beschäftigten.

- **Duplizität** - Kann man den Chefs der Tech-Giganten noch glauben? Die Welt ist in Aufruhr, weil führenden Industriellen plötzlich ethische Flügel gewachsen sind. Anscheinend von ihren Erfindungen überwältigt, forderten sie eine Pause bei der Entwicklung der KI, während [hinter den Kulissen](#) einige die Flucht nach vorn fortsetzten. Da erklärt einer dem [US-Kongress](#), welche absolute Gefahr die KI darstellt und wie notwendig ihre Regulierung ist. Vier Monate zuvor hatte er jedoch in einem Interview, das *auf wundersame Weise* aus dem



dans un interview qui a *miraculeusement* disparu de la Toile. Heureusement, [The Internet Archive](#) l'a retrouvé.

- **Inauguration du centre d'innovation UNLIMITRUST** - Le 6 juin dernier, la Suisse s'est enrichie d'un campus de premier plan grâce à [SICPA](#), leader mondial des encres de sécurité pour billets de banque et acteur majeur des solutions d'authentification, d'identification et de traçabilité sécurisées. [Unlimitrust](#) est le premier hub dédié à l'émergence de l'économie de la confiance, un domaine essentiel qui comme la résilience et la souveraineté ne cesse pourtant de se dégrader. En tout cas, il y a de quoi faire pour remonter la pente et avec Unlimitrust, SICPA offre à la Suisse un outil de très haute valeur. Merci.
- **Association FUTURS** - Le 13 juin, grâce à une brochette de passionnés menés par le Dr. Quentin Ladetto, responsable de la prospective chez armasuisse, est née cette association qui vise à promouvoir et développer la prospective, l'exploration d'idées émergentes et le rapport positif à l'incertitude. Une très belle soirée inaugurale, où tout le monde s'est pris aux jeux des questions qui avaient été préparées et la démonstration que [l'association futurs](#) relève d'un vrai besoin. Peut-être réussissons-nous (*digi*Volution en est déjà membre) à faire mentir la citation de Pierre Dac : «*La prévision est difficile surtout lorsqu'elle concerne l'avenir!*».
- **Einweihung des Innovationszentrums UNLIMITRUST** - Am 6. Juni wurde die Schweiz durch [SICPA](#), den Weltmarktführer für Sicherheitsdruckfarben für Banknoten und Hauptakteur für sichere Authentifizierungs- Identifizierungs- und Rückverfolgbarkeitslösungen, um einen erstklassigen Campus bereichert. [Unlimitrust](#) ist der erste Hub, der sich mit der Entstehung der Vertrauenswirtschaft befasst, einem wesentlichen Bereich, der wie die Resilienz und die Souveränität immer weiter abnimmt. SICPA bietet der Schweiz mit Unlimitrust ein sehr wertvolles Instrument an, um sich in die richtige Richtung zu entwickeln. Danke.
- **Der Verein FUTURS** - Am 13. Juni wurde dank einer Gruppe von Enthusiasten unter der Leitung von Dr. Quentin Ladetto, dem Verantwortlichen für prospektive Forschung bei armasuisse, diese Vereinigung gegründet, um die Zukunftsforschung, die Erforschung neuer Ideen und den positiven Umgang mit Ungewissheit zu fördern und zu entwickeln. Es war ein sehr schöner Abend, an dem die Insights zeigten, dass der [Verein futurs](#) einem echten Bedürfnis entspricht. Vielleicht gelingt es uns (*digi*Volution ist bereits Mitglied), das Zitat von Pierre Dac Lügen zu strafen: «*Prognosen sind schwierig, besonders wenn sie die Zukunft betreffen!*».

Futur^S



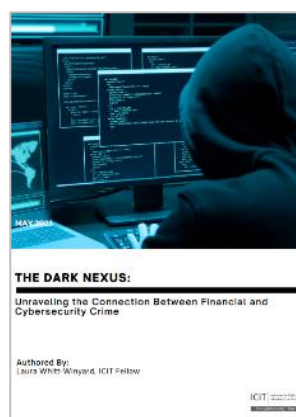
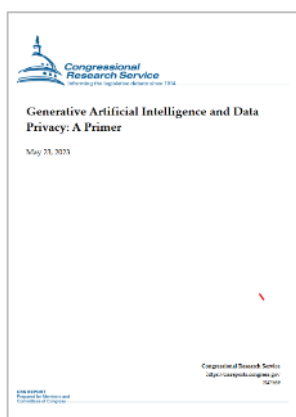
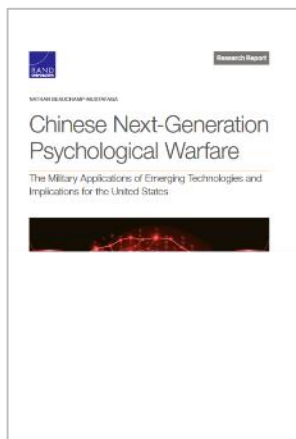


- **Vie privée** - Il y a 15 jours, nous nous inquiétons du projet de loi européenne présenté par le [gouvernement espagnol](#) qui exigerait des entreprises technologiques qu'elles analysent leurs plateformes à la recherche de contenu illégal et pour cela affaiblissent la cryptographie. La Suisse meilleur élève? Pas avec le [canton de Thurgovie](#) qui voulait introduire une disposition légale qui aurait permis à la police d'accéder, sans mandat, au téléphone portable de toute personne. Et comment seront gérées les données issues de la numérisation de la [vignette autoroutière](#)? Espérons que l'[enquête](#) sur l'utilisation par les grands acteurs économiques suisses des données de leurs clients permettra de faire un bout de chemin dans la bonne direction.
- **Privatsphäre** - Vor zwei Wochen waren wir besorgt über den Entwurf eines EU-Gesetzes, der von der [spanischen Regierung](#) vorgelegt wurde und von Technologieunternehmen verlangen würde, ihre Plattformen auf illegale Inhalte zu untersuchen und dafür die Kryptographie zu schwächen. Ist die Schweiz ein besserer Schüler? Nicht mit dem [Kanton Thurgau](#) der eine gesetzliche Bestimmung einführen wollte, die es der Polizei erlaubt hätte, ohne richterlichen Beschluss auf das Mobiltelefon jeder Person zuzugreifen. Und wie werden die Daten aus der Digitalisierung der [Autobahnvignette](#) verwaltet? Hoffen wir, dass die [Recherche](#) zur Nutzung der persönlichen Daten der Kunden durch grosse Schweizer Wirtschaftsakteure einen Schritt in die richtige Richtung bringt.

BOOKS & REPORTS

Voici les livres et publications d'intérêts découverts durant nos recherches des dernières deux semaines.

Hier sind die Bücher und Publikation von Interesse, die wir bei unseren Recherchen in den letzten zwei Wochen gefunden haben.





En bref - ▶ La CIA savait, grâce à la [Hollande](#), que les Ukrainiens envisageaient de saboter les gazoducs Nordstream. L'ont-ils fait? [Réponse de Dmitry Medvedev](#), ancien président de la Russie et vice-président du conseil de sécurité du Kremlin: « *Si nous partons de la complicité avérée des pays occidentaux dans la destruction des [gazoducs] Nordstream, nous n'avons plus aucune restriction, même morale, pour nous abstenir de détruire les câbles de communication de nos ennemis, posés au fond des océans* ». Encore un thème que nous avons traité dès les premiers jours de guerre ; la Suisse a-t-elle fait des planifications prévisionnelles si cela devait arriver? ▶ Aux USA une violation majeure de la sphère privée a été constatée et rapportée par [l'ODNI](#), l'Office de la directrice nationale du renseignement, Mme Avril Haines. Certes sur le fond un résultat peu surprenant, mais c'est son ampleur qui interpelle. La raison de tout cela? Les agences ne peuvent pas espionner les citoyens, alors... elles achètent les données au secteur privé.

Nous vous souhaitons une enrichissante découverte des [articles et liens](#) sélectionnés et nous réjouissons de vous retrouver bientôt.

In Kürze - ▶ Die CIA wusste dank [Holland](#), dass die Ukrainer planten, die Nordstream-Gaspipelines zu sabotieren. Haben sie das getan? [Antwort von Dmitry Medvedev](#), ehemaliger Präsident Russlands und stellvertretender Vorsitzender des Kreml-Sicherheitsrates: «*Wenn wir von der erwiesenen Komplizenschaft der westlichen Länder bei der Zerstörung der Nord Stream-Pipelines ausgehen, gibt es für uns keine Einschränkung, nicht einmal eine moralische, um davon abzusehen, die Kommunikationskabel unserer Feinde auf dem Meeresgrund zu zerstören*». Ein weiteres Thema, das wir seit den ersten Tagen des Krieges behandelt haben, ist die Frage, ob die Schweiz ihre Eventualplanung für den Fall eines solchen Ereignisses vorgenommen hat.

▶ In den USA wurde eine schwere Verletzung der Privatsphäre festgestellt und von [ODNI](#), dem Büro der Nationalen Direktorin für Nachrichtendienste, Frau Avril Haines, gemeldet. Die Ergebnisse sind zwar nicht überraschend, aber das Ausmass ist bemerkenswert. Was ist der Grund für all dies? Die Behörden können die Bürger nicht ausspionieren, also... kaufen sie die Daten vom Privatsektor.

Wir wünschen Ihnen viele lehrreiche Entdeckungen in den ausgewählten [Artikeln und Links](#) und freuen uns darauf, Sie bald wiederzusehen.



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 ; ils sont disponibles à l'adresse <https://www.digivolution.swiss/dv-blog>. 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; Sie finden diese unter <https://www.digivolution.swiss/dv-blog>. Interessierte finden auf dieser Seite auch den Link zur Anmeldung.