digiVolution
Prepare for the next

*d*V-News

Les billets de *digi*Volution / *digi*Volution's Newsletters
[10.04.2024 – Édition / Ausgabe Nr. 99]

Alarm!

Chers Lectrices et Lecteurs

Voici les ***d*V-News 08-2024** et leur sélection d'articles et liens. Dans cette édition nous voulons **sonner une fois encore l'alarme.** Deux faits récents motivent notre cri: les **statistiques de la cybercriminalité en Suisse** et **le cas *xz Utils***. Ces deux sujets structurent ce 99ème billet et illustrent l'urgence pour la Suisse de disposer d'une ***«vision pour une société sûre, résiliente et souveraine au temps de la mutation numérique»***. Cette proposition, chaque jour plus impérative, était déjà au cœur de notre commentaire sur le RAPOLSEC 21. Il n'a pas été entendu.

La Suisse doit élever le débat du numérique et se doter d'un solide et durable avantage stratégique. Cessons de n'être que des suiveurs !

Liebe Leserinnen und Leser

Hier sind die ***d*V-News 08-2024** und eine Auswahl an Artikeln und Links. In dieser Ausgabe schlagen wir erneut **Alarm**. Zwei jüngste Ereignisse sind Anlass für unseren Apell: die **Statistiken zur Cyberkriminalität in der Schweiz** und der **Fall *xz Utils***. Diese beiden Themen gestalten diesen 99. Beitrag und zeigen auf, wie dringend die Schweiz eine «***Vision für eine sichere, resiliente und souveräne Gesellschaft im Zeitalter der digitalen Mutation***» benötigt. Dieser täglich dringlichere Aufruf, stand bereits im Mittelpunkt unseres Kommentars zu SIPOL B 21. Er wurde nicht angehört.

Die Schweiz muss die Debatte hochfahren und sich einen soliden und nachhaltigen strategischen Vorteil verschaffen. Hören wir auf, nur Mitläufer zu sein!

Notre travail vous est utile? Il vous inspire? Merci de le soutenir par un DON.

Ist unsere Arbeit für Sie nützlich? Inspirierend? Bitte unterstützen Sie uns mit einer SPENDE.

digiVolution

TWINT

ALARM !

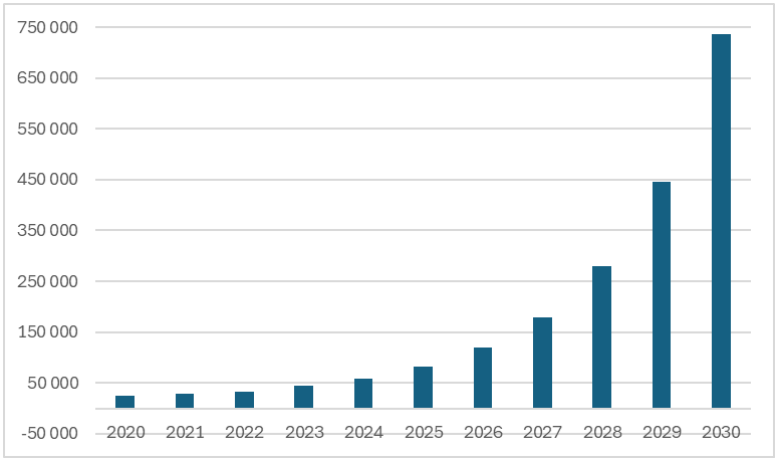
Depuis 2020 seulement, la Suisse dispose d'une statistique policière sur les cyberdélits. Lors de la première publication, l'Office fédéral de la statistique faisait état de 24'400 cas annoncés. En 2023, ce sont désormais 43'839 cas qui ont été rapportés par les forces de l'ordre, soit une augmentation de 80% en 4 ans. Entre 2022 et 2023, la progression a été de 31%. La plupart des délits sont de nature économique, avec 40'496 cas recensés, en hausse de 36,5% pour 2023. En cause, principalement l'escalade du phishing (+70%), l'utilisation frauduleuse de systèmes de paiement ou d'identités pour des escroqueries (+66%) et les arnaques liées aux petites annonces, où les objets payés ne sont pas livrés (+23,1%).

Prenons le risque de projeter une augmentation annuelle des cyberdélits de +5%. En 2030, la progression annuelle sera alors de +65% avec un total de près de 740'000 cyberdélits. Si cette progression se confirme, alors les chiffres qui seront publiés dans un an pour 2024 seront de 59'000 cas et de 83'000 pour 2025.

ALARM !

Erst seit 2020 gibt es in der Schweiz eine polizeiliche Statistik über Cyberkriminalität. Anlässlich der ersten Veröffentlichung meldete das Bundesamt für Statistik 24'400 Fälle. Im Jahr 2023 wurden 43'839 Fälle von den Strafverfolgungsbehörden gemeldet, was einem Anstieg von 80% innerhalb von 4 Jahren entspricht. Zwischen 2022 und 2023 betrug der Anstieg 31%. Die meisten Straftaten sind wirtschaftlicher Natur, mit 40'496 erfassten Fällen, was einem Anstieg von 36,5% bis 2023 entspricht. Die Hauptursachen sind die Zunahme von Phishing (+70%), die betrügerische Nutzung von Zahlungssystemen oder falsche Identitäten für Betrügereien (+66%) und Kleinanzeigenbetrug, bei dem bezahlte Objekte nicht geliefert werden (+23,1%).

Riskieren wir die Prognose eines jährlichen Anstiegs der Cyberkriminalität von +5%. Im Jahr 2030 würde der jährliche Anstieg damit +65% betragen, mit fast 740'000 Cyberdelikten. Wenn dieser Anstieg sich bestätigt, dann werden die Zahlen, die in einem Jahr für 2024 veröffentlicht werden, 59'000 Fälle betragen, 83'000 für 2025.



Exagéré? Alarmiste? Peut-être. En France, la progression depuis 2020 est de 400%. Selon Statista, la facture mondiale de la cybercriminalité atteindra 13'820 milliards $ en 2028, soit plus de 10% du PIB mondial. Et ce sont les pays riches qui seront le plus touchés. Selon le Bitkom, en 2022 ce sont 3.8% du PIB de

Übertrieben? Panikmachererei? Vielleicht. In Frankreich beträgt der Anstieg seit 2020 400%. Laut Statista werden die weltweiten Kosten für Cyberkriminalität bis 2028 auf 13'820 Mrd. Dollar ansteigen, was mehr als 10% des weltweiten BIP entspricht. Und es sind die reichen Länder, die am stärksten

l'Allemagne qui sont partis en fumée, soit 206 milliards €. Rapporté à la Suisse, c'est comme si nous avions en 2022 jeté par la fenêtre 5 fois le budget de l'armée. Quelle est la part due uniquement à la criminalité et celle due aux frictions géopolitiques et au *cyber in war*? Difficile à dire, mais les tensions mondiales croissantes ne vont pas réduire les risques.

Que traduisent ces chiffres? Une augmentation du nombre de cyberdélits ou du nombre d'annonces? Le reporting aux autorités pénales s'améliore, mais ces chiffres montrent sans aucun doute une augmentation des cyberdélits. Et ce n'est là que la pointe de l'iceberg, car la zone grise est importante. Il y a les cas non détectés et surtout les cas non annoncés. Selon le Département US de justice, seul un cas sur sept est annoncé aux autorités de poursuite pénale. Au moins 85% de la cybercriminalité reste ainsi cachée.

Ceux que ces chiffres dérangent trouveront toujours des excuses pour les relativiser et repousser les mesures qui s'imposent à plus tard, mais **la conclusion qui s'impose est que les cyberdéfenseurs sont en passe de perdre la bataille**. **Facture salée en vue!** Surtout avec l'accélération due à l'IA et à l'informatique quantique.

Depuis la création de *digi*Volution nous ne cessons d'alerter sur cette réalité, en insistant sur le besoin d'une approche holistique et systémique. En effet, les problèmes de sécurité de la société numérique ne sont pas que d'ordre technologique. Ils sont tout aussi largement provoqués par des problèmes politiques, de ressources humaines, matérielles ou énergétiques notamment.

Qu'est-ce qui est vraiment entrepris pour maîtriser cette **situation qui porte tous les symptômes d'une catastrophe annoncée**? Que faut-il faire pour que la Suisse se mette enfin à investir massivement dans de véritables solutions pour sa **sécurité à l'ère numérique?** Nous avons besoin de **beaucoup plus de nouvelles idées**.

betroffen sein werden. Die deutsche Branchenorganisation Bitkom schätzt, dass 2022 3,8% des deutschen BIPs vernichtet wurden, was 206 Mrd. € entspricht. Bezogen auf die Schweiz ist dies so, als hätten wir 2022 das Fünffache des Militärbudgets aus dem Fenster geworfen. Wie viel davon ist allein auf Kriminalität zurückzuführen und wie viel auf geopolitische Reibungen und *Cyber in war*? Schwer zu sagen, aber die zunehmenden weltweiten Spannungen werden die Risiken nicht verringern.

Was bedeuten diese Zahlen? Ein Anstieg der Cyberkriminalität oder der Anzeigen? Die Meldung an die Strafverfolgungsbehörden verbessert sich, aber diese Zahlen zeigen zweifelsohne eine Zunahme der Cyberkriminalität. Dies ist jedoch nur die Spitze des Eisbergs, denn die Grauzone ist gross. Es gibt nicht entdeckte Fälle und vor allem nicht gemeldete Fälle. Nach Angaben des US-Justizministeriums wird nur einer von sieben Fällen den Strafverfolgungsbehörden gemeldet. Mindestens 85% der Cyberkriminalität bleibt somit verborgen.

Diejenigen, die diese Zahlen bezweifeln, werden immer Ausreden finden, um sie zu relativieren und notwendige Massnahmen aufzuschieben, aber die **Schlussfolgerung ist, dass die Cyberverteidiger kurz davor stehen den Kampf zu verlieren. Eine hohe Rechnung in Sicht!** Insbesondere mit der Beschleunigung durch KI und Quantum Computing.

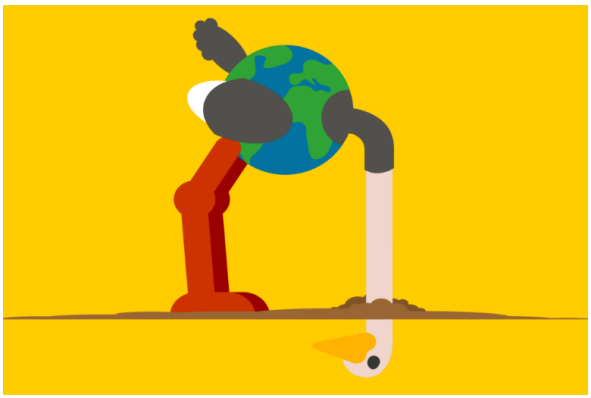
Seit der Gründung von *digi*Volution wurde immer wieder auf diese Fakten hingewiesen und die Notwendigkeit eines ganzheitlichen und systemischen Ansatzes betont. Die Sicherheitsprobleme der digitalen Gesellschaft sind nicht nur technologischer Art. Sie werden gleichermassen durch politische, personelle, materielle und energetische Probleme verursacht.

Was wird wirklich unternommen, um **diese Situation, die alle Symptome einer angekündigten Katastrophe aufweist**, unter Kontrolle zu bringen? Was muss getan werden, damit die

La confiance, la résilience et la souveraineté numériques ne se construiront pas à coup de slogans, mais d'actions concrètes. *digi*Volution répète depuis sa création que ce sont là des sujets STRATÉGIQUES, VITAUX et URGENTS. Et de nombreuses propositions ont été formulées. L'Occident craint le déferlement de hordes de blindés russes. Dans quelques années peut-être, mais **c'est maintenant que notre société est attaquée et de manière croissante là où elle est la plus faible, dans ses dépendances et vulnérabilités informationnelles et numériques**. Il serait temps de se réveiller, de regarder les problèmes en face et de mettre de véritables priorités.

Schweiz endlich massiv in echte Lösungen für ihre **Sicherheit im digitalen Zeitalter** investiert? Wir brauchen **viel mehr neue Ideen**.

Digitales Vertrauen, Resilienz und Souveränität werden nicht durch Schlagworte, sondern durch konkrete Massnahmen geschaffen. *digi*Volution hat seit ihrer Gründung immer wieder betont, dass dies STRATEGISCHE, LEBENSWICHTIGE und DRINGENDE Themen sind. Und es wurden viele Vorschläge gemacht. Der Westen fürchtet den Ansturm russischer Panzerhorden. Vielleicht in ein paar Jahren, aber **unsere Gesellschaft jetzt angegriffen, und zwar in zunehmendem Masse dort, wo sie am schwächsten ist, in ihren informationellen und digitalen Abhängigkeiten und Verwundbarkeiten.** Es ist Zeit, aufzuwachen, den Problemen ins Auge zu sehen und echte Prioritäten zu setzen.



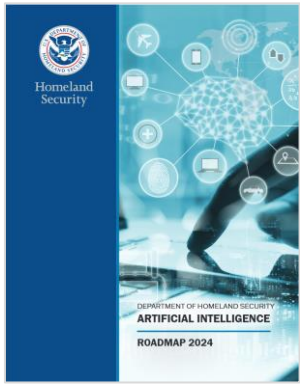
To prevent global catastrophe, governments must first admit there's a problem [link]

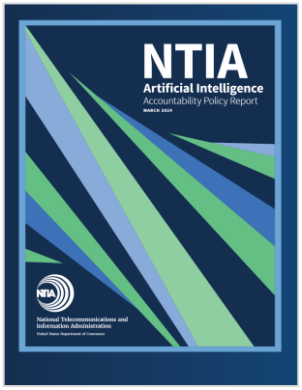
BOOKS & REPORTS

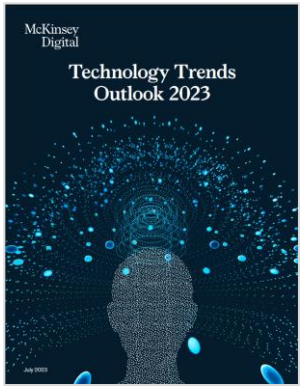
Voici la liste des livres et publications d'intérêt découverts lors de nos recherches durant les dernières semaines. Vous les retrouverez sur dVPedia à la rubrique dVLibrary.

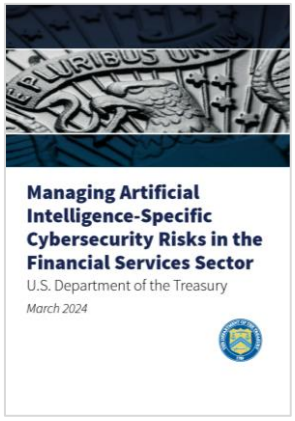
BOOKS & REPORTS

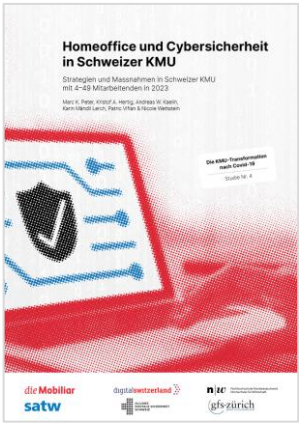
Dies ist eine Liste relevanter Bücher und Publikationen, auf die wir bei unseren Recherchen der letzten Wochen gestossen sind. Sie finden sie auf dVPedia unter dVLibrary.











Open Source – Who is responsible?

Nous avons souvent évoqué le thème de la souveraineté, c'est-à-dire la capacité d'une entité (individu, organisation, entreprise, État) à décider et à agir en toute autonomie, donc aussi à assumer la pleine responsabilité de ses actes. Le quasi-incident récent xz Utils nous a incité à nous intéresser à la question des **logiciels open source**.

Vous pensiez que derrière chaque ligne de code se trouve une entité juridiquement responsable? Oubliez! Diverses *communautés* mettent certes du temps et des compétences à disposition pour élaborer du code mis ensuite gracieusement à disposition du public… MAIS!

Lorsque des bénévoles vont nettoyer des ruisseaux envahis de déchets, s'ils oublient quelques emballages ou bouteilles en plastique, ce n'est certes pas propre, mais c'est sans conséquence systémique. Lorsqu'en revanche des bénévoles développent du code que personne ne contrôle vraiment et que ces briques technologiques se retrouvent partout, jusqu'au cœur de notre vie et à notre insu durant des décennies, **qui endosse quelle responsabilité en cas de dysfonctionnement?** Pourtant les conséquences peuvent être énormes.

Les passionnés de l'open Source argumentent volontiers que la *communauté* veille au grain et s'autocontrôle. Mais qui se cache derrière ce terme. Un *chevalier blanc*? Un *génie-zéro-défaut*? Il peut aussi s'agir de loups déguisés en brebis nourrissant l'ambition de

Open Source – Wer ist zuständig?

Wir haben oft über das Thema Souveränität gesprochen, d.h. die Fähigkeit einer Einheit (Einzelperson, Organisation, Unternehmen, Staat), selbständig zu entscheiden und zu handeln und somit die volle Verantwortung für ihre Handlungen zu übernehmen. Der jüngste Beinahe-Zwischenfall xz Utils hat uns dazu veranlasst, uns mit dem Thema **Open-Source-Software** zu befassen.

Dachten Sie, dass hinter jeder Code-Zeile eine rechtlich verantwortliche Instanz steht? Vergessen Sie es! Verschiedene *Communities* stellen zwar Zeit und Fachwissen zur Verfügung, um Code zu entwickeln, der dann der Öffentlichkeit kostenlos zur Verfügung gestellt wird... ABER!

Wenn Freiwillige einen mit Müll verschmutzten Bach reinigen und dabei ein paar Plastikverpackungen oder -flaschen übersehen, ist das zwar nicht sauber, aber es hat keine systemischen Folgen. Wenn jedoch Freiwillige Code entwickeln, den niemand wirklich kontrolliert, und wenn diese technologischen Bausteine überall zu finden sind, sogar mitten in unserem Leben und ohne unser Wissen über Jahrzehnte hinweg, **wer trägt dann die Verantwortung, wenn es schief geht?** Die Konsequenzen können enorm sein!

Die Liebhaber des freien Codes argumentieren gerne, dass die *Gemeinschaft* aufpasst und sich selbst kontrolliert. Aber wer verbirgt sich hinter diesem Begriff? Ein *weisser Ritter*? Ein *fehlerloses Genie*? Es kann sich auch um Wölfe im Schafspelz handeln, die den

glisser quelques lignes malveillantes dans des briques logicielles essentielles à Internet et que seuls connaissent quelques individus. C'est ce qui est arrivé dans le cas *xz Utils*.

Les géants de la tech emploient des centaines de milliers de personnes pour développer leurs produits. Ils consacrent des efforts croissants pour produire du code exempt de failles. Malgré cela leurs produits sont perclus de fautes et la situation ne semble pas s'améliorer dès lors que l'IA s'en mêle. Surtout si les géants de la tech eux-mêmes sont négligents en matière de sécurité. **Mais au moins sont-ils juridiquement responsables pour leurs produits.**

Les vulnérabilités sont (en principe) corrigées par les éditeurs au fur et à mesure des trouvailles. Beaucoup découvertes par nous, les *utilisateurs (payants) / bêta-testeurs*. Lorsqu'un patch est publié, il est impératif de le déployer au plus vite dans sa propre infrastructure, car les malveillants lisent aussi les publications sur les vulnérabilités et leurs correctifs ; ils savent donc en même temps que nous quand notre sécurité est compromise. Malheureusement il est courant qu'entreprises comme particuliers mettent des jours, des mois, parfois même des années avant de réagir. Et pendant ce temps, les vilains se baladent !

Et dans le monde de l'open source, cela se passe comment? Quels sont les processus? Qui est responsable? Il est fort probable qu'il n'y ait personne au bout du fil. Et est-ce que la *communauté* produit moins de bugs que l'industrie? Comme le démontre le cas *xz Utils*, une collection de librairies sous Linux et de nombreux systèmes Unix pour compresser les données, **l'open source n'est pas immunisé contre les bugs et ceux-ci peuvent être fortuits, mais aussi intentionnels**.

Le hasard a voulu qu'un programmeur découvre une porte dérobée installée par une main probablement étatique dans une de ces briques logicielles ignorées du grand public, mais déployées à l'échelle mondiale pour la

Ehrgeiz haben, ein paar bösartige Zeilen in Softwarebausteine einzufügen, die für das Internet unerlässlich sind und nur wenigen Personen bekannt sind. Dies geschah im Fall von *xz Utils*.

Die Tech-Giganten beschäftigen Hunderttausende von Menschen, um ihre Produkte zu entwickeln. Sie unternehmen immer grössere Anstrengungen, um fehlerfreien Code zu produzieren. Trotzdem sind ihre Produkte fehlerhaft und die Situation dürfte sich nicht verbessern, sobald die KI ins Spiel kommt. Insbesondere wenn die Tech-Giganten in Bezug auf die Sicherheit selber nachlässig sind. **Aber zumindest sind sie rechtlich verantwortlich für ihre Produkte.**

Die Schwachstellen werden (in der Regel) von den Herstellern gepatcht, sobald sie gefunden werden. Viele davon wurden von uns, den (zahlenden) Nutzern/Betatestern, entdeckt. Sobald ein Patch veröffentlicht wird, ist es zwingend erforderlich, ihn so schnell wie möglich in der eigenen Infrastruktur umzusetzen, da auch böswillige Angreifer die Veröffentlichungen über Sicherheitslücken und ihre Patches lesen und daher zur gleichen Zeit wie wir wissen, wann unsere Sicherheit kompromittiert ist. Leider ist es üblich, dass sowohl Unternehmen als auch Privatpersonen Tage, Monate, sogar Jahre brauchen, um zu reagieren. Und unterdessen sind die Bösen unterwegs!

Wie sieht es in der Welt der Open Source aus? Wie laufen die Prozesse ab? Wer ist verantwortlich? Es ist sehr wahrscheinlich, dass es niemanden gibt, der am anderen Ende der Leitung sitzt. Und produziert die *Community* weniger Fehler als die Industrie? Nichts ist weniger sicher. Wie der Fall *xz Utils*, eine Sammlung von Bibliotheken unter Linux und vielen Unix-Systemen zur Datenkomprimierung, zeigt, ist **Open Source nicht gegen Fehler immun und diese können sowohl zufällig als auch beabsichtigt sein**.

Der Zufall wollte es, dass ein Programmierer ein Backdoor entdeckte, die von einer

maintenance des serveurs. Ce logiciel produit par quelques bénévoles a été manipulé et s'est trouvé à un cheveu d'être distribué avec des fonctions malveillantes. Les concepteurs de cette faille auraient pu ensuite, sans opposition, accéder à un nombre incalculable de systèmes, dans le monde entier.

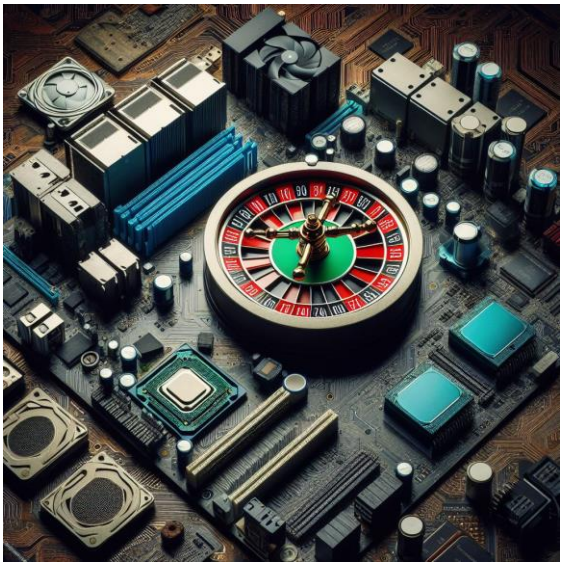
Qui est responsable de la qualité de ces logiciels *libres*? Savez-vous qu'en surfant sur le net avec vos processus les plus vitaux, ceux-ci dépendent d'un socle dont vous ne savez rien, pour lequel personne n'est officiellement en charge, contrôlé et comptable en cas d'incident ?

S'exprimant sur ce cas *xz Utils* le «pape» de la cybersécurité, Bruce Schneier, parle de chance que cette porte dérobée ait pu être découverte à temps. Mais il écrit également qu'il ne s'agit certainement pas d'un cas isolé. **Mais peut-on subordonner la sécurité de nos processus vitaux à des amateurs, à la chance ou à la roulette?**

vermutlich staatlichen Hand in einem der Softwarebausteine installiert worden war, der der Öffentlichkeit nicht bekannt sind, aber weltweit zur Wartung von Servern eingesetzt wird. Diese von einigen Freiwilligen erstellte Software wurde manipuliert und war nur eine Haarbreite davon entfernt, mit bösartigen Funktionen verbreitet zu werden. Die Entwickler dieser Schwachstelle hätten sich dann ohne Widerstand Zugang zu unzähligen Systemen auf der ganzen Welt verschaffen können.

Wer ist für die Qualität dieser *freien* Software verantwortlich? Wissen Sie, dass, wenn Sie mit Ihren wichtigsten Prozessen im Internet surfen, diese von einer digitalen Basis abhängen, von der Sie nichts wissen, für die niemand offiziell verantwortlich ist, von niemanden kontrolliert wird und der im Falle eines Vorfalls niemand zur Rechenschaft gezogen wird?

Der «Papst» der Cybersicherheit, Bruce Schneier, sprach in Bezug auf den Fall *xz Utils* vom Glück, dass die Hintertür rechtzeitig entdeckt wurde. Er schreibt jedoch auch, dass dies sicherlich kein Einzelfall ist. **Aber können wir die Sicherheit unserer lebenswichtigen Prozesse von Amateur, dem Zufall oder dem Roulette überlassen?**



Finissons sur un peu d'humour: en informatique on connaissait les Easter eggs. Maintenant il y a les cyberpoissons d'avril.

C'est tout pour cette édition. Nous espérons qu'elle vous a plu. Nous vous souhaitons une enrichissante découverte des articles et liens sélectionnés et vous retrouverons dans 15 jours.

Merci de souscrire à dVPedia et ainsi de soutenir son développement au profit de tous.

Und zum Schluss, ein wenig Humor: in der Informatik kennt man die Easter Eggs. Jetzt gibt es auch die Cyberaprilscherze.

Das war's für diese Ausgabe. Wir wünschen Ihnen viele lehrreiche Erkenntnisse mit den ausgewählten Artikeln und Links und sehen uns in zwei Wochen wieder.

Bitte registrieren Sie sich für dVPedia und unterstützen Sie damit seine Entwicklung zum Nutzen aller.

[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. 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.*