Les billets[i] de *digi*Volution / *digi*Volution's Newsletters
[03.07.2023 – Édition / Ausgabe Nr. 79]

Tipping point?

Chers Lectrices et Lecteurs

Voici les ***d*V-News 12-2023** et leur sélection d'articles et liens.

Point de bascule, tournant, seuil critique, moment charnière, point de rupture…

À la suite de la vague de cyberattaques récemment subies par la Suisse (et ce n'est certainement pas terminé), des menaces proférées par M. Medvedev de s'attaquer aux câbles sous-marins en représailles aux sabotages de Nord Stream, des nombreuses pénuries qui menacent la chaîne d'approvisionnement, à commencer par l'énergie électrique pour l'hiver prochain, de la facture toujours plus insupportable de la cybercriminalité, l'image globale de l'espace numérique est pour le moins inquiétante.

Nombreuses sont les situations qui pourraient devenir critiques et, en se combinant entre elles, *simplement* dégénérer. Si l'on considère l'amoncellement de nuages numériques noirs pesant sur la société, il est difficile de déborder d'optimisme. Pourtant la plupart des individus et des organisations se comportent encore comme s'ils ne voyaient pas cette situation. Étrange quand on sait le coût moyen d'un cyberincident et leurs conséquences visibles et invisibles. D'ailleurs quel sera le coût total réel de la cyberattaque contre Xplain?

Ce cas permet une fois encore de mettre en évidence une réalité incontournable en cybersécurité: l'anticipation est reine, mais sans cartographie précise du présent et du passé avec leurs vulnérabilités et héritages, aucune

Liebe Leserinnen und Leser

Dies sind die ***d*V-News 12-2023** und eine Auswahl an ausgewählten Artikeln und Links.

Wendepunkt, Scheideweg, kritische Schwelle, Knackpunkt, Zäsur…

Nach der jüngsten Welle von Cyberangriffen auf die Schweiz (und es ist sicherlich noch nicht zu Ende), Medvedevs Drohungen, als Vergeltung für die Nord Stream-Sabotage Unterseekabel anzugreifen, den zahlreichen Engpässen in der Versorgungskette, angefangen bei der Stromversorgung im nächsten Winter, und den immer unerträglicheren Konsequenzen der Cyberkriminalität ist das Gesamtbild des digitalen Raums, gelinde gesagt, beunruhigend.

Es gibt viele Situationen, die kritisch werden und in Kombination miteinander *einfach* eskalieren könnten. Wenn man bedenkt, wie viele dunkle digitale Wolken über der Gesellschaft schweben, ist es schwer, optimistisch zu sein. Dennoch verhalten sich die meisten Menschen und Organisationen so, als ob sie diese Lage nicht sehen würden. Das ist seltsam, wenn man bedenkt, wie hoch die durchschnittlichen Kosten eines Cybervorfalls sind und ihre sichtbaren und unsichtbaren Konsequenzen. Und wie hoch werden die Gesamtkosten des Cyberangriffs auf Xplain tatsächlich sein?

Dieser Fall zeigt wieder einmal eine unumgängliche Realität in der Cybersicherheit auf: Antizipation ist alles, aber ohne genaue Kartografie der Gegenwart und der Vergangenheit

analyse de risques ni stratégie crédible et durable ne peut être élaborée. Non seulement l'échec est programmé, mais en cas d'incident un cauchemar attend aussi les responsables qui ne savent pas où commencer. Et c'est du vécu, croyez-nous !

Bien entendu que l'écosystème numérique suisse dispose de nombreux atouts, mais il nous paraît toujours plus impératif et urgent de répondre au risque de *tipping point* pouvant naître de la conjonction de tous ces défis. Quelles réponses la société, et notre pays en particulier, veut-elle apporter à cette situation? Dans ce billet nous n'en avons mentionné que quelques-uns, mais la liste est longue et l'attentisme actuel, ce manque de volonté collective de vraiment les prendre à bras le corps, nous paraît particulièrement irresponsable. Nous sommes assis sur une bombe à retardement dont nous avons par ailleurs une connaissance très imparfaite, une sorte de «*faille de San Andreas numérique*», mais nous continuons à faire comme si cela n'avait pas d'importance. En fait il manque une réflexion de fond sur la société numérisée. Voulons-nous corriger cela avant d'atteindre le point de rupture? Actuellement ce que faisons s'appelle une *fuite numérique en avant*.

mit ihren Verwundbarkeiten und Altlasten kann keine glaubwürdige und nachhaltige Risikoanalyse und Strategie entwickelt werden. Der Misserfolg ist dann nicht nur vorprogrammiert, sondern im Falle eines Zwischenfalls erwartet die Verantwortlichen ein Albtraum, da sie nicht wissen, wo sie anfangen sollen. Und das ist die Realität; glaub uns!

Natürlich hat das digitale Ökosystem der Schweiz viele Stärken, aber es wird immer wichtiger und dringender, dass wir auf die Gefahr eines *Tipping Point* eingehen, der durch das Zusammentreffen all dieser Herausforderungen entstehen könnte. Wie will die Gesellschaft, und unser Land im Besonderen, auf diese Lage antworten? In diesem Beitrag haben wir nur einige wenige genannt, aber die Liste ist lang und die derzeitige abwartende Haltung, der fehlende kollektive Wille, diese Probleme wirklich anzugehen, erscheint uns besonders unverantwortlich. Wir sitzen auf einer tickenden Zeitbombe, über die wir im Übrigen nur sehr unvollkommen Bescheid wissen, einer Art «*digitalem San Andreas Graben*», aber wir tun weiterhin so, als ob das keine Rolle spielt. Eigentlich fehlt ein grundlegendes Nachdenken über die digitalisierte Gesellschaft. Wollen wir es korrigieren bevor wir den Punkt des Zusammenbruchs erreichen? Was wir derzeit, tun heisst eine *digitale Flucht nach vorn*.

Source : https://marketoonist.com/2023/06/impact-of-chatgpt.html

Petit *cyber-digest*

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

- **XPLAIN** - De nombreux détails sur la cyberattaque qui a affecté cette firme d'Interlaken sont désormais connus. Et plus on creuse, pire semble être la situation avec désormais des données sensibles sur des affaires judiciaires et sur des personnes, dont nos conseillers fédéraux. Ce n'est pas reluisant et nécessite désormais un état-major de crise politico-stratégique « fuite de données ». Espérons que cette débâcle sera pour la Suisse le même électrochoc que celui vécu en 2007 par l'Estonie devenue depuis *premier de classe cyber*. Et soyons clairs, cette fois un petit peu de *cybercosmétique* ne suffira pas. C'est un chantier national qu'il faut entreprendre à tous les étages. Fini de se croire encore épargné et de ricaner quand d'autres se font avoir? La Suisse doit passer au minimum la vitesse supérieure.
- **Droits fondamentaux** – Le 19 juin dernier, le canton de Genève a approuvé à 94% l'inscription dans sa constitution d'un droit à l'intégrité numérique. Un pas historique qui, on l'espère, trouvera rapidement son pendant dans la Constitution fédérale.
- **Dossier électronique du patient (DEP)** – Sur le principe, il est bien entendu louable que le Conseil fédéral mette la pression. Il reste toutefois de nombreuses questions sans réponse dans ce secteur «atomisé» en une multitude d'intervenants et 26 cantons. Les cas récemment portés à l'attention du public montrent que la cybersécurité dans ce secteur est faible alors qu'il est une cible privilégiée de criminels que la souffrance de leurs victimes laisse insensible. Exiger les meilleurs standards et les fixer dans la loi est bien évidemment impératif (*what else?*), mais cela ne constitue aucunement une garantie. Et *quid* de la synchronisation avec l'identité électronique? Qui aura (dans

Kleines *Cyberdigest*

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

- **XPLAIN** - Viele Details des Cyberangriffs auf die Firma aus Interlaken sind nun bekannt. Und je tiefer man gräbt, desto schlimmer scheint die Situation zu werden, da nun sensible Daten über Gerichtsfälle und Personen, darunter auch unsere Bundesräte, bekannt werden. Das ist nicht schön und erfordert nun einen politisch-strategischen Krisenstab «Datenabfluss». Hoffentlich wird dieses Debakel der Schweiz einen ähnlichen Schock versetzen, wie Estland 2007, das seitdem *Cyberklassenbester* geworden ist. Und seien wir ehrlich: Ein bisschen Cyberkosmetik wird dieses Mal nicht ausreichen. Es ist ein nationales Projekt, das auf allen Ebenen in Angriff genommen werden muss. Es ist vorbei mit dem Glauben, noch verschont zu sein und zu kichern, wenn andere getroffen werden. Die Schweiz muss mindestens einen Gang höher schalten.
- **Grundrechte** – Am 19. Juni hat der Kanton Genf mit 94% Zustimmung ein Recht auf digitale Integrität in seiner Verfassung verankert. Ein historischer Schritt, der hoffentlich bald auch in der Bundesverfassung seine Spiegelung finden wird.
- **Elektronisches Patientendossier (EPD)** - Im Prinzip ist es natürlich lobenswert, dass der Bundesrat Druck ausübt. Es gibt aber noch viele unbeantwortete Fragen in diesem Sektor, der durch eine Vielzahl von Akteuren und 26 Kanonen «atomisiert». Die kürzlich bekannt gewordenen Fälle zeigen, dass die Cybersicherheit im Gesundheitssektor tief ist, obwohl er ein bevorzugtes Ziel von Kriminellen ist, die das Leid ihrer Opfer nicht berührt. Die besten Standards zu fordern und sie gesetzlich zu verankern ist natürlich ein Muss (*what else?*), aber es ist keine Garantie. Und was ist mit der Synchronisation mit der e-ID? Wer wird (im Detail und nicht nur

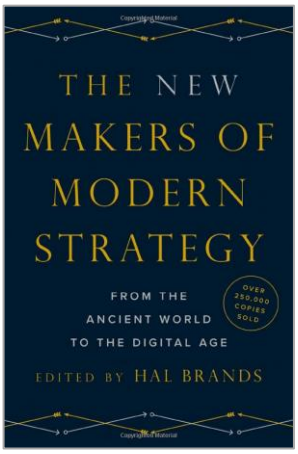
le détail et pas simplement « les professionnels de santé » et «pour les besoins de la recherche») et comment accès à ces données? Et seront-elles centralisées? Car en cas de grosse attaque, le secteur entier de la santé risque la panne systémique…

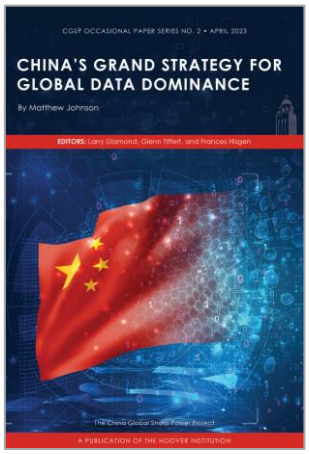
«Gesundheitsprofis» und «für Forschungszwecke») und wie Zugang zu diesen Daten haben? Und werden sie zentralisiert? Denn im Falle eines Grossangriffs droht dem gesamten Gesundheitssektor ein systemischer Ausfall…

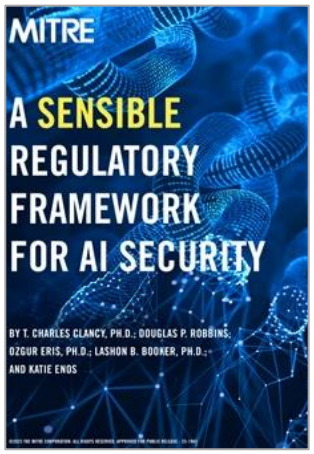
BOOKS & REPORTS

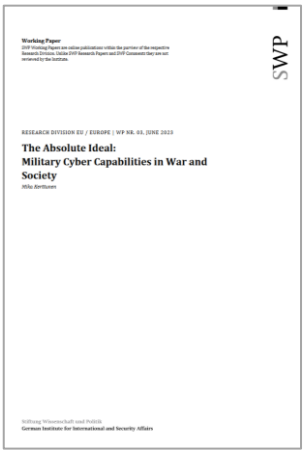
Voici les livres et publications d'intérêts découverts durant nos recherches des dernières deux semaines.

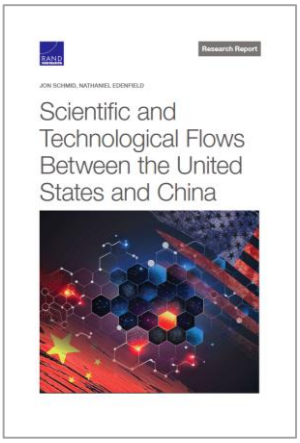
Hier sind die Bücher und Publikation von Interesse, die wir bei unseren Recherchen in den letzten zwei Wochen gefunden haben.

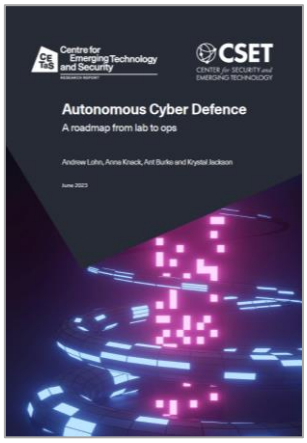


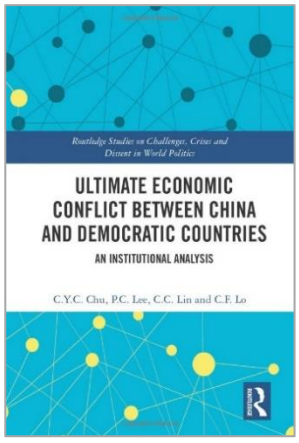












En bref – ▸La Chine est confirmée comme principale source des attaques *Advanced Persistant Threats* APT. Lors du premier trimestre 2023, elle aurait été responsable de 79% des attaques d'origine étatique. Le rapport de juin du Trellix Advanced Research met notamment en évidence une augmentation des attaques contre les secteurs de la finance, des télécommunications et de l'énergie. ▸Le U.S.

In Kürze – ▸China ist als Hauptquelle für APT-Angriffe (*Advanced Persistant Threats*) bestätigt. Im ersten Quartal 2023 soll sie für 79% der Angriffe aus staatlichen Quellen verantwortlich sein. Der Bericht von Trellix Advanced Research vom Juni zeigt eine Zunahme von Angriffen auf den Finanz-, Telekommunikations- und Energiesektor. ▸Das U.S. Government Accountability Office GAO stellt fest, dass die

Government Accountability Office GAO constate quant à lui que la numérisation est présente dans tous les processus et opérations de fabrication et de contrôle industriel des armements nucléaires, mais que la *National Nuclear Security Administration* NNSA et ses sous-traitants n'en sont qu'aux premiers stades des efforts nécessaires, même après plusieurs années. *Intéressante* perspective pour un pays traditionnellement attaqué de toutes parts et détenteur de 5'500 armes nucléaires…

Après les attaques contre Colonial Pipeline et SolarWinds, voici de quoi relativiser (un petit peu) certaines attaques virulentes contre la cybersécurité en Suisse!

Nous vous souhaitons une enrichissante découverte des articles et liens sélectionnés et nous réjouissons de vous retrouver bientôt.

Digitalisierung alle Prozesse und Vorgänge bei der Herstellung und industriellen Kontrolle von Atomwaffen durchdringt, dass die *National Nuclear Security Administration* NNSA und ihre Lieferanten jedoch auch nach mehreren Jahren noch in einem frühen Stadium der notwendigen Anstrengungen sind. Dies ist eine *interessante* Perspektive für ein Land, das traditionell von allen Seiten angegriffen wird und 5'500 Atomwaffen besitzt...

Nach den Angriffen auf die Colonial Pipeline und SolarWinds, das relativiert (ein wenig) einige der heftigen Angriffe auf die Cybersicherheit in der Schweiz.

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.*