Les billets[i] de *digi*Volution / *digi*Volution's Newsletters
[31.01.2022 – 43ème édition]

cyberimmaturity.ch?

Chers Lectrices et Lecteurs,

Nous avons le plaisir de vous adresser les ***d*V-News 03-2022** et leur sélection d'articles et de liens pour illustrer l'actualité de la dernière quinzaine et inspirer vos réflexions. Comme annoncé dans notre précédent billet, le *Bulletin of the Atomic Scientists* a tenu sa conférence annuelle le 20 janvier. Bonne nouvelle, l'horloge de l'apocalypse n'a pas changé par rapport à 2020 et 2021. Mais … le record établi en 2020 – à 100 secondes des *portes du destin* – reste inchangé, une situation préoccupante qui n'étonnera pas ceux qui observent les tensions du monde. Et la cyberattaque contre le CICR n'est que la terrible démonstration que dans le cyberespace, même les valeurs les plus fondamentales sont à nouveau violées.

Liebe Leserinnen und Leser!

wir freuen uns, Ihnen die dV-News 03-2022 und eine Auswahl an Artikeln und Links zukommen zu lassen, die die Nachrichten der letzten zwei Wochen widerspiegeln und Sie zum Nachdenken anregen sollen. Wie in unserem letzten Beitrag angekündigt, hielt das Bulletin of the Atomic Scientists am 20. Januar seine Jahreskonferenz ab. Gute Nachrichten: Die Weltuntergangsuhr hat sich im Vergleich zu den Jahren 2020 und 2021 nicht verändert. Aber ... der 2020 aufgestellte Rekord – 100 Sekunden von den *Toren des Schicksals* entfernt – bleibt unverändert, eine besorgniserregende Situation, die diejenigen, die die Spannungen in der Welt beobachten, nicht überraschen wird. Und der Cyberangriff auf das IKRK ist nur ein schrecklicher Beweis dafür, dass im Cyberraum selbst die grundlegendsten Werte wieder verletzt werden.

Dans notre précédent billet, nous nous sommes interrogés sur l'état du monde. Intéressons-nous cette fois à quatre facteurs pour illustrer le **degré de cyberimmaturité de la Suisse** alors que notre

In unserem letzten Beitrag haben wir uns über den Zustand der Welt Gedanken gemacht. Dieses Mal wollen wir uns auf vier Faktoren konzentrieren, um den **Grad der Cyberunreife der Schweiz**

pays dispose de moyens et de compétences largement au-dessus de la moyenne internationale.

Responsabilité numérique des entreprises – Avant la publication du rapport de la fondation Ethos, ceux qui pensaient encore que les grandes entreprises suisses géraient plutôt bien la digitalisation en ont pris pour leur grade. En effet, sur les 48 plus grandes sociétés cotées au SMI, seules 12 ont répondu au questionnaire, un exercice qui a par ailleurs mis en évidence le manque de cartographie de leurs propres *assets*. Notre économie est-elle aux mains de cybersomnambules? Quel est l'état réel des 617'655 autres entreprises? Est-ce mesurable? Pourrions-nous trouver de l'inspiration dans le modèle – même s'il est imparfait – du Pentagone? Nos assurances ne seraient certainement pas les moins intéressées.

Bases légales – Alors que les USA et l'UE mettent les bouchées doubles, près de 5 ans après l'intervention parlementaire qui a réclamé au Conseil fédéral de se pencher sur la question, nous n'avons toujours pas d'obligation pour les opérateurs d'infrastructures critiques d'annoncer des cyberattaques. Pourtant celles-ci pourraient avoir de terribles conséquences pour la société et l'économie. S'agissant des médias sociaux, l'UE vient de mettre en place un ambitieux dispositif pour encadrer les VLOP's (*Very Large Online Platforms*). En Suisse, les questions du Parlement (1, 2) à ce sujet restent sans réponses crédibles. S'alignera-t-on une fois encore et avec des années de retard sur l'UE? Avec quels dégâts d'ici là?

Protection des données – Avec sa loi sur la protection des données, notre pays a juste réussi, après des années de tergiversations, à réinventer la roue. Mais en moins bien que l'EU et son RGPD que presque toutes les entreprises suisses doivent appliquer, leurs principaux clients étant européens. A ce sujet, Le Temps relayait en 2018 une lettre ouverte au titre sans ambiguïté: "*Nous mettons en danger l'économie suisse*". Vendredi, ce même quotidien titrait : "*Les préposés suisses à la protection des données crient au secours - Moyens dérisoires, demandes qui explosent, course face à la numérisation… Vendredi, les*

zu veranschaulichen, obwohl unser Land über Mittel und Kompetenzen verfügt, die weit über dem internationalen Durchschnitt liegen.

Digitale Verantwortung der Unternehmen – Wer vor der Veröffentlichung des Berichts der Ethos Stiftung noch glaubte, dass die grossen Schweizer Unternehmen die Digitalisierung recht gut bewältigen, wurde eines Besseren belehrt. Denn von den 48 grössten im SMI kotierten Unternehmen haben nur 12 den Fragebogen beantwortet, eine Übung, die ausserdem den Mangel an einer Übersicht ihrer eigenen *Assets* aufzeigte. Ist unsere Wirtschaft in den Händen von Cybersschlafwandlern? Wie ist der tatsächliche Zustand der anderen 617'655 Unternehmen? Ist das messbar? Könnten wir uns von dem – wenn auch unvollkommenen – Modell des Pentagons inspirieren lassen? Unsere Versicherungen wären sicherlich nicht am wenigsten interessiert.

Rechtsgrundlagen – Während die USA und die EU mit Hochdruck daran arbeiten, haben wir fast fünf Jahre nach dem parlamentarischen Vorstoss, der den Bundesrat aufforderte, sich mit dieser Frage zu befassen, immer noch keine Meldepflicht für die Betreiber kritischer Infrastrukturen bei Cyberangriffen. Dabei könnten diese schreckliche Folgen für die Gesellschaft und die Wirtschaft haben. Was die sozialen Medien betrifft, so hat die EU gerade ein ehrgeiziges System zur Regulierung von VLOPs (*Very Large Online Platforms*) eingeführt. In der Schweiz bleiben die Anfragen des Parlaments dazu (1, 2) ohne glaubwürdige Antworten. Wird man sich wieder einmal und mit jahrelanger Verspätung an die EU anpassen? Mit welchem Schaden bis dahin?

Datenschutz – Mit seinem Datenschutzgesetz hat es unser Land nach jahrelangem Zögern gerade noch geschafft, das Rad neu zu erfinden. Aber nicht so gut wie die EU und ihre DSGVO, die fast alle Schweizer Unternehmen anwenden müssen, da ihre wichtigsten Kunden aus Europa kommen. Zu diesem Thema berichtete Le Temps 2018 über einen offenen Brief mit dem unmissverständlichen Titel "*Wir bringen die Schweizer Wirtschaft*

préposés romands à la protection des données ont dressé un tableau sombre de la situation". Et n'oublions pas le dossier enlisé de l'identité numérique. Quant à Alibaba, auquel le Conseil fédéral veut confier le stockage de nos données, la prochaine passe d'armes est programmée. Et pour ceux qui l'ont manqué, nous recommandons le film d'Arte récemment diffusé "Les nouveaux soldats de la Chine", en espérant qu'il contribuera à faire bouger les mentalités.

Dimension stratégique – Nous avons déjà plusieurs fois fait part de nos réserves sur le rapport de politique de sécurité du Conseil fédéral. A lire la version finale, notre constat est simple: "consultation = exercice alibi". Le dernier article de Bruno Lezzi dans la NZZ ne dit pas autre chose. Espérons que la stratégie britannique de cybersécurité centrée sur une réponse "*whole of society*" fera des émules et aidera la Confédération à sortir de ses silos. L'hyperconnexion fait en effet de chaque entité de la société (individus, entreprises, communes, etc.) un contributeur à la cybersécurité collective. Et pour y parvenir, un effort massif avec de véritables priorités dans les budgets et les agendas s'impose, en particulier en matière de formation. Ainsi seulement la caricature de Chapatte perdra de son hyperréalisme.

in Gefahr". Am Freitag titelte dieselbe Zeitung: "*Schweizer Datenschutzbeauftragte rufen um Hilfe - Geringe Mittel, explodierende Anfragen, Wettlauf mit der Digitalisierung... Am Freitag zeichneten die Datenschutzbeauftragten der Romandie ein düsteres Bild der Situation*". Und vergessen wir nicht das festgefahrene Dossier der digitalen Identität. Was Alibaba betrifft, dem der Bundesrat die Speicherung unserer Daten anvertrauen will, ist der nächste Waffengang vorprogrammiert. Und für diejenigen, die ihn verpasst haben, empfehlen wir den kürzlich ausgestrahlten Arte-Film "Chinas neue Soldaten" in der Hoffnung, dass er dazu beiträgt, das Bewusstsein der Leute zu schärfen.

Strategische Dimension – Wir haben bereits mehrfach unsere Vorbehalte gegenüber dem Sicherheitspolitischen Bericht des Bundesrates geäussert. Wenn man die endgültige Version liest, ist unsere Feststellung einfach: "Konsultation = Alibiübung". Der letzte Artikel von Bruno Lezzi in der NZZ sagt nichts anderes. Es bleibt zu hoffen, dass die britische Cybersicherheitsstrategie, die sich auf einen "*whole of society*"-Ansatz konzentriert, Nachahmer findet und dem Bund hilft, aus seinen Silos auszubrechen. Die Hypervernetzung macht nämlich jede Einheit der Gesellschaft (Einzelpersonen, Unternehmen, Gemeinden usw.) zu einem Beitrag zur kollektiven Cybersicherheit. Und um dies zu erreichen, bedarf es massiver Anstrengungen mit echten Prioritäten in den Budgets und Agenden, insbesondere im Bereich der Ausbildung. Nur so wird die Karikatur von Chapatte ihren Hyperrealismus verlieren.

Rappelons qu'en Allemagne on estime que 6.6% du PIB est rongé par le cancer de la cybercriminalité. En admettant généreusement que la Suisse soit deux fois meilleure que son grand voisin, c'est toute de même près de 20 milliards CHF qui partent annuellement en fumée. Et cela sans parler d'une situation de guerre qui pourrait se prolonger dans le cyberespace.

Chers Lectrices et Lecteurs, recevez toutes nos excuses pour toutes ces mauvaises nouvelles. Nous aimerions pouvoir vous relater une majorité de faits positifs, mais l'actualité et les défauts de gouvernance de notre pays nous en privent.

Avec ce billet, nous souhaitons cependant aussi dire MERCI à celles et ceux qui, semaine après semaine, partagent leurs découvertes et observations avec *digi*Volution et contribuent ainsi très concrètement à notre travail de veille stratégique et à ce billet.

Nous nous réjouissons de vous retrouver dans 15 jours.

In Deutschland werden schätzungsweise 6,6% des BIP vom Krebsgeschwür der Cyberkriminalität zerfressen. Wenn man grosszügig annimmt, dass die Schweiz doppelt so gut ist wie ihr grosser Nachbar, sind es immer noch fast 20 Milliarden CHF jährlich, die in Rauch aufgehen. Und das ganz zu schweigen von einer Kriegssituation, die sich im Cyberspace fortsetzen könnte.

Liebe Leserinnen und Leser, wir möchten uns für all diese schlechten Nachrichten entschuldigen. Wir würden Ihnen gerne eine Vielzahl von positiven Ereignissen berichten, aber aufgrund der aktuellen Ereignisse und der Gouvernanzfehler in unserem Land ist uns dies nicht möglich.

Mit diesem Beitrag möchten wir aber all jenen DANKE sagen, die Woche für Woche ihre Entdeckungen und Beobachtungen mit *digi*Volution teilen und so ganz konkret zu unserer Arbeit der strategischen Aufklärung und zu diesem Newsletter beitragen.

Wir 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.*