

dV-News

Les billetsⁱ de *digiVolution* / *digiVolution's* Newsletters
[28.02.2024 - Édition / Ausgabe Nr. 96]

Strategic vs. tactic

Chers Lectrices et Lecteurs

Voici les **dV-News 05-2024** et leur sélection d'[articles et liens](#). L'événement le plus significatif de cette dernière quinzaine aura été sans conteste le [démantèlement par les forces de sécurité de plusieurs pays du gang de cyber-criminels LockBit](#), un des principaux acteurs de la scène de ransomware. [Un succès qui appartient déjà au passé...!](#)

Strategic vs. tactic

Avec ce 96^{ème} billet, notre ambition a été d'éclaircir cette question. Chemin faisant, nous sommes une fois encore arrivés à la conclusion qu'il est impératif **que chacun comprenne l'importance de la dimension stratégique des défis de la mutation numérique et des cybermenaces**. Se limiter à une compréhension technique et tactique de ces phénomènes ne suffit pas, tout comme il est vain de ne se poser les questions qu'une fois les incidents constatés alors que guette le tsunami des menaces à venir dopées par l'IA et l'informatique quantique.

Comprendre les cyberphénomènes n'est cependant pas donné à chacun, car rares sont les exemples disponibles **et** compréhensibles. Grâce toutefois à la [NZZ qui a décidé, par la plume de Lukas Mäder, d'expliquer en détail la cyberattaque subie le 24 mars 2023](#), chacun peut se plonger dans les heures, jours et semaines difficiles vécues par l'entreprise et mesurer les séquelles subsistant un an plus tard.

Liebe Leserinnen und Leser

Hier sind die **dV-News 05-2024** und eine Auswahl an [Artikeln und Links](#). Das bedeutendste Ereignis der letzten zwei Wochen war eindeutig [die Zerschlagung der Cyberkriminellenbande LockBit](#), einer der Hauptakteure in der Ransomware-Szene, durch die Sicherheitskräfte mehrerer Länder. [Ein Erfolg, der schon der Vergangenheit angehört...!](#)

Strategic vs. tactic

Mit diesem 96. Newsletter wollen wir dieser Frage nachgehen und kommen erneut zum Schluss, dass **ausnahmslos alle die Bedeutung der strategischen Dimension der Herausforderungen der digitalen Mutation und der Cyberbedrohungen** verstehen müssen. Es reicht nicht aus, sich auf ein technisches und taktisches Verständnis dieser rasanten Entwicklungen zu beschränken! Gewiss ist es zwecklos, erst dann Fragen zu stellen, wenn Angriffe vorgefallen sind und zugleich der Tsunami künftiger Bedrohungen durch KI und Quantumcomputing droht.

Das Verständnis von Cyberphänomenen ist jedoch nicht jedermanns Sache, da es wenige verständliche **und** nachvollziehbare Beispiele gibt. [Dank Lukas Mäder, der in einem ausführlichen Erfahrungsbericht den Cyberangriff vom 24. März 2023 auf die NZZ](#) beschreibt, ist es möglich, die schwierigen Stunden, Tage und Wochen, die das Unternehmen erlebte,



Même si l'article est en allemand (il existe plein de solutions pour le traduire...), nous recommandons à toutes les entreprises et organisations sa lecture attentive, car pour beaucoup d'autres, une telle attaque aurait été fatale. Alors, permettez-nous de poser la question à ceux qui n'ont toujours pas fait le nécessaire: «Êtes-vous prêt à assumer une faillite et à expliquer ses causes à vos collaborateurs et à vos clients» ?

Et pour ceux qui sont prêts, pourquoi n'iriez-vous pas expliquer aux récalcitrants qu'être prêt n'est ni impossible ni ruineux et que cela peut les sauver? Et que signifie «être prêt»? Quelques mesures techniques et un peu de sensibilisation ne suffisent pas. Ce sont bien entendu des pas nécessaires, mais la cyberattaque contre la NZZ montre combien l'organisation, la formation du personnel, la communication, les processus et les aspects juridiques font partie du dispositif, auxquels il faut ajouter la gestion des risques et le suivi de situation comme pour tous les autres domaines.

Il faut inlassablement répéter que l'infrastructure IT de l'entreprise n'est pas une simple commodité technique. Les interdépendances sont telles, qu'une panne peut devenir rapidement systémique et donc une menace pour toute l'organisation et ses partenaires. D'ailleurs les attaquants le savent bien, qui prennent souvent le temps de cibler d'autres rouages essentiels, comme d'aller jusqu'à [saboter les sauvegardes](#) et ainsi de détruire également la capacité de résilience de leurs victimes.

Si la pensée tactique ne suffit pas, le mot *stratégique* ne signifie pas non plus *stratosphérique* ou *étatique*. Le Larousse est clair: c'est «*l'art de coordonner des actions, de manœuvrer habilement pour atteindre un but*». C'est donc à la portée de tout le monde et permet à toute organisation de prendre de bonnes décisions et d'éviter des issues funestes. Même au sein d'une PME ou d'une petite commune **il faut penser et agir stratégiquement**.

zu verstehen und die Nachwirkungen noch fast ein Jahr später zu ermessen.

Wir empfehlen allen Unternehmen und Organisationen, diesen Artikel aufmerksam zu lesen, denn für viele wäre ein solcher Angriff fatal gewesen. Die Frage an diejenigen, die es noch nicht getan haben, lautet: «*Sind Sie bereit, einen Konkurs zu riskieren und Ihren Mitarbeitenden und ihrer Kundschaft die Gründe dafür zu erklären*»?

Und für diejenigen, die bereit sind, gehen Sie hin und erklären den Unwilligen, dass es weder unmöglich noch ruinös ist, bereit zu sein und sie das retten kann? Und was bedeutet «*bereit sein*»? Ein paar technische Massnahmen und ein wenig Sensibilisierung reichen nicht aus. Gewiss sind dies notwendige Schritte, aber der Cyberangriff auf die NZZ zeigt, wie Organisation, Personalschulung, Kommunikation, Prozesse und rechtliche Aspekte Teil der Vorkehrungen sind, zu denen – wie in allen anderen Bereichen – Risikomanagement und Lageüberwachung gehören.

Es muss immer wieder betont werden, dass die IT-Infrastruktur eines Unternehmens nicht lediglich eine technische Annehmlichkeit ist. Die Abhängigkeiten davon sind unterdessen so gross, dass ein Ausfall schnell zu einem systemischen Problem und damit einer Bedrohung für das gesamte Unternehmen und seine Partner werden kann. Das wissen auch die Angreifer, die sich oft die Zeit nehmen, andere wichtige Zahnräder zu beschädigen und sogar die [Backups zu sabotieren](#), um die Resilienz ihrer Opfer ebenfalls zu zerstören.

Wenn **taktisches Denken nicht ausreicht**, bedeutet das Wort *strategisch* auch nicht *stratosphärisch* oder *staatlich*. Für die St. Gallen Business School, ist Strategie «*die Kunst und die Wissenschaft, alle Kräfte eines Unternehmens so zu entwickeln und einzusetzen, dass ein möglichst profitables, langfristiges Überleben gesichert wird*». Sie ist also für alle zugänglich und kann jede Organisation ermöglichen, gute Entscheidungen zu treffen und fatale Folgen zu vermeiden. Selbst in einem KMU



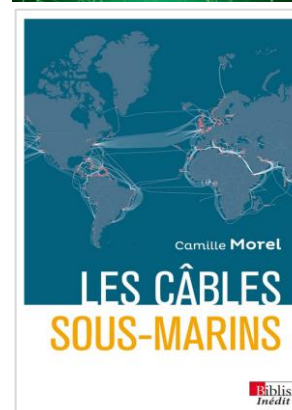
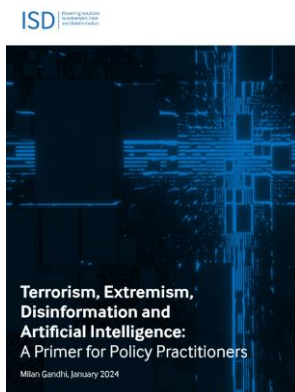
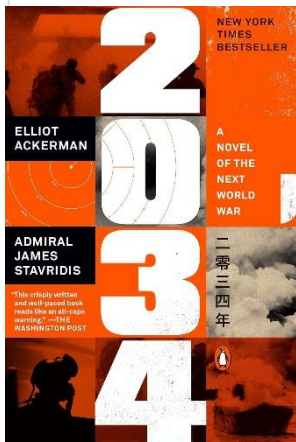
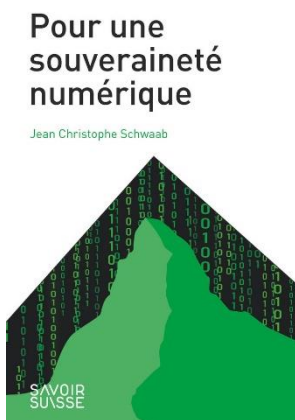
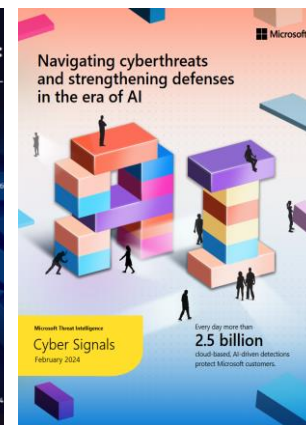
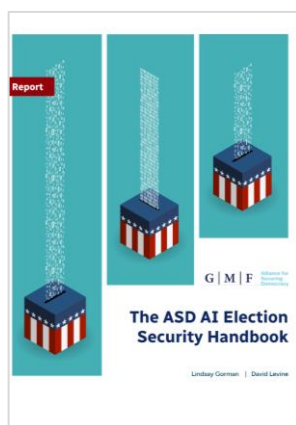
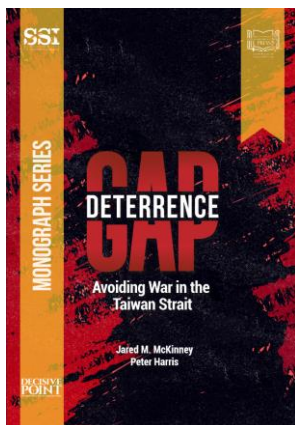
oder einer kleinen Gemeinde muss strategisch gedacht und gehandelt werden.

BOOKS & REPORTS

Voici la liste des livres et publications d'intérêt découverts lors de nos recherches durant les deux dernières semaines. Et sur [dVPedia](#), la rubrique [dVLibrary](#) avec son [tout nouveau look and feel](#) comprend déjà une centaine de titres avec leurs références et un résumé.

BOOKS & REPORTS

Hier die Liste der Bücher und Publikationen von Interesse, auf die wir anlässlich unserer Recherchen der letzten zwei Wochen gestossen sind. Und auf [dVPedia](#) bietet die Rubrik [dVLibrary](#) mit ihrem neuen [Look and Feel](#) bereits 100 Titel mit Referenzen und einer Zusammenfassung an.





News significatives de la quinzaine

► **LockBit down!** - Comme introduit plus haut, l'action contre ce groupe de criminels russophones qui a fait plus de 2300 victimes en moins de 3 ans, dont 30 établissements de santé entre août 2023 et février 2024 est une bonne nouvelle. Le fruit de [mois de travail des forces de l'ordre de renseignement](#), y inclus la Suisse. Quelle suite espérer? La masse d'informations gagnée et de saisies opérées aurait dû empêcher une rapide renaissance du groupe. Toutefois l'exemple de [ALPHV/BLACKCAT](#), soi-disant démantelé en décembre par le FBI et qui [déclarait annuler les limites qu'il s'était imposé](#) de ne pas attaquer les hôpitaux et les centrales nucléaires, aurait dû rendre tout le monde prudent. En effet, [LockBit semble être déjà de retour](#). De quelle manière le groupe fera-t-il payer la communication inutilement victorieuse et [contre-productive](#) de certains? Voilà donc un succès tactique, mais sous l'angle stratégique, la [situation reste inchangée](#) et l'avenir sombre. Les espoirs soulevés par cette action sont déjà douchés.



► [ChatGPT est-il devenu fou?](#) - Oui, selon ChatGPT lui-même qui le 21 février s'est mis à diffuser des résultats qualifiés par ses utilisateurs de «*hallucinated garbage*». Interrogé, ChatGPT a répondu plus tard: «*La panne majeure de ChatGPT a été causée par un problème au niveau du serveur backend qui a entraîné l'indisponibilité du service pendant environ 40 minutes*». Espérons que [l'appel de](#)

Wichtige Nachrichten der letzten Wochen

► **LockBit down!** - Wie bereits erwähnt, ist die Aktion gegen diese russischsprachige kriminelle Gruppe, die in weniger als drei Jahren mehr als 2300 Opfer forderte, darunter 30 Gesundheitseinrichtungen zwischen August 2023 und Februar 2024, eine gute Nachricht. Das Ergebnis [monatelanger Arbeit der Strafverfolgungsbehörden und Nachrichtendienste](#), inkl. der Schweiz. Was kommt nun? Die Masse der gewonnenen Informationen und Beschlagnahmungen hätte eine rasche Wiederbelebung der Gang verhindern sollen. Das Beispiel von [ALPHV/BLACKCAT](#), die im Dezember angeblich vom FBI aufgelöst wurde und nun [erklärten, dass ihre selbst auferlegten Beschränkungen](#), Krankenhäuser und Atomkraftwerke nicht anzugreifen, nicht mehr gelten, hätte jedoch alle vorsichtig machen müssen. Denn [LockBit sollte bereits zurück sein](#). Wie wird die Gruppe einige Leute für ihre unnötig siegreiche und [kontraproduktive](#) Kommunikation zur Kasse bitten? Dies war ein taktischer Erfolg, aber aus strategischer Sicht bleibt die [Lage unverändert](#) und die Zukunft düster. Die Hoffnungen, die durch diese Aktion geweckt wurden, sind bereits gedämpft.



► [Ist ChatGPT verrückt geworden?](#) - Ja, laut ChatGPT selbst, die am 21. Februar anfang, Ergebnisse zu verbreiten, die von ihren Nutzern als «*hallucinated garbage*» bezeichnet wurden. Auf Anfrage antwortete ChatGPT später: «*Die grössere Panne von ChatGPT wurde durch ein Problem im Backend-Server verursacht, was dazu führte, dass der Service für etwa 40 Minuten nicht verfügbar war*».

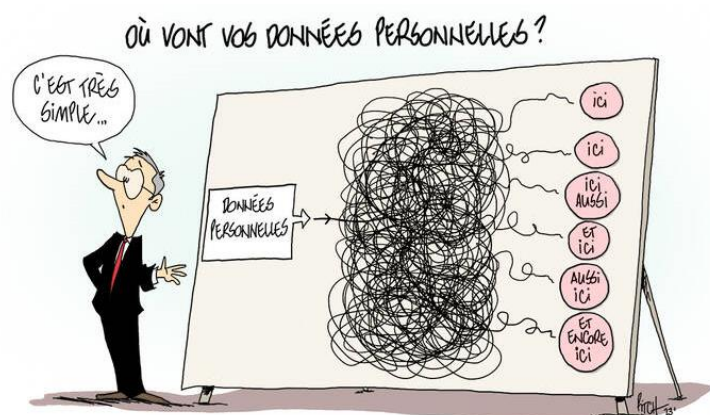


[Gary Marcus, qui écrivait le 7 février](#) «Please, developers and military personnel, don't let your chatbots grow up to generals» sera entendu. La tentation de faire de l'IA un avantage stratégique conduira inmanquablement certains à ne pas entendre ces mises en garde. En termes de risques, il s'agira de ne pas oublier de **laisser un KILL SWITCH humain au centre**. Qui se préoccupe de cet aspect stratégique en Suisse?

► **Souveraineté numérique** - Tout indique que cette bataille est loin, très loin même d'être gagnée. En Suisse, les pessimistes la qualifient même de *largement perdue* suite notamment aux récentes annonces de l'armée qui utilise désormais Microsoft 365 pour la planification des cours de répétition et les tâches hors service et alors que la [migration des unités administratives de la Confédération](#) bat son plein. Chez *digiVolution* nous ne baisserons pas les bras et nous reviendrons sur cette question clé. Dans l'intervalle, nous attirons votre attention sur une publication à venir de [Heidi News: «Razia sur nos données»](#), à mettre en miroir (voir la rubrique Books & Reports) avec l'ouvrage de [Jean Christophe Schwaab «Pour une souveraineté numérique»](#).

Hoffentlich wird der [Aufruf von Gary Marcus erhört wird, der am 7. Februar schrieb](#): «Please, developers and military personnel, don't let your chatbots grow up to generals». Die Versuchung, KI zu einem strategischen Vorteil zu machen, wird unweigerlich dazu führen, dass einige diese Warnungen nicht befolgen. In Bezug auf die Risiken wird es darum gehen, **einen menschlichen KILL SWITCH im Mittelpunkt zu lassen**. Wer kümmert sich in der Schweiz um diesen strategischen Aspekt?

► **Digitale Souveränität** - Alles deutet darauf hin, dass dieser Kampf noch lange, sehr lange nicht gewonnen ist. In der Schweiz bezeichnen Pessimisten die Entwicklung sogar als *weitgehend verloren*, insbesondere nach den jüngsten Ankündigungen der Armee, Microsoft 365 für die Planung von Wiederholungskursen und ausserdienstlichen Aktivitäten zu verwenden und dies während die [Migration der Verwaltungseinheiten des Bundes](#) in vollem Gange ist. Wir von *digiVolution* werden nicht aufgeben und auf diese Schlüsselfrage zurückkommen. In der Zwischenzeit möchten wir Sie auf eine bevorstehende Veröffentlichung von [Heidi News aufmerksam machen: «Razia sur nos données»](#), die mit dem Buch von [Jean Christophe Schwaab «Pour une souveraineté numérique»](#) verglichen werden kann (siehe die Rubrik Books & Reports).



Source: <https://www.heidi.news/explorations/razia-sur-vos-data/razia-sur-nos-data-comment-nos-entreprises-servent-la-soupe-a-google-et-facebook>

► **Super année électorale et IA** - À l'exemple de [SORA de OpenAI](#), l'IA fait des progrès

► **Superwahljahr und KI** - Am Beispiel von [SORA von OpenAI](#) macht die KI täglich



quotidiens en matière de génération de contenus, spectaculaire dans ce cas. Voilà de quoi inquiéter l'industrie audiovisuelle ainsi que tous ceux qui craignent pour les processus démocratiques de cette année 2024 chargée en scrutins divers et donc une cible privilégiée pour la désinformation.

Fortschritte bei der Generierung von Inhalten, in diesem Fall sogar spektakulären. Dies ist ein Grund zur Sorge für die audiovisuelle Industrie und all jene, die um die demokratischen Prozesse im Jahr 2024 fürchten – ein Jahr mit vielen Wahlen und damit ein beliebtes Ziel für Desinformation.



Le 15 février, OpenAI a dévoilé Sora, un modèle d'IA générative capable de créer des séquences vidéo réalistes à partir d'instructions textuelles | Am 15. Februar stellte OpenAI Sora vor, ein generatives KI-Modell, das aus textbasierten Anweisungen realistische Videosequenzen erstellen kann.

Merci de souscrire à [dVPedia](#) et ainsi de soutenir son développement au profit de tous.

Bitte registrieren Sie sich für [dVPedia](#) und unterstützen Sie damit seine Entwicklung zum Nutzen aller.

dVPedia



Your daily cyber security forecast!

Merci également de soutenir par vos [DONS](#) notre travail au profit de la sécurité, de la résilience et de la souveraineté de la Suisse.

Bitte unterstützen Sie auch unsere Arbeit für die Sicherheit, Resilienz und Souveränität der Schweiz mit Ihrer [SPENDE](#).



digiVolution



Nous vous souhaitons une enrichissante découverte des [articles et liens](#) sélectionnés et vous retrouverons dans 15 jours.

Wir wünschen Ihnen viele lehrreiche Erkenntnisse mit den ausgewählten [Artikeln und Links](#) und sehen uns in zwei Wochen wieder.



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 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>. Interessierte finden auf dieser Seite auch den Link zur Anmeldung.