Les billets[i] de *digi*Volution / *digi*Volution's Newsletters
[17.01.2023 – 68ème édition]

OPSEC

Chers Lectrices et Lecteurs

Voici les ***d*V-News 02-2023** et leur sélection d'articles et de liens, une édition qui s'intéresse au domaine de l'OPSEC, ou *operations security* avec, comme d'habitude, un point sur quelques aspects saillants de la cyberactualité et la rubrique «Books & Reports».

Liebe Leserinnen und Leser

Dies sind die ***d*V-News 02-2023** mit einer Auswahl an Artikeln und Links, eine Ausgabe, die sich mit dem Thema OPSEC oder *operations security* befasst, und wie üblich mit einem Überblick über einige Highlights der Cyberaktualität und der Rubrik «Books & Reports».

OPSEC

De quoi sera faite 2023? Sur le plan conflictuel, cela ne s'annonce d'ores et déjà pas bien et c'est dans cet environnement très disputé que la protection de l'information est plus importante que jamais.

Et si nous , utilisateurs, apprenions à réfléchir à nos actes? Traverserions-nous, les yeux bandés, une artère principale au moment du rush? Sortirions-nous en pleine tempête de neige vêtus d'un simple T-shirt? Il se trouvera bien sûr toujours des personnes à l'intelligence et à la responsabilité limitées pour le faire, mais l'écrasante majorité des gens fait juste.

OPSEC

Wie wird das Jahr 2023 aussehen? In Bezug auf Konflikte sieht es schon jetzt nicht gut aus, und in diesem hart umkämpften Umfeld ist der Informationsschutz wichtiger denn je.

Was wäre, wenn wir Nutzer lernen würden, über unsere Handlungen nachzudenken? Würden wir bei hohem Verkehrsaufkommen mit verbundenen Augen eine Hauptverkehrsstrasse überqueren? Würden wir nur mit einem T-Shirt bekleidet in einen Schneesturm gehen? Natürlich wird es immer Menschen mit geringer Intelligenz und Verantwortungsbewusstsein geben, die ähnliches tun, aber die überwiegende Mehrheit der Menschen verhält sich richtig.

Pourtant, s'agissant de nos smartphones, il semble que nous ayons quelques progrès à faire. Nous les utilisons, semble-t-il, sans trop nous poser de questions quant aux risques. Interrogés, la plupart diront être très prudents, mais les faits racontent une autre histoire.

Il y a eu ces artilleurs ukrainiens dont la position a été révélée par une application de calcul des éléments de tir de leurs canons. Seulement, le groupe russe Fancy Bear l'avait modifiée à leur insu… Ensuite il y a eu ces soldats américains utilisant Strava pour leur footing et qui ainsi trahissaient l'emplacement et la disposition de bases militaires confidentielles. On mentionnera ces 800 criminels arrêtés dans le monde entier après une opération sans précédent grâce à une faille dans l'application de messagerie «sécurisée» qu'ils utilisaient ou ces policiers californiens dont l'application pour la conduite des opérations diffusait des informations sur leurs activités et sur les suspects qu'ils traquaient. Et on se souviendra aussi du comportement irresponsable de la Première ministre britannique. À Makiïvka, dans l'est de l'Ukraine, au soir du Nouvel An, plus de 100 jeunes Russes sont morts pour n'avoir pas appliqué les consignes. Repérée à cause de leurs portables, leur caserne a été rasée par l'artillerie ukrainienne. Combien de fois faudra-t-il le dire: les smartphones sont des mouchards! Oubliée l'affaire de NSO Group et de Pegasus?

Dans tous ces exemples, les règles de base de l'OPSEC, la sécurité opérationnelle, ont été bafouées. Nous serions tous bien avisés de réfléchir avant de nous exposer et d'exposer autrui en raison de notre manque de discipline informationnelle. Les règles sont pourtant simples et disponibles partout en ligne.

Et dans les entreprises, combien prennent leur portable lors de discussions stratégiques? L'argument du « c'est trop cher », cela s'écarte aussi parfois avec un simple bocal à confiture comme illustré ci-dessous. La sécurité est d'abord une affaire de volonté.

Was unsere Smartphones betrifft, sind allerdings Fortschritte fällig. Offenbar nutzen wir sie, ohne uns allzu viele Gedanken über die Risiken zu machen. Auf Nachfrage würden die meisten sagen, dass sie sehr vorsichtig sind, aber Fakten erzählen eine andere Geschichte.

Da gab es diese ukrainischen Artilleristen, deren Position von einer Smartphone-App verraten die für die Berechnung der Angriffsziele verwendet wurde. Die russische Gruppe Fancy Bear hatte die App versehentlich verändert... Dann gab es die amerikanischen Soldaten, die Strava für ihr Jogging nutzten und so den Standort und die Anordnung von vertraulichen Militärbasen verrieten. Erwähnen wir auch die 800 Kriminellen, die weltweit nach einer beispiellosen Operation aufgrund einer Schwachstelle in der von ihnen verwendeten «sicheren» Messaging-App festgenommen wurden, oder die kalifornischen Polizisten, deren App zur Durchführung von Einsätzen Informationen über ihre Aktivitäten und die von ihnen verfolgten Verdächtigen verbreitete. Und auch das unverantwortliche Verhalten der britischen Premierministerin wird in Erinnerung bleiben. In Makijewka in der Ostukraine starben am Silvesterabend mehr als 100 junge Russen, weil sie die Anweisungen nicht befolgt hatten. Ihre Kaserne wurde von der ukrainischen Artillerie zerstört, weil sie wegen der Nutzung ihrer Smartphones entdeckt wurde. Wie oft muss man es noch sagen: Smartphones sind Wanzen! Ist der Fall der NSO Group und Pegasus schon vergessen?

In all diesen Fällen wurden die grundlegenden Regeln der OPSEC, die operative Sicherheit, missachtet. Wir alle wären gut beraten, darüber nachzudenken, bevor wir uns und dritte aufgrund unserer mangelnden Informationsdisziplin blossstellen. Dabei sind die Regeln einfach und überall online verfügbar.

Und in Unternehmen, wie viele haben ihr Handy während strategischen Gesprächen dabei? Das Argument «das ist zu teuer» lässt sich indessen auch mit einem einfachen Marmeladenglas ausräumen, wie unten dargestellt. Sicherheit ist in erster Linie eine Frage des Willens.

Cyberactualité

Bien que la dernière quinzaine ait été plutôt calme, deux éléments ont particulièrement retenu notre attention.

- **Guerre en Ukraine** – Lors de son audition par la Commission de la défense nationale et des forces armées, le général Bonnemaison, commandant cyber des armées françaises, COMCYBER, a fait un point sur la situation cyber du conflit. Comme beaucoup d'analystes militaires qui ne se laissent pas submerger par l'émotion ambiante, il reste prudent quant à l'importance du cyber, ne la sur- ou sous-estime pas, tout en rappelant que le conflit a commencé avant 2014. Une analyse simple et efficace. Et pour ceux qui auraient besoin d'un état des lieux détaillés, nous recommandons la chronologie de la National Security Archive.
- **Cyberassurance** – Nous en discutions l'été passé et le mentionnions dans notre 64ème billet en novembre dernier, les cyberrisques pourraient bien devenir inassurables. Le CEO de Zurich Assurance est on ne peut plus clair. Cette évolution doit alarmer chaque décideur, car elle signifie que les victimes vont se retrouver seules. Et

Cyber-Aktualität

Obwohl die letzten zwei Wochen eher ruhig waren, haben zwei Themen unsere Aufmerksamkeit besonders auf sich gezogen.

- **Krieg in der Ukraine** – Bei einer Anhörung des französischen Ausschusses für nationale Verteidigung und Streitkräfte gab General Bonnemaison, der Cyberkommandeur der französischen Streitkräfte, COMCYBER, einen Überblick über die Cybersituation des Konflikts. Wie viele Militäranalysten, die sich nicht von den vorherrschenden Emotionen überwältigen lassen, bleibt er vorsichtig, was die Bedeutung des Cybers angeht, über- oder unterschätzt sie nicht und erinnert daran, dass der Konflikt schon vor 2014 begonnen hat. Eine einfache und effektive Analyse. Und für diejenigen, die eine detaillierte Bestandsaufnahme benötigen, empfehlen wir die Chronologie des amerikanischen National Security Archive.
- **Cyberversicherung** – Wir haben es letzten Sommer diskutiert und im letzten November in unserem 64. Newsletter erwähnt: Cyberrisiken könnten bald unversicherbar werden. Der CEO der Zurich Assurance

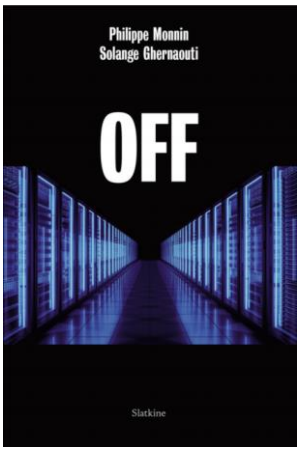
pour une entreprise, une cyberattaque sévère signifiera la faillite pure et simple. Et si d'aventure des assureurs continuent à offrir ce type de prestation, ce sera de toute manière lié à des conditions drastiques. Donc oui, la cybersécurité n'est depuis longtemps plus une option et va commencer à coûter aussi pour ceux qui se sont défilés jusqu'ici, pensant que cela n'arrive qu'aux autres. Voilà donc une évolution à prendre au sérieux et sans tarder, car les choses pourraient bien changer rapidement du côté des assureurs, alors que les risques ne font que croître, comme le rappelle à nouveau le WEF cette année et que Comparitech **qualifie les conséquences à venir de terrifiantes.**

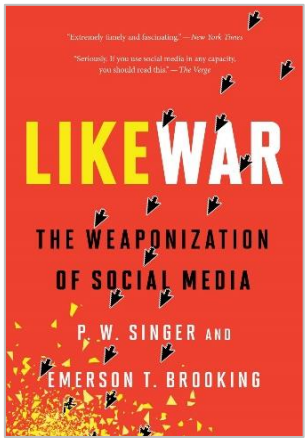
macht das sehr deutlich. Diese Entwicklung muss jeden Entscheidungsträger alarmieren, denn sie bedeutet, dass die Opfer auf sich allein gestellt sein werden. Und für ein Unternehmen bedeutet dies, im Falle eines schweren Angriffs, dass es in Konkurs gehen wird. Und falls die Versicherer diese Art von Cyber-Leistungen weiterhin anbieten, wird dies in jedem Fall an drastische Bedingungen geknüpft. Ja, Cybersicherheit ist schon lange keine Option mehr und wird auch diejenigen kosten, die sich bisher gedrückt haben, weil sie dachten, dass dies nur den anderen passiert. Das WEF hat dieses Jahr erneut daran erinnert, dass die Risiken immer grösser werden, und Comparitech **bezeichnet die zu erwartenden Folgen als erschreckend**.

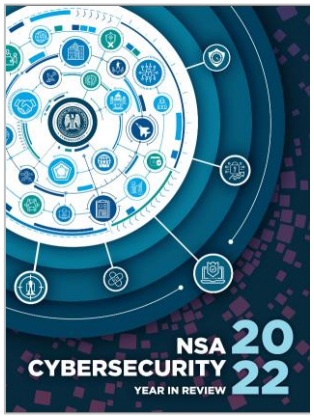
BOOKS & REPORTS

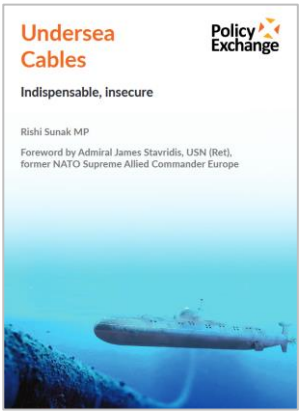
Voici les livres et publications d'intérêts découverts durant nos recherches de cette quinzaine. Nous recommandons en particulier le livre de Solange Ghernaouti, OFF !

Hier sind die Bücher und Publikation von Interesse, die wir bei unseren Recherchen in diesen zwei Wochen entdeckt haben. Besonders empfehlenswert ist Solange Ghernaoutis Buch OFF!









Et chez digiVolution? – En plus de l'organisation de notre événement phare Swisscyberhub, nous travaillons à plein régime pour lancer dV-Net. Ce sera le 24 janvier que notre outil passera du stade «essai pilote» à «opérationnel». Un pas essentiel après 18 mois d'investissement et un bel avenir au service des décideurs.

Où va le monde? – Nous vous invitons à ne pas manquer le prochain Bulletin of the Atomics Scientists du 24 janvier. On verra alors si les prévisions de l'horloge de l'apocalypse se sont encore dégradées…!

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

Wie weiter bei digiVolution? – Neben der Organisation unseres Flagship-Events Swisscyberhub arbeiten wir mit Hochdruck an der Einführung von dV-Net. Am 24. Januar wird unser Tool vom Status «Pilotversuch» zu «operativ» übergehen. Ein wesentlicher Schritt nach 18 Monaten Investition und mit einer schönen Aussicht im Dienste der Entscheidungsträger.

Wie geht es mit der Welt weiter? – Wir empfehlen Ihnen, das nächste Bulletin of the Atomics Scientists vom 24. Januar nicht zu verpassen. Dann werden wir sehen, ob sich die Prognosen der Weltuntergangsuhr weiter verschlechtert haben...!

Wir wünschen Ihnen bereicherndes Wissen mit 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.*