Les billets[i] de *digi*Volution / *digi*Volution's Newsletters
[14.02.2023 – 70ème édition]

The Insider Threat

Chers Lectrices et Lecteurs

Voici les ***d*V-News 04-2023** et leur sélection d'articles et de liens. Déjà le numéro 70, et à une exception près, toujours un autre titre et de nouveaux thèmes. Dans cette édition nous avons choisi de nous emparer d'un sujet délicat…

La menace de l'intérieur

En 2022, le NCSC a enregistré une croissance des cyberdélits annoncés de près de 60%. De son côté, la police vaudoise estime que seuls 10% des cas lui sont annoncés. Mais en se penchant sur les statistiques, on s'aperçoit rapidement que les cyberattaques ne sont pas juste le fait de vilains hackers de l'extérieur!

En novembre 2022, notre Centre national pour la cybersécurité informait au sujet d'une faille critique identifiée sur plus de 2'800 serveurs Microsoft Exchange en Suisse. Un mois plus tard, il envoyait une lettre recommandée à 2'000 exploitants, les invitant à combler cette faille de sécurité. Le 2 février, plus de 660 serveurs étaient toujours vulnérables. Comment qualifier les propriétaires de ces serveurs qui les laissent sans protection? Simplement de *dangereux irresponsables!* Ce comportement est comparable à ces touristes qui se baladent en haute montagne munis d'espadrilles et qui imaginent qu'en cas de pépin quelqu'un viendra les chercher. C'est comme ce vacancier qui se fait voler les effets laissés dans une voiture ouverte ou qui s'étonne d'avoir été cambriolé après avoir étalé ses photos de vacances sur les réseaux sociaux. Bien sûr que le

Liebe Leserinnen und Leser

Dies sind die ***d*V-News 04-2023** und eine Auswahl an Artikeln und Links. Schon die 70. Ausgabe, und bis auf eine Ausnahme immer ein anderer Titel und neue Themen. Und diesmal haben wir uns für ein heikles Thema entschieden…

Die Insider-Bedrohung

Im Jahr 2022 verzeichnete der NCSC einen Anstieg der gemeldeten Cybervorfälle um fast 60%. Die Waadtländer Polizei ihrerseits schätzt, dass ihr nur 10% der Fälle gemeldet werden. Aber wenn man sich die Statistiken ansieht, stellt man schnell fest, dass Cyberangriffe nicht nur von externen bösen Hackern erfolgen!

Im November 2022 informierte unser Nationales Zentrum für Cybersicherheit über eine kritische Schwachstelle, die bei über 2'800 Microsoft Exchange-Servern in der Schweiz festgestellt wurde. Einen Monat später schickte es 2'000 Betreibern einen eingeschriebenen Brief, in dem sie aufgefordert wurden, die Sicherheitslücke zu schliessen. Am 2. Februar waren immer noch mehr als 660 Server gefährdet. Wie soll man die Besitzer dieser Server bezeichnen, die sie ungeschützt lassen? Einfach als *gefährliche Unverantwortliche!* Dieses Verhalten ist vergleichbar mit Touristen, die mit Turnschuhen im Hochgebirge unterwegs sind und davon ausgehen, dass sie im Falle eines Problems von jemandem abgeholt werden. Es ist wie bei dem Urlauber, dem die Sachen aus einem offenen Auto gestohlen werden oder der sich

voleur venait de dehors, mais le vrai problème est à chercher à l'intérieur.

Selon le WEF, près de 95 % des incidents de cybersécurité de l'année dernière – pour un coût de 8'000 milliards et avec des perspectives alarmantes – sont à mettre sur le compte d'une erreur humaine.

Nouveau? Aucunement. Souvenons-nous de cet informaticien du Service de renseignement de la Confédération sorti avec tout un disque dur, du vol des données de la banque HSBC, ou encore de l'affaire Snowden. En Valais, les autorités ont même dû récemment mettre en détention préventive le développeur d'un logiciel utilisé par plusieurs polices communales alors qu'il menaçait de publier des données sensibles sur le darknet.

Lorsque chez *digi*Volution nous définissons le cyberespace et les acteurs malveillants, nous rappelons systématiquement la réalité de cette menace intérieure. Si l'écrasante majorité de nos collaborateurs est fantastique, une seule personne malveillante suffit à ruiner toute une organisation.

über einen Einbruch wundert, nachdem er seine Urlaubsfotos in sozialen Netzwerken verbreitet hat. Natürlich kam der Dieb von draussen, aber das eigentliche Problem ist intern zu suchen.

Laut WEF waren fast 95% der Cybersicherheitsvorfälle des letzten Jahres - mit Kosten in Höhe von 8 Billionen Dollar und alarmierenden Aussichten - auf menschliches Versagen zurückzuführen.

Ist das neu? Keineswegs. Erinnern wir uns an den Informatiker des Nachrichtendienstes des Bundes der mit einer ganzen Festplatte unterwegs war, den Datendiebstahl bei der Bank HSBC oder die Snowden-Affäre. Im Wallis mussten die Behörden kürzlich sogar den Entwickler einer Software, die von mehreren Gemeindepolizeien verwendet wird, in Untersuchungshaft nehmen, weil er damit drohte, sensible Daten im Darknet zu veröffentlichen.

Wenn wir bei *digi*Volution den Cyberraum und die böswilligen Akteure definieren, erinnern wir systematisch an die Realität dieser Insider-Bedrohung. Während die überwältigende Mehrheit unserer Mitarbeiterinnen und Mitarbeiter fantastisch ist, reicht eine einzige bösartige Person in der Tat aus, um eine ganze Organisation zu ruinieren.

Les quelques exemples ci-dessus montrent combien les moteurs de la menace intérieure sont nombreux : naïveté, négligence, manque de formation, manipulation, chantage, manque de règles et de contrôles, appât du gain, vengeance, corruption, bêtise, idéalisme… Comment les entreprises et les

Die obigen Beispiele zeigen, dass es viele Ursachen für innere Bedrohungen gibt: Naivität, Nachlässigkeit, mangelnde Ausbildung, Manipulation, Erpressung, fehlende Regeln und Kontrollen, Geldgier, Rache, Korruption, Dummheit, Idealismus, ... Wie sollten Unternehmen und Institutionen dagegen immun

institutions y seraient-elles immunisées? Le personnel qui utilise des véhicules et des machines est formé à leur emploi. On leur impose des règles de sécurité, un outillage particulier et ils n'ont pas accès à tout. Alors pourquoi n'applique-t-on pas systématiquement de tels principes aussi au numérique?

En 2020, le documentaire *The Social Dilemma* estimait que la donnée avait remplacé le pétrole en tant bien le plus précieux pour faire fonctionner la société, une conclusion à laquelle nous adhérons sans réserve chez *digi*Volution. Mais pourquoi donc la donnée est-elle traitée avec autant de légèreté coupable dans le cyberespace?

Selon le rapport 2023 Insider Threat Report, plus de la moitié des entreprises interrogées indiquent avoir été confrontées à une menace interne au cours de l'année écoulée et 8% d'avoir à déplorer plus de 20 cas.

Notre question est simple: de combien – en nombre et impact – réussirions-nous à réduire les cyberincidents si chaque acteur comprenait sa responsabilité et faisait les choses correctement? N'approcher la mutation numérique et la cybersécurité que sous l'angle technologique est une faute majeure. Cela revient à confondre la commodité avec le but. La clé de notre cybersécurité, c'est l'être humain et c'est la raison pour laquelle chez *digi*Volution nous nous focalisons depuis notre première heure sur les décideurs.

Cyberactualité

Voici les sujets qui ont retenu notre attention.

- **Une quinzaine mouvementée en Suisse** – Après la Zurich Assurance au Japon, le CHUV, les CFF et l'Université de Zürich auraient également été récemment victimes de cyberattaques. Face à la vague croissante d'actes malveillants dans le cyberespace, l'inquiétude monte et un groupe d'industries suisses de premier plan vient de créer la *Swiss Industry Cyber-Security Association* dans le but de s'échanger des informations sensibles et de servir d'interlocuteur auprès des autorités. Un

sein? Die Mitarbeiter, die Fahrzeuge und Maschinen benutzen, werden für den Umgang mit ihnen geschult. Sie müssen Sicherheitsregeln befolgen, spezielle Werkzeuge benutzen und haben nicht überall Zugang. Warum werden solche Prinzipien nicht konsequent auch auf die digitale Welt übertragen?

In dem Dokumentarfilm *The Social Dilemma* aus dem Jahr 2020 wurde festgestellt, dass Daten inzwischen als wertvollstes Gut gelten um die Gesellschaft am Laufen zu halten – eine Schlussfolgerung, der wir bei *digi*Volution uneingeschränkt zustimmen. Aber warum wird mit Daten im Cyberraum so leichtfertig umgegangen?

Laut dem 2023 Insider Threat Report gaben mehr als die Hälfte der befragten Unternehmen an, im vergangenen Jahr mit einer internen Bedrohung konfrontiert gewesen zu sein, und 8% hatten mehr als 20 Fälle zu beklagen.

Unsere Frage ist einfach: Wie stark - in Bezug auf Anzahl und Auswirkungen - könnten wir Cybervorfälle reduzieren, wenn sich jeder Akteur seiner Verantwortung bewusst wäre und sich korrekt verhalten würde? Es ist ein grosser Fehler, den digitalen Wandel und die Cybersicherheit nur aus der technologischen Perspektive zu betrachten. Damit wird die Commodity mit dem Zweck verwechselt. Der Schlüssel zu unserer Cybersicherheit ist der Mensch, und deshalb fokussieren wir bei *digi*Volution seit Anfang an auf die Entscheidungsträger.

Cyberaktualität

Hier sind die Themen, die unsere Aufmerksamkeit erregt haben.

- **Bewegte zwei Wochen in der Schweiz** – Nach der Zurich Assurance in Japan wurden kürzlich auch das CHUV, die SBB und die Universität Zürich Opfer von Cyberattacken. Angesichts der wachsenden Welle bösartiger Aktivitäten im Cyberraum wächst die Besorgnis und eine Gruppe führender Schweizer Unternehmen hat die *Swiss Industry Cyber-Security Association* gegründet, um sensible Informationen auszutauschen und als Ansprechpartner für

développement qui illustre la vision de *défense en profondeur* que nous prônons depuis longtemps chez *digi*Volution. La cybersécurité est en effet l'affaire de tous.

- **Cyberdéfense aux heures de bureau** – En février 2014, la Suisse découvrait que son aviation n'assurait la police de l'air qu'aux heures de bureau; six ans plus tard, notre aviation est opérationnelle H24. Mais voilà que l'on découvre que c'est sa cyberdéfense qui travaille sur le *mode heures de bureau*. Malgré les explications fournies, nombreuses sont les questions ouvertes. On peut notamment s'interroger sur le besoin annoncé en personnel supplémentaire, car alors où sont les militaires du bataillon cyber formés spécifiquement pour renforcer les structures professionnelles?
- **Dépendance systémique** – Le 25 janvier, les utilisateurs de Microsoft 365 ont fait la désagréable expérience de leur dépendance. Durant près de 3 heures, une fausse manipulation sur un routeur WAN a entraîné des conséquences mondiales. Voici un exemple on ne peut plus parlant de perte de souveraineté, de l'individu jusqu'à l'État. Le monde politique s'est indigné face aux dépendances européennes par rapport au gaz russe. Et là, il fait quoi? Allons-nous enfin comprendre les risques d'une externalisation naïve et incontrôlée de ce que les entreprises et communautés publiques ont de plus cher: leurs données et leur traitement?
- **Telegram** – Les militants anti-guerre russes faisaient confiance à Telegram, cette application de messagerie prétendument sécurisée. Pourtant les services de sécurité russes semblent tout connaître de leurs mouvements. Mais voilà qu'en creusant, on se rend compte que cette solution de sécurité qui se vantait de tenir tête au Kremlin serait à ses ordres, tenue par l'argent…!

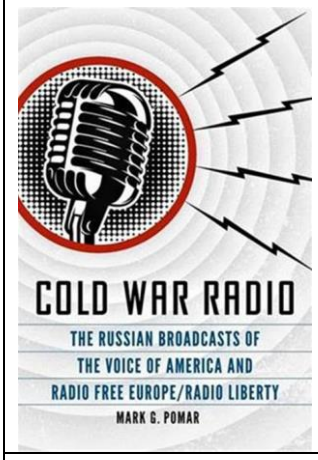
die Behörden zu fungieren. Diese Entwicklung verdeutlicht die Vision einer tiefgreifenden Verteidigung, die wir bei *digi*Volution schon seit langem vertreten. Cybersicherheit geht uns alle an

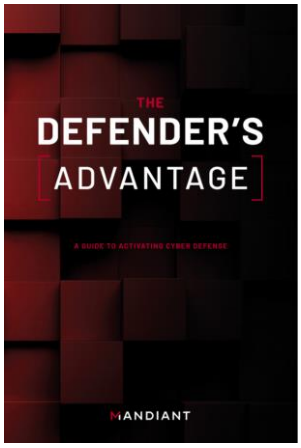
- **Cyberdefence zu Bürozeiten** – Im Februar 2014 stellte die Schweiz fest, dass ihre Luftwaffe nur zu Bürozeiten die Luftpolizei sicherstellen konnte; sechs Jahre später ist unsere Luftwaffe rund um die Uhr einsatzbereit. Nun wurde bekannt, dass die Cyberdefence im *Bürozeitmodus* arbeitet. Trotz der Erklärungen bleiben viele Fragen offen. Insbesondere der angekündigte Bedarf an zusätzlichem Personal ist fraglich, denn wo sind die Soldaten des Cyberbataillons, die speziell für die Verstärkung der professionellen Strukturen ausgebildet werden?
- **Systemische Abhängigkeit** – Am 25. Januar mussten die Nutzer von Microsoft 365 eine unangenehme Erfahrung mit ihrer Abhängigkeit machen. Während fast drei Stunden hatte eine Fehlbedienung an einem WAN-Router weltweite Folgen. Ein anschauliches Beispiel für den Verlust der Souveränität, vom Individuum bis zum Staat. Die Politik hat sich über die Abhängigkeit Europas von russischem Gas empört. Und was tun sie jetzt? Werden wir endlich die Risiken einer naiven und unkontrollierten Auslagerung des Wertvollsten, was öffentliche Unternehmen und Gemeinschaften haben, verstehen: ihre Daten und deren Verarbeitung?
- **Telegram** - Russische Anti-Kriegs-Aktivisten vertrauten auf Telegram, die angeblich sichere Messenger-Applikation. Doch die russischen Sicherheitsdienste scheinen alles über ihre Aktivitäten zu wissen. Aber wenn man tiefer gräbt, stellt man fest, dass diese Sicherheitslösung, die sich rühmte, der Kremlin die Stirn zu bieten, auf seinen Befehl hinarbeitet und finanziell zusammengehalten wird...!

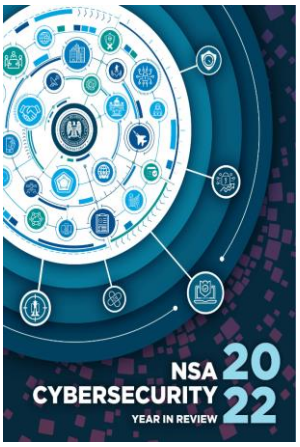
BOOKS & REPORTS

Voici les livres et publications d'intérêts découverts durant nos recherches de cette quinzaine.

Hier sind die Bücher und Publikation von Interesse, die wir bei unseren Recherchen in diesen zwei Wochen entdeckt haben.







Et chez digiVolution? – Le 3 mars [08:30-16:15] nous contribuerons à Lavey-les-Bains, à l'Université de printemps de l'Académie de police. Le 18 mars à Morges au Rubicube [09:15-18:00], nous soutiendrons la conférence du *Forum de la Venoge*, «BLACKOUT23 - Approvisionnement et sécurité énergétique». Du 5 au 7 avril, nous serons au FIC pour encourager nos voisins à venir à Fribourg au Swiss CyberHub dont le programme général sera rendu public très prochainement.

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

Wie weiter bei digiVolution? – Am 3. März [08:30-16:15] werden wir an der Frühjahrsuniversität der Polizeiakademie in Lavey-les-Bains teilnehmen. Am 18. März unterstützen wir in Morges im Rubicube [09:15-18:00] die Konferenz des *Forum de la Venoge*, «BLACKOUT23 - Energieversorgung und -sicherheit». Vom 5. bis 7. April werden wir am FIC teilnehmen, um unsere Nachbarn zu ermutigen, nach Freiburg zum Swiss CyberHub zu kommen deren allgemeines Programm nächste Woche bekannt gegeben wird.

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.*