Zeitschrift: Revue Militaire Suisse
Band: - (2018)
Heft: [2]: Numéro Thématique 2

Artikel: Cyber Security "Best Practice"
Autor: Frey, Stefanie / Bartsch, Michael
DOI: https://doi.org/10.5169/seals-823455

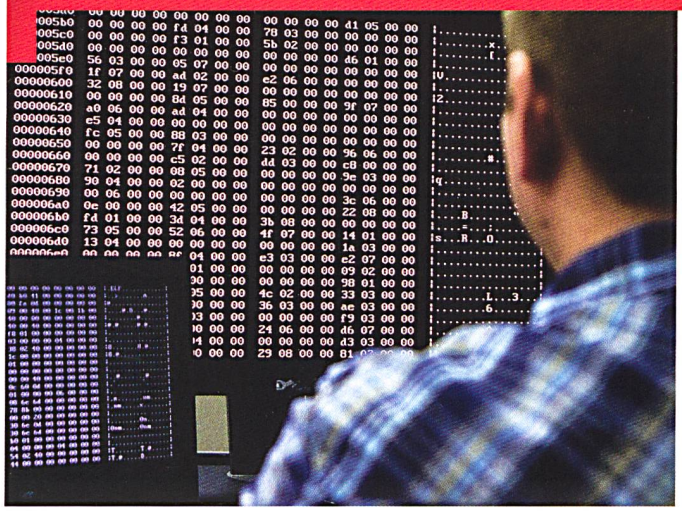
Nutzungsbedingungen
Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Siehe Rechtliche Hinweise.

Conditions d'utilisation
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. Voir Informations légales.

Terms of use
The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. See Legal notice.

Download PDF: 19.10.2024

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch



L'auteur vient de présenter un nouvel ouvrage sur ce thème en 2018.

Cyber

Cyber Security « Best Practice »

Dr. Stefanie Frey, Michael Bartsch
Deutor Cyber Security Solutions Switzerland GmbH

Internet est devenu l'un des espaces économiques et commerciaux les plus importants pour tous les Etats, l'économie et la société. Aujourd'hui, on ne peut plus en faire abstraction. Par des mécanismes de digitalisation, d'automatisation et d'interconnexion, de plus en plus de milieux sociaux ainsi que de processus de commerce sont mis en réseaux. Cela a mené à une spirale technologique qui produit encore plus rapidement les nouvelles technologies et les espaces d'utilisation. Ainsi un champ d'activité varié et lucratif a pris naissance pour des activités criminelles dans et par Internet. Quelle méthode de Cyber-attaque (Cyber- Crime, Cyber-espionnage, Cyber-sabotage) est appliquée par les auteurs, cela dépend de l'objectif de la Cyber-attaque. Le fait est qu'aujourd'hui, chacun se trouve dans le viseur des auteurs.

Les probabilités de cyber-attaques et de leurs effets augmentent constamment. Ainsi la probabilité de Cyber-attaques est évalué au niveau 5, dans le *Risks Report* du World Economic Forum (WEF) 2017, après le terrorisme, la migration et la destruction de l'environnement. Le WEF Report 2018 envisage plus de risques que jamais auparavant et se concentre en particulier sur quatre domaines clé: La destruction de l'environnement, les atteintes à la cyber-sécurité, les coûts économiques et les tensions géopolitiques et estime les Cyber-attaques au niveau 3 et la fraude et le vol de données au niveau 4.[1]

L'étude de défense économique Bitkom de 2017[2] indique que plus que la moitié des entreprises interrogées sont devenues victime de l'espionnage économique, de sabotage ou de vol de données en Allemagne (53 %) au cours des dernières deux années. Ainsi un dommage annuel d'environ 55 milliards d'euros a été créé,[3] Comme le Président de Bitkom, Achim Berg, le disait lors de la publication de l'étude :

« *Les entreprises doivent entreprendre beaucoup plus pour leur sécurité numérique qu'elles ne le font. L'étude montre que le danger pour l'entreprise de tous secteurs et de chaque taille est réel. Chacun peut devenir victime de l'espionnage, du sabotage ou du vol de données.* »[4]

Exemples de « Best Practice » Cyber Security

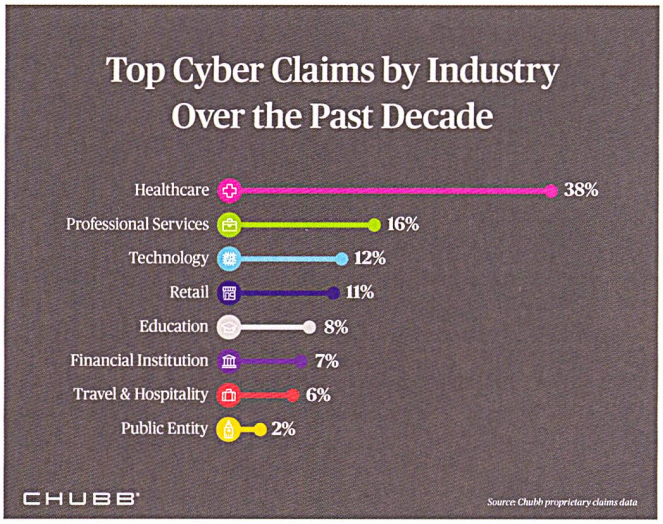
C'est pourquoi, les deux auteurs se sont décidés à traiter résolument du sujet et ont publié en 2017 un premier livre *Cyber-stratégies pour l'entreprise et les administrations : des mesures pour l'augmentation de la résilience* par Springer Vieweg Verlag. De ce livre, il est à retenir que des Etats ont reconnu l'existence des cyber-menaces et des 193 membres de l'Union internationale des télécommunications (UTI), la moitié a développé des cyber-stratégies. Les plus grandes entreprises ne sont pas, encore et malheureusement, des exemples de « Best Practice » qui auraient été prêtes à communiquer sur leur cyber-stratégie et cyber-sécurité. Ainsi l'idée était née d'écrire à la suite du premier livre, un autre sur les exemples de « Best Practice » en matière de cyber-sécurité.

1 Global Risks Report World Economic Forum 2018: https://www.weforum.org/reports/the-global-risks-report-2018, http://www3.weforum.org/docs/WEF_GRR18_Report.pdf.

2 l'étude Bitkom 2017 : https://www.bitkom.org/Presse/Presseinformation/Spionage-Sabotage-Datendiebstahl-Deutscher-Wirtschaft-entsteht-jaehrlich-ein-Schaden-von-55-Milliarden-Euro.html. C'est le résultat d'une étude de l'Association Numérique Bitkom pour laquelle 1069 chefs d'entreprise et responsables de sécurité étaient interrogés, représentatifs de tous les secteurs. En comparaison de la première étude, deux ans auparavant, la part des entreprises concernées s'est accrue non seulement de 51 à 53 pour cent, mais le dommage s'est accru d'environ 8 pour cent, de 51 à 55 milliards d'euros.

3 Pour la Suisse, il n'y a malheureusement aucune étude semblable et aucun chiffre sur de Cyber-attaques sur les entreprises suisses.

4 l'étude Bitkom 2017 : https://www.bitkom.org/Presse/Presseinformation/Spionage-Sabotage-Datendiebstahl-Deutscher-Wirtschaft-entsteht-jaehrlich-ein-Schaden-von-55-Milliarden-Euro.html.



Il sera publié en coopération avec des Co-auteurs compétents des domaines de l'Etat et des administrations, de la défense, de l'industrie IT (utilisateur, fabricant et prestataire de services) ainsi que de la recherche et de l'enseignement. Deux exemples intéressants de la pratique sont ainsi apportés, par lesquels des victimes de cyber-attaques exposent leurs incidents. La première contribution décrit une Cyber-attaque sur l'hôpital de Lukas à Neuss en 2016. La deuxième contribution décrit le dommage considérable pour un commerce d'E-commerce d'un cas de fraude sur une famille suisse, déjà en 2008, mais qui peut se passer encore aujourd'hui. Le livre contient plus de 40 contributions sur plus de 600 pages et il sera publié en août 2018 par Springer Verlag.

Les exemples de « Best Practice » en matière de développement de Cyber-stratégies sont présentés en référence à des fondations de Partnerships Privés-Public, d'architectures de sécurité lors des élections par électronique, de Cyber-Defence dans l'OTAN, en Suisse et en Autriche, à l'étude sur les dommages par Cyber-attaques pour l'économie nationale et la protection des données personnelles durant la construction d'un « Security Monitoring System des Deutschen Bahn ». En ce moment, seulement quelques « Best Practices » peuvent être présentées, car le contenu thématique et la quantité de documents sont lacunaires.

Chez l'utilisateur IT, seulement quelques contributions ont pu être trouvées malheureusement, parce que les entreprises, liées par le secret, voulaient rester anonymes. Ou parce qu'elles n'avaient tout simplement aucune solution (encore) de « Best Practice ». Pour étendre ce sujet à un public plus large, la « Practice Cyber Security Conférence », pour une « Best Practice Cyber Security », aura lieu le 12 décembre à Berlin, suite à la publication du livre.[5]

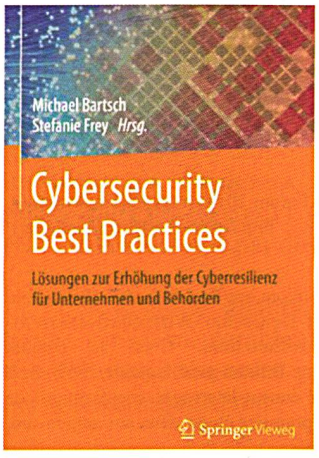
Le besoin et la nécessité existent pour développer la prise de conscience et la compréhension de la Cyber-sécurité, dans le cadre d'une « culture de sécurité » et établir une meilleure compréhension des faiblesses, menaces et risques pour les systèmes IT et les réseaux. C'est pourquoi, la Cyber-sécurité devrait être l'un des objectifs stratégiques les plus importants des Etats et des entreprises.

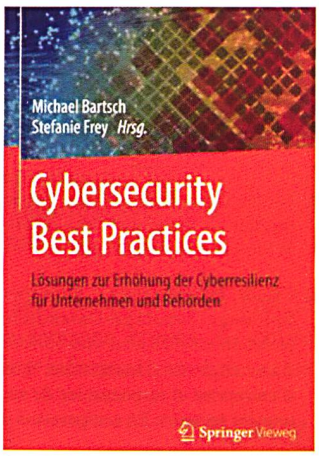
Les deux auteurs de « Deutor Cyber Security Solutions » souhaitent à l'avenir que de plus en plus de « Best Practices » aident les utilisateurs à éviter les Cyber-attaques et que chaque « roue » numérique ne doive pas être réinventée. Les efforts ne doivent pas diminuer, comme le conseiller d'Etat genevois Pierre Maudet l'a écrit si excellemment dans sa contribution :

« La sécurité ne se décrète pas une fois pour toutes. Elle doit être construite et maintenue. Elle doit aussi être adaptée aux risques et aux besoins changeants de la population. Elle doit aussi tenir compte de l'évolution des attentes et des demandes. Pour toutes ces raisons, la sécurité ne doit pas être prise pour argent comptant. Elle doit être maintenue jour après jour et requiert régulièrement, de nouvelles réflexions, des choix du courage et des investisements. »

S. F. ; M. B.

Les auteurs sont atteignables sous : info@deutor.ch
Texte traduit de l'allemand par le cap Gérard Raedler.





5 Annonce et programme : https://gpec.de/index.ph