ASA | SVV

Les assureurs sont des acteurs importants au sein du cyberécosystème

Interview | 17 avril 2024

Dans l’entretien, Christophe Hauert explique les dangers majeurs auxquels sont exposées les entreprises en cas de cyberattaque, la valeur ajoutée d’un certificat de cybersécurité et le rôle du secteur de l'assurance au sein du cyberécosystème.

Christophe Hauert, vous êtes secrétaire général de l'association à but non lucratif Cyber-Safe. Qu’est-ce qui vous a poussé à vous engager personnellement dans la cybersécurité ?

J'ai rédigé ma thèse de doctorat en sciences politiques sur les normes internationales. Le sujet portait sur le mode d’élaboration des normes et la manière dont elles sont ensuite adoptées par le marché. J’avais surtout envie de m’interroger sur le lien entre technologie et questions de société. La cybersécurité en est un bon exemple, car elle ne comporte pas uniquement des aspects techniques, mais aussi des aspects sociaux et organisationnels. Ma contribution, c’est d’apporter mes connaissances en matière de normes.

En 2018, nous avons créé l'association et le label Cyber-Safe pour aider les PME à renforcer leur cyberrésilience. Deux raisons nous ont amenés à prendre cette décision : premièrement, il était évident pour nous que la cybersécurité est importante pour toutes les structures, y compris pour les entreprises de petite taille. Ces dernières travaillent souvent avec des prestataires de services informatiques, et cela soulève fréquemment un problème de confiance. Les PME hésitent à suivre les recommandations de leurs prestataires parce qu'elles pensent que ceux-ci veulent avant tout leur vendre quelque chose. Nous nous sommes alors dit qu’il fallait un prestataire tiers qui n’a aucun intérêt commercial et se contente de dispenser des conseils pour combler le manque de compétences.

Deuxièmement, les coûts sont en général très élevés, car de nombreuses PME ne veulent ou ne peuvent pas se permettre d’honorer des factures à cinq chiffres. Or bien souvent, elles n’ont pas conscience des risques auxquels elles sont exposées. Nous avons donc réfléchi à ce que nous pourrions proposer de sérieux qui prenne tous les aspects possibles en compte, ceci pour 5000 francs environ. L'idée était d'appliquer le principe de Pareto, c'est-à-dire d'obtenir 80 pour cent d'efficacité avec 20 pour cent d'investissement.

Dans l’entretien: Christophe Hauert, secrétaire général de l'association à but non lucratif Cyber-Safe

À cela s'ajoute le fait que la cybersécurité ne relève malheureusement pas encore des éléments mis en avant par les entreprises pour se démarquer de la concurrence. Nous entendons faire bouger les choses. Nous sommes convaincus qu'il faut des incitations économiques pour les PME afin qu’elles en retirent une valeur ajoutée. Les entreprises investissent dans la cybersécurité, notamment pour gagner la confiance de leurs clients.

> « La cybersécurité ne relève malheureusement pas encore des éléments mis en avant par les entreprises pour se démarquer de la concurrence. »

Sur le marché, gagner la confiance de l’autre n’est pas une mince affaire. En matière de cybersécurité, le plus difficile est de convaincre les entreprises, et notamment les PME, que cet aspect est essentiel pour elles. C'est pourquoi nous avons adopté une approche participative de la cybersécurité. Nous ne voulions pas nous appuyer uniquement sur des spécialistes en informatique, ils auraient probablement mis au point une Rolls-Royce. Nous avons donc également invité des utilisateurs, c'est-à-dire des PME, à s’asseoir autour de la table pour discuter d'approches pragmatiques. Cela a permis d’inciter les spécialistes à formuler des exigences réalisables.

Quelle est votre vision pour le label Cyber-Safe ?

Nous entendons créer un écosystème, car nous n'y arriverons pas seuls. Nous devons travailler tous ensemble. Les incitations économiques pourraient consister dans le fait que les PME ayant obtenu le label puissent par exemple souscrire une cyberassurance à un tarif plus avantageux ou remporter plus facilement des appels d’offre des pouvoirs publics. Il faut toujours qu'il y ait aussi une valeur ajoutée économique. D'ailleurs, le label représente également un intérêt pour les banques lorsqu’il s’agit d’octroyer des crédits aux PME. L'objectif, c’est que le label soit reconnu par le plus grand nombre possible d'assurances qui proposent des cyberassurances. Nous souhaitons que les associations professionnelles et les chambres de commerce s'emparent également du sujet. La cybersécurité devrait devenir la norme.

Quels sont les plus grands dangers pour les PME ?

Nous en arrivons ici à l'analyse des risques. Les trois grands dangers sont la confidentialité (confidentiality), l'intégrité (integrity) et la disponibilité (availability). Je demande à chaque PME combien de temps elle pourrait travailler sans accéder à ses données. Quels seraient les coûts impliqués si toutes

les données devenaient soudain publiques et accessibles à tous ? Quel impact auraient une fuite et une perte de données sur son chiffre d'affaires ? Les principaux dangers résident dans la compromission de la confidentialité ou l'indisponibilité des données.

Pourquoi les PME sont-elles victimes de cyberattaques ?

La cybercriminalité consiste en une criminalité de masse. Les pirates informatiques visent tout le monde. Ils s'attaquent à ceux qui cliquent. Il est erroné de penser que mes données n'ont aucune valeur. À cet effet, il faut faire une distinction : les données d'une entreprise ont une valeur sur le darknet et une valeur pour l'entreprise elle-même si elle n'y a plus accès et qu'elle doit les reconstituer. Il faut toujours comparer une offre avec les coûts possibles. Elle n'est peut-être pas aussi chère que cela et consiste vraisemblablement en un investissement intelligent.

> « La question n'est pas de savoir si une entreprise sera touchée par une cyberattaque, mais quand. »

Comment les PME peuvent-elles se protéger efficacement ? Pourquoi la prévention est-elle si importante ?

Au début du processus, nous voulons savoir combien de personnes ne peuvent plus travailler en cas de panne et quel est le montant des dommages en francs. Tout le monde comprend cela. Les mesures de cybersécurité, on ne les prend pas pour faire plaisir au service informatique, mais pour assurer la bonne marche des affaires. Il s'agit de déterminer le risque opérationnel en cas de panne.

La cybersécurité n'est pas un projet ponctuel, c'est l'affaire des chefs. Cela implique une définition claire des responsabilités et des contrôles qualité réguliers. Il faudrait systématiquement commencer par une analyse des risques et se poser ensuite les questions suivantes : comment nous protéger ? Quelle assurance souscrire ? À quels services avoir recours ? En d'autres termes : de quelle protection minimale avons-nous besoin et avec quel risque pouvons-nous vivre ? Ensuite, il s'agit de prendre des mesures. Il faut considérer les choses dans une analyse coûts-bénéfices.

La prévention, c'est un effort minime qui en vaut la peine. Il est essentiel d'agir à la fois sur la probabilité de survenance des cyberrisques et sur leurs répercussions. Par exemple, une campagne de sensibilisation au phishing devrait réduire la probabilité de cliquer sur un lien malveillant. Et une bonne sauvegarde des données minorer l'impact d'un cyberincident. Ainsi, la probabilité d'une cyberdéfaillance est plus faible, les entreprises sont mieux protégées et peuvent également s'attendre à des dommages moins graves en cas d'incident.

Quel est le rôle des assureurs en matière de cyberprévention ?

Les assureurs sont des acteurs de premier plan au sein du cyberécosystème. Il y a souvent des malentendus : soit j'opte pour une cybercertification, soit pour une cyberassurance. Mais ce n'est pas la bonne manière de considérer les choses, les deux sont complémentaires. Des mesures préventives sont incontournables et constituent également une condition préalable à la souscription d'une cyberassurance. Elles sont un levier non négligeable pour inciter les clients à adopter de bonnes pratiques. Dans ce contexte, les assureurs proposent différents services complémentaires tels qu'un processus de réaction aux incidents ou une équipe de gestion de crise. Ils jouent également un rôle essentiel, car ils sensibilisent les PME aux cyberrisques. Ils entretiennent généralement une relation de longue date avec leur clientèle, ce qui leur permet plus facilement d'aborder cette problématique.

> « Dans les entreprises, la cybersécurité, c'est l'affaire des chefs et devrait devenir la norme »

Pourquoi une certification en matière de cyberrésilience est-elle nécessaire ? Quels en sont les avantages ?

L'un des avantages d'une certification en matière de cyberrésilience réside dans le fait que les entreprises mettent en avant leur gestion responsable des cyberrisques pour se démarquer de leurs concurrents. Les PME savent où elles en sont et ce qu'elles doivent faire. Par ailleurs, un certificat garantit que les mesures de protection de base sont effectivement mises en œuvre. Bien sûr, même avec une cybercertification, un risque résiduel subsiste. Or, sans label, il n'y a pas de valeur ajoutée.

Différentes cybercertifications sont proposées sur le marché, à des tarifs plus ou moins élevés. Par exemple, une certification selon la norme ISO 27001 (système de gestion de la sécurité de l'information) coûte souvent plusieurs dizaines de milliers de francs. C'est pourquoi nous sommes une association à but non lucratif et offrons une protection avec des factures généralement à quatre chiffres. Nous avons déjà labellisé 250 organisations, en majorité des PME et des communes.

Sans mentir, Monsieur Hauert, vous êtes-vous déjà fait avoir par des courriels de phishing ?

Non, ou alors pas à ma connaissance (il rit). Nous créons nous-mêmes nos courriels de phishing, je suis donc sensibilisé à cette question. Ceci explique probablement cela. Mais j'ai aussi toujours été extrêmement prudent. En cas de doute, il est recommandé de ne pas cliquer sur le lien et de contacter l'expéditeur par un autre canal afin de vérifier la teneur du message.

Sur la personne :

Christophe Hauert (1978) est titulaire d'un doctorat en sciences politiques de l'université de Lausanne. Sa thèse porte sur la normalisation internationale du point de vue de l'économie politique et sur le rôle des consommateurs dans la reconnaissance et l'adoption des normes ISO. Il exerce actuellement comme chercheur senior à l'université de Lausanne et est également secrétaire général du label suisse de cybersécurité, le label Cyber-Safe, créé par et pour les PME et les communes afin de les rendre plus sûres et plus résistantes.

Cyberrisques | Risques majeurs | Sécurité | Prévention

Vous pourriez être intéressé par ce qui suit

Add to PDF generator

« Beaucoup sous-estiment les risques réels »

René Harlacher, chief underwriting officer auprès de Zurich Suisse et membre du comité Non-vie de l'ASA, explique les problèmes que cela crée.

Rapport annuel 2022 19.06.2023

Plus

Add to PDF generator

Renforcer ensemble la cyberrésilience dans le secteur financier

Quel rôle assume le Swiss FS-CSC en matière de cyberprévention et de gestion des crises ? Interview

d'Alexandra Arni, PDG, et de Gabor Jaimes, membre du conseil d’administration.

Interview 30.01.2024

Plus

Add to PDF generator

« La cybersécurité, c’est l’affaire des chefs »

Pour accroître leur cyberrésilience à long terme, les entreprises ont besoin de mesures de protection efficaces, mais aussi et surtout d’une stratégie claire.

Rapport annuel 2022 19.06.2023

Plus
