CVCI
CHAMBRE VAUDOISE
DU COMMERCE ET
DE L'INDUSTRIE

PME ET CYBERSÉCURITÉ
L'HEURE DE VÉRITÉ

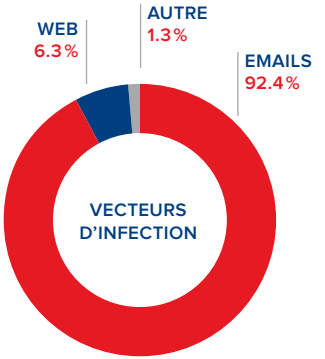
Étude réalisée par la Chambre vaudoise du commerce et de l'industrie.
Textes : Jean-François Krähenbühl, chargé de communication, jfk@cvci.ch
Conception et réalisation : BuxumLunic
Impression : PCL Presses Centrales SA
Mars 2023

SOMMAIRE

1 INTRODUCTION

En 2018, la Chambre vaudoise du commerce et de l'industrie (CVCI) a publié l'étude « Les entreprises vaudoises face aux enjeux de la cybersécurité » pour faire le point sur la réelle menace que faisait peser le piratage informatique sur notre économie. Cette enquête s'achevait sur un constat préoccupant : « Les PME n'ont, de loin, pas toutes conscience des risques liés au cyberespace et de leurs conséquences, et elles doivent impérativement prendre en compte ce paramètre dans leur réflexion stratégique. C'est d'autant plus vrai qu'elles constituent la colonne vertébrale de l'économie vaudoise et qu'elles sont, de ce fait, garantes de la prospérité du Canton. »

Qu'en est-il quatre ans plus tard ? La CVCI a voulu le savoir au travers d'une nouvelle étude qui révèle que le péril cyber a encore pris de l'ampleur avec l'accélération de la numérisation. La sophistication dont font preuve les hackeurs a fait exploser les cas de piratage et, avec eux, les demandes de rançon. A dire d'expert, 40 % des PME passeraient même à la caisse. Le télétravail, dopé par la pandémie, a contribué à compliquer cette donne sécuritaire pour les entreprises. De ce fait, les PME sont de plus en plus visées par les piratages informatiques. Même si les entreprises ont davantage pris conscience de ces dangers, elles constituent toujours des cibles faciles dans la mesure où les PME ne disposent pas toujours des moyens nécessaires pour investir autant dans leur sécurité informatique que les grandes sociétés. Cela vaut autant pour le matériel que pour le facteur humain. Trop souvent, le manque de sensibilisation à l'intention des employés pousse ces derniers à cliquer sur des liens malicieux. L'email reste le vecteur le plus important d'infection avec plus de 90 % des cas.



SOURCE: 2018 VERIZON DATA BREACH INVESTIGATIONS REPORT

C'est dire s'il reste beaucoup à faire pour parer à la menace cyber. La formule déclinée sans cesse selon laquelle « la question n'est pas de savoir si une PME va être attaquée, mais quand » conserve toute son actualité.

Notre enquête dans le monde du piratage fait le point sur les nouveaux périls informatiques qui menacent les entreprises tout en fournissant des outils pour faire face à ce fléau. Nous avons sondé nos membres pour évaluer leur degré de préparation face aux cyberattaques. La publication que vous tenez entre les mains aborde par ailleurs divers aspects en lien avec la cybersécurité comme le rôle des institutions privées et des collectivités publiques dans la résilience informatique des entreprises, ainsi qu'une série de bonnes pratiques à suivre pour se protéger au mieux des cyberattaques et d'y faire face au mieux lorsqu'elles surviennent.

SEULS 42,39 %
DES SONDÉS
DIFFUSENT
UNE INFORMATION
RÉGULIÈRE
SUR LEUR INTRANET,
ALORS
QU'UN PETIT TIERS
PROCÈDE À DES TESTS
DE PHISHING.

II
PRISE DE CONSCIENCE DES ENTREPRISES VAUDOISES

Le sondage ciblé que nous avons réalisé l'an dernier auprès d'une centaine d'entreprises de toutes tailles et de tous secteurs confirme que la cybersécurité est devenue un enjeu central pour les entreprises, au même titre que les soucis d'approvisionnement énergétique et de la supply chain. Par rapport à notre étude d'il y a quatre ans, les résultats montrent une plus grande prise de conscience des chefs d'entreprise face aux cyber-risques. En 2018, un tiers des sociétés sondées estimaient ne pas être concernées par les cyber-risques, notamment en raison de leur petite taille. Aujourd'hui, plus de 90 % disent que la cybersécurité est une préoccupation. Cela ne signifie pas pour autant qu'elles investissent suffisamment pour leur protection. Les coûts dans ce domaine restent un facteur important.

Les sociétés sondées s'informent pour les ⅔ par les médias et par Internet, et pour un peu plus de 50 % à travers les associations professionnelles. Les formations représentent 43 % des informations recueillies.

S'agissant des infrastructures informatiques, notre enquête révèle que 96,74 % des entreprises disposent d'un pare-feu, alors que 88 % ont des sauvegardes multiples et procèdent à des mises à jour régulière des systèmes. Un peu moins de 50 % protègent leurs données via un cloud et un tiers cryptent leurs données. C'est bien, mais cela ne garantit pas une protection efficace. Le point faible des entreprises reste le collaborateur qui, par mégarde ou par méconnaissance, va cliquer sur un document ou un lien compromis reçu par messagerie. D'où l'importance de sensibiliser le personnel. A ce propos, notre sondage montre que plus de 90 % des sociétés disent se préoccuper de cet aspect. Seules 42,39 % diffusent une information régulière sur leur intranet, alors qu'un petit tiers procède à des tests de phishing. En outre, 54,44 % d'entre elles dispensent des formations spécifiques au personnel ou le projettent.

90%
DES SONDÉS
SE PRÉOCCUPENT
DE CYBERSÉCURITÉ

A la question de savoir si elles avaient été victimes de cyberattaques, 20 % ont répondu par l'affirmative. Sur celles-ci, seules 42,86 % ont annoncé le piratage aux autorités et moins de 5 % ont payé une rançon. Côté dommages subis, les entreprises concernées les estiment entre 4000 et 30 000 francs. Les mesures de protection contre les cyberattaques impliquent de gros investissements pour 16,48 % des sociétés sondées. Un peu moins de 40 % les jugent assez importants alors qu'une proportion identique les estime peu importants.

Un tiers révèle avoir souscrit une cyberassurance, ce qui indique que ce moyen de se prémunir prend de l'ampleur et semble même promis à un bel avenir. Le spécialiste du domaine qui s'exprime dans notre étude le confirme, d'ailleurs.

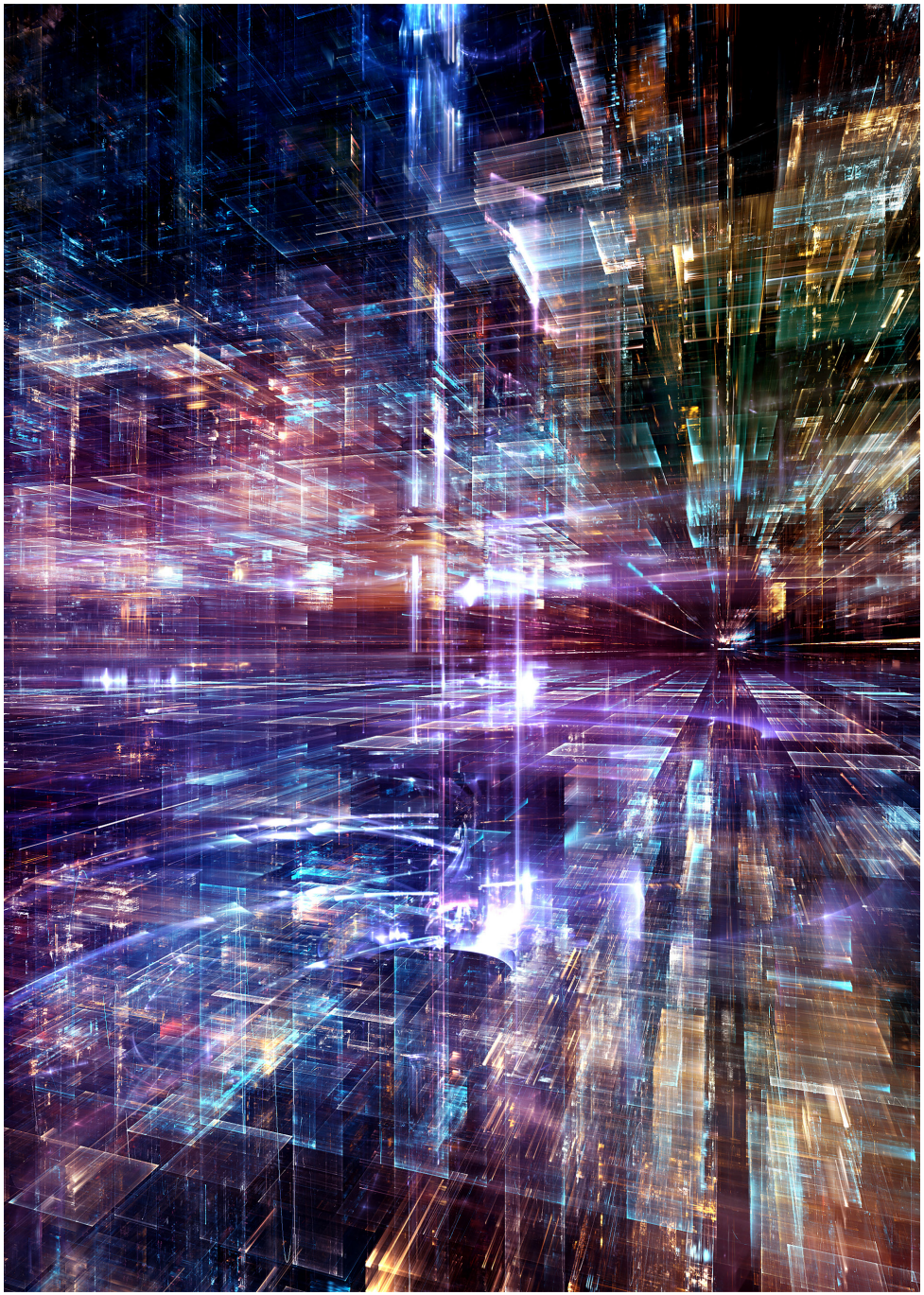
La politique d'information de la Confédération dans le secteur de la défense du cyberespace est évaluée avec une certaine circonspection par nos entreprises membres. Ainsi, seules 3,26 % d'entre elles la jugent très bonne et 34,78 % bonne. La moitié des sociétés sondées estiment qu'elle peut mieux faire, alors qu'un peu plus de 10 % la jugent carrément insuffisante.

Le dernier volet de notre sondage, qui a trait à la mise en œuvre du RGPD et, prochainement, de la loi sur la protection des données, a donné un résultat mitigé : 46,67 % des entreprises sondées s'en sont préoccupé, alors que 53,33 % ne semblent guère s'en soucier.

Globalement, la prise de conscience des dangers cyber a progressé ces dernières années. La question des équipements informatiques et de la sensibilisation des collaborateurs reste centrale. Se protéger, c'est bien. Mais au-delà de ces aspects, aujourd'hui, les spécialistes du domaine estiment que la priorité consiste pour les entreprises à se préparer, et à savoir réagir quand la PME est attaquée, car malgré tous les systèmes de protection et la sensibilisation, une attaque peut survenir. D'où l'importance de se préparer à la gestion de crise (plan de continuité), à savoir prévoir ce qui doit être protégé et comment. Où est-ce que la PME place ses forces ? Quelle est la première personne à appeler ? Il faut être très pratique lorsque de tels cas surviennent.

20%
DES SONDÉS
DISENT AVOIR ÉTÉ VICTIMES
D'UNE CYBERATTAQUE

LES SPÉCIALISTES DU DOMAINE ESTIMENT QUE LA PRIORITÉ CONSISTE POUR LES ENTREPRISES À SE PRÉPARER, ET À SAVOIR RÉAGIR QUAND LA PME EST ATTAQUÉE.



ÉVOLUTION AU COURS DES DERNIÈRES ANNÉES

Le Centre national pour la cybersécurité (NCSC), centre de compétences de la Confédération en la matière, constate que le nombre de cyberattaques par courriel ou par message instantané ne cesse d'augmenter. Le mode opératoire des cybercriminels repose souvent sur l'envoi d'un email frauduleux conçu pour sembler authentique et qui vous demande de fournir des informations personnelles sensibles. Ces messages d'hameçonnage contiennent pourtant souvent des erreurs grammaticales, des fautes d'orthographe et d'autres erreurs flagrantes que les grandes entreprises ne commettraient pas. Les logos sont souvent imités grossièrement.

Les auteurs tentent aussi de piéger leurs victimes en leur adressant des courriels leur promettant des gains importants ou un héritage quelconque ou encore en prétendant que leur ordinateur a été piraté. Il n'est pas toujours facile de repérer l'escroquerie, car les cybercriminels deviennent de plus en plus astucieux. Ils abusent fréquemment des faiblesses psychologiques de leurs victimes en leur insufflant un sentiment de peur ou d'urgence, ou en tirant profit de leur affolement et de leur inattention.

Dans une interview donnée à Swissmem en février 2022, faîtière de l'industrie des machines, Florian Schütz, directeur du NCSC, explique que «les auteurs de cyberattaques sont très innovants et appliquent sans cesse de nouveaux scénarios. Chaque semaine, le NCSC recense sur son site Internet des nouvelles méthodes. Les agresseurs opèrent de manière toujours plus professionnelle. Certains groupes se spécialisent dans des domaines particuliers de toute la panoplie d'attaques criminelles. D'autres cherchent de manière ciblée les maillons faibles. Tout comme les pirates informatiques s'adaptent aux nouvelles circonstances, les entreprises doivent également analyser et actualiser régulièrement leurs systèmes de sécurité.»

42E
RANG
PLACE DE LA SUISSE
AU CLASSEMENT MONDIAL DE
LA CYBERSÉCURITÉ DE L'UIT

En ce début d'année, le Centre national de cybersécurité (NCSC) a constaté un regain d'intensité des cyberfraudes dites « arnaques au CEO » ou « arnaques au président » en Suisse. Les criminels visent surtout les entreprises de Suisse romande. Ils ne se contentent plus d'envoyer des courriels, mais appellent souvent leurs victimes. Ce type d'arnaques fait référence à des malversations pour lesquelles les fraudeurs cherchent d'abord les noms du directeur et du responsable financier de l'entreprise ciblée. Pour ce faire, ils se servent de sources accessibles publiquement sur le Web. Ils falsifient ensuite un e-mail prétendument envoyé par le CEO, à l'attention du responsable financier. Le message demande d'effectuer un paiement pour une affaire prétendument urgente et confidentielle.

Toutefois, relève le NCSC, les escrocs ne se contentent pas de l'email et vont ainsi jusqu'à appeler le responsable financier par téléphone. Ils s'y présentent comme un certain Me Muller, employé d'un cabinet d'audit connu. Au cours de la conversation, ils affirment connaître le directeur de l'entreprise et que celui-ci les a directement dirigés vers le responsable financier. Ajoutant que le directeur les contacterait rapidement par courriel avec des instructions pour le paiement.

Pour prévenir ce type d'arnaque, le rapport du NSCS formule plusieurs recommandations. Il convient notamment de sensibiliser tous les collaborateurs, y compris celles et ceux qui travaillent au service financier ou qui ont des postes clés. Il est en outre conseillé de faire preuve de la plus grande vigilance avec les demandes de paiement. « Tous les processus relatifs aux opérations de paiement doivent être clairement réglementés au sein de l'entreprise et appliqués par les collaborateurs et collaboratrices dans tous les cas », souligne encore le NCSC.

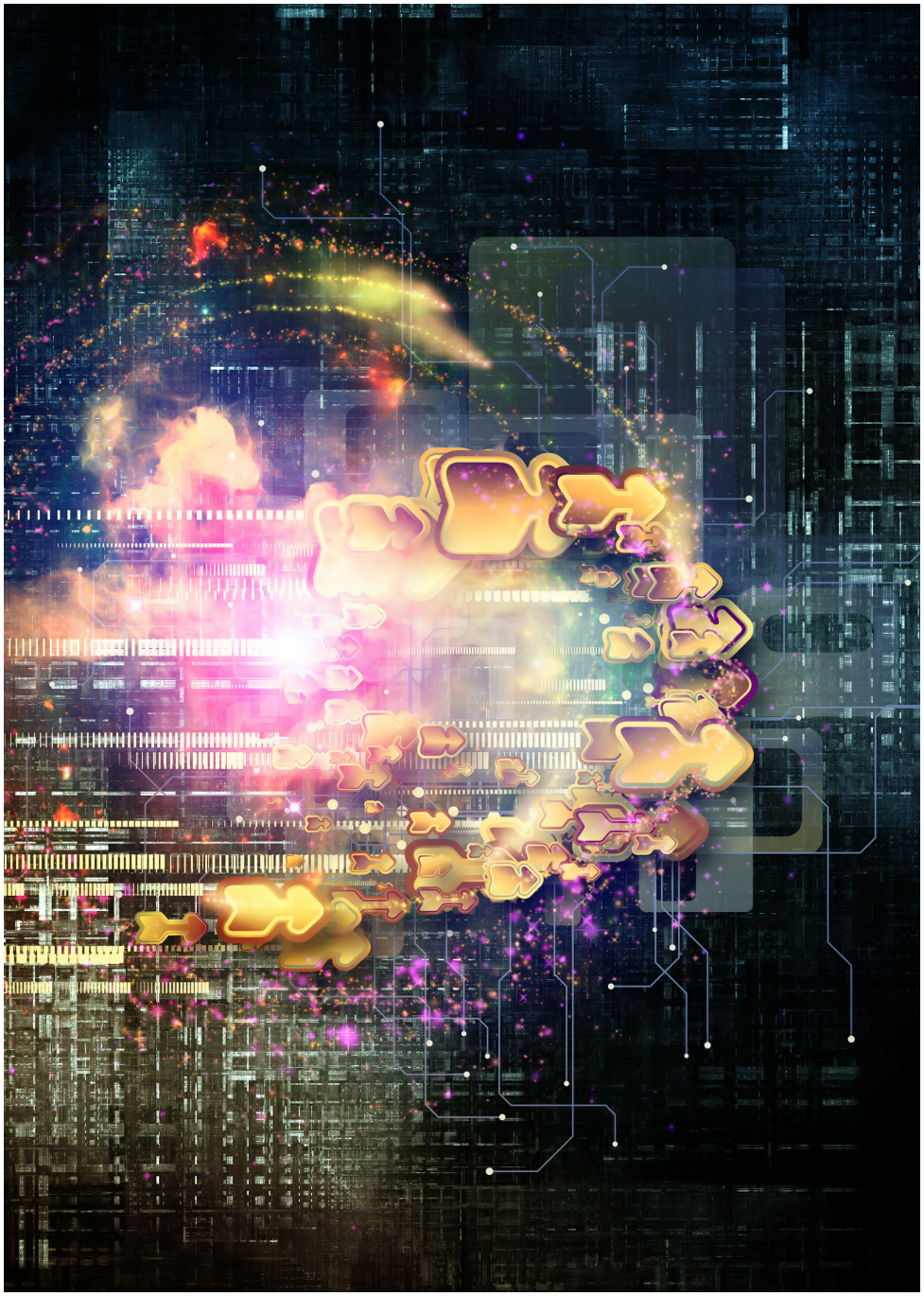
A l'instar des opérations malveillantes rapportées par le NCSC, les cybercriminels n'hésitent plus à multiplier des canaux de communication pour perpétrer leurs arnaques. Comme en témoigne la récente vague de cyberattaques et de cyberescroqueries touchant des hôtels et leurs clients via une plateforme de réservation.

La pandémie de Covid-19, qui a touché la planète au début de 2020, a clairement accéléré la numérisation dans le monde entier à travers la généralisation du télétravail, accentuant ainsi la vulnérabilité des entreprises aux cyberattaques.

Le NCSC formule sur son site des recommandations de base à l'intention des entreprises : établir un plan de communication ; préparer un plan de continuité d'activité ; informer les clients de façon proactive en cas de pertes de données, et avertir le préposé fédéral à la protection des données selon le type des données compromises ; déposer une dénonciation pénale à la police cantonale.

50 000
FRANCS
BUDGET ANNUEL MOYEN NÉCESSAIRE
POUR LA CYBERPROTECTION

LA PANDÉMIE DE COVID-19 A ACCÉLÉRÉ **LA NUMÉRISATION DANS LE MONDE** ENTIER À TRAVERS **LA GÉNÉRALISATION DU TÉLÉTRAVAIL**, ACCENTUANT AINSI LA VULNÉRABILITÉ DES ENTREPRISES AUX CYBERATTAQUES.



IV
LE RÔLE DES COLLECTIVITÉS PUBLIQUES

La question du rôle que doivent jouer la Confédération et les cantons dans le domaine de la cybersécurité est récurrente. Dans une motion déposée en 2021, la conseillère aux Etats fribourgeoise Johanna Gapany s'étonnait que « seules les infrastructures critiques font l'objet d'une protection fédérale contre les cyberattaques. Toutefois, il n'existe aucune protection en faveur des administrations publiques et des PME dans leur ensemble. Pourtant, aussi bien les PME que les administrations publiques cantonales et communales constituent des infrastructures critiques pour assurer le bon fonctionnement du pays. » La parlementaire demandait donc au Conseil fédéral « d'étendre la protection fédérale contre les cyberattaques aux cantons, aux communes et aux PME dans leur ensemble ».

Dans sa réponse, le gouvernement a admis « la très grande importance que revêtent la protection des PME ainsi que celle des administrations cantonales et communales contre les cyberattaques ». Il rejetait toutefois les critiques de la motionnaire concernant un manque d'engagement dans ce domaine, expliquant qu'il avait pris différentes mesures dans le cadre de la Stratégie nationale de protection de la Suisse contre les cyber-risques, en créant notamment le Centre national pour la cybersécurité (NCSC) en 2019. Il poursuivait en relevant qu'il était prêt à étoffer, en les adaptant aux besoins, les prestations que la Confédération fournit aux administrations et aux PME, et à élaborer les bases légales nécessaires à cet effet. Il maintenait cependant qu'en vertu du principe de subsidiarité, « la responsabilité de la protection contre les cyberattaques ne peut être reportée sur la Confédération, mais qu'elle doit continuer d'incomber aux administrations et aux PME ».

Les choses bougent néanmoins du côté de Berne : en mai 2022, le Conseil fédéral a pris connaissance du rapport d'évaluation de l'efficacité de la stratégie nationale de protection de la Suisse contre les cyber-risques 2018–2022 et a décidé de créer 25 postes supplémentaires dédiés à la protection contre les cyber-risques. Début décembre, il a décidé de rattacher le Centre national pour la cybersécurité (NCSC) au sein du Département fédéral des finances (DFF) et de le transformer ainsi en office fédéral. Le DDPS a chargé ce dernier de mettre en place les structures du nouvel office, en collaboration avec le DFF, d'ici à fin mars 2023.

25
POSTES
SUPPLÉMENTAIRES SERONT DÉDIÉS À LA LUTTE CONTRE LES CYBER-RISQUES

L'office disposera d'une septantaine de postes de travail et ses activités resteront inchangées par rapport à celles du NCSC. Il demeurera une unité civile de l'administration fédérale. Il aura pour mission d'aider la population et les acteurs économiques à gérer les cyberincidents, de mettre à disposition un guichet national unique pour le signalement des cyberattaques et les questions sur le sujet, de diffuser informations, avertissements et mesures de protection concernant les cybermenaces, de sensibiliser le grand public et d'assurer la protection de l'administration fédérale.

Parallèlement, le Gouvernement souhaite mettre en place une obligation de signaler les cyberattaques contre les infrastructures critiques, à savoir les autorités publiques, les hôpitaux et laboratoires, les entreprises actives dans l'énergie, les Hautes écoles, les organisations ayant des tâches publiques (sauvetage, traitement des eaux), les banques et les assurances. Début décembre, il a adopté à l'intention du Parlement le message relatif à la modification de la loi sur la sécurité de l'information au sein de la Confédération. Le projet crée les bases légales nécessaires à l'obligation de signaler pour les exploitants d'infrastructures critiques et définit les tâches du Centre national pour la cybersécurité (NCSC), qu'il institue comme guichet unique de signalement des cyberattaques. L'une des principales préoccupations formulées pendant la consultation est que cette obligation soit mise en œuvre avec le moins de formalités possible et qu'elle n'entraîne pas de charge administrative supplémentaire importante.

Afin que les signalements soient aussi simples que possible à effectuer, le NCSC mettra à disposition un formulaire électronique qui pourra être rempli facilement et, au besoin, être transmis directement à d'autres services. En outre, le projet de modification de la loi n'oblige pas seulement les entreprises à participer à la protection contre les cyberattaques, mais contraint également le NCSC à offrir aux auteurs de signalements, à titre subsidiaire, un soutien pour faire face aux cyberattaques. Par ailleurs, la loi définit la manière dont le NCSC aide les entreprises et la population à se protéger contre les cybermenaces. Elle règle notamment la fonction du NCSC en tant que guichet pour les questions relatives aux cybermenaces et pour le signalement des cyberattaques.

Dans le cadre de la modification de cette loi la question s'est posée de savoir si les entreprises privées, a fortiori les PME, devaient elles aussi être soumises à une obligation de signalement. A ce propos, le CVCI avait soutenu que celle-ci constituait a priori une atteinte à la liberté économique. Cela dit, au vu de l'importance de la problématique, elle ajoutait qu'une telle obligation pourrait être envisagée dans la mesure où elle n'implique pas des démarches administratives lourdes. La CVCI était en tous les cas d'avis qu'une sensibilisation accrue des collaborateurs au sein des entreprises est indispensable.

LE CONSEIL FÉDÉRAL
A DÉCIDÉ DE FAIRE
DU CENTRE NATIONAL
POUR LA CYBERSÉCURITÉ
UN OFFICE FÉDÉRAL
À PART ENTIÈRE.

V
L'APPUI DU SECTEUR PRIVÉ

Les autorités fédérales le rappellent régulièrement dans leurs diverses communications : les entreprises et les institutions sont en premier lieu responsables de leur protection contre les cyberattaques. L'Etat estime donc qu'il joue un rôle subsidiaire dans ce domaine, du moins dans notre pays. Nos voisins de l'Union européenne ont adopté une vision plus interventionniste en investissant des centaines de millions de francs depuis plus de dix ans. Le positionnement est différent en Suisse.

Dans le secteur privé, quantité de sociétés spécialisées dans la cybersécurité proposent leurs services aux entreprises. A côté de cela, un certain nombre d'organismes œuvrent dans le domaine pour épauler les sociétés. C'est notamment le cas de l'association Le Clusis.

Interview de sa présidente.

«ADOPTER LES BONS RÉFLEXES SÉCURITAIRES DOIT DEVENIR UNE HABITUDE»

Ancienne conseillère d'Etat et conseillère nationale, la Neuchâteloise Sylvie Perrinjaquet a siégé à Berne au sein de la Commission de politique de sécurité et c'est dans ce cadre qu'elle a été sollicitée par le Clusis. Cette association suisse, fondée en 1989, est une plateforme d'échanges dans le domaine de la sécurité de l'information qui réunit des experts provenant de l'environnement cyber et du monde politique, économique et académique en Suisse et à l'étranger. Sylvie Perrinjaquet en est aujourd'hui la présidente.

Le Clusis est reconnu comme un pôle d'expertise dans le domaine de la sécurité de l'information. Quel est son rôle et quels services offre-t-il?

Le Clusis propose principalement de la sensibilisation, de la formation liée à la cybersécurité et à la confiance numérique, au travers de conférences, en présentiel ou virtuel. L'Association met à disposition des experts issus de l'environnement IT, pour des conférences portant sur des contenus spécifiques. Nous favorisons la mise en relation entre les personnes concernées et nous répondons aux consultations de la Confédération. Le Clusis participe en outre à une émission mensuelle sur Léman Bleu, «CyberEtik», qui aborde des thèmes liés à la confiance numérique et à sa sécurité, à l'intention des entreprises. Nous sommes une force de proposition pour nombre de partenariats.

Qui peut recourir à ses services et pour quel prix?

Toutes les entreprises, associations, fondations, particuliers ou structures désireuses d'obtenir des informations de notre part peuvent nous rejoindre. La cotisation annuelle s'élève à 250 francs par membre individuel, 500 francs par membre entreprise, le reste de notre financement étant assuré par des sponsors. Le Clusis collabore aussi avec les universités et les HES. Je pense par ailleurs que nous avons tout un travail à faire dans le domaine de l'école obligatoire au niveau de la maturité numérique.

En observant le domaine cyber depuis quelques années, on peut avoir le sentiment que les PME n'ont pas toutes pris la mesure des risques de cyberattaques: votre avis?

Je pense que les PME sont confrontées à deux problèmes. Au niveau interne, les collaborateurs et les collaboratrices constituent le risque le plus important en raison de leur manque de conscience des dangers liés au piratage. A l'externe, les risques proviennent de leurs fournisseurs ou intermédiaires qui n'ont pas forcément mis en place un concept de sécurité informatique. Ont-ils pris la mesure de ces dangers? Je n'en suis pas certaine, notamment déjà au niveau de leur modèle de gouvernance. Aujourd'hui, je pars du principe qu'un chef d'entreprise, un conseil d'administration ou toute entité décisionnelle doit en permanence se poser la question quant à savoir si la sécurité de ses données sensibles, son modèle de management sont intégrés dans la gestion de l'entreprise et accompagnent les processus d'un point de vue financier. Ces enjeux numériques impliquent des investissements, parfois conséquents. Dans tout budget, la sécurité informatique doit être intégrée, car une entreprise hackée peut perdre ses données, ses domaines d'expertise, ses compétences et même fermer!

Quelles sont les nouvelles menaces cyber pour les entreprises?

Les attaques sont plus sophistiquées, mais elles auront toujours le même objectif: prendre vos données sensibles, vos compétences et la valeur de votre entreprise.

A quoi les sociétés doivent-elles faire attention?

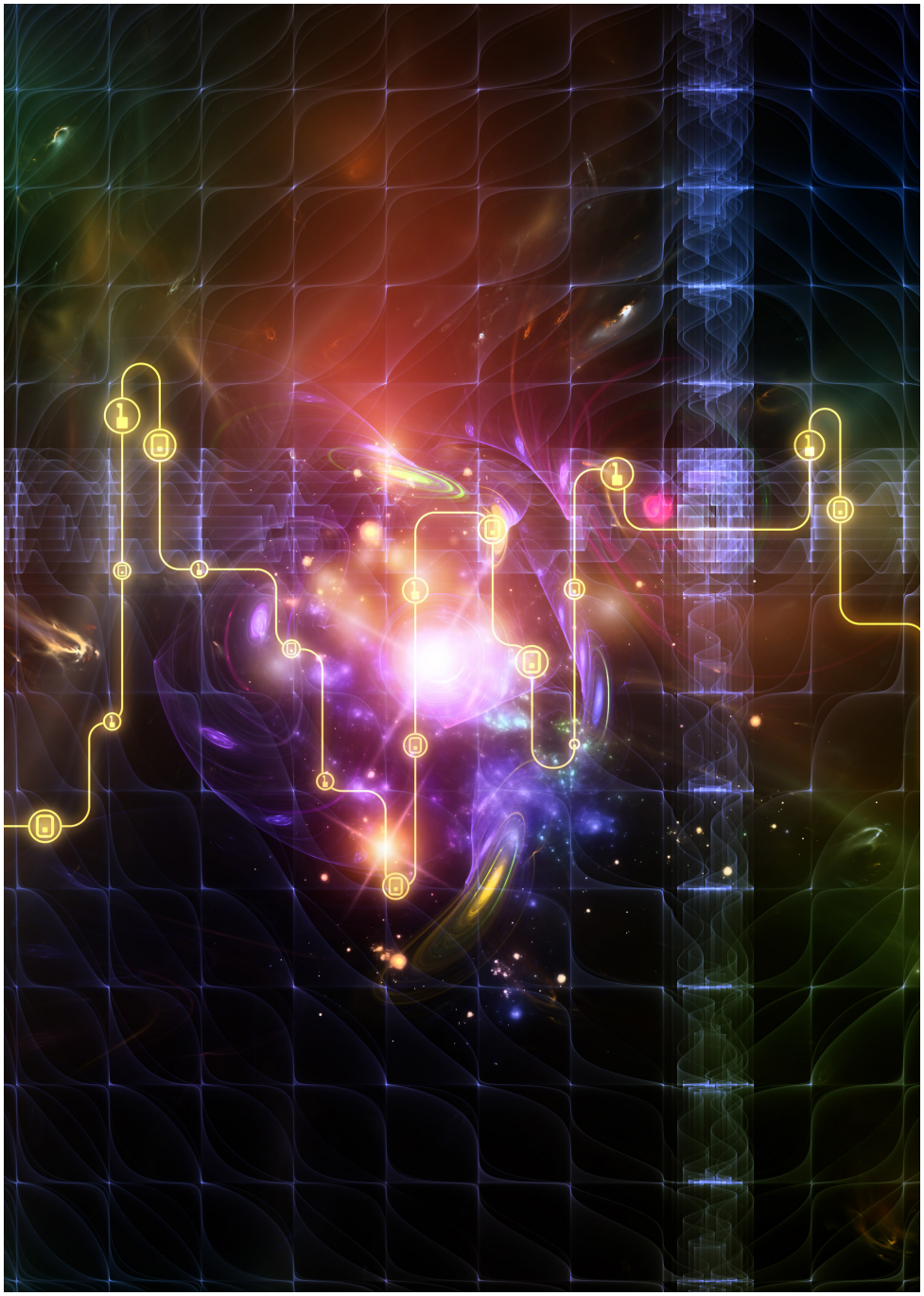
Elles doivent absolument former leurs collaborateurs et collaboratrices et cela régulièrement! Adopter les bons réflexes sécuritaires doit devenir une habitude, un mode de fonctionnement naturel. Autre paramètre à gérer: le télétravail, qui s'est largement répandu pendant la pandémie. A la maison, est-ce que les employés et employées respectent les processus? Avec quel ordinateur travaillent-ils? Ont-ils accès aux données sensibles de l'entreprise? Cela vaut également pour le télétravail hors frontière. Et puis, une entreprise qui conclut des contrats avec un fournisseur suisse ou étranger doit aussi s'assurer que ce dernier a mis en place les mesures de sécurité, comme ISO 27001. Cela doit figurer dans le contrat.

Selon vous, les collectivités publiques, Confédération en tête, informent-elles suffisamment les entreprises et les particuliers sur les cyber-risques? Quel doit être leur rôle?

Je pense que la Confédération met à disposition toutes les informations utiles pour une entreprise, mais c'est à cette dernière d'aller les chercher et c'est complexe! Le site du Centre national pour la cybersécurité (NCSC) est très complet. Je suis consciente qu'une PME n'a pas forcément le temps de se pencher sur la problématique. Le Clusis doit jouer un rôle pour transmettre, vulgariser et cibler ces informations pour que les entreprises les mettent en place. On voit cela avec l'entrée en vigueur, en septembre 2023, de la nouvelle loi sur la protection des données (nLPD). C'est une obligation. Combien de sociétés s'y préparent-elles? Peu en vérité. C'est un beau défi pour les entreprises, qui vont devoir définir quelles sont leurs données sensibles, entre autres. Elles doivent vraiment s'y préparer, car on ne peut plus ignorer la sécurité cyber.

Quelles sont les priorités dans le domaine cyber?

Renforcer les modèles de gouvernance, de management et appliquer en bonne et due forme la nLPD constituent pour moi des priorités. Le Clusis ambitionne de contribuer à renforcer la maturité des entreprises et la collaboration avec les écoles, ainsi que la coopération avec les parlementaires. Le numérique ne fait pas encore totalement partie de la réflexion des Chambres fédérales. Jusqu'à fin 2022, le domaine cyber était réparti entre plusieurs départements. Le Conseil fédéral vient de transférer l'Office fédéral de la cybersécurité au DDPS de Viola Amherd, cela renforcera la cybersécurité en Suisse et devrait permettre une meilleure communication auprès des citoyens et citoyennes et des PME implantées en Suisse.



VI
UN PROGRAMME POUR SOUTENIR LES PME

Sensibiliser les entreprises aux cyber-risques est à la fois l'affaire des collectivités publiques et d'organismes privés. Des initiatives de toutes sortes ont émergé ces dernières années dans le domaine. Dans l'Arc lémanique, l'une d'elles mérite une mention particulière : il s'agit de la Trust Valley. Lancée conjointement par les cantons de Vaud et de Genève avec le concours d'institutions académiques et d'acteurs économiques privés, elle constitue une alliance visant à promouvoir toute l'expertise de la région dans le domaine de la confiance numérique et la cybersécurité.

Ce pôle de compétences unique favorise l'éclosion de projets novateurs, comme le programme Trust4SMEs, que la CVCI cofinance. Il propose à un certain nombre de PME de renforcer leur cyber-résilience.

Présentation à travers l'interview de sa CEO, Lennig Pedron.

«NOTRE RÉGION A TOUT POUR BIEN FAIRE»

CEO de la Trust Valley, Lennig Pedron vient de l'entreprenariat. La cybersécurité est devenue une passion qu'elle exerce depuis plus de quinze ans. Elle intervient aussi sur mandats, notamment auprès des autorités policières. Prise de température de l'écosystème vaudois.

Trust Valley regroupe tout ce que l'Arc lémanique compte de compétences en matière de confiance numérique et de cybersécurité. Quel bilan tirez-vous après trois ans d'activités ?

La Trust Valley a été lancée officiellement en octobre 2020. Le besoin de se mettre en réseau et de mettre en mouvement cet écosystème lémanique a été confirmé pour arriver à des résultats concrets. Cela se fait à travers des programmes et des projets pour faire avancer la maturité numérique de la région.

Quels sont les nouveaux périls numériques auxquels les PME sont confrontées ? Quels conseils leur donnez-vous ?

On ne va pas arrêter tous les cybercriminels. Ils sont bien organisés et ne cessent de se développer. Ils auront de toute manière toujours une longueur d'avance. L'idée reste de se prévenir les uns les autres. On essaie d'instiller l'idée de coopération régionale puisque si une PME déclare un piratage, cela sert aux autres. La priorité, c'est de se préparer, et de savoir réagir quand la PME est piratée. Ce que l'on voit, c'est l'importance du niveau de préparation à la gestion de crise (plan de continuité), à savoir prévoir ce qui doit être protégé et comment. Où est-ce que je place mes forces ? Quand les PME ont un peu de budget, elles font souvent un audit de sécurité et proposent une sensibilisation aux collaborateurs. Aujourd'hui, on leur dit plutôt d'imaginer des cas de piraterie. Comment réagissent-elles ? Qui est la première personne à appeler ? Il faut être très pratique dans un tel cas. Il y a un grand besoin d'information.

Trust Valley a lancé au printemps 2022 le programme Trust4SMEs, qui a offert à 25 PME une série d'interventions destinées à renforcer la compréhension des cyber-risques et à mieux se préparer à l'inévitable. Quel est le bilan ? L'expérience se poursuivra-t-elle ?

Pour les PME, la participation au programme Trust4SMEs va de 1500 à 5000 francs selon la taille de l'entreprise. Avec le programme, on offre a minima 50 000 francs de prestations sur une année. Cela équivaut au budget annuel moyen nécessaire de cyberprotection. Le programme s'est terminé le 9 février dernier. On l'a prolongé pour finir par une grande sensibilisation destinée à 600 collaborateurs de ces 25 PME. Ce programme pilote a été très riche avec des ateliers, des rencontres, des cercles de discussion. Le constat que l'on fait est que les PME ont besoin d'ateliers concrets avec des partages d'expériences entre pairs. Un autre constat est que les PME nous ont demandé que l'on s'adresse à leurs conseils d'administration et à leurs directions pour qu'ils prennent conscience de la problématique et qu'ils s'engagent, ce qui n'est pas encore toujours le cas. Il y a beaucoup de pression sur les équipes opérationnelles, dont la cybersécurité n'est pas le cœur de métier. Beaucoup de cas ont été médiatisés. La prise de conscience existe, il faut maintenant s'engager et monter en compétence. On réfléchit à créer un groupe d'alumni permettant à ceux-ci de suivre les développements de notre programme, qui est reconduit.

Selon des chiffres que vous avez articulés récemment, 40 % des entreprises hackées paient une rançon alors que les autorités recommandent de ne pas céder. Un commentaire ?

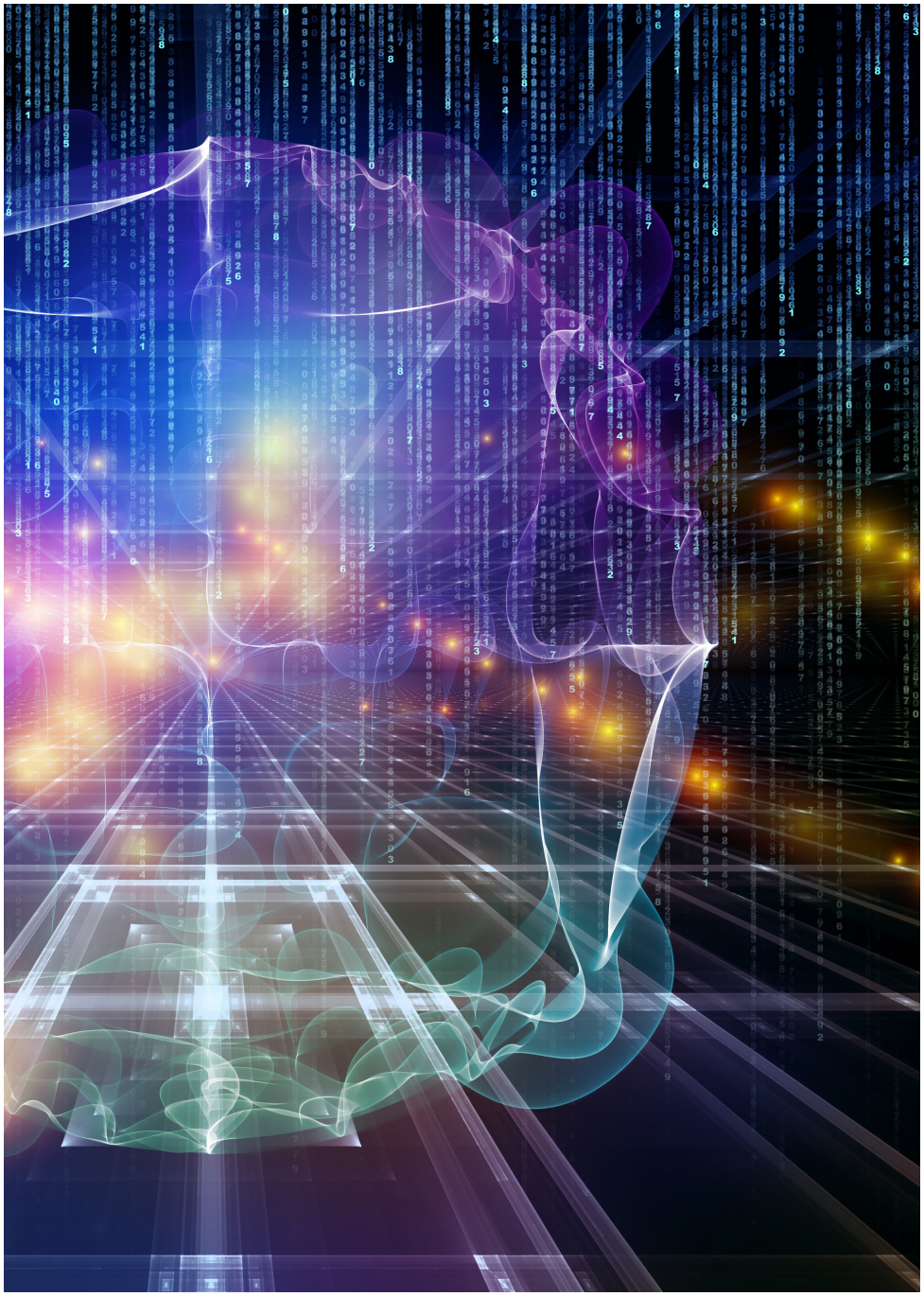
La bonne pratique consiste à ne pas payer la rançon, mais cela dit, lorsqu'on se trouve dans une situation d'urgence, soit on ferme soit on paie. Il existe des cyberassurances qui remboursent. Mais je dirais qu'il s'agit d'une décision personnelle. La ville de Rolle a décidé de ne pas payer de rançon et voit ses données se balader sur le Darknet. Mais je ne vois pas une collectivité payer et financer de facto des criminels. Une assurance américaine a payé une rançon de 41 millions de dollars…

Le classement mondial de la cybersécurité de l'Union internationale des télécommunications (UIT) plaçait en 2021 la Suisse à la 42e place mondiale, entre la Macédoine du Nord et le Ghana. La Suisse peut mieux faire…

La Suisse reste un petit pays et de fait, il n'est pas si aisé de se mettre au niveau des grands. Si on était membre de l'UE, on pourrait bénéficier du système européen, mais ce n'est pas le cas. L'Office fédéral qui sera positionné sous le DDPS à Berne peut nous aider à progresser dans ce classement. Brad Smith, patron de Microsoft, a exprimé qu'avec nos Hautes écoles et nos entreprises de pointe dans la cybersécurité, on est la région au monde qui a tout pour bien faire. On dispose donc d'une marge de progression assez bonne.

Selon vous, les collectivités publiques, Confédération en tête, informent-elles suffisamment les entreprises et les particuliers sur les cyber-risques ? Quel doit être leur rôle ?

L'information et le soutien doivent encore progresser. Quand on a monté notre programme Trust4SMEs, il a fallu en premier lieu convaincre le privé et le public. Le premier à réagir a été le canton de Vaud, qui a investi et renouvelé en 2023. Aujourd'hui le programme approche le million de francs suisses. Au niveau fédéral, il y a le Centre national pour la cybersécurité (NCSC) qui devient un Office fédéral dédié à la cyber. Berne a décidé maintenant de subventionner notre programme. On travaille à la réalisation d'une plateforme commune pour mettre à disposition l'information au plus près des entreprises. On sent que ça commence à bouger. Bien sûr, nos voisins européens, plus paternalistes, ont investi des centaines de millions de francs depuis plus de dix ans. Le positionnement est différent en Suisse, mais le mouvement est en marche. Cela reste une avancée. Nous avons tout pour bien faire : il reste à se donner les moyens pour aller dans le bon sens.



VII
LA PLACE GRANDISSANTE DES CYBERASSURANCES

La multiplication des cyberattaques ces dernières années a incité les assurances privées à proposer des couvertures pour permettre aux entreprises de se prémunir contre ce genre de risques. Ce marché se développe constamment et connaît actuellement une forte croissance. Ce domaine concerne la prévention et l'accompagnement des clients. Dans des cas de cyberextorsion, certaines assurances prennent en charge le paiement d'une rançon.

Une entreprise piratée, quelle que soit sa taille, peut faire faillite en quelques semaines. Si elle n'a plus accès aux listes de clients, aux commandes et à ses agendas, elle est condamnée à fermer boutique. Le besoin des entreprises de transférer une partie de ces risques impliquera un fort développement du marché de l'assurance dans ce domaine.

Interview de Jesús Pampín, spécialiste en matière de cyberassurances.

«LA DEMANDE DES PME EST PLUS FORTE»

Chef de service à la Vaudoise Assurances et membre du Groupe de travail Cyber de l'Association Suisse d'Assurances (ASA), Jesús Pampín est convaincu que le marché de la cyberassurance va connaître un grand essor ces prochaines années.

Les entreprises suisses sont-elles selon vous suffisamment préparées aux cyber-risques ?

Je distingue trois grands groupes. Tout d'abord, les plus grandes entreprises sont montées en puissance ces dernières années en matière de protection de leurs infrastructures IT et de sensibilisation auprès de leurs collaborateurs. Elles restent toutefois encore relativement sensibles à une bonne maîtrise des outils/plateformes utilisées par leurs sociétés locales et aux sous-traitants auxquels elles font appel. Quant aux plus petites entreprises, sans faire de généralités, la maturité informatique n'est pas encore optimale. Cette responsabilité ne peut cependant pas être imputée aux seules TPE/PME. Une culture d'« hygiène informatique » doit être promue à large échelle pour protéger de manière conséquente l'ensemble de la société, y compris les individus. Enfin, les institutions publiques prennent conscience de la très forte exposition à laquelle elles font face et des défis de taille auxquels elles devront répondre à l'avenir.

Ces risques sont-ils devenus plus importants avec le conflit russo-ukrainien ?

L'invasion de l'Ukraine par la Russie a laissé planer pour la première fois un réel risque de cyberguerre massive. Avant l'offensive officielle sur le territoire ukrainien, le pays a été la cible de cyberattaques russes. Tout le monde s'attendait à une catastrophe numérique avec le déclenchement de ce conflit. Or ce n'est pas arrivé et c'est une vraie surprise. À l'échelle planétaire, en revanche, les Etats réalisent l'urgence de renforcer la sécurité informatique de leurs infrastructures/entreprises dans ce nouvel environnement.

Le secteur de l'assurance exclut les risques de guerre de ses conditions générales. Un assureur ne peut pas couvrir des actes de guerre massifs à une échelle où il est impossible de mutualiser un risque. Toutefois, dans l'environnement actuel, on se rend compte qu'une offensive militaire peut être qualifiée de différentes manières. Il en va de même pour les cyberattaques qui seraient menées par des Etats contre d'autres Etats. Ceci peut créer des incertitudes quant aux couvertures d'assurance en place tant pour les clients que pour les compagnies d'assurance. Le marché londonien de l'assurance via Lloyd a bien tenté de répondre à cette problématique sans toutefois avoir trouvé « la solution » qui répondra à tous les cas de figure. La volonté reste de pouvoir continuer à assurer des actes de terrorisme tout en excluant les actes de guerre.

La cyberassurance émerge depuis des années et elle se développe très vite. Quels risques couvre-t-elle ?

Le marché compte quatre volets. Le premier a trait à l'assistance, au soutien en situation de crise, comme lorsqu'un client voit ses écrans bloqués à la suite d'une cyberattaque. C'est là où l'on peut amener une plus-value aux TPE/PME. Nous offrons en plus une assistance en informatique pour tout type de souci lié à la technologie.

Le deuxième volet s'applique aux propres dommages et le troisième concerne les dommages aux tiers. Les propres dommages sont ceux subis par l'entreprise notamment pour récupérer ses données. À cela s'ajoutent les aspects forensiques, c'est-à-dire savoir ce qui s'est passé pour que cela ne se reproduise pas, et enfin tout ce qui est en lien avec la restauration de l'image de l'entreprise.

Il y a aussi l'aspect central concernant la demande de rançon, car il existe beaucoup de cas de ce type. Sur le marché, il y a un véritable débat autour de ce sujet. Les autorités déclarent qu'il ne faut pas payer les rançonneurs. À titre personnel, je préfère accompagner la PME concernée plutôt qu'elle parte en faillite. Devoir payer une rançon est certes le dernier recours. En France, par exemple, l'Etat a demandé aux assurances d'accompagner les PME dans ce domaine-là.

Le quatrième volet se rapporte à la fraude, comme l'arnaque au président. Cela se passe par un appel téléphonique, il n'y a pas d'intrusion du système informatique. C'est l'humain qui est en cause, et cela aussi peut être assuré.

Tous les cyberrisques sont-ils assurables ? Et à quels tarifs ?

Depuis les cas de piratage informatique des villes de Rolle et de Montreux, le marché s'est refermé. La demande des PME est plus forte et, en parallèle, il y a un resserrement de l'offre en termes de sommes garanties à disposition. Au niveau des prix, le minimum s'élève à 800 francs pour une prime annuelle pour une petite PME dite « classique ». La fourchette s'étend entre 3000 et 5000 francs pour une couverture d'un million de francs. Pour une commune, la prime se situe plutôt entre 5000 et 20 000 francs Mais il est très difficile de donner des estimations, car cela dépend beaucoup des secteurs d'activités et le marché est en perpétuelle évolution.

Quels conseils donneriez-vous à un entrepreneur ? De s'assurer à tout prix ?

Il faut rester calme dans un premier temps. Ce n'est jamais dans la précipitation que l'on prend les meilleures décisions. Pour moi, la première chose consiste à réaliser un audit de sécurité, se poser les bonnes questions et faire un état des lieux : quelles sont les données sensibles ? Où sont-elles stockées ? Quelle est l'infrastructure informatique ? etc. Cela permet à la PME de mieux visualiser ses risques et de connaître quels sont ses réels besoins en matière d'assurance. Ainsi, elle peut actualiser les contrats avec ses prestataires informatiques qui sont en place depuis de nombreuses années, sans avoir fait l'objet d'une mise à jour.

L'essor de ces cyberassurances va-t-il se poursuivre ?

Oui, car aujourd'hui nous vivons dans une ère numérique. Une entreprise hackée peut faire faillite en quelques semaines. Il peut s'agir de grandes ou de petites entreprises, comme une menuiserie par exemple. Plus d'accès aux agendas, aux listes de clients, aux commandes et la boutique est condamnée à fermer. Le marché de la cybercriminalité est très lucratif et en forte croissance. Par conséquent, le besoin des entreprises de transférer une partie de ces risques est tout aussi important. Cela impliquera un fort développement du marché de l'assurance dans ce domaine.

Par ailleurs, les différentes réglementations (LPD/RGPD) se renforcent au niveau suisse, européen, mais aussi mondial. Le besoin de transférer une partie de ces risques provoque une forte croissance dans ce domaine. Je suis persuadé que l'industrie de l'assurance peut constituer un excellent axe pour contribuer à gagner ensemble en maturité dans ce domaine qui expose toutes les sociétés et tous les individus. Aujourd'hui, tous les acteurs doivent avancer sur le sujet. Il s'agit d'une thématique qui devrait figurer dans les priorités d'un Etat. De manière plus globale, un pays où les entreprises et les individus possèdent un niveau de maturité de premier plan bénéficiera de fait, d'un avantage concurrentiel considérable.

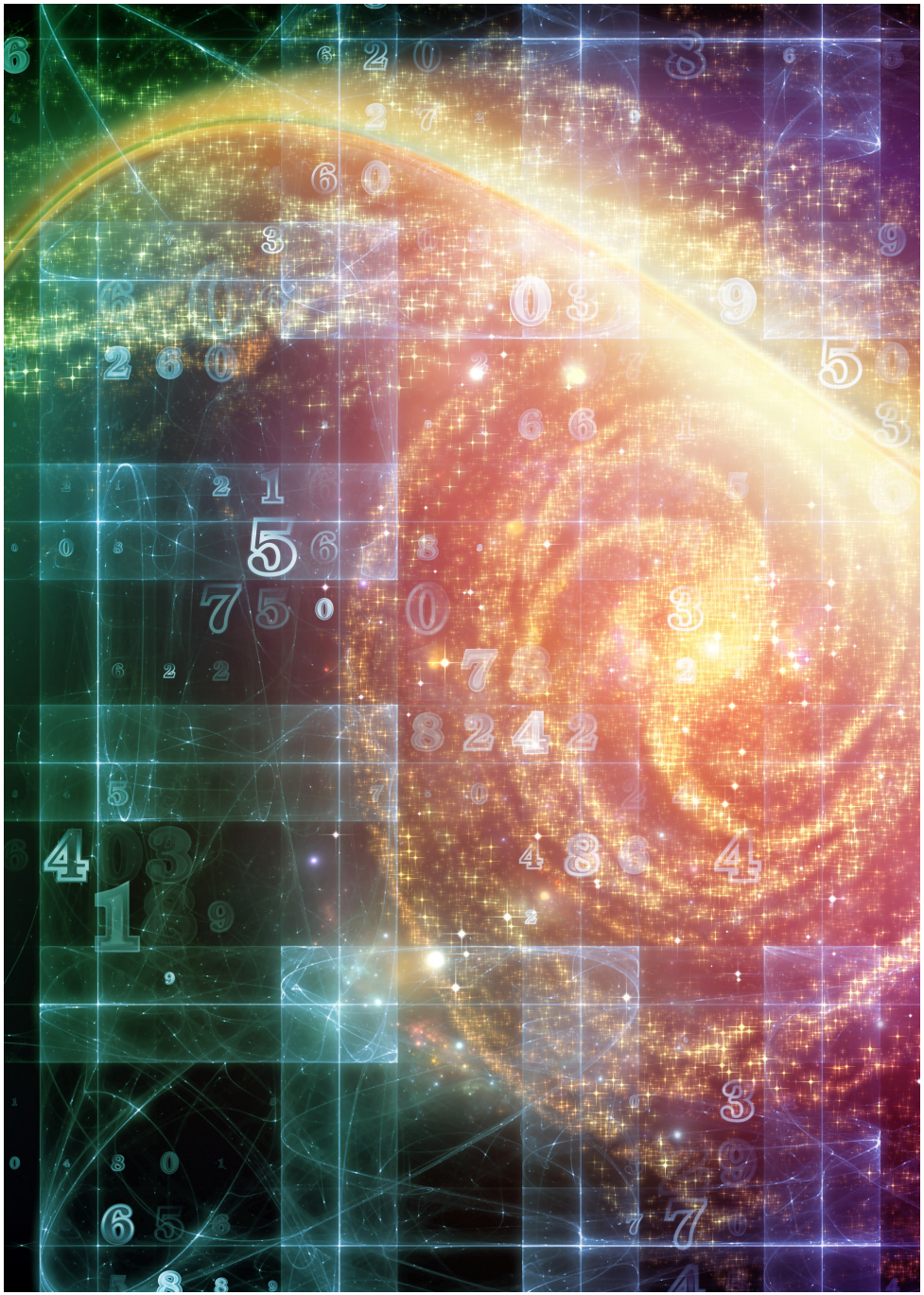
Votre branche est-elle en contact avec les autorités, coopère-t-elle dans le domaine cyber ? Et si oui, de quelle manière ?

Nous sommes en contact avec les autorités via notre association faîtière (ASA). Tous les acteurs dans ce domaine doivent coopérer et cela bénéficiera à chacun.

Votre conclusion ?

Si on veut protéger le monde économique et les entreprises suisses, il faut disposer d'une forte valeur ajoutée au niveau de la protection informatique. À mon sens, c'est primordial. Et si le secteur de l'assurance peut être un soutien et un pilier de la démarche, ce sera une excellente chose.

« UN PAYS
OÙ LES ENTREPRISES
ET LES INDIVIDUS
POSSÈDENT UN NIVEAU
DE MATURITÉ
DE PREMIER PLAN
BÉNÉFICIERA DE FAIT,
D'UN AVANTAGE
CONCURRENTIEL
CONSIDÉRABLE. »



VIII
LES BONNES PRATIQUES EN CINQ POINTS

« L'IMPULSION DOIT VENIR DU TOP MANAGEMENT »

Stéphane Droxler, patron du Bureau de conseil en gouvernance des données DP&S, considère que la gouvernance d'une entreprise a un rôle central à jouer dans la politique à conduire contre les cyberrisques. Il rappelle quels sont les principes qui doivent guider les sociétés dans ce domaine.

« La gestion d'un cyberincident doit se préparer en amont. Ces décisions doivent être prises au plus haut niveau de l'entreprise. Il faut anticiper, s'organiser, allouer les ressources humaines et financières nécessaires à ce type de risque. L'impulsion doit donc venir du top management. » Professionnel certifié par l'IAPP en matière de protection des données personnelles, Stéphane Droxler connaît bien le dilemme qui se pose au manager lorsque celui-ci doit aborder le thème de la cybersécurité : « Oser poser les bonnes questions et challenger les réponses alors qu'il s'agit d'un sujet qu'il ne maîtrise pas. »

Toute entreprise, quelle que soit sa taille, doit se prémunir au mieux contre les cybermenaces. Les questions que le manager doit se poser sont multiples : Sommes-nous protégés ? Comment puis-je en être sûr ? Protégeons-nous correctement les données de nos clients ? Sommes-nous en conformité avec les lois ? Que font nos concurrents ? « C'est ce qui manque aujourd'hui dans la plupart des entreprises, souligne l'expert. Combien d'entre elles prennent véritablement le temps de procéder à une analyse des risques globaux et de leur cyberdépendance ? »

Pour Stéphane Droxler, la situation difficile des entreprises en matière de cyber-résilience vient du fait que la sécurité n'est bien souvent considérée que du point de vue technologique. La problématique posée est cependant infiniment plus large. La CVCI considère que ce domaine est de première importance pour les entreprises. Dans le cadre de la présente étude, nous avons demandé à Stéphane Droxler de résumer en cinq points les bonnes pratiques permettant de limiter les risques encourus par l'usage des technologies de l'information. Ils ont trait à la gouvernance, à l'organisation, à la formation, aux technologies de sécurité et, enfin, à la maintenance et à l'évolution de l'IT.

~~CINQ BONNES PRATIQUES~~ INDISPENSABLES

1

Gouvernance.
Analyser les risques propres à son (ses) activité(s), adopter une stratégie de gestion de ses risques, définir les rôles et attribuer les responsabilités (qui peut accéder à quoi), allouer les ressources nécessaires, fixer des objectifs clairs et suivre régulièrement l'avancement du programme de sécurité.

2

Organisation.
Connaître la valeur de ses données et la dépendance de l'entreprise par rapport à ses systèmes informatiques permet de mieux protéger ce qui doit l'être. Cela passe par une meilleure maîtrise de ses processus, une gestion adéquate des droits d'accès ainsi que l'évaluation systématique des mesures de sécurité organisationnelles et techniques pour tout nouveau produit ou service. La formalisation de ces éléments, au travers d'une cartographie et de documents facilement disponibles, constitue une réponse appropriée aux exigences, y compris légales, en matière de protection des données.

3

Formation.
Mettre en place un programme de sensibilisation du personnel aux cyber-risques, accueillir les nouveaux arrivants par une formation adéquate en leur indiquant les règles en place, tester régulièrement la vigilance des utilisateurs permet de réduire significativement les risques de cyberattaque et de divulgation accidentelle de données.

4

Moyens technologiques.
Plutôt que d'investir dans des technologies sans savoir à quoi elles vont servir, il faut définir des contrôles adaptés au risque et utiliser les fonctionnalités souvent existantes des systèmes déjà en place. Cela doit permettre de regagner la visibilité perdue sur l'environnement informatique et ainsi améliorer la capacité de détection des anomalies.

5

Enfin, il faut mettre l'accent sur la **maintenance et l'évolution** des outils informatiques grâce à une bonne maîtrise de qui fait quoi sur quels systèmes. La gestion des prestataires est fondamentale dans une perspective de bonne gouvernance des risques cyber, et du risque induit par les tiers notamment.

« ON LE VOIT,
DE NOMBREUSES PISTES
SONT À EXPLOITER
POUR PASSER
D'UN STATUT DE VICTIME
PASSIVE À CELUI
D'ACTEUR RESPONSABLE,
CONSCIENT DE SON RÔLE
ET DE SON IMPORTANCE
DANS L'ÉCOSYSTÈME
NUMÉRIQUE »,

CONCLUT STÉPHANE
DROXLER.

IX
CONCLUSION ET ENGAGEMENTS DE LA CVCI

Être à l'écoute de l'économie et de ses transformations figure parmi les valeurs centrales que défend la CVCI. La numérisation galopante et les risques que celle-ci induit s'inscrivent clairement dans cette perspective. C'est pourquoi la Chambre s'engage pour informer et soutenir ses membres quant aux risques liés à la criminalité informatique. Elle publie régulièrement des conseils et des informations sur le domaine par le biais de son magazine « demain » et de nombreuses newsletters. Elle met aussi sur pied des événements sur cette thématique. Un webinaire sur la cybersécurité organisé en nos murs ces derniers mois a attiré 50 participants en présentiel et 110 en distanciel. Cet événement a débouché sur la création d'une feuille de route en collaboration avec la Police cantonale vaudoise et la société Navixia. Ce document contient un grand nombre d'informations utiles aux entreprises, notamment les bons réflexes à instaurer pour prévenir une cyberattaque, ainsi qu'une série de conseils sur les comportements à observer si une intrusion malicieuse s'est malheureusement réalisée. La mise en réseau de nos membres et le partage qui en découle contribuent à la prise de conscience de tous ces enjeux.

Soutenu par la CVCI, le programme Trust4SMEs de la Trust Valley (voir chapitre VI) a démontré si besoin était que les entreprises doivent gagner en maturité dans le domaine de la cybersécurité. L'événement « Sensibilisation cyber XXL et résultats de campagnes phishing », qui a clos ce programme le 9 février dernier à l'EPFL, a prouvé qu'en formant les collaborateurs, les risques de piratage diminuaient significativement. Une campagne de cyberattaques organisée par de « gentils » hackeurs dans le cadre ce de programme a ciblé pendant deux mois les collaborateurs des 25 entreprises participantes. Au bout des deux mois, le pourcentage de gens piégés est passé de plus de 35 % à moins de 10 %.

Un dernier bon conseil : utilisez des phrases de passe plutôt que des mots de passe avec des lettres et des chiffres. Il doit s'agir d'une phrase longue, difficile à « craquer », mais facile à retenir. Privilégiez quatre mots formant ensemble une phrase n'ayant aucun sens. Recourez aussi à un gestionnaire de mots de passe qui permet de réunir tous vos sésames à un seul endroit sécurisé. Activez enfin l'identification forte, dont l'accès est basé sur une validation en deux étapes. L'utilisateur doit entrer un mot de passe et un code de sécurité qu'il recevra par exemple sur son smartphone.

Se protéger, former et informer restent les trois piliers de la cybersécurité pour les entreprises. La CVCI va continuer de marteler ce message ces prochaines années.

Jean-François Krähenbühl

LIENS UTILES

CYBERSÉCURITÉ
VAUD

FEUILLE DE ROUTE CVCI
CYBERCRIMINALITÉ/CYBERSÉCURITÉ

START-UP ACTIVES
DANS LE DOMAINE CYBER

CHAMBRE VAUDOISE
DU COMMERCE ET DE L'INDUSTRIE

Avenue d'Ouchy 47
1006 Lausanne
T. 021 613 35 35
cvci@cvci.ch
www.cvci.ch

TRANSPORTS PUBLICS
M2 ou bus TL n° 2
Maladière-Lac / Désert
arrêts Jordils

HORAIRES D'OUVERTURE
Lundi au vendredi
07 h 45 – 12 h 00
13 h 30 – 17 h 00

VOTRE PARTENAIRE

AU CŒUR DE L'ÉCOSYSTÈME