Haute école des sciences
appliquées de Zurich

School of
Management and Law

Les PME suisses face aux cyber-risques

Une enquête sur les attitudes des employés et les failles comportementales

Carlo Pugnetti, ZHAW Institute for Risk & Insurance
Carlos Casián, Allianz Suisse

En collaboration avec:

Allianz

Éditeur
ZHAW School of Management and Law
St.-Georgen-Platz 2
Boîte postale
8401 Winterthur
Suisse

Institute for Risk & Insurance (IRI)
www.zhaw.ch/en/sml/institutes-centres/iri/

Auteur/Coordonnées
Dr. Carlo Pugnetti
carlo.pugnetti@zhaw.ch

Janvier 2021

Éditorial

L'évolution et l'adoption généralisée de la technologie ouvrent de nouvelles possibilités passionnantes d'améliorer notre quotidien grâce à de meilleurs produits et services, mais aussi à des contacts humains de plus grande qualité et plus fréquents. Malheureusement, elles ouvrent aussi de nouvelles perspectives aux malfaiteurs. Nous savons d'expérience que ceux-ci peuvent être intelligents, bien équipés et créatifs et qu'ils sauront exploiter les failles technologiques ou humaines des défenses que nous mettons en œuvre. Ces évolutions sont également importantes pour les assureurs qui couvrent ces risques émergents.

La question est particulièrement cruciale pour les petites et moyennes entreprises (PME) suisses, souvent en première ligne de l'évolution du marché et de l'innovation, mais dont les moyens en termes de cybersécurité sont limités. Ces dernières années, nous avons pu observer à quel point ces entreprises sont la cible des cybercriminels. Chez Allianz Suisse, nous avons toujours fourni à nos clients d'excellents produits, des services personnalisés et des solutions révolutionnaires, et cette nouvelle étude va dans le sens de notre démarche d'innovation.

L'attitude des employés face aux risques cybernétiques est un élément déterminant de la protection globale de l'entreprise et du mécanisme de réponse. La Haute école des sciences appliquées de Zurich (ZHAW) a élaboré une recherche passionnante axée sur le comportement des clients en matière d'assurance, à laquelle nous sommes fiers d'être associés. Cette étude a notamment identifié d'intéressantes clés de compréhension des attitudes des salariés des PME, en termes de comportements et de culture, et formulé des recommandations claires et instructives, tant pour les sociétés que pour leurs fournisseurs de technologies et d'assurance.

J'espère que vous trouverez cette publication éclairante et inspirante.

Severin Moser

CEO, Allianz Suisse

Résumé

Les attaques cybernétiques constituent un problème de plus en plus sensible pour les PME suisses. Près d'un tiers d'entre elles ont en déjà été victimes, et quatre pour cent ont fait l'objet d'un chantage subséquent. Dans la plupart des cas, les problèmes ont commencé par des attaques par hameçonnage, les malfaiteurs ayant exploité une erreur ou une négligence d'un employé pour accéder au système informatique. Nous avons interrogé de nombreux salariés de PME suisses afin de comprendre comment leur attitude face aux attaques cybernétiques peut influer sur cette vulnérabilité et de suggérer des mesures correctives concrètes. Les entretiens ont été menés sur la base de métaphores profondes afin de comprendre les moteurs culturels et émotionnels cachés du comportement, plutôt que les éléments rationnels visibles. Nous avons élaboré trois recommandations pour tirer parti de la culture proactive des PME et réduire la dépendance aux prestataires tiers: sensibiliser, responsabiliser les employés et concevoir un mode de reprise.

Sommaire

Introduction

1.1. LES PME SUISSES FACE AUX CYBER-RISQUES

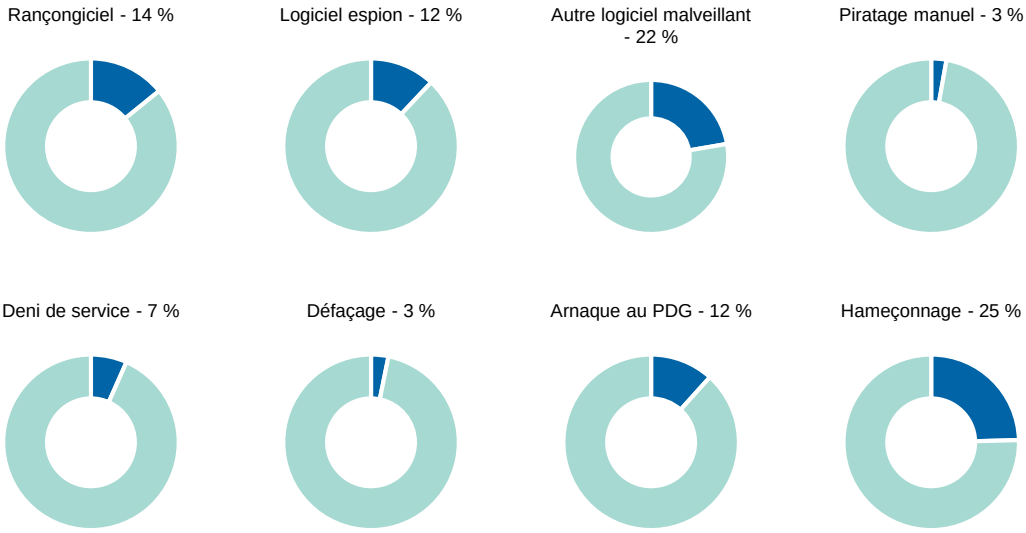
Les fuites de données ou les failles de sécurité, l'espionnage, les attaques de pirates, les rançongiciels, les attaques par déni de service et les erreurs des employés représentent les principales causes de cyberincidents, qui sont de plus en plus fréquents et coûteux. Une évolution observable dans le baromètre des risques d'Allianz (2020), fruit de la contribution de plus de 2700 experts internationaux en matière de risques: Les incidents cybernétiques ont supplanté l'interruption des activités au rang de principal risque. L'interconnectivité croissante de l'économie implique que les sociétés sont plus exposées aux attaques cybernétiques, et les signalements d'attaques et de vols de données spectaculaires se multiplient. Les entreprises s'exposent à des préjudices pouvant atteindre plusieurs millions, à une atteinte à leur image et même à une interruption de leurs activités susceptible de compromettre leur existence en cas de vol de données par des pirates, de contamination de leurs réseaux par des logiciels malveillants ou de paralysie de leurs serveurs (Allianz, 2020). Severin Moser, CEO d'Allianz Suisse, estime que les conséquences de la cybercriminalité coûtent chaque année plus de 600 milliards d'USD à l'économie mondiale (NZZ, 2019). Un phénomène qu'il est toutefois difficile de quantifier précisément, compte tenu du manque de chiffres fiables et des nombreux cas non signalés. Le groupe de travail sur les risques cybernétiques de l'Association suisse d'assurances estime que le coût annuel s'élève à 9,5 milliards de CHF rien qu'en Suisse, et ce chiffre progresse (ASA, 2018).

Les PME, définies comme les entreprises de moins de 250 salariés, représentent 99 % des sociétés et pourvoient aux deux tiers des emplois en Suisse (Office fédéral de la statistique, 2020). Elles jouent un rôle décisif dans l'économie suisse et sont lourdement affectées par les attaques cybernétiques. Près d'un tiers des PME suisses en ont déjà été victimes, et quatre pour cent d'entre elles ont fait l'objet d'un chantage subséquent (Mändli Lerch et Repic, 2017). Même si les données des plus petites entreprises présentent un intérêt moindre pour les cybercriminels, elles restent des cibles de choix pour deux raisons: D'une part, elles offrent la possibilité d'extorquer une rançon grâce à un rançongiciel et, de l'autre, elles constituent une voie d'accès pour attaquer les entreprises plus grandes qui collaborent avec elles (Heer, 2020). La Centrale d'enregistrement et d'analyse pour la sûreté de l'information, integrée dans le Centre national pour la cybersécurité (NCSC) en juillet 2020, a signalé une hausse du risque d'attaques par rançongiciels début 2020 (MELANI, 2020a). Une menace qui progresse encore et qui, après avoir quadruplé en 2019, représente désormais l'incident cybernétique le plus fréquent (Trustwave, 2020). Les exemples d'entreprises suisses victimes d'attaques par rançongiciels sont nombreux, et quatre d'entre eux sont évoqués au chapitre suivant.

De récentes études se sont penchées plus précisément sur les attaques cybernétiques dirigées contre les PME dans des pays voisins. Dreissigacker et al. (2020) estime que, en Allemagne par exemple, 40 à 50 % des PME comptant plus de dix salariés sont chaque année exposées à une cyberattaque, même si la plupart d'entre elles sont contrées et ne causent aucun dommage. Un chiffre légèrement plus bas que pour les sociétés de plus grande envergure, qui sont chaque année 50 à 60 % à être victimes de telles attaques. L'étude analyse également le taux annuel de chacune des grandes catégories de cyberattaques, comme résumé à l'illustration 1. Les PME peuvent s'attendre à subir une tentative d'hameçonnage tous les quatre ans et une attaque par rançongiciel tous les sept ans, des chiffres à peu près identiques à ceux applicables aux sociétés plus conséquentes. A l'inverse, les arnaques au PDG et le piratage manuel sont nettement moins fréquents chez les PME, sans doute parce que, dans ces structures, le PDG joue un rôle plus concret et que le gain financier potentiel est moindre. Les études menées dans d'autres pays européens affichent des résultats similaires, avec parfois d'importants écarts, mais la comparaison directe est rendue difficile par la diversité des méthodes de recherche employées et des mécanismes de signalement. D'une manière générale, elles confirment toutefois que les cyberattaques représentent une menace substantielle pour les PME.

Illustration 1: Taux annuel estimé de cyberattaques dirigées contre les PME

TAUX ESTIME DE CYBERATTAQUES DIRIGEES CONTRE LES PME PAR ANNEE ET PAR TYPE EN ALLEMAGNE EN 2018 ET 2019



Source: Dreissigacker et al. (2020)

Les cyber-malfaiteurs adaptent régulièrement les attaques d'ingénierie sociale, notamment l'hameçonnage, en fonction des événements d'actualité marquants, comme les événements sportifs ou, actuellement, la pandémie de Covid-19. Mais presque toutes les familles de logiciels malveillants connues se sont répandues sous couvert de la Covid-19, le plus souvent au moyen d'e-mails contenant une pièce jointe contaminée ou un lien vers un site Web infecté (MELANI, 2020b). Le nombre d'e-mails d'hameçonnage a bondi durant la pandémie; à titre d'exemple, des escrocs se faisant passer pour des employés de l'Organisation mondiale de la santé (OMS) ont ciblé les fonds de secours aux victimes de la Covid-19 et attiré les utilisateurs vers des sites Web malveillants au moyen de fausses publicités (de Moura et al., 2020). Des attaques par hameçonnage ont également visé de manière spécifique les nouvelles conditions de travail. Beaucoup d'utilisateurs n'étaient pas accoutumés aux logiciels de conférence et de collaboration ni aux messages envoyés par ces plateformes, ce qui a rendu les e-mails d'hameçonnage encore plus difficiles à déceler (MELANI, 2020b). Plusieurs articles soulignent la vulnérabilité des sociétés induite par les erreurs humaines et l'importance des attaques par hameçonnage. Si l'infrastructure technique reste essentielle, les salariés sont souvent victimes de dispositifs bien pensés, exposant ainsi leur entreprise à une fraude ou à logiciel malveillant (Pugnetti et al., 2019). Les PME suisses sont généralement mal protégées contre les cyber-risques, notamment en termes de services d'atténuation et de reprise (Pugnetti et Schneebeli, 2020).

Cette recherche a pour but de comprendre les failles potentielles liées à la représentation que les salariés ont de la cybercriminalité et à la culture d'entreprise des PME, mais aussi de suggérer des mécanismes de défense utilisables par les entreprises ainsi que des formations et services pouvant être fournis par des tiers.

1.2. EXEMPLES D'ATTAQUES CYBERNETIQUES MAJEURES EN SUISSE

Les médias ont relaté plusieurs cyberattaques dirigées contre des PME suisses. Quatre d'entre elles ont été particulièrement significatives pour les entreprises que nous avons interrogées dans cette étude et sont décrites plus en détail ci-dessous.

1.2.1. OFFIX AG, 2019

Le 15 mai 2019, OFFIX AG, un fournisseur d'équipement de bureau qui emploie près de 250 personnes et dégage un chiffre d'affaires de 300 millions de CHF (Papedis, n.d.), a été victime d'une attaque par rançongiciel (Jochum, 2019). Le pirate aurait intercepté un échange d'e-mails avec un client, dont il aurait ensuite usurpé l'identité. Un salarié de l'entreprise a alors reçu une demande de certification, a cliqué sur le lien fourni et le virus a infecté le

système informatique de l'entreprise. Les premières anomalies se sont manifestées le lendemain et, le 17 mai, il est devenu évident qu'il ne «restait plus rien» des outils informatiques: les bases de données avaient été effacées et les paramètres d'usine restaurés sur plusieurs serveurs. Plusieurs interfaces clients pour la passation de commandes avaient également été effacées et OFFIX n'avait plus aucune trace des commandes entrantes ni des ventes. Une rançon de 45 bitcoins (qui représentait alors une valeur de 350 000 CHF) a été demandée en échange du déchiffrement des données. Un expert externe en cybercriminalité a été recruté, et la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) ainsi que la police ont été alertées. Il a ensuite été demandé aux clients de passer commande par téléphone, fax ou grâce aux adresses e-mails nouvellement créées avant que toute la société ne soit mise hors ligne. Par chance, le pirate a commis une erreur et, d'autre part, un expert informatique avait fait une sauvegarde d'une importante application sur un disque dur externe à peine quelques semaines auparavant. OFFIX a ainsi pu restaurer une partie de sa base de données, puis rétablir ses systèmes informatiques (Severin, 2019). Selon le CEO, Martin Kelterborn, si le préjudice financier est impossible à quantifier, l'attaque a «coûté très, très cher» (Jochum, 2019).

1.2.2. Swisswindows, 2019

En mai 2019, Swisswindows, professionnel de la fenêtre aux quelque 170 salariés (Borkert, 2020), a vu sa production mise à l'arrêt pendant plus d'un mois à cause d'une attaque par rançongiciel. Les pirates ont probablement eu accès au réseau de la société via un e-mail insoupçonnable et ont chiffré l'ensemble de ses données. Les commandes n'étaient plus visibles et les employés n'avaient pas accès aux données des clients et des machines. L'entreprise était paralysée. Un prestataire informatique externe avait effectué des sauvegardes de données quotidiennes, mais les fichiers de sauvegarde étaient rattachés au serveur de l'entreprise et, par conséquent, inaccessibles. Les cybercriminels ont exigé une importante rançon en bitcoins pour déchiffrer les données, mais l'entreprise a décidé de ne pas la payer et d'investir à la place dans le remplacement de son infrastructure informatique, au demeurant nécessaire (Klein, 2020). Mais en février 2020, le personnel a été subitement avisé que la société était en faillite. La cyberattaque avait encore accentué les difficultés liées à l'actuel ralentissement des principales activités de l'entreprise, contribuant ainsi à sa chute (SRF, 2020).

1.2.3. Meier Tobler, 2019

Meier Tobler, spécialiste de la technique du bâtiment au chiffre d'affaires de 500 millions de CHF et aux quelques 1300 salariés (Meier Tobler, 2020), a été victime d'une attaque par rançongiciel en juillet 2019 (Luzerner Zeitung, 2019). Les assaillants ont utilisé un logiciel malveillant contenu dans une pièce jointe à un e-mail (Schäppi, 2020). Le système SAP central, le système de contrôle de l'entrepôt, la ligne téléphonique filaire, le site Web et toutes les adresses e-mail ont cessé de fonctionner (Lüscher et Niedermann, 2019). Selon le communiqué de presse de l'entreprise, l'événement a eu de lourdes répercussions sur les ventes et les bénéfices:

> Malgré la mise en œuvre des procédures d'urgences prévues en amont et la mise en place rapide d'une infrastructure provisoire, il n'a pas été possible d'empêcher une interruption dans les livraisons. Les ventes au détail ont immédiatement chuté de près de 5 millions de CHF. Un recul similaire a ensuite affecté le segment de la production de chaleur, à cause du manque de disponibilité des systèmes informatiques.

Le surcoût direct de la gestion de l'attaque a entamé les bénéfices annuels pour 2019 de 1 million de CHF. Depuis, la société a rebâti son infrastructure informatique avec les tout derniers critères de sécurité (Meier Tobler, 2020).

1.2.4. Stadler Rail, 2020

Stadler Rail fabrique des véhicules ferroviaires. Elle compte 11 000 salariés et affiche des revenus mondiaux de plus de 3,2 milliards de CHF (Stadler Rail, 2020a). Il ne s'agit donc pas d'une PME. Mais la cyberattaque dont elle a été victime a été évoquée par les participants à l'étude, d'où sa pertinence. Le 7 mai 2020, «le réseau informatique de Stadler a été attaqué par un logiciel malveillant. La société a immédiatement déployé des mesures de sécurité et a fait intervenir les autorités compétentes. Une enquête approfondie est en cours.» (Stadler Rail, 2020b). Les malfaiteurs ont exercé un chantage sur Stadler en publiant les données volées et ont réclamé le paiement de six millions d'USD en bitcoins. Dans un entretien donné à inside-it.ch, la société a confirmé «qu'il s'agit de documents et de données confidentiels volés à Stadler par des moyens criminels» (Anz, 2020). Stadler a refusé de payer la rançon. D'autres dossiers ont à plusieurs reprises été publiés afin d'accentuer la pression car la société ne pliait pas (Griesser Kym, 2020). Stadler n'a toutefois jamais envisagé de céder aux exigences des maîtres-chanteurs et de payer – et «ne le fera pas» (Anz, 2020).

1.3. PROTEGER VOTRE ENTREPRISE

Toutes les entreprises doivent déterminer les risques qu'elles souhaitent éviter, atténuer, transférer ou supporter elles-mêmes dans le cadre de leur processus décisionnel en matière de gestion des risques. Il est donc essentiel qu'elles comprennent les solutions d'assurance qui s'offrent à elles et quel niveau de protection aurait pu être fourni dans les affaires décrites ci-dessus. Les attaques cybernétiques peuvent causer des pertes propres, comme les coûts de restauration des données et d'interruption des activités régulières. Les polices d'assurance standard couvrent les dégâts matériels et l'interruption de l'activité qui en résulte si la cause du dommage est assurée (p. ex. un incendie). Mais une cyberattaque n'entraîne pas nécessairement de dégâts matériels, et il est donc rare que l'assurance soit invoquée. En outre, les sociétés peuvent s'exposer à des recours en responsabilité civile exercés par des tiers après une cyberattaque, notamment si des données clients sont divulguées ou effacées. L'assurance responsabilité civile traditionnelle couvre les recours liés aux dommages corporels et aux biens, ainsi que la perte financière qui en découle. L'assurance responsabilité civile couvrant une perte purement financière n'est généralement destinée qu'à des groupes professionnels spécifiques et n'est donc pas très répandue.

Les polices d'assurance commerciale classiques n'ont qu'une chose en commun: elles ne couvrent pas spécifiquement les cyber-risques. Le préjudice et les effets d'une cyberattaque sont parfois assurés par ce type de produits, mais ils ne sont pas spécifiquement conçus pour permettre aux entreprises de contrôler les cyber-risques. Notons que les risques cybernétiques sont apparus à l'ère de l'Internet et que les premières couvertures spécifiques ont été élaborées à l'aube du nouveau millénaire, en réponse à cette nouvelle menace. En Suisse, les premières polices d'assurance contre les cyber-risques ont été introduites par les assureurs internationaux de grandes entreprises en 2015, tandis que les solutions d'assurance complètes pour les PME ont été lancées en 2017. Ces solutions regroupent généralement une assurance responsabilité civile, la couverture des pertes propres et la gestion de crise, et intègrent une protection juridique contre la cybercriminalité, l'ingénierie sociale et les cyber-risques. Ces produits mettent l'accent sur les cyberattaques ainsi que sur les fautes commises par les employés et les atteintes à la protection des données. En plus de l'indemnisation des préjudices subis, les entreprises ont accès à un réseau d'experts en technologie de l'information, communication de crise et protection juridique qui leur permet de déterminer l'ampleur du sinistre, d'accélérer la réparation des dégâts et d'éviter ou d'atténuer l'atteinte à la réputation de la société. Le tableau 1 donne un aperçu des couvertures de cyberassurance usuelles actuellement disponibles (Pugnetti et al., 2019).

Tableau 1: Couvertures de cyberassurance actuelles

COUVERTURES DE CYBERASSURANCE ACTUELLES

Responsabilité civile Recours et réclamations de tiers	- Atteintes à la protection des données - Perte de données - Détournement / perte de fonctionnalité - Communication numérique - Paiement électronique / pénalités contractuelles - Transmission de logiciels malveillants
Pertes propres Pertes subies par l'assuré	- Coûts de restauration - Interruption de l'activité - Vol par attaque cybernétique - Cyber-chantage - Procédures officielles de protection des données
Gestion de crise Services en cas de sinistre	- Services de police scientifique - Coûts d'information - Communication de crise - Coûts d'urgence
Protection juridique Litiges liés à des cyber-risques	- Droit contractuel - Violation des droits de la personnalité - Usurpation d'identité - Utilisation frauduleuse de cartes de crédit et d'informations bancaires - Domaine Internet
Cybercriminalité - Ingénierie sociale Pertes financières dues à une fraude commise par un tiers	- Fraude par utilisation d'une fausse identité - Fraude par détournement de flux de trésorerie - Fraude par utilisation de fausses identités

1.4. ENTRETIENS BASES SUR LES METAPHORES PROFONDES

Les recherches menées auprès des consommateurs se sont longtemps concentrées sur la compréhension des structures cognitives, à savoir les systèmes de croyance, en accentuant la structure au détriment du contenu (Olson et Reynolds, 1983). Toutefois, une meilleure façon de décrire et de représenter les consommateurs est le modèle mental, qui prend en compte des représentations qui ne sont pas fondées sur la croyance, comme les attitudes, les sentiments, les images, les souvenirs, les valeurs, etc. (Christensen et Olson, 2002). Il s'accorde également mieux avec l'idée qui prévaut actuellement dans la neuroscience cognitive selon laquelle les pensées sont basées sur des images (Damasio, 1994). Les outils de recherche et d'élicitation ont évolué pour tenter de saisir la complexité supplémentaire des modèles mentaux – notamment la technique d'élicitation de la métaphore de Zaltman, ou ZMET. La ZMET repose notamment sur l'hypothèse de l'importance du contenu tacite inconscient, c'est-à-dire les connaissances cachées et l'importance des images dans les modèles mentaux. La ZMET utilise des images pour aider les informateurs à identifier et à communiquer un contenu (Zaltman, 1997). Elle a servi à éliciter les moteurs émotionnels profonds des comportements et les choix des consommateurs (Zaltman et Zaltman, 2008).

La technique se décompose en trois étapes. Dans un premier temps, les personnes interrogées sont invitées à penser à un sujet et à sélectionner des images qui représentent leurs pensées et leurs sentiments à son égard. Elles sont ensuite interrogées afin de comprendre les significations qu'elles donnent à ces images et des liens sont établis avec les idées sous-jacentes par des techniques de laddering. Enfin, les résultats sont générés en créant des cartes consensuelles des concepts centraux et des grands thèmes de signification (Christensen et Olson, 2002). Il en résulte un ensemble de thèmes que les personnes interviewées associent au sujet étudié. L'intention n'est pas de générer des résultats significatifs sur le plan statistique, mais de faire resurgir des informations cachées. Cette technique a été employée dans plusieurs études, y compris par les auteurs de cette étude dans le cadre de projets de conseil ainsi que dans une étude publiée sur le ressenti des nouveaux clients dans le domaine des assurances. Dans celle-ci, par exemple, les nouveaux clients ont clairement fait part de leur frustration face au jargon technique de la profession et de leur manque de connaissance des marques d'assurance (Pugnetti et Bekaert, 2018).

1.5. METHODOLOGIE

Nous avons sélectionné trois PME dont les activités ont trait à l'ingénierie mécanique et nous avons réalisé des entretiens basés sur les métaphores profondes auprès de 17 salariés volontaires aux profils variés, y compris des membres de la direction et du personnel administratif, des ouvriers et des employés de terrain. Il leur a été demandé de choisir 3 à 5 images illustrant leur ressenti à l'annonce de cyberattaques (tableau 2). Ils ont ensuite été interrogés sur la signification des images choisies.

Tableau 2: Question de recherche

Question de recherche	Que ressentez-vous lorsque vous entendez parler de cyberattaques?

Les entretiens ont été réalisés en septembre 2020 de manière conjointe par les deux auteurs dans les locaux de chaque société. Ils ont duré environ une heure chacun, en fonction du nombre d'images utilisées et des questions induites par la discussion. Les résultats ont ensuite été évoqués lors de différents ateliers et consolidés afin d'établir les cartes consensuelles et de définir les grands thèmes présentés. Ces thèmes sont abordés dans les sections suivantes, à l'aide des images originales et en reprenant les propos des personnes interrogées. Certaines images originales ont été remplacées par des visuels identiques pour des questions de droits.

Les personnes interrogées se sont décrites de la manière indiquée dans le tableau 3:[1]

Tableau 3: Auto-description des personnes interrogées

AUTO-DESCRIPTION DES PERSONNES INTERROGEES

1	Serviable, ne veut faire de mal à personne	10	Amical, prend soin des autres
2	Personne à l'attitude positive	11	Ouvert mais prudent
3	Discret et réfléchi	12	Rationnel mais ouvert
4	Heureux de vivre	13	Prudent
5	Discret, ne cherche pas les problèmes	14	Jovial, souple
6	Loyal, à l'écoute	15	Conformiste mais ouvert
7	Personne positive	16	Responsable
8	Centré sur les objectifs	17	Communicatif et curieux
9	Discret et fiable		

[1] Afin de préserver la confidentialité, l'ordre ne correspond pas à celui dans lequel les entretiens ont été réalisés

Résultats

Les entretiens ont révélé plusieurs dénominateurs communs. L'un des thèmes récurrents a été la nature géopolitique des cyberattaques, les liens avec le crime organisé et la motivation financière. Le pirate était perçu comme un «professionnel», doté de compétences expertes et d'un excellent équipement, pas nécessairement toujours comme un être malfaisant. En général, les personnes interrogées se sentaient impuissantes à reconnaître les cyberattaques ou à s'en protéger. Elles se sentaient par conséquent vulnérables, tout en ayant conscience des dangers des attaques par hameçonnage et des effets potentiellement dévastateurs des attaques cybernétiques. Beaucoup de participants ont évoqué la récente affaire Meier Tobler. Parallèlement, ils ne se sentaient pas suffisamment importants, n'appartenant pas à une société suffisamment conséquente pour être la cible d'attaques. En cas d'urgence, ils se fieraient à des prestataires de service externes pour résoudre le problème. Enfin, les participants ont révélé une attitude très positive en matière de résolution des problèmes et d'identification de solutions de manière autonome, y compris en recourant au besoin à des méthodes désuètes.

Tableau 4: Thèmes communs et légendes des images

	THEME	LEGENDES DES IMAGES
1	**Politique internationale et crime organisé**	Service secret Homme de l'ombre Le butin
2	**Le hacker mythique**	Le hacker Espace de travail agréable Bandit ou bienfaiteur?
3	**Sentiment d'impuissance**	Aimant à données Manipulation sociale Questions sans réponse
4	**Sentiment de vulnérabilité**	Surveillance Attention! Hameçonnage
5	**Issue catastrophique**	Effraction moderne Attaque contre notre fournisseur J'espère que non!
6	**Cela ne me concerne pas**	Le monde entier Peur Soutien personnel
7	**Proactif et engagé**	Brouillard Planification Comme au bon vieux temps

Ces réponses nuancées et variées à une question relativement directe témoignent d'une réflexion élaborée. Elles ont permis d'identifier plusieurs aspects à améliorer et de formuler des recommandations claires pour les PME suisses et leurs prestataires de services.

2.1. POLITIQUE INTERNATIONALE ET CRIME ORGANISE

Les cyberattaques étaient perçues comme s'inscrivant dans une conspiration internationale, avec des enjeux politiques mondiaux. Si plusieurs participants ont cité des attaques cybernétiques proches d'eux ou de leur entreprise (majoritairement Meier Tobler, comme indiqué précédemment), ils les ont généralement placées dans le contexte de confrontations politiques internationales. Les élections américaines et la supposée ingérence russe ont souvent été citées en exemple, tout comme le terrorisme. La Suisse était toutefois considérée comme un havre de sécurité, car dotée d'un système politique plus stable. Les personnes interrogées avaient malgré tout conscience que le crime organisé est une force puissante qui coordonne les cyberattaques. Pour réussir, les attaques nécessitent la coordination de plusieurs spécialistes et des ressources en termes de données sur le long terme, ce qui implique une organisation. Le gain financier a été cité comme l'un des moteurs des cyberattaques, mais le désir de pouvoir a également été mentionné quelquefois. Si la dimension politique peut donner l'impression que la cybercriminalité est un concept éloigné, les motifs financiers et criminels la rendent plus proche et concrète, et donc plus tangible pour les participants.

Illustration 2: Service secret

SERVICE SECRET

La structure du pouvoir à l'échelle internationale connaît d'importants changements, et peu importe si quelques personnes meurent. Mais les choses sont différentes en Suisse, car tout le système est plus sûr.

Illustration 3: Homme de l'ombre

HOMME DE L'OMBRE

Personne ne connaît son identité, mais il s'agit clairement du crime organisé, de la mafia. On peut toujours appeler la police ou se retirer, mais la confrontation directe est trop dangereuse.

Illustration 4: Le butin

LE BUTIN

L'argent, beaucoup d'argent. Au bout du compte, tout tourne autour de l'argent.

La tendance à associer la cybercriminalité aux grandes forces géopolitiques tout en présumant que la Suisse est un havre de sécurité peut rendre les PME suisses vulnérables. Les salariés risquent de ne pas être aussi attentifs qu'ils le devraient. Mais reconnaître le rôle du crime organisé et ses motifs financiers est un signe positif.

2.2. LE HACKER MYTHIQUE

La personne qui commet l'attaque a souvent été désignée par le terme anglais de «hacker» et décrite comme un personnage encapuchonné derrière un ordinateur. Toutes les personnes interrogées ont indiqué qu'un hacker ne ressemble sans doute pas vraiment à cela et qu'il peut s'agir d'un homme aussi bien que d'une femme. Les pirates étaient perçus comme possédant une expertise technique considérable et comme bénéficiant d'espaces de travail bien équipés – en réalité mieux équipés que la plupart de leurs victimes potentielles. Les hackers n'étaient pas généralement vus comme des êtres malfaisants. Ils ont souvent été identifiés comme de potentiels agents du bien – qui révèlent des réseaux pédophiles ou des corruptions, par exemple. Ces perceptions antagonistes ouvrent la voie à des hackers éthiques, qui éprouvent les défenses d'une société contre une juste rémunération.

Illustration 5: Le hacker

LE HACKER

Connecté à plusieurs personnes dans plusieurs pays. Anonyme et terrifiant.

Illustration 6: Espace de travail agréable

ESPACE DE TRAVAIL AGREABLE

J'ignore pourquoi il a tant d'appareils, mais il les utilise tous. Il peut même pirater des entreprises préparées et bien protégées.

Illustration 7: Bandit ou bienfaiteur?

BANDIT OU BIENFAITEUR?

Mes sentiments sont neutres. Il pourrait être un criminel ou un lanceur d'alerte.

Les réponses données ont confirmé une conscience de la nature complexe des cyberattaques et de ce qui les motive, ainsi que des possibles bénéfices de l'activité des lanceurs d'alerte. Toutefois, en associant les attaques à des forces géopolitiques supérieures, ils risquent de les reléguer à un scénario dans lequel leur PME et eux sont «trop insignifiants» pour attirer une attention inopportune – ce qui accroît automatiquement leur vulnérabilité.

2.3. SENTIMENT D'IMPUISSANCE

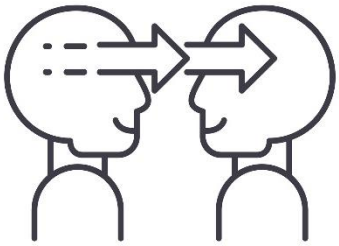
Les participants ont ouvertement évoqué l'opacité des cyberattaques et leur manque de compréhension des dynamiques. Les données peuvent être minées sans que personne ne le remarque, comme un aimant qui attire les métaux ferreux. Les réactions aux cyberattaques peuvent être influencées et manipulées au fil du temps, sans que personne ne s'en aperçoive. Plusieurs questions restent sans réponse – qui est à l'origine des attaques et pour quelle raison, et comment faut-il réagir pendant ou après une attaque. Le sentiment global actuel est un sentiment d'impuissance face aux attaques cybernétiques. Ce n'est pas un signe positif, car cela décourage l'implication active et l'adoption de mesures de défense raisonnables. A l'inverse, cela augure d'un auditoire intéressé et motivé pour les campagnes d'information et les programmes de formation destinés à renforcer les connaissances en la matière.

Illustration 8: Aimant à données

AIMANT A DONNEES

Les données peuvent être extraites d'un réseau comme un aimant qui attire tout à lui.

Illustration 9: Manipulation sociale



MANIPULATION SOCIALE

On abuse de la confiance. Si un employé ne prête pas attention, il peut commettre une erreur et perdre son emploi.

Illustration 10: Questions sans réponse

QUESTIONS SANS REPONSE

Pourquoi a-t-il fait cela? Que pouvons-nous faire? Nous ne pouvons pas apporter de réponse ni trouver de solutions par nous-mêmes.

Malheureusement, le sentiment d'impuissance entraîne la passivité, tant dans la préparation aux cyberattaques que dans la réponse qui y est apportée. La responsabilité de la cyberprotection est alors confiée à des tiers plus compétents et spécialisés, au lieu de continuer à se concentrer sur le rôle que chaque salarié joue dans la sécurité de l'entreprise. Des programmes de formation dédiés doivent être élaborés afin de sensibiliser aux comportements à risque et de faire connaître les outils permettant aux employés d'être plus proactifs.

2.4. SENTIMENT DE VULNERABILITE

Les personnes interrogées savent qu'elles sont observées lorsqu'elles naviguent sur Internet. Elles n'apprécient pas ce sentiment et se plaignent de leur incapacité à se prémunir contre cette surveillance. Elles savent qu'on peut abuser de leur confiance pour porter atteinte à leur employeur et qu'elles peuvent directement ou indirectement en pâtir. L'une des personnes interrogées a fait la comparaison avec le fait d'ouvrir la porte à un inconnu qui pourrait pénétrer dans le bâtiment et voler l'équipement. De plus, nous avons tous une vie privée et des comportements que nous n'aimerions pas voir divulgués. Cela nous rend vulnérables et incapables de nous défendre contre une attaque. Les hackers exploitent notre vulnérabilité et se fraient un accès par des attaques par hameçonnage conçues pour nous prendre par surprise.

Ce sentiment de vulnérabilité étant déplaisant, la réaction humaine classique est d'éviter d'y penser. Comme un répondant l'a dit, «si nous pensions à tout ce qui peut arriver, nous ne nous connecterions jamais à Internet». Mais avoir conscience de la gravité des attaques par hameçonnage est un signe encourageant du niveau de connaissances que les employés possèdent déjà en matière de cyberattaques et, par conséquent, il s'agit d'un point de référence pertinent dans les sessions de formation.

Illustration 11: Surveillance

SURVEILLANCE

Une personne regarde par-dessus l'épaule de cette jeune femme. Elle ne peut pas l'empêcher. Je n'aime pas avoir cette sensation.

Illustration 12: Attention!

ATTENTION!

Cette personne subit un chantage – un élément de sa vie privée a été rendu public. Il a commis une erreur sur un réseau social.

Illustration 13: Hameçonnage

HAMEÇONNAGE

Des données sont volées par des attaques par hameçonnage. Vous pouvez tenter de vous protéger avec un antivirus et d'autres programmes, mais cela ne vous protégera pas contre des professionnels.

Avoir conscience d'être observé est une bonne chose et peut motiver à mieux évaluer les risques et à être plus prudent sur Internet. Comprendre la menace spécifique que représente l'hameçonnage est important et positif. L'hameçonnage est la façon la plus sournoise d'exploiter les vulnérabilités humaines parce qu'il permet aux malfaiteurs de recueillir des informations sans être vus et prend beaucoup de temps avant d'être repéré. Pour y faire face, il faudra notamment apprendre aux gens à répondre aux demandes en ligne avec une prudence adéquate.

2.5. ISSUE CATASTROPHIQUE

Les participants percevaient les cyberattaques comme une autre forme de cambriolage, dont la seule tentative est elle aussi préjudiciable et inquiétante. L'incident qui a paralysé Meier Tobler, un fournisseur, a fait prendre conscience de l'issue potentiellement catastrophique d'une telle attaque. Si la société a finalement pu rétablir ses activités, le préjudice financier était important et les personnes interrogées elles-mêmes ont été impactées dans leurs activités quotidiennes. Fait intéressant, si elles faisaient preuve de soutien et de compréhension envers les problèmes de leur partenaire commercial, elles étaient aussi manifestement irritées par le fait que les problèmes n'aient pas pu être résolus plus rapidement. D'une manière générale, les participants avaient largement conscience de la possibilité de paralysie des systèmes informatiques et des conséquences dévastatrices que cela aurait sur leur activité.

Illustration 14: Effraction moderne

EFFRACTION MODERNE

Les cyberattaques ne sont que la façon moderne d'entrer par effraction chez quelqu'un. La protection normale ne suffit pas à empêcher la personne d'entrer et cela cause des dommages quoi qu'il arrive – ne serait-ce qu'une fenêtre brisée.

Illustration 15: Attaque contre notre fournisseur

ATTAQUE CONTRE NOTRE FOURNISSEUR

Notre fournisseur était totalement automatisé et a été attaqué. Il ne pouvait plus fonctionner et a perdu des millions. Cela pourrait nous arriver aussi.

Illustration 16: J'espère que non!

J'ESPERE QUE NON!

Tout peut vous exploser au visage.

La sensibilisation aux potentielles conséquences des cyberattaques constitue clairement un point de départ pour les programmes de formation. Il était également évident que la bienveillance envers les partenaires commerciaux affectés par des cyberattaques était limitée, ce qui indique que la période de restauration, avant des effets à long terme sur les relations commerciales, peut être relativement courte. En cas d'attaque, il est par conséquent vital de restaurer les opérations aussi rapidement que possible.

2.6. CELA NE ME CONCERNE PAS

Si les personnes interrogées ont admis leurs propres vulnérabilités, elles se considèrent aussi comme ayant peu de valeur et, par conséquent, peu susceptibles d'attirer une attention inopportune. Dans une certaine mesure, cette façon de penser s'appliquait aussi à l'entreprise pour laquelle elle travaille. Les PME étaient vues comme trop petites par rapport aux multinationales. Les entretiens ont également révélé un sentiment sous-jacent que les risques pouvaient être surestimés et que la crainte d'une attaque pouvait induire des mesures inutiles et potentiellement préjudiciables. Toutefois, si la société était attaquée, des prestataires de service externes apporteraient des solutions et leur expertise pour résoudre le problème, de la même manière qu'une bonne infirmière traite les patients malades dans un hôpital bien équipé. Cette comparaison-ci suggère une possible faiblesse du système. Nous nous en remettons volontiers aux soins des médecins et des infirmières et nous ne nous soignerions pas nous-mêmes si nous étions gravement malades. De la même manière, nous pouvons assumer qu'il est de facto plus judicieux de laisser la sécurité numérique aux seules mains des experts.

Illustration 17: Le monde entier

LE MONDE ENTIER

Dès que la prise est branchée, le monde entier est connecté et nous avons accès à l'ensemble des connaissances. Un changement très positif.

Illustration 18: Peur

PEUR

Peur infondée de tout ce qui se passe en ligne, alors que nous sommes relativement protégés. Une trop grande protection est inutile.

Illustration 19: Soutien personnel

SOUTIEN PERSONNEL

C'est ainsi qu'une société se sent lorsqu'elle est attaquée – comme une personne malade et qui a besoin d'experts externes et d'un équipement spécialisé pour être soignée.

L'impression d'être trop petit et insignifiant pour être la cible des cybercriminels est sans doute l'aspect le plus inquiétant dans la façon dont beaucoup de salariés de PME pensent. Si les particuliers peuvent ne pas être la cible ultime d'une attaque, ils peuvent constituer à leur insu le maillon le plus faible de la chaîne, si les cybercriminels peuvent accéder aux systèmes d'une société par leur intermédiaire. Les petites PME ne seront peut-être pas directement dans la ligne de mire, mais elles peuvent néanmoins être des cibles faciles pour les criminels. La dépendance excessive à l'expertise de tiers peut également décharger les personnes de leur responsabilité quant au problème et à sa solution, restreignant encore la vigilance et la réactivité en cas de cyberattaque.

2.7. PROACTIF ET ENGAGE

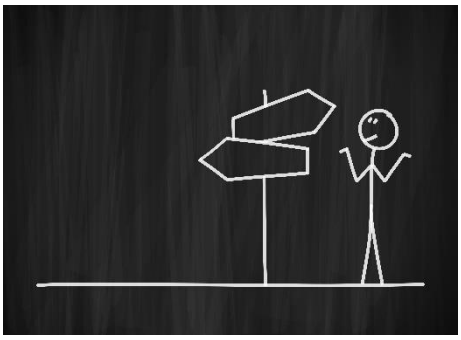
Les personnes interrogées ont eu des réactions incroyablement variées à l'évocation des potentielles attaques et perturbations opérationnelles. Loin d'être paralysées, elles ont affiché leur motivation pour s'attaquer au problème et aller de l'avant. Une route dans le brouillard – signalant un manque d'information – est donc une métaphore pour trouver la voie à suivre malgré l'adversité, et un panneau de signalisation en blanc le symbole de la nécessité de concevoir une solution. De nombreux outils basés sur des technologies et des processus de travail plus anciens peuvent être utilisés pour préserver le fonctionnement de la société en cas d'interruption.

Illustration 20: Brouillard

BROUILLARD

Lors d'une cyberattaque, tout est incertain, mais je veux aller de l'avant, trouver la voie conduisant à une solution. Je n'ai pas peur de ce qui se cache dans le brouillard, mais je dois avancer prudemment pour ne pas me perdre.

Illustration 21: Planification



PLANIFICATION

Vous devez trouver vous-mêmes vos repères, puisqu'il n'existe pas de solution toute faite. Les panneaux indiquent des directions différentes parce qu'un problème a toujours plusieurs solutions. Vous devrez peut-être utiliser votre téléphone portable personnel si les systèmes de la société sont en panne.

Illustration 22: Comme au bon vieux temps

COMME AU BON VIEUX TEMPS

Lors de l'attaque qui a frappé notre fournisseur, nous sommes repassés au téléphone, au stylo et au papier, comme au bon vieux temps. Cela a assez bien fonctionné, hormis le fait que toutes les données comptables étaient stockées dans le système.

Cet état d'esprit dynamique et le désir de poursuivre l'activité sont un formidable atout pour les PME. Au lieu d'attendre que des prestataires de services informatiques externes rétablissent la situation à la normale, les salariés ont voulu contribuer à préserver le fonctionnement de l'activité. Avec un peu de planification et de formation, les PME suisses devraient être capables de développer un flux de travail hors ligne basé sur la collaboration des employés, leur énergie et leur motivation. Cela permettrait d'éviter les interruptions brutales et graves dans leurs interactions avec les clients et de renforcer leur capacité à résister à une attaque cybernétique.

Discussion

Les employés interrogés ont rapporté toute une série d'émotions nuancées et différenciées lorsque nous les avons invités à réfléchir aux cyberattaques et à en discuter. Comme on pouvait s'y attendre, ces diverses émotions étaient contradictoires mais elles coexistaient dans l'esprit des membres du groupe. Elles peuvent être regroupées en sept grandes thématiques qui, d'une manière ou d'une autre, s'appliquent à l'ensemble des personnes interrogées. Chaque thématique a été abordée de manière individuelle à la section 2. Certains aspects peuvent être catégorisés plus en détail en fonction des caractéristiques spécifiques des employés, et sont examinés à la section suivante. En outre, nous avons pu formuler des recommandations pour les PME et leurs prestataires de services.

3.1. IMPACT PAR CATEGORIE DE SALARIES

Lors des entretiens, nous avons relevé d'autres signes d'attitudes variant en fonction de la catégorie de salariés. Les catégories et les différences sont purement empiriques et reflètent nos observations plus que des réflexions théoriques ou fondamentales. Nous estimons toutefois qu'elles éclairent notre discussion.

3.1.1. Personnel administratif et ouvriers

La première différence que nous avons constatée concerne le personnel administratif qui travaille dans les bureaux et les ouvriers qui travaillent dans l'atelier de fabrication ou sur les sites des clients. Les ouvriers ont habituellement peu accès aux systèmes informatiques – principalement ceux liés aux systèmes de fabrication – et ils se sentent donc généralement moins directement affectés par les cyberattaques. A l'inverse, le personnel administratif comprend parfaitement les conséquences de tels problèmes. Ils se rappellent de moments où leurs systèmes ont été en panne pendant de longues périodes, ou des conséquences sur leur propre travail de l'attaque contre Meier Tobler. Par conséquent, le personnel administratif devrait être disposé à soutenir l'élaboration de processus de secours et à les mettre en pratique régulièrement.

3.1.2. Jeunes et vieux

Une autre différence potentielle – suggérée par plusieurs participants – pourrait exister entre les salariés plus jeunes et plus âgés, étant sous-entendu que les personnes plus âgées pourraient être plus vulnérables aux attaques que les plus jeunes. Les salariés plus jeunes étaient clairement plus familiarisés avec la technologie numérique et plus actifs sur les réseaux sociaux. Les salariés plus âgés ont déclaré ne pas avoir grandi avec la technologie et la connaître toujours mal. Ils adoptaient, par conséquent une approche plus prudente – peut-être parce qu'ils étaient plus sensibilisés aux messages suspects, plus réticents à s'engager et plus disposés à demander conseil en cas de doute, notamment dans le cadre professionnel. Même s'il n'est pas possible de discerner le profil de risque réel, les réponses des personnes interrogées suggèrent que ces différences ne seraient pas déterminantes. Les salariés plus jeunes sont plus familiarisés avec la technologie et, donc, plus conscients des risques, mais les salariés plus âgés ont tendance à compenser leur manque de connaissance par un surcroît de prudence.

3.1.3. Experts et novices

Dans la même idée, il est possible de répartir les salariés en fonction de leur expertise numérique. Ce critère présentait une certaine corrélation avec celui de l'âge, mais les niveaux d'expertise spontanément décrits par les plus jeunes étaient manifestement très disparates. Les salariés plus compétents étaient également plus confiants quant à leur capacité à déceler des cyberattaques et à s'en remettre. Ils avaient également tendance à minimiser toute perte potentielle. Les salariés moins informés avaient tendance à se protéger en limitant leur activité en ligne et en n'utilisant que des plateformes spécifiques (p. ex. la banque en ligne) qu'ils jugeaient adéquatement sécurisées par un tiers. S'il est difficile de déterminer le véritable impact de ces différences, il n'est pas évident qu'une plus grande confiance réduise la vulnérabilité potentielle. Les salariés qui, subjectivement, se sentaient plus compétents – et qui sont par conséquent plus confiants – peuvent être moins réticents à prendre des risques, s'exposant ainsi à un danger plus conséquent.

3.1.4. Cadre professionnel et cadre personnel

Une autre différence concerne le comportement individuel et semble influencée par l'environnement (p. ex. le fait de travailler sur le système de messagerie de la société et sur un appareil personnel). Les participants ont indiqué être plus prudents dans un cadre professionnel, en partie à cause des interactions avec l'extérieur et les clients, et en partie parce qu'ils avaient l'impression que les dommages potentiels étaient plus importants. Le cadre professionnel tend aussi à être plus complexe, les conversations évoquant fréquemment les noms de clients et partenaires inconnus, renforçant encore la prudence. Plusieurs employés ont mentionné des e-mails frauduleux émanant de faux clients ou fournisseurs, de sorte que les défenses étaient généralement élevées. Les entretiens ont révélé une vigilance moindre dans le cadre personnel. Cela s'expliquait au moins en partie par le fait que les participants pensaient pouvoir repérer les noms ou fils de discussion suspects plus facilement et parce que la plupart d'entre eux ne se jugeaient pas suffisamment importants pour susciter une cyberattaque. Cette distinction peut constituer une menace si ce relâchement gagne le cadre professionnel ou si des appareils personnels sont piratés et utilisés pour compromettre les systèmes de l'entreprise. Une menace encore accrue si les employés sont régulièrement amenés à travailler à domicile, comme c'est le cas actuellement avec la pandémie de coronavirus.

3.2. RECOMMANDATIONS D'AMELIORATION

Nos recommandations d'amélioration sont basées sur quelques observations manifestes faites durant les entretiens. D'une manière générale, les employés sont motivés et proactifs; mais ils perçoivent souvent les cyberattaques comme un problème réservé aux experts. Si les experts sont effectivement nécessaires, chacun peut contribuer à concevoir des solutions et à se remettre d'une attaque. Il est par ailleurs difficile de déterminer dans quelle mesure les salariés sont conscients des risques et des conséquences potentielles pour leur société. Forts de ce constat, nous recommandons trois grands axes d'amélioration. Ces améliorations peuvent être mises en œuvre par les sociétés elles-mêmes ou par des prestataires de services, dans le cadre de leur offre. Ces recommandations s'ajoutent aux conseils standard donnés aux sociétés pour sécuriser leur infrastructure et atténuer la gravité des attaques potentielles. L'infrastructure devrait être renforcée par des pare-feux adéquats ainsi que des mesures de sécurité physiques et par un mot de passe, et il conviendrait de concevoir un plan de réponse d'urgence et de rétablissement. La gravité d'une attaque peut être contrôlée en identifiant et en protégeant les actifs plus précieux de la société, les «joyaux de la couronne». Il s'agit souvent de données exclusives, de renseignements sur les clients et de l'équipement de production. Les recommandations présentées dans cette étude sont destinées à enrichir ces conseils généraux, notamment pour les PME.

3.2.1. Sensibiliser

Les salariés semblent avoir conscience tant des conséquences potentiellement dramatiques des attaques cybernétiques que de leur propre vulnérabilité, notamment en cas de tentative d'hameçonnage. Dans le même temps, ils jugent leur entreprise trop insignifiante pour justifier une attaque. Les cyberattaques sont également perçues comme s'inscrivant dans un conflit politique mondial plutôt que comme une menace plus proche. Bien entendu, c'est une attitude dangereuse, et les statistiques nationales ainsi que plusieurs cas très médiatisés devraient servir d'avertissement. Ces informations doivent être communiquées directement et systématiquement aux employés. Ceux-ci devraient en outre être régulièrement informés du nombre d'attaques déjouées perpétrées contre l'infrastructure informatique de la société et des mesures que celle-ci prend pour se protéger (comme la mise à niveau des pare-feux). Il convient également de leur rappeler les habitudes simples qu'ils doivent adopter afin de réduire les risques. Les sociétés devraient également tester les défenses de leurs systèmes et la vulnérabilité de leurs employés, peut-être en employant des pirates éthiques – si elles en ont les moyens – puisque les employés ont de la sympathie pour les hackers qui travaillent pour la bonne cause. Les conclusions devraient être ensuite communiquées aux salariés afin de souligner l'importance du rôle qu'ils jouent dans la protection de la société.

3.2.2. Responsabiliser les employés

Il est communément admis que les pirates sont très compétents et bien équipés, que le monde cybernétique est complexe et que les prestataires de services spécialisés constituent la principale ligne de défense. Si c'est vrai

dans une certaine mesure et si les prestataires de services professionnels sont l'un des rouages d'un système de protection et de réponse efficace, ils ne peuvent pas fonctionner en vase clos. Confier la responsabilité de la cybersécurité à un tiers invite les salariés au laisser-aller, alors que leur comportement en ligne constitue une ligne de défense cruciale contre les attaques. Les salariés des PME ont également tendance à être dynamiques et désireux d'agir. En plus de sensibiliser les employés dans le cadre de leurs fonctions, il faut les encourager à participer à la découverte et au signalement des attaques et les enrôler dans la conception des solutions (voir la section 3.2.3 ci-dessous). Il doit être demandé aux prestataires de services externes de donner des instructions aux salariés et de les impliquer autant que possible.

3.2.3. Concevoir un mode de reprise

Dans le cas d'une attaque, ou plus habituellement, d'une erreur d'un système, les employés ne savent pas toujours comment réagir. La réaction ne devrait toutefois pas être improvisée ou aléatoire. Des scénarios devraient être planifiés à l'avance, avec les outils pertinents, et les éléments déclencheurs des procédures d'urgence doivent être clairement définis. Nos entretiens ont révélé que, en particulier, il peut être difficile d'accéder aux informations relatives à la facturation clients et aux spécifications techniques des produits lorsque l'on travaille hors ligne, et cela nécessite une attention toute particulière.

La conception d'un scénario sans informatique peut également être l'occasion d'un travail d'équipe et de tirer parti des connaissances de chaque employé. A titre d'exemple, les entreprises peuvent mettre en place un atelier, lors duquel les salariés tentent d'accomplir leur travail quotidien sans les outils informatiques habituels. De cette manière, ils découvriront rapidement quelles sont les informations vitales qui doivent être disponibles par des systèmes hors ligne, quelles tâches peuvent être effectuées sur des appareils personnels ou sur un support papier. Des outils peuvent alors être développés en temps normal et régulièrement testés lors d'exercices de mise en situation, où l'activité s'effectue sans l'infrastructure informatique standard. Le fonctionnement du mode de reprise doit comporter strictement les mêmes événements déclencheurs prédéterminés, en fonction du système affecté et de la durée de l'interruption.

Illustration 23: Recommandations d'amélioration

RECOMMANDATIONS D'AMELIORATION

PREPARER

SENSIBILISER

RESPONSABILISER LES EMPLOYES

CONCEVOIR UN MODE DE REPRISE

Conclusions

Les cyberattaques constituent un problème important et croissant, et les PME suisses n'y échappent pas. Les attaques par rançongiciels ciblées ont augmenté ces dernières années, de même que les autres menaces financières, et, d'une manière générale, les PME suisses ont elles aussi subi plus d'attaques par logiciel malveillant. Outre une infrastructure technologique bien conçue et à jour, la sensibilisation des employés et un comportement en ligne vigilant sont essentiels à tout mécanisme de défense; les attaques cybernétiques commençant habituellement par l'infiltration des systèmes informatiques via des attaques par hameçonnage. Ces attaques exploitent des failles humaines pour récupérer des mots de passe ou d'autres informatiques critiques. Des attaques par hameçonnage interviennent presque en permanence, et il s'écoule souvent plusieurs mois entre un hameçonnage réussi et l'attaque proprement dite, ce qui rend difficile le suivi et les rétroactions aux employés. Le degré «normal» de vigilance et le comportement en ligne des salariés sont par conséquent le meilleur indicateur de la vulnérabilité aux attaques par hameçonnage.

Pour cette étude, nous avons interrogé plusieurs employés de trois PME suisses afin de comprendre comment ils percevaient les cyberattaques. Notre recherche est basée sur des métaphores profondes, afin de comprendre les émotions et les moteurs cachés des comportements des salariés face aux menaces représentées par la cybercriminalité. Les réponses ont été combinées dans des thèmes communs qui mettent en avant la grande variété des pensées et émotions associées au monde numérique. Les employés inscrivaient les cyberattaques dans le contexte plus large de la politique mondiale, tout en reconnaissant leurs motivations purement financières et criminelles. Ils voyaient les hackers comme des opérateurs compétents et bien équipés, mais ils ne les percevaient pas systématiquement comme des êtres malfaisants. Ils se sentaient vulnérables et impuissants face aux cyberattaques et ils reconnaissaient le préjudice qu'elles sont susceptibles de causer. Parallèlement, ils avaient tendance à penser que leur société et eux-mêmes avaient trop peu d'importance pour en être la cible, et ils s'en remettaient à des tiers pour assurer leur protection en cas d'attaque. Toutefois, ils étaient globalement proactifs et désireux de contribuer à élaborer des solutions pratiques.

Nous avons proposé trois suggestions concrètes aux PME pour améliorer les recommandations générales existantes en matière de cybersécurité. Elles s'appuient sur les éléments positifs de la culture qui prévaut au sein des PME et concernent les aspects qui présentent les risques les plus importants. D'autres informations sont nécessaires pour sensibiliser les salariés, tout comme la fourniture d'outils appropriés, afin d'accompagner le passage à une prise en charge plus directe par les salariés des problèmes et de leurs solutions. De plus, les sociétés ont besoin de concevoir des procédures en cas de panne du système et de s'entrainer. D'autres recherches devraient étudier des différences éventuelles entre les employés qui répondent ou non aux attaques par hameçonnage, déterminer si les employés des grandes entreprises ont une attitude similaire envers la cybersécurité; et également si les mesures que nous suggérons ici atténuent la menace de cyberattaques.

Références

Allianz (2020). *Baromètre des risques 2020 d'Allianz*. (accès le 25 novembre 2020) https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2020-fr.html

Anz P. (2020). *Daten aus Cyber-Attacke auf Stadler Rail veröffentlicht*. (accès le 25 novembre 2020) https://www.inside-it.ch/de/post/daten-aus-cyber-attacke-auf-stadler-rail-veroeffentlicht-20200529

Borkert S. (2020). *Bankrott auch mit Cyberangriff begründet: Wurde Mörschwiler Swisswindows in den Ruin gehackt?*. (accès le 25 novembre 2020) https://www.tagblatt.ch/wirtschaft/bankrott-auch-mit-cyberangriff-begruendet-wurde-moerschwiler-swisswindows-in-den-ruin-gehackt-ld.1198956

Christensen G.L. et Olson J.C. (2002). Mapping Consumers' Mental Models with ZMET. *Psychology and Marketing*, Vol. 19 (6): 477-502. doi: 10.1002/mar.10021

Damasio A. R. (1994). Time-locked multiregional retroactivation: A systems level proposal for the neural substrates of recall and recognition. Dans P. D. Eimas & A. Galaburda (Eds.), *Neurobiology of cognition* (pp. 24–62). Cambridge, MA: MIT Press.

de Moura G. et al. (2020). *Cybersecurity Leadership Principles Lessons learnt during the COVID-19 pandemic to prepare for the new normal*. Forum économique mondial (accès le 25 novembre 2020) https://www.weforum.org/reports/cybersecurity-leadership-principles-lessons-learnt-during-the-covid-19-pandemic-to-prepare-for-the-new-normal

Dreissigacker A., von Skarczinski B. et Wollinger G.R. (2020).*Cyberangriffe gegen Unternehmen in Deutschland*. Kriminologisches Forschungsinstitut Niedersachsen e.V., Forschungsbericht 152

Office statistique fédéral (2020). *Chiffres sur les PME*. (accès le 25 novembre 2020) https://www.kmu.admin.ch/kmu/fr/home/faits-et-tendances/politique-pme-faits-et-chiffres/chiffres-sur-les-pme/entreprises-et-emplois.html

Griesser Kym T. (2020). *Nach Cyberangriff: Erpresser erhöhen Druck auf Stadler*. Tagblatt. (accès le 25 novembre 2020) https://www.tagblatt.ch/wirtschaft/erpresser-erhoehen-druck-auf-stadler-ld.1235844

Heer A. (2020). *Cybercriminalité à l'encontre des entreprises*. (accès le 25 novembre 2020) https://www.swisscom.ch/fr/magazine/securite-des-donnees-infrastructure/cyberattaques-entreprises-malware-phishing/

Jochum K. (2019). *Offix von massivem Hacker-Angriff getroffen*. (accès le 25 novembre 2020) https://www.inside-it.ch/de/post/offix-von-massivem-hacker-angriff-getroffen-20190703

Klein R. (2020). *Schweizer Fensterfirma Swisswindows AG geht nach Ransomware-Angriff pleite*. (accès le 25 novembre 2020) https://dataloft.ch/security/schweizer-fensterfirma-swisswindows-ag-geht-nach-ransomware-angriff-pleite/

Lüscher A., et Niedermann M. (2019). *Hacker legen Schweizer Grossunternehmen lahm*. SRF (accès le 25 novembre 2020) https://www.srf.ch/news/wirtschaft/geht-es-um-loesegeld-hacker-legen-schweizer-grossunternehmen-lahm

Luzerner Zeitung (2019). *Cyberattacke gegen Meier Tobler legt Betrieb weitgehend lahm*. (accès le 25 novembre 2020) https://www.luzernerzeitung.ch/wirtschaft/cyberattacke-gegen-meier-tobler-legt-betrieb-weitgehend-lahm-ld.1138900

Mändli Lerch K. et Repic, A. (2017). *Cyberrisiken in Schweizer KMUs*. (accès le 25 novembre 2020) https://gfs-zh.ch/wp-content/uploads/2017/12/Schlussbericht_CyberriskKMU_12122017.pdf

Meier Tobler (2020). *Geschäftsbericht 2019 Meier Tobler Group AG*. (accès le 25 novembre 2020) https://www.meiertobler.ch/de/content/download-file/6534/file/25.02.20%20Gesch%C3%A4ftsbericht%202019.pdf

MELANI (2020a). *Prudence: un nombre croissant de PME victimes de rançongiciels*. (accès le 25 novembre 2020) https://www.ncsc.admin.ch/ncsc/fr/home/aktuell/news/lettre-d-information/sicherheitsrisiko-durch-ransomware.html

MELANI (2020b). *Rapport semestriel 2020/1*. (accès le 25 novembre 2020) https://www.ncsc.admin.ch/ncsc/fr/home/dokumentation/berichte/rapports-sur-la-situation/rapport-semestriel-2020-1.html

Moser S. (2019). Cyberrisiken – die unterschätzte Gefahr. *Neue Zürcher Zeitung*. 22.05.2019.

Olson J. C., et Reynolds, T. J. (1983). Understanding consumers' cognitive structures: Implications for advertising strategy. Dans L. Percy & A. G. Woodside (Eds.), *Advertising and consumer psychology* (pp. 77–90). Lexington, MA: Lexington Books.

Papedis (n. d.). *Groupe OFFIX*. (accès le 25 novembre 2020) https://www.papedis.ch/fr/entreprise/groupe-offix/.

Pugnetti C. et Bekaert X. (2018). *A Tale of Self-Doubt and Distrust. Onboarding Millennials: Understanding the Experience of New Insurance Customers*. ZHAW School of Management and Law, ISBN 978-3-03870-021-0.

Pugnetti C. et Schneebeli M. (2020). Kundenbedürfnisse und Marktpenetration. Schweizer KMUs unterschätzen die Bedeutung von Dienstleistungen und Versicherungsdeckungen gegen Cyberrisiken. *Schweizer Versicherung*, janvier 2020.

Pugnetti C., Casián C., Staub N. et Ellenberger T. (2019). Cyber-Resilienz steigern. *Schweizer Versicherung*, octobre 2019.

Schäppi M. (2020). *Cyberattacke auf Meier Tobler, Dienstleister der Gesundheitsbranche*. (accès le 25 novembre 2020) https://www.infosec-health.ch/_Resources/Persistent/77d3731325caf3cb4a5060a02fea716d543be3c3/K_Ref2_Sch%C3%A4ppi_Cyberangriff%20auf%20DL%20der%20Gesundheitsb.pdf

Severin C. (2019). *Wie ein Schweizer KMU ohne Lösegeld, dafür mit Militärtaktik einen Hackerangriff überlebt hat*. (accès le 25 novembre 2020) https://www.offix.ch/media/cms/Offix/Media/NZZ_Cyber-Angriff%20auf%20KMU_OFFIX-Gruppe.pdf

SIA (2018). *Document de principe de l'ASA sur les cyberrisques*. Groupe de travail sur les cyberrisques, Association suisse d'assurances (accès le 25 novembre 2020) https://www.svv.ch/sites/default/files/2018-04/Grundlagenpapier%20CyberRisiken_Zusammenfassung_FR.pdf

SRF (2020). *Offenbar zwang eine Cyberattacke Swisswindows in die Knie*. (accès le 25 novembre 2020) https://www.srf.ch/news/regional/ostschweiz/konkurs-fensterhersteller-offenbar-zwang-eine-cyberattacke-swisswindows-in-die-knie

Stadler Rail (2020a). *Geschäftsbericht 2019*. (accès le 25 novembre 2020) https://www.stadlerrail.com/media/pdf/web_stadler_rail_gb19_de.pdf

Stadler Rail (2020b). *Cyber-attack against Stadler IT network*. (accès le 25 novembre 2020) https://www.stadlerrail.com/media/pdf/2020_0507_media%20release_cyber-attack_en.pdf

Trustwave (2020). *2020 Trustwave Global Security Report*. (accès le 25 novembre 2020) https://www.trustwave.com/en-us/resources/library/documents/2020-trustwave-global-security-report/

Zaltman G. (1997). Rethinking Marketing Research: Putting People Back In. *Journal of Marketing Research*, Vol. 34, 4. https://doi.org/10.1177/002224379703400402.

Zaltman G. et Zaltman L. (2008). *Marketing Metaphoria: What Deep Metaphors Reveal about the Minds of Consumers*. Harvard Business Press.

Tableaux

Illustrations

Auteurs

Dr. Carlo Pugnetti est chargé de cours à l'Institute for Risk & Insurance de la ZHAW. Ses recherches se concentrent sur l'évolution du comportement des clients dans l'assurance, notamment les changements déclenchés par l'adoption de la technologie et les différences entre les générations. Il explore également les liens entre l'innovation et la gestion des risques.

Avant de rejoindre la ZHAW, Carlo a occupé les fonctions de CEO d'Allianz Global Assistance en Suisse ainsi que d'autres postes au sein du Groupe Allianz – il a restructuré le département des sinistres du Fireman's Fund aux États-Unis, travaillé sur les questions stratégiques au sein de Group Development à Munich et dirigé un secteur d'activité international à Paris. Il a commencé sa carrière en tant que consultant pour Oliver Wyman.

Il est titulaire d'un Ph.D. en analyse des risques et d'un master en ingénierie électrique de l'université de Stanford.

Carlos Casián est assureur risques immobiliers et cyberrisques chez Allianz Suisse. Il a dirigé des programmes de formation en interne et en externe et a participé à plusieurs groupes d'experts. Il est conférencier pour Allianz sur les cyberrisques et il représente Allianz Suisse au sein du groupe de travail cybernétique de l'ASA.

Il a gravi tous les échelons de l'assurance, puisqu'il a commencé sa carrière chez Allianz Suisse il y a plus de dix ans. Ces dernières années, il s'est concentré sur les cyberrisques et leur incidence sur les profils de risque des sociétés.

Il est titulaire d'un BS en gestion d'entreprise, assorti d'une spécialisation en risque et assurance de la ZHAW.

Partenaires

Nous remercions chaleureusement nos sociétés partenaires, qui nous ont permis de nous entretenir avec leurs employés et ont soutenu l'étude.

Kurt Wyss, Partenaire
VTL Insurance + Partner AG

www.vtl.ch

Sokol Prendi, Head of Sales
Dätwyler Fertigungs-Technologie AG

www.daetwylerag.ch

Manuel Fischer, CEO
Fischer Wärmetechnik AG

www.heizprofi.ch

Terence Iseli, CEO
ISELI ENERGIE AG

www.iseli-energie.ch

Xavier Bekaert, Partner
Benthurst & Co.

www.benthurst.com

School of Management and Law

St.-Georgen-Platz 2
Boîte postale
8401 Winterthur
Suisse

www.zhaw.ch/sml

AACSB ACCREDITED

swissuniversities