innovation

OCTOBRE 2018

CYBERSÉCURITÉ

LES ENTREPRISES CONTRE-ATTAQUENT

Bilan

Présenté par swisscom

Connected Event: CyberSécurité

9 octobre 2018
Rolex Learning Center
9h- 14h

Quels sont les nouveaux défis dans la Cybersécurité? Comment faire face aux nouvelles menaces toujours plus sophistiquées? Quels sont les secteurs les plus touchés par les attaques cybernétiques? Nos intervenants vont fournir un éclairage diversifié, avec notamment les résultats d'une enquête effectuée par la CVCI, les actions entreprises par l'Etat et la perspective opérationnelle d'entreprises.

Inscriptions: swisscom.ch/connected-event

Agenda

08h30	Accueil café-croissant
09h00	Introduction et résultat sur l'enquête cybersécurité **Claudine Amstein, CVCI**
09h20	L'impulsion politique **Nuria Gorrite, Canton de Vaud**
09h35	Perspective académique **Jean-Pierre Hubaux, EPFL**
09h55	Suivi d'une discussion entre les trois intervenants et questions-réponses avec le public
10h10	Les enjeux de la cybersécurité **Philippe Vuilleumier, Swisscom**
10h30	L'écosystème des start-ups **Patrick Barbey, Innovaud**
10h45	Café- réseautage et démonstrations
11h15	SICPA - partage d'expériences **Philippe Gillet, SICPA**
11h35	SwissRe - partage d'expériences **Jeff Bohn, SwissRE**
11h55	Digital Trust – gestion intégrée de la sécurité **Lucile Van Kerrebroeck, AWK Group**
12h15	Suivi d'une discussion entre les trois intervenants et questions-réponses avec le public
12h30	Conclusion - Cocktail dînatoire et réseautage
14h00	Fin de l'événement

Modération: Raphaël Rollier

canton de vaud · innovaud · CVCI Chambre vaudoise du commerce et de l'industrie · EPFL École polytechnique fédérale de Lausanne · swisscom · Bilan

L'humain, ce maillon faible

A chaque attaque de hacker, à chaque vol de données, à chaque scandale qui éclate, les défenses se renforcent. Plus les intrusions se renouvellent, plus les entreprises vont bâtir des douves, rehausser les murailles, construire des tours, des créneaux et des mâchicoulis pour protéger leurs données, le trésor du XXIe siècle et de l'économie numérisée.

Mais, à l'instar des châteaux forts de l'époque médiévale, la faille ne vient souvent pas des fortifications de pierre. Mais de l'humain. Rome en 750? Tarpeia ouvre les portes aux envahisseurs sabins. Château-Gaillard en Normandie en 1204: une fenêtre mal fermée permet aux Français d'entrer. Chillon en 1536: la fuite de la garnison offre la forteresse aux Bernois. A chaque fois, ce sont les humains qui font (volontairement ou non) entrer les assaillants dans la place forte.

En 2018, la situation est similaire: à coup de doubles protections, d'intelligence artificielle ou, bientôt peut-être, de blockchain, les systèmes sont puissamment sécurisés. Mais quid des collaborateurs et de leurs pratiques? Quid des clients qui détiennent un compte pour se connecter? Quid des fournisseurs et sous-traitants qui ont accès au système?

Aujourd'hui plus qu'hier, adopter une hygiène numérique est stratégique pour sauvegarder son entreprise. Et pour diffuser les bonnes pratiques, il faut sensibiliser, former, accompagner, guider l'ensemble des personnes qui ont un lien avec le système interne.

Pas question de ne pas colmater les brèches dans les murailles évidemment. Mais à quoi sert-il de financer de lourds travaux de maçonnerie si la sentinelle ne pense pas à fermer la porte à clé pendant son tour de garde? Les hackers, ces spécialistes de la poliorcétique contemporaine, seraient bien embêtés s'ils devaient composer sans les inadvertances humaines.

Une bonne stratégie de cybersécurité, en 2018, passe donc par ces deux volets: sécurisation du système avec les outils et les méthodes les plus agiles et les plus efficaces et formation/sensibilisation sans cesse renouvelée des usagers (collaborateurs, fournisseurs, clients). A l'heure où les frontières s'estompent entre les sphères privée et professionnelle, chacune et chacun a tout à gagner à adopter des pratiques plus sûres. S'ils sont inconséquents, en plus du vol de données personnelles dans les entreprises, les particuliers aussi peuvent se faire pirater leurs réseaux sociaux, boîtes mail et autres éléments personnels.

MATTHIEU HOFFSTETTER
Rédacteur en chef adjoint
Responsable de bilan.ch

Sommaire

04 ENJEUX
Comment les entreprises peuvent se préparer, détecter et répondre à des cyberattaques

08 POLITIQUE
Nuria Gorrite, présidente du Conseil d'Etat vaudois, détaille la stratégie de son canton pour lutter contre la cybercriminalité

09 EN CHIFFRES
La Chambre vaudoise du commerce et de l'industrie a sondé ses membres: un sur deux se sent menacé par les cyberrisques

10 COMMUNICATION
Comment le groupe Swisscom sécurise-t-il les données? Entretien avec Philippe Vuilleumier, responsable au sein du géant suisse

11 INNOVATION
Portrait de quatre startups romandes qui développent des solutions ingénieuses dans la cybersécurité

14 DROIT
Les données, enjeu clé pour les études d'avocats. Témoignage.

15 FINANCE
Les banques sont des cibles de choix: l'exemple de la BCVs, qui multiplie les précautions contre les pirates du net

PHOTOSCOVER: DR, ÉDITO: HUC, DR

RÉDACTRICE EN CHEF
Myret Zaki

RÉDACTION
Chantal de Senger
Matthieu Hoffstetter
Joan Plancade, Marjorie Théry,
Myret Zaki

DIRECTEUR ARTISTIQUE
Pierre Broquet

MARKETING
Dahlia Al-Khudri, Jacques Molinari

ÉDITEUR
Tamedia SA

RÉDACTION PHOTO
David Huc

PUBLICITÉ
Tamedia SA
av. de la Gare 33 - 1001 Lausanne
Tél. +41 21 349 50 50
publicite.lausanne@tamedia.ch

DIRECTRICE ARTISTIQUE ADJOINTE
Charlène Martin

RÉDACTION
11, rue des Rois
1204 Genève
e-mail: bilan@bilan.ch
Tél. +41 22 322 36 36

Cyberattaques: être bien protégé ne suffit plus

Avec le virage numérique des entreprises, les risques financiers et de vol des données augmentent. Tour d'horizon des enjeux et des solutions à leur disposition. PAR MATTHIEU HOFFSTETTER

L'antivirus et le firewall: les deux armes majeures contre le piratage des années 1990 ont depuis longtemps laissé la place à un arsenal bien plus élaboré, complexe et évolutif. «La cybersécurité était alors un sujet parmi d'autres, une des missions du responsable de l'informatique. Mais les enjeux, comme les dangers et les procédures, n'avaient pas atteint le niveau actuel», confie la responsable cybersécurité d'un acteur genevois du secteur des matières premières.

«Quand j'ai fini ma formation à l'EPFL, nous étions huit dans la section cybersécurité. Aujourd'hui, ceux qui achèvent ce cursus sont sans doute dix fois plus nombreux», résume Steven Meyer, CEO de ZENData, société spécialisée dans le cyberrisque. Au cours des quinze dernières années, la mue numérique des entreprises de tous les secteurs s'est accélérée, avec une migration des données, des flux (y compris financiers) mais aussi des plateformes utilisées par les entreprises. Donc les entrées possibles pour des intrus.

Smartphones et applications, internet des objets, solutions cloud pour le stockage... les spécialistes doivent multiplier les postes à surveiller, autant de points névralgiques pour les entreprises. Pourtant, paradoxalement, «on ne peut pas dire qu'il y a eu un bond en avant incroyable des techniques des cybercriminels, juste davantage de failles et de criminels pour les exploiter. Les entreprises sont aujourd'hui plus dématérialisées. Donc l'impact est plus fort qu'il ne l'était auparavant. Et le type de données dématérialisées aujourd'hui a plus de valeur que ce qui circulait cinq ans en arrière. Beaucoup d'entreprises sont dépendantes de ces échanges. La conséquence est aujourd'hui plus grave», analyse Stéphane Koch, spécialiste en cybersécurité, et vice-président d'High-Tech Bridge.

> «Aujourd'hui, la question n'est plus «qui sera une cible?», mais «quand serai-je une cible?»

La vitesse de détection est cruciale

Difficile pourtant de freiner la transformation numérique des entreprises. Elles doivent s'adapter aux nouveaux usages, aussi bien du côté des clients que des partenaires (fournisseurs, sous-traitants) et des collaborateurs. «Nous constatons une maturité plus grande de la part des différents acteurs: les gens s'informent et cherchent des solutions. Je ne suis pas certain que ce soit une question de génération: les jeunes sont plus habitués au risque. Les anciens voulaient interdire beaucoup de choses au nom de la sécurité. Aujourd'hui, on se rend compte qu'il faut ouvrir plus pour intégrer la digitalisation», nuance Duilio Hochstrasser, «évangéliste de la sécurité» chez Swisscom.

«Avant, c'était simple de protéger les données qui étaient hébergées dans l'entreprise: on pouvait identifier et on avait un seul point d'accès. Aujourd'hui

avec le cloud, les données sont réparties un peu partout et ça devient quasiment impossible avec les moyens traditionnels. On ne peut pas tout bloquer sinon on castre le business. On sait qu'il y a des risques et qu'on sera attaqué, on sait que certaines attaques auront du succès. On doit détecter au plus vite ces attaques, qui peuvent durer plusieurs jours, semaines ou mois avec plusieurs vecteurs pour extraire les données. Dans cette phase, la vitesse de détection est cruciale. Autre facteur important, il faut avoir la capacité de répondre correctement, stopper l'attaque et sauver ce qui peut l'être», détaille Duilio Hochstrasser.

Steven Meyer confirme: «L'industrie de la cybersécurité a pivoté d'«on va prévenir toutes les attaques» vers «on va vous aider à répondre aux attaques». Quand on a tout, ce qui manque souvent, c'est «comment répondre en cas de crise». L'industrie met de plus en plus d'énergie dans ce volet.»

La faille des collaborateurs

Car la question n'est plus «qui sera une cible?», mais «quand serai-je une cible?». Les typologies des hackers (voir l'encadré page 6) et les multiples entrées potentielles rendent toute entreprise vulnérable. La mission des experts est donc non seulement de minimiser la vulnérabilité, mais aussi d'organiser la batterie de réponses aux attaques. Et pour minimiser les risques, il existe un levier universel: la sensibilisation et la formation des collaborateurs. «On attaque souvent l'humain car il est plus facile à attaquer que les plateformes et les infrastructures. Si on formait extrêmement bien les collaborateurs, les pirates se tourneraient de nouveau vers la technologie», assure Steven Meyer.

«Le compte Facebook d'une entreprise est géré par un employé, donc ça donne une porte d'entrée. Une attaque sur un privé peut donner une faille sur le pro. Ce que les employés font dans leur vie privée peut impacter la bonne marche de l'entreprise», renchérit Stéphane Koch.

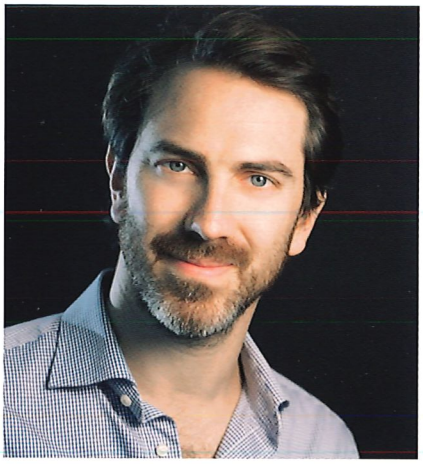
Duilio Hochstrasser, Security Product Manager chez Swisscom.

Si les réseaux sociaux et les apps ont offert aux pirates de nouvelles entrées, parfois avec la complicité innocente des collaborateurs, d'autres vecteurs se sont juste perfectionnés. «Nous assistons à une professionnalisation de l'utilisation de certains procédés. Voilà quelques années, les attaques par e-mails de phishing étaient facilement reconnaissables; désormais les pirates peuvent rédiger un courriel qui a toutes les apparences d'un véritable message d'un proche ou d'une entreprise, avec même des détails de nature à tromper la vigilance du destinataire», avertit Duilio Hochstrasser.

E-banking (lire notre article sur la BCVs en page 15), application pour gérer ses ménages ou comptes médias reliés à des identifiants réseaux sociaux: le quotidien regorge de failles dans lesquelles les pirates peuvent s'engouffrer.

«Aujourd'hui, les hackers préfèrent s'en prendre à l'humain qu'à la technologie car c'est ce qu'il y a de plus facile à bypasser», constate Steven Meyer. Une analyse partagée par Stéphane Koch: «Le collaborateur reste généralement un vecteur de programmation, comme dans les attaques par phishing. Il y a de plus en plus de mélanges entre domaines privé et professionnel et l'employé doit être sécurisé dans

PHOTOS: SHUTTERSTOCK, SWISSCOM



Steven Meyer, CEO de ZENData, société spécialisée dans le cyberrisque.

ses usages des deux natures.»

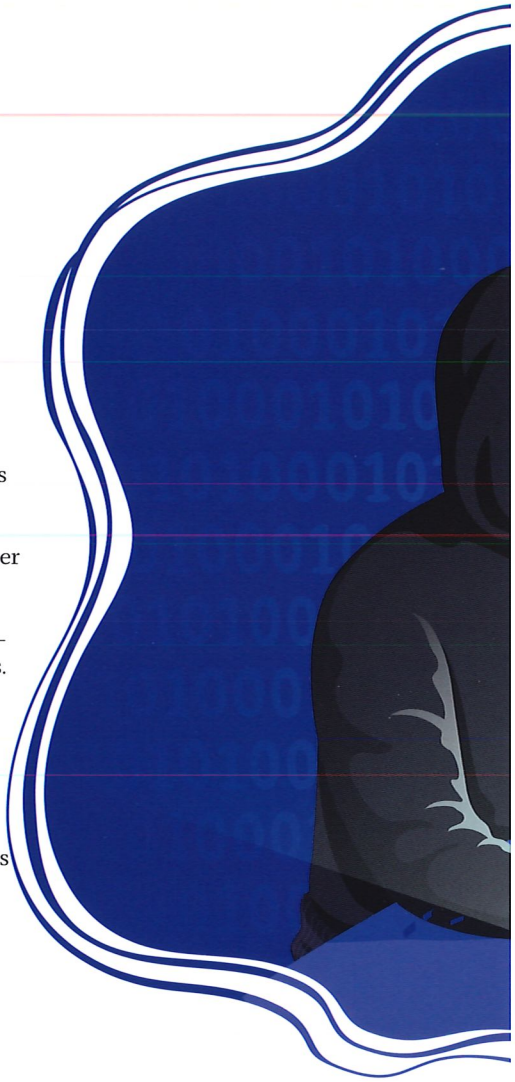
Mais comment passer de la formation des employés à leur prise de conscience? Au-delà des obligations légales ou réglementaires, Steven Meyer recommande d'expliquer raisons et enjeux et même d'ajouter une dimension ludique à cette politique vis-à-vis des employés: «Légalement, il faut diffuser auprès des collaborateurs une règle claire. Mais aussi leur exposer à tous pourquoi ces précautions sont prises. Comme pour les enfants, il faut expliquer les interdits. Dans 99% des cas, l'employé n'est pas malveillant mais fait des erreurs par méconnaissance. Une entreprise peut notamment mettre en place des tests, des procédures et des examens. Et en fin d'année, celui qui a le plus de points reçoit une récompense. Cela encourage le partage et la remontée d'expérience, notamment sous forme ludique.»

Certaines entreprises offrent une tablette ou un autre prix pour celui ayant signalé le plus d'e-mails de phishing dans l'année.

Au-delà des gratifications et du volet ludique, le collaborateur peut aussi réaliser l'importance de ces précautions. «La nature des données n'est pas toujours vitale, mais l'impact en termes de réputation peut faire autant voire plus de dégâts. Une attaque peut bloquer une entreprise dans son fonctionnement. Certaines entreprises bloquées ont dû déposer le bilan», rappelle Stéphane Koch. D'où l'importance d'apprendre de chaque cas: «Chez Swisscom, nous repérons et bloquons un nombre considérable d'attaques chaque mois. Chacune nous aide à améliorer les solutions car nous affinons nos réponses», ajoute Duilio Hochstrasser.

Recourir à des professionnels

Mais une fois dans le système, encore faut-il accéder aux données et être en mesure de les pirater et de les utiliser. Là encore, les entreprises disposent de solutions de plus en plus variées pour faire face. Mais comment faire le tri entre toutes les possibilités techniques? «Chaque entreprise doit évaluer à quel type de risque elle est exposée (surface d'exposition). En fonction de la nature de l'activité et de la valeur de ses données, on va mettre en place un plan de continuité de l'activité afin d'améliorer la résilience informatique de l'entreprise», conseille Stéphane Koch.



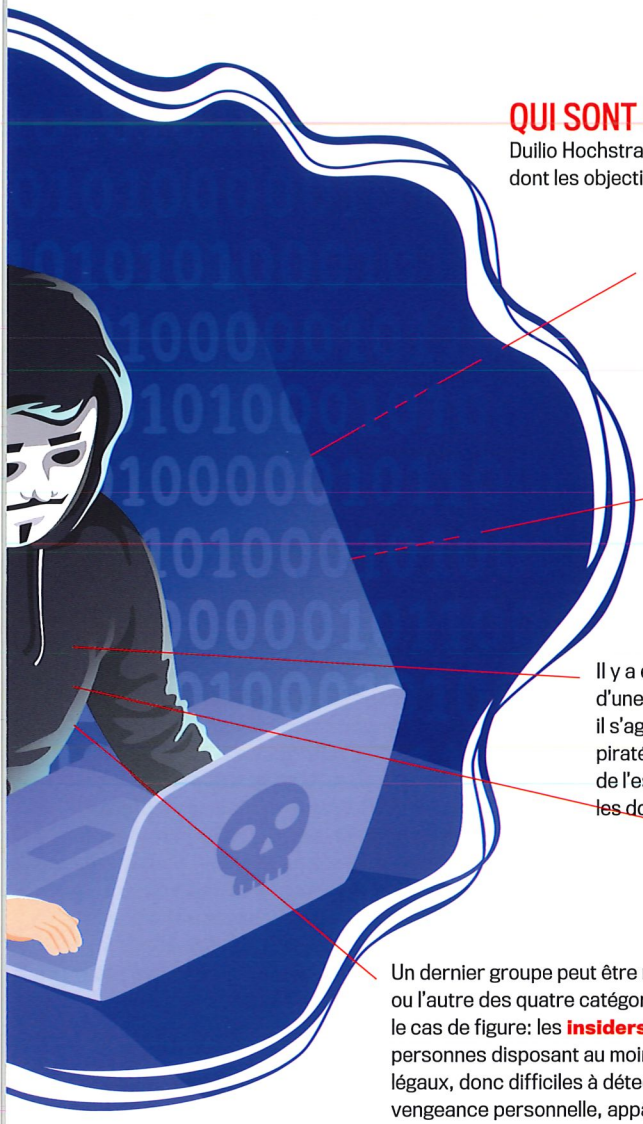
«Je me souviens de ce slogan d'un constructeur automobile français: «Qui mieux que Renault peut entretenir votre Renault.» Je dis «qui mieux qu'un pro du cloud peut sécuriser un service cloud?» Pour les objets connectés, la sécurité est la variable d'ajustement. Là où on devrait arriver, c'est un label de qualité qui atteste que tout a été fait dès le départ. Que l'industrie se l'impose à elle-même ou que les lois y obligent, on va y arriver au plus tard d'ici à une dizaine d'années au maximum», estime Steven Meyer.

«Quand on est un fournisseur de services, on va dire que le client va prendre toutes les solutions chez soi et que ces solutions vont dialoguer entre elles et être plus efficaces. Dans la réalité, tout est mouvant: il est impossible d'utiliser une même technologie. Il faut une capacité à agréger les informations de différents systèmes, corréler les informations et adapter les réponses», renchérit Duilio Hochstrasser.

LE SECTEUR DE LA FINANCE EST LE PLUS TOUCHÉ

PART DES CYBERATTAQUES SUR UN AN (10.2016 À 09.2017), SELON UNE ÉTUDE DE MANDIANT

Secteurs	Europe, Afrique et Moyen-Orient	Amériques	Asie Pacifique	Monde
Finance	24%	17%	39%	20%
Organismes gouvernementaux	18%	6%	7%	8%
Services commerciaux et professionnels	12%	18%	10%	16%
Energie	7%	5%	2%	5%
High-tech	7%	9%	10%	8%
Divertissement et médias	5%	11%	7%	10%
Commerce et tourisme	4%	10%	2%	8%
Santé	2%	12%	2%	9%
Autres	22%	12%	20%	15%



QUI SONT LES HACKERS?

Duilio Hochstrasser, de Swisscom, distingue plusieurs catégories d'auteurs de cyberattaques dont les objectifs, les moyens et les motivations sont sensiblement différents.

Il y a d'abord ceux qui agissent par **intérêt financier**. Il s'agit souvent d'opportunistes, qui ne ciblent pas une branche ou une entreprise en particulier, mais repèrent les plus faibles et s'y attaquent car ils voient un profit plus facile en regard des efforts et du temps qu'ils passent à pirater les systèmes.

Autre cas de figure: le **sabotage** dirigé par des organisations étatiques ou para-étatiques, dont l'objectif est de fragiliser, voire de paralyser, un secteur ou une entreprise spécifique qui nuit à leurs intérêts. Les auteurs d'attaques issues d'organisations étatiques sont très difficiles à bloquer car ils disposent souvent de moyens très importants.

Il y a encore l'**espionnage**, qu'il soit étatique ou pour le compte d'une entreprise concurrente. Ici encore, l'ambition est différente: il s'agit de collecter un maximum d'informations sur l'entreprise piratée. On observe cependant une spécialisation croissante de l'espionnage, car certaines cellules vont chercher à revendre les données collectées à des entreprises concurrentes ou à des Etats.

Les **activistes** politiques ou idéologiques sont eux le plus souvent désintéressés sur le plan financier, mais ils entendent perturber une activité ou une entreprise avec des messages de propagande. Ils ont moins de moyens pour mener leurs actions mais sont animés par des convictions et cela les rend au moins aussi puissants dans leur pouvoir de nuisance.

Un dernier groupe peut être rattaché à l'une ou l'autre des quatre catégories ci-dessus, selon le cas de figure: les **insiders**. Collaborateurs ou personnes disposant au moins d'accès privilégiés légaux, donc difficiles à détecter, ils agissent par vengeance personnelle, appât du gain ou convictions qui ont évolué.

D'où l'intérêt pour une entreprise d'externaliser ces missions pour les confier à des spécialistes. «Dans une PME, le responsable cybersécurité est parfois chargé à d'autres tâches liées à l'informatique. Mais un responsable informatique a-t-il le temps de faire sécuriser les systèmes? Et a-t-il les compétences suffisantes pour le faire correctement? Le plus grand problème quand une entreprise veut fonctionner en interne, c'est que les gens n'ont pas le temps de se former, de s'informer, et de corriger», regrette Steven Meyer.

A contrario, en confiant sa cybersécurité à des spécialistes externes, l'entreprise bénéficie des services de professionnels dévolus, mais aussi des retours d'expérience d'autres sociétés. «Nous travaillons sur la notion de trade intelligence: il s'agit, face aux menaces, d'acquérir le plus rapidement des savoirs sur les vecteurs, les solutions. Nous surveillons les nouvelles menaces, communiquons, et ceux qui en ont besoin adaptent leurs systèmes. Nous surveillons notamment le darknet pour savoir ce qui se prépare. A court terme, ce qui est très intéressant pour les clients, c'est que, si l'un des clients est attaqué par une forme inconnue, tous les autres clients servis par ce provider vont apprendre de cette expérience. Chacun profite de l'expérience des autres», argumente Duilio Hochstrasser. Sans compter qu'un provider pourra mettre en place une veille 24 heures sur 24 et 7 jours sur sept par des spécialistes, ce qui n'est pas forcément évident au sein d'une entreprise.

Et la police?

Quid de l'apport des autorités au combat pour la cybersécurité? Dans ce domaine, Berne reste en retard. «En Suisse, il manque des données statistiques. On veut que notre pays soit le coffre-fort numérique du monde. Mais on n'a pas de données statistiques fiables sur la cybercriminalité. Ni de réelle collaboration entre le secteur public, privé, et l'Etat. C'est important car ces données sont liées à l'économie. Si on réalise qu'on a 1 milliard de francs qui disparaît, qu'on ne peut pas investir dans l'économie helvétique, c'est important. C'est un indicateur crucial aussi pour des entreprises qui souhaitent s'implanter en Suisse», dénonce Stéphane Koch.

> «Le plus grand problème quand on fonctionne en interne, c'est que les gens n'ont pas le temps de se former»

L'expert dénonce le fait qu'il n'y ait «pas assez de ressources au niveau policier pour traiter les risques auxquels on est exposé. Les brigades de cybercriminalité des cantons viennent en support de la police judiciaire, à part à Zurich où elles suivent les affaires de A à Z. Et pas assez de juges formés à ces technologies non plus.» **B**

PHOTOS: HUC. FRREPIK

«Les criminels ont toujours une longueur d'avance»

Même s'il reste très prudent, l'Etat de Vaud est à la pointe en matière de lutte contre la cybercriminalité. Interview de Nuria Gorrite, présidente du Conseil d'Etat vaudois. PAR CHANTAL DE SENGER

Le canton de Vaud a-t-il déjà été victime d'attaques informatiques? Si oui, de quel ordre?
Nous en avons régulièrement, comme tous les Etats, mais ce sont principalement des attaques de phishing. Nous en comptons environ 400 par jour. Nous ne connaissons pas spécifiquement le profil des pirates car beaucoup ne sont pas domiciliés à l'endroit d'où est partie l'attaque. Nous savons juste que beaucoup proviennent de Russie et de Chine. Et qu'ils cherchent avant tout la soustraction financière.

Quel est le plus grand risque aujourd'hui pour l'Etat de Vaud?
Le premier risque est le vol de données. Cela veut dire que les pirates ont pénétré votre système et peuvent altérer vos données. Et il y a aussi bien sûr le risque financier avec des demandes de rançon ou des escroqueries.

Quelle est la stratégie du canton en matière de cybersécurité? Faites-vous des formations internes pour vos collaborateurs?
Nous offrons des modules de formation d'e-learning pour tous les collaborateurs de l'Etat. On a aussi réduit les accès d'administrateurs. Nous interdisons aussi aux collaborateurs de se «loguer» sur leurs e-mails privés depuis des postes de travail de l'Etat car c'est souvent par là qu'entrent les attaques.

Quels sont les moyens alloués pour lutter contre les attaques informatiques?
Nous avons demandé un premier crédit au Grand Conseil de 8,5 millions de francs pour sécuriser l'architecture des systèmes d'information de l'Etat de Vaud (DSI) et créer le Centre opérationnel de sécurité (SOC). J'ai sollicité récemment une deuxième demande de crédit pour renforcer encore le niveau de sécurité. Je rappelle qu'à mon arrivée au gouvernement en 2012, aucun budget n'était alloué pour lutter contre la cybercriminalité.

«Nous interdisons aux collaborateurs de se «loguer» sur leurs e-mails privés depuis des postes de travail de l'Etat»

Nuria Gorrite: «Nous comptons environ 400 attaques par jour.»

Que fait concrètement ce SOC?
Il s'agit d'un observatoire doté de 25 collaborateurs qui analyse en permanence toutes les attaques. Ce centre a été ouvert en 2014 avec la collaboration d'un partenaire. Le canton de Vaud se positionne depuis longtemps comme pionnier de la lutte contre la cybercriminalité, mais nous devons rester très prudents car les criminels ont toujours une longueur d'avance. Nous avons cependant la chance d'avoir des entreprises innovantes et des universités telles que l'EPFL qui font que nous avons un biotope adéquat pour améliorer notre sécurité.

Est-ce qu'il ne faudrait pas mener une lutte au niveau fédéral, centraliser la cyberdéfense?
Il y a le programme national de cybersécurité Melani avec qui nous avons collaboré dès le départ. Nous travaillons aussi avec des entreprises et le monde académique (UNIL et EPFL) avec qui nous développons «une intelligence collective». Nous avons aussi lancé le hastag «Ensembleplusforts» en collaboration avec Innovaud, la police cantonale et le service de la Promotion économique pour mettre toutes nos compétences en commun.

Est-ce que le gouvernement et le canton de Vaud développent la technologie blockchain qui se veut infaillible, notamment au niveau des attaques malveillantes?
Nous ne sommes pas à la pointe au niveau de la blockchain. Pour l'heure, nous ne sommes ni partisans ni adversaires de cette technologie. Elle peut sûrement amener plus de sécurité mais elle comporte aussi deux problèmes majeurs: déléguer les compétences de l'Etat est risqué et aussi la blockchain est très gourmande en énergie, ce qui n'est pas rationnel à l'heure des économies d'énergie. Pour nous, la blockchain n'est pas une solution à tous les problèmes. Il faut aussi rappeler que la blockchain sert aujourd'hui le bitcoin qui est la monnaie des criminels. En effet, les demandes de «rançon» sur internet sont toujours en bitcoin. ■

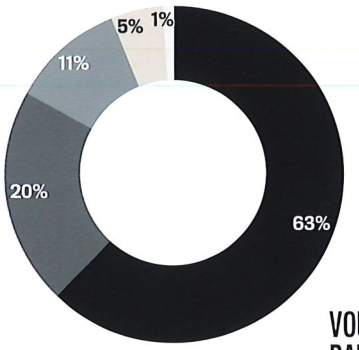
PHOTO: FLORIAN CELLA

Une entreprise vaudoise sur deux se sent vulnérable

En juin dernier, la Chambre vaudoise du commerce et de l'industrie (CVCI) a sondé ses membres sur la cybersécurité. **PAR MATTHIEU HOFFSTETTER**

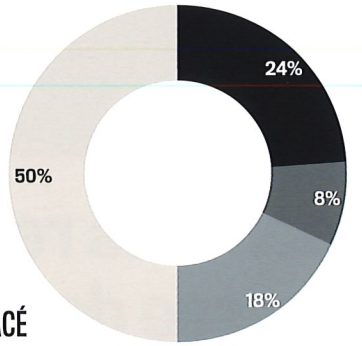
VOTRE ENTREPRISE A-T-ELLE DÉJÀ ÉTÉ VICTIME DE CYBERATTAQUES?

QUATRE SUR DIX ONT DÉJÀ ÉTÉ TOUCHÉES



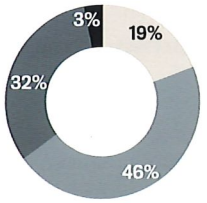
DES FORMATIONS SPÉCIFIQUES ONT-ELLES ÉTÉ MISES EN PLACE?

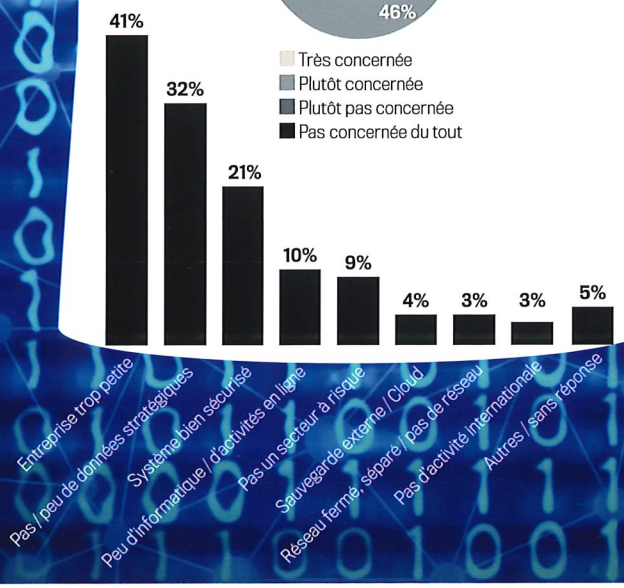
PEU DE COLLABORATEURS SONT FORMÉS



VOUS SENTEZ-VOUS MENACÉ PAR LES CYBERRISQUES?

CI-DESSOUS: LES EXPLICATIONS DE CELLES PEU OU PAS CONCERNÉES





Interviews réalisées par MIS Trend auprès des 2734 membres de la CVCI. 490 entreprises ont répondu.

* Les attaques sont classées selon leut but: fraude financière, sabotage, rançonnage, à des fins crapuleuses, espionnage ou volonté de déstabilisation.

Philippe Vuilleumier: «Pour rester à la pointe, nous organisons régulièrement des formations».

Swisscom: les recettes d'un géant suisse des données

Chargé de la sécurité au sein du groupe helvétique de télécommunications, Philippe Vuilleumier décrit la stratégie et les moyens déployés par son unité. PAR MATTHIEU HOFFSTETTER

A l'échelle suisse, Swisscom est sans doute l'une des entreprises qui génèrent et gèrent le plus de données clients. Comment celles-ci sont-elles sécurisées, alors même que l'accès des consommateurs aux données devient la règle? Entretien avec Philippe Vuilleumier, «head of group security».

Quelle est la stratégie globale de Swisscom en matière de sécurité et quels sont vos moyens pour la déployer?
La stratégie sécuritaire s'inscrit dans la stratégie d'entreprise et nous sert à soutenir les objectifs du groupe. A cette fin, nous avons groupé nos activités en quatre champs d'action: la prévention, la détection, l'intervention et, finalement, les bases ou la fondation. Ces différents domaines occupent environ 60 collaboratrices et collaborateurs. Nous définissons les standards sécuritaires et procédons à leur mise en œuvre sur la base d'un consulting interne assuré par nos soins. En parallèle, nous en assurons la promotion et donnons des formations. Pour terminer, nous vérifions régulièrement l'efficacité des mesures mises en place. Une unité de détection et réaction aux incidents sécuritaires (CSIRT) complète cet éventail. Nous avons créé le rôle de «security officer» pour soutenir au mieux les quatre grandes unités (Business Units) de Swisscom. Ces collègues font office de conseillers pour les responsables de ces grandes unités. Forts d'une longue expertise et d'un solide savoir-faire dans le domaine, au bénéfice de formations spécifiques, ils sont également dotés de personnalités leur permettant de s'opposer à des décisions susceptibles de mettre en péril les données ou la sécurité. Ce qui peut évidemment engendrer des tensions. Aussi avons-nous décidé, il y a quatre ans, de rattacher mon organisation – Group Security – directement au CEO. Cela montre une fois encore à quel point Swisscom prend la sécurité au sérieux.

«En 2017, nous avons créé un poste qui gère la gouvernance des données et l'adaptation aux législations»

Comment vos collaborateurs se tiennent-ils à jour face à ces menaces?
Le défi est en effet de taille. Dans le domaine de la cybersécurité, la vitesse à laquelle de nouvelles menaces, technologies ou autres défis apparaissent est phénoménale. Pour rester à la pointe, nous organisons régulièrement des formations et maintenons nos contacts avec d'autres unités chargées de la sécurité en Suisse et à l'étranger. Notre domaine regorge de passionnés qui aiment se tenir à jour et partager leur savoir. Mon équipe de management a ainsi pour rôle de promouvoir et de faciliter ces échanges. Pour sensibiliser d'autres experts (programmeurs, développeurs) chez Swisscom, nous avons mis en place des formations spécifiques, assorties d'un système de certification.

Que vont changer les nouvelles législations sur les données?
Depuis plusieurs années, un comité interdisciplinaire traite la question des données de façon éthique: utilisation, risques, attentes du grand public. Nous nous sommes fixé certaines restrictions quant à leur utilisation, par exemple le fait de ne pas les revendre. S'agissant du GDPR, nous sommes directement touchés car nous avons des entités en Italie et en Allemagne, mais aussi des clients qui viennent de l'UE. En 2017, nous avons engagé un processus de renforcement en embauchant un «data governance officer», qui gère la gouvernance des données ainsi que les aspects relatifs à l'adaptation à la législation européenne et la future loi suisse. Nous sommes pleinement conscients de l'importance du sujet.

La Suisse est-elle à la hauteur des enjeux?
Nous échangeons régulièrement nos idées avec les acteurs responsables en Suisse, dans le but de faire avancer la NCS (stratégie nationale de cybersécurité). Nous espérons en voir les premiers résultats concrets l'année prochaine. La Suisse doit toutefois encore faire des efforts pour mieux faire face aux cybermenaces. B

PHOTO: SWISSCOM

Quand la cybersécurité inspire des startups romandes très innovantes

Elles sont des dizaines à développer des solutions pour sécuriser le stockage ou l'accès aux données numériques. Coup de projecteur sur quatre d'entre elles, particulièrement ingénieuses.

ONEVISAGE: S'AUTHENTIFIER, BILLE EN TÊTE

PAR JOAN PLANCADE

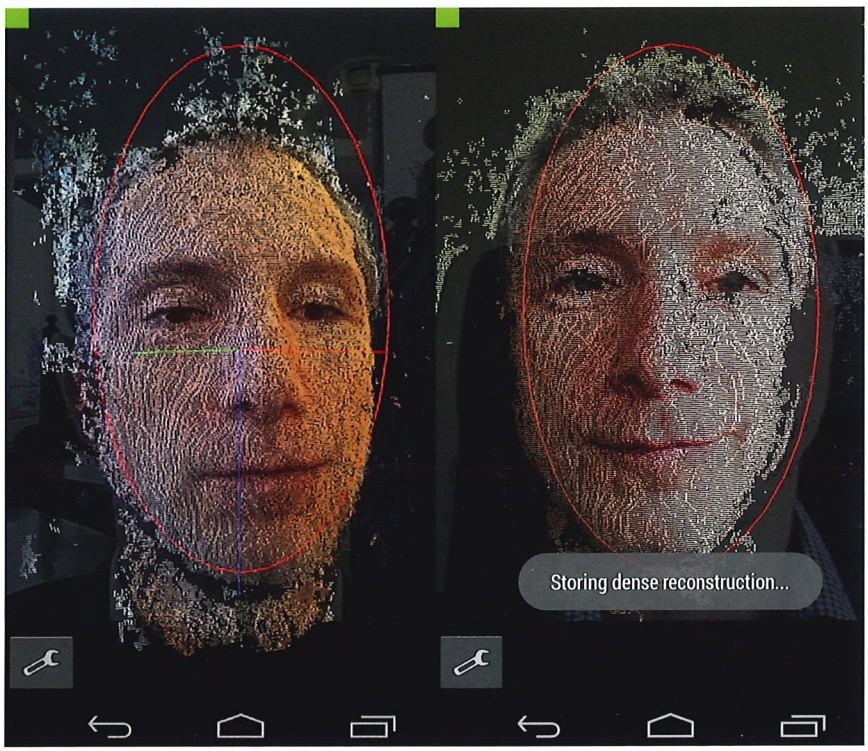
Pour Christophe Remillet, fondateur de OneVisage à Lausanne, l'histoire commence en 2013 après s'être fait hacker successivement sa carte bancaire et sa boîte mail. «J'ai compris que LA solution d'identification sécurisée était la reconnaissance faciale en 3D», encore inexistante alors.

Il s'est donc rapproché de l'ETH de Zurich et de l'Université de Bâle, «les plus avancées sur la question» pour développer une technologie permettant, via un smartphone, de recréer un visage en 3D, par un selfie vidéo où l'utilisateur tourne la tête à gauche, puis à droite, offrant une authentification avec une probabilité très élevée.

Lancé au printemps 2018, le produit a trouvé son premier client aux Etats-Unis, une société de management d'identité. OneVisage mène en parallèle une quinzaine de projets pilotes. Parmi eux, les grands intégrateurs, «type Temenos», qui proposent des services informatiques à l'industrie bancaire: «En intégrant notre solution à leurs produits, ils nous permettront de toucher très rapidement de nombreuses banques et des millions d'utilisateurs potentiels.»

Loin d'une concurrence, Christophe Remillet voit en la reconnaissance faciale de l'iPhone X une validation de son choix: «Cette technologie nécessite une caméra 3D, qui se retrouve dans le prix, alors que notre technologie est universelle, puisque fonctionnant avec n'importe quel smartphone. De plus, elle est contrôlée par l'entreprise et adaptée, par exemple, aux transactions sensibles comme des virements bancaires importants. Mais on remercie Apple pour le coup de projecteur.» B

Christophe Remillet a fondé OneVisage en 2013 à Lausanne.



Sa technologie recrée un visage en 3D via un selfie vidéo sur un smartphone.

PHOTOS: DR

CYBERHAVEN: LE TRAQUEUR DE DONNÉES

PAR JOAN PLANCADE

Quelles sont les données sensibles de l'entreprise? Où vont-elles? Qui y a accès? C'est pour répondre à ces questions que le spin-off de l'EPFL Cyberhaven, lancé en 2014, propose une solution qui trace de manière automatique les flux de données dans l'entreprise, et depuis l'entreprise vers l'extérieur. Elle effectue une analyse multisystèmes, incluant serveurs, cloud, Google Drive, mais aussi Office 365 pour les mails, puis génère une cartographie des flux. Active aux Etats-Unis via son bureau de Boston, la startup est notamment approuvée par Walmart et travaille également en Suisse auprès de banques privées.

Cristian Zamfir, cofondateur du spin-off de l'EPFL, lancé en 2014.

Cyberhaven est active aux Etats-Unis via son bureau de Boston.

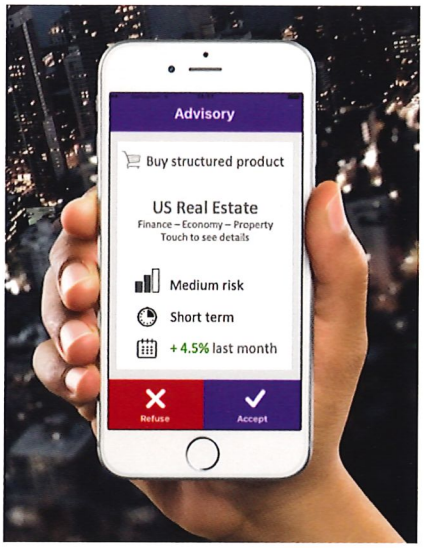
«Les entreprises se rendent compte qu'elles ne peuvent pas stopper toutes les attaques, relève Cristian Zamfir, cofondateur. Les données sont souvent la principale ressource, mais aussi le plus gros risque financier, réputationnel et légal. Le problème, c'est qu'aujourd'hui, beaucoup ne savent toujours pas quelles sont leurs données sensibles, ni par où elles transitent.»

SYSMOSOFT: SIGNER UN CONTRAT SUR SMARTPHONE

PAR JOAN PLANCADE

Renouveler une hypothèque, accepter une proposition d'investissement d'un gestionnaire de fortune ou recevoir des informations bancaires sensibles en utilisant son smartphone comme point de contact sécurisé sont autant d'applications possibles de la signature digitale gérée par la société Sysmosoft. Pour Frédéric Mauger, cofondateur de la société d'ingénierie basée à Yverdon (VD), le bénéfice est directement mesurable: «On gagne du temps et de l'argent. Plus besoin d'imprimer et d'envoyer une enveloppe timbrée, la transaction est instantanée. Depuis 2016, la signature électronique est régulée par l'UE et la Suisse et constitue un faisceau de preuves en cas de litige.»

Parmi la trentaine de clients de Sysmosoft, on trouve essentiellement des banques, notamment cantonales et privées, qui peuvent proposer le service à leurs clients pour les transactions sensibles. L'entreprise est actuellement en discussion avec des sociétés de travail temporaire pour faire signer électroniquement les contrats de travail de leurs collaborateurs à distance. ■



La signature digitale de Sysmosoft intéresse particulièrement les banques.

Frédéric Mauger, cofondateur de la société d'ingénierie basée à Yverdon.

PHOTOS: DR

Tel cette salle des serveurs, le produit développé par la startup romande stocke les cryptomonnaies de manière sécurisée.

METACO: LE COFFRE-FORT DES CRYPTOMONNAIES

PAR MARJORIE THÉRY

Créée en 2014, la startup romande Metaco s'est spécialisée dans les technologies blockchain et des actifs digitaux. Elle a notamment développé un coffre-fort numérique pour les cryptomonnaies et cryptoactifs, à destination du secteur financier. Objectif: les stocker de manière sécurisée. Metaco a fait partie de la sélection Bilan des 50 startups dans lesquelles investir.

Présenté en janvier 2018, son produit phare SILO a été développé en collaboration avec la société Guardtime, reconnue pour ses solutions de sécurité informatique au niveau des entreprises comme des gouvernements, et même certains projets liés à la défense.

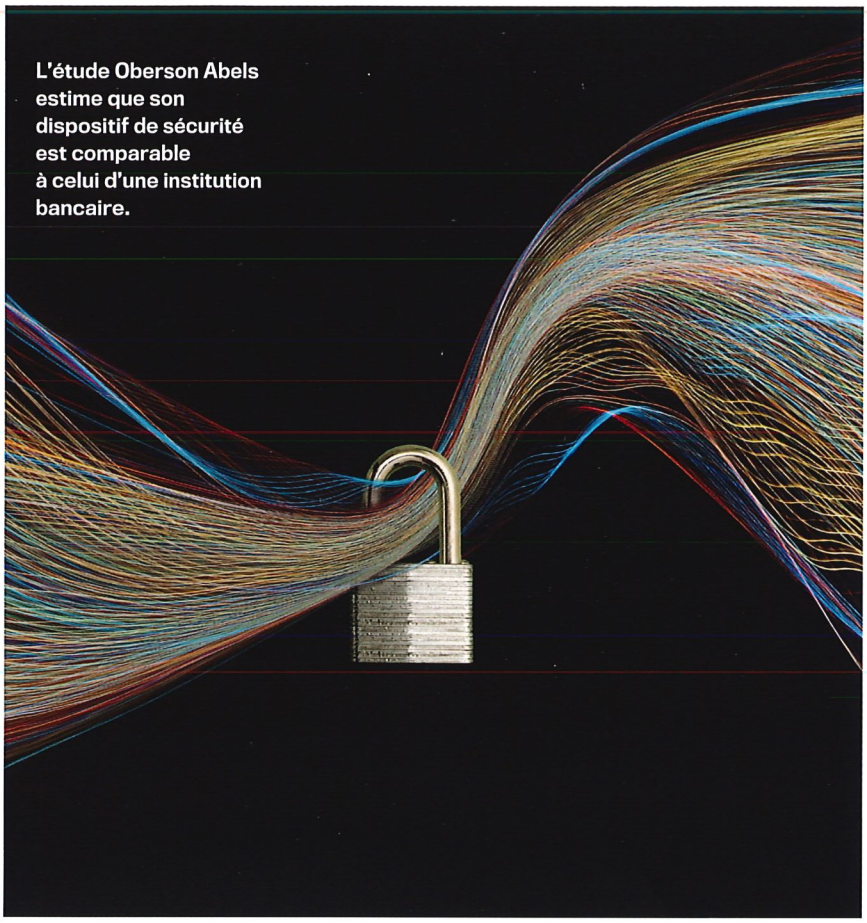
Pour Adrien Treccani, CEO et fondateur de l'entreprise: «Les systèmes IT actuels ne permettent pas de stocker les cryptomonnaies de façon suffisamment sécurisée, car on est responsable du stockage de toutes les clés de cryptage. Cela demande une expertise particulière et les banques ne veulent pas forcément prendre le risque de faire confiance à des plateformes externes pour cela. C'est là où nous apportons une vraie valeur ajoutée.»

Adrien Treccani, CEO et fondateur de Metaco, créée en 2014.

Après une première levée de fonds d'amorçage en 2016, Metaco a réalisé une nouvelle opération au printemps pour financer sa croissance. Parmi les investisseurs, tous sont des entreprises en lien avec la sécurité et/ou le secteur bancaire, qu'il s'agisse de Swisscom, La Poste, Avaloq ou encore Sicpa. Pour Adrien Treccani, ces nouveaux investisseurs sont aussi des partenaires commerciaux. «L'idée est de travailler ensemble, en collaboration, pour que ces entreprises puissent développer de nouveaux services grâce à nos outils.» Lors de l'annonce de ces partenariats, Johannes Höhener, head of Swisscom FinTech, avait d'ailleurs déclaré: «Nous sommes convaincus par la solution et les équipes de Metaco, et notre objectif est d'intégrer cette solution de custody des cryptoactifs de premier ordre dans notre offre de services liés à la blockchain.»

Adrien Treccani est confiant pour la suite. «Nous avons d'excellents partenaires et la demande du marché pour stocker de manière sécurisée les cryptomonnaies et cryptoactifs se développe de plus en plus.» B

PHOTOS: SHUTTERSTOCK, SÉBASTIEN ANEX



L'étude Oberson Abels estime que son dispositif de sécurité est comparable à celui d'une institution bancaire.

Les données, un enjeu clé pour les études d'avocats

Le cabinet Oberson Abels externalise sa sécurité informatique pour s'assurer qu'elle soit en pointe et professionnelle. Témoignage. PAR MYRET ZAKI

Pour une étude d'avocats, l'enjeu de la sécurité informatique n'est pas à prouver. Risque de réputation, risque de fuite de données de clients… les défis sont importants alors que le secret professionnel de l'avocat est plus absolu que le secret bancaire. Cela fait plusieurs années qu'Olivier Mermoud travaille pour l'étude d'avocats Oberson Abels, où il est actuellement chief technical officer (CTO).

«On a vu ces dernières années que la sécurité était très importante dans notre activité, tout comme elle devenait un thème majeur pour nombre de secteurs, constate-t-il. Le public en général devient de plus en plus sensible à ces problèmes, ce qui s'explique aussi par l'importance croissante des risques informatiques. Dès lors, les entreprises ne peuvent plus se contenter de services de base», note l'expert.

Il y a quelques années, la sécurité informatique pouvait se résumer à un firewall et un antivirus. Cette période est révolue, souligne Olivier Mermoud. «L'évolution des technologies et les compétences très poussées que l'on trouve dans d'autres pays nous forcent à nous adapter aux nouvelles menaces.» Seul problème, observe-t-il, les budgets informatiques n'ont souvent pas augmenté, tandis que les coûts, eux, prennent l'ascenseur. Dès lors, une bonne partie des budgets classiques est en train d'être absorbée par la sécurité. Le degré de spécialisation s'est accru. «Dans les PME, on pouvait partir du principe que l'entreprise pouvait gérer tous les aspects liés au client, infrastructure, support et sécurité. Aujourd'hui, on est obligé de déléguer une certaine partie du travail à des gens qui ont les compétences et ont suivi une formation dédiée.»

C'est pourquoi Oberson Abels a délégué ses services de sécurité à Swisscom, dans le respect du secret professionnel. Le firewall et la solution de filtrage web d'abord, puis le support 24 heures sur 24 et 7 jours sur 7 («24/7»), et à présent une grande partie de tout ce qui relève de la sécurité. «Comme ils gèrent le réseau national, ce sont les premiers informés quand il se passe quelque chose d'anormal.»

La sécurité est un domaine en constante évolution, ajoute-t-il: une solution ne sera pas bonne pour deux ou cinq ans. «Cela fait sens de passer par des systèmes ou des équipements fournis par un prestataire externe qui s'occupe des mises à jour et qui suit les menaces qui émergent et concernent la Suisse en particulier.» L'étude procède par des contrats d'abonnement qui confient à l'opérateur national la gestion quotidienne, en plus des améliorations. Elle a d'ailleurs été un client pilote pour certaines offres de Swisscom.

Des outils d'analyse

Aujourd'hui, l'étude Oberson Abels estime que son dispositif de sécurité est, dans une large mesure, comparable à celui d'une institution bancaire. «On s'inspire des recommandations de la Finma, même si nous ne sommes pas tenus de le faire par la loi. Il s'agit de montrer aux clients que leurs données sont importantes chez nous et que nous faisons le nécessaire pour les protéger.»

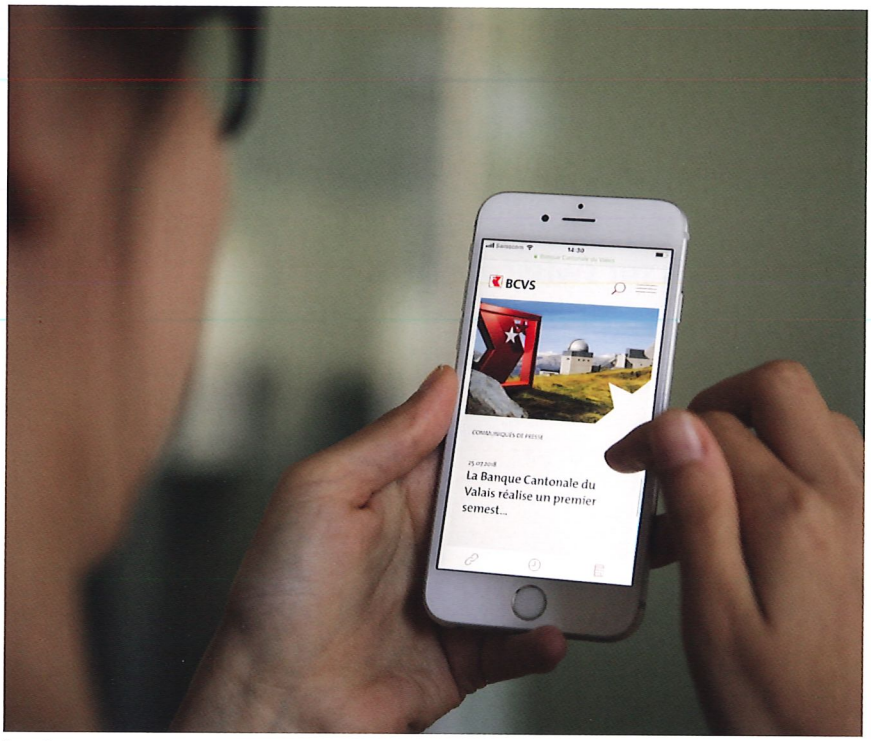
Cette protection passe par le cryptage, la séparation des données et la protection périmétrique, que ce soit par des firewalls, des antivirus ou des moyens plus «next gen» tels que des outils d'analyse qui peuvent détecter des comportements anormaux (tels qu'un volume de données en train de circuler à un endroit où il ne devrait pas) et déclencher des alertes. B

«On s'inspire des recommandations de la Finma, même si nous ne sommes pas tenus de le faire par la loi»
OLIVIER MERMOUD

PHOTO: JOHN LUND/GETTY IMAGES, DR

Les banques, cibles de choix pour les pirates

Claude-Alain Courtine, responsable sécurité informatique à la Banque Cantonale du Valais, multiplie les précautions pour se protéger contre tout incident majeur. **PAR MATTHIEU HOFFSTETTER**



Les banques suisses doivent répondre à des contraintes réglementaires drastiques.

Peu de secteurs en Suisse sont davantage visés par les cyberattaques que les banques. Sont surtout concernés certains grands établissements financiers suisses d'envergure mondiale ou des banques privées dont des clients peuvent susciter un intérêt, mais les banques cantonales ne sont pas épargnées.

A la Banque Cantonale du Valais (BCVs), Claude-Alain Courtine est responsable de la sécurité informatique. S'il se réjouit que son établissement «ait pu déjouer toutes les attaques à ce jour», il évoque «quelques tentatives sur les solutions e-banking». Pour se prémunir contre des attaques plus virulentes à l'avenir, il fait le maximum «pour limiter la surface d'attaque et bloquer les scans de l'extérieur».

Prendre les dangers le plus en amont possible peut se révéler salutaire. Claude-Alain Courtine cite ainsi le cas d'«un client appelé par une personne se faisant passer pour un employé de hotline. Il a eu un doute, puis a eu la présence d'esprit de nous contacter: nous l'avons aidé à mettre à jour son ordinateur et ses systèmes de sécurité.»

> «Faire appel à des prestataires spécialisés nous assure d'avoir des compétences à jour»

L'arrivée du Règlement général sur la protection des données (RGPD) a été planifiée de longue date par la BCVs: «Nous travaillons à toujours être en conformité avec les nouvelles exigences légales. Mais comme nous sommes dans un secteur extrêmement sécurisé, nous n'allons pas avoir trop de difficultés pour nous adapter.» L'univers bancaire, régenté par la Finma, ne peut se permettre d'écart: obligation de communiquer définie en cas d'attaque, données bancaires hébergées uniquement en Suisse dans des centres de données consacrés à ce type de contenus, focus sur les potentiels piratages de données en interne (norme Finma 2008-21)... les contraintes sont drastiques.

Claude-Alain Courtine: la BCVs a «pu déjouer toutes les attaques à ce jour».

Mais ces obligations réglementaires n'exonèrent pas la banque valaisanne de multiplier les précautions: «Nous faisons appel à beaucoup de spécialistes pour être au fait des dernières tendances. Car nous n'avons pas la taille critique pour tout faire en interne. Nous faisons aussi challenger les partenaires par d'autres partenaires pour vérifier leur fiabilité. Par exemple, si un réseau sécurisé est développé par un tiers, nous le soumettons à des tests de pénétration. Faire appel à des prestataires spécialisés nous assure d'avoir des compétences à jour; et nous bénéficions des retours d'information et d'expérience.»

L'importance des Security Analytics

Le principal axe de travail actuellement? «Pendant plusieurs années, nous avons beaucoup travaillé sur la protection. Aujourd'hui, nous sommes davantage focalisés sur la détection. Comme le risque zéro n'existe pas, nous travaillons à pouvoir toujours répondre à un potentiel incident. Pour la détection, un des axes majeurs réside dans les Security Analytics pour corréler tous les systèmes afin de détecter une potentielle activité. Autre point crucial: les cellules de crise; nous travaillons sur la continuité d'activité en cas d'incident, aussi bien en matière de cybersécurité que de catastrophe naturelle, par exemple», détaille Claude-Alain Courtine. B

PHOTO: DAVID HUC, LINDAPHOTO.CH/BCVS

Les cyberattaques peuvent se présenter sous de multiples facettes.

Les méthodes d'attaque sont de plus en plus élaborées et la protection contre les menaces devient de plus en plus complexe. Équipez votre entreprise pour l'avenir numérique – avec notre cybersécurité, optimisée pour la Suisse.

Davantage d'informations sur swisscom.ch/security

swisscom