CYBER LE POINT FORT ANALYSE
Publié le 08 févr er 2023 17 00. Mod fié le 09 février 2023 18 08

L'Etat se défend contre les hackers, mais qui défend la population?

par Grégoire Barbey

En Suisse, c'est surtout le privé qui s'organise pour renforcer la sécurité informatique des particuliers et des entreprises. La création du nouvel office dédié à la cybersécurité pourrait permettre à la Confédération d'en faire davantage.

Cet article a été publié dans notre newsletter du soir, Le Point fort. N'hésitez pas à vous inscrire, c'est gratuit.

L'armée suisse se défend contre les cyberattaques, et a même l'intention de demander des moyens supplémentaires, comme l'a révélé la *RTS*. De même, l'administration fédérale peut compter sur le Centre national pour la cybersécurité en cas de problème. Mais qui protège les particuliers et le secteur privé?

Pourquoi la question se pose. La Suisse est une cible privilégiée: les cyberattaques auraient augmenté de 61% en 2022, contre 26% en moyenne en Europe, selon les données de *Checkpoint* En première ligne: les petites et moyennes entreprises, qui n'ont bien souvent pas les ressources pour se protéger efficacement.

La Confédération semble avoir conscience des enjeux, puisqu'elle compte transformer son centre national en véritable office fédéral à la cybersécurité en 2023. En attendant, certains acteurs s'inquiètent du manque de soutien effectif au secteur privé. Faut-il que l'Etat se montre plus volontaire?

La conseillère aux Etats fribourgeoise Johanna Gapany (PLR) avait déposé une motion en septembre 2021 demandant que le Conseil fédéral étende la protection fédérale en matière de cybersécurité aux cantons, communes et PME.

Si elle a retiré son texte en attendant de voir ce que la Confédération va mettre en œuvre avec son nouvel office dédié à la cybersécurité, elle estime légitime de s'interroger sur la responsabilité de l'Etat. Et ajoute:

> «J'attends en priorité de cette réorganisation une collaboration continue avec les polices cantonales qui sont au front, tout comme des efforts pour recruter les personnes les plus compétentes pour traiter les cyberattaques et en éviter autant que possible.»

Ce que l'Etat fait actuellement. La police ne fournit pas de soutien technique en cas de cyberattaque. Son rôle est de constater les faits et relever les preuves qui peuvent permettre de remonter aux auteurs du délit. «Nos clients sont souvent orientés vers nous par la police», confirme Steven Meyer, directeur de l'entreprise de cybersécurité genevoise Zendata. Selon lui, la police aimerait pouvoir faire plus, mais elle n'en a ni les moyens ni le mandat.

Sur le plan fédéral, le Centre national pour la cybersécurité, créé en 2020, joue surtout un rôle de prévention et de conseil. Des informations sont disponibles sur son site web, et un guichet en ligne permet aux entreprises et aux individus de signaler des incidents ou des vulnérabilités.

Une analyse de la situation et des recommandations sur la suite de la procédure sont proposées, mais cette démarche d'annonce est essentiellement utile à des fins statistiques – le Centre national pour la cybersécurité peut émettre des alertes s'il constate que certaines formes d'attaques se multiplient.

En principe, les autorités ne fournissent donc pas d'assistance technique aux victimes de cyberattaque. Du moins, officiellement. Dans les faits, ça dépend de la situation.

- Plusieurs sources ont confié à *Heidi.news* que de telles interventions peuvent avoir lieu si la structure qui subit une cyberattaque peut être considérée comme une «infrastructure critique» ou a «un caractère critique pour l'image de la Suisse».
- C'est aussi la stratégie d'autres pays, comme le Royaume-Uni.

Le privé s'organise. Dans ces circonstances, des initiatives privées voient le jour Certaines bénéficient d'ailleurs du soutien des autorités.

- Quelques géants de l'industrie suisse ont créé la Swiss Industry Cyber-Security Association pour favoriser entre eux l'échange confidentiel d'informations en cas de cyberattaque et se proposer comme interlocuteur crédible auprès des autorités fédérales et cantonales.
- La TrustValley, une organisation fondée par des acteurs privés et publics, a lancé l'an dernier un programme de soutien de 12 mois intitulé «Trust4SMEs» qui permet à 25 PME romandes triées sur le volet de bénéficier d'un coaching personnalisé, de formations et de sensibilisations en matière de cybersécurité. Programme qui sera reconduit en avril 2023.
- Le CyberPeace Institute, une ONG basée à Genève, s'est spécialisé dans l'accompagnement des organisations humanitaires, souvent peu préparées aux cyber-risques.

Ce que l'Etat pourrait faire de plus. Pour Lennig Pedron, directrice de la TrustValley, la création du nouvel office fédéral de la cybersécurité doit être l'occasion pour les autorités de «créer des ponts» avec la population et l'économie pour renforcer l'éducation et la sensibilisation.

De son côté, Steven Meyer (Zendata) verrait d'un bon œil la création d'un numéro vert qui permettrait aux individus et entreprises de poser leurs questions en matière de cybersécurité.

Selon Fabien Leimgruber, responsable de programmes au CyberPeace Institute, la Suisse doit surtout améliorer son action en matière de prévention et d'éducation:

> «Aujourd'hui, on parle de cyberharcèlement à l'école, mais on n'entre pas dans les questions de cyberattaques ou même d'hygiène numérique. Pourtant, une population éduquée est un élément clé pour réduire l'impact des attaques »

La vulnérabilité des PME découle en partie de celle de ses employés: plus ceux-ci sont à même d'observer de bonnes pratiques numériques, moins ils exposeront leur entreprise à des risques inconsidérés. Une bonne partie des cyberattaques repose sur de l'ingénierie sociale ou des failles de sécurité basiques, comme un mot de passe transparent ou stocké en clair

Fabien Leimgruber met aussi en garde contre une communication trop focalisée sur les cyberattaques: cela participe selon lui à générer de la peur au sein de la population. Les bonnes pratiques doivent être utilisées au quotidien, pas seulement pour se protéger des hackers malveillants.

Le nouvel office fédéral, dont les contours doivent être présentés au printemps 2023, tiendra t-il compte de ces suggestions?