



Infrastructures

Les cyberattaques se multiplient – combattons-les ensemble

02.05.2022

D'un coup d'oeil

La cybersécurité nous concerne tous, les milieux économiques tout comme la société. Elle n'est plus, depuis longtemps, un sujet abstrait réservé à des spécialistes de l'informatique. Au contraire, elle est devenue extrêmement concrète et omniprésente. Les médias se font régulièrement l'écho de cyberattaques ciblant des entreprises et des administrations suisses. Certains parmi vous ont peut-être aussi été victimes de criminalité sur internet. Le nombre d'attaques annoncées dans les médias ne représente qu'une fraction de celles perpétrées. Car elles sont nombreuses et ne sont pas toutes connues ou identifiées. Les experts aiment à dire qu'il existe désormais deux catégories d'entreprises: celles qui ont déjà été hackées et celles qui ne le savent pas encore.

La numérisation croissante a des conséquences positives pour l'essentiel. Elle s'accompagne malheureusement aussi d'une multiplication et d'une diversification des possibilités d'attaque pour les criminels de l'espace numérique. Beaucoup d'objets sont désormais connectés et reliés à internet, que ce soit la voiture de fonction, la surveillance vidéo ou la fraiseuse. Chaque nouvel appareil que nous connectons à notre infrastructure réseau augmente le risque que des cybercriminels trouvent une faille et l'exploitent. Dans ce contexte, il est décisif que nous apprenions par quels moyens nous pouvons nous protéger efficacement. Pour cela, il faut un minimum de discipline: effectuer les mises à jour nécessaires, changer régulièrement de mot de passe et vérifier le bon fonctionnement des systèmes. Toute négligence accroît directement les possibilités d'attaque pour les cybercriminels. De nombreuses entreprises ont déjà pris des dispositions importantes à cet égard, mais ce n'est souvent pas le cas des particuliers. Ainsi, l'augmentation du télétravail a coïncidé avec une hausse considérable des attaques. Au lieu de les lancer via le réseau de l'entreprise, les auteurs ont exploité les failles de sécurité des réseaux privés des employés.

Personne n'est à l'abri d'une attaque dans le cyberspace. Plus de 200 signalements sont effectués auprès du Centre national pour la cybersécurité toutes les semaines – les experts partent du principe que les incidents non signalés sont beaucoup plus nombreux. En 2022, on déplore déjà des victimes d'importance dans l'économie et l'administration. Le ransomware est très utilisé: un nombre croissant d'entreprises suisses se voient soudain confrontées à la question de savoir si elles doivent payer pour le déverrouillage de leurs données bloquées par des logiciels malveillants.

Lorsque les victimes faciles sont nombreuses, c'est la promesse d'un butin rapide et cela encourage de nouvelles attaques. Mais qu'impliquent ces risques pour l'économie suisse et que faut-il faire? Nous sommes nombreux à avoir pris conscience du danger de cyberattaque, mais cela ne suffit pas. Il faut une analyse détaillée des risques, la volonté de se confronter aux périls et de trouver des solutions adéquates.

Cette question ne peut pas être simplement déléguée à un responsable informatique. La direction de l'entreprise comme les collaborateurs doivent être encore davantage sensibilisés aux risques, car on a beau numériser, l'être humain reste le plus grand risque sous l'angle de la sécurité. C'est là que la culture d'entreprise entre en jeu: elle doit s'emparer de cette question.

Il faut en outre disposer du savoir-faire nécessaire pour prévenir au mieux les attaques et trouver des solutions concrètes en cas de cyberattaque. Pour toutes les entreprises, pas seulement celles prises en compte dans l'étude, y compris les PME, de telles mesures représentent souvent un défi. Pourtant, la cybersécurité revêt une importance fondamentale pour leur succès voire leur survie.

En tant qu'association, nous avons à cœur de contribuer à sensibiliser tous les acteurs de l'économie et de la société aux risques dans le cyberspace. Nous devons adapter notre comportement et déployer les moyens appropriés pour nous protéger. Je tiens personnellement à y contribuer et à informer les milieux économiques suisses sur la cybersécurité. La présente étude doit contribuer à accroître la visibilité de cette question, à mettre en évidence la nécessité d'agir au sein des entreprises et à nous aider tous à renforcer notre défense par rapport aux risques inhérents à l'économie numérique.

Ce texte est la préface de l'étude «Cyber Risk Management in grösseren Schweizer Unternehmen» réalisée par la Haute école de Lucerne, en collaboration avec La Mobilière et economiesuisse.



Monika Rühl
Présidente de la direction