Raetzo Carole		
Faire face à la montée de la cybercriminalité		
Cosignataires : 0	Réception au SGC : 16.02.23	

Dépôt

La Suisse est une cible privilégiée : les cyberattaques auraient augmenté de 61 % en 2022, contre 26 % en moyenne en Europe. L'explosion des annonces de cyberattaques ces derniers mois n'est ni un hasard, ni une fatalité. Elle est principalement due à la professionnalisation des groupes de pirates informatiques ainsi qu'au perfectionnement de leurs techniques et outils, mais pas seulement. En effet, nous avons actuellement un décalage évident entre l'efficacité et la rapidité de leurs attaques et notre niveau général de préparation pour les contrer.

En première ligne : les petites et moyennes entreprises, qui n'ont, bien souvent, pas les ressources pour se protéger efficacement. Elles sont de plus en plus visées par les hackers, qui profitent du fait qu'elles ne peuvent investir autant dans leur sécurité informatique que les grands groupes.

Loin d'être à l'abri, certaines communes n'ont souvent pas le budget ni les formations nécessaires pour faire face à ces nouvelles menaces. Elles risquent de voir ces attaques se multiplier dans les années à venir, menaçant l'intégrité des données qu'elles détiennent et le bon fonctionnement de leur administration de façon générale.

La première moitié de ce mois de février démontre l'ampleur du phénomène : le serveur d'Epicentre à Romont a été victime d'une cyberattaque avec soustraction de données., l'Université de Zurich également ainsi que les Chemins de fer fédéraux CFF.

Clairement visés par les pirates depuis quelques années, les établissements de santé font également face à de multiples cybermenaces. A noter qu'une attaque réussie peut entraîner des pannes et des interruptions des systèmes tant d'information que de communication et en menacer la disponibilité, la confidentialité ainsi que l'intégrité.

La Confédération semble avoir conscience des enjeux puisqu'elle compte transformer son centre national pour la cybersécurité, le NCSC, en véritable Office fédéral à la cybersécurité en 2023. Toutefois, se défendre contre une cyberattaque requiert, à l'image des pompiers appelés en urgence, une action préparée et régulièrement exercée. Cela nécessite d'adopter des procédures d'intervention précises et rapides permettant un retour à la normale maîtrisé.

Comme nous avons appris, dès le plus jeune âge, les règles de base de la sécurité routière, il est désormais essentiel d'apprendre et de transmettre les bonnes pratiques en matière de cybersécurité.

Au vu de ce qui précède, je pose les questions suivantes au Conseil d'Etat :

1. Quelles sont les pistes envisagées par le Conseil d'Etat pour permettre aux petites communes de se prémunir contre la cybercriminalité ?
2. Une force d'intervention cantonale dépêchée en renfort pour la réponse à une cyberattaque est-elle envisagée par le Conseil d'Etat ?
3. Proposer aux collectivités une boîte à outils alimentée par les bonnes pratiques et des standards minimaux en matière de cybersécurité est-elle envisagée ?
4. Il y a eu Rolle, Montreux, Bülach, victimes de cyberpirates, mais plus largement aujourd'hui, toutes les communes sont dans le viseur., d'où la question suivante : n'est-il pas temps de mutualiser les moyens de lutte ?
5. Les établissements de santé restent des structures très connectées, avec un nombre important de postes de travail informatiques et de dispositifs biomédicaux reliés à des réseaux. Mieux vaut prévenir que guérir : audit de sécurité, schémas directeurs avec plans d'action, audit de conformité, scan de vulnérabilité, test de pénétration des équipements. Dans les réseaux de santé et les milieux hospitaliers, des audits ont-ils été entrepris afin de préserver les données patients et assurer le secret médical ? Un plan B a-t-il été établi en cas de paralysie du système informatique ?

6. Les demandes de couvertures d'assurances cyber-risque explosent et les primes prennent l'ascenseur. Des partenariats public-privé sont de plus souvent évoqués pour faire face aux dégâts causés par les cybercriminels : une partie du risque serait portée par les assureurs mais au-delà d'un certain seuil, la collectivité prendrait le relais. Quelle est la position du Conseil d'Etat sur cette thèse ?

Le Conseil d'État tient à souligner d'emblée que la prévention de la cybercriminalité est avant tout de la responsabilité des entreprises. A titre d'illustration, PromFR a organisé en 2022 des ateliers de prévention et d'évaluation de la maturité des entreprises en matière de cybersécurité à travers Platinn. Cependant, les résultats de cette initiative sont pour l'instant faiblement probants car malgré les rappels et les relances, peu d'entreprises ont participé à ce type de démarche.

Le Conseil d'État considère ainsi qu'il ne s'agit pas d'un problème de subvention, mais plutôt de prévention et de responsabilisation des entreprises. L'existence d'une garantie étatique risquerait de décourager les entreprises d'agir elles-mêmes pour se protéger des risques.

Enfin, le Conseil d'État estime que les partenariats public-privé pour faire face aux dégâts causés par la cybercriminalité pourraient être une piste à explorer, mais ceux-ci doivent actuellement être fondés sur la prévention sans subvention ou prise en charge des risques par la collectivité au-delà d'un certain seuil. Le marché des assurances doit fonctionner sans l'intervention de l'État.

—