

Les dépenses pour la sécurité augmentent, les efforts aussi

La violence des jeunes, la pollution sonore et le littering font partie de la vie quotidienne dans beaucoup de communes. Selon l'expérience de Christoph Zulauf, directeur régional à Berne et membre de la direction suisse de Securitas SA, la situation en matière de sécurité a évolué de diverses manières ces dernières années. «Dans les communes rurales, la situation est plutôt stable, tandis que les agglomérations doivent faire face à des défis considérables dans certains cas. Les autorités sont souvent confrontées à la violence des jeunes, à la consommation excessive d'alcool et aux déchets», explique Luc A. Sergy, directeur de l'Association des entreprises suisses de services de sécurité (AESS). Des chiffres concrets sur l'évolution de la situation sécuritaire dans les communes ne sont disponibles qu'en Suisse romande. Selon Luc A. Sergy, les dépenses de sécurité en 2018 seront passées de 7,8 à 21% à Bienne, par exemple, de 30,2 à 50% dans le canton de Neuchâtel et de 16,2 à 21% dans le canton de Vaud. Christoph Zulauf, de Securitas, estime de son côté qu'à l'avenir, des concepts de sécurité vont devoir être appliqués, en particulier dans les communes d'agglomération. Luc A. Sergy abonde dans le même sens – «même si la criminalité se déplace de plus en plus vers internet».

Sensibiliser à la collecte

Ne pas diminuer les efforts: cette devise s'applique également au littering. Les résultats du dernier sondage de la Communauté d'intérêts pour un monde propre (IGSU) le montrent: la sensibilisation et une infrastructure de collecte dense sont efficaces contre le littering. Pour la quatrième année consécutive, la population suisse perçoit une diminution du littering. A leur tour, de nombreuses villes et communes enregistrent une légère amélioration. Patrick Vaucher, Gestion des déchets à Vevey: «Nous intensifions la sensibilisation dans les écoles, lors des événements et dans les espaces publics. A mes yeux, le contact direct avec la population et la coopération avec les entreprises générant des déchets comme les commerces servant des repas à emporter sont les principaux facteurs de réussite.»

De nombreuses villes et communes recourent de plus en plus aux offres d'IGSU.



Les mesures telles que le Clean-Up-Day font l'objet d'un soutien étonnant de la part de la population. Ici une photo prise dans le cadre d'une action à Vevey (VD).

Photo: IGSU

Des offres qui sont d'ailleurs de plus en plus populaires. «Les mesures telles que le Clean-Up-Day font l'objet d'un soutien étonnant de la part de la population», se réjouit Nora Steimer, directrice d'IGSU. «Les gens veulent contribuer à la propreté de leur environnement et y consacrent aussi leur temps libre.» Au Clean-Up-Day 2019, plus de 650 actions place nette ont été enregistrées, avec au total quelque 40 000 participants ayant marqué leur engagement lors des journées de nettoyage en septembre. Soit environ 120 actions et 10 000 participants de plus que l'année dernière.

Les projets de parrainage de sites suscitent aussi un grand intérêt. En 2018, l'IGSU lançait le site web www.parrainagesite.ch, dont la vocation est de soutenir les organisateurs à mettre en œuvre des projets de parrainage de sites. Une initiative qui a incité plusieurs villes et communes à conduire leurs propres projets. Aujourd'hui, 23 institutions ont publié leurs projets en cours ou nouveaux sur ce site web. Jusqu'à 80 parrains ont rejoint chaque projet et à présent, ils libèrent régulièrement certaines zones de leurs déchets sur une base bénévole.

Depuis la fondation d'IGSU il y a 13 ans, les équipes d'ambassadeurs IGSU sillonnent les villes et les communes et parlent avec les passant(e)s du littering et du recyclage. En été 2019, ils sont intervenus dans plus de 50 villes et 25 écoles, réalisant un total de 16 500 heures de sensibilisation.

Contre une consigne sur les bouteilles

Fort de ce constat, l'IGSU se positionne clairement contre l'introduction d'une consigne sur les emballages de boissons: seulement 7% des objets abandonnés sur la voie publique sont des canettes et des bouteilles pouvant être rendues contre une consigne. Au moins 93% du littering resteraient par terre, à savoir tous les mégots de cigarettes, emballages de repas à emporter, journaux, dépliant, sacs, sachets de chips, pots de yaourt, couverts en plastique, etc. En plus, une consigne entraînerait la disparition forcée des points de collecte de l'aluminium, du verre et du PET dans les espaces publics. Contreproductif selon l'IGSU: plus il est confortable pour la population d'éliminer correctement ses matières recyclables et ses déchets, moins il y aura d'ordures par terre. *red*

Les cybercriminels cherchent à manipuler leurs victimes potentielles

Presque toutes les cyberattaques fonctionnent grâce à une certaine participation des victimes. Celles-ci doivent par exemple divulguer un mot de passe, cliquer sur un lien vers un site malveillant ou ouvrir un document envoyé par e-mail. Les cybercriminels essayent donc d'abord de réunir un maximum d'informations sur leurs victimes potentielles. Ces informations sont ensuite utilisées afin de leur présenter une histoire crédible avec beaucoup de détails véridiques. Le courriel envoyé paraît ainsi plus vraisemblable et augmente les chances que la victime potentielle fasse une erreur.

L'ingénierie sociale, c'est-à-dire la manipulation de victimes potentielles, peut prendre différentes formes. Souvent, les recherches sont effectuées en ligne, sans que la victime ne le remarque. Mais il est aussi possible qu'un pirate informatique découvre qu'un employé communal pratique un certain type de sport pendant ses loisirs. Il cherche alors par ce biais à entrer en contact personnel avec la victime, crée un rapport de confiance et tente ainsi d'obtenir des informations. Il y a quelques années, les cybercriminels ont découvert un nouveau «modèle d'affaires», ce qu'on appelle l'arnaque au président (CEO Fraud). Les pirates se font passer pour un dirigeant d'entreprise et prient en son nom le service financier de virer une importante somme d'argent. La première victime suisse de ce genre d'escroquerie a été une PME fribourgeoise qui a ainsi perdu 1 million de francs. Afin de se protéger contre de



Les pirates se font passer pour un dirigeant d'entreprise et prient le service financier de virer une importante somme d'argent. La première victime suisse de ce genre d'escroquerie a été une PME fribourgeoise; elle a ainsi perdu 1 million de francs.

Photo: Shutterstock

telles attaques, une signature collective devrait être exigée pour les versements. L'escroc doit alors manipuler au moins deux personnes, ce qui est nettement plus difficile. Une classification des données (par ex. avec les mentions «interne», «confidentiel» et «secret») décrit leur sensibilité et la manière de les gérer. Dans l'Administration fédérale, les données classées «confidentielles» sont uniquement transférées via des courriels

cryptés. Les données classées «secrètes» ne peuvent être transmises que par un coursier et doivent être stockées sur des appareils complètement isolés.

Max Klaus
Directeur adjoint de la Centrale
d'enregistrement et d'analyse pour la
sûreté de l'information MELANI

Infos: www.ncsc.ch

Sensibiliser au cyberrisque

En mai 2018, le Conseil fédéral a adopté la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018-2022¹. Le plan de mise en œuvre² y afférent et le plan de mise en œuvre des cantons³, qui fait partie intégrante du plan national, visent expressément, parmi les mesures prises, à renforcer la sensibilisation aux cyberrisques.

En effet, une conscience accrue des menaces dans le cyberspace peut conduire les utilisateurs de technologies de l'information et de la commu-

nication, y compris les communes, à modifier leur comportement. Ils peuvent ainsi profiter pleinement des possibilités du numérique tout en écartant les risques évitables.

Des informations complémentaires destinées aux communes seront disponibles au cours du deuxième semestre 2020. En collaboration avec différents partenaires, le réseau national de soutien aux enquêtes dans la lutte contre la criminalité informatique (NEDIK) travaille actuellement à l'élaboration d'une brochure d'information, laquelle sera distribuée en temps voulu par l'Association des communes suisses.

¹ Unité de pilotage informatique de la Confédération UPIC (2018). Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) pour les années 2018 à 2022. URL: <https://tinyurl.com/yd2zb269> (état au 30.3.2020).

² Unité de pilotage informatique de la Confédération UPIC (2019). Plan de mise en œuvre de la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) pour les années 2018 à 2022. URL: <https://tinyurl.com/y86kxqp8> (état au 30.3.2020).

³ Réseau national de sécurité (2019). Plan de mise en œuvre des cantons. URL: <https://tinyurl.com/y8w698bm> (état au 30.3.2020).