Circulation Un conducteur conteste la limite de deux véhicules maximum par plaque minéralogique interchangeable. » 9

Deux équipes d'Estavayer à l'assaut du Splash

Défi Deux équipes staviacoises participeront à une course d'obstacles déjantée à la piscine de Bellerive, à Lausanne. Se défieront notamment Nicolas Baechler et Raphaël Zadory, deux amis d'enfance. » 12

Les communes du canton de Fribourg s'estiment plutôt bonnes élèves en matière de cybersécurité

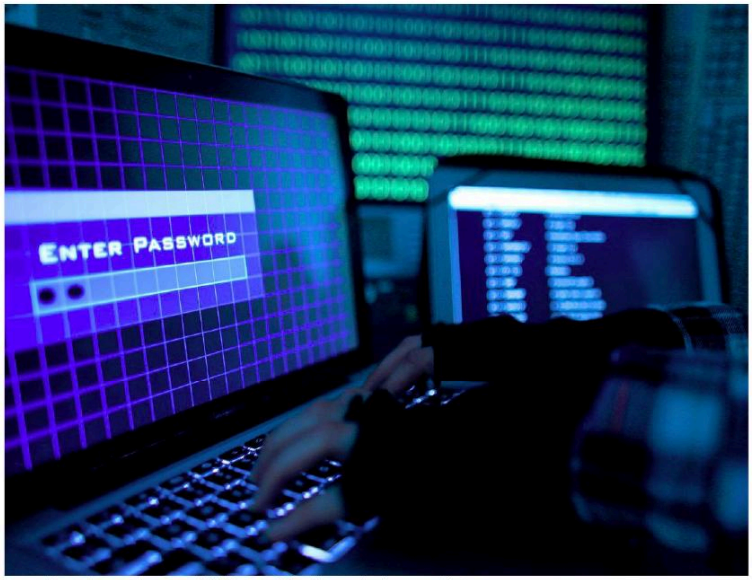
Une «sacrée mise à niveau»

« STÉPHANE SANCHEZ

Gestion du risque » En matière de sécurité informatique, près de 50% des administrations romandes n'ont ni formation, ni plan d'urgence, ni inventaire de leur matériel et de leurs données. «Il manque beaucoup de choses», résumait en juin dernier l'Association des communes suisses (ACS), sur la base d'un sondage. La moitié des communes fribourgeoises seraient-elles donc à la rue? Ce n'est pas la vision de certains acteurs ou connaisseurs des communes du canton, qui restent cependant modestes face aux hackers et aux failles.

«Les communes ont en main de quoi prévenir, agir et réagir»

Micheline Guerry-Berchier



La surveillance des connexions a permis à Villars-sur-Glâne d'intervenir précocement. Keystone

Micheline Guerry-Berchier, pourtant directrice de l'Association des communes fribourgeoises (ACF), s'étonne des chiffres avancés par sa faîtière: «Cela ne correspond pas à notre évaluation générale du terrain que nous avons pu partager lors des formations.» Après l'attaque que Rolle a signalée en août 2021, l'ACF a en effet organisé cinq soirées de cours entre décembre 2021 et mars 2022 avec la contribution de communes, de l'Ecole d'ingénieurs (HEIA-FR) et de la police cantonale. Quelque 260 participants (élus ou collaborateurs) y ont pris part. En janvier 2025, ils étaient 150. «En comparaison intercantonale, cette participation est forte.»

La police cantonale fait la même appréciation. Elle regarde en outre comme «bénéfique pour la sécurité en général» le fait que «des communes pionnières apportent leur point de vue et expérience» à d'autres. François Buntschu était aussi l'un des intervenants du cours de janvier dernier. Ce que ce professeur à l'HEIA-FR en retire: «Les communes et leurs prestataires sont conscients des risques, ainsi que des procédures en cas d'attaque.»

Procédures connues

La directrice de l'ACF renchérit: «Les communes de toutes tailles ont en main les informations pour prévenir, agir et réagir en cas de cyberattaque. Elles ont pu comparer ou renforcer leur système de contrôle interne si nécessaire. Certaines communes ont demandé à leurs prestataires de réaliser ou faire réaliser des audits de sécurité de leurs infrastructures. D'autres ont entamé des démarches de certification ou de labellisation.»

Cyber-Safe.ch, promu par l'Office fédéral de la cybersécurité, est l'un de ces labels. Surtout active en terres vaudoises, l'association a été sollicitée par «une dizaine de communes fribourgeoises depuis 2021», précise son secrétaire général et fondateur, Christophe Hauert. «Absence de mise à jour et de sauvegarde des données: à l'époque, les audits étaient inquiétants. Aujourd'hui, on parle de chiffrement des données, de gestion des périphériques mobiles et de précision des contrats de prestation. En quatre ans, on a vu une sacrée mise à niveau, y compris chez les prestataires.»

Des terminaux

La ville de Fribourg possède son propre service informatique (18,5 EPT, dont 1 pour la sécurité) mais ne communique pas sur ce sujet. Partout ailleurs, le recours à l'expertise externe est la règle. La petite commune du Châtelard s'y fie totalement: «Tout est sur le nuage, même les applications métiers (comptabilité, contrôle de l'habitant, etc.), confie le syndic David Fattebert, aussi président de l'ACF. Les ordinateurs sont comme des terminaux auxquels nos deux seules administratrices ont accès. Leurs directives viennent des prestataires, qui font les analyses de risque et les informent.»

Topo similaire à Ursy (4100 âmes): «Nous avons passé un audit en 2023. Nous avons un inventaire et un plan d'urgence. Rien n'est hébergé en local, et notre prestataire assure la sécurité», résume le syndic Philippe Dubey. Même Bulle, sur la base d'une analyse coûts/bénéfice, opte pour une gouvernance interne et garde «les compétences clés» (sans informaticien), mais recourt à des prestataires certifiés, indique Alain Sansonnens.

Collaborateurs sensibilisés

«La ville s'aligne sur les bonnes pratiques et a conduit une vaste analyse des risques», précise Alain Sansonnens, chargé de communication bullois, en évoquant des audites externes, des contrôles réguliers et des processus de gestion d'incidents établis. Depuis 2021, les collaborateurs bullois sont sensibilisés par des campagnes de simulation ou des ateliers.

«L'objectif est l'apprentissage et l'augmentation du signalement, pas la stigmatisation.» L'exercice porte notamment sur le phishing – ces mails ou SMS qui incitent les collaborateurs à cliquer sur un lien vers un faux portail, où ils divulguent sans le savoir leurs identifiants ou des données confidentielles à des usurpateurs.

L'intelligence artificielle renforce aujourd'hui les hackers, et Bulle dit tenir compte de ce nouvel outil – qui assiste aussi les cyberdéfenseurs. Mais «les règles de base restent primordiales, note la police cantonale: environnement informatique sécurisé et à jour, collaborateurs sensibilisés et formés.» »

Villars-sur-Glâne jugée réactive pour déjouer une cyberattaque

En juin, la commune a décelé très tôt une attaque de certains de ses serveurs. Elle a pu éviter le pire.

Le 18 juin dernier, la commune de Villars-sur-Glâne observait des connexions non autorisées sur certains de ses serveurs. Après analyse, aucun élément n'a permis de déduire «que des données auraient été volées ou compromises». Le retour à la normale a pris une semaine. C'est que «l'attaque a été décelée à un stade précoce grâce à une veille optimale», salue la police cantonale, aussitôt alertée – tout comme l'Office fédéral de la cybersécurité (OFCS).

Ces dernières années, Villars-sur-Glâne avait déjà fait un bond sécuritaire en obtenant un label: «Cela aide à réagir», confie humblement l'informaticien de la commune, Sergio Serras. «Il y a eu une alerte. J'en ai parlé au prestataire. On n'a pas laissé aux hackers le temps d'aller plus loin. Ça s'est joué en quelques minutes.»

Les hackeurs de Villars-sur-Glâne ont-ils été identifiés? «C'est probablement un groupement d'activistes», avance la police cantonale. «Quand ils aboutissent, ils se dévoilent dans leur demande de rançon ou sur les réseaux, comme NoName057 (16) qui avait annoncé la paralysie du site de la ville de Fribourg (*LL* du 19 juin 2023). Mais quand l'attaque est au stade préparatoire, une analyse est nécessaire. Nous attendons le rapport d'un prestataire externe.»

Le coût dû à l'incident? «De l'ordre de 100 000 francs. Des experts externes mandatés ont passé des heures à analyser le système», explique le syndic, Bruno Marmier. «Cet incident a été l'opportunité d'accélérer et d'étendre la mise en œuvre de dispositifs de sécurité et d'amélioration qui vont au-delà des exigences minimales, pour assurer une défense proactive», complète Sergio Serras.

Mais le pire a été évité: «Réussie, une cyberattaque génère plusieurs mois de perturbations, d'investigations, de corrections et de réinstallations, pour autant que la sauvegarde soit propre», commente Christophe Hauert, secrétaire général de Cyber-Safe.ch. Et cela peut coûter cher: «Il suffit de se demander combien de collaborateurs pourront encore travailler durant ce laps de temps, combien coûtera la reconstitution des données (si elle est possible) ou si les données volées pourront être utilisées contre des tiers. Il y a aussi un risque d'action en dommages et intérêts…»

La police cantonale relève de son côté «la rapidité d'annonce» dont Villars-sur-Glâne a fait preuve. «Cela permet de signaler la faille aux autres partenaires et infrastructures à risques similaires, afin de prévenir d'autres attaques.» » SZ

LES AUTORITÉS CIBLÉES

Depuis le 1er avril, les exploitants d'infrastructures critiques – dont les communes, en tant qu'autorités – ont l'obligation d'annoncer les attaques subies à l'Office fédéral de la cybersécurité. Au 2 septembre, l'OFCS indique provisoirement avoir reçu 117 signalements, qui mêlent parfois plusieurs procédés – saturation de services, effraction, vol d'accès, fuite de données, demande de rançon, logiciel malveillant ou autres. Les autorités (25 signalements) sont au sommet du classement, devant le secteur financier (23). Les communes ou leur canton ne sont pas distingués. De son côté, la police cantonale recense durant ces dernières années «moins de 5 annonces» provenant de communes. SZ