Prévenir les cybercrimes

Guide à l'intention des communes

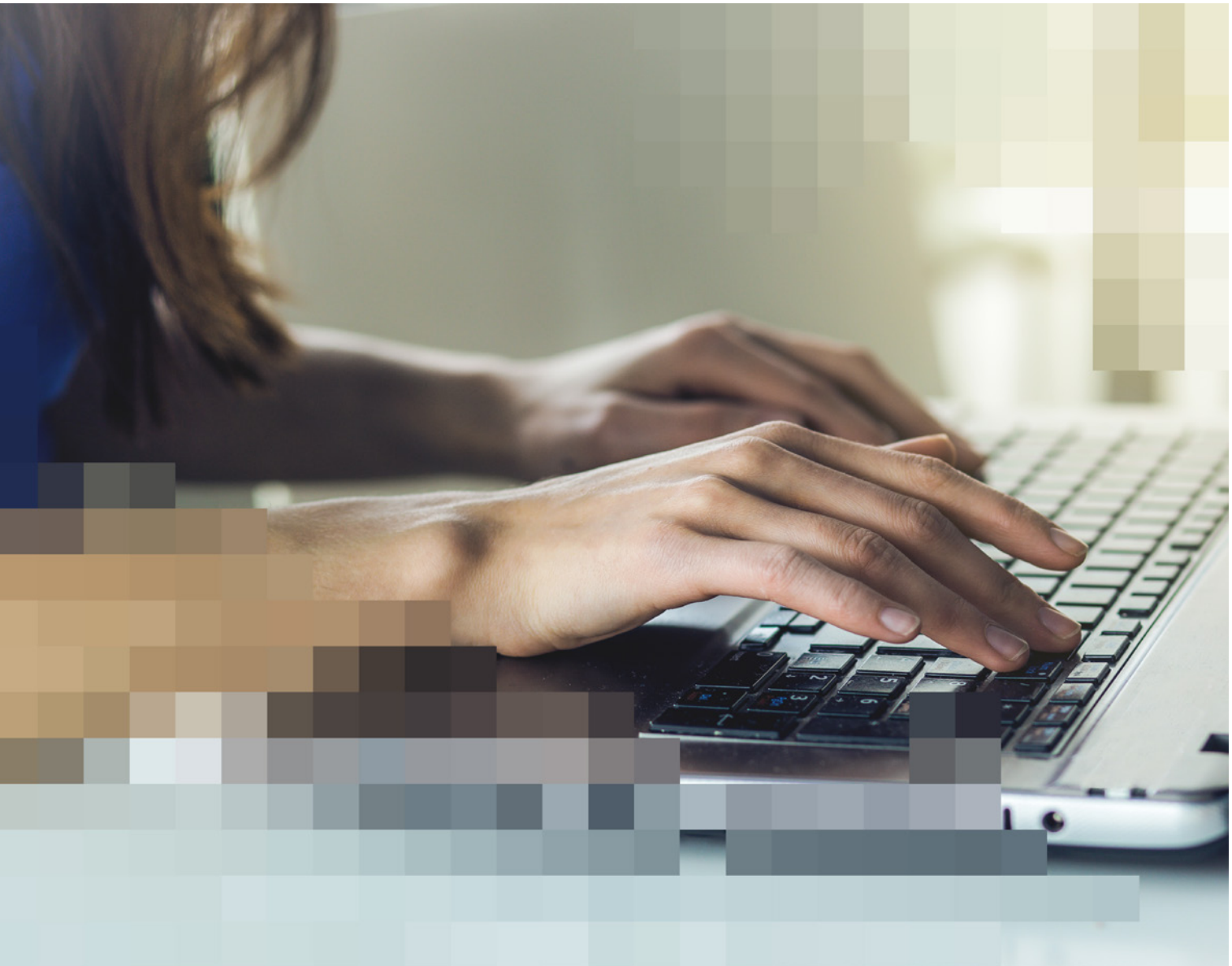

Table des matières

1 En quoi la cybercriminalité concerne-t-elle votre commune?

Proximité accrue avec les citoyennes et citoyens, amélioration de la promotion touristique et économique, prestations rapides et transmédias: la numérisation offre aux communes de nombreuses possibilités. Parallèlement, elle requiert de nouveaux processus et rend les communes de plus en plus dépendantes de technologies de l'information et de la communication (TIC, ci-après «informatiques») opérationnelles ainsi que des prestataires assurant ce genre de services. Et les criminels en profitent.

Dans son rapport de situation 2019[1], le Service de renseignement de la Confédération constate que l'administration publique est la cible de cyberattaques. Tout le monde peut être concerné: de l'administration communale à l'approvisionnement électrique. L'attaque peut par exemple mettre hors ligne un site internet ou toucher l'ensemble du réseau. Outre les dommages financiers, dans certains cas des informations confidentielles tombent entre de mauvaises mains. Avec des conséquences gravissimes: perte de données, suppression de systèmes, actions en dommages-intérêts pour violation de la protection des données ou atteinte à la réputation en sont quelques exemples.

Les cyberattaques peuvent détruire durablement la confiance de la population envers l'administration.

Les informations qui suivent donnent aux communes (petites et moyennes) des recommandations concrètes sur la manière de se protéger de la cybercriminalité et de réagir en cas d'attaque. Nous contribuons ainsi à mettre en œuvre les mesures de la «Stratégie nationale de protection de la Suisse contre les cyberrisques 2018–2022»[2], qui a pour tâche – commune à tous les niveaux étatiques et à d'autres partenaires – de protéger la Suisse dans le domaine cybernétique.

Par ailleurs, nous voulons vous encourager à annoncer les incidents importants à la police. Car seule la collaboration entre autorités de poursuite pénale et entités attaquées permettra d'identifier les criminels et de les condamner, ce qui peut combattre durablement la cybercriminalité.

1 Service de renseignement de la Confédération (2019). La sécurité de la Suisse 2019. Rapport de situation du Service de renseignement de la Confédération. www.vbs.admin.ch
2 Conseil fédéral (2018). Stratégie nationale de protection de la Suisse contre les cyberrisques 2018–2022. www.isb.admin.ch/isb/fr/home/themen/cyber_risiken_ncs.html

2 Comment des criminels peuvent-ils porter préjudice à votre commune?

Les cybercriminels exercent du chantage et prennent les communes pour cible en menaçant de divulguer des données sensibles ou en paralysant des services, notamment dans la sécurité de l'approvisionnement.

2.1 Méthodes des arnaqueurs et arnaqueuses

Les pirates induisent la «cible» en erreur afin qu'elle fasse quelque chose qu'elle ne ferait pas d'elle-même. Dans la plupart des cas, il s'agit de l'inciter à ouvrir une pièce jointe à un courriel, à cliquer sur un lien, à indiquer des données personnelles, telles que mots de passe, ou à effectuer un versement.

Une méthode courante s'appelle manipulation sociale (social engineering). Au préalable, les pirates s'informent de multiples manières sur la structure administrative, organisationnelle ou entrepreneuriale. C'est possible grâce aux informations publiées sur le site internet de l'administration communale ou les réseaux sociaux par exemple. Ils cherchent ensuite une «cible» qu'ils confrontent à un scénario sur mesure. Les pirates cherchent par exemple à obtenir les noms d'utilisateur et mots de passe en se faisant passer au téléphone pour un collaborateur ou une collaboratrice d'une entreprise de logiciel. Sous prétexte de graves problèmes informatiques et en feignant de connaître l'entreprise, ils désorientent la personne visée jusqu'à ce qu'elle divulgue les informations souhaitées. Dans leurs courriels ou durant leurs appels, les pirates empruntent parfois également le nom d'une unité administrative, comme les contributions ou les fournisseurs d'énergie.

Types de manipulation

Hiérarchie	Les pirates utilisent la structure hiérarchique de l'organisation et poussent à agir. Souvent sous une fausse identité, ils somment le collaborateur ou la collaboratrice au nom d'une personne supérieure à partager des informations sensibles ou à exécuter un versement.
Urgence	Les pirates font croire à la «cible» qu'elle doit agir en toute hâte.
Convoitise/curiosité	Les pirates promettent à la personne visée un gain ou une surprise si elle ouvre le fichier ou clique sur un lien.
Peur/colère	Les pirates menacent la personne visée, au cas où elle n'exécuterait pas l'ordre. Ou ils font des déclarations manifestement inexactes, que l'on peut corriger en cliquant sur un lien préjudiciable.
Sympathie	Le sujet abordé fait vibrer la corde sensible de la «cible». Celle-ci veut s'associer afin de régler un problème.

2.2 Variantes en matière de chantage et de vol

Les criminels ont accès à votre réseau communal grâce à des données d'accès volées, des logiciels malveillants ou des systèmes mal sécurisés. S'ils trouvent des données intéressantes, ils les cryptent ou vous menacent de les publier ou de les effacer si vous ne versez pas de rançon. Parfois les données sont copiées et vendues à des tiers ou utilisées pour des versements par e-banking.

Procédés fréquents

Rançongiciel (ransomware)	Des logiciels malveillants sont envoyés en grand nombre, par exemple par courriel. Les victimes ainsi trouvées sont ensuite espionnées afin de récolter des informations. En cas de succès, les pirates prennent le contrôle et commencent à crypter les données. Le cas échéant, des données seront également volées. Les maîtres-chanteurs exigent une rançon (angl. ransom) pour décrypter les données.
Chevaux de Troie e-banking	À part le chantage, les cybercriminels visent surtout à manipuler les ordres de paiement. Ils utilisent à cet effet des chevaux de Troie e-banking: ce sont des programmes permettant aux pirates d'avoir accès aux comptes e-banking d'une victime. Ils sont souvent envoyés par courriel (p.ex. camouflés en facture ou en dossier de candidature).
Hameçonnage (phishing)	Les destinataires sont avertis par courriel, site internet, cybertéléphonie ou SMS que certaines données d'accès ne sont plus sûres ou plus actuelles et invités à les modifier via le lien donné. Ce lien mène cependant à un site internet falsifié. Si les destinataires s'y connectent, ils permettent aux pirates d'obtenir des données d'accès, par exemple, celles de la carte de crédit ou des mots de passe pour les courriels ou une autre compte.
DDoS (déni de service distribué)	DDoS est l'acronyme de Distributed Denial of Services. Lors d'une telle attaque, les services, tels que le site internet, la messagerie électronique ou l'installation téléphonique numérique, sont submergés de très nombreuses demandes. Le système tombe alors en panne et l'administration ou le prestataire ne peut plus accomplir ses tâches. Une rançon devrait être versée pour stopper l'attaque. Les pirates utilisent parfois les attaques DDoS pour détourner l'attention de la vraie «frappe numérique» au moyen de données d'accès volées auparavant.
Accès à distance (remote access)	Comme son nom l'indique, l'accès à distance permet d'accéder de l'extérieur à un ordinateur ou à un réseau, par exemple en télétravail ou pour une télémaintenance effectuée par l'assistance informatique. Les pirates utilisent également cet accès à distance, pour atterrir sur les réseaux de l'administration ou d'un prestataire, par exemple au moyen de tentatives d'hameçonnage ou d'attaques sur les mots de passe ou sur des composantes non sécurisées, voire obsolètes du réseau.

3 Comment pouvez-vous protéger votre commune?

Différentes mesures techniques et organisationnelles sont nécessaires pour se protéger de cyberattaques. Certaines peuvent être exécutées par les cadres communaux eux-mêmes, d'autres sont à discuter avec les responsables informatiques internes ou externes. Vous trouvez un résumé des mesures de protection détaillées ci-après, sous forme d'aide-mémoire en fin de document.

3.1 Mesures organisationnelles

> **Régler les responsabilités**
Nommez dans votre administration un ou une responsable des différentes tâches concernant la sécurité des systèmes informatiques. Clarifiez également les rôles et les responsabilités relatifs à l'organisation des cas d'urgence ou de crise ainsi que leurs compétences respectives. Vous devez au préalable identifier les interfaces avec vos partenaires afin de vous concerter au niveau des processus. Définissez avec votre responsable informatique les incidents sécuritaires, dont vous voulez absolument être informé(e). C'est le cas des incidents touchant votre propre infrastructure ou celle de votre prestataire informatique.

> **Faire l'inventaire de son environnement informatique**
Établissez une liste détaillée de votre infrastructure informatique. Vous savez ce que vous devez protéger et surveiller, seulement si vous connaissez votre infrastructure informatique, vos services, ordinateurs, utilisateurs et utilisatrices, etc.

> **Prendre des précautions**
Une bonne stratégie contre les cyberattaques commence avant tout incident: des processus bien rodés et des voies de recours à la hiérarchie sont indispensables pour garder le contrôle.

Définissez quels fichiers journaux (PV des événements informatiques) sont enregistrés et combien de temps. Le mieux serait de les centraliser. Des fichiers journaux détaillés aident à saisir l'origine de l'attaque, à obtenir des informations sur les systèmes infectés dans votre propre réseau et à prendre des mesures correctives. Vu leur importance, les aspects relatifs à la protection des données des fichiers journaux ne doivent en aucun cas être négligés. Clarifiez les questions concernant les fichiers journaux et la détection d'attaques avec votre responsable informatique.

Stratégie en amont des situations d'urgence

> Dispositif communicationnel et plan de crise adaptés à la grandeur de la commune et concertés avec le prestataire.

> Liste de contacts (services internes et externes, prestataires).

> Réflexions
  > relatives à la perte totale du paysage informatique (remplacement, reprise des activités, perte de données, etc.),
  > relatives aux moyens de communication utilisés si les systèmes informatiques ne sont plus disponibles.

> Scénarios d'urgence informatique, exercices et examen de la vulnérabilité de l'infrastructure.

> **Régler le traitement des informations et des données sensibles**
Faites un inventaire de vos données et informations et définissez-en les éléments sensibles. Concevez un plan de protection pour ces éléments. Les dispositions cantonales et communales relatives à la protection des données peuvent être consultées sur le site internet de votre canton et de votre association des communes (voir également chapitre 4: «Solliciter un soutien»).

Réfléchissez bien aux informations que vous publiez sur votre site internet ou sur les réseaux sociaux, car elles sont récoltées par les pirates. La personne responsable des affaires financières ayant accès à l'e-banking ne devrait pas être mentionnée sur votre site internet. Par principe, aucune information ou donnée confidentielle ne devrait être transmise via des canaux impersonnels, tels que téléphone ou courriel. Les informations confidentielles destinées à un service externe devraient être systématiquement cryptées ou envoyées par courrier.

Montrez-vous prudent(e) dans l'utilisation des services de cybernuage employés par de nombreux programmes. Demandez-vous quelles données doivent être enregistrées localement et lesquelles dans le cybernuage. Les données sensibles ne devraient jamais être confiées à un cybernuage sans être cryptées. Avant toute utilisation d'un service de cybernuage, lisez les conditions générales (CG) du prestataire et veillez aux dispositions légales en matière de protection des données, car celles-ci ne peuvent pas être transmises, par exemple à des fins commerciales. Renseignez-vous auprès de votre préposé(e) à la protection des données. Vous trouvez une aide en matière de protection des données et la liste d'adresses des préposés sur le site de privatim de la Conférence des Préposé(e)s suisses à la protection des données, www.privatim.ch

> **Utiliser des mots de passe sûrs**
Définissez des règles contraignantes pour les mots de passe, appliquez-les systématiquement et demandez à votre personnel d'en faire autant. Un mot de passe devrait compter douze signes au minimum et comporter majuscules, minuscules, chiffres et caractères spéciaux. Dans l'idéal, il est généré arbitrairement et ne se rapporte pas à des informations personnelles, comme le nom ou la date de naissance. Une authentification à deux facteurs procure une protection supplémentaire. Évitez absolument d'utiliser le même mot de passe à plusieurs endroits! S'il est difficile de se rappeler de plusieurs mots de passe, il vaut la peine de recourir à un gestionnaire de mots de passe.

En suivant ces règles, vous n'êtes pas obligé(e) de changer périodiquement de mots de passe. Par contre, il faut les changer dès que des tiers pourraient en avoir eu connaissance ou qu'un membre du personnel quitte l'administration communale.

Sensibiliser le personnel administratif et les membres de milice[3]
La protection contre les cyberattaques est du ressort des cadres communaux. En fait partie la sensibilisation du personnel. Les secrétaires communaux endossent beaucoup de responsabilités au sein de l'administration communale et doivent prendre de plus en plus de décisions de nature informatique. Il est recommandé de former les secrétaires communaux spécialement dans ce domaine et d'investir dans des programmes de sensibilisation à la sécurité destinés au personnel administratif et aux membres de milice. Organisez-les de concert avec d'autres communes ou votre association cantonale des communes. Cela peut réduire le travail et les coûts. L'aide-mémoire «Conseils à l'intention du personnel communal» donne des informations à l'intention de votre personnel.

3 Politiciens et politiciennes, personnes extérieures, etc.

> **Prudence avec les courriels**
Les logiciels malveillants atterrissent sur votre ordinateur souvent à travers des pièces jointes, camouflées en pseudo-factures ou en dossiers de candidature. Bloquez la réception de pièces jointes dangereuses. Vous trouvez une liste détaillée et actualisée de telles pièces jointes sur le site de GovCERT[4]. Assurez-vous qu'aucune macro d'origine incertaine ne puisse s'exécuter dans les documents Office. Parlez-en avec votre responsable informatique. Définissez par quels moyens de communication votre personnel peut annoncer des événements douteux (courriel, ordinateur, appel téléphonique, etc.) et activez, si possible, une fonction pour annoncer des courriels douteux.

Faites preuve de vigilance lorsque vous communiquez avec les citoyennes et citoyens. N'envoyez des courriels qu'en texte brut et montrez-vous économe en pièces jointes. Évitez les documents Office dotés de macros, préférez les documents PDF. Fournissez des liens mais ne renvoyez pas à des sites exigeant nom d'utilisateur, mot de passe ou d'autres données. La majorité des courriels frauduleux ne sont pas personnalisés, par conséquent adressez-vous si possible à vos citoyennes et citoyens en mentionnant leurs noms et prénoms.

Qui connaît les vulnérabilités de son système peut le préserver des cybercriminels.

> **Protéger ses comptes bancaires en ligne**
Pour vos paiements, utilisez un ordinateur séparé, avec lequel vous ne surfez pas sur internet ni ne recevez de courriels. Parlez avec votre responsable informatique de la possibilité de procéder à vos versements en ligne dans un secteur séparé des autres applications (technique du bac à sable, sandbox) ou dans un système virtuel spécifique, particulièrement bien protégé.

Clarifiez l'ensemble des processus relatifs au trafic des paiements. Ceux-ci doivent être respectés par le personnel dans tous les cas. Par exemple, le principe du double contrôle et/ou la signature collective: ici, les paiements doivent être visés par un utilisateur ou une utilisatrice supplémentaire de l'e-banking avant d'être déclenchés. C'est d'autant plus nécessaire si plusieurs membres du personnel peuvent effectuer des paiements. Discutez avec votre banque des mesures de sécurité possibles.

4 www.govcert.ch/downloads/blocked-filetypes.txt

3.2 Mesures techniques

> **Sauvegarder les données**
Définissez un processus réglant la sauvegarde régulière de vos données (back-up) et respectez-le systématiquement. Évaluez la quantité de données en nombre de jours, que vous pouvez vous permettre de perdre et stockez une copie supplémentaire de votre sauvegarde séparément (offline) et hors murs (offsite). Exercez-vous – ainsi que la personne qui assure votre suppléance – de temps en temps à restaurer une sauvegarde, afin que ce processus vous soit familier en cas de besoin. Assurez-vous de conserver les sauvegardes antérieures durant plusieurs mois.

> **Procéder à des mises à jour de sécurité**
Un vieux logiciel est une porte d'entrée prisée par les logiciels malveillants. Assurez-vous que vos systèmes soient toujours actualisés, également votre système de gestion de contenu (Content Management System, CMS) de vos pages internet. La plupart des CMS offre une fonction de mise à jour automatique et simple à activer.

> **Installer un logiciel antivirus**
Installez un logiciel antivirus sur chaque ordinateur et activez la protection en temps réel. Veillez à ce qu'il soit actualisé régulièrement et qu'il effectue un examen complet du système chaque jour.

> **Sécurisez votre accès à distance**
L'accès à distance à votre réseau ne devrait jamais être protégé par une authentification simple (nom d'utilisateur et mot de passe). Utilisez au moins une authentification à deux facteurs ou installez une liaison sûre via un réseau privé virtuel (VPN). C'est également valable pour l'accès de responsables informatiques externes.

4 À quoi devriez-vous veiller en cas d'externalisation des prestations informatiques?

Veuillez trouver ci-après quelques conseils au cas où vous externalisez votre infrastructure informatique et en confiez la gestion à une ou plusieurs entreprises externes. L'aide-mémoire «Votre commune est-elle bien protégée contre les cyberattaques?» mentionne d'autres exigences à inclure dans le catalogue de prestations et à couvrir par le contrat conclu avec le prestataire informatique. Cependant, la responsabilité ne peut être ni externalisée, ni déléguée. En cas d'incident, la commune peut se retrouver au bout de la chaîne de responsabilités.

La responsabilité incombe au cadre communal.

> **Se baser sur les exigences minimales**
Au moment où vous recevez des systèmes informatiques intégrés, vous devez en contrôler la sécurité. Renseignez-vous auprès du service informatique de votre canton ou de votre association des communes sur les CG et directives adéquates lorsque vous avez recours à des prestations informatiques. Ces directives devraient faire partie intégrante des relations contractuelles entre vous et vos prestataires informatiques externes. Il y a lieu de régler l'obligation légale de garder le secret pour les tiers s'occupant de la maintenance et de la gestion de vos systèmes informatiques et de ne pas autoriser un accès inutile à des données sensibles. Il convient également de procéder à des mises au point et de conclure des conventions avec chaque entreprise enregistrant des données (entreprise de cybernuage).

> **Choisir un prestataire informatique spécialisé**
Des certifications selon des normes reconnues de protection des données et de sécurité de l'information ou des rapports de contrôle de tiers indépendants peuvent être utiles pour choisir un prestataire (voir l'aide-mémoire «Normes et guides recommandés dans le domaine informatique»). Vous n'êtes pas obligé(e) de choisir un partenaire certifié. Mais il est recommandé que les prestataires informatiques puissent montrer qu'ils remplissent les exigences que vous posez et qu'ils peuvent assurer la disponibilité et la sécurité requises. Faites-le analyser ou confirmer par un service indépendant.

> **Effectuer des audits de sécurité**
Il convient de contrôler régulièrement que les prestations définies dans le contrat sont effectuées au moyen d'un référentiel d'audit reconnu, par exemple sur la base de COBIT (Control Objectives for Information and Related Technology) de l'ISACA (Information Systems Audit and Control Association). Ayez recours aux services d'organes de contrôle indépendants. Le prestataire informatique peut également obtenir une attestation ISAE 3402 Type 2 (International Standard on Assurance Engagements), également connue comme rapport SOC 2 (Service Organization Control). L'organe de contrôle évalue la sécurité, la disponibilité, l'intégrité et la confidentialité.

> **Collaborer avec d'autres communes**
Si votre administration communale n'est financièrement pas en mesure d'acheter tous les services d'un prestataire informatique, collaborez avec d'autres communes intéressées. Cela vous offre de meilleures conditions d'achat et réduit les charges d'acquisition. Une autre option est d'externaliser cette tâche à une commune plus grande.

> **Solliciter un soutien**
Différents services administratifs, associations et organisations proposent des informations pertinentes en matière d'externalisation de prestations informatiques et des aides tels que guides, notices et modèles de contrat pour la collaboration avec des prestataires informatiques.

Exemples de services administratifs, associations et organisations:

Technologies de l'information et de la communication (TIC)

> Les services informatiques cantonaux mettent à disposition des guides et des aides, par exemple l'Office d'informatique et d'organisation (OIO) du canton de Berne, www.be.ch/oio
> Les associations de communes peuvent proposer un soutien. Vous trouvez la liste de ces associations sur www.chgemeinden.ch/fr/
> Auprès de l'Office fédéral pour l'approvisionnement économique du pays (OFAE), vous trouvez la norme minimale pour les TIC, www.ofae.admin.ch
> Le Centre national pour la cybersécurité[5] (NCSC), www.ncsc.ch, dispose d'informations du service de renseignement et des équipes d'intervention en cas d'urgence informatique d'autres pays (Computer Emergency Response Teams, CERT) ainsi que sur des mesures préventives. Si votre prestataire informatique n'en est pas encore membre, adressez-vous à outreach@ncsc.ch
> Les CG de la Conférence suisse sur l'informatique (CSI) conviennent aux activités informatiques de l'administration publique, qui comportent des modèles contractuels, https://sik.swiss/fr/
> Le label cyber-safe.ch a été mis au point par l'Association suisse pour le label de cybersécurité. Il définit les exigences minimales spécifiques aux communes ou PME. Un questionnaire en ligne permet d'identifier les cyberrisques des communes ou PME, www.cyber-safe.ch

Marchés publics

> Le site d'eGovernment Suisse, www.egovernment.ch, et l'association simap.ch, www.simap.ch, vous donnent un aperçu des pages de l'administration fédérale, des cantons et des grandes villes sur les marchés publics.

Protection des données

> Le site de privatim de la Conférence des Préposé(e)s suisses à la protection des données, www.privatim.ch, offre une aide en matière de protection des données et une liste des préposés à la protection des données.
> Pour le traitement des données par des particuliers et des organes fédéraux, c'est le préposé fédéral à la protection des données et à la transparence (PFPDT) qui est compétent, www.edoeb.admin.ch

5 Depuis le 1er janvier 2020, différentes tâches fédérales relatives au cyberdomaine ont été réunies sous un même toit, celui du Centre national pour la cybersécurité (NCSC). Cela concerne notamment, la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI).

5 Que devez-vous faire en cas d'attaque?

Mesures d'urgence en cas de cyberattaque

Isoler
> Séparer immédiatement tous les systèmes du réseau. N'oubliez pas d'éteindre le WLAN.

Contacter
> Contactez votre responsable informatique ainsi que tous les interlocuteurs de l'organisation dont vous avez besoin pour maîtriser l'attaque.
> Examinez s'il y a lieu de contacter la police et d'effectuer une dénonciation pénale. Attendez que la police ait sauvegardé les traces avant de restaurer les systèmes. Des spécialistes de la police vous conseillent et vous secondent pour savoir comment procéder, sauvegardent les traces et enquêtent. Vous trouvez sur www.suisse-epolice.ch le numéro de téléphone du poste de police le plus proche.

Annoncer
> Annoncez une attaque également auprès du NCSC, www.ncsc.ch. De même, vous devriez informer votre association des communes sur l'incident, car plusieurs communes peuvent le cas échéant être touchées.
> N'oubliez pas de procéder aux déclarations obligatoires, par exemple concernant la protection des données.

Vos responsables informatiques ou d'autres spécialistes vous aident à réparer votre infrastructure et le cas échéant à la restaurer.

La prochaine attaque ne sera peut-être pas la dernière: intégrez le savoir acquis pour améliorer la qualité, les processus internes, la documentation, la pratique ainsi que la conduite et la culture d'entreprise.

6 Comment pouvez-vous contribuer à identifier les pirates?

6.1 N'hésitez pas à annoncer un incident

L'expérience montre que de nombreux délits cybernétiques sont liés et présentent des similarités. Toute plainte et toute dénonciation peut livrer un indice décisif sur les auteurs.

La police n'est pas intéressée à vos secrets administratifs et n'intervient pas sur votre infrastructure. Lors d'une attaque, elle cherche uniquement des informations et des traces pertinentes pour élucider le délit. L'enquête est soumise au secret de fonction. En outre, les dispositions de la protection des données doivent également être respectées. Les craintes qu'une dénonciation ait un impact négatif, tel que la mise en sûreté d'ordinateurs sur une longue période ou la publication d'un cas, sont infondées. La police vous prend très au sérieux et en général convient d'abord avec vous des mesures de poursuite pénale. Vous pouvez également en tout temps faire appel à votre assistance juridique. Dans la plupart des cas, il est possible de trouver une manière de procéder convenant aux deux parties.

En cas de cyberattaque, agir rapidement peut réduire le dommage.

6.2 Annoncer immédiatement les incidents

Annoncez le plus rapidement possible à la police ou au ministère public les incidents de nature pénale, par exemple un accès indu à un système de traitement des données. Surtout s'il a provoqué un dommage. Plus vous attendez, plus il est probable que de précieuses traces soient effacées. De plus, toute action peut rendre des traces inutilisables, voire les effacer. N'importe quel poste de police enregistre une plainte. Sur le site en ligne Suisse ePolice (www.suisse-epolice.ch) vous trouvez le numéro de téléphone du poste de police le plus proche.

Réfléchissez également à la possibilité d'annoncer un incident sans dommage ou toute tentative d'infraction aux autorités de poursuite pénale ou au NCSC. Les indications fournies au NCSC ne peuvent cependant pas être utilisées pour une plainte pénale, ni dans une procédure pénale.

Conseils pour les cadres communaux en matière de protection contre les cyberattaques

N'importe quelle commune peut faire l'objet d'une cyberattaque. Grâce à quelques mesures de précaution vous pouvez cependant mieux protéger votre commune.

Clarifier les responsabilités et prendre des précautions

> Réglez les responsabilités en matière de sécurité informatique ainsi que les interfaces avec vos partenaires. Des processus bien rodés et des voies de recours à la hiérarchie sont indispensables pour garder le contrôle.

Protéger ses données

> Réglez le traitement des informations et données. Aucune donnée sensible ne devrait être transmise via un canal impersonnel.
> Montrez-vous prudent(e) dans l'utilisation de services de cybernuage. Avant tout recours à une entreprise de cybernuage, lisez les conditions générales et veillez aux dispositions de protection des données. Les données sensibles ne devraient jamais être confiées à un cybernuage sans être cryptées.
> Définissez un processus réglant la sauvegarde régulière (back-up) de vos données et stockez-en une copie supplémentaire séparément (offline) et hors murs (offsite).

Utiliser des mots de passe sûrs

> Un mot de passe devrait compter douze signes au minimum et comporter majuscules, minuscules, chiffres et caractères spéciaux. Une authentification à deux facteurs procure une protection supplémentaire. Évitez absolument d'utiliser le même mot de passe à plusieurs endroits! À la place, ayez recours à un gestionnaire de mots de passe et générez un mot de passe par application.

Sensibiliser le personnel administratif et les membres de milice (politiciens, politiciennes, personnes extérieures, etc.)

> Les secrétaires communaux endossent beaucoup de responsabilités et doivent prendre de plus en plus de décisions de nature informatique. Il est recommandé de former les secrétaires communaux spécialement dans ce domaine et d'investir dans des programmes de sensibilisation à la sécurité destinés au personnel administratif et aux membres de milice.

Prudence avec les courriels

> Bloquez la réception de pièces jointes dangereuses et assurez-vous qu'aucune macro d'origine incertaine ne puisse s'exécuter dans les documents Office. Définissez par quels moyens de communication votre personnel peut annoncer des événements douteux (courriel, ordinateur, appel téléphonique, etc.) et activez, si possible, une fonction pour annoncer des courriels douteux.

Être à jour

> Installez un logiciel antivirus et assurez-vous qu'il soit automatiquement actualisé sur l'ensemble des ordinateurs et serveurs de votre réseau.

Sécuriser son accès à distance

> Protégez l'accès à distance à votre réseau par une authentification à deux facteurs. Dans l'idéal, installez une liaison sûre via un réseau privé virtuel (VPN).

Veiller à avoir un accès sécurisé aux comptes bancaires en ligne

> Protégez vos comptes bancaires en ligne en utilisant un ordinateur ou un secteur séparé des autres applications (technique du bac à sable, sandbox) ou encore un système virtuel spécifique, particulièrement bien protégé. Réglez les processus relatifs au trafic des paiements en instaurant, par exemple, le principe du double contrôle et / ou la signature collective.

Conseils à l’intention du personnel communal, afin d’éviter les cybercrimes

La protection contre les cyberattaques est du ressort des cadres communaux. En fait partie la sensibilisation du personnel. Celui-ci devrait appliquer les mesures suivantes au quotidien:

Prudence avec les courriels

> Montrez-vous méfiant(e) face à des liens ou des pièces jointes à des courriels envoyés par des personnes inconnues. Soyez particulièrement prudent(e) en ouvrant des documents Office; n’activez jamais la macro. N’hésitez pas à poser des questions à l’expéditeur ou expéditrice, si quelque chose vous paraît inhabituel, même s’il s’agit d’une personne connue! La prudence est de mise également avec l’icone «réponse»: vérifiez si le courriel va réellement à la bonne personne. Le mieux serait d’écrire vous-même l’adresse électronique.

Utiliser des mots de passe sûrs

> Un mot de passe devrait compter douze signes au minimum et comporter majuscules, minuscules, chiffres et caractères spéciaux. Ne communiquez jamais mots de passe, données d’accès ou informations bancaires par téléphone, courriel ou formulaire internet que vous pouvez ouvrir grâce à un lien.
> Évitez absolument d’utiliser le même mot de passe à plusieurs endroits.

Veiller aux données sensibles

> Réfléchissez bien à quelles informations vous publiez par exemple sur le site internet ou les réseaux sociaux ou à celles que vous discutez dans les transports publics.
> Les informations confidentielles destinées à un service externe devraient être systématiquement cryptées ou envoyées par courrier.

Votre commune est-elle bien protégée contre les cyberattaques?

Votre administration communale est-elle bien protégée contre les cyberattaques et s'y est-elle correctement préparée? Cet aide-mémoire vous aide à approfondir les questions les plus importantes en matière de cybersécurité. Un «je ne sais pas» ou un «non» signifie que vous devriez clarifier la question. Une chose est sûre: les mesures de protection contre les cyberattaques ne peuvent pas être déléguées à votre personnel, mais doivent être prises et coordonnées par les cadres communaux.

Au cas où vous avez externalisé votre infrastructure informatique, vérifiez que les points suivants sont couverts par le contrat avec votre prestataire informatique.

	Oui	Non	Ne sais pas
Tâches, compétences, responsabilités			
Votre administration communale a-t-elle défini qui est responsable de la cyberprotection?	○	○	○
La personne responsable a-t-elle les connaissances requises en cyberprotection et la capacité de la gérer? Continue-t-elle à se former régulièrement?	○	○	○
La personne responsable a-t-elle la position hiérarchique nécessaire et les compétences spécifiques pour mettre en œuvre les mesures de cyberprotection?	○	○	○
Disposez-vous de directives relatives à l'utilisation sûre des appareils et données informatiques?	○	○	○
Ces directives et les mesures de cybersécurité sont-elles rigoureusement mises en œuvre et régulièrement vérifiées?	○	○	○
Sensibilisation du personnel administratif et des membres de milice			
Existe-t-il des directives internes relatives à l'utilisation sûre des courriels, des données numériques et d'internet à l'intention de votre personnel?	○	○	○
Votre personnel connaît-il ces directives et les comprend-il?	○	○	○
Votre personnel met-il ces directives rigoureusement et correctement en œuvre?	○	○	○
Votre personnel est-il régulièrement informé et sensibilisé à la cyberprotection, par exemple à l'utilisation correcte des courriels?	○	○	○
Directives de protection des données			
Les données de vos systèmes (dispositifs de stockage et de sauvegarde des données, terminaux, serveurs) sont-elles cryptées?	○	○	○
Avez-vous connaissance des prescriptions légales relatives à la sauvegarde et au traitement des données?	○	○	○
Connaissez-vous vos obligations résultant des prescriptions légales sur les données à caractère personnel?	○	○	○
Les prescriptions en vigueur relatives à la protection des données sont-elles rigoureusement et correctement mises en œuvre au sein de votre administration communale?	○	○	○
Dans votre administration communale, l'accès physique à l'infrastructure des ordinateurs, serveurs et réseau est-il correctement protégé contre des tiers?	○	○	○
Directives sur les mots de passe et administration des utilisateurs			
Votre administration communale dispose-t-elle de directives sur l'utilisation des mots de passe?	○	○	○
Existe-t-il des directives définissant qui a accès à quelles données?	○	○	○
Ces directives sont-elles rigoureusement et correctement mises en œuvre?	○	○	○
Protection actualisée contre les logiciels malveillants			
Vos appareils sont-ils protégés contre des logiciels malveillants (programme antiviral)?	○	○	○
Pare-feu configuré et actualisé			
Votre réseau et vos systèmes informatiques sont-ils protégés par un pare-feu?	○	○	○
Des règles spécifiques au pare-feu ont-elles été définies (p.ex. restriction géographique)?	○	○	○
Votre pare-feu est-il régulièrement actualisé?	○	○	○

	Oui	Non	Ne sais pas
Segmentation du réseau			
Les différents secteurs de votre administration communale, par exemple personnel et comptabilité, sont-ils séparés?	○	○	○
Utilisez-vous un ordinateur ou système séparé uniquement pour vos transactions par e-banking?	○	○	○
Accès à distance			
L'accès à distance à l'infrastructure d'ordinateurs, serveurs et réseau de votre administration communale est-il protégé (réseau privé virtuel [VPN], authentification à deux facteurs)?	○	○	○
Actualiser les appareils et systèmes liés à internet			
Utilisez-vous la possibilité d'actualiser automatiquement vos logiciels?	○	○	○
Les appareils et systèmes dont les logiciels ne sont pas automatiquement actualisés sont-ils régulièrement mis à jour, par exemple par le producteur?	○	○	○
Les appareils mobiles utilisés dans l'environnement de votre administration communale sont-ils régulièrement actualisés?	○	○	○
Le système de gestion du contenu (CMS) de votre site internet est-il à jour?	○	○	○
Réseau sans fil (WLAN) sécurisé et crypté			
Votre réseau sans fil est-il crypté et sécurisé?	○	○	○
Existe-t-il un réseau sans fil séparé pour votre personnel et pour vos hôtes?	○	○	○
Sauvegarde			
Appliquez-vous un processus de sauvegarde (back-up) des données?	○	○	○
Vérifiez-vous régulièrement le fonctionnement et la lisibilité des sauvegardes?	○	○	○
Une copie supplémentaire de la sauvegarde est-elle stockée de manière séparée (offline) et hors murs (offsite)?	○	○	○
Précautions minimales pour gérer les situations d'urgence			
Avez-vous défini des mesures d'urgence en cas d'incident informatique?	○	○	○
La personne responsable et vos interlocuteurs en cas d'incident informatique (p.ex. dysfonctionnement, attaque, etc.) sont-ils définis et disponibles?	○	○	○
Existe-t-il des plans opérationnels de réaction et de redémarrage?	○	○	○
Savez-vous comment est réglé le contrôle des systèmes et les voies de recours à la hiérarchie?	○	○	○
Pouvez-vous repérer les traces numériques? Si non: est-ce assuré à l'externe?	○	○	○
L'accès physique aux systèmes est-il assuré (pour le repérage des traces numériques)?	○	○	○
Avez-vous suffisamment de mémoire à disposition pour sauvegarder les moyens de preuve?	○	○	○
L'obligation de documenter tous les systèmes importants (p.ex. dans une base de gestion de configuration, configuration management database, CMDB) est-elle réglée?	○	○	○
Contrat avec le prestataire informatique			
Les points susmentionnés de cette évaluation sont-ils couverts par le contrat qui vous lie à votre prestataire informatique?	○	○	○
Les responsabilités en cas de dommage et les limites à l'obligation au titre des prestations définies (p.ex. force majeure) sont-elles réglées dans le contrat?	○	○	○
Les niveaux de service pour le fonctionnement normal et d'urgence sont-ils clairement formulés (cela concerne les services mandatés pour les objectifs de sécurité requis, p.ex. disponibilité, confidentialité et intégrité)? Des notions telles que fonctionnement d'urgence ou incident critique sont-elles définies?	○	○	○
Avez-vous prévu une stratégie de sortie? Est-elle définie dans le contrat, notamment pour les solutions de cybernuage?	○	○	○

Document basé sur le test rapide de cyberprotection pour PME d'ICTswitzerland et d'autres partenaires, www.cybersecurity-check.ch

Normes et guides recommandés dans le domaine informatique

Des certifications selon des normes reconnues de protection des données et de sécurité de l'information ou des rapports de contrôle de tiers indépendants peuvent être utiles pour choisir un prestataire informatique. Vous n'êtes pas obligé(e) de choisir un partenaire certifié. Mais il est recommandé que les prestataires informatiques puissent montrer qu'ils remplissent les exigences que vous posez et qu'ils peuvent assurer la disponibilité et la sécurité requises. Faites-le analyser ou confirmer par un service indépendant.

Il existe un grand nombre de normes et de guides différents. Les prestataires informatiques devraient bien connaître les ISO 27001, ISO 22301, ISO 9001 et ISO 14001 et y être conformes. Si d'autres normes sont utilisées, l'entreprise doit en prouver la conformité (Compliance Mapping). En cas de besoin de protection accru, vous devez formuler vos propres exigences.

Exemples de normes et guides:

Gestion de crise, continuité des activités, reprise d'activité après sinistre
> ISO 22301, Systèmes de management de la continuité des activités
> ISO 27031, Préparation des technologies de la communication et de l'information pour la continuité d'activité
> BS 11200, Crisis management: guidance and good practice

Sécurité des données et de l'information
> ISO 27001, Systèmes de management de la sécurité de l'information
> ISO 27701, Extension d'ISO 27001 au management de la protection de la vie privée
> ISO 30141, Architecture de référence de l'Internet des objets (IoT) – Confidentialité des données
> Orientation conforme au Règlement général de l'Union Européenne 2016/679 sur la protection des données (RGPD)
> NIST Cyber Security Framework

Guides techniques
> EN 50173, Systèmes de câblage générique
> EN 50600, Installations et infrastructures de centres de traitement de données
> ANSI/TIA-942, Centres de traitement de données

Autres (surtout pour les fournisseurs de matériel)
> ISO 9001, Systèmes de management de la qualité
> ISO 14001, Systèmes de management environnemental

Guide pour mandants
> ISO 22300, Sécurité et résilience — vocabulaire
> ISO 22318, Continuité de la chaîne d'approvisionnement
> ISO 27036, Sécurité d'information pour la relation avec le fournisseur
> ISO 31010, Management du risque

Impressum

Police cantonale bernoise, Centre national pour la cybersécurité (NCSC) et Réseau national de sécurité (RNS) pour le Réseau national de soutien aux enquêtes dans la lutte contre la criminalité informatique (NEDIK)

Avec la collaboration de l'Office d'information et d'organisation du canton de Berne (OIO), de l'Association des communes bernoises (ACB) et de l'Association des Communes Suisses (ACS)

Contact: Police cantonale zurichoise, NEDIK, cyc_nedik@kapo.zh.ch

Photographies: iStock

Ihre **POLIZEI**
Votre **POLICE**
La vostra **POLIZIA**

Kantonale und Städtische Polizeikorps
Corps de police cantonaux et municipaux
Corpi di polizia cantonali e comunali