Schweizerischer Verein des Gas- und Wasserfaches SVGW
Société Suisse de l'Industrie du Gaz et des Eaux SSIGE
Società Svizzera dell'Industria del Gas e delle Acque SSIGA
Swiss Gas and Water Industry Association SGWA

W1018 f Edition mars 2019

REGLEMENTATION

Recommandation

Norme minimale pour garantir les technologies de l'information et de la communication (TIC) requises pour l'approvisionnement en eau

Annexe 3 Recommandations destinées aux distributeurs d'eau desservant une zone avec moins de 5000 habitants

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'économie,
de la formation et de la recherche DEFR

Office fédéral pour l'approvisionnement économique du pays OFAE
Secrétariat domaine TIC

SSIGE, Grütlistrasse 44, case postale 2110, 8027 Zurich
Téléphone 044 288 33 33, Fax 044 202 16 33, www.ssige.ch

Schweizerischer Verein des Gas- und Wasserfaches SVGW
Société Suisse de l'Industrie du Gaz et des Eaux SSIGE
Società Svizzera dell'Industria del Gas e delle Acque SSIGA
Swiss Gas and Water Industry Association SGWA

W1018 f Edition mars 2019

REGLEMENTATION

Recommandation

Norme minimale pour garantir les technologies de l'information et de la communication (TIC) requises pour l'approvisionnement en eau

Annexe 3 Recommandations destinées aux distributeurs d'eau desservant une zone avec moins de 5000 habitants

IMPRESSUM

Font foi les conditions générales publiées à l'adresse suivante :
www.sssige.ch/CGV

En vente auprès de l'Administration de la SSIGE
(support@svgw.ch)

SSIGE, Grütlistrasse 44, case postale 2110, 8027 Zurich
Téléphone 044 288 33 33, Fax 044 202 16 33, www.ssige.ch

SOMMAIRE

1 Introduction

Les acteurs de l'approvisionnement en eau forment un groupe extrêmement hétérogène. Un outil d'évaluation séparé basé sur Excel est à la disposition des distributeurs d'eau dont la zone d'approvisionnement comprend plus de 5000 habitants. Quant aux distributeurs d'eau dont la zone d'approvisionnement compte moins de 5000 habitants, il leur est conseillé de mettre en œuvre les recommandations fournies ici.

2 Sécurité de l'information chez un petit distributeur d'eau

2.1 Axes prioritaires en matière de mesures

Afin d'accroître pleinement la sécurité de l'information dans une PME, il convient de prendre en compte les trois domaines que sont la technique, l'organisation et les processus, et le comportement personnel (fig. 1).

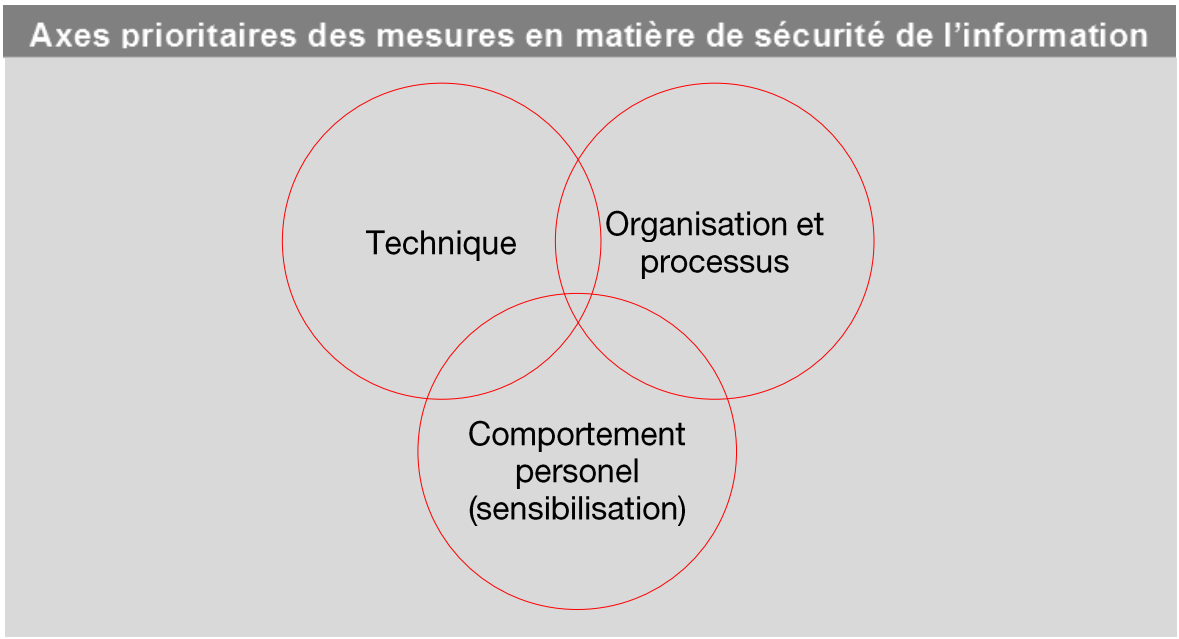

Fig. 1 Axes prioritaires des mesures en matière de sécurité de l'information

2.2 Technique

Les solutions techniques augmentent la complexité et coûtent cher. Il est judicieux de miser sur les bonnes pratiques et de renoncer à des expériences onéreuses. La liste suivante présente des exemples de mesures relevant des bonnes pratiques :

- deux centres de calcul sur différents sites ; systèmes redondants,
- un zonage réseau adapté,
- cryptage des appareils mobiles,
- pare-feu, filtre web, protection contre les maliciels,
- système de NAC (network access control, ou contrôle d'accès au réseau),
- logiciel de gestion des appareils mobiles,
- système électronique d'accès.

2.3 Organisation et processus

Les mesures organisationnelles sont appliquées là où les mesures techniques ne s'avèrent pas pertinentes et sont trop complexes. En voici quelques exemples :

- inventaire des actifs existants,
- processus d'attribution des autorisations (principe du double contrôle / double signature),
- prévention des situations d'urgence (p. ex. scénarios, alerte, organisation, mesures immédiates, décisions réservées, exploitation d'urgence, retour au fonctionnement normal),
- conclusion d'un accord de confidentialité avec les collaborateurs,
- conclusion d'un accord de confidentialité avec les partenaires externes,
- classification des documents,
- processus de gestion des risques,
- concept d'élimination.

2.4 Comportement individuel

Si l'être humain est capable d'identifier de nouvelles méthodes d'attaque et de mettre en place des mécanismes de protection ad hoc, il constitue aussi la plus grande menace. Cette ressource précieuse doit être utilisée au profit de la sécurité de l'information. Il s'agit de sensibiliser les personnes à un traitement responsable des informations et d'en appeler à la responsabilité individuelle. Voici quelques exemples :

- Toujours mettre son ordinateur portable et son porte-documents dans le coffre.
- Utiliser des mots de passe compliqués (dits « forts » ou « robustes »).
- Faire preuve de prudence en présence d'e-mails inconnus.
- Détruire les documents papier confidentiels (p. ex. au moyen d'une déchiqueteuse) et ne pas se contenter de les jeter à la poubelle.
- Ne pas passer d'appels téléphoniques confidentiels dans les lieux publics.

3 18 étapes pour améliorer la sécurité de l'information

3.1 Approche fondée sur les risques

L'approche fondée sur les risques permet à chaque distributeur d'eau (qu'il soit grand ou petit) de recenser le risque de manière autonome et d'établir sa propre propension au risque. Cette dernière peut varier fortement en fonction de la taille du service des eaux. Ainsi, il se peut qu'une défaillance des TIC soit plus facile à résoudre manuellement chez un petit distributeur d'eau que chez un grand.

3.2 Recommandations aux petits distributeurs d'eau

L'aide suivante s'adresse en particulier (mais pas seulement) aux distributeurs d'eau de plus petite taille, pour lesquels une mise en œuvre globale du cadre de cybersécurité est impossible. Elle ne remplace toutefois pas l'évaluation des risques ni la définition de sa propre propension au risque. Les recommandations suivantes sont considérées comme des aides et des instructions en matière de bonnes pratiques. Elles comprennent 18 points principaux (recommandations) comportant chacun plusieurs sous-éléments. L'exhaustivité de la mise en œuvre doit être adaptée à l'approche fondée sur les risques du service des eaux. En conséquence, il est possible d'appliquer certains ou la totalité des sous-éléments, voire des sous-éléments supplémentaires. L'essentiel est que le distributeur d'eau puisse prouver l'exhaustivité de la mise en œuvre en fonction de son approche fondée sur les risques et l'améliorer de façon cyclique.
L'aide suivante se base sur le programme en 10 points élargi de l'association InfoSurance[1] **:**

	Mesures pour une protection de base efficace[2]
1.	**Protégez vos données en faisant régulièrement des backups**
	Il existe différentes manières de perdre des données : elles peuvent être écrasées par erreur, rendues illisibles à cause d'un défaut sur le disque dur, voire détruites par un incendie ou un dégât des eaux. Vous pouvez éviter de tels désagréments en faisant régulièrement des backups de vos données. • En règle générale, il convient d'effectuer des backups de sécurité pour toutes les données dont le contenu est vital pour la poursuite de votre activité. De même, les configurations de logiciels devraient également faire l'objet de sauvegardes. • La fréquence de ces backups dépend de l'activité et de la taille de votre entreprise. Ceci dit, une PME devrait sauvegarder ses données au moins une fois par semaine. • Désignez par écrit les responsables des sauvegardes de sécurité et établissez une liste de contrôle des backups effectués. • Sauvegardez toujours vos données sur des supports mobiles (bande magnétique et autres supports amovibles). • De même, il serait bon d'effectuer des copies des documents importants pour lesquels vous ne disposez que d'une version papier (contrats ou autres) et de les conserver hors de l'entreprise. • Attention ! Certains documents comme les bilans, les comptes de résultat, les livres de comptes, les inventaires, les justificatifs comptables et la correspondance commerciale doivent être conservés pendant dix ans.

[1] InfoSurance – Plus de sécurité pour les systèmes informatiques des petites et moyennes entreprises (PME). Une protection accrue grâce au programme en 10 points élargi. https://www.kmu.admin.ch/kmu/fr/home/savoir-pratique/gestion-pme/infrastructure-ti/infrastructure-securite-ti.html. Sur ce site Internet, cliquer sur l'onglets Downloads, puis sur le premier lien vers « Plus de sécurité pour les systèmes informatiques des petites et moyennes entreprises (PME) ».

[2] Les recommandations sont considérées comme respectées lorsque tous les points ont été totalement mis en œuvre. L'exhaustivité de la mise en œuvre repose principalement sur l'approche fondée sur les risques de l'entreprise, et non sur les sous-éléments énumérés ici.

	• Vérifiez régulièrement que les données sauvegardées sur les supports de stockage sont accessibles. Une sauvegarde n'a de sens que si les données ont été correctement copiées sur le support. • Songez à sauvegarder vos données sur des supports externes. La sauvegarde de vos données sur un support externe représente un niveau supplémentaire de résilience, p. ex. en matière d'attaques par ransomware. En outre, dans la mesure du possible, les backups ne devraient pas être effectués au même endroit que les données originales.		
	Etat d'avancement de la mise en en œuvre		
	Totalement mis en œuvre Commentaire :	Partiellement mis en œuvre Commentaire :	Non mis en œuvre Commentaire :
2.	**Effectuez toujours les dernières mises à jour de votre antivirus.**		
	Des programmes nuisibles, tels que les virus et les vers, peuvent paralyser votre infrastructure TIC et mettre ainsi la vie de votre entreprise en péril. • Les virus informatiques peuvent modifier, corrompre, voire détruire complètement données et programmes. Ces programmes malveillants peuvent vous être transmis en pièce jointe d'un e-mail, par messagerie instantanée, etc. Sur Internet, ces virus sont souvent déguisés en programmes gratuits, pseudo-utiles ou de divertissement, et s'activent par un simple clic de souris. • Les systèmes informatiques mal protégés sont souvent pervertis pour propager des virus et pour lancer des attaques ciblées contre une société tierce. Un chef d'entreprise qui ne prend pas les mesures suffisantes afin de protéger ses systèmes informatiques fait preuve de négligence et s'expose à des poursuites pénales. • Un programme antivirus offre une protection contre les virus et vers connus. Il identifie les intrus et les met hors d'état de nuire. • Installez un programme antivirus sur tous les serveurs, postes de travail et ordinateurs portables. • Les cybercriminels ne cessent de mettre au point de nouveaux virus, raison pour laquelle il convient d'actualiser continuellement votre programme antivirus. Quoi qu'il en soit, les mises à jour doivent être effectuées chaque jour. • Demandez à vos collaborateurs de signaler immédiatement au responsable TIC les messages d'alerte aux virus.		
	Etat d'avancement de la mise en en œuvre		
	Totalement mis en œuvre Commentaire :	Partiellement mis en œuvre Commentaire :	Non mis en œuvre Commentaire :
3.	**Protégez votre navigation sur internet**		
	Si vous avez des portes coupe-feu dans votre entreprise, vous veillez certainement à ce qu'elles soient toujours bien fermées. Dans le monde d'Internet et de l'échange électronique de données, c'est le pare-feu qui remplit cette fonction sécuritaire. • En l'absence de pare-feu, des personnes non autorisées peuvent s'immiscer dans votre système informatique, exécuter des tâches à votre insu, utiliser votre ordinateur pour lancer des attaques illégales contre des tiers, ou encore accéder à des données commerciales pouvant relever de la loi sur la protection des données. • Vous trouverez dans le commerce des produits faisant office à la fois de pare-feu et d'antivirus. Ces produits combinés sont particulièrement indiqués pour les petites entreprises. • Plusieurs systèmes d'exploitation disposent d'un pare-feu intégré. Profitez systématiquement de cette possibilité et activez ces pares-feux.		

	• Si vous utilisez un réseau local sans fil (WLAN) dans votre entreprise, veillez à ce qu'il fonctionne correctement et soit sécurisé. • Toutes les passerelles réseau doivent être sécurisées par un pare-feu. • Tout le trafic Internet doit passer au crible du pare-feu. N'autorisez aucun autre accès à Internet (p. ex. via modem). • N'utilisez aucun ordinateur portable ou réseau local sans fil privé au sein de votre entreprise sans une protection ad hoc ni l'autorisation écrite du responsable TIC. • Protégez la configuration de votre pare-feu avec un mot de passe complexe.		
	Etat d'avancement de la mise en en œuvre		
	Totalement mis en œuvre Commentaire :	Partiellement mis en œuvre Commentaire :	Non mis en œuvre Commentaire :
4.	**Effectuez régulièrement les mises à jour de vos logiciels**		
	Contrôlez-vous régulièrement le niveau d'huile et la pression des pneus de votre voiture ? C'est souhaitable … De la même manière que vous entretenez régulièrement votre véhicule, vous devez veiller à ce que les programmes informatiques de votre entreprise soient régulièrement mis à jour pour être toujours parfaitement actualisés. • Les logiciels actuels contiennent souvent des millions de lignes codées. Or malgré les contrôles, il arrive parfois qu'une erreur s'y glisse. Pour un fabricant, il est pratiquement impossible de tester chaque application dans tous les environnements et configurations possibles C'est pourquoi les fabricants proposent régulièrement des patchs correctifs qui permettent de rectifier les erreurs connues. • Si vous ne mettez pas régulièrement vos logiciels à jour, des cybercriminels peuvent exploiter des failles connues pour manipuler des données ou abuser de votre infrastructure à des fins peu scrupuleuses. • Soyez le moins vulnérable possible en n'installant que les programmes dont vous avez vraiment besoin, et désactivez les services, validations de réseaux et autres protocoles inutiles. • Installez les tout derniers patchs correctifs de vos systèmes d'exploitation et applications. • Installez dès que possible les mises à jour de sécurité disponibles. • Installez les patchs sur tous les ordinateurs fixes et portables, y compris ceux de vos collaborateurs externes.		
	Etat d'avancement de la mise en en œuvre		
	Totalement mis en œuvre Commentaire :	Partiellement mis en œuvre Commentaire :	Non mis en œuvre Commentaire :
5.	**Choisissez des mots de passe compliqués**		
	Il suffit de connaître le nom et le mot de passe d'un utilisateur pour se connecter dans un système à sa place et abuser de son identité (informatique) et de tous ses droits d'accès ! Le vol de mots de passe permet ainsi aux cyberpirates d'accéder, à peu de frais, à des informations commerciales confidentielles. Faites-en sorte qu'on ne puisse usurper des identités au sein de votre entreprise. • Les mots de passe permettant d'accéder aux ordinateurs, systèmes d'exploitation et applications de votre entreprise doivent être modifiés immédiatement par le responsable TIC. • Invitez vos collaborateurs à choisir des mots de passe compliqués qu'ils devront changer régulièrement. Tous doivent être conscients du fait qu'ils seront tenus responsables des actions commises sous leur nom d'utilisateur.		

	• Les mots de passe complexes sont composés d'au moins 8 caractères, dont des majuscules, des minuscules, des chiffres et des caractères spéciaux. • N'utilisez pas de mots de passe contenant le nom, le numéro de passeport ou d'AVS, ou la date de naissance d'un de vos proches. • Ne vous servez pas de mots de passe pouvant se trouver dans un dictionnaire (toutes langues confondues). • N'écrivez jamais vos mots de passe sur un bout de papier, à moins de le conserver sous clé ! • Ne communiquez jamais votre mot de passe à des tiers.		
	Etat d'avancement de la mise en en œuvre		
	Totalement mis en œuvre Commentaire :	Partiellement mis en œuvre Commentaire :	Non mis en œuvre Commentaire :
6.	**Protégez vos appareils mobiles**		
	Les téléphones mobiles et ordinateurs portables en connexion WLAN sont à la fois pratiques et multitâches. Mal employés, ces appareils représentent cependant un risque important pour la sécurité. Quiconque est tenu, pour des raisons professionnelles, de stocker des données sensibles sur un appareil mobile doit prendre des mesures spéciales. • Tous les appareils mobiles doivent être protégés par un mot de passe compliqué (cf. point 5), et les données doivent être stockées sous forme cryptée. Sinon, des personnes non autorisées pourraient accéder aux informations commerciales de votre entreprise en cas de perte ou de vol d'un portable. • Les appareils mobiles ne devraient contenir que les données strictement nécessaires à leur fonction. • Il faut régulièrement contôler les appareils mobiles pour détecter les logiciels malveillants (par ex. virus), car ils sont synchronisés avec les autres ordinateurs de l'entreprise (via les fonctions de messagerie électronique, par ex.). • Une connexion WLAN mal configurée peut permettre aux cybercriminels de s'immiscer, en quelques minutes et à une distance de plus d'un kilomètre, dans le réseau de votre entreprise. Il convient de réglementer tout particulièrement l'utilisation de points d'accès publics et externes à Internet (HotSpots). • Activez le Bluetooth sur vos appareils (téléphones et ordinateurs portables) uniquement en cas de besoin et à l'abri des regards indiscrets. Autrement, votre appareil peut réagir à votre insu à des sollicitations étrangères (dans un rayon allant jusqu'à 100 mètres). • Activez le cryptage du transfert de données sans fil (WPA2). • Pour acheminer des données confidentielles, utilisez exclusivement des connexions protégées par un réseau privé virtuel (VPN).		
	Etat d'avancement de la mise en en œuvre		
	Totalement mis en œuvre Commentaire :	Partiellement mis en œuvre Commentaire :	Non mis en œuvre Commentaire :
7.	**Expliquez vos directives pour l'utilisation des TIC**		
	Sans directives claires et contraignantes, vos collaborateurs ne savent pas ce qu'ils ont le droit de faire et de ne pas faire en tant qu'utilisateurs des TIC. Mais les règles ne sont véritablement prises au sérieux que si elles sont respectées par les supérieurs. Vous devez donc servir d'exemple pour tous les aspects liés à la sécurité. • Formulez par écrit les directives pour l'utilisation des TIC comme composante des conditions d'engagement et informez les collaborateurs.		

	• Abordez régulièrement le problème de la sécurité dans votre entreprise en variant les approches. • Organisez des campagnes de sensibilisation sur ce thème une ou deux fois par an. C'est facile à réaliser et cela nécessite très peu de moyens : courriels à l'ensemble de vos collaborateurs, circulaires internes, affichage à la cantine, articles dans le journal de l'entreprise, etc. • Organisez une formation de base pour tous vos collaborateurs (en vous inspirant de cette brochure, p. ex.). Les principaux objectifs d'apprentissage sont les suivants : – Avantages de la sécurité des TIC – Création de mots de passe compliqués – Utilisation sécurisée d'Internet, de la messagerie électronique et de l'antivirus – Classement des documents • Définissez – l'installation et l'utilisation de programmes et matériel n'appartenant pas à la sphère de l'entreprise (jeux, clés USB, ordinateurs portables privés, etc.), – la navigation sur Internet (ce qui est permis et ce qui ne l'est pas), – l'utilisation de la messagerie électronique (confidentialité, transfert, adresses e-mail privées, chaînes de lettres, etc.), – le traitement des informations confidentielles, – la procédure à suivre en cas d'incident lié à la sécurité. • Informez vos collaborateurs des sanctions auxquelles ils s'exposent s'ils ne respectent pas ces directives.		
	Etat d'avancement de la mise en en œuvre		
	Totalement mis en œuvre Commentaire :	Partiellement mis en œuvre Commentaire :	Non mis en œuvre Commentaire :
8.	**Protégez l'environnement de votre infrastructure TIC**		
	Savez-vous qui entre et qui sort de votre entreprise chaque jour ? Quelques dispositions suffisent pour éviter que des personnes non autorisées puissent accéder à des informations commerciales importantes. Un système de sécurité visible et dynamique est aujourd'hui un critère de qualité qui ne manquera pas d'inspirer confiance à vos clients et à vos fournisseurs. À quoi bon s'équiper du meilleur pare-feu si des inconnus peuvent s'introduire dans vos bureaux ? • Tous les accès à vos locaux et au site de votre entreprise doivent être fermés ou surveillés. Si cela est impossible, limitez-vous à la partie bureaux. • Ne permettez pas aux visiteurs, clients et connaissances de circuler sans surveillance dans votre entreprise. • Toute personne tierce à l'entreprise doit être accueillie à la réception, accompagnée pendant toute la durée de sa visite et raccompagnée jusqu'à la sortie. • Si vous n'avez pas de réception permettant de surveiller l'accès, il convient de verrouiller la porte d'entrée et d'apposer une plaque « Prière de sonner ». • Assurez-vous que toutes les ouvertures (fenêtres, portes, etc.) disposent d'un système de protection efficace contre les effractions. • Clés et badges doivent être correctement gérés et leurs listes mises à jour. Soyez parcimonieux dans la distribution des passe-partout, dont il convient de réexaminer la nécessité des autorisations au moins une fois par an. • Les collaborateurs qui quittent définitivement l'entreprise doivent remettre leurs clés, badges et autres droits d'accès. • Installez votre serveur dans un local climatisé et fermant à clé. Si cela est impossible, enfermez-le dans un caisson (rack). • N'entreposez pas d'objets inflammables tels que du papier, ni dans le local du serveur, ni à proximité immédiate.		

	• Ne placez pas d'imprimante réseau dans des pièces accessibles au public afin de protéger vos documents des regards indiscrets. • Enfermez les câbles de connexion réseau qui traversent les pièces accessibles au public. Même chose pour vos modems, stations centrales (hubs), routeurs et commutateurs (switchs). • Il devrait être interdit aux visiteurs d'utiliser des appareils d'enregistrement (téléphone portable, etc.) dans les zones sensibles de leur distributeur d'eau.		
	Etat d'avancement de la mise en œuvre		
	Totalement mis en œuvre Commentaire :	Partiellement mis en œuvre Commentaire :	Non mis en œuvre Commentaire :

	Mesures pour améliorer la confidentialité		
9.	**Réglementez la protection de l'accès aux données**		
	Il est possible d'utiliser abusivement des informations par le biais d'un accès non autorisé. Protégez par conséquent vos données de façon appropriée, de sorte que seules les personnes habilitées puissent y accéder. • Quiconque accède à des données sans autorisation est susceptible de les consulter, de les copier, de les modifier ou de les supprimer. • Établissez qui est habilité à accéder à telle ou telle application TIC ou information. Il convient d'attribuer les droits d'accès selon la fonction occupée (p. ex. secrétariat, vente, comptabilité, ressources humaines, administrateur système). • On prendra soin par ailleurs d'accorder uniquement les droits d'accès nécessaires à l'exécution des tâches de chacun (selon le principe de connaissance sélective). Les droits d'accès seront établis à chaque fois par la personne responsable. • Le régime des autorisations doit faire l'objet d'une documentation. Il s'agit de consigner, pour chacun de vos collaborateurs, la fonction occupée au sein de l'entreprise et les droits d'accès correspondants (applications et données). Ces autorisations devront être régulièrement passées en revue et adaptées en conséquence. • Lorsque des collaborateurs quittent définitivement l'entreprise ou en cas de changements dans l'organigramme interne, il faut bloquer ou modifier immédiatement les comptes utilisateur correspondants, ainsi que les droits d'accès y afférents. • Les comptes des responsables systèmes et des administrateurs feront l'objet d'une attention particulière, dans la mesure où ils disposent généralement de droits très étendus.		
	État d'avancement de la mise en œuvre		
	Totalement mis en œuvre Commentaire :	Partiellement mis en œuvre Commentaire :	Non mis en œuvre Commentaire :
10.	**Verrouillez l'accès à vos supports mobiles et cryptez les données lors des transferts**		
	Le transfert non sécurisé de données confidentielles (par e-mail, p. ex.) peut les exposer au regard de tiers. En cas de perte de vos appareils mobiles, vos données risquent de tomber entre de mauvaises mains. Pour garantir la confidentialité de vos données, vous devez procéder à leur cryptage aussi bien pour les stocker sur vos appareils que lors des transferts. • Les courriels peuvent être lus par des tiers. Il convient donc de crypter les e-mails dont le contenu est confidentiel (p. ex. envoi avec IncaMail).		

	• Les appareils mobiles tels que les ordinateurs portables doivent en général faire l'objet d'un cryptage. • Pour acheminer des données confidentielles, utilisez exclusivement des connexions protégées par un réseau privé virtuel (VPN) (cf. point 6).		
	État d'avancement de la mise en œuvre		
	Totalement mis en œuvre Commentaire :	Partiellement mis en œuvre Commentaire :	Non mis en œuvre Commentaire :
11.	**Sensibilisez vos collaborateurs**		
	Vos collaborateurs n'appliqueront les mesures de sécurité que s'ils sont sensibilisés au problème. Expliquez-leur la raison de ces mesures et le comportement à adopter lorsqu'ils ont à traiter des données confidentielles. Faites signer un accord de confidentialité à votre personnel et à vos partenaires externes. • Vos collaborateurs, qu'ils soient internes ou externes à l'entreprise, traitent souvent des données confidentielles. Ces personnes doivent donc être conscientes qu'il leur incombe de prendre les mesures correspondantes pour garantir la confidentialité de ces informations. • Incluez une clause de confidentialité dans le contrat de travail de vos collaborateurs. De même, créez un cadre contractuel pour régir vos rapports avec les collaborateurs externes et les partenaires. Cet accord de confidentialité fixe les règles relatives à la protection et à l'utilisation des informations confidentielles. • Sensibilisez les nouveaux collaborateurs dès leur embauche aux questions liées à la sécurité des TIC. • Informez vos collaborateurs des sanctions auxquelles ils s'exposent s'ils ne respectent pas les directives.		
	Etat d'avancement de la mise en en œuvre		
	Totalement mis en œuvre Commentaire :	Teilweise umgesetzt. Kommentar:	Non mis en œuvre Commentaire :
12.	**Réglementez l'élimination des informations et des supports de données**		
	Les informations confidentielles peuvent tomber entre de mauvaises mains si elles ne sont pas correctement éliminées. Expliquez à vos collaborateurs comment éliminer les données et les supports (sous forme papier ou électronique) de manière sûre et respectueuse de l'environnement. • Réglementez l'élimination : – des vieux papiers (journaux, publicités et autres documents publics) – de tous les autres documents internes et confidentiels – du carton – des supports de données électroniques tels que les clés USB, les CD et les disques durs externes • Définissez la manière dont les archives doivent être éliminées. • Informez vos collaborateurs des sanctions auxquelles ils s'exposent s'ils ne respectent pas les directives.		
	Etat d'avancement de la mise en en œuvre		
	Totalement mis en œuvre Commentaire :	Partiellement mis en œuvre Commentaire :	Non mis en œuvre Commentaire :

	Massnahmen für mehr Verfügbarkeit		
13.	**Vérifiez vos systèmes TIC**		
	Vos systèmes TIC doivent toujours être opérationnels à 100 %. C'est pourquoi ils doivent faire l'objet d'une maintenance régulière et correcte, qui limitera les perturbations et préviendra les dommages. • Contrôlez régulièrement le fonctionnement de vos systèmes TIC : – Le système de backup est-il au point ? – Les données sauvegardées sont-elles effectivement lisibles ? – L'alimentation sans interruption (ASI) est-elle opérationnelle ? – Y a-t-il des messages d'erreur dans l'historique système ? • Prenez également en compte les aspects organisationnels : – Les dispositions légales et autres directives sont-elles respectées ? – Le plan d'urgence a-t-il été vérifié ? • Les opérations de contrôle et de maintenance doivent avoir lieu à intervalles réguliers. • Établissez une liste de maintenance : – Quel équipement doit être vérifié et entretenu, quand et par qui. – Veillez à ce que les opérations de maintenance soient contrôlables et compréhensibles. • Faites signer un accord de confidentialité au personnel externe chargé de la maintenance (cf. point 11).		
	Etat d'avancement de la mise en en œuvre		
	Totalement mis en œuvre Commentaire :	Partiellement mis en œuvre Commentaire :	Non mis en œuvre Commentaire :
14.	**Protégez l'accès au réseau de votre entreprise par une authentification à deux facteurs**		
	Pour des raisons de sécurité, l'accès externe au réseau de l'entreprise présuppose une authentification à deux facteurs (aussi appelée authentification à double facteur ou bifactorielle). Considérée comme la norme industrielle usuelle, cette dernière offre une protection adéquate. • Définissez les variantes d'accès possibles telles que : – l'accès basé sur les applications – l'accès basé sur le réseau – l'accès VPN de site à site • Définissez des catégories (collaborateurs internes et externes, clients, fournisseurs et invités) et déterminez quelle variante d'accès est associée à quel groupe de personnes et à quel service.		
	Etat d'avancement de la mise en en œuvre		
	Totalement mis en œuvre Commentaire :	Partiellement mis en œuvre Commentaire :	Non mis en œuvre Commentaire :
15.	**Équipez vos ordinateurs d'une alimentation sans interruption**		
	Si votre activité nécessite de hauts niveaux de disponibilité de vos données et de vos systèmes TIC, vous ne pouvez pas vous permettre de subir la moindre défaillance. Une alimentation sans interruption (ASI) protège vos systèmes d'une coupure de courant et des pics de tension (dus p. ex. à la foudre), permettant ainsi d'éviter la perte de données. • L'alimentation sans interruption (ASI) doit être branchée entre la source d'électricité habituelle et les appareils à protéger.		

	• En cas de panne de courant, la batterie de l'ASI prend le relais et se charge d'alimenter les composants de façon à ce qu'ils puissent s'éteindre normalement. • De plus, une ASI peut agir comme un filtre et protéger vos systèmes contre les fluctuations de tension. • Outre votre serveur, d'autres périphériques importants doivent être raccordés à l'ASI. Il s'agit notamment des principaux ordinateurs du réseau, des routeurs et des systèmes de backup. • Listez les composants qui doivent être reliés à l'ASI. Cette liste vous permettra de déterminer la puissance nécessaire de l'ASI. • Contrôlez régulièrement les batteries de l'ASI et remplacez-les immédiatement le cas échéant (cf. point 13).		
	Etat d'avancement de la mise en en œuvre		
	Totalement mis en œuvre Commentaire :	Partiellement mis en œuvre Commentaire :	Non mis en œuvre Commentaire :
16.	**Misez sur la redondance des éléments importants**		
	La défaillance d'un élément essentiel de votre réseau, comme un serveur, peut coûter très cher et perturber l'exploitation. Beaucoup d'entreprises ignorent à quel point elles dépendent de systèmes critiques. Pour permettre à votre société de reprendre son activité le plus rapidement possible après une panne, il est recommandé de disposer de systèmes TIC redondants (p. ex. disques durs, composants réseau ou serveurs complets). • La redondance signifie que vous disposez d'au moins un appareil ou système de remplacement identique à même de prendre la relève en cas de défaillance. • Pour prévenir une panne de disque dur, on peut recourir à la méthode de la mise en miroir de disques. En cas de défaillance du disque dur, d'autres disques durs prennent automatiquement le relais, sans que l'exploitation soit interrompue. Il convient de conserver les données importantes de façon géo-redondante. • Concluez des contrats de service avec vos fournisseurs de matériel informatique et de logiciels, dans lesquels figureront les temps de réaction, les délais de livraison, etc. • Vous pouvez également élaborer avec eux des plans pour les scénarios d'urgence (cf. point 17). • N'utilisez que des composants de marques réputées, dans la mesure où ils sont généralement de bonne qualité et ont été soumis à des tests intensifs. • En plus de la redondance de vos systèmes TIC, songez également à une connexion Internet redondante. • L'essentiel est que vos appareils de remplacement soient identiques et déjà préconfigurés afin de pouvoir prendre immédiatement le relais en cas d'événement.		
	Etat d'avancement de la mise en en œuvre		
	Totalement mis en œuvre Commentaire :	Partiellement mis en œuvre Commentaire :	Non mis en œuvre Commentaire :
17.	**Établissez un plan d'urgence**		
	Personne n'est à l'abri d'une catastrophe et on se sent souvent impuissant face aux situations les plus graves. Mais savoir quel comportement adopter en cas d'urgence peut permettre de limiter le sinistre. Il est donc nécessaire de planifier à l'avance la conduite à tenir et les actions à mettre en œuvre. • Envisagez les situations d'urgence susceptibles de se présenter dans votre entreprise et réfléchissez à la façon dont il faudrait réagir dans les différents cas. Imaginez les scénarios suivants : panne des TIC, incapacité du personnel, perte des postes de travail ou des locaux et défaillances de partenaires externes et prestataires de services.		

	• En cas d'urgence, il faut donner l'alerte rapidement et agir vite. Chacun doit savoir exactement qui est la personne responsable et qui alerter. Pour cela, établissez un plan d'alerte et définissez les responsabilités. • Élaborez un plan d'urgence. Il prévoit notamment les mesures immédiates à prendre pour déclencher l'exploitation d'urgence, les dispositions régissant le déroulement des opérations et les actions visant à rétablir rapidement le fonctionnement normal de l'entreprise. • Enseignez à vos collaborateurs la conduite à tenir en cas d'urgence et les mesures immédiates à prendre. • L'être humain réagit souvent de façon intuitive en situation de stress. C'est pourquoi il convient d'entraîner sa capacité à adopter la bonne conduite en situation critique. • Documentez correctement tous vos composants TIC. Conservez cette documentation à l'extérieur de votre entreprise. • Cette documentation contiendra notamment une liste des utilisateurs, des groupes et des différentes autorisations (cf. point 9), le plan du réseau, les configurations des systèmes, la description des installations, les concepts, les procédures de travail et la description des postes d'intérêt stratégique pour la sécurité. Procédez régulièrement à la mise à jour de cette documentation. • Étudiez un mode de fonctionnement dégradé pour les systèmes TIC. Celui-ci devra garantir un niveau maximal de disponibilité afin de permettre une reprise rapide de l'activité. • Testez le temps de réaction du système de secours selon vos besoins en disponibilité. Une panne de serveur peut-elle vraiment être réparée dans le temps imparti ?		
	Etat d'avancement de la mise en en œuvre		
	Totalement mis en œuvre Commentaire :	Partiellement mis en œuvre Commentaire :	Non mis en œuvre Commentaire :
18.	**Diffusez le savoir-faire**		
	Chez les distributeurs d'eau de plus petite taille, les connaissances stratégiques sur les systèmes TIC (p. ex. SCADA) sont souvent détenues par une seule et même personne. En cas d'absence ou de départ de cette dernière, l'entreprise risque de se trouver en difficulté. • Le savoir stratégique repose sur la capacité à configurer, à faire fonctionner et à entretenir les systèmes TIC de l'entreprise. Faites-en sorte que ce savoir soit documenté et partagé par plusieurs personnes. • La maladie, un accident, le décès ou le départ de votre responsable TIC peut provoquer la perte de ce précieux savoir. • Pour éviter une telle perte en cas de défaillance, veillez à ce que les systèmes et processus essentiels fassent l'objet d'une documentation. Cela aidera également les successeurs et les nouveaux collaborateurs à se repérer rapidement. • Conservez les mots de passe importants en double (p. ex. dans un coffre). • Sécurisez les informations significatives liées aux activités des collaborateurs qui quittent l'entreprise.		
	Etat d'avancement de la mise en en œuvre		
	Totalement mis en œuvre Commentaire :	Partiellement mis en œuvre Commentaire :	Non mis en œuvre Commentaire :

Tab. 1 18 étapes pour améliorer la sécurité des TIC

4 Appendice

4.1 Liste des figures

4.2 Liste des tableaux