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 4 Exemples de mis en œuvre

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

SOMMAIRE

1 Introduction 5

2 Exemple de mise en œuvre n° 1 (grand distributeur d'eau) 6

2.1 Vue d'ensemble de Spécimen SA 8
2.2 Étendue de l'évaluation 9
2.3 Aperçu des résultats 10
2.4 Recommandations d'action 13
2.5 Conclusion 14

3 Exemple de mise en œuvre n° 2 (distributeur d'eau de taille moyenne) 15

3.1 Vue d'ensemble de Modèle2 SA 17
3.2 Assessment-Scope (Assessment-Umfang) 18
3.3 Aperçu des résultats 19
3.4 Recommandations d'action 23
3.5 Conclusions 27

4 Exemple de mise en œuvre n° 3 (petit distributeur d'eau) 28

4.1 Vue d'ensemble de Modèle3 SA 30
4.2 Aperçu des résultats 31
4.3 Conclusions 44

5 Appendix 45

5.1 Liste des figures 45
5.2 Liste des tableaux 45

Rapport sur la cybersécurité du distributeur d'eau Modèle3 SA

Rapport d'évaluation conformément à la norme minimale TIC OFAE/SSIGE pour les distributeurs d'eau desservant moins de 5000 habitants

Basé sur la norme minimale TIC pour l'approvisionnement en eau | Version 0.12, 2018 (04 mai 2018)

4 Exemple de mise en œuvre n° 3 (petit distributeur d'eau)

Equipe d'auditeurs/rédaction

Nom	Prénom	Organisation	Fonction
Walder	Dario	OFAE	Auditeur/direction de projet

Interlocuteurs au sein de Modèle3 SA

Nom	Prénom	Organisation	Fonction
Sandra	Muster	Modèle3 SA	Fontanière
Peter	Muster	Modèle3 SA	Membre du conseil

Le contenu de ce rapport d'évaluation est « ~~CONFIDENTIEL~~ » et s'adresse exclusivement à Modèle3 SA.

Exclusion de responsabilité

Le présent document présentant les résultats d'évaluation conformément à la norme minimale TIC OFAE/SSIGE (état au 04.05.2018) a été élaboré en toute bonne foi par les auditeurs. L'Office fédéral pour l'approvisionnement économique du pays (OFAE), les associations impliquées (p. ex. SSIGE), les experts et les entreprises, ainsi que les collaborateurs ou l'équipe d'auteurs déclinent toute responsabilité, qu'elle soit expresse ou implicite. La responsabilité relative à de potentiels dommages ainsi qu'à la sécurité d'exploitation incombe uniquement aux utilisateurs).

Synthèse

L'Office fédéral pour l'approvisionnement économique du pays[18] (OFAE) et la Société Suisse de l'Industrie du Gaz et des Eaux[19] (SSIGE) recommandent depuis 2018 la mise en œuvre de la norme minimale TIC pour l'approvisionnement en eau. Pour les distributeurs d'eau dont la zone d'approvisionnement englobe plus de 5000 habitants, un cadre de cybersécurité complet (annexe 2 de la norme minimale TIC) ainsi qu'un outil d'évaluation basé sur Excel est mis à disposition. L'entreprise Modèle3 SA approvisionne quant à elle moins de 5000 habitants : elle est par conséquent tenue d'appliquer les recommandations simplifiées de l'annexe 3 de la norme minimale TIC (programme en 18 points). Le présent rapport présente de façon claire les résultats de l'évaluation basée sur ces recommandations et fournit des recommandations d'action en vue d'améliorer les points faibles identifiés.

La présente évaluation vise à déterminer l'état d'avancement de la mise en œuvre, par Modèle3 SA, des 18 points recommandés pour les petits distributeurs d'eau dans le cadre de la norme minimale TIC de l'OFAE/SSIGE. Pour 13 des 18 points, le niveau de maturité du distributeur répond aux recommandations de la norme. En revanche, cinq d'entre eux restent à améliorer pour atteindre le niveau de sécurité préconisé.

Modèle3 SA exploite elle-même son système de gestion des processus au sein du poste de commande, mais elle a externalisé dans le cloud tous les autres services (p. ex. hébergement de messagerie électronique). L'organisation aborde activement les questions de cybersécurité et de sécurité d'exploitation de l'installation. L'évaluation conforme aux recommandations destinées aux distributeurs d'eau approvisionnant moins de 5000 habitants a confirmé ce constat. 13 des 18 mesures pour une protection de base efficace sont appliquées en intégralité par Modèle3 SA, ou le risque correspondant est connu et accepté. Cinq des mesures ne sont que partiellement mises en œuvre et nécessitent les actions suivantes :

- **Mise à jour régulière des logiciels antivirus** (surtout sur les appareils personnels ayant accès au système de gestion des processus) ainsi que des systèmes d'exploitation.
- **Attribution de comptes individuels** dotés de mots de passe sûrs, notamment pour le système de gestion des processus.
- **Test de l'alimentation électrique sans interruption** et si possible également de l'exploitation en îlot (fonctionnement de la distribution d'eau par l'utilisation du courant autoproduit).
- **Élaboration et application de directives** pour l'utilisation d'appareils mobiles avec accès au SGP.
- **Vérification régulière des progrès dans la mise en œuvre** des présentes recommandations et réalisation cyclique d'une évaluation de cybersécurité conformément aux recommandations (annexe 3) de la norme minimale TIC de l'OFAE/SSIGE.

[18] Site de l'approvisionnement économique du pays : www.bwl.admin.ch [consulté le 27 avril 2018].

[19] Site de la Société Suisse de l'Industrie du Gaz et des Eaux : www.ssige.ch [consulté le 27 avril 2018].

4.1 Vue d'ensemble de Modèle3 SA

Modèle3 SA met à disposition des ménages, ainsi que de l'industrie et des commerces, de l'eau potable ainsi que de l'eau sanitaire. Elle approvisionne …[20] habitants. Elle assure également la fourniture d'eau en quantité suffisante pour lutter contre les incendies.

Organisation
Le distributeur d'eau s'acquitte de sa mission de façon autonome et sous sa propre responsabilité. Il collabore avec d'autres communes et des tiers, notamment avec la commune …[21], dans la mesure où cela est nécessaire à l'exécution appropriée et économique de sa mission. L'organisation est …

Collecte des eaux
La collecte des eaux a majoritairement lieu dans les sources de …[22].

Organisation informatique
Modèle3 SA repose majoritairement sur une organisation autonome et n'est rattachée à aucune commune, ni aucun canton du point de vue informatique. Elle entretient elle-même son système de gestion des processus et bénéficie dans ce cadre du soutien du fabricant. À l'inverse, la majeure partie de l'informatique de bureau est externalisée (p. ex. services de messagerie sur le cloud ou stockage de données auprès de …[23] (cloud)). Ainsi, hormis le serveur (matériel) destiné au système de gestion des processus, Modèle3 SA n'exploite aucun matériel elle-même. Même les appareils de travail pour l'accès à distance (p. ex. ordinateurs portables) sont achetés par les collaborateurs eux-mêmes (BYOD[24]).

Modèle3 SA travaille en étroite collaboration avec le distributeur d'eau …[25]. Dans la mesure où Modèle3 SA ne dispose que d'un accès limité aux ressources humaines, une collaboration avec le distributeur …[26] a été visée dans le cadre du service de piquet Ce dernier dispose par conséquent d'un accès dédié au système de gestion des processus de Modèle3 SA (et vice versa) et peut, si nécessaire, intervenir en prenant le contrôle. Le raccordement au réseau de conduites (eau) des distributeurs …[27] et …[28] constitue un autre aspect des efforts de résilience existants. Le distributeur …[29] possède notamment assez de capacités pour soutenir de manière satisfaisante Modèle3 SA en cas de perturbation. Modèle3 SA exploite à cette fin (ainsi que pour le fonctionnement normal en hiver) deux pompes lui appartenant au sein d'une station de pompage du distributeur …[30].

[20] Pour des raisons de confidentialité, aucune information permettant d'identifier l'organisation examinée n'est publiée

[21] Ibid.

[22] Ibid.

[23] Ibid.

[24] BYOD: Bring your own device. Ce concept désigne notamment l'utilisation d'appareils mobiles privés ayant accès au système de gestion des processus.

[25] Pour des raisons de confidentialité, aucune information permettant d'identifier l'organisation examinée n'est publiée.

[26] Ibid.

[27] Ibid.

[28] Ibid.

[29] Ibid.

[30] Ibid.

4.2 Aperçu des résultats

Modèle3 SA exploite elle-même son système de gestion des processus au sein du poste de commande, mais elle a externalisé dans le cloud tous les autres services (p. ex. hébergement de messagerie électronique). L'organisation aborde activement les questions de cybersécurité et de sécurité d'exploitation de l'installation. L'évaluation conforme aux recommandations destinées aux distributeurs d'eau approvisionnant moins de 5000 habitants a confirmé ce constat. 13 des 18 mesures pour une protection de base efficace sont appliquées en intégralité par Modèle3 SA. Cinq des mesures ne sont que partiellement mises en œuvre et nécessitent encore des actions :

- **Mesure 2 (effectuez toujours les dernières mises à jour de votre antivirus)** : cet aspect n'est que partiellement mis en œuvre par Modèle3 SA. Une politique en matière d'antivirus ne s'appliquant pas uniquement au système de gestion des processus (SGP), mais aussi aux appareils personnels, est nécessaire, notamment en raison du concept de BYOD. La gestion des antivirus sur le serveur dans le poste de commande ainsi que tous les autres appareils (p. ex. ordinateurs portables personnels avec accès au SGP) doivent être consignée par écrit et faire l'objet d'une communication.
- **Mesure 4 (effectuez régulièrement les mises à jour de vos logiciels) :** cet aspect n'est que partiellement mis en œuvre par Modèle3 SA. Il est recommandé de consigner par écrit les directives concernant le système d'exploitation pour le SGP et les appareils personnels des collaborateurs ayant accès au SGP.
- **Mesure 5 (choisissez des mots de passe compliqués) :** cet aspect n'est que partiellement mis en œuvre par Modèle3 SA, notamment parce que le système d'exploitation du serveur SGP n'est actuellement protégé que par un mot de passe commun. Il est recommandé à Modèle3 SA d'instaurer également des mots de passe individualisés pour chaque utilisateur, même au sein du système d'exploitation Windows destiné au serveur SGP.
- **Mesure 6 (protégez vos appareils mobiles) :** cet aspect n'est que partiellement mis en œuvre par Modèle3 SA, en raison de sa taille et des ressources disponibles, notamment car il n'existe aucune directive concernant les appareils privés des collaborateurs, qui sont cependant susceptibles d'accéder au SGP. Élaborez et communiquez des directives claires en matière d'actualisation régulière des antivirus et des autres logiciels sur les appareils mobiles disposant d'un accès au SGP (voir également recommandation d'action au point 4).
- **Mesure 13 (vérifiez vos systèmes TIC) :** cet aspect n'est que partiellement mis en œuvre par Modèle3 SA. L'ASI ne fait pas encore l'objet de tests réguliers. Un processus de test régulier de l'ASI doit être élaboré et appliqué de façon correspondante. Ce test pourrait par exemple faire l'objet d'une discussion avec le fabricant lors de la réception du nouveau SGP.

Les résultats de l'évaluation de cybersécurité conformément à la norme minimale TIC de l'OFAE/SSIGE (au 20 mai 2018) sont présentés en détails ci-après :

	Mesures pour une protection de base efficace[31]		
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 10 ans. • 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.		
	État d'avancement de la mise en œuvre		
	Entièrement mis en œuvre Commentaire : Cet aspect est mis en œuvre conformément à la taille et aux ressources disponibles de Modèle3 SA, toutefois, un potentiel d'optimisation subsiste en matière de backup et il devrait porter sur l'approvisionnement en eau en fonction des ressources disponibles.	Partiellement mis en œuvre Commentaire :	Non mis en œuvre Commentaire :
	Le fontainier est responsable de la réalisation régulière des sauvegardes (backup). Il les effectue personnellement chaque semaine (le vendredi). Les backups concernent notamment les données système du système de gestion des processus. Parallèlement au backup sur place, le fabricant du système effectue également une sauvegarde du système de gestion des processus. Les modalités et l'ampleur de cette sauvegarde sont définies par Mo-dèle3 SA dans le cadre d'un service level agreement (SLA) avec le fabricant. L'intégrité de la sauvegarde est vérifiée visuellement par le surveillant d'exploitation (ou le fontainier). Ce dernier n'est cependant pas chargé de lire activement et de vérifier simultanément le backup et les processus de rétablissement, que ce soit de façon autonome ou avec l'aide du fabricant. Les données de bureau (e-mails, contrats, etc.) peuvent être stockées sur le cloud. Les documents importants, comme les contrats signés, sont conservés dans les archives de la commune. Une copie de chaque document est effectuée et sauvegardée sur le cloud. Des SLA définissant les modalités du stockage sont établis avec le fournisseur de service de cloud. Recommandation d'action : • Pour assurer la fonctionnalité de la sauvegarde ainsi que du processus de rétablissement et son fonctionnement correct, même en cas de crise, il est recommandé de s'exercer à pratiquer le processus de rétablissement, dans l'idéal via la sauvegarde. Il est en outre possible de discuter du processus de rétablissement avec le fabricant et de vérifier les SLA correspondants. Ce dernier doit garantir à Modèle3 SA qu'il est en mesure de rétablir le système de gestion des processus dans le délai défini, en cas de perturbation brutale. • Les tâches et les responsabilités du fontainier en matière de backup doivent être consignées par écrit et communiquées, notamment aux nouveaux arrivants.		

[31] On considère les recommandations comme respectées lorsqu'elles sont entièrement mises en œuvre. L'exhaustivité de la mise en œuvre se détermine en première ligne en fonction de l'approche basée sur le risque de l'entreprise et non en fonction des sous-rubriques indiquées ici.

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.		
	État d'avancement de la mise en œuvre		
	Totalement mis en œuvre Commentaire :	Partiellement mis en œuvre Commentaire : Cet aspect est partiellement mis en œuvre par Modèle3 SA. Une politique en matière d'antivirus est nécessaire, non seulement pour le SGP mais aussi pour les appareils personnels, notamment en raison du concept BYOD.	Non mis en œuvre Commentaire :
	Modèle3 SA exploite son propre serveur pour le fonctionnement du système de gestion des processus. Ce serveur n'est accessible que via un pare-feu depuis l'extérieur du poste de commande. Le PC au sein du poste de commande est lui-même protégé par un antivirus. Celui-ci est automatiquement actualisé chaque jour et son bon fonctionnement est assuré par le surveillant d'exploitation. Quatre personnes (surveillant d'exploitation, fontainier, fontainier suppléant, responsable des stations de pompage) ont accès au système de gestion des processus via VPN à partir de leurs appareils personnels. Il n'existe aucune directive concernant l'actualisation de l'antivirus sur les appareils personnels. Recommandation d'action : • La gestion des antivirus sur le serveur dans le poste de commande ainsi que tous les autres appareils (p. ex. ordinateurs portables personnels avec accès au SGP) doivent être consignée par écrit et faire l'objet d'une communication.		
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 relativement facile 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.		

	État d'avancement de la mise en œuvre		
	Totalement mis en œuvre Commentaire : Cet aspect est entièrement mis en œuvre conformément à la taille et aux ressources disponibles de Modèle3 SA.	Partiellement mis en œuvre Commentaire :	Non mis en œuvre Commentaire :
	Modèle3 SA a décidé d'utiliser un pare-feu pour le système de gestion des processus. Seul un port est ouvert, tandis que tous les autres demeurent fermés. La configuration des pares-feux est sécurisée par un mot de passe sûr. Il est possible d'accéder au système de gestion des processus via VPN (« par Internet »), mais seulement après identification avec nom d'utilisateur et mot de passe, puis connexion (à l'aide d'un mot de passe sûr) au système de gestion des processus. Pour toutes les autres prestations (p. ex. services de messagerie de …[32] ou stockage sur le cloud de …[33]), des SLA correspondant aux différents niveaux de sécurité sont mis en place. Modèle3 SA n'utilise par ailleurs aucun système de WLAN. Le système de gestion des processus lui-même (à l'exception de certaines interfaces VPN) ne dispose d'aucun accès direct à Internet (p. ex. via un navigateur Internet).		
4.	**Effectuez régulièrement les mises à jour de vos logiciels**		
	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.		
	État d'avancement de la mise en œuvre		
	Totalement mis en œuvre Commentaire :	Partiellement mis en œuvre Commentaire : Cet aspect est partiellement mis en œuvre par Modèle3 SA. Une politique en matière d'antivirus est nécessaire, non seulement pour le SGP mais aussi pour les appareils personnels, notamment en raison du concept BYOD.	Non mis en œuvre Commentaire :
	Le système d'exploitation du serveur (Windows) est régulièrement et automatiquement actualisé, ce qui fait l'objet d'une vérification mensuelle par le surveillant d'exploitation. Le système de gestion des processus est soumis à des actualisations moins régulières. Le niveau logiciel du SGP est actualisé tous les 3 ou 4 ans (pour des raisons financières et de ressources humaines). Les composants matériels du SGP sont remplacés à intervalles plus espacés (environ tous les 20 ans). Le risque inhérent à cet aspect est accepté. Il n'existe cependant aucune directive concernant l'actualisation des logiciels (p. ex. système d'exploitation, antivirus) pour les appareils personnels des collaborateurs ayant accès au SGP). Recommandation d'action : • Il est recommandé de consigner par écrit les directives concernant le système d'exploitation pour le SGP et les appareils personnels des collaborateurs ayant accès au SGP.		

[32] Ibid.

[33] Ibid.

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.		
	État d'avancement de la mise en œuvre		
	Totalement mis en œuvre Commentaire :	Partiellement mis en œuvre Commentaire : Cet aspect n'est que partiellement mis en œuvre par Modèle3 SA, notamment parce que le système d'exploitation du serveur SGP n'est actuellement protégé que par un mot de passe commun.	Non mis en œuvre Commentaire :
	Modèle3 SA utilise des mots de passe individuels, aussi bien pour le SGP que pour l'informatique de bureau. Actuellement, il n'existe toutefois qu'un mot de passe unique et commun pour le système d'exploitation (Windows), mais il est prévu de mettre en place des mots de passe personnalisés aussi pour le système d'exploitation (juin 2018). Lors d'un colloque professionnel, le fontainier de Modèle3 SA s'est informé sur la cybersécurité et s'est appuyé sur ses nouvelles connaissances pour augmenter la complexité des mots de passe. Les mots de passe correspondent désormais aux critères évoqués lors du colloque, conformément aux dernières recommandations. Intervention recommandées : • Il est recommandé à Modèle3 SA d'instaurer également des mots de passe individualisés pour chaque utilisateur, également au sein du système d'exploitation Windows destiné au serveur SGP.		
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 contrôler 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).		

	État d'avancement de la mise en œuvre		
	Totalement mis en œuvre Commentaire :	Partiellement mis en œuvre Commentaire : Cet aspect n'est que partiellement mis en œuvre par Modèle3 SA, en raison de sa taille et des ressources disponibles, notamment car il n'existe aucune directive concernant les appareils privés des collaborateurs, qui sont cependant susceptibles d'accéder au SGP.	Non mis en œuvre Commentaire :
	Les appareils personnels de trois collaborateurs de Modèle3 SA et d'un collaborateur du distributeur …[34] permettent d'accéder au SGP et de prendre le contrôle. Dans le cadre du service de piquet, il existe un contrat de collaboration avec le distributeur …[35]. En principe, les données ne sont pas enregistrées sur les appareils personnels, mais sur les solutions de cloud mises à disposition. Il n'existe cependant aucune directive en matière de cybersécurité (p. ex. au sujet des mots de passe) pour les collaborateurs. Recommandation d'action : • Élaborez, communiquez et testez des directives claires (p. ex. des mots de passe sûrs) pour l'accès via VPN, au SGP et aux solutions de cloud. • Élaborez et communiquez des directives claires en matière d'actualisation régulière des antivirus et des autres logiciels sur les appareils mobiles disposant d'un accès au SGP (voir également recommandation d'action au point 4).		
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 : – 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.		
	État d'avancement de la mise en œuvre		
	Totalement mis en œuvre Commentaire : Cet aspect est entièrement mis en œuvre conformément à la taille et aux ressources disponibles de Modèle3 SA.	Partiellement mis en œuvre Commentaire :	Non mis en œuvre Commentaire :

[34] Pour des raisons de confidentialité, aucune information permettant d'identifier l'organisation examinée n'est publiée.

[35] Ibid.

	Lors de l'embauche et de la dissolution des contrats de travail, les collaborateurs sont sensibilisés à la question de la sécurité des données et de la confidentialité. Cet aspect est consigné par écrit dans le contrat de travail. Les possibilités relatives à l'installation de logiciels dans le SGP sont très limitées et seul l'administrateur système peut s'en charger. Aucune règle n'est cependant définie pour les appareils personnels. Le fontainier s'informe régulièrement (p. ex. à l'occasion de colloques professionnels) sur les thématiques d'actualité dans le domaine de la cybersécurité et met en œuvre de nouvelles recommandations ad hoc. Pour l'accès à distance du distributeur d'eau … [36], la cybersécurité est réglementée dans le cadre du contrat de piquet.		
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.		
	État d'avancement de la mise en œuvre		
	Totalement mis en œuvre Commentaire : Cet aspect est entièrement mis en œuvre conformément à la taille et aux ressources disponibles de Modèle3 SA.	Partiellement mis en œuvre Commentaire :	Non mis en œuvre Commentaire :
	La salle de commande (ainsi que le serveur SGP) est protégée contre l'accès physique de personnes non autorisées. La porte d'accès est renforcée et équipée de barreaux. Les fenêtres et les conduits d'aération sont également protégés contre les effractions. La salle de commande est également dotée d'une alarme. Les clés d'accès à la salle de commande sont confiées uniquement à quatre personnes autorisées, conformément au principe de moindre privilège.		

[36] Pour des raisons de confidentialité, aucune information permettant d'identifier l'organisation examinée n'est publiée.

	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 : Cet aspect est entièrement mis en œuvre conformément à la taille et aux ressources disponibles de Modèle3 SA.	Partiellement mis en œuvre Commentaire :	Non mis en œuvre Commentaire :
	L'accès aux données est réglementé en fonction d'un concept de droits. Les droits de lecture sont plus largement octroyés que les droits d'écriture. Il existe des droits d'accès individuels pour le SGP et les solutions cloud (messagerie, etc.). Pour les solutions cloud, il est en outre possible de rétablir des données supprimées intentionnellement ou non. Les droits d'administrateurs sont gérés de façon très stricte et sont octroyés à seulement trois parties (le fontainier, son suppléant et le surveillant d'exploitation). Le fabricant forme Modèle3 SA concernant l'attribution des droits. Celle-ci est assurée par le surveillant d'exploitation.		
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 : Cet aspect est entièrement mis en œuvre conformément à la taille et aux ressources disponibles de Modèle3 SA, ou les risques correspondants sont acceptés.	Partiellement mis en œuvre Commentaire :	Non mis en œuvre Commentaire :
	Les appareils mobiles (p. ex. BYOD) ne sont pas cryptés. Modèle3 SA a sciemment pris cette décision et accepte les risques correspondants. Les données issues du SGP sont transférées uniquement via un port dédié du pare-feu et une connexion VPN, elles bénéficient donc d'une protection adéquate. Les données stockées dans le cloud ne sont pas non plus activement cryptées par Modèle3 SA. Les risques correspondants sont cependant acceptés.		

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.		
	État d'avancement de la mise en œuvre		
	Totalement mis en œuvre Commentaire : Cet aspect est entièrement mis en œuvre conformément à la taille et aux ressources disponibles de Modèle3 SA.	Partiellement mis en œuvre Commentaire :	Non mis en œuvre Commentaire :
	Lors de l'embauche et de la dissolution des contrats de travail, les collaborateurs sont sensibilisés à la question de la sécurité des données et de la confidentialité. Cet aspect est consigné par écrit dans le contrat de travail. Les collaborateurs doivent lire et signer ces documents. Ce processus est bien établi et respecté.		
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.		
	État d'avancement de la mise en œuvre		
	Totalement mis en œuvre Commentaire : Cet aspect est entièrement mis en œuvre conformément à la taille et aux ressources disponibles de Modèle3 SA.	Partiellement mis en œuvre Commentaire :	Non mis en œuvre Commentaire :
	Le fabricant est chargé de l'élimination des supports de données.		

	Mesures pour améliorer la disponibilité		
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).		
	État d'avancement de la mise en œuvre		
	Totalement mis en œuvre Commentaire :	Partiellement mis en œuvre Commentaire : Cet aspect n'est que partiellement mis en œuvre par Modèle3 SA. L'ASI ne fait pas encore l'objet de tests réguliers.	Non mis en œuvre Commentaire :
	Le surveillant d'exploitation est chargé des travaux de maintenance réguliers. Il vérifie régulièrement les journaux système ainsi que le statut de l'ASI (alimentation sans interruption). Il contrôle également périodiquement l'intégrité des backups. Il n'effectue cependant aucun test régulier de l'ASI et des backups, mais cela pourrait être mis en place sans investissement important, notamment pour l'ASI. Interventions recommandées : • Un processus de test régulier de l'ASI doit être élaboré et appliqué de façon correspondante. Ce test pourrait par exemple faire l'objet d'une discussion avec le fabricant lors de la réception du nouveau SGP. • Concernant les backups, se reporter à la recommandation d'action de la mesure 1 (Protégez vos données en faisant régulièrement des backups).		
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.		
	État d'avancement de la mise en œuvre		
	Totalement mis en œuvre Commentaire : Cet aspect est entièrement mis en œuvre conformément à la taille et aux ressources disponibles de Modèle3 SA.	Partiellement mis en œuvre Commentaire :	Non mis en œuvre Commentaire :
	Des possibilités d'accès clairement définies sont disponibles. Elles sont différentes pour le SGP et pour le reste de l'informatique de bureau. Pour pouvoir accéder au SGP, deux étapes au moins sont nécessaires. Il convient tout d'abord de se connecter au serveur du SGP via VNP (ou localement dans le poste de commande), en entrant un mot de passe. Ce n'est qu'après cela qu'il est possible d'accéder au logiciel du SGP lui-même et de prendre le contrôle. Cette étape nécessite également un mot de passe. Des règles claires ont aussi été établies pour le personnel du service d'assistance		

	(contractuellement avec le fournisseur de services de cloud et le fabricant du SGP). Il est toujours possible d'attribuer des actions à une personne donnée et d'assurer ainsi le suivi. Intervention recommandée : • Lors de la réception du SGP, il convient de rediscuter des accès au système et de l'authentification correspondante et d'en reconfirmer les modalités.
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).
	État d'avancement de la mise en œuvre
	Totalement mis en œuvre Commentaire : Cet aspect est entièrement mis en œuvre par Modèle3 SA. L'exploitation en îlot ne fait toujours pas l'objet de tests réguliers. / Partiellement mis en œuvre Commentaire : / Non mis en œuvre Commentaire :
	Une ASI est à disposition pour le système de gestion des processus. Elle garantit le fonctionnement de l'installation pendant environ une heure. Au-delà de ce délai, l'installation doit être mise hors service. La distribution d'eau elle-même pourrait cependant continuer à être assurée. En effet, en raison de la déclivité naturelle de la collecte des eaux, seul l'approvisionnement en électricité de l'installation de traitement UV est nécessaire. Un générateur de secours est à disposition pour cette dernière. Tous les autres processus pourraient être encore commandés manuellement. Un contrat passé avec le distributeur …[37] prévoit en outre que ce dernier doit prêter main forte en cas d'incident. À cet effet, Modèle3 SA est reliée à une station de pompage du distributeur …[38], où elle dispose de sa propre pompe. En principe, Modèle3 SA devrait pouvoir permuter vers un état d'exploitation en îlot grâce à sa propre production électrique, mais cela n'a pas été testé depuis longtemps. Intervention recommandée : • L'exploitation en îlot grâce à la production électrique propre doit faire l'objet de tests réguliers en fonction du concept d'urgence et des possibilités (exploitation de l'installation UV à l'aide de courant autoproduit).
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.).

[37] Pour des raisons de confidentialité, aucune information permettant d'identifier l'organisation examinée n'est publiée.

[38] Ibid.

	• 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.		
	État d'avancement de la mise en œuvre		
	Totalement mis en œuvre Commentaire : Cet aspect est entièrement mis en œuvre conformément à la taille et aux ressources disponibles de Modèle3 SA.	Partiellement mis en œuvre Commentaire :	Non mis en œuvre Commentaire :
	Pour le serveur destiné à l'exploitation du SGP, certains composants sont disponibles de façon redondante (p. ex. carte réseau, disque dur). Un SLA a de plus été convenu pour le SGP, afin de garantir le remplacement des composants défaillants dans un temps donné. Pour les solutions de cloud, aucun composant n'est disponible de façon redondante. Cet aspect est couvert par le SLA. Les risques correspondants sont acceptés, car les processus-clés peuvent encore être maintenus manuellement même en cas de panne de l'informatique de bureau ou du SGP. Seul du courant pour l'installation de traitement UV est nécessaire.		
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 ?		
	État d'avancement de la mise en œuvre		
	Totalement mis en œuvre Commentaire : Cet aspect est entièrement mis en œuvre conformément à la taille et aux ressources disponibles de Modèle3 SA.	Partiellement mis en œuvre Commentaire :	Non mis en œuvre Commentaire :

<table>
<tr><td></td><td colspan="3">Le distributeur Modèle3 SA a élaboré un concept d'urgence en fonction des risques identifiés et défini contractuellement des délais de réactivité avec le fabricant. Un raccordement au réseau de conduites a par ailleurs été établi auprès du distributeur d'eau …[39]. Le distributeur …[40] est en outre raccordé au distributeur …[41] et peut également s'y approvisionner en eau en cas d'urgence.
Un contrat de piquet a été conclu avec le distributeur d'eau …[42] Des processus d'urgence sont aussi disponibles en cas de panne du SGP : ils permettent de maintenir la distribution d'eau. Aussi bien …[43] que …[44] pourrait continuer à fournir de l'eau à Modèle3 SA sans approvisionnement en électricité.</td></tr>
<tr><td>18.</td><td colspan="3">Diffusez le savoir-faire</td></tr>
<tr><td></td><td colspan="3">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.</td></tr>
<tr><td></td><td colspan="3">État d'avancement de la mise en œuvre</td></tr>
<tr><td></td><td>Totalement mis en œuvre
Commentaire :
Cet aspect est entièrement mis en œuvre conformément à la taille et aux ressources disponibles de Modèle3 SA.</td><td>Partiellement mis en œuvre
Commentaire :</td><td>Non mis en œuvre
Commentaire :</td></tr>
<tr><td></td><td colspan="3">Compte tenu de la petite taille de la commune, Modèle3 SA assure la distribution d'eau avec peu de personnel. Le fontainier n'a pas de suppléant direct et possède énormément de connaissances techniques. Son éventuelle absence pourrait cependant être palliée grâce au contrat de piquet établi avec le distributeur …[45]. Un échange de savoir-faire régulier est assuré avec le distributeur …[46].
En cas d'urgence, le fabricant du système de gestion des processus pourrait également assurer temporairement les tâches du surveillant d'exploitation. Il s'agirait cependant d'une mesure ad hoc. Il n'est pas prévu d'approfondir cette mesure de coopération et le risque correspondant est accepté.</td></tr>
</table>

Tab. 1 18 mesures pour améliorer la sécurité TIC

[39] Pour des raisons de confidentialité, aucune information permettant d'identifier l'organisation examinée n'est publiée.
[40] Ibid.
[41] Ibid.
[42] Ibid.
[43] Ibid.
[44] Ibid.
[45] Ibid.
[46] Ibid.

4.3 Conclusions

Les incidents de cybersécurité, qu'ils soient intentionnels ou qu'ils résultent d'erreurs de manipulation, peuvent avoir des conséquences désastreuses sur la distribution d'eau. Le système de gestion des processus et l'installation de traitement constituent des points faibles significatifs pour de nombreux distributeurs. Dans ce contexte, peu importe souvent que les habitants approvisionnés en eau potable se comptent par milliers ou soient seulement …[47] Comme le confirme nettement cette évaluation, les mesures de résilience (p. ex. sous la forme d'un concept d'urgence, d'une exploitation en îlot ou d'une collaboration avec les distributeurs d'eau alentours) constituent une part essentielle de la stratégie de cybersécurité et Modèle3 SA a mis en œuvre ces mesures en ce sens.

Modèle3 SA s'est préparée aux situations d'urgence à travers de nombreuses mesures, et ce, malgré des ressources limitées. Elle a notamment mis en place une organisation de piquet, une ASI, un concept d'urgence, une exploitation en îlot et une collaboration avec les distributeurs alentours, ainsi qu'un maintien des processus-clés sans le SGP (fonctionnement manuel). Elle n'a toutefois pas encore appliqué toutes les recommandations visées à l'annexe 3 de la norme minimale TIC. Le présent rapport d'évaluation, et notamment les recommandations d'action qu'il contient, visent à permettre à Modèle3 SA de respecter ces recommandations et représentent par conséquent une progression en matière de sécurité d'exploitation de la distribution d'eau.

[47] Ibid.