Norme minimale pour sécuriser la technologie de l'information et de la communication dans la filière alimentaire

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

Préface

L'avancée de l'informatique et l'interconnexion dans pratiquement tous les secteurs ouvrent des possibilités auxquelles un pays comme la Suisse, hautement développé et industrialisé, ne peut renoncer. Mais cette numérisation implique des risques nouveaux, que nous devons affronter. Le risque de cyberattaques ciblées visant l'infrastructure des technologies de l'information (TI) concerne tant les institutions publiques que les exploitants d'infrastructures critiques et d'autres entreprises traitant des informations particulièrement délicates.

La présente norme minimale pour sécuriser les technologies de l'information et de la communication dans la filière alimentaire (norme informatique minimale) concerne avant tout les secteurs clés de notre société moderne : là, les pannes ne sont pas tolérées, car elles affectent les systèmes informatiques des infrastructures critiques. Cela vaut pour l'approvisionnement tant alimentaire qu'énergétique ou pour la santé publique. La présente norme veut aider les entreprises de l'agroalimentaire à éviter les pannes informatiques ou à y remédier rapidement.

Cette norme informatique minimale est destinée à la filière alimentaire ; elle contient des directives reconnues et des recommandations pour améliorer la sécurité informatique. Elaborées par des experts, elles seront régulièrement actualisées. Les entreprises du secteur sont invitées à transposer volontairement les recommandations, dans le cadre d'une autorégulation. Cette norme est foncièrement destinée à toutes les entreprises impliquées dans la production, la distribution, l'importation et la transformation de denrées alimentaires.

Norme informatique minimale : mode d'emploi

La norme informatique minimale comprend plusieurs chapitres : les chapitres 1 et 2 constituent une introduction à l'approvisionnement en denrées alimentaires. Le chapitre 3 explique l'approche « défense en profondeur » *(Defense in Depth)*. Les chapitres 4 et 5 décrivent les mesures à mettre en œuvre et présentent des outils à utiliser, notamment celui d'auto-évaluation (sous Excel).

L'outil d'auto-évaluation permet de déterminer le degré de « maturité » d'une entreprise ou d'une organisation. On considère qu'une entreprise se conforme à la norme informatique minimale, dès qu'elle a atteint la valeur de consigne souhaitée *(cf. Overall Cybersecurity Maturity Rating)*.

Résumé

La numérisation en marche et la concentration de la filière alimentaire accroissent l'efficacité chez les producteurs et les détaillants, mais les rendent aussi bien plus tributaires des systèmes informatiques. Ainsi, pour gérer tous les flux de marchandises, les détaillants n'utilisent, aujourd'hui, plus qu'un seul système et les caisses ne peuvent fonctionner que grâce au système d'encaissement numérique. De plus, pour gérer sa production et donc fabriquer ses produits, l'agro-alimentaire recourt aux systèmes SCADA *(Supervisory Control and Data Acquisition,* soit système informatique surveillant et pilotant les processus techniques). Il est crucial de bien comprendre les défis actuels en matière de sécurité ainsi que les mesures disponibles pour les relever.

La présente norme informatique repose sur le *NIST Framework Core*[1] ainsi que sur les résultats de l'analyse de risques et de vulnérabilité dans la filière alimentaire, faite par l'Office fédéral pour l'approvisionnement économique du pays.[2]

[1] Le NIST Framework Core est une structure de cybersécurité mise au point par une autorité fédérale américaine (National Institut of Standards and Technology) et adoptée comme norme dans de nombreux pays.

[2] Analyse de risques et de vulnérabilité dans l'approvisionnement alimentaire, Office fédéral pour l'approvisionnement économique du pays, Berne 2016.

Sommaire

Contexte et aperçu

L'Office fédéral de l'approvisionnement économique du pays (OFAE) a analysé la filière alimentaire sous l'angle des vulnérabilités numériques dans le cadre de la Stratégie nationale de protection de la Suisse contre les cyber-risques (SNPC). Cette analyse de vulnérabilité est le fruit d'une réflexion commune associant Confédération et économie privée. Elle passe à la loupe les processus d'approvisionnement dans la filière alimentaire. Cette dernière, avec ses différents maillons (transformation, distribution, vente), est notamment tributaire des systèmes suivants :

- **systèmes Enterprise Ressource Planning** (ERP) : ils permettent de gérer les ressources (capital, personnel, équipements, matériel, informatique, communication, etc.). Selon les besoins de l'entreprise, le système ERP intègre un ou plusieurs des sous-systèmes suivants.
- **systèmes gérant les marchandises :** destinés essentiellement aux détaillants, ils permettent de piloter les flux de commandes et de livraisons, indispensables pour la plupart des aliments.
- **systèmes d'encaissement :** ils enregistrent les ventes d'aliments dans les magasins pour transmettre ces données aux systèmes gérant les marchandises.
- **systèmes gérant les processus** (SCADA) : ils pilotent la production des aliments et la préparation des livraisons dans les centrales de distribution.
- **systèmes logistiques :** ils planifient le chargement des marchandises en veillant à honorer efficacement les commandes des clients (cf. tournée).
- **systèmes de transactions financières :** ils permettent de gérer et de comptabiliser les transactions financières.
- **systèmes douaniers**
- **systèmes gérant les stocks**
- **systèmes de communication** (téléphone, courriel, etc.)

La production agricole a, elle aussi, tendance à s'informatiser : traite robotisée, abreuvement et affourragement automatiques ainsi que ventilation automatique ont tendance à se généraliser. L'analyse de vulnérabilité montre toutefois qu'il faut relativiser l'impact de l'informatique dans la filière alimentaire.

La norme minimale présente des recommandations pour améliorer la résilience des systèmes précités. Élaborée avec la CI Commerce de détail Suisse et Swiss Retail Federation, elle constitue une recommandation de branche pour prévenir les cyber-risques dans le secteur alimentaire. Son application facultative relève de l'autorégulation sectorielle.

1 Contexte et objectifs

La sécurité des technologies de l'information et de la communication (TIC) présuppose que chaque exploitant assume ses responsabilités en étant conscient des risques et en recourant à des systèmes fiables. S'il prend des mesures efficaces, conformément à celles préconisées par la présente norme, il pourra déjà prévenir un grand nombre de perturbations d'attaques informatiques, moyennant un investissement raisonnable. L'objectif de cette norme est de fournir aux entreprises un outil polyvalent pour améliorer la résilience de leur infrastructure TIC. Grâce à son approche basée sur le risque, cette norme permet d'introduire différents niveaux de protection, adaptés aux besoins de chaque entreprise.

1.1 Délimitation

L'Office fédéral pour l'approvisionnement économique du pays a mis au point la présente norme avec des experts externes. Il existe déjà nombre de normes, reconnues au niveau international, en matière de sécurité informatique. La plupart d'entre elles vont bien au-delà des préconisations du présent document (voir tableau 53). La présente norme ne prétend pas concurrencer ces standards internationaux, mais elle est compatible avec eux, même si sa portée est réduite. Son but est de simplifier l'entrée en matière tout en garantissant un bon niveau de sécurité.

Elle se concentre sur les processus industriels ayant une incidence directe sur l'approvisionnement alimentaire de la population suisse.

2 La filière alimentaire suisse

2.1 Généralités

En Suisse, la filière alimentaire rassemble des acteurs hétérogènes. Dans la production agricole, les exploitations de petite et moyenne importance prédominent, car le relief – essentiellement montagneux et alpin – de notre pays n'est pas favorable aux grandes exploitations. Tant dans les vallées qu'à la montagne, de nombreuses exploitations de petite taille n'ont pas encore pris le train de l'évolution structurelle et de la productivité accrue des grandes exploitations agricoles. Cette pluralité d'acteurs favorise les redondances dans la production agricole, le corollaire étant une moindre vulnérabilité face aux cyber-risques.

Pour transformer les matières premières agricoles, l'industrie alimentaire compte un nombre d'acteurs assez élevé. Il n'y a pas de monopoliste dont le retrait du marché pourrait remettre globalement en question l'approvisionnement alimentaire de la Suisse. Par exemple, les fromageries se comptent par centaines. L'approvisionnement en produits laitiers est assuré par quatre grands acteurs.[3] La transformation de la viande et l'embouteillage des eaux minérales font aussi intervenir un grand nombre d'acteurs. En revanche, très peu d'entreprises transforment les oléagineux en huiles et corps gras (3 grandes huileries) et les céréales (4 grandes minoteries), constituant un risque agrégé assez important.

Le commerce de détail est dominé par deux enseignes, Coop et Migros, qui couvrent trois bons quarts de l'approvisionnement suisse, d'où leur importance systémique. La paralysie d'un grand détaillant, due par exemple à une cyberattaque ciblant son système de commande ou d'encaissement, peut potentiellement suffire à perturber notre approvisionnement alimentaire. La logistique des détaillants et surtout les centrales de distribution jouent un rôle essentiel dans l'approvisionnement des succursales.

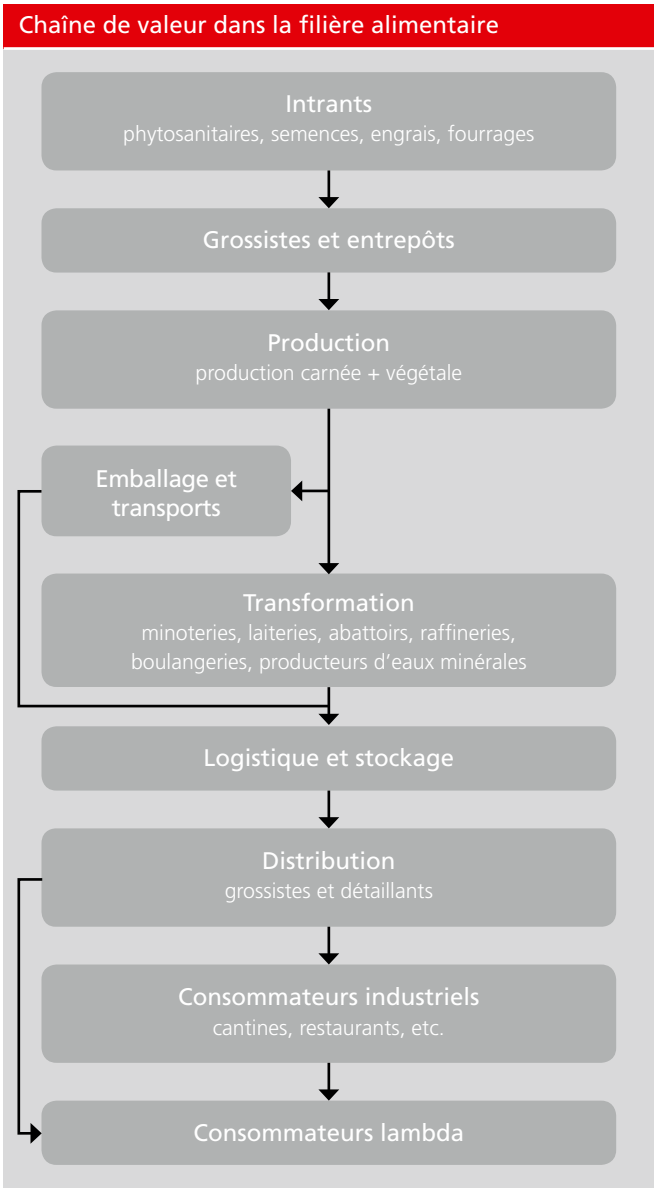

Figure 1 : Chaîne de valeur de la filière alimentaire

[3] *Emmi, Cremo, Hochdorf, Elsa. On dénombre par ailleurs quelque 90 laiteries industrielles.*

2.2 Prestations

La filière alimentaire est capitale pour approvisionner la population suisse. Tout acteur prépondérant dans ce secteur se doit de sécuriser ses systèmes numériques conformément à la présente norme.

Le sixième Rapport sur la nutrition en Suisse met en évidence une consommation moyenne de 3111 kcal par personne et par jour.[4] Selon les statistiques, l'apport nutritionnel se répartit essentiellement entre quatre catégories d'aliments (Figure 2). Les eaux minérales sont aussi prises en compte, vu qu'elles sont vitales dans l'approvisionnement alimentaire :[5]

1) céréales et sucres (glucides)
2) produits carnés (lipides et protéines)
3) produits laitiers[6] (lipides et protéines)
4) huiles et corps gras (lipides)
5) eaux minérales

Le citoyen suisse consomme essentiellement des denrées alimentaires issues de ces cinq catégories. Il couvre ainsi ses besoins en macronutriments (protéines, lipides et glucides). Pour une alimentation équilibrée, il est capital de bien répartir les kilocalories nécessaires entre ce trio. L'apport en protéines, en lipides et en glucides est surtout fourni par les céréales, les sucres, la viande, les produits laitiers ainsi que les huiles et les corps gras (Tableau 1). Ce trio couvre plus de 78 % des besoins en nutriments essentiels.[7]

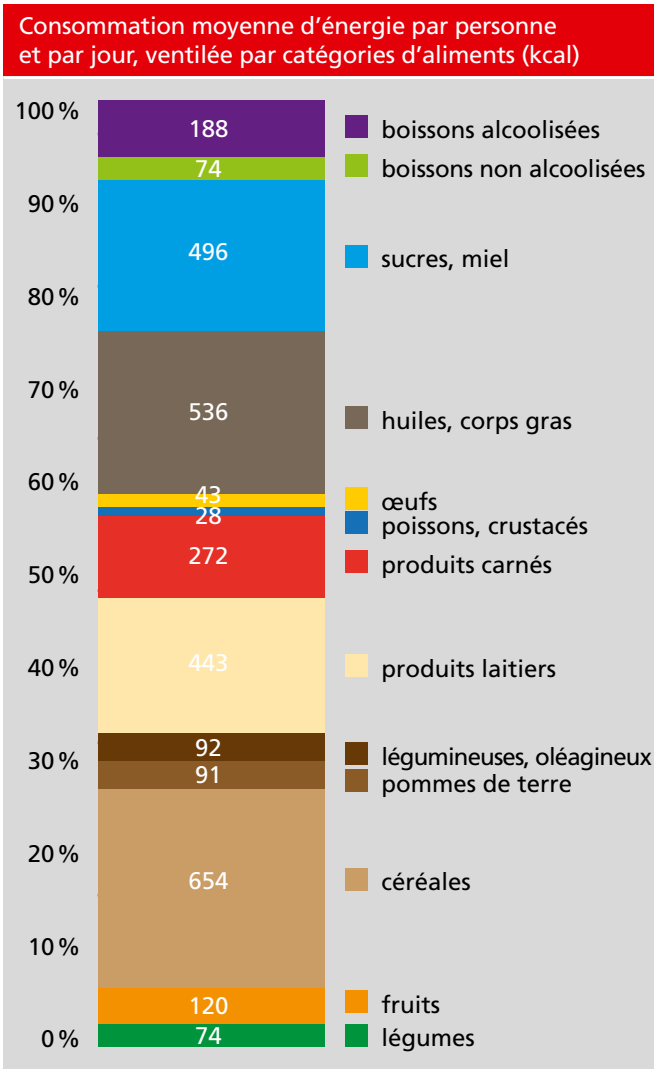

Figure 2 : Consommation moyenne d'énergie par personne/jour (kcal), par catégories de denrées alimentaires

Protéines	%	lipides	%	glucides	%
céréales	22,6 %	viande	14,3 %	céréales	38,6 %
viande	27,9 %	produits laitiers	22,9 %	sucres	35,2 %
produits laitiers	25,3 %	huiles et corps gras	47,6 %		
total	75,8 %	total	84,8 %	total	73,8 %

Tableau 1 : analyse qualitative de l'approvisionnement alimentaire

[4] Office fédéral de la santé publique : sixième rapport sur la nutrition en Suisse, p. 86 ss.

[5] Pour l'approvisionnement de la population en eau potable : nous renvoyons à l'analyse de vulnérabilité informatique consacré à ce secteur : publiée en 2016 par l'OFAE en allemand, mais pas encore traduite.

[6] y compris le beure

[7] Office fédéral de la santé publique : sixième rapport sur la nutrition en Suisse.

2.3 Processus critiques

La filière alimentaire est fortement tributaire des systèmes informatiques, tant dans le commerce de détail que dans l'industrie de transformation. Ils accompagnent tous les processus du commerce de détail. S'ils tombaient en panne, cela prétériterait considérablement l'approvisionnement alimentaire. Il en va de même pour la transformation des aliments : la chaîne industrielle ne peut fonctionner sans systèmes SCADA pilotant les processus. A l'inverse, les processus de production agricole ne sont aujourd'hui guère concernés par l'informatique. La figure ci-dessous présente les processus critiques de la filière.

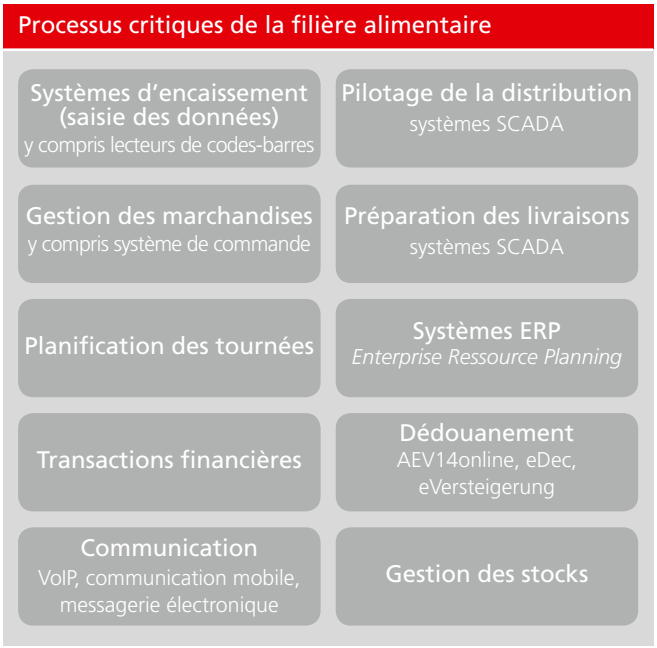

Figure 3 : Processus critiques de la filière alimentaire

Systèmes d'encaissement (enregistrement)

Les systèmes de caisses enregistreuses sont une solution informatique. Ils servent aussi à analyser les habitudes et les préférences des consommateurs, par ex. à travers les cartes de fidélité. Les systèmes d'encaissement utilisés échangent pour la plupart leurs données avec les systèmes gérant les marchandises ou systèmes ERP.

Gestion des marchandises

Elle permet de représenter les flux de marchandises quant à leur valeur et leur quantité. Ce système contribue à tous les processus commerciaux, de l'achat à la vente, en passant par la gestion des stocks.

Gestion des stocks

Assistance numérique permettant d'optimiser les stocks en fonction de la demande.

Planning des tournées

Assistance numérique permettant d'optimiser l'allocation des ressources à disposition, en concentrant les besoins de transport de plusieurs clients sur une ou plusieurs tournées, en fonction des délais de livraison requis, des limites de charge et des capacités de chargement des véhicules, des temps de pause et des heures de travail des conducteurs ainsi que des cycles de maintenance des véhicules, tout en comprimant autant que possible les coûts de transport.

Transactions financières (paiement)

Assistance numérique pour effectuer des paiements sans numéraire, comptabiliser les transactions et exécuter les ordres de paiement. L'offre concernant les systèmes de paiement sans numéraire s'est considérablement développée ces dernières années.

Communications

Ensemble des TIC utilisées pour la communication. En font notamment partie la téléphonie vocale en mode *Voice over IP* (VoIP), EDI (*Electronic Data Interchange* selon les standards GS1), les messageries électroniques et la communication mobile. Les systèmes de communication jouent un rôle essentiel dans la filière alimentaire.

Gestion de la production (SCADA)
Assistance numérique de la surveillance et du pilotage des équipements techniques (appareils, machines, installations et systèmes biologiques).[8] Les systèmes pour gérer la production (SCADA) pilotent les installations produisant les aliments (par ex. dans les huileries, les raffineries sucrières, les abattoirs, les minoteries, les boulangeries, les laiteries, la mise en bouteilles de l'eau minérale, etc.).

Préparation des livraisons (SCADA)
Assistance numérique de tous les modes de préparation des livraisons, en mode Pick-by-Voice ou par scanner. Préparer les livraisons à l'aide de listes imprimées à cocher est une solution purement théorique, tant elle implique un énorme surcroît de travail. Les systèmes pour préparer les livraisons sont utilisés par la plupart des transformateurs et par tous les détaillants. Ils constituent un élément crucial dans la logistique du secteur alimentaire (par ex. dans les centrales de distribution).

Enterprise Ressource Planning (ERP)
Application complexe ou environnement multi-logiciels soutenant la planification globale des ressources de l'entreprise. Les systèmes ERP complexes sont souvent subdivisés en plusieurs sous-systèmes (modules d'application) qui peuvent être combinés librement selon les besoins de l'entreprise.

Dédouanement
Parmi les systèmes de dédouanement, on citera en particulier les applications *AEV14online*, eDec et *eVersteigerung*. Ces systèmes servent à dédouaner les marchandises avec efficacité et ponctualité.

De nombreux produits et groupes de produits font l'objet de contingents tarifaires : viande, charcuterie, œufs, céréales panifiables, fruits, légumes, pommes de terre, produits laitiers. L'application *eVersteigerung* permet une mise en adjudication de ces contingents. Ceux qui ne sont pas totalement utilisés peuvent encore être transférés à un tiers, via AEV14online, jusqu'à l'échéance. Au moment où la marchandise arrive à la douane, elle est comparée avec les données de la mise en adjudication et dédouanée en conséquence. Ces modalités facilitent la procédure et réduisent le travail administratif.

[8] *Supervisory Control and Data Acquisition*

Défense en profondeur

3 Éléments d'une stratégie de défense en profondeur

3.1 Aperçu de la « défense en profondeur »

Une entreprise doit axer sa stratégie de sécurité informatique sur la protection des équipements TIC indispensables aux processus opérationnels. Une approche à plusieurs niveaux est nécessaire : au plan international, on l'appelle *Defense-in-Depth,* soit défense en profondeur. En combinant plusieurs mesures de sécurité, on peut protéger les équipements TIC d'une entreprise. Le principe militaire qui veut qu'un ennemi aura plus de difficultés à surmonter un système de défense multicouche complexe qu'à franchir une simple barrière est à la base de cette stratégie. En parallèle, il faut étudier les méthodes et les modes opératoires des agresseurs potentiels pour préparer des systèmes de défense adaptés. Dans le secteur de la sécurité informatique, le plan de défense en profondeur vise à détecter les atteintes à la sécurité des TIC, pour réagir à ces atteintes et en réduire les effets, ou du moins en atténuer l'impact. La défense en profondeur poursuit une approche holistique qui vise à protéger toutes les ressources (TIC) contre n'importe quel risque. Une entreprise devrait consacrer ses ressources à se protéger des risques connus et à cerner les risques potentiels. Des mesures appropriées doivent protéger l'intégralité des systèmes TIC. Cela comprend les personnes, les processus, les bâtiments, les données et les appareils. Un agresseur ne constitue une menace pour un système TIC que s'il parvient à détecter et exploiter une faille dans l'un de ces éléments. Les entreprises doivent régulièrement de contrôler l'efficacité des mesures de protection et les adapter aux nouvelles menaces, si nécessaire.

3.2 Systèmes de contrôle industriels (SCI) ou *Industrial Control Systems (ICS)*

Certaines failles dangereuses (« exploits ») peuvent rester longtemps indécelables, vu l'architecture complexe des SCI, resp. SCADA[9], alors qu'elles constituent une « cyberattaque persistante ». La mise en œuvre du plan défense en profondeur, décrit ci-dessus, offre une protection adaptée contre ces menaces.

Voici quelques méthodes d'attaque typiques visant les SCI :

- attaques via Internet d'un SCI accessible via Internet pour établir un accès à distance permanent,
- accès à distance à un SCI en utilisant des données d'accès volées,
- attaques d'un SCADA en profitant des failles de l'interface Web,
- contamination d'un SCI par des logiciels malveillants sur des supports corrompus (clés USB, smartphone, etc.),
- attaques de la bureautique (par ex. via des courriels d'hameçonnage, infections par téléchargement furtif, etc.) visant à pénétrer dans un SCI par n'importe quelle interface.

Fondamentalement, il existe des différences importantes entre la bureautique et un SCADA lorsqu'on met en œuvre des plans de défense en profondeur. Tableau 2 liste les sujets liés à la sécurité et les implications différentes pour les TIC et les SCI.

[9] *Les termes SCI et SCADA sont synonymes dans le présent document.*

Thématique sécuritaire	TIC (p. ex. bureautique)	SCI/SCADA (p.ex. gestion de la production)
Antivirus	Largement répandu. Facile à distribuer et à mettre à jour. Les utilisateurs ont la possibilité de le personnaliser. Une protection par antivirus peut être configurée au niveau de l'équipement ou d'une entreprise.	Les besoins de place en mémoire et le ralentissement des échanges de données pour cause d'analyse par l'antivirus peuvent affecter le fonctionnement d'un SCI. Les sociétés doivent conserver des logiciels sans assistance pour protéger leurs équipements les plus anciens. Les solutions antivirus recourent souvent à des dossiers « d'exception » dans les environnements SCI pour éviter la mise en quarantaine de fichiers stratégiques.
Mises à jour de sécurité *(Update Management)*	Doivent être précisément définies, appliquées à toute l'entreprise et automatisées grâce à des accès à distance.	Délais et planification prennent du temps jusqu'à ce que les correctifs soient correctement installés ; toujours tributaire du fournisseur ; peut (temporairement) stopper le SCI ; d'où l'obligation de définir un « risque acceptable ».
Cycles de vie de la technologie *(Technology Support Life Cycle)*	2 à 3 ans, plusieurs fournisseurs, développement et mises à niveau constants.	10 à 20 ans, souvent un seul fournisseur ou prestataire de service sur tout le cycle de vie, sa fin générant de nouveaux risques pour la sécurité.
Méthodes de tests et d'audits *(Testing and Audit Methods)*	Utilisation de méthodes modernes (si possible automatisées). Les systèmes sont normalement suffisamment résilients et fiables pour supporter des évaluations *(assessments)* sans interrompre l'exploitation.	Les méthodes d'évaluation automatisées ne conviennent pas forcément, vu le haut degré de personnalisation par ex. Les risques qu'une erreur se produise pendant une évaluation sont élevés. De fait, les évaluations en cours de production sont généralement plus délicates.
Gestion des modifications *(Change Management)*	Planifiées et périodiques. Respectant les exigences de l'entreprise: durées minimale + maximale de fonctionnement d'un appareil.	Processus complexe avec un impact possible sur les activités de l'entreprise. Une planification stratégique et individuelle est indispensable.
Classification des actifs *(Asset Classification)*	Cas normal et arrive chaque année. Les dépenses + investissements sont planifiés en fonction des résultats.	Faite seulement si nécessaire ou sur demande. Faute d'inventaire, les contre-mesures ne sont souvent pas adaptées à l'importance de l'élément système.
Réaction + analyse en cas d'incidents *(Incident Response and Forensics)*	Facile à développer et à mettre en œuvre. Au besoin, se conformer aux prescriptions réglementaires (protection des données).	Se concentre principalement sur le redémarrage du système. Processus d'analyse peu réglementés.

Tableau 2 : Différences selon TIC et SCI

Thématique sécuritaire	TIC (p. ex. bureautique)	SCI/SCADA (p.ex. gestion de la production)
Sécurité physique *(Physical Security)*	Variable: faible pour la bureautique et forte pour les centres de calculs protégés.	Normalement, la sécurité physique est bonne.
Développement de logiciels sécurisés *(Secure Software Development)*	Partie intégrante du processus de développement.	Historiquement, les SCI étaient conçus comme des systèmes distincts. Il n'était pas prévu d'intégrer la sécurité dans leur développement. Les fournisseurs de SCI ont fait des progrès, mais moins que dans le domaine des TIC. Il n'existe guère de solutions pour sécuriser a postériori les éléments centraux des SCI.
Règles de sécurité	Prescriptions réglementaires générales, selon le secteur (pas pour tous les secteurs).	Normes réglementaires propres au secteur (mais pas pour tous les secteurs).

Tableau 2 : Différences selon TIC et SCI

Lorsqu'on établit un plan de défense en profondeur pour un SCI/SCADA, il faut prendre en compte les éléments suivants :

- coûts pour sécuriser les anciens systèmes selon les normes actuelles
- tendance croissante à connecter les SCI aux réseaux de l'entreprise
- possibilité de fournir un accès à distance aux utilisateurs des environnements TIC et SCI
- obligation de faire confiance à sa propre chaîne d'approvisionnement
- surveillance et protection des protocoles propres aux SCI, avec des outils modernes
- capacité à rester constamment informé des nouvelles menaces planant sur les SCI

L'approche défense en profondeur complique les attaques directes des systèmes TIC et augmente la probabilité de détecter rapidement des comportements suspects ou inhabituels dans le système. Cette approche permet également de créer des zones distinctes pour mettre en œuvre de technologies permettant de détecter les intrusions dans le système *(Intrusion-Detection-Technology)*. Les éléments représentatifs d'une stratégie de défense en profondeur sont présentés au Tableau 3.

Éléments d'une stratégie de défense en profondeur	
Programme de gestion des risques	• reconnaissance des risques pour la sécurité • profil de risques • gestion minutieuse (inventaire) des équipements TIC
Architecture de cybersécurité	• normes/recommandations • lignes directrices • mode opératoire
Sécurité physique	• protection des terminaux • surveillance des accès au centre de contrôle • vidéosurveillance, contrôle des accès et barrières
Architecture de réseau	• zones de sécurité standards • « zones démilitarisées» (DMZ) • réseaux locaux virtuels
Périmètre de sécurité réseau	• pare-feu • accès à distance et authentification • serveurs intermédiaires/hôtes
Sécurité de l'hôte	• gestion des correctifs et des points faibles • terminaux • appareils virtuels
Contrôle de la sécurité	• systèmes de détection d'intrusion • journaux des audits de sécurité • problèmes de sécurité et contrôle des incidents
Gestion des fournisseurs	• gestion et contrôle de la chaîne fournisseurs • services d'infogérance et externalisation • utilisation de services nuagiques
Facteurs humains	• lignes directrices • mode opératoire • formation et conscientisation

Tableau 3 : Éléments d'une stratégie de défense en profondeur

3.3 Gestion des risques

3.3.1 Programme de gestion des risques

Il faut comprendre les risques auxquels une entreprise est exposée (menaces informatiques) pour mettre en œuvre une stratégie de défense en profondeur. Ils doivent être gérés en fonction de la propension au risque dans l'entreprise. Les responsables de l'exploitation et de la maintenance des systèmes TIC doivent pouvoir identifier, évaluer et traiter les cyber-risques. Cela exige une bonne connaissance des scénarios de menace, des processus opérationnels et techniques, ainsi que des technologies en jeu. On ne peut intégrer dans les tâches quotidiennes une stratégie de défense en profondeur qu'après avoir analysé ces paramètres. La direction de l'entreprise doit définir la sécurité comme prérequis à toutes ses activités informatiques.

Les règles énoncées ci-dessus ne sont que des principes généraux. Certaines applications TIC sont particulièrement importantes, voire critiques, notamment dans les systèmes de contrôle industriels ou SCI. Pour concevoir une architecture de sécurité SCI efficace, il faut que les risques d'entreprise soient rapportés aux exigences fonctionnelles (opérationnelles) du SCI. Cela peut avoir des incidences dans le monde réel (par ex. un périmètre de sécurité autour d'un centre de calcul). Les décideurs, à tous les niveaux de l'entreprise, doivent comprendre l'importance des cyber-risques et être activement impliqués dans leur processus de gestion. Il faut faire régulièrement des analyses de risques pour les systèmes, applications et processus cruciaux, y compris pour les réseaux associés. Elles doivent être effectuées selon des règles strictes, suivant une approche structurée et systématique.

3.3.2 Cadre pour gérer les risques *(framework)*

Les analyses des risques informatiques devraient être intégrées dans la gestion globale des risques et être effectuées régulièrement sur des objets de recherche clairement définis. Il s'agit par exemple de systèmes, de processus et d'applications stratégiques (même en cours de développement) ainsi que d'autres systèmes, réseaux et services dont ils dépendent.

Ce cadre pour gérer les risques permet d'affecter aux risques identifiés des responsables qui vont surveiller (monitorage), évaluer et mettre en œuvre des mesures permettant de circonscrire les risques dans des limites préalablement définies comme acceptables (= propension au risque).

3.3.3 Analyse des risques

Il faut clairement définir la portée de l'analyse des risques informatiques, décrire les processus opérationnels et les éléments techniques pertinents (et d'éventuels facteurs externes), puis pondérer ces facteurs et éléments. Ainsi on aura défini le contenu et les limites de l'analyse.

3.4 Analyse d'impact sur les affaires

Cette analyse permet d'évaluer quel serait l'impact (réaliste voire dans le pire des cas) d'une composante TIC corrompue (y compris les personnes, les données, les processus, les services ou les réseaux) sur les activités d'une entreprise, et ce, à divers titres (financier, opérationnel, juridique, réputationnel, sanitaire).

Enfin, il faut déterminer l'impact sur ses activités que l'entreprise est prête à assumer si ses ressources informatiques ne sont pas disponibles contrairement à ce qui était prévu. Par conséquent, il convient de définir les exigences et les niveaux de protection nécessaires pour assurer la disponibilité, l'intégrité et la confidentialité des ressources TIC choisies en fonction d'un risque jugé acceptable.

3.5 Mesures

Il faut identifier, examiner et avaliser les mesures à prendre pour se prémunir contre les risques décrits dans l'analyse d'impact. La direction de l'entreprise doit les avaliser en même temps que les plans précisant la marche à suivre.

On doit aussi penser à évaluer le risque résiduel pour tous les équipements dans l'environnement considéré et à le gérer de manière adéquate (l'atténuer, le contourner, le transférer ou l'accepter), selon la propension au risque de l'entreprise.

Il faut déterminer le risque maximal acceptable pour chaque équipement *(asset)*, ce qui permet de calculer les risques informatiques (cumulés).

3.6 Architecture de la cybersécurité

Une architecture de cybersécurité comprend des mesures spécifiques et leur place stratégique dans le réseau afin d'instaurer une couche de sécurité requise pour une défense en profondeur. Elle facilite également la collecte d'informations sur les flux de données entre tous les systèmes et sur leurs connexions. L'architecture de cybersécurité devrait être en phase avec l'inventaire des installations et des ressources TIC pour garantir que les flux informatiques sont globalement identifiés dans l'entreprise.

Une architecture de cybersécurité devrait être en adéquation avec le *NIST Framework Core* et prendre en compte la protection de la confidentialité, de l'intégrité et de la disponibilité des données, des services et des systèmes. Pour ce faire, il faut élaborer un plan de mise en œuvre respectant la culture d'entreprise et les objectifs stratégiques, tenant adéquatement compte des besoins de sécurité et indiquant les ressources requises. En général, une architecture de cybersécurité est complétée par une liste de tâches qui détaille les résultats espérés (signalant des problèmes et l'urgence de poursuivre l'analyse en profondeur pour établir des plans plus précis), établit les agendas des projets, évalue les besoins en ressources et cerne les principaux facteurs de dépendance du projet.

3.7 Sécurité physique

Les mesures de sécurité (physique) réduisent le risque de pertes accidentelles ou intentionnelles, ou de dommages causés aux équipements informatiques de l'entreprise ou dans le voisinage. Les équipements à protéger comprennent le matériel comme les outils et les installations, l'environnement (au sens écologique) et le voisinage ainsi que ce qui relève de la propriété intellectuelle, notamment les données propriétaires (paramètres de configuration ou fichiers clients). Les contrôles de sécurité doivent fréquemment répondre à des exigences spécifiques question environnement, sécurité, réglementation, droit, etc. Les entreprises doivent adapter les contrôles de sécurité et les contrôles techniques à leurs besoins de protection. Pour garantir une protection globale, la sécurité physique comprend également la protection des composantes informatiques *(= security)* et des données sur l'environnement informatique. La sécurité de nombreuses infrastructures TIC est étroitement liée à la sécurité des installations *(= safety)*. L'objectif est de mettre les employés à l'abri du danger sans entraver leur travail ou à cause de procédures d'urgence. Les contrôles de sécurité sont des mesures actives ou passives qui limitent l'accès à toutes les composantes de l'infrastructure TIC. Ces mesures de protection doivent notamment empêcher les cas suivants :

- visiteurs indésirables aux endroits critiques
- modifications physiques, manipulations, vols ou autres disparitions voire destructions de systèmes, d'infrastructures, d'interfaces de communication, voire de sites
- observations inopportunes d'installations critiques, émanant de curieux, de photographes ou de personnes faisant d'autres sortes de relevés
- introduction ou installation non autorisée de nouveaux systèmes, infrastructures, interfaces de communication ou autre équipement informatique
- introduction subreptice d'appareils (clés USB, point d'accès sans fil, *Bluetooth* ou mobiles), destinés à endommager des équipements, intercepter des communications ou nuire d'une autre manière

Pour répondre aux besoins de sécurité informatique, il faut protéger les équipements, y compris les systèmes et le matériel réseau, la bureautique (imprimantes en réseau et appareils multifonctions) et les équipements spéciaux (par ex. les SCI) tout au long de leur cycle de vie, de l'acquisition (achat ou location) à leur élimination, en passant par la maintenance.

Les appareils portables (ordinateurs portables, tablettes et smartphones) et leurs données doivent également être protégés contre le piratage, la perte et le vol en configurant les paramètres de sécurité, en limitant les accès, en installant des logiciels de sécurité et en gérant les appareils de manière centralisée.

3.8 Gestion des cycles de vie du matériel *(hardware)*

L'achat ou la location de matériel robuste et fiable doit toujours se faire en respectant les exigences de sécurité. Les éventuels points faibles du matériel doivent toujours être identifiés.

L'objectif est de garantir que les équipements offrent les fonctionnalités désirées et ne compromettent pas la sécurité des informations et des systèmes critiques ou sensibles et ce, tout au long de leur cycle de vie.

3.9 Configuration des appareils portables

Pour protéger les données contre les accès non autorisés, la perte et le vol, les appareils portables (ordinateurs portables, tablettes et smartphones) doivent toujours avoir une configuration standardisée qui réponde aux exigences de sécurité.

Le but de cette configuration standardisée est de garantir, même en cas de perte ou de vol, la sécurité informatique des données stockées ou envoyées sur l'appareil portable.

3.10 Systèmes de contrôle industriels

Les systèmes de contrôle industriels (SCI) doivent être surveillés et contrôlés conformément aux exigences de sécurité. Il faut notamment les protéger techniquement et physiquement afin de garantir les processus cruciaux pour l'approvisionnement.

3.11 Architecture réseau SCI

Une architecture réseau résistante et sécurisée constitue l'une des principales conditions à toute défense efficace contre les attaques. Chaque interface, chaque passerelle, chaque connexion représente un danger potentiel. Il faut donc impérativement connaître et gérer en conséquence tous les processus normalement supportés par les réseaux et les équipements. Le principe de base consiste à grouper et à segmenter correctement l'architecture réseau. L'important est de subdiviser l'architecture réseau au moins en deux zones de sécurité. La première zone de sécurité (dédiée aux systèmes d'organisation) englobe les systèmes informatiques de planification et de répartition des ressources (p. ex. ERP, système de gestion des marchandises). La seconde zone de sécurité (dédiée aux systèmes de production) englobe les systèmes (SCADA) servant à piloter la production ou la vente des denrées alimentaires.

La figure 4 illustre schématiquement la géographie numérique de la filière alimentaire, avec ses canaux de communication usuels et ses zones de sécurité, en particulier la dichotomie entre systèmes IT (Information Technology) et OT (Operational Technology).[10]

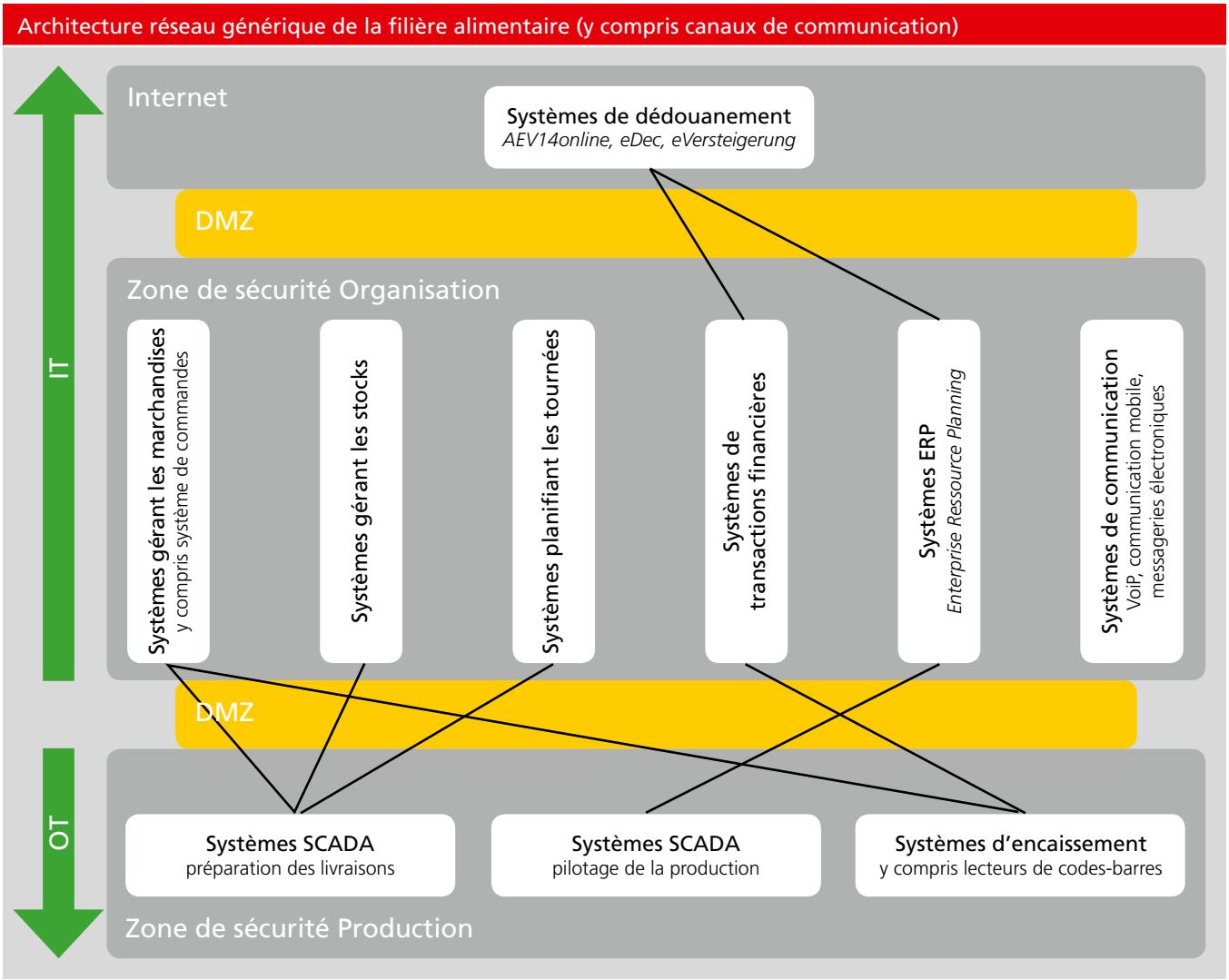

Figure 4 : Architecture réseau générique pour les entreprises du secteur alimentaire (y. c. communication)

[10] *L'architecture réseau SCI illustrée ici est un exemple type à ajuster selon les besoins de chaque entreprise.*

3.12 Périmètre de sécurité des réseaux SCI/SCADA

Le coût d'une installation SCI et la maintenance d'une infrastructure de réseau homogène exigent souvent une connexion entre le SCI et le réseau d'entreprise. Cette connexion représente un important risque pour la sécurité, elle devrait être techniquement protégée. Si les réseaux doivent absolument être interconnectés, il est fortement recommandé de n'autoriser qu'un minimum de connexions (voire des connexions uniques) via un pare-feu et une DMZ (segment de réseau séparé). Les serveurs SCI contenant des données du réseau d'entreprise doivent être placés dans une de ces zones « démilitarisées ». Les connexions avec l'extérieur doivent être recensées et limitées le plus possible via le pare-feu. En outre, des systèmes de détection d'anomalies permettent de surveiller les échanges de données et de les valider.

3.13 Sécurité des hôtes

Une couche de sécurité supplémentaire doit être apportée au niveau du poste de travail (hôte). Les pare-feu protègent la plupart des appareils contre les intrusions extérieures. Un bon système de sécurité exige cependant des défenses à plusieurs niveaux. Une sécurisation complète du réseau implique de sécuriser tous les ordinateurs hôtes. Cette couche de sécurité doit permettre à un opérateur d'utiliser divers systèmes d'exploitation et différentes applications tout en assurant une protection correcte des équipements.

Les directives sur les mots de passe doivent être identiques pour tous les utilisateurs d'un système. Les noms de comptes classiques (administrateur par ex.) doivent être modifiés. Les utilisateurs auront tendance à contourner des pratiques trop restrictives, en notant leur mot de passe (sur des post-it par ex.) ou en utilisant systématiquement des chaînes de caractères semblables. La complexité des règles relatives aux mots de passe devrait être adaptée au niveau d'autorisation des utilisateurs. On peut aussi exiger des changements de mots de passe à intervalles réguliers.

Les recommandations générales suivantes devraient être mises en œuvre par les entreprises pour chaque hôte SCI et chaque appareil doté d'un accès au réseau de l'entreprise (quel que soit le système d'exploitation) :

- installer et configurer un pare-feu spécifique pour l'hôte
- régler si possible les écrans de veille à intervalles très courts, obligeant de redonner le mot de passe
- installer régulièrement les correctifs des systèmes d'exploitation et mettre à jour les micrologiciels
- configurer les logs (journaux) et les activer sur tous les appareils
- désactiver les services et les comptes non utilisés, de même que ceux qui ne sont plus utilisés
- remplacer les services non sécurisés (Telnet, Remote Shell ou FTP) par des solutions plus sûres (sTelnet, SSH, sFTP, etc.)
- ne pas autoriser les utilisateurs à désactiver des services
- effectuer et contrôler les sauvegardes des systèmes, surtout si elles ne sont pas gérées de manière centralisée
- activer ou remplacer les modules de sécurité fournis avec le système d'exploitation (scanners de sécurité) par des logiciels plus performants
- appliquer les mêmes stratégies aux ordinateurs portables et autres appareils portable non connectés en permanence au réseau de l'entreprise. Il est aussi recommandé de crypter les disques durs des équipements portables.

3.14 Surveillance de la sécurité

L'utilisation de systèmes de Monitoring et de composants réseau qui détectent les comportements anormaux et les « signatures d'attaque » ajoute de la complexité à un environnement informatique ou à un SCI. Les fonctions de surveillance et de détection selon le plan de défense en profondeur sont toutefois indispensables pour protéger les équipements critiques. Une barrière électronique autour du réseau SCI ne suffit pas à protéger les ressources critiques contre une intrusion. Le plan de défense en profondeur prévoit qu'une entreprise soit alertée dès que possible par son système de surveillance en cas de problème de sécurité. La plupart des entreprises ont une surveillance standard dans leur environnement informatique. Elles oublient souvent de le faire pour leurs réseaux SCI.

Il est indispensable :

- d'effectuer des audits de sécurité exhaustifs, indépendants et réguliers (secteurs critiques dans l'entreprise, processus, applications et systèmes/réseaux supportés); ainsi que
- de surveiller les risques informatiques, de respecter les éléments des exigences légales, réglementaires et contractuelles importants pour la sécurité et d'informer régulièrement la direction de l'entreprise sur la sécurité informatique.

3.15 Politique de sécurité informatique

Une fois qu'on a défini, maintenu et contrôlé la stratégie globale de sécurité informatique, la direction d'une entreprise peut fixer des lignes directrices claires, les défendre tant dans l'application des exigences que dans la gestion des risques.

3.16 Gestion des fournisseurs

La gestion des fournisseurs concerne l'identification et la gestion des risques liés aux technologies de l'information pour les fournisseurs externes (matériel + logiciels, services d'externalisation, services nuagiques, etc.). Respecter les exigences en matière de sécurité informatique par le biais de contrats formels permet de minimiser les risques.

3.17 Les facteurs humains

Les erreurs humaines posent de nombreux défis aux entreprises. Les mesures techniques de protection ne peuvent jamais garantir qu'aucune erreur ne se produise, que ce soit par malveillance ou par négligence. Dans une entreprise, le risque d'erreur est directement lié au taux d'employés inexpérimentés ou peu qualifiés. Lutter contre d'éventuels actes malveillants commis par ses propres collaborateurs confronte une entreprise à un autre genre de défi. Elle doit, pour ce faire, résoudre divers problèmes.

3.17.1 Les cycles de la vie professionnelle

La sécurité informatique doit être un souci permanent, dans toute la période d'occupation (de l'embauche à la retraite). Cela implique de nombreuses mesures de sécurité, par exemple lors du transfert de ressources (matériel, accès aux systèmes), ou l'obligation de protéger les accès aux locaux et bâtiments. Un programme de formation pertinent doit sensibiliser les employés à la sécurité et définir leurs comportements en matière de sécurité. L'entreprise doit retenir par écrit l'avancement et le déroulement de ces formations.

L'objectif est de s'assurer que les employés ont les compétences, les connaissances et les outils nécessaires pour défendre les valeurs de l'entreprise tout en respectant les consignes de sécurité informatique en vigueur dans l'entreprise.

3.17.2 Les règles et directives

Des règles et des directives claires et réalistes définissent le comportement des employés en matière de sécurité. Elles donnent un cadre et prévoient des contrôles pour protéger les systèmes en appliquant ces règles. Elles décrivent également les modes opératoires et définissent les attentes de l'entreprise envers ses collaborateurs. Les consignes et les instructions déterminent ce qui doit être respecté ainsi que la manière de sanctionner les infractions.

3.17.3 Les processus

L'organisme responsable de la sécurité informatique est chargé de gérer la sécurité et les spécificités de ses processus. Sa fonction première est de protéger les informations et les données de l'entreprise. Les processus de gestion de la sécurité doivent être appliqués aux systèmes de contrôle industriels. Pour ce faire, il faut définir les processus précisant la manière d'opérer ou de configurer certains systèmes. Ces processus doivent être normalisés et reproductibles. L'entreprise formera toujours ses nouveaux collaborateurs afin de maintenir un niveau de sécurité constant, ce qui garantit qu'ils connaissent toutes les réglementations et normes requises. Le processus de détection d'un cyberaccident *(Intrusion Detection)* est extrêmement important. Les procédures de sécurité liées au réseau sont cruciales pour les protocoles propriétaires et les systèmes patrimoniaux.

3.17.4 Tâches et responsabilités dans les secteurs critiques de l'entreprise

Il faut clairement définir et attribuer à des personnes compétentes les tâches et les responsabilités dans les environnements critiques, les processus, les applications (y compris les systèmes et réseaux supportés) et les informations.

L'objectif est de susciter chez les employés un sentiment de responsabilité individuelle. Un tel climat dans une entreprise aide les employés à effectuer leurs tâches en respectant les prescriptions de sécurité informatique.

3.17.5 Communication et programme de sensibilisation à la sécurité

Un programme de sensibilisation à la sécurité et une politique de communication en découlant responsabilisent les employés et favorisent les comportements adaptés, à tous les niveaux hiérarchiques de l'entreprise.

L'objectif est d'obtenir dans une entreprise un climat qui favorise les comportements de sécurité individuels. Chacun devrait pouvoir prendre des décisions en fonction du risque dans sa sphère de compétences.

Assessment Framework

4 NIST Framework

L'objectif du cadre NIST et de ses recommandations est de mettre à disposition des opérateurs d'infrastructures critiques et d'autres entreprises liées à des TIC un outil leur permettant d'accroître, de manière autonome et responsable, leur résilience face aux risques de sécurité. Le cadre NIST se fonde sur un choix de normes, de directives et de règles de bonnes pratiques; il est technologiquement neutre.

En bref

Le *NIST Framework Core* reprend le principe d'une approche proportionnelle aux risques pour contrecarrer et gérer les risques de cybersécurité. Il a cinq fonctions :

1) identifier (Identify)
2) protéger (Protect)
3) détecter (Detect)
4) réagir (Respond)
5) récupérer (Recover)

Implémentation des *Tiers*

Le *NIST Framework* comprend 4 niveaux, appelés *Implementation Tiers.* Ils décrivent le niveau de protection qu'une entreprise a mis en place. Ces niveaux vont de partiel (*Tier* 1) à dynamique (*Tier* 4). Pour déterminer son niveau de protection, une entreprise doit parfaitement connaître ses pratiques de gestion des risques, le genre de menaces plausibles, les exigences légales et réglementaires, ses objectifs commerciaux et ses besoins organisationnels.

Les définitions des niveaux *Tier* sont les suivantes:

Tier 0 : pas mis en œuvre

Bien que l'entreprise ou l'organisation soit consciente que la mesure considérée devrait en fait déjà être réalisée depuis longtemps, elle n'a encore rien entrepris.

Tier 1 : partiellement mis en œuvre

Le niveau 1 signifie que les processus de gestion des risques ainsi que les exigences organisationnelles pour la sécurité des TIC ne sont pas formalisés (pas de règles fixées). Les risques informatiques sont généralement gérés au jour le jour, en mode réactif. Il existe un programme intégré pour gérer les risques au niveau organisationnel, mais on n'a pas instauré une véritable prise de conscience des risques informatiques ou une approche globale pour y faire face dans l'entreprise. Cette dernière ne dispose généralement pas de processus pour relayer en son sein les informations sur la cybersécurité. Il en va de même pour les autres risques informatiques, l'entreprise n'a le plus souvent pas prévu de processus standardisés pour communiquer ou coordonner ses activités avec ses partenaires externes.

Tier 2 : conscient des risques

Les entreprises qui optent pour un classement au niveau 2 disposent généralement de processus pour gérer leurs risques informatiques. Cependant, ces programmes ne sont pas concrètement appliqués ni obligatoires. Au niveau organisationnel, les risques informatiques sont intégrés dans un système de gestion global et tous les niveaux de l'entreprise ont été sensibilisés aux risques informatiques. On enregistre généralement dans l'entreprise un manque de volonté pour gérer et améliorer la sensibilisation aux risques informatiques, actuels et futurs. Les processus et méthodes approuvés sont définis et mis en œuvre. Les collaborateurs disposent de ressources suffisantes pour effectuer leurs tâches de cybersécurité. Les informations sur la cybersécurité sont partagées de manière informelle au sein de l'entreprise. Cette dernière est consciente de son rôle et n'hésite pas à communiquer avec ses partenaires externes (clients, fournisseurs, prestataires de services, etc.) sur les questions de cybersécurité. Il n'existe cependant aucun processus standardisé pour collaborer ou échanger des informations avec ces partenaires.

Tier 3 : reproductible

Les entreprises de niveau 3 ont formellement validé leurs plans pour gérer les risques et leurs instructions pour les faire appliquer en leur sein. La gestion des risques informatiques est définie dans les directives de l'entreprise. Les risques informatiques sont standardisés et les directives pour y remédier font l'objet de mises à jour régulières. Cette pratique tient compte des nouveaux besoins de l'entreprise, des progrès technologiques et d'un environnement où les menaces sont mouvantes, que ce soit à cause de nouveaux acteurs ou d'une nouvelle législation.

La documentation interne décrit les processus et procédures pour gérer les nouveaux risques. Des méthodes standardisées sont définies pour répondre à l'évolution des menaces. Les collaborateurs ont les connaissances et les compétences nécessaires pour accomplir leurs tâches.

L'entreprise sait qu'elle est tributaire de ses partenaires externes. Elle partage les informations qui lui permettent, face à des incidents, de prendre elle-même des décisions.

Tier 4 : dynamique

Le niveau 4 signifie qu'une entreprise répond entièrement aux exigences des niveaux 1 à 3, et qu'en plus, elle analyse en permanence ses propres processus, méthodes et capacités pour les adapter, le cas échéant. Il est indispensable de bien documenter tous les incidents de cybersécurité pour pouvoir continuellement s'améliorer. L'entreprise tire les leçons nécessaires de l'analyse des incidents passés et adapte, de manière dynamique, ses processus et techniques de sécurité aux technologies de pointe et à l'évolution des menaces. La gestion des risques informatiques fait intégralement partie de la culture d'entreprise. Les enseignements tirés des incidents passés, les informations provenant de sources externes et la surveillance constante des systèmes et réseaux internes sont constamment intégrés dans le processus de gestion des risques. L'entreprise partage en permanence ses informations avec ses partenaires en recourant à des processus standardisés.

n/a : pas de réponse

Après que l'organisation ou l'entreprise ait procédé à l'évaluation de ses risques, cette mesure n'est consciemment pas mise en oeuvre.

Profils

Un profil est le résultat de l'ajustement aux standards, aux directives et aux bonnes pratiques du *Cybersecurity Framework,* conjugué à un scénario d'implantation individuel. Les profils peuvent servir à identifier les meilleures options d'amélioration au regard de la cybersécurité, par exemple en comparant un profil réel et un profil souhaité. L'outil d'évaluation fourni avec la présente norme minimale de sécurité numérique sert précisément à paramétrer un tel profil. L'évaluation des 106 activités répertoriées dans le questionnaire donne des résultats agrégés d'après les cinq fonctions du *Cybersecurity Framework* (identifier, protéger, détecter, réagir, récupérer). Le niveau minimal requis est réputé atteint lorsque la « cote globale de l'évaluation de la cybersécurité » indique des valeurs (sous rubrique « réel ») correspondant au moins aux valeurs minimales requises (sous rubrique « Souhaité »). Les instructions concernant le mode opératoire sont intégrées à l'outil d'évaluation.

Exemple d'évaluation de la cybersécurité

Cote globale de l'évaluation de la cybersécurité	réalité	cible
Identifier *(Identify)*	2.8	2.6
Protéger *(Protect)*	2.7	2.6
Détecter *(Detect)*	2.9	2.6
Réagir *(Respond)*	2.0	2.6
Récupérer *(Recover)*	1.4	2.6

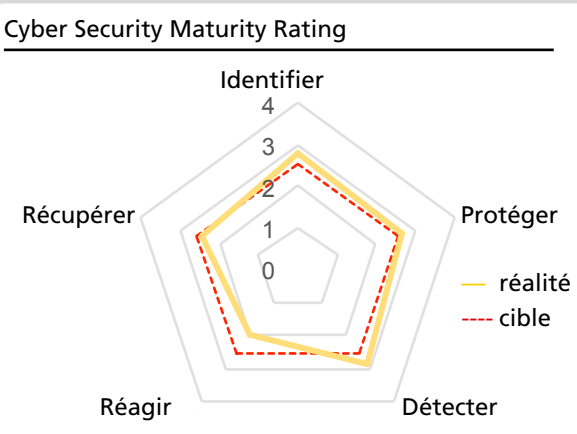

Figure 5 : Exemple de cote globale de l'évaluation de la cybersécurité

4.1 Identifier (*Identify)*

Inventaire et organisation *(Assest Management)*

Les données, les personnes, les appareils, les systèmes et les installations d'une entreprise sont identifiés, catalogués et évalués. L'évaluation se fait en fonction de leur criticité pour les processus opérationnels à mettre en place et de la stratégie de l'entreprise en matière de risque.

Désignation	Tâche
ID.AM-1	Développez un processus d'inventaire garantissant en permanence un recensement exhaustif de vos équipements TIC *(Asset)*.
ID.AM-2	Inventoriez toutes les plateformes, licences et applications logicielles dans votre entreprise.
ID.AM-3	Listez tous les flux de communication et de transferts de données en interne.
ID.AM-4	Listez tous les systèmes TIC externes cruciaux pour votre entreprise.
ID.AM-5	Établissez des priorités pour les ressources inventoriées (équipements, applications, données) selon leur criticité.
ID.AM-6	Définissez clairement les rôles et les responsabilités en matière de cybersécurité.

Tableau 4 : Tâches ID.AM

Norme	Référence
CCS CSC 1	1, 2
COBIT 5	BAI09.01, BAI09.02, BAI09.05, DSS05.02, APO02.02, APO03.03, APO03.04, PO01.02, DSS06.03
ISA 62443-3:2013	SR 7.8
ISO 27001:2013	A.6.1.1, A.8.1.1, A.8.1.2, A.8.2.1, A.11.2.6
NIST-SP-800-53 Rev. 4	AC-4, CA-3, CA-9, PL-8, CM-8, AC-20, SA-9, CP-2, RA-2, SA-14, CP-2, PS-7, PM-11

Tableau 5 : Références ID.AM

Environnement de l'entreprise *(Business Environment)*

Les objectifs, les tâches et les activités de l'entreprise sont hiérarchisés et évalués.
Cette information sert à répartir les responsabilités.

Désignation	Tâche
ID.BE-1	Définissez, documentez et communiquez le rôle exact de votre entreprise dans la chaîne d'approvisionnement (critique).
ID.BE-2	Identifiez et communiquez l'importance de votre entreprise en tant qu'infrastructure vitale et sa position dans le secteur critique.
ID.BE-3	Évaluez et hiérarchisez les objectifs, les tâches et les activités dans l'entreprise.
ID.BE-4	Listez tous les systèmes TIC externes cruciaux pour votre entreprise.
ID.BE-5	Priorisez les ressources inventoriées (équipements, applications, données) selon leur criticité.

Tableau 6 : Tâches ID.BE

Norme	Référence
CCS CSC 1	1, 2
COBIT 5	BAI09.01, BAI09.02, BAI09.05, DSS05.02, APO02.02, APO03.03, APO03.04, PO01.02, DSS06.03
ISA 62443-3:2013	SR 7.8
ISO 27001:2013	A.6.1.1, A.8.1.1, A.8.1.2, A.8.2.1, A.11.2.6
NIST-SP-800-53 Rev. 4	AC-4, CA-3, CA-9, PL-8, CM-8, AC-20, SA-9, CP-2, RA-2, SA-14, CP-2, PS-7, PM-11

Tableau 7 : Références ID.BE

Règles *(Governance)*

Une bonne gouvernance fixe les responsabilités, surveille et s'assure que les exigences réglementaires, juridiques et opérationnelles soient respectées dans la sphère d'activité.

Désignation	Tâche
ID.GV-1	Édictez des directives sur les besoins en sécurité informatique dans votre entreprise.
ID.GV-2	Convenir entre les responsables internes (gestion des risques par ex.) et des partenaires externes, des rôles et des responsabilités en matière de sécurité informatique.
ID.GV-3	Vérifiez que votre entreprise respecte toutes les exigences légales et réglementaires en matière de cybersécurité, y compris au niveau de la protection des données.
ID.GV-4	Assurez-vous que les cyber-risques sont bien intégrés dans la gestion des risques pour toute l'entreprise.

Tableau 8 : Tâches ID.GV

Norme	Référence
COBIT 5	APO01.03, EDM01.01, EDM01.02, APO13.02, MEA03.01, MEA03.04, DSS04.02
ISA 62443-3:2013	
ISO 27001:2013	A.5.1.1, A.6.1.1, A.7.2.1, A.18.1
NIST-SP-800-53 Rev. 4	PM-1, PS-7, PM-9, PM-11

Tableau 9 : Références ID.GV

Analyse de risque *(Risk Assessment)*

L'entreprise analyse l'impact des cyber-risques sur ses activités, ses équipements et son personnel, y compris les risques réputationnels.

Désignation	Tâche
ID.RA-1	Identifiez les faiblesses (techniques) de vos équipements et documentez-les.
ID.RA-2	Participez à des forums et à des réunions d'experts pour échanger des informations et être au courant des cybermenaces.
ID.RA-3	Identifiez et documentez les cybermenaces, aussi bien internes qu'externes.
ID.RA-4	Identifiez l'impact potentiel des cybermenaces sur vos activités et évaluez leur probabilité d'occurrence.
ID.RA-5	Évaluez les risques pour votre entreprise en fonction des menaces, des vulnérabilités, de l'impact (sur ses activités) et de leur probabilité d'occurrence.
ID.RA-6	Définissez les mesures à prendre immédiatement lorsqu'un risque se concrétise et fixez des priorités.

Tableau 10 : Tâches ID.RA

Norme	Référence
COBIT 5	APO12.01, APO12.02, APO12.03, APO12.04, APO 12.05, APO 13.02, DSS04.02
ISA 62443-3:2013	4.2.3, 4.2.3.9, 4.2.3.12
ISO 27001:2013	A.12.6.1, A.18.2.3, A.6.1.4
NIST-SP-800-53 Rev. 4	CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5, PM-15, PM-16, SI-5, RA-3, SI-5, PM-12, RA-2, PM-9, PM-11, SA-14

Tableau 11 : Références ID.RA

Stratégie pour gérer les risques *(Risk Management Strategy)*

Définissez les priorités, les restrictions et les risques maximaux supportables pour votre entreprise. Évaluez vos risques opérationnels sur cette base.

Désignation	Tâche
ID.RM-1	Définissez les processus de gestion des risques, gérez-les activement et faites-les confirmer par les personnes impliquées ou les parties prenantes.
ID.RM-2	Définissez et communiquez les risques supportables pour votre entreprise.
ID.RM-3	Assurez-vous que les risques supportables sont évalués en prenant en compte l'importance de votre entreprise du fait qu'elle exploite une infrastructure critique. Prenez également en considération, dans votre analyse, les risques propres au secteur.

Tableau 12 : Tâches ID.RM

Norme	Référence
COBIT 5	APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02, APO12.06
ISA 62443-3:2013	4.3.4.2, 4.3.2.6.5
ISO 27001:2013	
NIST-SP-800-53 Rev. 4	PM-8, PM-9, PM-11, SA-14

Tableau 13 : Références ID.RM

Gestion des risques liés à la chaîne d'approvisionnement *(Supply Chain Riskmanagement)*

Définissez les priorités, les restrictions et les risques maximaux que votre entreprise peut accepter par rapport à ses fournisseurs.

Désignation	Tâche
ID.SC-1	Définissez des processus clairs pour gérer les risques liés à une perturbation dans la chaîne d'approvisionnement. Faites contrôler et valider ces processus par toutes les parties prenantes.
ID.SC-2	Identifiez les fournisseurs et les prestataires de services cruciaux pour vos systèmes, composants et services critiques à partir des processus définis ci-dessus et fixez les priorités.
ID.SC-3	Exigez de vos fournisseurs et prestataires de services qu'ils s'engagent contractuellement à développer et mettre en œuvre des mesures appropriées pour atteindre les objectifs du processus pour gérer les risques liés à la chaîne d'approvisionnement.
ID.SC-4	Faites un suivi systématique pour vous assurer que tous vos fournisseurs et prestataires de services remplissent leurs obligations conformément aux exigences. Faites-le vérifier régulièrement par des rapports d'audit ou par les résultats des tests techniques.
ID.SC-5	Définissez avec vos fournisseurs et prestataires les processus pour réagir et récupérer après des problèmes de cybersécurité. Validez ces processus par des simulations.

Tableau 14 : Tâches ID.SC

Norme	Référence
COBIT 5	APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05
ISA 62443-3:2013	4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14, 4.3.2.6., 4.3.2.5.7, 4.3.4.5.11 7
ISO 27001:2013	A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2, A.15.2.1, A.15.2.2, A.17.1.3
NIST-SP-800-53 Rev. 4	SA-9, SA-12, PM-9, RA-2, RA-3, SA-12, SA-14, SA-15, SA-11, CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9

Tableau 15 : Références ID.SC

4.2 Protéger *(Protect)*

Gestion des accès *(Access Control)*

Veiller à ce que l'accès physique et logique (à distance) aux équipements et installations TIC ne soient possibles que pour les personnes, processus et appareils autorisés et à ce que seules les activités prévues soient permises.

Désignation	Tâche
PR.AC-1	Définissez un processus clair pour octroyer et gérer les autorisations et les données d'identification pour utilisateurs, appareils/machines et processus.
PR.AC-2	Assurez-vous que seules les personnes autorisées ont physiquement accès aux équipements TIC. Prenez des mesures concrètes pour garantir que les ressources TIC sont protégées contre tout accès physique non autorisé.
PR.AC-3	Définissez les processus pour gérer les accès à distance.
PR.AC-4	Définissez les niveaux d'autorisation en étant le plus restrictif possible et séparez les fonctions.
PR.AC-5	Contrôlez que l'intégrité de votre réseau est protégée. Séparez votre réseau au niveau logique comme physique, si c'est nécessaire et judicieux.
PR.AC-6	N'attribuez des identités numériques qu'à des personnes ou à des processus que vous avez clairement identifiés.

Tableau 16 : Tâches PR.AC

Norme	Référence
COBIT 5	DSS05.04, DSS06.03, DSS01.04, DSS05.05, APO13.01, DSS01.04, DSS05.03, DSS05.04, DSS05.05, DSS05.07, DSS06.03, BAI08.03
ISA 62443-3:2013	SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.13, SR 2.1, SR 2.6, SR 3.1, SR 3.8, SR 2.2, SR 2.3
ISO 27001:2013	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3, A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.6.1.2, A.7.1.1, A.9.1.2, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6, A.9.4.1, A.9.4.4
NIST-SP-800-53 Rev. 4	AC-2, IA Family, PE-2, PE-3, PE-4, PE-5, PE-6, PE-9, AC-17, AC-19, AC-20, AC-2, AC-3, AC-5, AC-6, AC-16, AC-24, IA-2, IA-4, IA-5, IA-8

Tableau 17 : Références PR.AC

Sensibilisation et formation *(Awareness and Training)*

Assurez-vous que vos employés et vos partenaires externes sont correctement formés et conscients de tous les aspects de la cybersécurité. Veillez à ce qu'ils exécutent les Tâches impactant la sécurité conformément aux exigences et aux processus définis.

Désignation	Tâche
PR.AT-1	Veillez à ce que tous vos collaborateurs soient sensibilisés et formés en matière de cybersécurité.
PR.AT-2	Veillez à ce que les utilisateurs ayant des niveaux d'autorisation élevés soient conscients de leur rôle et de leurs responsabilités.
PR.AT-3	Veillez à ce que tous les acteurs extérieurs à votre entreprise (fournisseurs, clients, partenaires) soient conscients de leur rôle et de leurs responsabilités.
PR.AT-4	Veillez à ce que tous les cadres soient conscients de leurs rôles spécifiques et de leurs responsabilités.
PR.AT-5	Veillez à ce que les responsables de la sécurité physique et de la sécurité informatique soient conscients de leurs rôles spécifiques et de leurs responsabilités.

Tableau 18 : Tâches PR.AT

Norme	Référence
COBIT 5	APO07.03, BAI05.07, APO07.02, DSS06.03, APO07.03, APO10.04, APO10.05
ISA 62443-3:2013	4.3.2.4.2, 4.3.2.4.3
ISO 27001:2013	A.7.2.2, A.6.1.1
NIST-SP-800-53 Rev. 4	AT-2, AT-3, PM-13, PS-7, SA-9, AT-3, PM-7

Tableau 19 : Références PR.AT

Sécurité des données *(Data Security)*

Assurez-vous que les informations, les données et leurs supports sont gérés de manière à protéger la confidentialité, l'intégrité et la disponibilité des données, conformément à la stratégie de votre entreprise pour gérer les risques.

Désignation	Tâche
PR.DS-1	Assurez-vous que les données stockées sont protégées (contre toute atteinte ou préjudice en termes de confidentialité, d'intégrité et de disponibilité).
PR.DS-2	Assurez-vous que les données sont protégées pendant leur transmission (contre toute atteinte ou préjudice en termes de confidentialité, d'intégrité et de disponibilité).
PR.DS-3	Veuillez à ce qu'un processus formel soit défini pour votre matériel TIC afin de protéger les données lorsque des équipements sont supprimés, déplacés ou remplacés.
PR.DS-4	Veillez à disposer d'une réserve de capacité suffisante afin que vos données soient toujours disponibles.
PR.DS-5	Assurez-vous que des mesures appropriées sont mises en œuvre contre les fuites de données (« pompage »).
PR.DS-6	Définissez un processus pour vérifier l'intégrité du micrologiciel, des systèmes d'exploitation, des logiciels d'application et des données.
PR.DS-7	Ayez un environnement informatique pour le développement et les tests qui soit totalement indépendant des systèmes de production.
PR.DS-8	Définissez un processus pour vérifier l'intégrité du matériel utilisé.

Tableau 20 : Tâches PR.DS

Norme	Référence
COBIT 5	APO01.06, BAI02.01, BAI06.01, DSS06.06, BAI09.03, APO13.01, BAI07.04, BAI03.05.4
ISA 62443-3:2013	SR 3.4, SR 4.1, SR 3.1, SR 3.8, SR 4.1, SR 4.2, SR 7.1, SR 7.2, SR 5.2
ISO 27001:2013	A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7, A.12.3.1, A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3
NIST-SP-800-53 Rev. 4	SC-28, SC-8, CM-8, MP-6, PE-16, AU-4, CP-2, SC-5, AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4, SI-7, CM-2, SA-10

Tableau 21 : Références PR.DS

Règles de protection des données *(Information Protection Processes and Procedures)*

Assurez-vous que les données sont protégées pendant leur transmission (contre toute atteinte ou préjudice en termes de confidentialité, d'intégrité et de disponibilité).

Désignation	Tâche
PR.IP-1	Générez une configuration standard pour l'infrastructure d'information et de communication, ainsi que pour les systèmes de contrôle industriel. Assurez-vous que cette configuration par défaut obéit aux règles usuelles de sécurité (par ex. redondance N-1, configuration minimale, etc.).
PR.IP-2	Définissez un processus « cycle de vie » pour le développement de systèmes.
PR.IP-3	Définissez un processus pour contrôler les changements de configuration.
PR.IP-4	Assurez-vous que des sauvegardes informatiques *(Backups)* sont effectuées, gérées et testées régulièrement (+ qu'on peut restaurer les données sauvegardées).
PR.IP-5	Contrôlez que toutes les exigences (réglementaires) et les directives concernant les équipements « physiques » soient respectées.
PR.IP-6	Contrôlez que les données soient toujours détruites selon les prescriptions.
PR.IP-7	Développez et améliorez régulièrement vos processus de sécurité informatique.
PR.IP-8	Discutez de l'efficacité des différentes technologies de protection avec vos partenaires.
PR.IP-9	Instaurez des processus pour réagir aux cyberincidents *(Incident Response-Planning, Business Continuity Management, Incident Recovery, Disaster Recovery)*.
PR.IP-10	Testez les plans d'intervention et de récupération.
PR.IP-11	Tenez compte de la cybersécurité dès le processus de recrutement (en vérifiant les antécédents ou par des contrôles de sécurité personnels, par ex.).
PR.IP-12	Développez et mettez en œuvre un processus pour traiter les failles repérées.

Tableau 22 : Tâches PR.IP

Norme	Référence
COBIT 5	BAI10.01, BAI10.02, BAI10.03, BAI10.05, APO13.01, BAI06.01, BAI01.06, APO13.01, DSS01.04, DSS05.05, BAI09.03, APO11.06, DSS04.05, DSS04.03, APO07.01, APO07.02, APO07.03, APO07.04, APO07.05
ISA 62443-3:2013	SR 7.6
ISO 27001:2013	A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5, A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4, A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3, A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3, A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7, A.16.1.6, A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3, A.12.6.1, A.18.2.2
NIST-SP-800-53 Rev. 4	CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8, CP-4, CP-6, CP-9, PE-10, PE-12, PE-13, PE-14, PE-15, PE-18, MP-6, A-2, CA-7, CP-2, IR-8, PL-2, PM-6, AC-21, CA-7, SI-4, CP-2, IR-8, IR-3, PM-14, RA-3, RA-5, SI-2

Tableau 23 : Références PR.IP

Maintenance *(Maintenance)*

Veillez à ce que la maintenance et la réparation des composantes des systèmes TIC et du SCI soient effectuées conformément aux directives et méthodes en vigueur.

Désignation	Tâche
PR.MA-1	Veillez à ce que le fonctionnement, la maintenance et les éventuelles réparations des équipements soient enregistrés et documentés (journalisation). Assurez-vous qu'elles sont effectuées rapidement et en ne recourant qu'à des moyens testés et approuvés.
PR.MA-2	Enregistrez et documentez également les travaux de maintenance de vos systèmes distants. Assurez-vous qu'aucun accès non autorisé n'est possible.

Tableau 24 : Tâches PR.MA

Norme	Référence
COBIT 5	BAI09.03, DSS05.04, APO11.04, DSS05.02, APO13.01
ISA 62443-3:2013	
ISO 27001:2013	A.11.1.2, A.11.2.4, A.11.2.5, A.15.1.1, A.15.2.1
NIST-SP-800-53 Rev. 4	MA-2, MA-3, MA-4, MA-5

Tableau 25 : Références PR.MA

Technologie de protection *(Protective Technology)*

Installez des solutions techniques pour assurer la sécurité et la résilience de votre système et de vos données selon les exigences et processus.

Désignation	Tâche
PR.PT-1	Définissez les exigences pour les audits et les enregistrements de journaux. Générez et vérifiez ces journaux régulièrement, selon les exigences et les directives.
PR.PT-2	Assurez-vous que les supports amovibles sont protégés et que leur utilisation se fait dans le strict respect des directives.
PR.PT-3	Veillez à ce que votre système soit configuré pour toujours fonctionner, même en mode dégradé (système renforcé).
PR.PT-4	Assurez la protection de vos réseaux de communication et de contrôle.
PR.PT-5	Définissez des scénarios pour les différents modes de fonctionnement de vos systèmes. Par ex. : fonctionnalités en cas d'attaque, fonctionnalités pendant la phase de récupération, fonctionnalités normales pendant l'exploitation.

Tableau 26 : Tâches PR.PT

Norme	Référence
COBIT 5	APO11.04, DSS05.02, APO13.01, BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05
ISA 62443-3:2013	SR 2.3, SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.4, SR 2.5, SR 2.6, SR 2.7, SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.2, SR 7.6
ISO 27001:2013	A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9, A.9.1.2, A.13.1.1, A.13.2.1, A.17.1.2, A.17.2.1
NIST-SP-800-53 Rev. 4	AU Family, MP-2, MP-4, MP-5, MP-7, AC-3, CM-7, AC-4, AC-17, AC-18, CP-8, SC-7, CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6

Tableau 27 : Références PR.PT

4.3 Détecter *(Detect)*

Anomalies et incidents *(Anomalies and Events)*

Veillez à ce que les anomalies et autres événements (exceptionnels) soient détectés à temps et que le personnel soit conscient de l'impact potentiel de ces incidents.

Désignation	Tâche
DE.AE-1	Définissez des valeurs par défaut pour les opérations réseau licites et les flux de données prévus pour les utilisateurs et les systèmes. Surveillez ces valeurs en permanence.
DE.AE-2	Assurez-vous que les incidents de cybersécurité détectés sont analysés quant à leurs objectifs et méthodes.
DE.AE-3	Assurez-vous que les informations sur les incidents de cybersécurité provenant de différentes sources et capteurs sont compilées et exploitées.
DE.AE-4	Déterminez les conséquences probables des incidents.
DE.AE-5	Définissez les valeurs limites au-delà desquelles les incidents de cybersécurité doivent générer des alertes.

Tableau 28 : Tâches DE.AE

Norme	Référence
COBIT 5	DSS03.01, APO12.06
ISA 62443-3:2013	SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2
ISO 27001:2013	
NIST-SP-800-53 Rev. 4	AC-4, CA-3, CM-2, SI-4, AU-6, CA-7, IR-4, IR-5, IR-8, SI-4

Tableau 29 : Références DE.AE

Surveillance *(Security Continuous Monitoring)*

Veillez à ce que le système TIC, équipements compris, soit régulièrement contrôlé pour pouvoir détecter les incidents de cybersécurité et vérifier l'efficacité des mesures de protection.

Désignation	Tâche
DE.CM-1	Mettez en place une surveillance permanente du réseau pour détecter les incidents de cybersécurité potentiels.
DE.CM-2	Mettez en place une surveillance continue (monitorage) de tous les équipements et des bâtiments pour détecter les incidents de cybersécurité.
DE.CM-3	Mettez en place un monitorage des cyberactivités des employés pour détecter les incidents de cybersécurité potentiels.
DE.CM-4	Veillez à pouvoir détecter les maliciels.
DE.CM-5	Veillez à pouvoir détecter les maliciels sur les appareils portables.
DE.CM-6	Assurez-vous que les activités des prestataires de services externes sont surveillées (monitorées) pour détecter d'éventuels incidents de cybersécurité.
DE.CM-7	Surveillez votre système en permanence pour être certain que des activités ou accès liés à des personnes, équipements ou logiciels non autorisés seront détectés.
DE.CM-8	Procédez à des tests de vulnérabilité.

Tableau 30 : Tâches DE.CM

Norme	Référence
COBIT 5	DSS05.01, DSS05.07, APO07.06, BAI03.10
ISA 62443-3:2013	SR 6.2, SR 3.2, SR 2.4
ISO 27001:2013	A.12.4.1, A.12.2.1, A.12.5.1, A.14.2.7, A.15.2.1, A.12.6.1
NIST-SP-800-53 Rev. 4	AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4, AU-13, CM-10, CM-11, SI-3, SC-18, SI-4, SC-44, PS-7, SA-4, SA-9, CM-8, PE-3, PE-6, PE-20, SI-4, AU-12, RA-5

Tableau 31 : Références DE.CM

Processus de détection *(Detection Processes)*

Maintenez, testez et entretenez les processus et les instructions pour détecter les incidents de cybersécurité.

Désignation	Tâche
DE.DP-1	Définissez clairement les rôles et les responsabilités pour que tous sachent bien qui est responsable de quoi et qui a telles ou telles compétences.
DE.DP-2	Assurez-vous que les processus de détection correspondent aux exigences et conditions fixées.
DE.DP-3	Testez vos processus de détection.
DE.DP-4	Communiquez aux personnes concernées (par ex. fournisseurs, clients, partenaires, autorités) les incidents que vous avez détectés.
DE.DP-5	Améliorez en permanence vos processus de détection.

Tableau 32 : Tâches DE.DP

Norme	Référence
COBIT 5	DSS05.01, APO13.02, APO12.06, APO11.06, DSS04.05
ISA 62443-3:2013	SR 3.3, SR 6.1
ISO 27001:2013	A.6.1.1, A.18.1.4, A.14.2.8, A.16.1.2, A.16.1.6
NIST-SP-800-53 Rev. 4	CA-2, CA-7, PM-14, SI-3, SI-4, AU-6, CA-2, CA-7, RA-5

Tableau 33 : Références DE.DP

4.4 Réagir *(Respond)*

Plan d'intervention *(Response Planning)*

Élaborez un plan d'intervention pour traiter les incidents de cybersécurité détectés. Assurez-vous qu'en cas d'incident ce plan d'intervention est exécuté correctement et en temps utile.

Désignation	Tâche
RS.RP-1	Assurez-vous que le plan d'intervention est correctement suivi et rapidement exécuté si un incident de cybersécurité est détecté.

Tableau 34 : Tâches RS.RP

Norme	Référence
COBIT 5	BAI01.10
ISA 62443-3:2013	
ISO 27001:2013	A.16.1.5
NIST-SP-800-53 Rev. 4	CP-2, CP-10, IR-4, IR-8

Tableau 35 : Références RS.RP

Communications *(Communications)*

Contrôlez que vos processus de réaction soient coordonnés avec ceux des parties prenantes, internes et externes. Selon le type d'incident, veillez à pouvoir bénéficier du soutien des autorités si la situation l'exige.

Désignation	Tâche
RS.CO-1	Assurez-vous que toutes les personnes connaissent leurs tâches et la marche à suivre lorsqu'elles doivent réagir à un incident de cybersécurité.
RS.CO-2	Définissez des critères pour les communications et assurez-vous que les incidents de cybersécurité sont signalés et traités conformément à ces critères.
RS.CO-3	Partagez les informations sur les incidents de cybersécurité relevés – ainsi que les enseignements qui en découlent – selon ces critères prédéfinis.
RS.CO-4	Coordonnez-vous avec les parties prenantes selon ces critères.
RS.CO-5	Améliorez la sensibilisation aux incidents de cybersécurité grâce à des échanges réguliers avec vos partenaires.

Tableau 36 : Tâches RS.CO

Norme	Référence
COBIT 5	
ISA 62443-3:2013	
ISO 27001:2013	A.6.1.3, A.16.1.2
NIST-SP-800-53 Rev. 4	CP-2, CP-3, IR-3, IR-8, CA-2, CA-7, IR-4, IR-8, PE-6, RA-5, SI-4, PM-15, SI-5

Tableau 37 : Références RS.CO

Analyses *(Analysis)*

Effectuez régulièrement des analyses afin de réagir correctement en cas d'incidents de cybersécurité.

Désignation	Tâche
RS.AN-1	Assurez-vous que les alertes émanant de systèmes de détection sont prises en compte et déclenchent des enquêtes.
RS.AN-2	Veillez à pouvoir évaluer correctement l'impact d'un incident de cybersécurité.
RS.AN-3	Effectuez une analyse technique après chaque incident.
RS.AN-4	Classez les incidents selon les exigences du plan d'intervention.

Tableau 38 : Tâches RS.AN

Norme	Référence
COBIT 5	DSS02.07
ISA 62443-3:2013	SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1
ISO 27001:2013	A.12.4.1, A.12.4.3, A.16.1.5, A.16.1.6, A.16.1.7, A.16.1.4
NIST-SP-800-53 Rev. 4	AU-6, CA-7, IR-4, IR-5, PE-6, SI-4, CP-2, IR-4, AU-7, CP-2, IR-5, IR-8

Tableau 39 : Références RS.AN

Circonscrire les dommages *(Mitigation)*

Faites tout pour éviter qu'un incident de cybersécurité se propage afin de limiter les éventuels dommages.

Désignation	Tâche
RS.MI-1	Assurez-vous que les incidents de cybersécurité peuvent être circonscrits et que vous pouvez stopper leur impact.
RS.MI-2	Assurez-vous de pouvoir réduire l'impact des incidents de cybersécurité.
RS.MI-3	Veillez à réduire au maximum les failles ainsi découvertes ou référencez-les comme des risques acceptables.

Tableau 40 : Tâches RS.MI

Norme	Référence
COBIT 5	
ISA 62443-3:2013	SR 5.1, SR 5.2, SR 5.4, A.12.2.1, A.16.1.5
ISO 27001:2013	A.12.2.1, A.16.1.5, A.12.6.1
NIST-SP-800-53 Rev. 4	IR-4, CA-7, RA-3, RA-5

Tableau 41 : Références RS.MI

Améliorations *(Improvements)*

Améliorez régulièrement la réactivité de votre entreprise face aux incidents de cybersécurité en tirant les enseignements des incidents précédents.

Désignation	Tâche
RS.IM-1	Assurez-vous que les enseignements tirés des précédents incidents de cybersécurité sont intégrés à vos plans d'intervention.
RS.IM-2	Actualisez vos stratégies de réaction.

Tableau 42 : Tâches RS.IM

Norme	Référence
COBIT 5	BAI01.13
ISA 62443-3:2013	
ISO 27001:2013	A.16.1.6
NIST-SP-800-53 Rev. 4	CP-2, IR-4, IR-8

Tableau 43 : Références RS.IM

4.5 Récupérer *(Recover)*

Plan de restauration *(Recovery Planning)*

Contrôlez que les processus de récupération sont tenus à jour pour être exécutés en tout temps, permettant ainsi une récupération rapide des systèmes.

Désignation	Tâche
RC.RP-1	Assurez-vous que le plan de récupération est suivi à la lettre en cas d'incident de cybersécurité.

Tableau 44 : Tâches RC.RP

Norme	Référence
COBIT 5	DSS02.05, DSS03.04
ISA 62443-3:2013	
ISO 27001:2013	A.16.1.5
NIST-SP-800-53 Rev. 4	CP-10, IR-4, IR-8

Tableau 45 : Références RC.RP

Améliorations *(Improvements)*

Améliorez constamment vos processus de récupération après les incidents de cybersécurité en tirant les enseignements des incidents précédents.

Désignation	Tâche
RC.IM-1	Assurez-vous que les enseignements tirés des précédents incidents de cybersécurité sont intégrés à vos plans de récupération.
RC.IM-2	Actualisez vos stratégies de récupération.

Tableau 46 : Tâches RC.IM

Norme	Référence
COBIT 5	BAI05.07
ISA 62443-3:2013	
ISO 27001:2013	
NIST-SP-800-53 Rev. 4	CP-2, IR-4, IR-8

Tableau 47 : Références RC.IM

Communication *(Communications)*

Veillez à coordonner vos actions de récupération avec vos partenaires internes et externes (fournisseurs de services Internet, CERT, autorités, intégrateurs de systèmes, etc.).

Désignation	Tâche
RC.CO-1	Anticipez les réactions du public pour ne pas dégrader la réputation de votre entreprise.
RC.CO-2	Veillez à ce que votre entreprise retrouve vite une image positive après un incident de cybersécurité.
RC.CO-3	Communiquez à l'interne aux parties prenantes tout ce que vous avez entrepris en matière de récupération, sans oublier les cadres et la direction.

Tableau 48 : Tâches RC.CO

Norme	Référence
COBIT 5	EDM03.02
ISA 62443-3:2013	
ISO 27001:2013	
NIST-SP-800-53 Rev. 4	CP-2, IR-4

Tableau 49 : Références RC.CO

Conclusions

La défense en profondeur privilégie l'approche proportionnelle aux risques : chaque entreprise ou organisation peut définir par elle-même sa sensibilité aux risques, les mesures à prendre pour réduire ces risques et leur ordre de priorité. La responsabilité de la cybersécurité reste ainsi l'apanage de l'entreprise. La présente norme minimale de sécurité numérique propose un outil d'évaluation, le NIST Framework Core, qui permet aux acteurs de la filière alimentaire de fortifier la résilience de leurs processus informatisés. Il existe bien d'autres possibilités de valorisation (analyse comparative, échanges d'expériences au sein de la branche/banque nationale de données, analyses d'écart, audits tiers, etc.). La mise en œuvre pratique et les échanges entre acteurs, associations et Confédération, inciteront à expérimenter encore d'autres possibilités d'application.

Outre la présente norme minimale de sécurité numérique, l'Approvisionnement économique du pays propose aux entreprises du secteur alimentaire un outil d'évaluation en format excel[11], qui reprend les recommandations de ladite norme. Cet outil est particulièrement utile pour l'évaluation de la cote de maturité d'une entité sous l'angle de la sécurité numérique. La présente norme minimale est un document de référence qui introduit le sujet tout en servant de référentiel en cas de question.

La présente norme minimale de sécurité numérique est une recommandation dont la mission est de susciter la réflexion chez les acteurs de la filière alimentaire sous l'angle de la cybersécurité. La sécurité numérique n'étant pas un état en soi, mais un processus, cette norme a pour mission d'encourager le processus de maturation et d'aider à sa réalisation.

[11] *Téléchargeable à l'adresse suivante: https://www.bwl.admin.ch/bwl/fr/home/themen/ikt/ikt_minimalstandard.html*

Annexe

6.1 Recommandations pour l'amélioration de la sécurité numérique

La présente recommandation propose un modèle d'évaluation et un outil d'évaluation structurés autour d'une démarche systématique visant l'amélioration de la sécurité numérique dans l'entreprise. Les entités de taille assez importante auront les ressources nécessaires et les collaborateurs formés (p. ex. dans le commerce de détail) et n'auront aucune difficulté à mettre en œuvre cette recommandation. Elles sont susceptibles d'avoir déjà mis en place le modèle proposé dans la présente norme ou un modèle similaire. La filière alimentaire repose sur de nombreux acteurs formant un ensemble extrêmement hétérogène. Certaines entités très critiques sont, d'après leur taille (nombre de collaborateurs et ressources pour la sécurité numérique), plutôt comparables à une petite entreprise. La mise en œuvre complète du modèle proposé peut représenter un défi considérable pour ce genre d'entreprise. La démarche doit être proportionnelle de manière à permettre aux petites entreprises de réaliser au minimum les 21 étapes retenues ci-dessous :

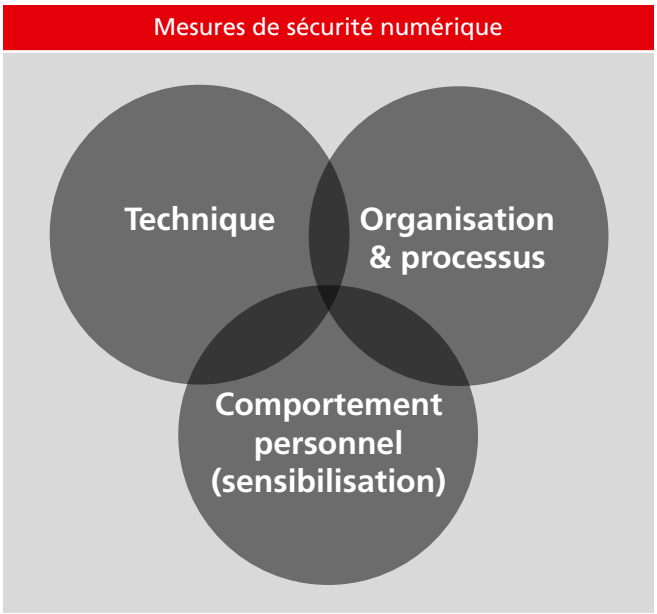

Figure 6 : Mesures de sécurité numérique

Technique

Les solutions techniques augmentent la complexité et les coûts. Il vaut mieux s'appuyer sur les bonnes pratiques qui ont déjà fait leur preuve et renoncer aux expérimentations coûteuses.

Exemples :

- deux centres de calcul, systèmes redondants ;
- cryptage des appareils portables ;
- pare-feu, filtre web, protection anti-maliciels ;
- banc d'essai ;
- Network Access Control System ;
- Mobile Device Management Software ;
- système électronique de contrôle d'accès.

Organisation

Les mesures organisationnelles sont prises là où les mesures techniques ne sont pas judicieuses ou trop complexes.

Exemples :

- processus d'attribution des droits d'accès (principe des 4 yeux/double signature) ;
- prévention des cas d'urgence (p. ex. scénarios, alarme, organisation, mesures d'urgence, décisions réservées, exploitation d'urgence, retour à l'exploitation normale) ;
- accord de maintien du secret avec les collaborateurs ;
- accord de confidentialité avec les partenaires externes ;
- classification des documents ;
- programme d'élimination des documents.

Comportement personnel

Chaque collaborateur peut identifier toute nouvelle méthode d'attaque et mettre en place les mécanismes de protection adéquats. En même temps, le facteur humain est aussi l'une des principales menaces. La sensibilisation du personnel face au traitement responsable des informations et l'appel à la responsabilité personnelle sont les vecteurs de motivation visant à améliorer la sécurité numérique.

Exemples :

- conserver le notebook et la mallette toujours dans le coffre ;
- utiliser des mots de passe complexes ;
- prudence dans le traitement des courriels de provenance inconnue ;
- détruire les documents confidentiels (p. ex. déchiqueteur à documents) au lieu de les jeter simplement à la corbeille ;
- aucune discussion confidentielle par téléphone dans les lieux publics.

6.1.1 21 Étapes vers l'amélioration de la sécurité informatique

Approche proportionnelle aux risques

L'approche proportionnelle aux risques permet à toute entreprise (macroentreprise ou PME) de définir d'elle-même le risque et son attitude face au risque. Selon la taille de l'entreprise, l'attitude face au risque peut fortement diverger. Par exemple, dans une macroentreprise, la défaillance du système de gestion des marchandises peut provoquer des pertes énormes en termes de finances ou de réputation. La même défaillance a des effets beaucoup moins importants ou reste sans effets sur un microtransformateur (attendu que les flux de commandes et de marchandises quotidiens sont connus ou que des mesures de résilience simples sont déjà en place). Cette approche proportionnelle aux risques permet aux entreprises, indépendamment de leur taille d'origine, de se concentrer sur l'amélioration de la sécurité numérique en fonction de leurs possibilités (collaborateur, connaissance, finances, etc.).

Aide à l'application des recommandations

La présente aide s'adresse en particulier (mais pas seulement) aux petites et moyennes entreprises qui n'ont pas les moyens de concrétiser globalement le *NIST Framework Core* (voir chap. 6). Elle ne remplace pas l'évaluation des risques ainsi que la définition de l'attitude face aux risques. Il est recommandé de réduire de manière circonstanciée les risques identifiés dans le cadre de cette analyse de risque, conformément aux contrôles NIST (cf. chap. 6). Les recommandations suivantes servent de référentiel pour l'utilisateur et ne remplacent pas le *NIST Framework Core*.

L'aide se base sur le programme en 10 points élargi de l'Association Infosurance :[12]

Mesures pour une protection de base efficace			
1)	**Protégez vos données en faisant régulièrement des backups**		
	Il existe différentes manières de perdre des données: elle peuvent être écrasées par erreur, rendues illisibles à cause d'un défaut sur le disque dur, voire détruites par un incendie ou un dégât d'eau. 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 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 dont 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 résultats, 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.		
	Concrétisation		
	Totalement mis en œuvre. Commentaire :	Partiellement mis en œuvre. Commentaire :	Pas mis en œuvre. Commentaire :
2)	**Effectuez toujours les dernières mises à jour de votre antivirus**		
	Des programmes nuisibles, tels que par exemple les virus et les vers, peuvent paralyser vos infrastructures informatiques et mettre ainsi la vie de votre entreprise en péril. • Les virus informatiques peuvent modifier, corrompre, voire même détruire complètement données et programmes. Ces programmes malveillants peuvent vous être transmis en pièce jointe d'un email, par messagerie instantanée, etc. Sur Internet, ces virus sont souvent déguisés en programmes gratuits, pseudo-utiles ou de divertissement et s'activent en 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 pour 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 les 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 (clients) 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. Quoiqu'il en soit, les mises à jour doivent être effectuées chaque jour. • Demandez à vos collaborateurs de signaler immédiatement au responsable informatique les messages d'avertissement virus.		
	Concrétisation		
	Totalement mis en œuvre. Commentaire :	Partiellement mis en œuvre. Commentaire :	Pas mis en œuvre. Commentaire :

[12] *Téléchargeable à l'adresse suivante: http://www.kmu.admin.ch/dam/kmu/fr/dokumente/savoir-pratique/Informatique-et-IT/InfoSurance_10_Points_Programme_FR.pdf.download.pdf/InfoSurance_10_Points_Programme_FR.pdf*

Mesures pour une protection de base efficace			
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 de l'Internet et de l'échange électronique de données, c'est le pare-feu qui remplit cette fonction sécuritaire. • En l'absence de pare-feu, n'importe qui peut s'immiscer dans votre système informatique, exécuter des taches à votre insu, utiliser votre ordinateur pour lancer des attaques illégales contre des tiers, ou bien encore accéder à des données commerciales confidentielles relevant de la loi sur la protection des données. • Vous trouverez dans le commerce des produits faisant à la fois office de pare-feu et d'antivirus. Ces produits combinés sont particulièrement indiqués pour les petites entreprises. • Les systèmes d'exploitation disposent en général d'un pare-feu intégré. Profitez systématiquement de cette possibilité et activez ces pare-feu. • Si vous utilisez un réseau local sans fil (WLAN) dans votre entreprise, veillez à ce qu'il soit sûr et sécurisé. • Toutes les passerelles réseau doivent être sécurisées par un pare-feu. • Tout le trafic Internet doit passer à travers le crible du pare-feu. N'autorisez aucun autre accès à Internet (par ex. via modem). • N'utilisez aucun ordinateur portable ou réseau local sans fil privé sans protection adéquate ni autorisation écrite du responsable informatique. • Protégez la configuration de votre pare-feu avec un mot de passe complexe.		
	Concrétisation		
	Totalement mis en œuvre. Commentaire :	Partiellement mis en œuvre. Commentaire :	Pas mis en œuvre. Commentaire :
4)	**Effectuez régulièrement les mises à jour de vos logiciels**		
	De la même manière que vous entretenez régulièrement votre voiture, vous devez veiller à ce que les programmes informatiques de votre entreprise soient régulièrement mis à jour pour être toujours au top niveau. • Les logiciels actuels contiennent souvent des millions de lignes codées. Or malgré les contrôles, il arrive parfois qu'une erreur se faufile à travers ces lignes. 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 rattraper les erreurs connues. • Si vous ne mettez pas à jour régulièrement vos programmes, 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 et n'installez donc 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.		
	Concrétisation		
	Totalement mis en œuvre. Commentaire :	Partiellement mis en œuvre. Commentaire :	Pas mis en œuvre. Commentaire :

Mesures pour une protection de base efficace

5) Choisissez des mots de passe complexes

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 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 informatique.
- Invitez vos collaborateurs à choisir des mots de passe compliqués qu'ils devront changer régulièrement. Ils 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.
- N'utilisez aucun mot de passe pouvant se trouver dans un dictionnaire.
- 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.

Concrétisation

Totalement mis en œuvre. Commentaire :	Partiellement mis en œuvre. Commentaire :	Pas mis en œuvre. Commentaire :

6) Protégez vos appareils portables

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. Aussi, quiconque est tenu, pour des raisons professionnelles, de stocker des données sensibles sur un appareil portable, doit prendre des mesures spéciales.

- Tous les ordinateurs portables doivent être protégés par un mot de passe compliqué (cf. point 5) et les données stockées doivent être protégées par un code d'accès. Sinon, n'importe qui pourrait accéder aux données commerciales de votre entreprise en cas de perte ou de vol d'un portable.
- Les appareils portables ne devraient contenir que les données strictement nécessaires à leur fonction.
- Les appareils portables doivent être passés régulièrement à l'antivirus, car ils sont synchronisés avec les autres ordinateurs de l'entreprise, à travers les fonctions de messagerie électronique par exemple.
- Une connexion WLAN mal configurée peut permettre aux cybercriminels de s'immiscer, en quelques minutes et jusqu'à une distance 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, PC de poche) 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 ultraconfidentielles, utilisez exclusivement des connexions protégées par un réseau privé virtuel (VPN).

Concrétisation

Totalement mis en œuvre. Commentaire :	Partiellement mis en œuvre. Commentaire :	Pas mis en œuvre. Commentaire :

Mesures pour une protection de base efficace			
7)	**Expliquez vos directives pour l'utilisation des moyens informatiques**		
	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'utilisateur informatique. 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. • Intégrez vos directives pour l'utilisation des moyens informatiques dans les contrats de travail et expliquez-les à vos collaborateurs. • Abordez régulièrement le problème de la sécurité dans votre entreprise en multipliant les approches. • Organisez des campagnes de sensibilisation sur ce thème une à deux fois par an. C'est facile à réaliser et cela nécessite très peu de moyens: courriels à tous 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 par exemple). Objectifs : – avantages de la sécurité informatique – création de mots de passe compliqués – pratique sécurisée d'Internet et de la messagerie électronique – classement des documents • Réglementez – 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 autorisé ou non) – l'utilisation de la messagerie électronique (confidentialité, transfert, boîtes de messagerie privées, chaînes de lettres, etc.) – le mode de gestion 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 et appliquez ces sanctions en cas de nécessité.		
	Concrétisation		
	Totalement mis en œuvre. Commentaire :	Partiellement mis en œuvre. Commentaire :	Pas mis en œuvre. Commentaire :

Mesures pour une protection de base efficace			
8)	**Protégez l'environnement de vos infrastructures informatiques**		
	Savez-vous qui entre et qui sort de votre entreprise chaque jour ? Quelques dispositions suffisent pour éviter que n'importe qui puisse accéder à des informations commerciales importantes. Un système de sécurité visible est aujourd'hui un critère de qualité qui ne manquera pas d'inspirer confiance à vos clients et à vos fournisseurs. A 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 n'est pas possible, 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 clés passepartout qu'il convient de réexaminer 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 n'est pas possible, enfermez le serveur dans un caisson *(rack)*. • N'entreposez pas d'objets inflammables (papier par exemple) ni dans le local du serveur, ni à proximité. • Ne placez pas d'imprimante réseau dans des pièces accessibles au public pour 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.		
	Concrétisation		
	Totalement mis en œuvre. Commentaire :	Partiellement mis en œuvre. Commentaire :	Pas mis en œuvre. Commentaire :

Mesures pour améliorer la confidentialité			
9)	**Réglementez la protection de l'accès aux données**		
	Mettez votre entreprise à l'abri des accès non-autorisés et protégez vos données pour 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 telles ou telles ressources informatiques ou informations. Il convient d'attribuer les droits d'accès selon la fonction occupée (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. Ces autorisations devront être régulièrement passées en revue pour être adaptées le cas échéant à la situation courante. • Lorsque des collaborateurs quittent définitivement l'entreprise ou dans le cas de changements dans l'organigramme interne, il convient de bloquer ou de modifier les comptes d'utilisateur correspondants, ainsi que les droits d'accès qui vont avec. • Les comptes des responsables systèmes et des administrateurs feront bien sûr l'objet d'une attention particulière, dans la mesure où ils disposent généralement de droits très étendus.		
	Concrétisation		
	Totalement mis en œuvre. Commentaire :	Partiellement mis en œuvre. Commentaire :	Pas mis en œuvre. Commentaire :
10)	**Verrouillez l'accès à vos appareils portables et cryptez les données lors des transferts**		
	Le transfert non sécurisé de données confidentielles (par courriel par ex.) risque de les soumettre à des regards plus ou moins indiscrets. En cas de perte de votre ordinateur portable, vos données risquent de tomber dans de mauvaises mains. Pour garantir la confidentialité de vos données, vous devez procéder à leur cryptage aussi bien pour les stocker sur vos ordinateurs portables que lors des transferts. • Les courriels peuvent être lus par des tiers. Il convient donc de crypter les messages dont le contenu est confidentiel. • Les appareils portables tels que notebooks doivent être cryptés par principe. • Pour acheminer des données confidentielles, utilisez exclusivement des connexions protégées par un réseau privé virtuel (VPN) (cf. aussi point 6).		
	Concrétisation		
	Totalement mis en œuvre. Commentaire :	Partiellement mis en œuvre. Commentaire :	Pas mis en œuvre. Commentaire :

Mesures pour améliorer la confidentialité			
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. Le cas échéant. Faites signer un accord de confidentialité à vos collaborateurs et partenaires externes. • Vos collaborateurs, qu'ils soient internes ou externes à l'entreprise, manipulent souvent des données confidentielles. Ces personnes doivent donc avoir bien clair à l'esprit les mesures à adopter pour garantir la confidentialité des informations traitées. • Incluez une clause de confidentialité dans le contrat de travail de vos collaborateurs. De même, créez un cadre contractuel pour régir vos rapports avec collaborateurs externes et 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 de l'information. • Informez vos collaborateurs des sanctions auxquelles ils s'exposent s'ils ne respectent pas ces directives et appliquez ces sanctions en cas de nécessité.		
	Concrétisation		
	Totalement mis en œuvre. Commentaire :	Partiellement mis en œuvre. Commentaire :	Pas mis en œuvre. Commentaire :
12)	**Réglementez l'élimination des informations et des supports de données**		
	En cas d'élimination non conforme, des informations confidentielles peuvent parvenir dans de mauvaises mains. Expliquez à vos collaborateurs comment éliminer de manière sûr et écocompatible les informations et les supports de données (papier, supports électronique de données). • Réglementez les modalités d'élimination : – du vieux papier (journaux, publicités et autres documents officiels) – de tous les autres documents internes et confidentiels – du carton – des supports électroniques de données tels que clés USB, CD et disques durs externes • Fixez les modalités d'élimination des archives. • Informez vos collaborateurs des sanctions auxquelles ils s'exposent s'ils ne respectent pas ces directives et appliquez ces sanctions en cas de nécessité.		
	Concrétisation		
	Totalement mis en œuvre. Commentaire :	Partiellement mis en œuvre. Commentaire :	Pas mis en œuvre. Commentaire :

Mesures pour améliorer la disponibilité			
13)	**Vérifiez vos systèmes informatiques**		
	Votre système informatique doit toujours être opérationnel à 100%. Pour cela, il doit faire l'objet d'une maintenance préventive et régulière qui diminuera le risque de pannes et de préjudices. • Contrôlez régulièrement l'opérationnalité de votre système informatique : – Le système de backup est-il au point ? – Les données sauvegardées sont-elles effectivement lisibles ? – Le système d'alimentation sans interruption (ASI) est-il opérationnel ? – Y a-t-il des messages d'erreur dans l'historique système ? • Les aspects organisationnels sont également à prendre en compte : – Les dispositions réglementaires 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 contrôle : – Définissez le calendrier et les responsabilités des opérations de maintenance. – Les opérations de maintenance doivent être contrôlables et compréhensibles. • Faites signer un accord de confidentialité au personnel externe chargé de la maintenance (cf. point 11).		
	Concrétisation		
	Totalement mis en œuvre. Commentaire :	Partiellement mis en œuvre. Commentaire :	Pas mis en œuvre. Commentaire :
14)	**Protégez l'accès à votre réseau d'entreprise par une authentification à deux facteurs**		
	Pour des raisons de sécurité, l'accès externe au réseau d'entreprise nécessite une authentification à deux facteurs. Cette procédure offre une protection appropriée et est un standard industriel reconnu. • Définissez les variantes d'accès possibles : – accès par application – accès par réseau – accès VPN *(site-to-site)* • Définissez les catégories (collaborateurs internes, collaborateurs externes, clients, fournisseurs, invités) et attribuez les droits d'accès en fonction des services.		
	Concrétisation		
	Totalement mis en œuvre. Commentaire :	Partiellement mis en œuvre. Commentaire :	Pas mis en œuvre. Commentaire :

Mesures pour améliorer la disponibilité			
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 informatiques, vous devez tout faire pour éviter une panne de courant. Une alimentation sans interruption (ASI) protège vos systèmes informatiques d'une coupure de courant et des surcharges (foudre), permettant ainsi d'éviter la perte de données. • L'appareil d'alimentation sans interruption (ASI) doit être installé 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. • Par ailleurs, les ASI permettent de stabiliser la tension d'alimentation de vos appareils. • Votre serveur bien sûr, mais aussi d'autres périphériques importants doivent être équipés d'un appareil ASI, comme les principaux ordinateurs d'un réseau, le routeur, le système de backup, etc. • Faites l'inventaire des composants qui doivent être branchés sur l'appareil de secours ASI. Cette liste vous permettra de déterminer la puissance nécessaire de votre appareil USV. • Contrôlez régulièrement les batteries de l'appareil ASI et remplacez-les le cas échéant (cf. point 13).		
	Concrétisation		
	Totalement mis en œuvre. Commentaire :	Partiellement mis en œuvre. Commentaire :	Pas mis en œuvre. Commentaire :
16)	**Misez sur la redondance des modules importants**		
	Un serveur qui tombe en panne par exemple peut avoir de graves répercussions économiques et paralyser votre entreprise. Beaucoup d'entreprises ignorent à quel point elles dépendent de certains matériels informatiques essentiels. Pour permettre à votre entreprise de reprendre son activité le plus vite possible après une panne, il est recommandé de disposer de systèmes redondants (disques durs, composants de réseau ou serveurs complets). • La redondance signifie que vous disposez d'au moins un appareil ou système de rechange identique à même de prendre la relève en cas de panne. • 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 de travail, d'autres disques durs prennent automatiquement le relais, sans interrompre les activités en cours. • Souscrivez des contrats de service après-vente avec vos fournisseurs de matériel informatique et de logiciels dans lesquels vous préciserez bien les temps de réaction, les délais de livraison, etc. • Vous pouvez également élaborer avec eux des scénarios d'urgence (cf. point 17). • N'utilisez que des composants de marques reconnues, dans la mesure où ils sont généralement de bonne qualité, ayant été soumis à des tests intensifs. • Au-delà de la redondance de vos systèmes informatiques, songez également à une connexion Internet redondante. • L'essentiel est que vos modules de secours soient identiques et qu'ils soient préconfigurés afin de pouvoir prendre immédiatement le relais.		
	Concrétisation		
	Totalement mis en œuvre. Commentaire :	Partiellement mis en œuvre. Commentaire :	Pas mis en œuvre. Commentaire :

Mesures pour améliorer la disponibilité

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. Pour cela, il est nécessaire de planifier à l'avance la conduite à tenir et les actions à mettre en œuvre.

- Envisagez les situations d'urgence qui pourraient se présenter dans votre entreprise et réfléchissez à la façon dont il faudrait réagir dans les différents cas. Imaginez les scénarios suivants: panne du système informatique, 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 res ponsable et qui alerter. Pour cela, établissez un plan d'alerte et une note technique sur la répartition des responsabilités.
- Votre plan d'urgence doit prévoir les mesures à prendre pour l'activation du plan d'urgence, la gestion de la situation d'urgence et le rétablissement rapide du fonctionnement normal de l'entreprise.
- Enseignez à vos collaborateurs la conduite à suivre en cas d'urgence et les premières mesures qu'ils doivent prendre.
- L'individu 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 régulièrement tous vos composants informatiques. Cette documentation doit être conservée à l'extérieur de l'entreprise.
- Cette documentation contiendra notamment une liste des utilisateurs, des groupes et des différentes autorisations (cf. point 9), le plan du réseau, les configurations système, 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 informatiques. Celui-ci devra garantir un haut niveau de disponibilité afin de permettre une prompte reprise de l'activité.
- Testez le temps de réaction du système de secours selon vos besoins en disponibilité. Une panne de serveur peut-elle être vraiment réparée dans les temps ?

Concrétisation

Totalement mis en œuvre. Commentaire :	Partiellement mis en œuvre. Commentaire :	Pas mis en œuvre. Commentaire :

18) Gérez et distribuez le savoir-faire

Dans les PME de plus petite taille, les connaissances informatiques stratégiques 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, faire fonctionner et entretenir les systèmes informatiques d'une entreprise. Faites en sorte que le savoir stratégique soit documenté et partagé par plusieurs personnes.
- La maladie, un accident, un décès ou le départ de votre responsable informatique peut provoquer la perte de ce précieux savoir.
- Veillez à ce que les procédures et systèmes importants fassent l'objet d'une documentation appropriée. Cela facilitera les successeurs et nouveaux collaborateurs à se repérer rapidement (cf. point 17).
- Conservez les mots de passe importants en double dans un coffre.
- Sécurisez les informations significatives liées aux activités de vos collaborateurs démissionnaires.

Concrétisation

Totalement mis en œuvre. Commentaire :	Partiellement mis en œuvre. Commentaire :	Pas mis en œuvre. Commentaire :

Mesures dans le secteur alimentaire			
19)	**Connexion redondante au *WAN/Cloud***		
	La défaillance du *WAN/Cloud* peut interrompre la connexion aux systèmes centraux, aux systèmes décentralisés et aux systèmes clients. • connexion redondante au *WAN* pour tous les systèmes vitaux de la filière alimentaire.		
	Concrétisation		
	Totalement mis en œuvre. Commentaire :	Partiellement mis en œuvre. Commentaire :	Pas mis en œuvre. Commentaire :
20)	**Utilisez des plateformes autonomes pour la production et la logistique**		
	La défaillance du *WAN/Cloud* peut interrompre la connexion aux systèmes centraux, aux systèmes décentralisés et aux systèmes clients. Les systèmes de vente, de production et de logistique ne sont alors plus disponibles. • segmenter le réseau : – réseau administratif transversal intégrant tous les systèmes centraux – réseaux locaux pour chaque site de production et chaque site logistique • veiller au fonctionnement autonome des systèmes SCI/SCADA indépendamment du *WAN* : – gestion des systèmes de production et de stockage – systèmes de bâtimotique et de surveillance – systèmes de logistique et de préparation des livraisons – systèmes d'encaissement		
	Concrétisation		
	Totalement mis en œuvre. Commentaire :	Partiellement mis en œuvre. Commentaire :	Pas mis en œuvre. Commentaire :
21)	**Utilisez une norme de communication (p. ex. EDI *Electronic Data Interchange*)**		
	GS1 Suisse est l'association professionnelle qui contribue à la création de valeur pour des réseaux durables. GS1 Suisse est membre de GS1, réseau mondial qui regroupe plus d'une centaine d'organismes nationaux et dont les membres bénéficient de prestations de qualité répondant à des standards communs. GS1 est une plateforme de compétence pour l'optimisation globale de la logistique, de la chaîne logistique et de la gestion de la demande en Suisse et au Liechtenstein. Nous vous recommandons : – d'appliquer les normes internationales de GS1 – d'utiliser les modèles de procédure recommandés – de suivre la formation continue pratique		
	Concrétisation		
	Totalement mis en œuvre. Commentaire :	Partiellement mis en œuvre. Commentaire :	Pas mis en œuvre. Commentaire :

Tableau 50 : 21 étapes pour améliorer la protection des informations

6.1.2 Cinq mesures de sécurité pour les systèmes de contrôle industriels

Voici cinq mesures importantes que les organisations peuvent appliquer dans leurs environnements SCI/SCADA. L'application de ces mesures permettra d'évoluer vers un environnement de sécurité plus résistant tout en réduisant considérablement le risque pour les systèmes d'exploitation.

Cinq mesures de sécurité pour les systèmes SCADA
1) Identifiez, réduisez et assurez toutes les connexions réseau de votre environnement SCADA.
2) Rendez votre système SCADA et les systèmes auxiliaires plus résistants en désactivant les services, ports et protocoles inutiles, en activant les fonctions de sécurité disponibles et en créant des procédures résistantes pour la gestion des configurations.
3) Surveillez et évaluez en permanence la sécurité des systèmes SCADA et des réseaux ainsi que de leurs interconnexions.
4) Intégrez une approche proportionnelle aux risques et autodéfensive pour protéger les systèmes et les réseaux SCADA.
5) Gérez les exigences « humaines » des systèmes SCADA en fixant les critères de responsabilisation des individus en fonction de leurs prestations, en créant des directives et en proposant des formations de sécurité SCADA pour tous les exploitants et administrateurs.

Tableau 51: Cinq mesures de sécurité pour les systèmes SCADA

6.2 Références, documents et normes

Le présent document tient compte des concepts, recommandations et mesures de diverses normes et autres documents normatifs (Tableau 52).

Titre	Année	Éditeur(s) et description
Mesures de protection des systèmes de contrôle industriels (SCADA)	2013	Éd. : **Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI** Basées sur des documents américains de l'Industrial *Control Systems Cyber Emergency Response Team* (SCADA-CERT) ainsi que du *National Institute of Standards and Technology* (NIST), ces instructions décrivent en 8 pages, de façon succincte et pragmatique, les 11 principales mesures à mettre en œuvre par les exploitants SCADA.
Analyse des risques et de la vulnérabilité du secteur Approvisionnement alimentaire	2016	Éd. : **Office fédéral pour l'approvisionnement économique du pays (OFAE)** Cette analyse des risques et des vulnérabilités repose sur la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) et sur la stratégie nationale pour la protection des infrastructures critiques (PIC). Elle a pour but d'analyser la vulnérabilité aux défaillances ou aux perturbations des TIC dans le secteur partiel critique de l'approvisionnement en électricité.
Guide pour la protection des infrastructures critiques (Guide PIC)	2015	Éd. : **Office fédéral de la protection de la population (OFPP)** Ce guide constitue un instrument d'examen et, le cas échéant, d'amélioration de la résilience des infrastructures critiques. Il est notamment conçu pour être utilisé dans des sous-secteurs (aussi appelés secteurs partiels) critiques (tels que l'approvisionnement en électricité) par les exploitants, les associations sectorielles (comme l'AES) et les autorités compétentes. Le guide décrit pour l'essentiel une procédure potentielle de gestion des risques: analyse (identification des ressources, vulnérabilités, risques), évaluation, mesures et leurs mise en œuvre, contrôle et amélioration. Cette procédure peut tout à fait ou devrait être intégrée aux processus de gestion existants ou exécutée sur la base de ces derniers.
Stratégie nationale pour la protection des infrastructures critiques (PIC)	2012	Éd. : **Office fédéral de la protection de la population (OFPP)** La stratégie transcrit le champ d'application, désigne les infrastructures critiques (notamment l'approvisionnement en électricité de criticité très importante) et fixe les principes directeurs de la PIC. La stratégie nationale PIC s'adresse à tous les services qui ont des responsabilités dans ce domaine, en particulier aux différentes autorités concernées, aux responsables politiques et aux exploitants d'infrastructures critiques (p. ex. entreprises d'approvisionnement en énergie EAE).
Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC)	2012	Éd. : **Unité de pilotage informatique de la Confédération (UPIC)** La protection des infrastructures TIC contre les cyberrisques représentant un intérêt majeur pour la Suisse, le Conseil fédéral a ordonné l'élaboration d'une stratégie nationale visant à protéger notre pays contre de tels risques. Cette stratégie a pour but de dresser un panorama actuel de ces risques et de montrer les moyens dont dispose la Suisse pour y faire face, où se situent les lacunes et comment y remédier le plus efficacement possible. La stratégie identifie les structures existantes et définit des objectifs ainsi que 7 champs d'action assortis de mesures ad hoc (p. ex. analyses des risques et des vulnérabilités d'un secteur partiel tel que l'approvisionnement en électricité – cf. ci-dessus).

Titre	Année	Éditeur(s) et description
Loi fédérale sur l'approvisionnement économique du pays (loi sur l'approvisionnement du pays, LAP)	État 2016	Éd. : **Assemblée fédérale de la Confédération helvétique** Cette loi régit les mesures visant à garantir l'approvisionnement du pays en biens et services vitaux lors d'une pénurie grave à laquelle les milieux économiques ne peuvent pas faire face par leurs propres moyens. La Confédération peut encourager, dans les limites des crédits autorisés, des mesures prises par des entreprises de droit privé ou public pour garantir l'approvisionnement économique du pays si ces mesures contribuent à renforcer substantiellement les préparatifs nécessaires pour garantir les systèmes d'approvisionnement et infrastructures vitaux en cas de pénurie grave. La présente norme minimale de sécurité numérique dans la filière alimentaire constitue l'une de ces mesures.
Loi fédérale sur les denrées alimentaires et les objets usuels (loi sur les denrées alimentaires, LDAl)	État 2013	Éd. : **Assemblée fédérale de la Confédération helvétique** Cette loi a pour but de protéger la santé du consommateur des risques présentés par les denrées alimentaires et les objets usuels qui ne sont pas sûrs, de veiller à ce que la manipulation des denrées alimentaires et des objets usuels se fasse dans de bonnes conditions d'hygiène et de protéger le consommateur contre les tromperies relatives aux denrées alimentaires.
Etude sectorielle KRITIS «*Ernährung und Wasser*»	État 2015	Éd. : **Office fédéral allemand de la sécurité des technologies de l'information (BSI)** L'Office fédéral allemand de la sécurité des technologies de l'information (BSI) est l'un des organes centraux parmi les autorités allemandes en charge de la protection des infrastructures critiques. Le BSI cultive les échanges avec les organismes sectoriels, publie les normes et les directives régissant les principaux aspects de la sécurité numérique. Il est également en charge de la direction des projets nationaux et de la coordination de l'UP KRITIS. Le BSI contribue ainsi à la mise en œuvre de la stratégie nationale de protection des infrastructures critiques (stratégie KRITIS) et de la stratégie nationale de cybersécurité. Dans ses travaux, le BSI acquiert une connaissance exacte du fonctionnement des secteurs critiques et de l'importance des infrastructures liées à ces secteurs (études KRITIS).
Gestion des risques et des situations de crise dans l'approvisionnement alimentaire en Autriche (EV-A)	État 2015	Éd. : **JOANNEUM RESEARCH, Agrarmarkt Austria** Le rapport condense les résultats du projet de gestion des risques et des situations de crises pour l'approvisionnement alimentaire en Autriche (EV-A), qui a été financé par l'Office fédéral autrichien des transports, de l'innovation et de la technologie dans le cadre du programme autrichien de promotion de la recherche sur la sécurité KIRAS.

Tableau 52 : Publications de la Confédération helvétique, des services administratifs et des associations constituant des références importantes pour la filière alimentaire.

Le Tableau 53 répertorie les normes internationales qui ont été partiellement prises en compte dans la présente norme.

Titre	Année	Éditeur(s) et description
ISO 27001:2013 *Information technology – Security techniques – Information security management systems – Requirements* ISO 27002:2013 *Information technology – Security techniques – Code of practice for information security controls*	2013	Éd. : **Organisation internationale de normalisation (ISO)** Cette norme détaille les exigences relatives à un système de management de la sécurité de l'information (SMSI). La suite ISO 27k comprend un série de *normes concernant la sécurité de l'information,* dont les suivantes présentent intérêt ici : • 27000:2016 Vue d'ensemble et vocabulaire (:2016 indique l'année de publication) • 27001:2013 Exigences: principes de base avec contrôles et objectifs de contrôle en annexe • 27002:2013 Guide pour les contrôles • 27003:2010 Lignes directrices pour la mise en œuvre • 27005:2011 Gestion des risques Désormais les plus répandues, les normes de sécurité ISO 27000 devraient s'avérer décisives dans les années à venir. Aujourd'hui déjà, la bonne approche consiste à observer les normes de sécurité ISO. Contrairement à d'autres textes normatifs comme IT-Grundschutz ou les normes de l'ANSI/ISA ou du NIST, elles ne sont pas aussi détaillées, sont utilisables de manière flexible et peuvent être améliorées et étendues en permanence sur une plus longue période.
Guide to Industrial Control Systems (ICS) Security SP 800-82 Rev.2	2015	Éd. : ***National Institute of Standards and Technology (NIST)*** Ce guide fournit une introduction complète aux SCADA, aux topologies et aux architectures, identifie les menaces et les vulnérabilités, et formule des recommandations pour les contre-mesures et l'atténuation des risques. Des contrôles spécifiques aux SCADA, basés sur le cadre 800-53 du NIST, sont également présentés.
ISA 62443 *Industrial communication networks – Network and system security*	2009 ss	Éd. : ***International Society of Automation (ISA)*** Série d'un total de 13 normes de sécurité et rapports techniques en matière de systèmes de contrôle-commande industriels (IACS). Ces normes sont généralement applicables dans le domaine de l'automatisation industrielle et ne sont pas spécifiques à l'approvisionnement en électricité. Elles se basent sur les normes ISO 27000 et les étoffent par l'ajout de différences et de particularités propres à l'automatisation industrielle. Il convient de mentionner notamment le traitement de l'architecture réseau et zonale, qui n'est guère ou pas aussi détaillé dans d'autres normes.
Recommended Practice: Improving Industrial Control System Cybersecurity with Defense in Depth Strategies	2016	Éd. : ***Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)*** Édition revue et corrigée d'une précédente publication datant de 2006. Introduction complète à la stratégie de défense en profondeur dans le cadre de la sécurité des systèmes de contrôle industriels.

Tableau 53 : Normes nationales et internationales relatives à la sécurité numérique

Titre	Année	Éditeur(s) et description
BSI IT-Grundschutz-Kataloge 15e addendum 2016 *BSI-Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz* (V1.2 2014) *BSI Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz*	2016	Éd. : ***Bundesamt für Sicherheit in der Informationstechnik (BSI)*** À l'aide des normes 100-1 à 100-4 du BSI, l'«*IT-Grundschutz*» (méthodologie de protection de base des technologies de l'information) décrit une procédure de mise en place et de maintien d'un système de management de la sécurité de l'information (SMSI). Les catalogues et le compendium de l'*IT-Grundschutz* détaillent la mise en œuvre des mesures et des objectifs qui en découlent. Le SMSI ainsi créé satisfait aux exigences de la norme ISO 27001 et dispose d'un équivalent aux recommandations de la norme ISO 27002. La sécurité peut être introduite et contrôlée selon les procédures de l'*IT-Grundschutz* développées par le BSI, mais aussi conformément aux normes de la famille ISO 27000. Ces deux options sont compatibles dans leur approche. Elles sont utilisées pour mettre en place et exploiter un SMSI, qui identifie les risques dans le domaine de la sécurité de l'information et les réduit à un niveau acceptable par le biais de mesures appropriées. Alors que l'analyse et l'évaluation des risques constituent un élément essentiel d'un SMSI conforme à la norme ISO 27001, cette analyse n'est requise que dans certains cas particuliers pour l'*IT-Grundschutz* du BSI. Les catalogues de cette protection de base décrivent par le menu la procédure permettant de réduire au maximum les risques. Quant aux normes ISO, elles laissent davantage de place à l'interprétation et offrent une plus grande souplesse, mais fournissent également des instructions et un soutien moins détaillés. À l'inverse, l'approche de l'*IT-Grundschutz,* comme son nom l'indique, offre une « protection de base ». L'effort requis pour obtenir la certification ISO est moindre.
BSI ICS Security-Kompendium	2013	Éd. : ***Bundesamt für Sicherheit in der Informationstechnik (BSI)*** Ce compendium est un ouvrage de référence destiné à faciliter l'accès à la sécurité informatique dans les SCADA. Les bases nécessaires à la compréhension des SCADA, les processus y afférents, les normes pertinentes et un lien concret avec l'*IT-Grundschutz* y sont expliqués, les différences et lacunes des normes établies, et en particulier de l'*IT-Grundschutz* dans le domaine de la sécurité SCADA étant mises en lumière.
BSI-Standard 100-1 Managementsysteme für Informations-sicherheit (ISMS)	2008	Éd. : ***Bundesamt für Sicherheit in der Informationstechnik (BSI)*** Cette norme décrit les méthodes, les tâches et les activités pertinentes qui font le succès d'un SMSI et précise les tâches qui incombent à la direction. La méthodologie de l'*IT-Grundschutz,* qui explique pas à pas comment développer un SMSI dans la pratique et cite des mesures concrètes pour tous les aspects relevant de la sécurité de l'information, favorise la mise en œuvre des recommandations. La norme 100-1 s'adresse aux responsables de l'exploitation informatique, aux délégués à la sécurité, ainsi qu'aux experts et conseillers en sécurité chargés de la gestion de la sécurité de l'information.
BSI-Standard 100-2 IT-Grundschutz Vorgehensweise	2008	Éd. : ***Bundesamt für Sicherheit in der Informationstechnik (BSI)*** La procédure de l'*IT-Grundschutz* décrit, étape par étape, comment mettre en place et exploiter un système de management de la sécurité de l'information dans la pratique et à l'aide des catalogues de cette protection de base. Elle se penche de façon très approfondie sur la manière d'élaborer en pratique un concept de sécurité, sur le choix des mesures de sécurité adéquates, ainsi que sur les éléments à prendre en compte lors de la mise en œuvre.

Titre	Année	Éditeur(s) et description
BSI-Standard 100-3 Risikoanalyse	2008	Éd. : ***Bundesamt für Sicherheit in der Informationstechnik (BSI)*** Ce document décrit une méthodologie pour réaliser des analyses de risques, qui complètent un concept de sécurité existant en matière de protection de base des technologies de l'information. Les dangers présentés dans les catalogues de l'*IT-Grundschutz* sont utilisés comme outils. Une différence essentielle par rapport à la plupart des autres méthodes d'analyse de risques est l'omission totale de la probabilité de survenance des dommages.
BSI-Standard 100-4 Notfallorganisation	2008	Éd. : ***Bundesamt für Sicherheit in der Informationstechnik (BSI)*** Ce document décrit une méthodologie pour mettre en place un système de gestion des cas d'urgence fondée sur les procédures figurant dans la norme 100-2 et les complétant. Il présente tous les processus au sein d'une organisation pour cas d'urgence, de l'analyse d'impact sur les affaires à la gestion de crise, en passant par le retour à l'exploitation normale et les activités continues de processus en dehors des situations de crise.
ISA 95/ISO 62264 Enterprise Control System Integration	2010 ss	Éd. : ***International Society of Automation (ISA)*** Série de 5 normes relatives à l'intégration des systèmes informatiques d'entreprise et de contrôle-commande.
Framework for Improving Critical Infrastructure Cybersecurity	2014	Éd. : ***National Institute of Standards and Technology (NIST)*** Ce cadre découle de l'exigence posée par le décret présidentiel américain intitulé «*Improving Critical Infrastructure Cybersecurity*» (Améliorer la cybersécurité des infrastructures critiques), datant de 2013. Il s'agit d'une compilation de différentes orientations visant à déterminer le statut actuel d'une entreprise et à définir une feuille de route pour l'amélioration des pratiques de cybersécurité en se référant à d'autres cadres et normes tels que ISO 27001, ISA 62443, NIST 800-53 et COBIT.
Communication network dependencies for ICS/SCADA Systems	2016	Éd. : ***European Union Agency for Network and Information Security (ENISA)*** Ce rapport se focalise sur les aspects des réseaux de communication et de l'intercommunication entre les systèmes SCI/SCADA et l'identification des vulnérabilités, des risques, des menaces et des conséquences en matière de sécurité pouvant être causés par les systèmes cyber-physiques. Il comporte également un certain nombre de recommandations destinées à réduire les risques détectés. La principale conclusion de l'étude préliminaire est une liste de pratiques et de directives éprouvées visant à limiter autant que possible la surface des systèmes ICS/SCADA exposée aux attaques. Le document a pour objectif principal de fournir un aperçu des dépendances des réseaux de communication des systèmes ICS/SCADA et d'identifier les ressources critiques en matière de sécurité et les scénarios d'attaques et menaces réalistes contre ces réseaux de communication.

Tableau 53 : Normes nationales et internationales relatives à la sécurité numérique

6.3 Glossaire

Abréviation	Description
BSI	*Bundesamt für Sicherheit in der Informationstechnik* (Allemagne)
Détaillant	Entreprise opérant dans la distribution et la vente d'aliments
DMZ	*Demilitarized Zone* (zone démilitarisée), réseau informatique avec accès sécurisé (il est souvent utilisé pour garantir une séparation logique entre deux zones de réseaux)
DNS	*Domain Name System*
eDec	Déclaration électronique des données. Système de l'Administration fédérale des douanes pour déclarer les marchandises importées.
ENISA	*European Union Agency for Network and Information Security*
ERP	*Enterprise Ressource Planning-System*
Facility Control	Technique du bâtiment, pilotage et surveillance des installations
Field	*Champ*
FINMA	Autorité fédérale de surveillance des marchés financiers
HIDS	*Host Intrusion Detection System*
HMI	*Human Machine Interface,* organe ou action permettant de mettre en contact un être humain avec une machine
IaaS	*Infrastructure as a Service*
ICS	Synonyme de « SCADA »
IDS	*Intrusion Detection System*
IP	*Internet Protocol*
IPS	*Intrusion Prevention System*
ISA	*International Society of Automation*
ISO	Organisation internationale de normalisation
MELANI	Centrale d'enregistrement et d'analyse pour la sûreté de l'information
MOU/MOA	*Memorandum of Understanding/Agreement*
MPLS	*Multiprotocole Label Switching,* technologie utilisée pour les transferts de données
MPLS-TP	*Multiprotocole Label Switching Transport Profile*
NAC	*Network Access Control*
NIST	*National Institute of Standards and Technology*
OFAE	Office fédéral pour l'approvisionnement économique du pays
OFPP	Office fédéral de la protection de la population
OT	*Operational Technology* (en particulier systèmes SCADA)
PaaS	*Platform as a Service*
PC	*Personal Computer*

Abréviation	Description
PDH	*Plesiochronous Digital Hierarchy,* technologie utilisée pour les communications vocales et les transferts de données
Pilotage de la production	voir SCADA
Producteur (paysan)	Il est chargé de produire des ressources (céréales, betteraves sucrières, élevage du bétail, etc.)
PRTG Network Monitor	*PRTG Network Monitor* est une solution complète de monitorage de réseau pour surveiller les durées de téléchargement et de téléversement, du trafic et de l'utilisation.
Réseau de communication	Réseau de communication interne pour les données et le vocal.
SaaS	*Software as a Service*
SCADA	*Supervisory Control and Data Acquisition,* surveillance et pilotage des processus techniques. Le système SCADA intègre, outre la surveillance et le pilotage, les capteurs, les lignes, les ordinateurs et la centrale de télégestion du système (de production). Citons notamment les systèmes pour préparer livraisons, pour gérer la production des transformateurs et pour l'encaissement chez les détaillants. L'abréviation « SCADA » est ici synonyme de « SCI ».
SCI	Synonyme de « SCADA »
SDH	*Synchronous Digital Hierarchy,* technologie utilisée pour la communication vocale et le transfert des données
SIEM	*Security Incident and Event Management*
SLA	*Service Level Agreement,* convention de prestations
SMSI	Système de management de la sécurité de l'information
TED	Traitement électronique des données
Télégestion	Télégestion du réseau, des stations et des centrales électriques
TI	Technologie de l'information, ici en particulier Office-IT/bureautique. Tout ce qui n'est pas OT/SCADA.
TIC	Technologies de l'information et de la communication
Transformateur	Il utilise des matières premières (céréales, viande, huile, etc.) pour les transformer en produits. Relève de l'industrie agro-alimentaire.
UPIC	Unité de pilotage informatique de la Confédération
VoIP	*Voice over IP*
VPN	*Virtual Private Network*
WAN	*Wide Area Network*

Tableau 54 : liste des abréviations

6.4 Liste des figures

6.5 Liste des tableaux

Auteurs et experts de la première édition

Prénom, nom	entreprise	fonction
Dario Walder	OFAE	auteur principal/ direction du projet
Daniel Caduff	OFAE	co-auteur
Walter Stadelmann	AEP	co-auteur/expert
Maximilian Müller	Emmi	expert/assurance qualité
Ralf Kraekel	Migros	expert/assurance qualité
Philippe Gehring	Cremo	expert/assurance qualité
Franz Leugger	Coop	expert/assurance qualité
Fabian Heiz	Coop	expert/assurance qualité

Chronologie

Date	bref descriptif
septembre 2016	L'équipe TIC-alimentation de l'AEP commence ses travaux.
octobre 2017	premier jet du document en cours d'élaboration
décembre 2017	discussions sur le premier jet TIC-alimentation AEP
février 2018	discussions sur le second jet TIC-alimentation AEP
avril 2018	discussions sur le troisième jet TIC-alimentation AEP
juin à novembre 2018	consultation des associations professionnelles
octobre 2018	consultations au sein de l'AEP

Exclusion de responsabilité

Le présent document contient des recommandations pour améliorer la sécurité des systèmes informatiques utilisés dans la filière alimentaire ainsi que des systèmes de pilotage industriel dans l'agroalimentaire. Il a été rédigé scrupuleusement par les personnes et équipes ayant participé à sa création. L'Office fédéral pour l'approvisionnement économique du pays décline toute responsabilité, explicite ou implicite. Cela vaut aussi pour les experts, entreprises et collaborateurs impliqués. Seul l'utilisateur est responsable de la sécurité informatique et des dégâts éventuels dans son exploitation.

Impressum et interlocuteurs

Editeur
Office fédéral pour l'approvisionnement économique du pays (OFAE)
Bernastrasse 28, CH-3003 Bern
info@bwl.admin.ch, www.bwl.admin.ch
Téléphone +41 58 462 21 71

Associations consultées
CI Commerce de détail Suisse
Swiss Retail Federation