step by STEP

Liste de contrôle OT et IT TIC Norme minimale

024 Cybersécurité dans les Systèmes de contrôle de la production OT et Réseaux administratifs IT

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

Documents d‘intervention

Prévention

Les informations techniques et les exemples pratiques servent de base à la prévention (mesures de précaution et considérations avant qu'un événement ne se produise) et d’outil de planification pour la mise en œuvre de rénovations et d’agrandissements.

Documents d‘intervention

Sur la base des instructions et des conditions spécifiques locales, des instructions d'action applicables à votre station d’épuration peuvent être répertoriées dans les formulaires correspondants step by STEP. En cas d'incident, cela permet une évaluation rapide de la situation et le déclenchement d'actions réfléchies.

Formulaires d’intervention

Documents qui vous sont utiles avant, pendant et après un événement:

F_1 Avis d‘incident
F_1.1 Evaluation primaire

F_4 Avis de fin d‘incident
F_4.1 Analyse des dommages, prévention

F_10 Cas individuels

Table des matières Page

1. Mise en œuvre des normes minimales en matière de TIC OT et IT

1.1 Introduction

La norme minimale en matière de TIC de l'OFAE (Office fédéral de l'approvisionnement économique du pays) divise la prévention des cyberattaques et de leurs effets en cinq points. La liste de contrôle présentée ici a la même structure que la norme minimale TIC pour améliorer la résilience Informatique. Elle est également divisée en cinq fonctions sur la base du NIST Cybersecurity Framwork Core:

1. Identifier (Identify),

2. Protéger (Protect),

3. Détecter (Detect),

4. Réagir (Respond) et

5. Récupérer (Recover).

Nous recommandons d'effectuer la mise en œuvre avec tous les spécialistes impliqués et de consulter le document "Norme minimale pour améliorer la résilience Informatiques". Les contrôles individuels contiennent une référence à l'activité ou aux activités correspondantes de l'outil d'évaluation des normes minimales TIC. Cet outil est disponible sous la forme d'un fichier Excel qui guide l'utilisateur à travers les différentes fonctions.

→ https://www.bwl.admin.ch/bwl/fr/home.html

La liste de contrôle et la norme minimale en matière de TIC ne servent pas à traiter un événement. Ils montrent s'il y a lieu d'agir en ce qui concerne les mesures préventives de protection contre les cyberattaques.

Les listes de contrôle step by STEP ont été mises au point pour mettre en pratique la norme minimale en matière de TIC. Les listes de contrôle sont basées sur l'application pratique de la norme minimale TIC dans les stations d'épuration des eaux usées et ont été complétées par d'autres points sur la base de l'expérience pratique.

Les listes de contrôle step by STEP permettent aux opérateurs de procéder à une auto-évaluation sans avoir à se familiariser avec la norme minimale TIC.

Étant donné que la norme minimale en matière de TIC contient de nombreux termes techniques, il est recommandé de consulter un expert indépendant en sécurité (non-affilié au fournisseurs IT ou OT) pour la sécurité de l'information (cybersécurité) pendant la mise en œuvre. Cet expert coordonne, accompagne et vérifie la définition des mesures techniques et organisationnelles et leur mise en œuvre entre les différents acteurs.

L'éditeur de step by STEP peut fournir des informations pour aider à l'évaluation des entreprises appropriées.

1.2 Réalisation de l'auto-évaluation

Avec les listes de contrôle step by STEP ci-dessous, l'opérateur peut effectuer une auto-évaluation sans avoir à se familiariser avec la norme minimale TIC.

Les listes de contrôle step by STEP contiennent les questions et les points essentiels. Grâce à leur traitement et à leur mise en œuvre, l'exploitant atteint un niveau élevé de sécurité et de fiabilité pour ses systèmes.

Répondez aux questions des listes de contrôle suivantes. Si vous n'êtes pas en mesure de répondre à plusieurs questions par un OUI clair, il est nécessaire d'agir. Les listes de contrôles vous permettent d'identifier la personne la mieux placé afin de vous aider dans votre tâche. Pour cela, il vous suffit de vous référer aux cinq colonnes de droite : IT, BT, CT, OT et WP.

Afin de garantir la sécurité informatique, l'échange entre l'opérateur, le spécialiste de la sécurité, le fournisseur de systèmes informatiques et d'OT est nécessaire. Ceci garantit un fonctionnement sûr et ininterrompu. L'externalisation de la sécurité informatique n'est donc pas recommandée. La mise en œuvre des mesures techniques et organisationnelles peut être coordonnée, accompagnée, contrôlée et exécutée avec la participation d'experts externes.

2. step by STEP listes de contrôle de la cybersécurité

Les listes de contrôles step by STEP Cyber Security se réfèrent chacune à la norme minimale TIC et les cinq colonnes tout à droite indiquent qui doit être inclus dans les étapes respectives.

2.1 Inventaire et identification

Afin d'analyser et de planifier les mesures, un inventaire des différents systèmes et des risques associés doit être établi. Cela permet de développer une stratégie de sécurité efficace et adaptée à l'installation.

IT = Fournisseur informatique BT = Opérateur CT = Expert en cybersécurité OT = Fournisseur de systèmes de contrôle
WP = Fournisseur d'outils (par ex. fournisseur du programme pour le plan de maintenance)

x = Responsable (x) = A consulter

Manquement	Référence TIC	IT	BT	CT	OT	WP
Disposez-vous d'un inventaire de tous les systèmes TIC (PC, imprimantes, routeurs, etc., au moins tous les appareils ayant une adresse IP)?	ID.AM-1	(x)	x		(x)	
Disposez-vous d'un inventaire des logiciels utilisés (système d'exploitation, Office, programmes, etc.)?	ID.AM-2	(x)	x		(x)	(x)
Avez-vous classé le matériel et les logiciels en fonction de leur criticité? Quelle est l'importance des différents systèmes pour le fonctionnement de l'installation?	ID.AM-5		x	(x)		
Avez-vous clairement défini et documenté les rôles et les tâches des employés en matière de sécurité informatique? Les utilisateurs peuvent être des tiers.	ID.AM-6		x	(x)		
Avez-vous élaboré des lignes directrices et des règlements concernant la sécurité des systèmes informatiques et avez-vous communiqués aux utilisateurs/employés lesdites lignes directrices?	ID.GV-1		x	(x)		
Avez-vous identifié et hiérarchisé les risques auxquels vos systèmes sont exposés? Ces risques sont-ils acceptables pour votre entreprise?	ID.RA-5		x	(x)		
Avez-vous fait l'objet d'un examen des mesures de sécurité de l'information par une autorité indépendante au cours des trois dernières années?	Alternative à ID.RA, ID.RM, ID.SC, car leur mise en œuvre prend beaucoup de temps.		x	x		

Criticité

Sous le terme de "Criticité" on comprend l'importance d'une ressource dont la disparition constituerait une menace existentielle pour l'installation. Pour classer la criticité, il faut tenir compte non seulement de l'unité d'observation, mais aussi de l'environnement qu'elle affecte.

Par exemple, si le logiciel d'un système informatique fonctionne mal, il faut tenir compte des effets potentiels qui affectent à la fois le système lui-même et son environnement.

A propos d'ID.AM-5 : Classification de criticité possible

Criticité	Conséquences en cas de dysfonctionnement
Forte	OT - Un mauvais comportement de l'OT entraîne des perturbations dans les processus ou dans l'archivage des données. IT – Le dysfonctionnement informatique rend des données sensibles accessibles à des personnes non autorisées ou empêche les processus administratifs (par exemple, paiement des salaires, allocation de fonds) ou conduit à des décisions erronées en raison de données incorrectes.
Modérée	Les dysfonctionnements qui peuvent entraîner la défaillance de composants ou de composants de l'installation ou la perte de données.
Aucune	Tout autre type de dysfonctionnement.

2.2 Protéger

L'étape suivante consiste à protéger les systèmes identifiés afin de prévenir l'infection par les logiciels malveillants et d'en minimiser l'impact. Les mesures de protection doivent être adaptées aux tâches des systèmes et ne doivent pas entraver leur fonctionnement.

IT = Fournisseur informatique BT = Opérateur CT = Expert en cybersécurité OT = Fournisseur de systèmes de contrôle
WP = Fournisseur d'outils (par ex. fournisseur du programme pour le plan de maintenance)

x = Responsable (x) = A consulter

Manquement	Référence TIC	IT	BT	CT	OT	WP
Avez-vous limité les droits des utilisateurs (accès en lecture/écriture aux fichiers, modification des paramètres système, etc.) sur les systèmes? (Adapter les droits aux tâches des employés de l'entreprise, aussi peu de droits que possible, autant que nécessaire).	PR.AC-4		x	(x)		
Avez-vous séparé le système de contrôle et le réseau d'automatisation (OT) du reste de l'infrastructure TIC (réseau de bureau, IT) soit physiquement, soit avec un pare-feu?	PR.AC-5	(x)	x		(x)	
Vos employés sont-ils régulièrement formés et informés sur les cyber-risques?	PR.AT-1		(x)	x		
Les données sont-elles régulièrement sauvegardées à distance?	PR.IP-4	(x)	x		(x)	
La sauvegarde des données est-elle testée régulièrement?	PR.IP-4/PR.IP-10	(x)	x		(x)	
Dans la mesure du possible, installez-vous les mises à jour logicielles dès qu'elles sont disponibles?	PR.MA-1	(x)	x		(x)	
Utilisez-vous des technologies de protection (logiciel antivirus, filtrage et surveillance du Web, si possible)?	PR.PT-4	(x)	x	(x)	(x)	
Vérifiez-vous régulièrement l'actualité des technologies de protection?	PR.PT-4	(x)	x			
Vous assurez-vous que lors de l'e-banking, les paiements doivent être approuvés par deux personnes?	Supplément		x			

2.3 Détecter

Pendant longtemps, on se limitait à la protection de l'information. Aujourd'hui, les attaques sont si sophistiquées que la détection des attaques est une discipline à part entière de la sécurité de l'information.

La question n'est plus de savoir si on est attaqué, mais à quel moment on se rend compte qu'on a été attaqué. Comme le montre le cas « RUAG », cela peut prendre des années.

Dans cette optique, des mesures doivent être prises pour détecter rapidement l'attaque afin de minimiser les dégâts.

Les questions suivantes montrent si vous êtes en mesure de détecter les incidents de cybersécurité.

IT = Fournisseur informatique BT = Opérateur CT = Expert en cybersécurité OT = Fournisseur de systèmes de contrôle
WP = Fournisseur d'outils (par ex. fournisseur du programme pour le plan de maintenance)

x = Responsable (x) = A consulter

Manquement	Référence TIC	IT	BT	CT	OT	WP
Les accès et les messages système au niveau du réseau et des données sont-ils enregistrés de manière qu'il soit possible de déterminer, pour une période raisonnable, qui a utilisé quel système à quel moment et qui a accédé à quelles données?	DE.CM-1 bis DE.CM-3	(x)	x	(x)	(x)	
Si le fournisseur du système l'autorise : Les systèmes sont-ils régulièrement analysés à l'aide d'un logiciel antivirus à jour?	DE.CM-7	(x)	x	(x)	(x)	
Des analyses de vulnérabilité sont-elles effectuées régulièrement?	DE.CM-8		x	x	(x)	
Les employés sont-ils encouragés à signaler activement les soupçons et les incidents?	Supplément		x			
Vérifie-t-on régulièrement si les mots de passe des comptes de messagerie de l'entreprise ont été publiés lors d'une fuite de données?	Supplément		x	(x)		

Les mesures de détection doivent être élaborées avec un spécialiste de la sécurité et exécutées par l'opérateur.

2.4 Réagir

Si les cybercriminels parviennent à trouver une faille dans l'architecture de cybersécurité malgré toutes les mesures préventives, l'existence d'un plan d'urgence est d'un grand avantage afin d'éviter la panique et les manipulations fautives.

Si une attaque est détectée, il est important de pouvoir réagir aussi rapidement et calmement que possible. Pour ce faire, l'ampleur et les effets de l'attaque doivent être déterminés le plus rapidement possible. Un plan d'intervention en cas d'incident permet d'y parvenir. La réduction des dommages, tels que la propagation à d'autres segments du réseau, ne peut avoir lieu que si des plans d'intervention appropriés sont en place. La planification de la réaction, la communication et la coordination ainsi que l'analyse et l'atténuation de l'attaque font partie des compétences de base de Réagir.

Le plan d'intervention en cas d'incident devrait comprendre au moins les éléments suivants:

- Traitement des machines infectées: Celles-ci doivent être physiquement déconnectées du réseau pour prévenir ou minimiser la propagation de l'incident (débranchez la prise réseau et non le cordon d'alimentation!).
- Message:
  - Qui est responsable à l'interne?
  - Qui doit être informé en plus?
  - Est-il nécessaire de prévenir le fournisseur du système et/ou la centrale MELANI?
  - Les numéros de téléphones pertinents devraient être disponibles directement dans le plan d'intervention en cas d'incident.
- Temps de réaction.
  - Combien de temps peut-on tolérer que le système soit en panne?
  - Les différents fournisseurs peuvent-ils fournir les pièces de rechange et l'assistance nécessaires dans ce délai?
- Procédure d'analyse de l'incident.
- Instruction pour la restauration des systèmes infectés.

IT = Fournisseur informatique BT = Opérateur CT = Expert en cybersécurité OT = Fournisseur de systèmes de contrôle
WP = Fournisseur d'outils (par ex. fournisseur du programme pour le plan de maintenance)

x = Responsable (x) = A consulter

Manquement	Référence TIC	IT	BT	CT	OT	WP
Un plan d'intervention en cas d'incident a-t-il été élaboré? (Ce document doit être disponible "offline" sur papier)	RS.RP-1		x	x		
Le plan d'intervention en cas d'incident contient-il des mesures immédiates que vous pouvez utiliser sans aide extérieure pour limiter la propagation de l'incident?	RS.MI-1		x	x		
Le plan d'intervention en cas d'incident est-il révisé régulièrement, les procédures décrites sont-elles mises à l'essai et le plan est-il amélioré?	RS.RP-1, RS.IM-2	(x)	x	(x)	(x)	
Des temps de réponse garantis ont-ils été convenus avec les fournisseurs de systèmes?	RS.CO-3	x	x	(x)	x	

L'exploitant doit élaborer et tester le plan d'intervention en cas d'incident en collaboration avec le spécialiste de la sécurité, et, en fonction de la situation, avec les fournisseurs de système.

Afin de contenir efficacement une infection, l'opérateur doit être en mesure d'exécuter le plan lui-même. Cela permet de convenir de temps d'intervention plus longs avec le fournisseur du système.

2.5 Récupérer

Après une attaque, les données et les systèmes sont restaurés selon le plan testé. Tout d'abord, le moment du début de l'attaque doit être déterminé pour assurer la récupération des données à partir de sauvegardes non infectées. Il est également nécessaire d'enquêter sur la cause de l'incident afin de pouvoir prendre des précautions spécifiques contre de nouvelles attaques.

IT = Fournisseur informatique BT = Opérateur CT = Expert en cybersécurité OT = Fournisseur de systèmes de contrôle
WP = Fournisseur d'outils (par ex. fournisseur du programme pour le plan de maintenance)

x = Responsable (x) = A consulter

Manquement	Référence TIC	IT	BT	CT	OT	WP
Pouvez-vous déterminer l'heure de l'incident à partir des fichiers journaux disponibles?	RC.RP-1	(x)	x	(x)	(x)	
Après un incident, pouvez-vous récupérer toutes les données et tous les systèmes nécessaires à l'aide d'un plan de récupération?	RC.RP-1	(x)	x	(x)	(x)	
Pouvez-vous déterminer la cause d'un incident et apporter les améliorations appropriées aux mesures de protection, à la sauvegarde des données et au plan d'intervention?	RC.IM-1, RC.IM-2	(x)	x	(x)	(x)	
Avez-vous déterminé à qui (p. ex. la direction, les autorités, les employés) vous devez fournir des renseignements sur l'incident?	RC.CO-1 bis RC.CO-3		x			
Signalez l'incident à la police.	RC.CO-1 bis RC.CO-3		x			

3. Manuel à l'intention des utilisateurs de systèmes informatiques

3.1 Général IT et OT

Les points suivantes illustrent les domaines où il est possible d'optimiser et d'accroître la cybersécurité.

- Ne laissez pas les courriels, les appels téléphoniques ou les messages d'erreur informatique vous mettre sous pression.
- Si vous soupçonnez un incident de cybersécurité ou si vous n'êtes pas certain, demandez l'avis d'un collègue ou de votre fournisseur de services informatiques.

3.2 Mot de passe IT et OT

Les questions et réponses suivantes illustrent les domaines où il est possible d'optimiser et d'accroître la cybersécurité.

- Les mots de passe sont personnels et ne doivent jamais être partagés. Les fournisseurs sérieux n'ont pas besoin d'un mot de passe personnel pour vous aider.
- Utilisez des mots de passe différents pour chaque application et chaque site Web. Vous êtes donc certain que tous les services ne sont pas compromis lorsqu'un mot de passe tombe entre les mains d'un adversaire.
- Utilisez des gestionnaires de mots de passe tels que KeePass ou LastPass pour gérer les mots de passe.
- Utilisez de longs mots de passe. Idéalement, les mots de passe devraient être composés de lettres, de chiffres et de caractères spéciaux. Avec les gestionnaires de mots de passe, vous pouvez générer les mots de passe automatiquement.
- Pour les services Internet, utilisez l'authentification à 2 facteurs, si possible.

3.3 Internet IT

Les questions et réponses suivantes illustrent les domaines où il est possible d'optimiser et d'accroître la cybersécurité.

- Malheureusement, tous les services offerts sur Internet ne sont pas de bonne foi. Faites appel à des fournisseurs connus et assurez-vous d'utiliser leurs offres via le site officiel.
- Vérifiez l'adresse des liens via la barre d'état de votre navigateur.
- Le cadenas vert du navigateur indique seulement si la connexion est cryptée ou non. Il n'y a aucune indication si vous visitez la bonne page ou non.
- Commandez les logiciels auprès de votre responsable informatique et ne le téléchargez pas vous-même sur Internet.
- N'installez aucun logiciel vous-même sur l'ordinateur professionnel.

3.4 Courriel IT

Les questions et réponses suivantes illustrent les domaines où il est possible d'optimiser et d'accroître la cybersécurité.

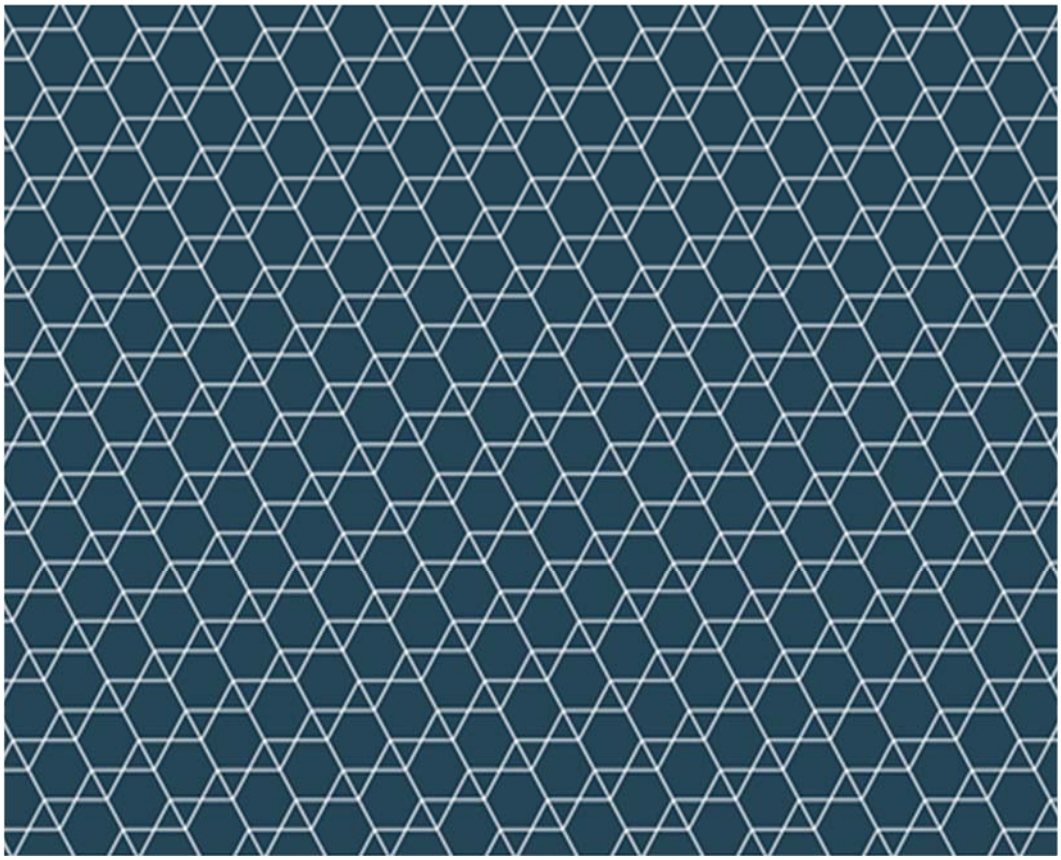
- Supprimer les e-mails suspects. Si le message suspect a été envoyé par un contact connu, confirmez par téléphone que le courriel vient bien de la personne en question. Les courriels sont suspects si
- le contenu est étrange: il promet une offre trop bonne? La méfiance s'installe en le lisant?
- il n'y a pas de salutation personnelle disponible.
- il contient des liens vers des pages officielles pour la saisie des données (mot de passe, carte de crédit, ...).
- Vous recevez des courriels inattendus contenant des renseignements personnels précis. Ces renseignements peuvent être recueillis sur des sites de réseaux sociaux. Les courriels d'hameçonnage sont particulièrement convaincants.
- ils contiennent des mots suscitant l'intérêt du lecteur, tels que "les détails de votre carte de crédit ont été volés".
- le texte crée une pression temporelle. Urgence.
- il vous sera demandé de confirmer votre mot de passe .
- ils contiennent des liens vers de faux sites Web, par exemple au lieu de www.google.com, www.g00gle.com. Vérifiez les liens dans les courriels avant de cliquer en passant votre souris sur le lien et en vérifiant l'adresse Internet qui apparaît.

3.5 Matériel et clés USB, connexion USB IT et OT

Les questions suivantes et leurs réponses illustrent les possibilités d'optimisation et d'augmentation de la cybersécurité.

- Ne connectez à votre ordinateur que du matériel approuvé par l'entreprise.
- Vérifiez les clés USB avec votre logiciel antivirus.
- Vérifiez si le port USB est fermé ou désactivé.

step by STEP



step by STEP
Otto-Jaag-Strasse 15
8600 Dübendorf
info@step-ara.ch
www.step-ara.ch
Questions en allemand: Max Schachtler 044 818 80 24
Questions en français: Tony Reverchon 021 804 70 34 ou Michael Mattle 021 654 91 21