step by STEP

Informations techniques

023 Cybersécurité OT et IT Norme minimale de base en matière de TIC

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.

Onglet

→ 024
Liste de contrôle Cybersécurité dans les systèmes de contrôle de production OT et les réseaux administratifs IT
Norme minimale en matière de TIC

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. Cyber-risques OT et IT

1.1 Introduction

L'OT (Operation Technology ; réseau d'automatisation) et l'IT (Information Technology ; réseau de bureau) modernes sont indispensables dans les entreprises. Les processus d'automatisation sont contrôlés, les données de processus archivées, la planification de la maintenance est organisée et toutes les tâches administratives sont exécutées sur la base d'une OT et d'une IT sécurisées. Selon l'organisation, les activités administratives telles que la comptabilité ou l'administration du personnel sont également exécutées par les sociétés elles-mêmes. Le support informatique est également devenu indispensable pour ces activités.

Exigences élevées en matière de disponibilité

En raison de la complexité des processus actuels, tels que les stations de pompage régulées et les processus biologiques complets, il n'est plus possible de maintenir l'exploitation d'une entreprise (comme les stations d'épuration des eaux usées, les entreprises industrielles, l'industrie et le commerce) sur une longue période de temps sans automatisation.

La technique de commande surveille un grand nombre de processus automatisés et permet une visualisation claire des états actuels. Sur la base de ces informations, l'opérateur peut contrôler les processus de l'installation, intervenir activement et les optimiser.

En raison de cette exigence, une haute disponibilité des systèmes OT et IT est absolument nécessaire.

Accroître le réseautage

L'accès Internet nécessaire à l'accès à distance à la technologie de contrôle pour simplifier le service de garde ou pour connecter des structures externes, ainsi que pour la gestion du réseau de canaux et les connexions cloud pour les données météorologique ou de réseau de canaux, comporte des risques majeurs pour la sécurité.

En raison de ces réseaux d'entreprise modernes, un concept de sécurité adapté pour la protection contre les cyber-attaques doit être revu régulièrement. Le rythme rapide des progrès technologiques continue de générer de nouveaux cyber-risques et nécessite une prise de conscience de ces dangers.

Ce document sert à actualiser le système de sécurité et se réfère à la norme TIC minimale de l'OFAE (Office fédéral de l'approvisionnement économique du pays) en matière de prévention

→ et à la liste de contrôle 024

1.2 Analyse des risques / dangers

Avec le développement de l'informatique et la mise en réseau croissante de différents systèmes, de nouvelles opportunités mais aussi de nouveaux dangers apparaissent pour les entreprises. Les attaques de pirates informatiques se sont développées à partir de défis d'adolescents dans les années 80 à un marché croissant valant auhourd'hui plusieurs milliards de dollars. Jusqu'à présent, les systèmes de commande et de surveillance des installations industrielles ont été pour la plupart isolés et ont donc été longtemps épargnés des conséquences de cette tendance.

L'augmentation du réseautage rend ces systèmes plus vulnérables à la manipulation et aux attaques de pirates informatiques.

Aujourd'hui, les exploitants d'installations industrielles sont la cible de telles attaques pour diverses raisons, comme par exemple l'extorsion d'argent, ou les dégâts collatéraux causés par une attaque à grande échelle, ainsi que d'actions politiquement motivées.

Raisons d'une cyberattaque

Les raisons possibles d'une cyberattaque contre une entreprise peuvent être:

- Extorsion d'argent.
- Exploitation de la puissance des ordinateurs (CryptoMining, botnet, tremplin pour d'autres attaques).
- L'entreprise prise comme cible d'essai / test d'attaque (aléatoire ou ciblée).
- Manipulation ou vol des données des processus.
- Sabotage (détérioration ou destruction du système, complet ou partiel).
- Espionnage (connaissance des processus).
- Vol d'argent, en déclenchant ou en détournant des paiements.

Comment les attaques peuvent se produire

Quels sont les vecteurs d'attaque possibles pour une entreprise?

- Clé USB.
- E-mails.
- Sites Internet (visite ou téléchargement de programmes).
- Appareils informatiques extérieur au réseau (ordinateurs portables, smartphones, tablettes, etc.).
- Points d'accès WiFi.

Quelles conséquences ces attaques peuvent-elles avoir?

Quelles peuvent être les conséquences d'une cyberattaque pour une entreprise?

- Infestation des systèmes par des virus ou des logiciels de cryptage (cryptage des données).
- Détérioration de systèmes individuels ou de l'ensemble des systèmes.
- Indisponibilité de systèmes individuels ou de l'ensemble des systèmes.
- Intervention / manipulation incorrecte du processus d'automatisation de l'installation.
- Manipulation ou destruction d'historique des données.

Une analyse des risques devra être préparée pour la mise en œuvre des mesures. Les mesures de sécurité devront être prises par ordre d'importance. Le risque d'être victime d'une cyberattaque se compose principalement de trois facteurs:

- Quelle est la probabilité que l'installation soit choisie comme cible d'une attaque?
- Quelle est la probabilité qu'une attaque soit un succès?
- Quels dommages le système subirait-il si une attaque réussissait?

Par exemple, pour les stations d'épuration des eaux usées, la probabilité d'être exposé à une attaque ciblée est relativement faible, mais avec de bonnes chances de succès. Le potentiel de dégâts est difficile à estimer et dépend des intentions de l'attaquant. Dans le cas de l'espionnage, il n'y aura que rarement des dommages directs pour l'installation, car les attaquants veulent

rester indétectables. À l'opposé, une attaque à motif politique cause autant de dégâts que possible afin de générer beaucoup d'attention.

De grands dangers existent dans le cas d'attaques non-ciblés qui se produisent tous les jours dans tout le pays par courrier électronique ou en visitant des sites Internet. De simples mesures de sécurité peuvent limiter massivement ou même empêcher complètement les effets possibles de telles attaques, comme le cryptage des données.

1.2.1 Risques pour l'opérateur

Si une entreprise se gère elle-même (par exemple une station d'épuration des eaux usées), elle exploite souvent un réseau administratif en plus du réseau de contrôle. Les risques financiers sont ici au premier plan. Mais l'exploitation de l'installation comporte également des risques pour l'exploitant.

Les risques possibles sont:

- Pertes financières dues à des vols via des applications e-banking.
- Pertes financières dues à l'extorsion de fonds.
- Pertes financières dues à la fraude.
- Responsabilité pour les dommages causés au système et aux tiers.

1.2.2 Risque d'incendie et d'explosion / danger d'explosion

En règle générale, le risque est faible si des précautions techniques et organisationnelles sont en place, telles que

- Sauvegarde régulière des données.
- Stockage séparé des données sauvegardées.

1.2.3 Risques pour l'installation

Une attaque contre une entreprise (p. ex. une station d'épuration des eaux usées) n'entraîne souvent pas en premier lieu la destruction des composants de l'installation, mais une panne ou un dysfonctionnement possible du système.

Les risques possibles sont:

- Dommages à l'installation dus à une défaillance du processus d'automatisation.
- Dommages à l'installation dus à une mauvaise manipulation de l'installation.
- Dommages à l'installation dus à un dysfonctionnement de l'installation.

1.2.4 Risques pour les plans d'eau

En fonction de la durée de la défaillance technique et de la partie de l'installation concernée, cela peut avoir un effet sur le fonctionnement et donc sur le résultat (par exemple: efficacité de l'épuration et limites de décharge). En cas de doute, il faut demander de l'aide ou en informer les autorités.

Les risques possibles sont:

- Panne du processus d'automatisation.
- Manipulation incorrecte du système.
- Dysfonctionnement du système.

2. Responsabilité IT et OT

2.1 Introduction

Dans le contexte d'une entreprise, il est important de faire la distinction entre l'IT classique (Information Technology; réseau de bureau) et l'OT (Operation Technology; réseau d'automatisation des processus), car ces deux réseaux remplissent des fonctions très différentes et sont donc soumis à des exigences différentes. Ces différences ont une influence sur les mesures de sécurité qui peuvent être prises, c'est pourquoi elles sont brièvement résumées ici.

2.2 IT (Information Technology; réseau bureautique)

Le réseau IT d'une entreprise sert à augmenter l'efficacité des tâches administratives et à faciliter leur réalisation. Des logiciels tels que Microsoft Office (Word, Excel, etc.) et Outlook sont disponibles sur un PC typique du réseau de bureau. Dans la plupart des cas, le réseau IT dispose d'un accès direct à Internet.

Le cycle de vie des différents composants du réseau IT est généralement assez court. Les mises à jour peuvent et doivent être installées rapidement, car elles n'ont généralement aucun effet négatif sur la fonctionnalité des systèmes. Si quelque chose ne fonctionne pas après une mise à jour, les effets sont rarement graves. L'utilisation de logiciels de protection tels que les antivirus est également possible sans problème. Les fichiers mal détectés n'entraînent pas de situations critiques dans un réseau de bureau.

2.3 OT (Operation Technology; réseau d'automatisation des processus)

L'objectif principal du réseau OT est d'établir des connexions entre les différents composants des processus d'automatisation afin qu'ils puissent échanger les données nécessaires au contrôle du processus. Les PC du réseau OT sont généralement équipés d'un logiciel de visualisation pour l'automatisation des processus ainsi que les divers outils requis par les automaticiens. Les automates qui contrôlent les processus sont également présents dans le réseau OT. Le réseau OT ne devrait pas avoir un accès direct à Internet.

Le cycle de vie des différentes composantes du réseau OT est généralement relativement long (plusieurs années). Les mises à jour ne peuvent pas toujours être installées rapidement, car elles peuvent nuire à la fonctionnalité de certains composants (anciens). Les pannes sur le réseau d'OT peuvent entraîner des interruptions de service, ce qui peut avoir de graves conséquences pour l'entreprise.

2.4 Responsabilité

En dernier lieu, la responsabilité de la cybersécurité incombe à l'exploitant. Lui seul peut déterminer la volonté de l'entreprise à prendre des risques, et prendre les mesures qui découle de ces décisions. Une fois ces mesures définies, il faut s'assurer que toutes les personnes concernées (comme les employés, les fournisseurs de systèmes, les partenaires) les connaissent et sont conscients de leur responsabilité envers celles-ci.

Afin de garantir la sécurité de l'IT et de l'OT, un échange entre les spécialistes de la sécurité, les fournisseurs de systèmes et l'exploitant est nécessaire. Les responsabilités doivent être clairement définies et, dans la mesure du possible, consignées dans un contrat (par exemple, dans lequel les fournisseurs de systèmes s'engagent à respecter la norme TIC minimale).

Il est donc recommandé qu'un spécialiste indépendant de la sécurité (et non un fournisseur IT ou OT) élabore un concept de sécurité pour la prévention des cyber-risques, et qu'il accompagne, vérifie et coordonne la définition des mesures techniques et organisationnelles et leur implementation entre les différents acteurs.

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

3. La prévention au moyen de la norme minimale en matière de TIC

3.1 Introduction

La norme minimale en matière de TIC de l'OFAE (Office fédéral de l'approvisionnement économique du pays) pour l'amélioration de la résilience des TIC est basée sur des normes internationalement reconnues en matière de sécurité de l'information. Elle est divisée en cinq fonctions basées sur le NIST Cybersecurity Framework Core :

1. Identifier (Identify),

2. Protéger (Protect),

3. Détecter (Detect),

4. Réagir (Respond) et

5. Récupérer (Recover).

Pour pouvoir protéger quelque chose, il est indispensable de le connaitre. Une analyse des risques sert à distinguer les risques acceptables des risques inacceptables et à mettre en œuvre des mesures de réduction des risques pour les risques inacceptables.

Résilience = Capacité des systèmes techniques à ne pas tomber complètement en panne en cas de panne partielle.

3.2 Connaître l'opération

Pour connaître une entreprise, il faut répondre aux questions suivantes:

- Qu'est-ce qui est fait?
- Comment cela se fait-il?
- Quelles sont les conditions-cadres à respecter?
- Qui en est responsable?
- Comment le mesure-t-on?

Les réponses constituent la base de la documentation de l'entreprise et de la gestion des risques qui s'ensuit.

3.3 Gestion des risques

Améliorer la résilience des TIC est un projet à long terme. Celui-ci est réalisé au moyen d'un processus de gestion des risques qui est subdivisé en trois sous-processus:

- Analyse des risques.
- évaluation des risques.
- maîtrise des risques.

et qui tient compte de la disposition de l'entreprise et de sa volonté à prendre des risques.

3.4 Mettre en œuvre des mesures de protection sur la base d'une stratégie de défense en profondeur (Defense-in-Depth)

La défense en profondeur signifie l'utilisation coordonnée de plusieurs mesures de sécurité pour protéger les données d'une entreprise. La stratégie repose sur le principe militaire selon lequel il est plus difficile pour un ennemi de surmonter un système de défense complexe et à plusieurs niveaux, qu'un système avec une seule barrière.

Les composantes d'une stratégie de défense en profondeur comprennent:

- Logiciel antivirus.
- Pare-feux.
- Programmes anti-logiciels espions et
- un système de mots de passe à plusieurs niveaux.

Afin de s'infiltrer sur un ordinateur de l'entreprise, tous ces systèmes de défense doivent être franchi.

Alors qu'un pare-feu était pendant longtemps la première et la dernière mesure de sécurité contre les attaques, nous avons maintenant:

- Réseaux segmentés.
- Ordinateurs protégés par un logiciel antivirus.
- Mises à jour automatisées du système.
- Suivi du comportement de l'utilisateur et
- surveillance active du réseau.

Cette redondance des mécanismes de sécurité retarde l'intrusion d'un agresseur et donne le temps de mettre en œuvre des contre-mesures et d'éviter les répétitions.

Comparés aux systèmes d'information et de communication conventionnels, les systèmes d'automatisation ont une longue durée de vie. S'ils fonctionnent de manière stable, ils peuvent être utilisés sans mise à jour et représentent donc un risque majeur pour la sécurité.

L'implémentation de mises à jour peut même entraver ou empêcher la fonctionnalité requise. En outre, l'utilisation d'un logiciel antivirus peut entraîner la destruction éventuelle de fichiers critiques (faux positifs). Ces deux mesures de sécurité peuvent donc avoir un impact négatif sur les opérations.

L'isolement du réseau OT est donc la mesure de sécurité la plus importante. Le concept de défense en profondeur devrait également être appliqué ici, par exemple:

- Restrictions des droits.
- Définir les cycles d'entretien.
- N'effectuer que des mises à jour testées.
- Implementer une sécurité accrue pour les systèmes adjacents, comme les ordinateurs de bureau.

4. L'examen de cas individuels

L'expérience acquise au cas par cas permet une adaptation continue des mesures. Chaque entreprise peut modifier les cas individuels en fonction de ses propres circonstances et ajouter d'autres cas individuels.

Les mesures concrètes prises dépendent de la situation de l'entreprise concernée.

4.1 Exemples d'attaques

Virus informatique

Stuxnet est un virus informatique découvert en 2010 spécialement conçu pour attaquer un système de surveillance et de contrôle Siemens (Simatic S7). Le logiciel malveillant a pu pénétrer dans des réseaux isolés et charger des composants modifiés sur un système de contrôle afin de manipuler le processus et de saboter le système.

Il est peu probable d'être victime d'un tel scénario, car l'effort de développement est extrêmement important. Cependant, l'évolution rapide de la cybercriminalité augmente de manière inéluctable le risque d'une attaque.

Ransomware

Les attaques par rançon/cryptage sont moins dramatiques, mais très répandues et peuvent causer autant de dommages. De plus, les installations gouvernementales sont une cible populaire pour les demandes de rançon, car les attaquants pensent avoir une chance élevée que la rançon soit payée.

Il est évident que la protection contre les attaques généralisées et facilement évitables devrait être renforcée avant de faire face à des attaques ciblées et techniquement avancées.

D'autres exemples sont décrits dans les chapitres suivants. En règle générale, ceux-ci sont toujours basés sur une combinaison des trois élèments suivant:

- motivation de l'attaquant.
- vecteur d'attaque.
- conséquences.

4.2 Infection par Ransomware via clé USB ou e-mail

Situation

- Cryptage d'ordinateurs de bureau, d'ordinateurs portables de secours, de stations de contrôle ou de serveurs.
- Demande de rançon.

Conséquences

Le cryptage de toutes les données peut limiter l'opérabilité du système de contrôle ou même le rendre inopérable. Tant que les automates ne sont pas affectés, l'installation reste fonctionnelle.

Détection

Une attaque Ransomware peut être détectée par une charge processeur élevée et un grand nombre d'accès aux fichiers.

Les signes d'une attaque peuvent être l'altération de la fonctionnalité du système de contrôle (ou d'un autre logiciel), un changement dans les extensions de fichiers (par exemple CRYPTED) ou une demande de rançon.

Mesures à prendre

Mesures IT	Mesures OT
Informer la ou les personnes responsables.	Informer la ou les personnes responsables.
Débrancher physiquement la machine du réseau (débrancher le câble réseau). Attention: Ne tirez pas sur le câble d'alimentation!	Débrancher physiquement la machine du réseau (débrancher le câble réseau). Attention: Ne tirez pas sur le câble d'alimentation!
Suivez les instructions de la ou des personnes responsables.	Suivez les instructions de la ou des personnes responsables.

Mesures qui peuvent être prises en accord avec la personne responsable:

- Faites une copie d'au moins une machine pour analyse.
- Réinstallez les machines.
- Restaurez les données des sauvegardes ou, si ce n'est pas possible, vérifiez si une clé pour cette variante de Ransomware est disponible →par exemple sur www.nomoreransom.org
- Identifiez la cause de l'infection (p. ex. à l'aide des journaux du système) et adaptez le concept de sécurité pour éviter que de tels cas se reproduisent à l'avenir.

Prévention

- L'utilisation de clés USB doit être évitée si cela est techniquement possible ("Least Privilege"). De plus, la charge du processeur doit être surveillée pour permettre une détection rapide d'une attaque.
- Des sauvegardes régulières du système ou au moins des données critiques sur le plan opérationnel devraient être effectuées.
- Un logiciel de protection qui détecte et bloque le cryptage devrait être installé et utilisé.

4.3 Infection botnet par un logiciel "infecté"

Situation

- Abus du réseau ou de la puissance de calcul dans le cadre d'un botnet.
- Infection d'autres appareils informatiques.

Conséquences

Outre l'utilisation abusive (et l'indisponibilité éventuelle) du réseau ou du processeur des systèmes concernés, une telle attaque peut également avoir pour conséquence que le fournisseur d'accès Internet coupe la connexion Internet au système, car il considère ce dernier comme un système nuisible. De même, les forces de l'ordre peuvent (à tort) considérer le système comme le point de départ d'une attaque, ce qui peut conduire à une intervention de celles-ci et aux perturbations opérationnelles associées.

Détection

Les infections de Botnet peuvent être détectées par l'augmentation de la charge du CPU et/ou du réseau, ainsi que par des connexions à des domaines de commande et de contrôle connus. Ceux-ci sont requis par les attaquants pour envoyer des commandes aux systèmes infectés ("bots").

Mesures à prendre

Mesures IT	Mesures OT
Informer la ou les personnes responsables.	Informer la ou les personnes responsables.
Débrancher physiquement la machine du réseau (débrancher le câble réseau). Attention: Ne tirez pas sur le câble d'alimentation!	Débrancher physiquement la machine du réseau (débrancher le câble réseau). Attention: Ne tirez pas sur le câble d'alimentation!
Suivez les instructions de la ou des personnes responsables.	Suivez les instructions de la ou des personnes responsables.

Mesures qui peuvent être prises en accord avec la personne responsable:

- Faites une copie d'au moins une machine pour analyse.
- Réinstallez la machine.
- Déterminer la cause de l'infection (par exemple à l'aide des journeaux du système) et adapter le concept de sécurité pour éviter que de tels cas se reproduisent à l'avenir.

Prévention

- Les logiciels ne doivent provenir que de sources fiables.
- Le réseau devrait être divisé en différents segments pertinents pour l'entreprise, ce qui peut réduire la propagation de ces infections et minimiser les dommages qui en résultent.
- Les utilisateurs ne devraient bénéficier que de privilèges minimaux, ce qui rend difficile l'installation réussie d'un cheval de Troie/Botnet.
- La charge du réseau et du processeur doit être surveillée pour permettre une détection rapide de l'attaque.

4.4 Manipulation des données de processus

Situation

- Valeurs incorrectes sur le système de visualisation des processus.
- Comportement incorrect des processus d'automatisation.
- Manipulation ou mise "hors service" du système de contrôle.

Conséquences

Selon l'ampleur de l'attaque, les conséquences peuvent varier de petites perturbations jusqu'à des dommages importants. En ce qui concerne les dommages matériels, toutefois, le système doit être protégé par des verrouillages physiques appropriés.

Les verrouillages physiques sont généralement définis lors de l'ingénierie du processus dans le cadre de l'analyse des risques.

Détection

La détection peut être difficile car les données incohérentes peuvent avoir plusieurs causes (dysfonctionnement du capteur, erreur de transmission des données, erreur de traitement des données, etc.) Les employés qui ont un "feeling" pour le système sont très précieux dans de tels cas.

Mesures à prendre

Mesures IT	Mesures OT
Informer la ou les personnes responsables.	Informer la ou les personnes responsables.
Débrancher physiquement la machine du réseau (débrancher le cable réseau). Attention: Ne tirez pas sur le câble d'alimentation!	Débrancher physiquement la machine du réseau (débrancher le cable réseau). Attention: Ne tirez pas sur le câble d'alimentation!
Débranchez le connecteur réseau du segment affecté du commutateur réseau principal/pare-feu afin que le segment affecté n'ait plus accès au reste du système.	Débranchez le connecteur réseau du segment affecté du commutateur réseau principal/pare-feu afin que le segment affecté n'ait plus accès au reste du système.
Aucun commentaire.	Contrôle visuel du bon fonctionnement des tâches critiques de l'entreprise (il n'est plus possible de se fier au système de contrôle à ce moment).
Suivez les instructions de la ou des personnes responsables.	Suivez les instructions de la ou des personnes responsables.

Comme ce type d'attaque exige un savoir-faire très spécialisé, on peut supposer qu'il s'agit d'une attaque ciblée. La Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) doit donc également en être informée.

→ https://www.melani.admin.ch/melani/fr/home/themen.html

Une fois l'attaque surmontée, il faut déterminer la cause de l'infection (par exemple à l'aide des journeaux du système) et adapter le concept de sécurité afin d'éviter de tels cas se reproduisent à l'avenir, ou au moins de les détecter plus rapidement.

Prévention

Étant donné que la nature de l'attaque indique un adversaire compétent et bien organisé, il est très difficile de se protéger contre de telles attaques.

La mise en œuvre rigoureuse de la «liste de contrôle OT et IT Cybersécurité» et des mesures preventives qui y sont mentionnées peut toutefois réduire considérablement le risque et les effets de tels attaques. → 024 Liste de contrôle OT et IT Cybersécurité

4.5 Vol et fraude

Situation

Manipulation par "ingénierie sociale": Un message intelligemment formulé pousse la victime à transférer de l'argent à l'adversaire.

Conséquences

La victime est persuadée de transférer une grande somme d'argent à l'attaquant. À cette fin, de faux faits sont presenté à la victime. Les auteurs utilisent souvent de fausses identités, par exemple en falsifiant des numéros de téléphone et des adresses électroniques.

Détection

La détection est difficile. La victime est soumise à des contraintes de temps et reçoit l'ordre de garder l'action confidentielle pour des raisons professionnelles.

Mesures à prendre

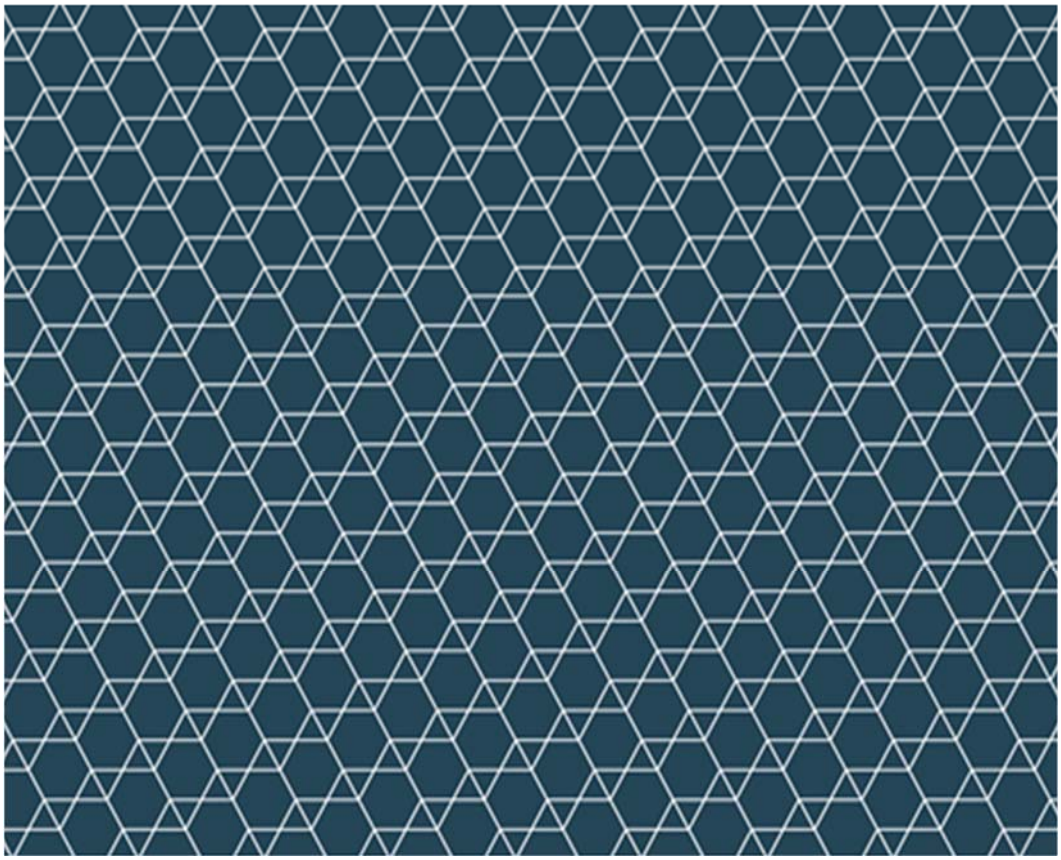
Mesures IT	Mesures OT
Informer la ou les personnes responsables.	Il n'y a pas de transfert d'argent avec OT.
Informer l'institution (banque, fournisseur, etc.) responsable du transfert et la persuader de bloquer ou d'annuler le transfert.	Il n'y a pas de transfert d'argent avec OT.

Prévention

Identifiez clairement le partenaire et le donneur d'ordre. En cas de doute, verifiez l'ordre par un canal de communication autre que celui par lequel la commande a été reçue. Ne laissez pas les messages vous mettre sous pression. Discutez les situations suspectes avec vos collègues.

Un climat ouvert et transparent, ainsi que des employés formés, contribuent à lutter contre l'ingénierie sociale.

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