rittmeyer
BRUGG

SÉCURITÉ INFORMATIQUE AU NIVEAU DES SYSTÈMES DE CONDUITE

Plus de sécurité pour la gestion de l'eau et de l'énergie

Système de conduite en danger ?

Éviter les manipulations indésirables

Lorsqu'un voleur essaie de pénétrer sur un site, il cherche les points faibles de la sécurité et les exploitent à ses propres fins. Les criminels agissent de la même façon en tentant de manipuler les infrastructures critiques d'un système d'approvisionnement ou de voler des données.

Les infrastructures complexes d'alimentation et d'élimination sont particulièrement vulnérables: elles sont mises en réseau à différents niveaux et de nombreux systèmes sont impliqués dans leur fonctionnement. De plus, le bon fonctionnement est essentiel car, sans alimentation en eau et en énergie, la vie publique s'arrête.

Du fait de **la dépendance croissante aux technologies d'information et de communication**, la disponibilité fiable aux infrastructures dites d'information est par conséquent essentielle. Un soin tout particulier doit donc être accordé à leur protection (Critical Information Infrastructure Protection, CIIP).

Souvent des parties de systèmes ou de processus sont modifiées ou remplacées sans considérer suffisamment, à ce moment-là, les conséquences sur l'ensemble du système. De **nouvelles failles de sécurité** apparaissent alors et rendent les installations vulnérables aux attaques éventuelles.

La plupart des entreprises s'accordent aujourd'hui à reconnaître comme une menace l'augmentation du nombre des attaques ciblées provenant du réseau et consacrent des budgets plus importants à la sécurité informatique. Toutefois, la course s'engage de plus en plus, car **le nombre d'incidents menaçant la sécurité progresse dramatiquement.**

«DES CONSÉQUENCES FONDAMENTALES SUR LES INFRASTRUCTURES AGISSENT SUR LE BON FONCTIONNEMENT DES SYSTÈMES DE MESURE, D'AUTOMATISATION ET DE SURVEILLANCE.»

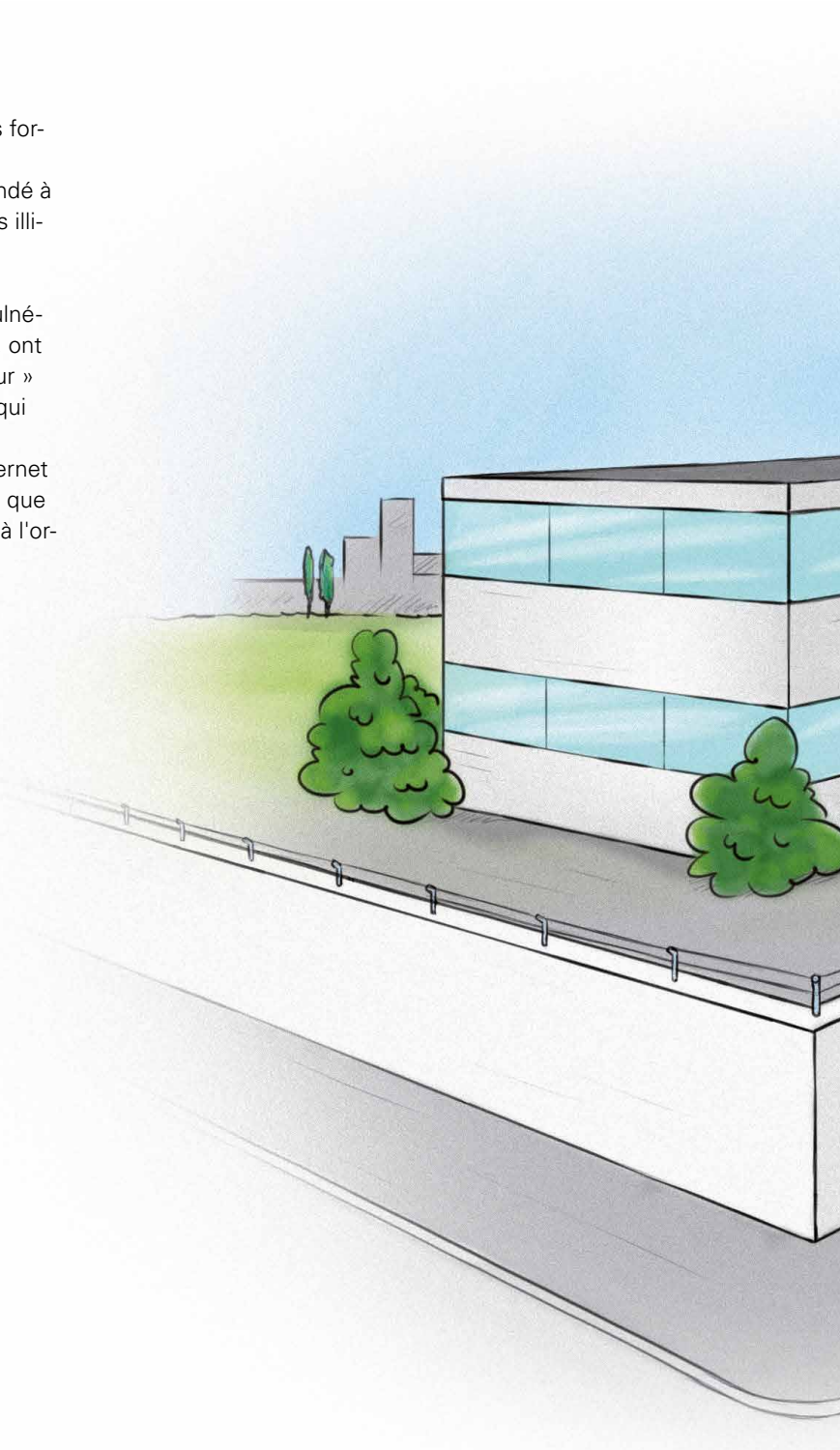
Êtes-vous vraiment bien protégé ?

La protection physique ne suffit pas

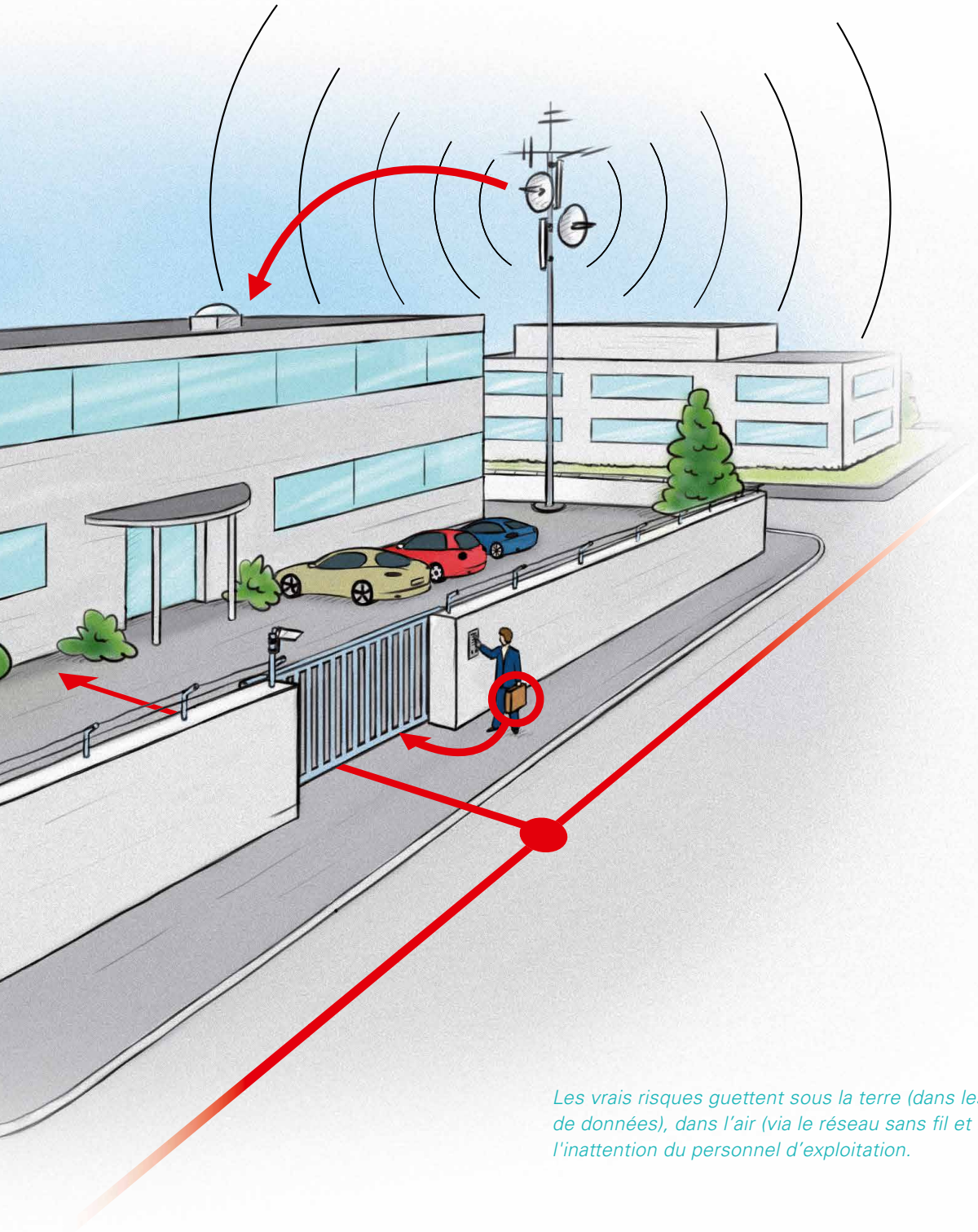
La protection physique des dispositifs de mesure et de conduite autour de la gestion hydraulique et énergétique est évidente, qu'il s'agisse de clôtures, de systèmes d'alarme ou de systèmes de fermeture. Mais la protection virtuelle est tout aussi importante.

Pour fermer des vannes ou agir sur des filtres, il n'est pas forcément nécessaire d'accéder à l'installation. De la même manière que le système d'alimentation peut être commandé à distance, les accès virtuels ouvrent les voies aux attaques illicites.

Les infrastructures d'information sont particulièrement vulnérables surtout celles qui, sciemment ou inconsciemment, ont des systèmes « internes » qui sont reliés avec « l'extérieur » tel que : l'ordinateur portable du service de permanence qui communique avec le poste de commande via le réseau mobile; l'ordinateur de supervision qui est connecté à Internet via le réseau bureautique; les clés USB infectées de virus que les collègues ont ramenées de chez eux puis raccordées à l'ordinateur du réseau.



«QUELQU'UN QUI SOUHAITE ATTAQUER UN SYSTÈME DE CONDUITE, DISPOSE DE NOMBREUSES POSSIBILITÉS D'Y ACCÉDER.»



Les vrais risques guettent sous la terre (dans les flux des autoroutes de données), dans l'air (via le réseau sans fil et le réseau mobile) et par l'inattention du personnel d'exploitation.

Les risques guettent partout

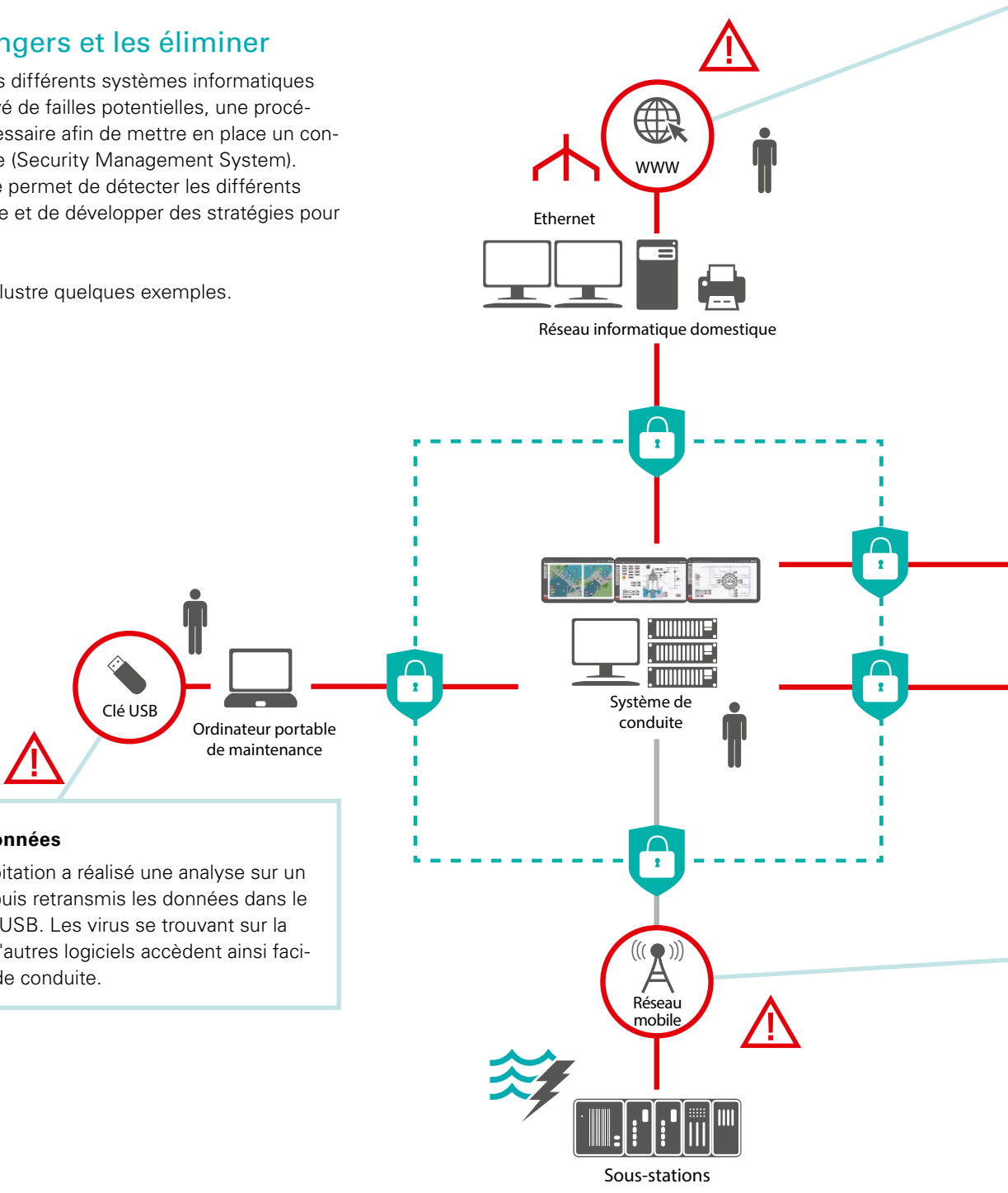
La détection et l'analyse systématiques des dangers sont essentielles

Les systèmes de conduite complexes sont vulnérables à de nombreux niveaux. Afin de protéger efficacement le système, des dispositions doivent être prises dans différents domaines.

Identifier les dangers et les éliminer

De par la complexité des différents systèmes informatiques ainsi que le nombre élevé de failles potentielles, une procédure structurée est nécessaire afin de mettre en place un concept de sécurité efficace (Security Management System). Seule une telle méthode permet de détecter les différents risques de manière fiable et de développer des stratégies pour les réduire.

Le graphique ci-contre illustre quelques exemples.



Exemple

Risque: trafic de données

Le personnel d'exploitation a réalisé une analyse sur un ordinateur externe, puis retransmis les données dans le système via une clé USB. Les virus se trouvant sur la clé USB provenant d'autres logiciels accèdent ainsi facilement au système de conduite.

Exemple

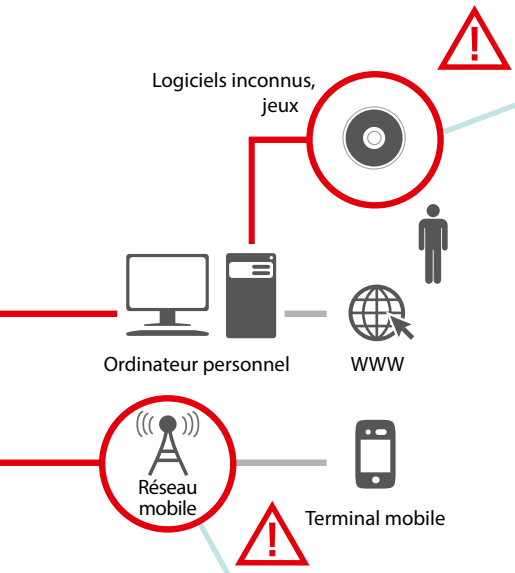
Risque: réseau bureautique

Le système de conduite était jusqu'à présent une unité autonome. Le système était fermé sans aucune connexion à Internet. Entre-temps, le chef d'exploitation gère depuis ce poste l'ensemble de l'installation, effectue des analyses et envoie des rapports électroniques aux autorités et à l'administration. L'ordinateur central a été, de manière presque inaperçue, relié au réseau de bureautique et par conséquent à Internet avec les dangers potentiels qui en découlent.

Exemple

Risque: postes de travail non protégés

Suite à un message d'alarme dans l'installation, l'employé du service de permanence accède au système de conduite depuis son ordinateur personnel. Les chevaux de Troie infiltrés par d'autres logiciels peuvent ainsi accéder au système de conduite.



«LA LISTE DES RISQUES POTENTIELS SE COMPLÈTE À L'INFINI.»

Exemple

Risque: connexions sans fil

L'accès au système de conduite est réalisé par terminal raccordé à un réseau sans fil (par exemple tablette tactile). Les postes éloignés sont connectés via le réseau sans fil. Si le réseau sans fil n'est pas suffisamment protégé, il est vulnérable depuis l'extérieur.

Professionnel et sécurisé

Le système de gestion de la sécurité de l'information ISMS pour des systèmes de conduite plus sûrs

Depuis plusieurs décennies, Rittmeyer conçoit et réalise dans le monde entier, des solutions dans la technique de mesure et de conduite. Cette compétence nous permet de vous assister à identifier les failles de sécurité de vos systèmes informatiques et à vous protéger efficacement contre les attaques.

La protection optimale Rittmeyer pour vos systèmes de conduite

Les systèmes de conduite Rittmeyer répondent aux exigences de sécurité envers les systèmes de commande et de télécommunication décrites dans les livres blancs de la BDEW (Fédération nationale allemande dans le secteur de l'eau et de l'énergie).

Rittmeyer propose en outre des prestations de service pour une protection complète, qui se base pour l'essentiel à sécuriser de manière durable les infrastructures de l'information de l'ensemble du processus en passant par l'approvisionnement, par les spécifications et conformités de fonctionnement, jusqu'aux scénarios de rétablissement de la sécurité après la violation du système.

«LE PLUS DE RITTMEYER : UNE PROTECTION COMPLÈTE POUR GARANTIR VOTRE SÉCURITÉ INFORMATIQUE.»

Prévention

A leurs livraisons, les systèmes de conduite Rittmeyer répondent aux exigences de la BDEW en matière de sécurité des systèmes de commande et de télécommunication.

Le personnel d'exploitation est instruit et formé à l'utilisation sécurisée des installations.

Les exploitants reçoivent des recommandations pour la mise en place et l'exploitation de leurs infrastructures informatiques.

Action

En fonction des exigences spécifiques en matière de sécurité de l'installation, la protection est planifiée et la fonctionnalité modélisée.

Rittmeyer réalise l'ensemble des dispositifs de conduite et les valide conformément aux différentes directives de sécurité.

Lors du service et de la maintenance, nous vérifions la fonctionnalité de la protection afin de la garantir durablement.

Détection

En tant que fabricant et fournisseur de solutions pour les systèmes de conduite, nous connaissons précisément les points critiques d'un système de conduite ainsi que les potentielles failles de sécurité.

Nous vérifions les équipements informatiques et le processus, analysons les problèmes et formulons des recommandations quant aux mesures à prendre pour garantir une sécurité adéquate.

Réaction

En cas de violation de la sécurité de l'installation, nous examinons l'activité suspecte. Après constatation de l'infraction, nous vous aidons à déterminer le risque, à l'analyser et à évaluer les traces numériques.

Étape par étape vers plus de sécurité

Profitez de notre expérience en matière de gestion de la sécurité informatique

Rittmeyer connaît très bien les techniques de réseau grâce à ses longues années d'expérience et s'appuie sur un savoir-faire informatique approfondi. Nous connaissons ainsi particulièrement bien les exigences liées à la sécurité informatique ainsi que les risques potentiels auxquels les systèmes de conduite sont soumis.

Grâce à notre aide, donnez à vos infrastructures d'information une base solide. Complet, comme décrit dans les cinq étapes ci-après, et toujours basé sur les structures existantes dans votre installation.

Vous déterminez cependant la zone d'application en fonction de vos besoins. Les spécialistes, nous les avons.

1 Analyse de la situation actuelle

Votre situation est examinée au niveau des risques potentiels que recèle votre **processus**, au niveau des points d'attaque que propose votre **infrastructure** et au niveau du soutien des **directives** en vigueur pour une utilisation en toute sécurité des technologies informatiques.

Vos avantages:

Vous connaissez votre situation. Toutes les mesures suivantes se basent sur la situation initiale examinée et peuvent donc être réalisées de manière optimale en termes de coût et d'efficacité.

2 Analyse des risques selon ISMS

Ensemble, nous **identifions** les dangers potentiels et **évaluons** la probabilité d'occurrence ainsi que leurs impacts.

Vos avantages:

Grâce à l'analyse systématique des risques, nous proposons des **mesures adéquates** selon leur degré d'importance, dont vous pourrez, en termes de coût, **efficacement optimiser leur réalisation**.

«LA SÉCURITÉ EST UN PROCESSUS. INVESTISSEZ DANS UNE VRAIE GESTION DE LA SÉCURITÉ ÉCONOMIQUE ET TOURNÉE VERS L'AVENIR AVEC RITTMEYER.»

3 Création d'un concept de sécurité informatique

Le concept de sécurité informatique regroupe trois zones d'action: **la disponibilité contrôlée** des systèmes matériels, **l'intégrité du logiciel** pour la protection contre la manipulation, ainsi que **la protection des données** contre une utilisation interne et externe illicite.

Vos avantages:

Vous recevez des recommandations concrètes qui décrivent, de manière **claire et compréhensible** pour chacun, **l'implémentation efficace** d'une protection.

4 Implémentation professionnelle

En s'appuyant sur le concept de sécurité informatique, les mesures concrètes sont réalisées. Si la mise en place **s'effectue par vos spécialistes**, nous vous fournissons **conseil et assistance**. Selon vos besoins, nos spécialistes peuvent également se charger de **l'implémentation** d'une partie du projet ou de toute la mise en œuvre.

Vos avantages:

L'impact des mesures prises est **garanti**; la solution mise en place de façon **professionnelle**.

5 Assurer la durabilité

Il est essentiel de maintenir à long terme une protection efficace. Ceci comprend aussi bien la mise à jour régulière, **la maintenance** de vos installations, ainsi que **la formation et la sensibilisation de vos employés** à la sécurité informatique ou les audits internes. En cas de besoin, nous vous assistons également pour **la certification de vos systèmes informatiques** selon ISO 20 000 et ISO 27 001.

Vos avantages:

Vous avez atteint vos objectifs: **une sécurité dont vous n'avez plus besoin de vous préoccuper.**

Rittmeyer, une société du BRUGG GROUP, développe et fournit des solutions de conduite et de mesure prêtes à l'emploi dédiées à l'approvisionnement en eau et en énergie, aux centrales hydrauliques et aux stations d'épuration. Depuis 1904, le nom Rittmeyer est synonyme de produits et de services haut de gamme. Rittmeyer se positionne comme partenaire auprès de ses clients et les accompagne pendant toute la durée de vie de leurs installations – de la conception à la formation en passant par la planification, la mise en service, l'installation et de nombreux services. Avec six succursales, un bureau de vente et des revendeurs dans plus de 25 pays, Rittmeyer est présent dans le monde entier.

www.rittmeyer.com

rittmeyer
BRUGG

Rittmeyer AG
Inwilerriedstrasse 57
BP 1660
CH-6341 Baar
+41 41 767 10 00
security@rittmeyer.com

82820.2.F | 1511 ERN