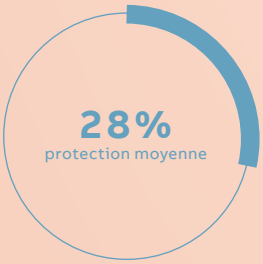
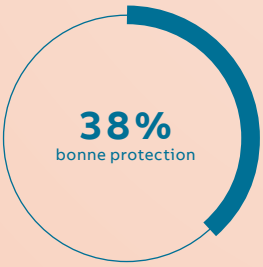
Bien se protéger: Aucune chance aux cyberattaques

—
La majorité des entreprises ont le sentiment d'être bien protégées contre les cyberattaques – même si beaucoup ont déjà été touchées par celles-ci. Et seule une petite proportion d'entre elles considère que la menace des cyberattaques est grande. Les infographies de cette page et des pages suivantes présentent les résultats de l'étude d'ICTswitzerland «Cyberrisques dans les PME suisses», dans le cadre de laquelle 300 petites et moyennes entreprises ont été interrogées.





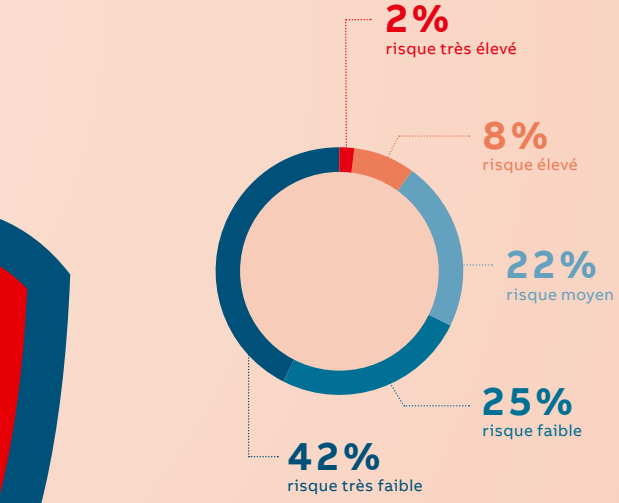
SÉCURITÉ PRÉSUMÉE
Plus de la moitié des PME suisses interrogées s'estime généralement bien ou très bien protégée contre les cyberattaques.

Depuis quelques années, on parle de plus en plus des cyberattaques qui menacent les processus industriels. Pourtant, de nombreux responsables sous-estiment encore les risques. Dans ce contexte, il est important de faire connaître les mesures de cybersécurité appropriées et de les développer. ABB a défini une approche progressive qui guide les clients à travers plusieurs étapes de développement afin d'obtenir la meilleure sécurité possible.

36%

DES MENACES SIGNIFICATIVES

36% des PME interrogées ont déjà été touchés par un malware tel qu'un virus ou un cheval de Troie. 6% ont déjà été confrontés à une perte de données et 4% à une extorsion de fonds.



FAIBLE PERCEPTION DES RISQUES

Seules 10% des PME interrogées estiment élevé ou très élevé le risque d'être touchés dans les prochaines années par une cyberattaque qui paralyserait leur activité pendant au moins une journée.

Lorsque l'on interroge les entreprises sur la cybercriminalité dans les entreprises, on constate un écart important entre les menaces objectives et leur perception subjective. Dans les petites et moyennes entreprises, le risque de cyberattaque est sous-estimé. Selon une étude mandatée par l'association faîtière ICTswitzerland et d'autres partenaires, plus d'un tiers des PME suisses a probablement déjà été touché par des cyberattaques. Pourtant, une majorité d'entreprises se sentent encore bien, voire très bien protégées. Une enquête menée par le cabinet d'audit et de conseil Deloitte montre également que les entreprises principalement actives sur le marché suisse en particulier se laissent bercer par un faux sentiment de sécurité. Entre autres aussi parce qu'elles ne détectent pas toujours les atteintes à la sécurité, faute d'outils de surveillance adaptés. Les conséquences d'une cyberattaque peuvent cependant être très graves. Les dommages potentiels vont des défaillances de l'exploitation jusqu'au vol de données sensibles.

Le facteur humain

Les facteurs humains tels que l'inattention ou le manque de formation des collaborateurs sont aussi un aspect important de la cybercriminalité. La transmission de connaissances et la

Illustration: ©istockphoto.com/akindo

sensibilisation constituent donc des mesures de prévention essentielles. Les menaces focalisant l'attention des médias – telles que WannaCry, le botnet Mirai, Industroyer ou (Not)Petya – amènent aussi les entreprises à repenser la sécurité informatique. Quant à la question de savoir qui se cache derrière les cyberattaques, de nombreuses entreprises tâtonnent encore dans le noir. En plus des groupes de pirates isolés, on suspecte souvent une criminalité économique organisée ou des organismes gouvernementaux d'être à l'origine de ces attaques. Cependant, on manque généralement d'informations fiables à ce sujet.

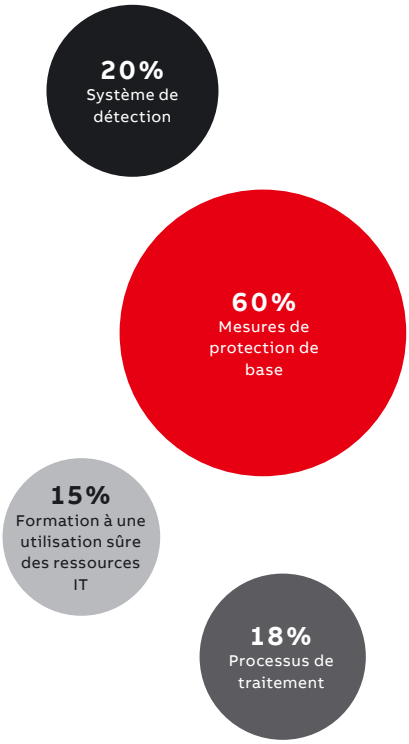
Attaque fatale: ICS Cyber Kill Chain
Les pirates extérieurs s'attaquant aux systèmes de contrôle industriels (ICS) suivent souvent le schéma de la Cyber Kill Chain, un schéma élaboré par Lockheed Martin pour décrire les cyberattaques et adapté par le SANS Institute. Ce schéma comprend deux grandes étapes qui décrivent une progression de plus en plus importante du pirate. Au cours de l'étape 1, le pirate aborde l'entreprise cible sur son réseau, en soi de la même façon que lors d'attaques «classiques». Au cours de l'étape 2, le pirate utilise l'accès au réseau de l'entreprise pour recueillir des informations détaillées sur l'équipement de commande et sa configuration. Sur la base de ces informations, le pirate élabore alors des plans d'attaque spécifiquement adaptés à l'entreprise et aux installations cibles, sélectionne les outils appropriés à cet effet ou, si nécessaire, développe de nouveaux outils et les paramètres en fonction de l'environnement cible.

SCION, l'architecture Internet du futur
Un groupe de travail de l'ETH Zurich travaille sur l'élimination de nombreuses failles de sécurité de l'Internet actuel avec la nouvelle architecture Internet SCION (Scalability, Control, and Isolation on Next-Generation Networks). David Basin (voir aussi sa rapide interview p. 14): «L'Internet n'a pas été développé du point de vue de la sécurité. La sécurité était un critère important dès le début du développement de l'architecture SCION. Les émetteurs peuvent eux-mêmes déterminer la façon dont les données transitent sur le réseau. Une fois le trafic de données orienté sur un chemin spécifique, il ne peut plus être réorienté par d'autres personnes. De surcroît, toutes les informations relatives au réseau sont protégées par cryptographie.»

«L'Internet n'a pas été développé du point de vue de la sécurité.»

Dangers généraux et attaques spécifiques
La technologie SCION n'en étant encore qu'à ses balbutiements, ABB aide ses clients à résoudre leurs problématiques actuelles en leur proposant un large éventail de solutions personnalisées pour gérer plus efficacement leur sécurité. Comme l'explique Ragnar Schierholz, responsable de la cybersécurité chez ABB Industrial Automation: «Dans le monde de l'IT, la disponibilité et la confidentialité des données sont essentiels. Dans notre environnement de technologie opérationnelle (TO) et ses équipements de commande hautement spécialisés, le plus important est le comportement déterministe du système. Il fait ce qu'il est censé faire.» L'IT et la TO se chevauchent et sont menacés par des dangers similaires, voire identiques. «Nous observons une dichotomie des dangers. Il y a d'une part des cybermenaces non ciblées face auxquelles des contre-mesures relative-

Protection incomplète



Seuls 60% des PME interrogées déclarent avoir réellement mis en œuvre des mesures de protection de base telles qu'un pare-feu ou un système de sauvegarde. Seule une entreprise sur cinq a mis en place des systèmes complets de détection des cyberincidents. Environ le même nombre a mis en place des processus définis pour le traitement de ces incidents.

—
Les collaborateurs qui ouvrent par erreur ou négligence des brèches dans les systèmes contribuent en grande partie à la propagation des cybermenaces.

ment simples, comme des patchs réguliers, peuvent aider. D'autre part, nous assistons à des attaques très ciblées, basées sur le principe de la Cyber Kill Chain», explique Ragnar Schierholz. Dans ce cas, les pirates essaient de se frayer progressivement un chemin jusqu'à l'équipement de commande. Face aux attaques contre les entreprises du secteur industriel et les installations isolées, il est crucial de connaître la façon de procéder du pirate et d'utiliser ces informations pour le repousser. «Une stratégie de défense efficace consiste, par exemple, à identifier et à observer un pirate à un stade précoce, à adapter les mesures de sécurité aux caractéristiques spécifiques de l'attaque identifiée et à l'empêcher ainsi d'aller plus loin», précise Ragnar Schierholz.

—
«Nous observons une dichotomie des dangers. Il y a d'une part des cybermenaces non ciblées, et d'autre part des attaques extrêmement ciblées.»

Gérer les différents cycles de vie

Les différents cycles de vie des appareils et des installations dans les domaines de la TO, de l'IT et des logiciels (malveillants) rendent plus difficile la défense contre les cybermenaces. Alors que les cycles de vie typiques dans l'industrie des processus sont d'au moins 10 à 20 ans, ils sont bien plus courts dans le monde de l'IT et des logiciels. «La disponibilité et la continuité des processus sont extrêmement importantes pour l'industrie», indique Ragnar Schierholz. «C'est pourquoi il est recommandé de réaliser chaque changement de version avec des mises à jour mineures tout au long de la durée de vie de l'installation afin de limiter au maximum le risque de projets de mise à niveau ou même d'arrêt de l'installation pour opérer des changements IT majeurs».

Détruire quatre mythes

«Nos services de conseil aux clients industriels commencent souvent par la nécessité de détruire les quatre mythes classiques de la cybersécurité», explique Ragnar Schierholz. Premier mythe: les petites entreprises et petites branches ne sont pas une cible de choix si elles ne sont pas sous les feux des projecteurs C'est faux, car tout ce qui vaut la peine d'être possédé vaut la peine d'être volé. Deuxième mythe: une sécurité élevée est une perte de temps et d'argent. Faux, car un équipement de

commande compromis empêche l'exécution des contrats dans les délais ou dans la qualité requise. De plus, les risques de sécurité non pris en compte entraînent une augmentation des primes d'assurance pour la continuité de l'activité, voire un refus des assureurs. Troisième mythe: notre système est hermétiquement cloisonné et n'a pas de connexion avec le monde extérieur. Encore faux, car le personnel doit entrer et sortir des données du système. Si aucune communication n'est établie, des solutions de contournement pratiques et dangereuses sont improvisées. Quatrième mythe: le système n'a pas de connexion directe avec Internet. Les pirates n'y ont donc pas accès. C'est encore faux, car la plupart des incidents sont des attaques en plusieurs étapes, et les pirates se déplacent sur les côtés du réseau de l'entreprise pour atteindre des cibles intéressantes.

Trois niveaux pour plus de cybersécurité
La destruction des mythes, la sensibilisation de la direction et des autres niveaux pertinents de l'entreprise, et l'identification des zones à haut risque sur la base de l'expérience partagée font partie du niveau 0 du modèle à trois niveaux d'ABB pour améliorer la cybersécurité.

Au niveau 1, l'entreprise introduit une protection de base, créant ainsi la base de la cybersécurité en son sein. Cela permet d'atténuer les risques les plus courants au moyen de contre-mesures et d'établir une compréhension détaillée des risques en fonction du contexte.

— «Les solutions de cybersécurité d'ABB aident les clients à faire de la cybersécurité un élément naturel de leur quotidien.»

Au niveau 2, sous l'intitulé «Défendez votre système», l'entreprise met en place un système de gestion de la sécurité basé sur les résultats de l'évaluation des risques, établit systématiquement des pratiques de sécurité et se conforme aux normes applicables.

Au niveau 3, l'entreprise maîtrise ses risques. Elle améliore continuellement son système de gestion de la sécurité en fonction du paysage des menaces et documente la conformité aux normes applicables.

ABB propose des modules complémentaires de la suite ABB Ability pour permettre aux entreprises de remplir les tâches à tous les niveaux du modèle. «Les solutions de cybersécurité d'ABB aident les clients à prendre de meilleures décisions, à renforcer leurs cyberdéfenses et à faire de la cybersécurité un élément naturel de

—
«Déterminer soi-même la manière dont les données transitent»

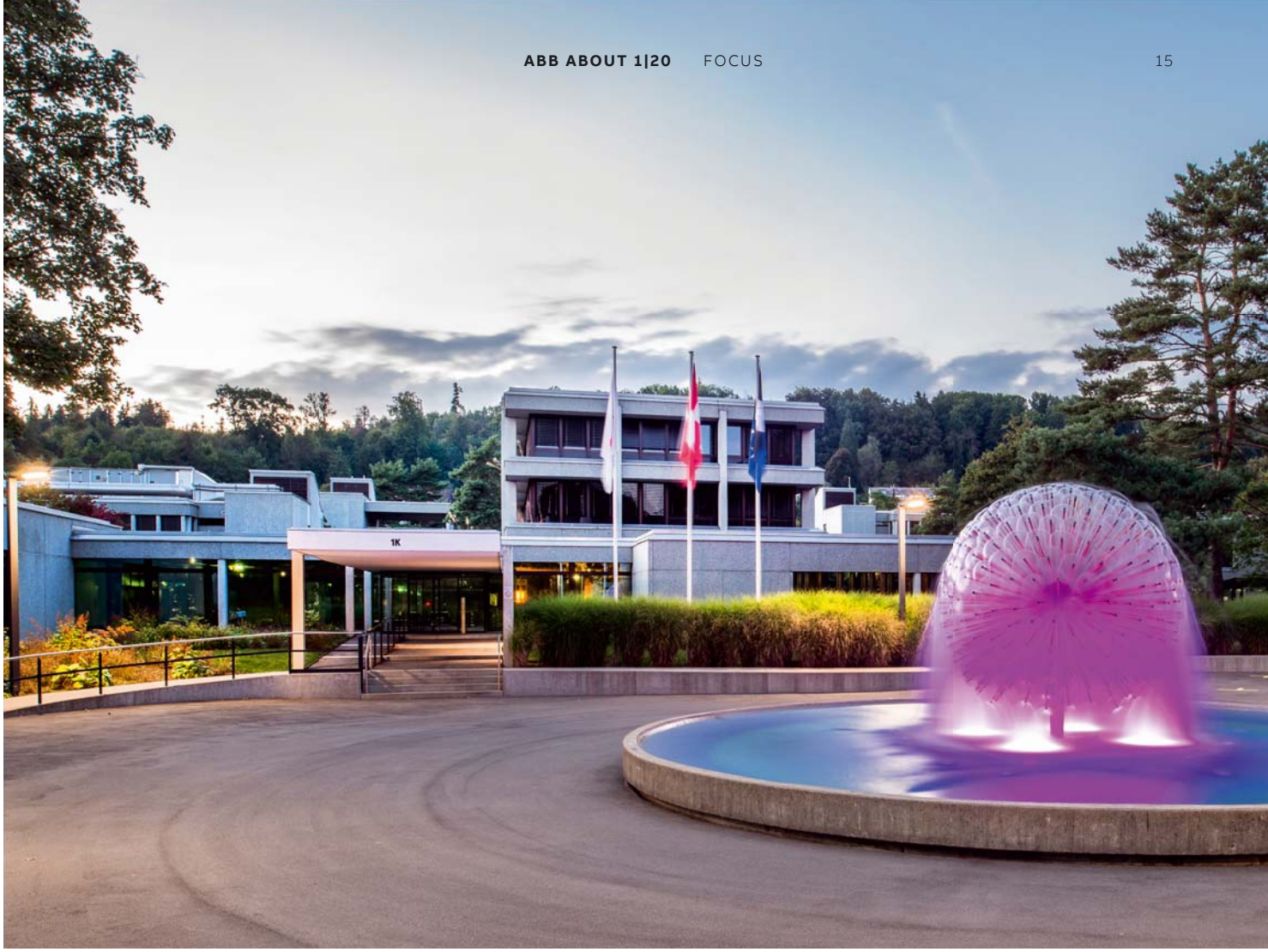
RAPIDE INTERVIEW DE DAVID BASIN
ETH ZURICH, INSTITUTE OF INFORMATION SECURITY

Quels sont les risques de sécurité liés à l'échange de données sur Internet tel que ce dernier existe aujourd'hui?
Les menaces de sécurité sont devenues omniprésentes. Les entreprises sont une cible de choix pour obtenir des informations, pratiquer l'extorsion de fonds ou détruire leurs systèmes et ainsi leur réputation. La situation est extrêmement problématique, même pour les systèmes cyber-physiques, surtout si un accès via Internet est possible.

De quelle manière la nouvelle architecture logicielle SCION rendrait-elle Internet plus sûr?
La sécurité était un critère important dès le début du développement de l'architecture SCION. Les émetteurs peuvent eux-mêmes déterminer la façon dont les données transitent sur le réseau. Une fois le trafic de données orienté sur un chemin spécifique, il ne peut plus être réorienté par d'autres personnes.

Dans quelle mesure la technologie SCION a-t-elle déjà fait ses preuves dans la pratique?
L'équipe qui entoure le professeur Adrian Perrig à l'ETH a créé le réseau SCIONLab afin de tester SCION dans des environnements à grande échelle. Et avec succès: SCIONLab connecte déjà plus de 50 systèmes autonomes dans plus de 15 pays. En outre, plusieurs fournisseurs d'accès à Internet utilisent déjà SCION, par exemple Swisscom depuis près de deux ans. Une offre visant le marché industriel sera disponible dans les prochains mois.

— Interview complète dans le magazine numérique: http://tiny.cc/davidbasin



leur quotidien», déclare Ragnar Schierholz. Les ensembles de services choisis peuvent être utilisés en autonomie par les clients ou être mis en œuvre et gérés par les centres de service d'ABB.

Prêts à relever les défis futurs

Les scientifiques du centre de recherche du groupe ABB à Baden-Dättwil travaillent sur d'autres solutions ABB pour la cybersécurité future. Ognjen Vukovic, chef de l'équipe de recherche sur la cybersécurité, indique à ce sujet: «Dans le cadre du projet Service Ledger, nous étudions l'utilisation de la technologie des chaînes de blocs (blockchain) dans un scénario de micro-réseau pour des contrats et une facturation intelligents entre les membres du micro-réseau». Pour débuter la mise en pratique, les chercheurs ont utilisé des compteurs intelligents à chaînes de blocs dans une installation pilote en Suisse. «Dans un autre projet, nous étudions les dangers qui pourraient se présenter à l'avenir en cas d'utilisation criminelle d'ordinateurs quantiques, car ces derniers peuvent cracker de nombreux algorithmes cryptographiques qui sont utilisés aujourd'hui», explique Ognjen Vukovic. Il est certes peu probable qu'il y ait des ordinateurs quantiques exploitables dans les dix à 20 prochaines années, mais les produits numériques d'ABB ont une durée de vie prévue de plus de 20 ans et doivent donc utiliser des algorithmes cryptographiques qui ne pourront pas être crackés par les ordinateurs quantiques. Un troisième projet à Baden-Dättwil concerne l'analyse de données hautement confidentielles. «De nombreux clients ne veulent pas envoyer sur le cloud des données très sensibles, par exemple des secrets industriels ou des informations sur les collaborateurs. Par conséquent, nous étudions des méthodes techniques comme le cryptage homomorphe qui nous permet d'analyser des données cryptées sans connaître la clé», souligne Ognjen Vukovic. Les applications déterminantes pour la sécurité et basées sur l'intelligence artificielle sont aussi un sujet d'étude. Les scientifiques d'ABB étudient comment mieux protéger ces systèmes contre des attaques très ciblées, qui sont souvent indétectables pour l'homme, mais peuvent avoir des conséquences très sérieuses.

Informations:
ragnar.schierholz@de.abb.com
ognjen.vukovic@ch.abb.com

—
En sécurité vers l'avenir: au centre de recherche du groupe ABB à Dättwil, les scientifiques travaillent sur la cybersécurité de demain – avec des technologies telles que les chaînes de blocs, les ordinateurs quantiques et le cryptage homomorphe.