CEBEO INDUSTRY • Hiver 2025 • Année 6 • Édition 10

CEBEO
INDUSTRY

DÉCRYPTAGE DE LA DIRECTIVE NIS2 : QUE SIGNIFIENT POUR VOUS LES NOUVELLES OBLIGATIONS

HOME & BUILDING | INDUSTRY

LÉGISLATION
Une cybersécurité efficace en 7 étapes

PRÉVENTION
La norme IEC 62443 pour fil rouge

OPPORTUNITÉ
NIS2 offre des opportunités supplémentaires aux fabricants de machines

cebeo
A Sonepar Company

10

ÉDITION

Une édition de
CEBEO NV/SA

SIÈGE SOCIAL :
Eugène Bekaertlaan 63, 8790 Waregem

ÉDITEUR RESPONSABLE :
Régis André
Eugène Bekaertlaan 63, 8790 Waregem

RÉDACTEUR EN CHEF :
Summer Vanhaverbeke

RÉDACTION :
Bart Vancauwenberghe

SECRÉTARIAT :
Julie Delannay

TRADUCTION ÉDITION FRANÇAISE :
Yamagata Europe

MISE EN PAGE :
ReMark Reclame

IMPRESSION :
GBL, Courtrai

CHER LEC-TEUR,

La directive sur la sécurité des réseaux et de l'information 2 (NIS2) introduite par l'Union européenne est cruciale pour l'industrie, car elle renforce la résilience numérique et réduit les cybermenaces. À une époque où les cyberattaques se multiplient, cette directive fournit un cadre juridique qui impose aux entreprises d'améliorer leurs mesures en matière de cybersécurité.

Les entreprises vulnérables aux cyberattaques risquent d'être victimes de fuites de données, d'interruptions de production et de pertes financières. En se conformant à la directive NIS2, les entreprises se rendent plus résilientes aux attaques et renforcent la confiance avec leurs clients et partenaires.

La directive encourage également la collaboration au sein et entre les secteurs. Elle oblige les entreprises à signaler les incidents et à partager les informations sur les menaces, ce qui contribue à un temps de réaction réduit et une meilleure prévention. Elle rend également la chaîne d'approvisionnement plus sûre, car toutes les parties concernées doivent se conformer à des normes strictes.

Pour les entreprises de secteurs essentiels tels que l'énergie, les soins de santé et les transports, la directive NIS2 ne constitue pas seulement une obligation, mais surtout un avantage stratégique. En s'y conformant de manière proactive, les entreprises renforcent leur position concurrentielle et prouvent qu'elles répondent aux exigences toujours plus nombreuses d'un monde (de production) numériquement connecté. C'est pourquoi l'industrie aurait tout intérêt à considérer le NIS2 avant tout comme un investissement nécessaire pour l'avenir.

Dans ce magazine, nous examinons en détail la valeur ajoutée de la directive NIS2 et la manière dont divers fabricants aident leurs clients finaux à s'y conformer. Bien que Cebeo ne soit pas soumise à la directive NIS2, il va de soi que nous mettons tout en œuvre pour atteindre nous-mêmes le niveau de cybersécurité le plus élevé possible. Nous vous donnerons quelques mots d'explication à ce sujet également.

Nous vous souhaitons une bonne lecture !

Summer Vanhaverbeke
Communications Coordinator

CONTENU

DÉCRYPTAGE DE LA DIRECTIVE NIS2 : QUE SIGNIFIENT POUR VOUS LES NOUVELLES OBLIGATIONS

KOEN PAUWELYN (SIEMENS) :

« Nous adoptons une approche progressive avec un certain nombre de priorités claires. »

PETER-JAN DELTOUR (PHOENIX CONTACT) :

« Il s'agit de trouver le bon équilibre entre investissement dans la cybersécurité et efficacité opérationnelle. »

THOMAS VASEN (HMS) :

« Les dispositions de la norme IEC 62443 contribuent effectivement à des processus industriels plus sûrs. »

FLORIAN DELANGHE (CEBEO) :

« L'informatique de pointe est très utile en termes de protection des données critiques et de fiabilité opérationnelle. »

32

STEVEN DEPUYDT (CEBEO) :

« Le plus grand danger qui nous guette réside dans les manipulations IT risquées effectuées par vos propres collaborateurs. »

CENTER FOR
CYBERSECURITY BELGIUM

SE CONFOR
DOIT ÊTRE U
DE NOM

RMER À LA LOI NIS2 NE PRIORITÉ POUR MBREUSES ENTITÉS

Une cyberattaque est le pinacle de la vulnérabilité en ligne : mieux vaut s'en protéger de manière optimale. C'est également l'objectif de la nouvelle loi belge NIS2 qui est entrée en vigueur depuis le 18 octobre. Qu'est-ce que cela implique exactement ? Comment s'y conformer ? Quels sont les risques auxquels vous vous exposez si vous ne vous y conformez pas ? Dirk De Paepe, Senior Certification Expert au CCB (Centre for Cybersecurity Belgium) nous explique tout de manière exhaustive.

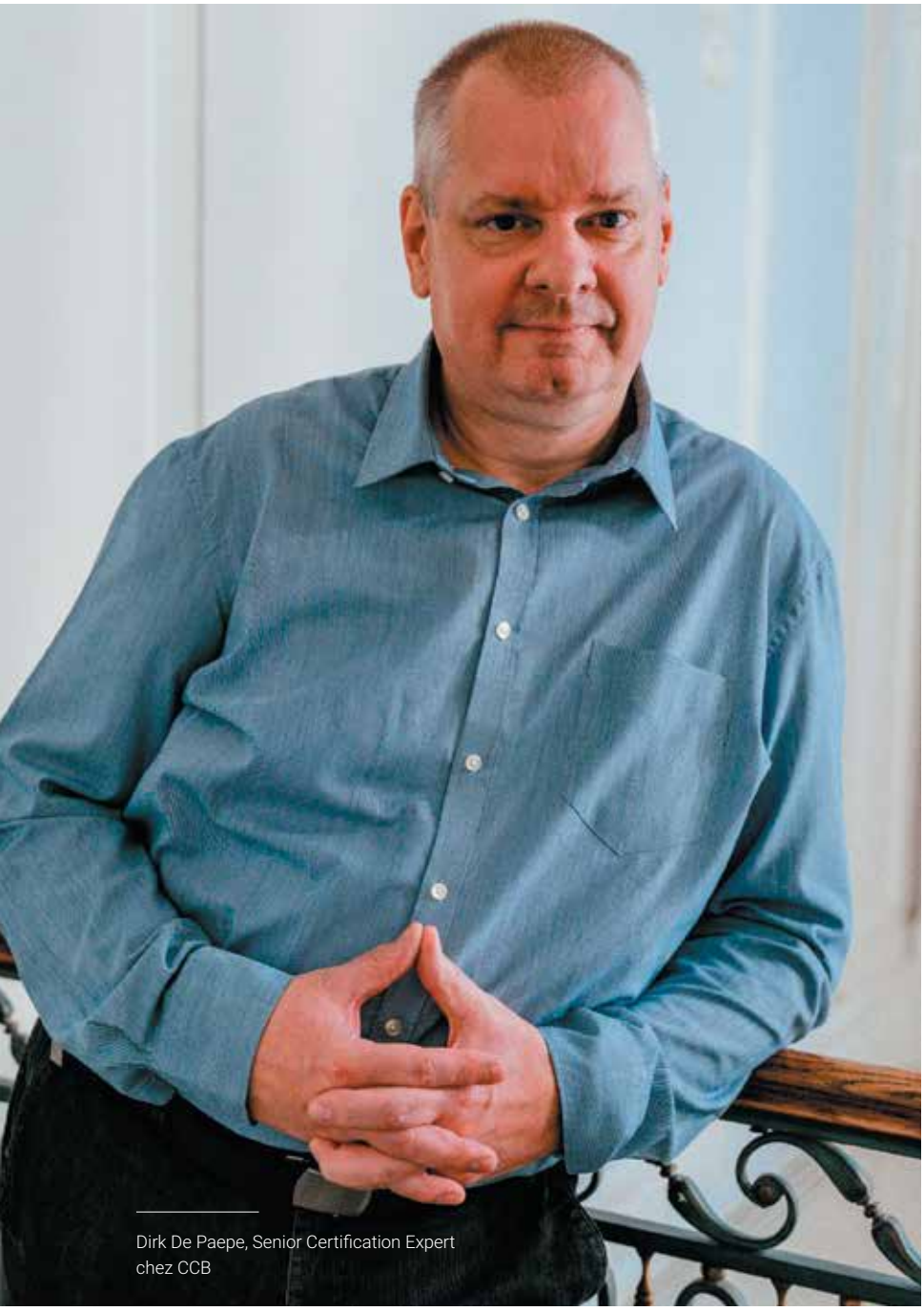
Poursuivez votre lecture en page 8

« La cybersécurité est devenue absolument incontournable »

Suite de la page 7

En 2016, l'Europe a publié une directive sur la cybersécurité que l'ensemble des États membres doit(devait) traduire en législation. En Belgique, cela a donné naissance le 7 avril 2019 à la loi NIS (NIS signifie « Network and Information Systems », NDLR).

« La Directive NIS européenne avait trois objectifs », souligne Dirk De Paepe. « Elle imposait aux gouvernements nationaux de prêter l'attention nécessaire à la cybersécurité. Deuxièmement, elle devait renforcer la collaboration entre les autorités en charge de la cybersécurité à l'échelle européenne. Elle devait en outre obliger les principaux opérateurs des secteurs les plus importants à prendre des mesures de sécurité et à signaler les incidents. »



Dirk De Paepe, Senior Certification Expert chez CCB

UNE NÉCESSITÉ ENCORE PLUS GRANDE

Cependant, la loi NIS1 n'a pas réussi non plus à atteindre tous les objectifs fixés. « Elle a eu des effets positifs en Europe, mais son champ d'application était trop limité, et elle manquait de clarté quant au groupe cible auquel elle s'appliquait. Une situation qui s'est traduite par une mise en application inefficace et l'imposition de sanctions. De plus, l'Europe a constaté une trop grande disparité au niveau des approches des différents États membres. Les besoins en matière de cybersécurité ont par ailleurs augmenté de manière considérable. Cela s'explique par une forte augmentation de la cybercriminalité, que l'on perçoit dans la hausse significative du nombre de menaces. Dans sa globalité, notre société est aussi devenue beaucoup plus dépendante du monde numérique et est beaucoup plus connectée, ce qui augmente sa vulnérabilité. »

« Nous constatons d'ores et déjà que de nombreux autres États membres prennent la Belgique pour exemple. »

Safeonweb.be

C'est pourquoi l'Europe a proposé une nouvelle mouture plus exigeante avec la directive NIS2. « Celle-ci conserve les mêmes objectifs que la NIS1, mais élargit considérablement le nombre d'entités et de secteurs concernés. Elle comprend également des mesures plus claires, des règles étendues en matière de notification d'incidents, des règles de sanction plus strictes et plus spécifiques et prévoit une plus grande responsabilisation du haut management de chaque entité. »

PIONNIER

La Belgique a pris cette nouvelle directive très au sérieux et est même la première à la traduire intégralement dans la nouvelle loi NIS2 qui est entrée en vigueur le 18 octobre 2024. « Le fait que le gouvernement attache une grande importance à cette loi et aux décisions exécutives qui en découlent est une bonne nouvelle. Nous constatons d'ores et déjà que de nombreux autres États membres prennent la Belgique pour exemple. Certains d'entre eux ont tendance à copier notre approche dans leur propre pays, ce qui pourrait représenter un avantage pour nos entreprises. Le CCB a joué un rôle déterminant dans l'élaboration de la loi NIS2 et s'est également concerté à ce sujet avec les parties intéressées et les autorités sectorielles. »

Poursuivez votre lecture en page 10

PLAN EN 7 ÉTAPES

En tant qu'entité, que devez-vous faire à présent à l'égard de la loi NIS2 ? Pour vous aider, le CCB a élaboré un plan en sept étapes, dont vous trouverez la version étendue en ligne.

« Il est crucial que les entreprises essentielles et importantes sécurisent également leur chaîne d'approvisionnement. »

Matériel de campagne © Safeonweb 2024

Suite de la page 9

Au cours des dernières semaines et des derniers mois, le CCB n'a pas ménagé ses efforts afin de tenir tout le monde informé. « Pour ce faire, nous avons utilisé des dizaines de présentations, des vidéos expliquant le plus clairement possible les bases fondamentales de la cybersécurité, ainsi que notre site Internet.

Nous mettons également un point d'honneur à répondre individuellement à toutes les demandes d'informations qui nous sont envoyées par e-mail. Bien entendu, nous avons également fourni d'amples informations aux fédérations sectorielles et aux organisations d'employeurs. Malgré tous ces efforts, nous constatons que de nombreuses organisations et entreprises tombent encore des nues lorsqu'elles entendent parler de la loi NIS2. C'est pourquoi nous poursuivrons sans relâche nos campagnes d'information au cours des mois à venir. »

ESSENTIEL OU IMPORTANT

En Belgique, nous opérons une distinction entre une entreprise importante et une entreprise essentielle. L'explication de cette distinction est disponible sur le site Internet du CCB et est reprise dans les annexes I et II de la loi NIS2 belge.

Le contrôle des mesures de cybersécurité prises est effectué par des organismes d'évaluation de la conformité (OEC). Il s'agit d'organisations autorisées par le CCB dont la liste est disponible en ligne (www.cyfun.be), avec les conditions à remplir pour devenir un OEC.

« Dans le cas des entités « importantes », les évaluations de la conformité régulières se font en principe sur base volontaire. Pour les entreprises « essentielles » par contre, ces évaluations de conformité régulières sont obligatoires. Généralement, les entités essentielles sont des organisations d'envergure opérant dans des secteurs très critiques et sont vitales pour un pays : si elles cessent de fonctionner en raison d'une cyberattaque, nombre de personnes en pâtissent.

Les entreprises d'utilité publique et les hôpitaux en sont de bons exemples. Les entreprises importantes (telles que les services de coursier) sont en général des organisations de taille moyenne opérant dans des secteurs très critiques et de grandes et moyennes organisations dans d'autres secteurs critiques où les cyberincidents peuvent également avoir de graves conséquences sur la société.
Il est en outre crucial pour les entreprises essentielles et importantes de sécuriser également leur chaîne d'approvisionnement. On peut donc en conclure que la loi NIS2 aura un impact important sur bon nombre d'entités. »

SANCTIONS

Vous n'avez que faire de la NIS2 en tant qu'entité ? Ce n'est pas une bonne idée. D'une part, vous vous tirez une balle dans le pied en négligeant la cybersécurité, et d'autre part, il s'agit également d'une loi : vous devez vous y conformer.

« Les entités qui ne s'y conforment pas et qui commettent donc des infractions vis-à-vis des mesures de gestion des risques et de la notification d'incident s'exposent dans un premier temps à des mesures administratives, telles que des avertissements et des instructions contraignantes. Si une entité essentielle s'abstient de le faire, une personne assumant des responsabilités dirigeantes, telle qu'un directeur général, peut même se voir temporairement interdire d'exercer ses fonctions au sein de cette entité. »

Des amendes substantielles sont également possibles. « Pour les entités importantes, celles-ci peuvent atteindre 7 millions d'euros, ou 1,4 % du chiffre d'affaires mondial total de l'exercice précédent (le montant le plus élevé étant retenu). Pour les entités essentielles, ce montant peut aller jusqu'à 10 millions d'euros, ou 2 % du chiffre d'affaires (le montant le plus élevé étant retenu). »

Poursuivez votre lecture en page 11

« À défaut de s'y conformer, la personne s'expose à des amendes ou à une interdiction temporaire d'exercer ses fonctions. »

Dirk De Paepe, Senior Certification Expert chez CCB

Suite de la page 11

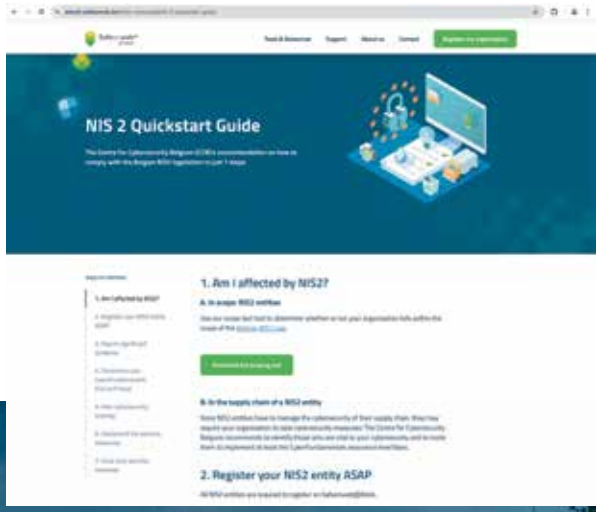
AU TRAVAIL

Il n'y a donc pas de temps à perdre pour se conformer à la loi NIS2. Dirk De Paepe recommande aux entités de commencer par la formation de base CyberFundamentals. « Celle-ci porte, par exemple, sur la réalisation et la vérification de backups : des backups qui tournent sur le même réseau et/ou ne fonctionnent pas ne vous seront d'aucune aide. En outre, il est très judicieux d'intégrer l'authentification multifacteurs (MFA, une méthode qui vérifie l'identité de l'utilisateur de plus d'une manière, NDLR). À défaut d'en disposer, l'entité court davantage le risque d'être victime des cybercriminels. Ceux-ci profitent souvent de la moindre faille de cybersécurité pour agir et ciblent aussi bien les grandes que les petites entreprises. »

À l'aide du « scope tool » dans le guide de démarrage rapide disponible sur le site Internet du CCB (www.cyfun.be), chaque entité peut vérifier si elle est importante ou essentielle. L'outil d'auto-évaluation CyFun® disponible sur ce même site vous donne, en tant qu'entité, une idée claire de votre niveau de cyber-résilience et vous permet de planifier et de budgétiser la manière dont vous pouvez accroître celle-ci afin de répondre aux exigences légales de la loi NIS2.

www.cyfun.be

www.safeonweb.be



Matériel de campagne © Safeonweb 2024

HIGH BAY GEN 5 FONCTIONNALITÉS AMÉLIORÉES, PERFORMANCE FIABLE: LA NOUVELLE GÉNÉRATION DE LUMINAIRES HIGH BAY

UNE CONCEPTION FIABLE, DES PERFORMANCES OPTIMALES

HIGH BAY GEN 5

Versions ON/OFF et DALI-2 fiables avec protection IP66 et IK10

UNE SOLUTIONS D'ÉCLAIRAGE ÉCONOME EN ÉNERGIE ET LUMINEUSE POUR DES APPLICATIONS INDUSTRIELLES EXIGEANTES

La nouvelle référence pour les applications industrielles intérieures avec des plafonds jusqu'à 18 m de hauteur nécessitant un éclairage intense : le HIGH BAY GEN 5 se distingue par son efficacité énergétique exceptionnelle et sa fiabilité, offrant un niveau de protection élevé (IP66/IK10) adapté aux environnements exigeants.
Grâce à la fonctionnalité MULTI LUMEN, le flux lumineux peut être ajusté sur deux niveaux de puissance, assurant un éclairage optimal en fonction des besoins spécifiques du site. Les modèles DALI-2 offrent une flexibilité accrue pour la gestion de l'éclairage.
Un crochet de montage est inclus, et des accessoires optionnels, tels que des réflecteurs, des réfracteurs et des supports de montage sont disponibles séparément, apportant une flexibilité supplémentaire à vos projets.
De plus, les HIGH BAY GEN 5 sont faciles à installer et bénéficient d'une garantie de 5 ans.

Découvrez-en plus ! BENELUX.LEDVANCE.COM

PARTENARIAT CEBEO SIEMENS

La conformité à la directive NIS2 est un défi plus que jamais d'actualité pour bon nombre d'entreprises industrielles. Celle-ci nécessite des adaptations au niveau IT, mais plus encore au niveau des technologies opérationnelles (OT). La cybersécurité est un sujet auquel Siemens accorde beaucoup d'attention, tant au sein qu'en dehors de l'entreprise. Trois spécialistes expliquent comment l'acteur technologique accompagne le client final industriel dans cette démarche.

Poursuivez votre lecture en page 16

SIEMENS SOUTIE
FINAUX INDUSTR
PROCESSUS DE C
À LA DIRECTIVE N

« La cybersécurité requiert des efforts à différents niveaux »

NT LES CLIENTS RIELS DANS LEUR CONFORMITÉ NIS2

« La segmentation du réseau est une étape importante, notamment pour sécuriser les machines obsolètes. »

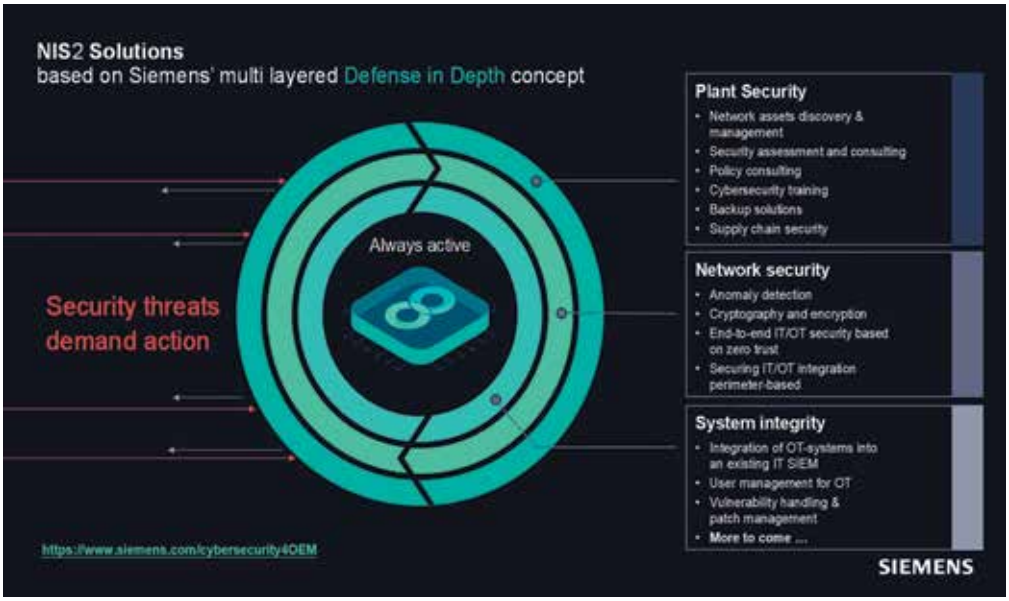
Gregory Putman, Sales Specialist communication industrielle pour la Wallonie

Suite de la page 15

« Bien entendu, la cybersécurité est une priorité absolue pour Siemens », lance Koen Pauwelyn, un Service Sales Specialist rompu à la cybersécurité de par sa fonction. « Des équipements IT et OT 100 % sûrs sont une exigence que bon nombre de nos clients reprennent dans leurs cahiers des charges. Notre portefeuille de services et de produits a, en ce sens, fortement évolué. Nous voulons jouer le rôle de chef de file, notamment en informant les clients de manière ciblée. »

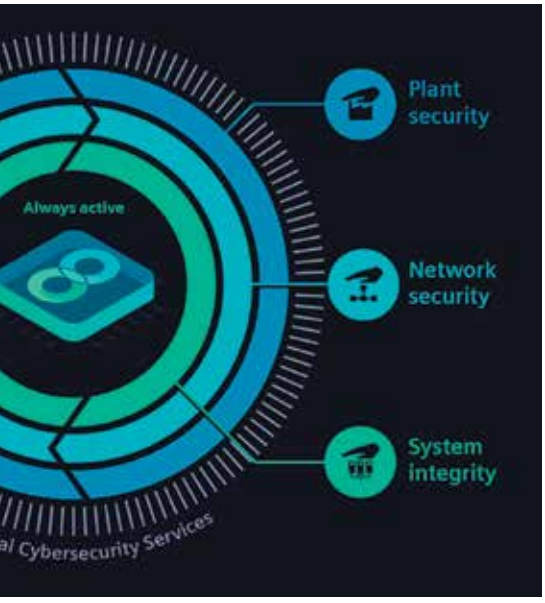
C'est d'ailleurs nécessaire, indique son collègue Bart Boumans (Sales Specialist en communication industrielle pour la Flandre). « Nous constatons encore régulièrement que des clients qui doivent être conformes à la directive NIS2 d'ici 2025, tombent des nues. Il en va de même pour les entreprises qui sont convaincues que cette dernière ne les concerne pas. Toutefois, s'il est question de fournisseurs d'une entreprise qui doit être « conforme à la directive NIS2 », ceux-ci ont tout intérêt à faire les efforts nécessaires, car les entreprises soumises à la directive NIS2 ont également pour tâche de sécuriser leur « chaîne d'approvisionnement. »

Chez Siemens, ils constatent souvent que les acteurs de l'industrie se concentrent principalement sur l'IT dans le cadre de la NIS2, alors que le volet OT mérite au moins autant d'attention. « Les PLC, les capteurs, les machines,… doivent également être sécurisés », poursuit Koen Pauwelyn. « C'est un réel défi, car les machines ont une bien plus longue durée de vie qu'un ordinateur portable, par exemple, et fonctionnent souvent avec des systèmes obsolètes qui ne peuvent plus être mis à jour. Même s'ils recourent à des technologies modernes, ils n'ont généralement qu'une seule occasion de les « patcher » par an, car ils travaillent 24 heures sur 24, et une entreprise ne peut se permettre de mettre la production à l'arrêt à tout bout de champ pour procéder à des mises à jour. »



PLAN D'ACTION

Il est donc grand temps d'élaborer une stratégie cohérente et de la mettre en œuvre. Siemens a un important rôle à jouer à ce niveau. Koen : « Il est difficile pour un intégrateur système d'évaluer ses propres réalisations en matière de cybersécurité. C'est un rôle dont nous pouvons nous charger, en tant que tierce partie. Nous commençons par une mesure de référence, qui reflète la situation actuelle. Sur la base de cette mesure, nous pouvons dresser une « feuille de route » qui reprend toutes les adaptations nécessaires pour se conformer à la directive NIS2. Parce qu'il est impossible de tout changer en une fois, nous adoptons une approche progressive avec quelques priorités claires. »



INTERACTION AVEC CEBEO

L'interaction entre Cebeo et des partenaires tels que Siemens peut apporter une valeur ajoutée face au défi que pose la mise en conformité à la directive NIS2. Gregory : « Cebeo fait clairement comprendre à ses clients en quoi consiste exactement la directive NIS2 et leur sert de guide en leur indiquant les étapes à suivre. Siemens peut fournir les informations et la formation adéquates, ainsi que l'accompagnement nécessaire dans le cadre du déploiement de la directive NIS2 au sein de l'organisation. »

Siemens conçoit la cybersécurité en différentes couches, selon le concept de « Defense in Dept ». La première couche est celle de la sécurité du réseau. « La segmentation du réseau est une étape importante, notamment pour sécuriser les machines obsolètes », précise Gregory Putman (Sales Specialist communication industrielle pour la Wallonie). « La mise en place de pare-feux pour de telles machines est également un moyen idéal de les sécuriser, afin de les isoler du reste du parc OT. »

L'intégrité du système est un deuxième pilier essentiel. « Celle-ci peut notamment être obtenue à l'aide du portail TIA (Total Integrated Automation), une plate-forme logicielle qui vous permet de programmer facilement et en toute sécurité des produits d'automatisation, tels que des PLC, grâce à une communication cryptée.

Poursuivez votre lecture en page 18

Bart Boumans, Sales Specialist en communication industrielle pour la Flandre

« Les entreprises soumises à la directive NIS2 ont également pour tâche de sécuriser leur 'chaîne d'approvisionnement'. »

« Il est essentiel de tester de temps à autre le bon fonctionnement des backups. »

Koen Pauwelyn,
Service Sales Specialist

Suite de la page 17

Le portail TIA comprend notamment un système de gestion des utilisateurs qui vous permet de définir clairement les autorisations de chacun. Cela permet également de déterminer l'approche en matière de gestion des utilisateurs pour les appareils OT à partir du système IT Active Directory (AD).

La « détection d'anomalies » est également essentielle. Il s'agit d'une approche avancée en matière de cybersécurité qui offre une protection en temps réel en détectant, analysant et signalant automatiquement toute activité suspecte »

SÉCURITÉ DES ÉQUIPEMENTS

Les entreprises ont également tout intérêt à investir dans la sécurité des équipements. « Cela entend notamment de protéger correctement votre infrastructure contre le monde extérieur. Pour bien aborder la sécurité des équipements, il faut d'abord informer vos collaborateurs comme il se doit, notamment en leur faisant suivre des formations générales sur la cybersécurité.

Nous constatons que les formations sont souvent un poste sur lequel les entreprises cherchent à faire des économies, mais qu'à (long) terme, cela peut avoir un impact négatif sur la productivité. Des formations plus ciblées en matière de cybersécurité, sur les programmes d'ingénierie par exemple, permet aussi souvent de mieux comprendre des sujets complexes qui sont connus de manière trop superficielle. »

Une cybersécurité totale n'existe pas, mais une surveillance adéquate permet d'éviter bien des désagréments. « L'intégration de systèmes d'alarme qui détectent les anomalies est un pas dans la bonne direction. Ces solutions surveillent votre réseau de manière passive : lorsqu'elles déclenchent une alarme, vous décidez des mesures à prendre. »

Chez Siemens, nous recommandons aux clients finaux d'utiliser le bon micrologiciel (avec les mises à jour de sécurité gratuites pour les PLC et autres composants OT) et de gérer de manière raisonnable les backups. « Il s'agit là aussi d'un pilier important de la directive NIS2. Il est essentiel de pouvoir récupérer des données grâce aux backups et d'en tester de temps en temps le bon fonctionnement.

Chaque entreprise doit s'efforcer d'élaborer un « plan de reprise après sinistre » clair, avec des mesures précises permettant d'agir rapidement en cas de problème. Pour ce faire, il convient de désigner un responsable qui veillera à ce que les procédures établies soient suivies à la lettre et qui, idéalement, teste aussi ces protocoles régulièrement. »

INFOS

Cliquez sur le lien suivant afin d'en savoir plus sur l'approche de Siemens à l'égard de la directive NIS2 :

CEBEO PARTNERSHIPS
PHOENIX CONTACT

PHOENIX CONTACT CONSEILLE À L'INDU D'INVESTIR EN PRIO LA CYBERSÉCURITÉ

Vous voulez éviter à tout prix que votre production soit mise à l'arrêt du jour au lendemain en raison de facteurs externes. Il s'agit pourtant d'un risque bien réel si vous négligez votre cybersécurité. C'est donc à juste titre que Phoenix Contact plaide pour sa mise en place. « Vous ne devez pas passer du tout au tout à marche forcée : le développement des procédures adéquates et le parcours d'adaptation de vos collaborateurs prennent également du temps », indique Peter-Jan Deltour, Head of OT & Cybersecurity chez Phoenix Contact Belgique.

Poursuivez votre lecture en page 22

USTRIE
ORITÉ DANS

« Le coût de la prévention est bien inférieur au prix à payer en cas de cyberattaque »

« Toutes les cyberattaques réussies dont est victime une PME ne font pas la une des journaux. Loin de là ! »

Suite de la page 21

Peter-Jan Deltour, Head of OT & La cybersécurité produits chez Phoenix Contact Belgique

En tant qu'entreprise technologique de premier plan, Phoenix Contact propose des solutions innovantes dans les domaines de l'électrotechnique et de l'automatisation. Vous les trouverez partout où des flux d'électricité ou de données doivent être connectés, distribués ou contrôlés. À cette fin, l'entreprise développe et fabrique divers produits tels que des barrettes de connexion , des alimentations, des PLC et des solutions d'IdO destinés aux secteurs de l'ingénierie mécanique, de l'énergie et de l'infrastructure, entre autres. Phoenix Contact aide les entreprises à travailler de manière plus efficace et sûre, toujours dans une optique durable et en mettant l'accent sur la numérisation.

LOI SUR LA CYBER-RÉSILIENCE (CYBER RESILIENCE ACT)

« Cet aspect de la sécurité est de plus en plus important », souligne Peter-Jan Deltour. « Nos produits doivent répondre aux exigences de l'industrie en matière de cybersécurité. D'ici 2027, ils devront également satisfaire aux normes de la loi sur la cyber-résilience qui s'adresse principalement aux fournisseurs de composants, comme nous. Cette nouvelle directive européenne souligne une fois encore la nécessité accrue de sécuriser efficacement les solutions IT et OT. »

Lors de l'intégration de la cybersécurité dans ses solutions, Phoenix Contact prend la norme IEC 62443 pour fil rouge. « C'est l'une des rares normes de cybersécurité qui se concentre également sur le marché industriel. Lorsque nos systèmes sont installés chez des clients finaux industriels, ils doivent fonctionner de manière optimale durant toute leur durée de vie - entendez par là les 20 années à suivre, grosso modo - et continuer de répondre aux exigences de sécurité à la fin de cette période. La norme IEC 62443 y veille par un volet intégral sur la protection et la sécurité des composants. Nos PLC répondent à ces exigences depuis 2019 déjà, avec une intégration systématique dans tous nos autres groupes de produits également. »

Avancer que la cybersécurité relève exclusivement de la responsabilité de votre service IT peut être risqué. « Souvent, ces personnes ne connaissent pas de manière suffisamment détaillée ce qu'implique la technologie opérationnelle. Il est donc judicieux de confier cette tâche à un partenaire disposant de connaissances approfondies, comme un fournisseur de ces composants, par exemple. »

AUDIT OBLIGATOIRE

En plus de sécuriser son propre portefeuille de produits, Phoenix Contact propose également des services afin d'aider les clients finaux à concevoir et implémenter la cybersécurité. Bon nombre d'entreprises se rendent compte qu'elles ont besoin d'une approche structurée en matière de cybersécurité pour leur OT, mais ignorent souvent par où commencer. Afin d'aider les clients finaux industriels à rendre leur infrastructure cybersécurisée, Phoenix Contact adopte une approche mûrement réfléchie.

« Tout d'abord, nous identifions tous les éléments (machines, hall d'usine…). Dans la plupart des cas, la documentation mise à disposition par les entreprises dans ce domaine ne correspond pas totalement à la réalité. Dès lors, si les entreprises souhaitent bénéficier de notre aide, cet audit est obligatoire, car nous devons savoir le plus précisément possible ce que nous devons sécuriser. »

Poursuivez votre lecture en page 24

Suite de la page 23

Deuxième étape : une analyse des risques. « Ne pas miser sur la cybersécurité est une grave erreur. Vouloir aller trop vite n'est pas une bonne idée non plus. La technologie en soi coûte de l'argent, mais entre-temps, vous devez également permettre aux procédures d'évoluer en parallèle et donner le temps à vos collaborateurs de se familiariser avec la nouvelle approche. Un rythme trop soutenu peut refroidir les gens, créant un effet inverse et augmentant encore le risque. Vos collaborateurs auront très certainement les meilleures intentions, mais en réalité, ils constituent dans de nombreux cas le maillon faible dans de tels processus. »

Cette analyse de risque résulte en une liste mettant en évidence les différents points névralgiques, grands comme petits. « Il incombe ensuite à l'entreprise d'établir les priorités ainsi qu'un timing pour les mettre en œuvre. Quoi qu'il en soit, vous pouvez commencer par quelques « gains rapides », tels qu'une configuration correcte des pare-feux. Vous devez toutefois veiller à planifier concrètement d'autres mesures, car elles peuvent avoir un impact sur le flux opérationnel de votre organisation. »

DEMANDE INDUITE PAR LES INCIDENTS

À vrai dire, on ne peut plus se permettre de reléguer la cybersécurité au second plan, estime Peter-Jan. « Heureusement, nous constatons que les entreprises sont de plus en plus nombreuses à demander de l'aide dans le cadre de cette démarche. Hélas, elles le font encore (trop) souvent après avoir déjà été confrontées à un incident, ou après qu'une cyberattaque ayant touché une entreprise ait été fort médiatisée. Sachez que ces annonces ne sont que la partie émergée de l'iceberg : toutes les cyberattaques réussies dont sont victimes les PME ne font pas la une des journaux. »

Il est vrai que la cybersécurité représente un coût, mais le prix de la prévention reste de toute façon bien inférieur à celui qu'il faut payer pour limiter au maximum l'impact d'une attaque. « De plus, la question n'est pas tant de savoir si une attaque se produira un jour, mais plutôt quand elle aura lieu, et quel en sera l'impact ? Il s'agit de trouver le bon équilibre entre investissement dans la cybersécurité et efficacité opérationnelle. Cet équilibre n'est pas simple, mais idéalement, la sécurité doit toujours peser un peu plus lourd dans la balance. »

« Nous devons savoir le plus précisément possible ce que nous devons sécuriser. »

Peter-Jan Deltour

PARTENAIRES

Cebeo, les intégrateurs de systèmes et les fabricants de machines jouent également un rôle important dans l'amélioration du niveau de cybersécurité au sein de notre industrie, estime Peter-Jan Deltour. « De par sa position, Cebeo est très proche du marché et très au courant de ce qui s'y passe. Elle dispose pour ce faire d'un soutien plus vaste lui permettant de détecter les problèmes et de prodiguer des conseils. Les intégrateurs et les fabricants de machines peuvent également être d'une grande valeur, sans s'en rendre compte.

En effet, il devient crucial pour les entreprises de sécuriser l'ensemble de leur « chaîne d'approvisionnement ». Le fait de savoir que les machines sont cybersécurisées de manière optimale offre une certaine tranquillité d'esprit et renforce la confiance envers les fabricants de machines qui peuvent dès lors bénéficier d'une publicité supplémentaire via le bouche-à-oreille. »

Peter-Jan salue les efforts de sensibilisation déployés depuis quelque temps déjà par le CCB (Center for Cybersecurity Belgium) et invite le secteur à poursuivre sur cette voie en investissant dans la sécurité numérique. « Il ne faut pas le voir comme une obligation, mais comme une étape nécessaire à une sécurisation accrue de vos processus. En tant qu'organisation certifiée TÜV pour la mise en œuvre de la norme IEC 62443 (tant en termes de gestion globale, que d'intégration de système et de sécurité des composants), Phoenix Contact veut souhaite apporter sa pierre à l'édifice. »

Grâce à Phoenix Contact, Audi a réalisé un concept de protection 360° dans la phase de planification, en tant que IEC 62443-2-4-Security Service certifiée TÜV.

CEBEO
PARTNERSHIPS
HMS

HMS INVITE LES FABRICANTS DE MACHINES À INTÉGRER DES NIVEAUX DE SÉCURITÉ DANS LES MACHINES

« La norme IEC 62443 est une bonne base sur laquelle progresser. »

Thomas Vasen,
Business Developer Network Security
chez HMS

NIS2 : tout cela est bien beau, mais comment s'assurer que l'on est en conformité si cette directive ne se traduit pas vraiment par des mesures concrètes ? Thomas Vasen, Business Developer Network Security chez HMS (Hardware Meets Software), estime qu'avec le CyberFundamentals Framework, la Belgique montre le bon exemple. « La mise en application de la norme IEC 62443 constitue un fil conducteur bien utile pour permettre aux fabricants de machines et au secteur d'intégrer la cybersécurité dans le volet OT des processus industriels de manière optimale. »

Poursuivez votre lecture en page 28

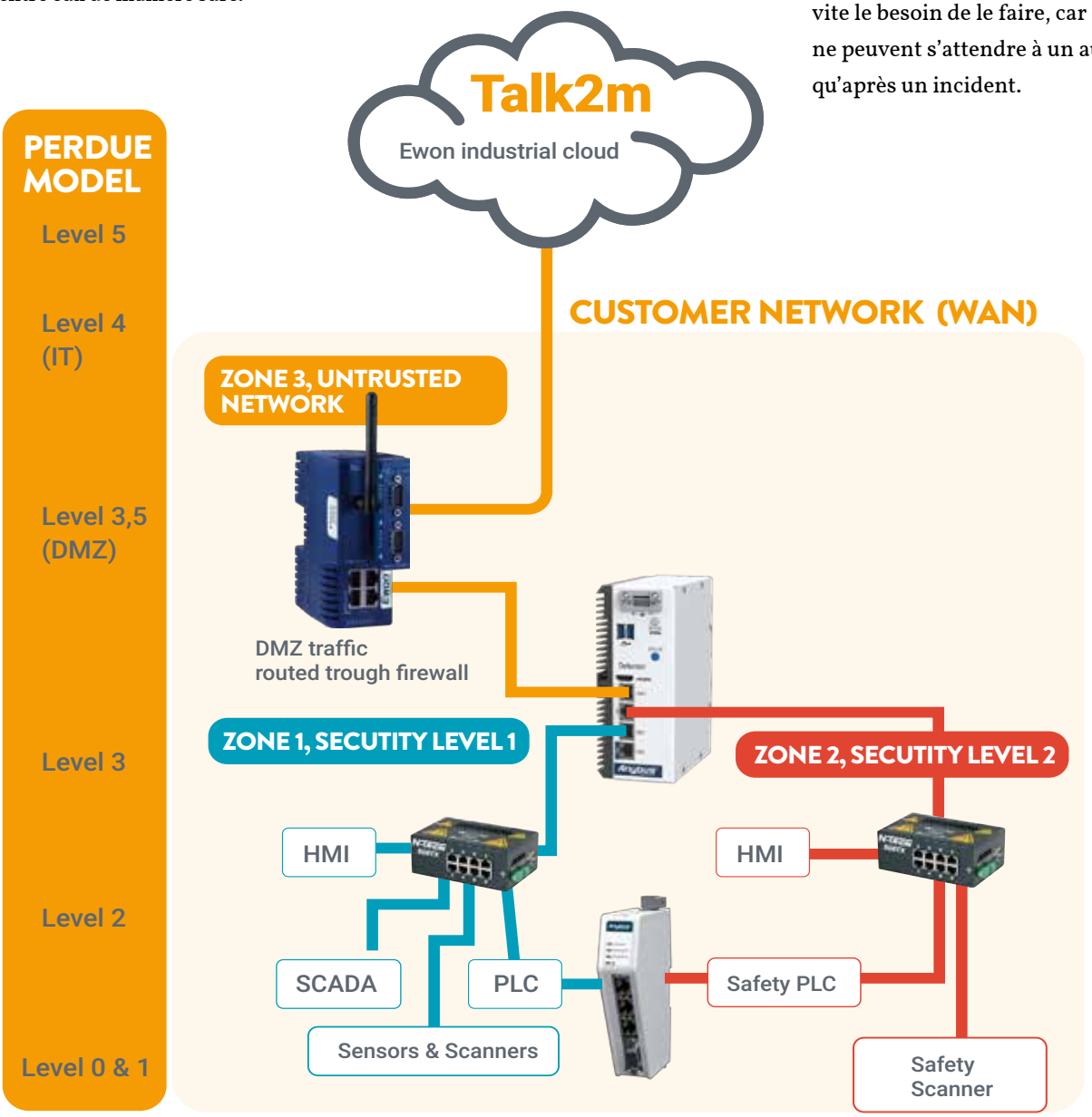
Suite de la page 27

PROTOCOLES DE MISE À JOUR

Voilà de nombreuses années que la cybersécurité est une priorité absolue pour HMS. De ce fait, ils ne savent que trop bien où se situent les principaux obstacles. « Nous constatons souvent l'absence d'authentification intégrée lors de l'utilisation de protocoles industriels. Pour pallier cela, il est généralement nécessaire de mettre ces protocoles à jour afin que les PLC (Programmable Logic Controllers) et autres dispositifs OT puissent communiquer entre eux de manière sûre. »

Ce n'est pas évident : souvent, les versions sécurisées ne sont pas encore disponibles ou tous les PLC et RTU (Remote Terminal Units) doivent être remplacés. Et les coûts sont en outre élevés. D'autres stratégies sont donc nécessaires pour protéger les réseaux OT dès aujourd'hui.

La solution se trouve dans la segmentation, une stratégie qui permet d'isoler les machines les unes des autres et de contrôler ainsi la communication entre les différentes zones des réseaux OT selon une politique « deny by default ». Cependant, la mise en œuvre nécessite souvent un arrêt temporaire de la production et c'est là que le bât blesse évidemment. « Les entreprises qui appartiennent aux « autres secteurs critiques » au sens de la directive NIS2 ressentent moins vite le besoin de le faire, car elles ne peuvent s'attendre à un audit qu'après un incident.



Dans le cas des « Secteurs très critiques au sens de la directive NIS2 », la situation est différente, car elles peuvent également faire l'objet d'audits inopinés. En outre, pour bon nombre d'entreprises, la cybersécurité des OT ne vient qu'en second lieu : l'urgence réside surtout dans la sécurisation du volet IT, notamment parce que les éventuels dysfonctionnements au niveau OT sont souvent dus à un problème IT. »

VISER LA CLARTÉ

Ajoutez à cela que dans bon nombre de pays européens, la directive NIS2 ne se traduit pas en une législation nationale concrète. « Il est dès lors recommandé de mettre les « meilleures pratiques » en application après une analyse des risques, mais celles-ci sont souvent différentes pour la plupart des secteurs. Il est quelque part logique que l'Europe intègre une certaine neutralité à cet égard avec la directive NIS2 puisqu'elle souhaite être indépendante des systèmes de certification. Mais cela crée une certaine ambiguïté. La Belgique l'a bien anticipé en créant le CyberFundamentals Framework, une série de mesures concrètes censées accroître la cyber-résilience d'une organisation. »

Le CyberFundamentals Framework repose sur quatre cadres de cybersécurité couramment utilisés, dont la norme IEC 62443. « Cet ensemble de normes définit les exigences et les processus pour l'implémentation et la maintenance des systèmes d'automatisation et de contrôle industriels sécurisés électroniquement », précise Thomas Vasen. « Quiconque sait lire entre les lignes de la directive NIS2 comprendra que l'Europe considère cette norme comme un fil rouge utile.

La lecture de la norme IEC 62443 se révélera peut-être fastidieuse, mais l'on comprendra rapidement que les normes proposées contribuent effectivement à rendre les processus industriels plus sûrs. »

Poursuivez votre lecture en page 30

« Pour bon nombre d'entreprises, la sécurité des OT n'arrive qu'à la deuxième place. »

Thomas Vasen,
Business Developer Network Security chez HMS

Suite de la page 29

HMS aide les clients finaux et fabricants de machines industriels à se conformer à la directive NIS2. « Tout d'abord, nous constatons un besoin important de formations et de consultance. Nous y répondons au travers de la formation Industrial Security Awareness, au cours de laquelle nous expliquons les risques d'une manière accessible - notamment par une démonstration effectuée par un hacker éthique - et clarifions simplement la manière de relever ce défi.

Dans une deuxième phase, nous pouvons procéder à un « redesign» d'un système en collaboration avec des intégrateurs système : comment fonctionnent une usine et son parc de machines, où se situent les risques les plus importants ? Par exemple : un fabricant de yaourts a tout intérêt à sécuriser un maximum la machine qui mélange le yaourt avec les fruits. En cas de problème, vider et nettoyer la machine vous fera perdre beaucoup de temps et d'argent. »

NIVEAUX DE SÉCURITÉ

Troisièmement, il convient de déterminer le niveau de sécurité de chaque machine - idéalement via la norme 62443 - avant d'y appliquer les exigences de segmentation souhaitées. « Le niveau de sécurité 1 (SL1) ne requiert qu'une segmentation « logique », tandis que le niveau SL2 requiert une segmentation physique. En divisant le parc de machines en segments plus petits, vous en améliorez la sécurité, les performances et la facilité de gestion. Des règles de sécurité et d'accès spécifiques permettent d'éviter que des utilisateurs non autorisés se fraient un chemin à travers le réseau ou que des menaces s'y propagent. »

« Quiconque sait lire entre les lignes de la directive NIS2 comprendra que l'Europe considère la norme IEC 62443 comme un fil rouge utile. »

UN CHOIX DÉLIBÉRÉ

Thomas invite l'industrie et les fabricants de machines à gérer ensemble la directive NIS2. « Quelles que soient les exigences, garantir une sécurité robuste pour vos processus opérationnels est avant tout un choix. Choisissez délibérément ce niveau de sécurité plus élevé et recourez à la norme 62443 afin d'évoluer vers un environnement de production résilient. Les fabricants de machines ne doivent pas se soustraire à leurs responsabilités, mais plutôt considérer la directive NIS2 comme un outil leur permettant d'offrir un service de meilleure qualité encore à leurs clients. »

Thomas Vasen y voit une tâche importante et une opportunité de taille pour les fabricants de machines. « Suite à la directive NIS2, les clients finaux industriels reçoivent de plus en plus de questions de la part de leurs compagnies d'assurance, qui veulent savoir comment ils sécurisent leur technologie opérationnelle. Une situation qui amènera l'industrie à demander aux fabricants de machines d'intégrer des niveaux de sécurité spécifiques dans leurs machines Ceux-ci devraient pouvoir choisir de prévoir le niveau SL1 de série, et demander un prix plus élevé à partir du niveau SL2. Tout le monde y gagne : le client industriel est conforme à la directive NIS2 et le fabricant de machines voit son business model amélioré. Ce qui devrait automatiquement mener à un réseau mieux sécurisé. »

CEBEO DÉPARTEMENT IT

« Réagir de manière proactive aux menaces potentielles »

Steven Depuydt, Chief Information Officer chez Cebeo

CEBEO INVESTIT MASSIVEMENT DANS LE PLUS HAUT NIVEAU DE CYBERSÉCURITÉ POSSIBLE

En tant que partenaire en équipements et solutions électrotechniques, Cebeo estime qu'il est important de vous montrer comment aborder efficacement votre cybersécurité. Ces dernières années, des investissements importants ont été consentis pour renforcer et développer le département IT. Steven Depuydt (Chief Information Officer) explique comment notre organisation fait de la cybersécurité une priorité absolue.

Poursuivez votre lecture en page 34

Suite de la page 33

Il y a sept ans, Steven Depuydt a rejoint Cebeo en tant que premier CIO à temps plein. « À l'époque, le département IT comptait 24 personnes. Aujourd'hui, il y en a pas moins de 66. Parmi elles, deux personnes travaillent à temps plein sur la cybersécurité : l'une se charge de mettre au point la stratégie et la planification, l'autre est ingénieur en sécurité. »

RUN, CHANGE, TRANSFORM

À son arrivée chez Cebeo, Steven a mis l'accent sur la planification et l'élaboration d'une transformation numérique intégrale. « Tant au niveau de l'infrastructure que du volet logiciel, tout a été ou est en train d'être complètement actualisé », explique-t-il. « Cela se reflète notamment dans les nouveaux serveurs, les réseaux et un pare-feu, mais également en ligne, les systèmes de gestion d'entrepôt et du transport, etc. Le département IT se concentre sur trois éléments : « Run » (tout ce qui est nécessaire pour être parfaitement opérationnel), « Change » (les changements et les innovations prévues) et « Transform » (tous les efforts qui s'inscrivent dans le cadre de la transformation numérique). À cette fin, un Center of Excellence a été créé et accueille notre personnel en charge de la cybersécurité.

Ils travaillent dans le respect de la norme ISO27001 (norme de qualité en matière de sécurité de l'information, NDLR) et ont pour ambition d'obtenir à terme ce certificat. »

En principe, Cebeo ne doit pas se conformer à la directive NIS2, mais nous mettons tout en œuvre pour atteindre un niveau de cybersécurité extrêmement élevé. « Un audit récent de PWC a montré qu'à cet égard, Cebeo fait partie des meilleures entités du groupe Sonepar, maison mère de Cebeo, tous pays confondus », poursuit Steven. « Des audits internes sont également menés régulièrement afin de nous mettre au défi à cet égard. Ainsi, nous organisons régulièrement des tests d'hameçonnage et des tests de pénétration pour voir dans quelle mesure notre infrastructure IT est résiliente face aux menaces potentielles. Nous travaillons de la manière la plus proactive possible à cet égard en sensibilisant nos collaborateurs et en leur proposant des formations en cybersécurité. En effet, le plus grand risque d'intrusion indésirable qui nous guette réside dans les manipulations IT potentiellement risquées effectuées par nos collaborateurs. »

DIX DOUVES

« J'ai récemment entendu un hacker éthique me dire qu'en tant qu'organisation, nous devions construire non pas une, mais dix 'douves' autour de notre 'château' », poursuit Steven. « C'est pourquoi nous faisons une multitude d'efforts afin d'optimiser notre cybersécurité. Nous y voyons en tous les cas un signal positif de la part du groupe Sonepar en faveur d'une approche globale et centralisée de ce phénomène. La fertilisation croisée entre les experts de ces différents pays apportera sans le moindre doute une grande valeur ajoutée dans ce domaine. »

« En tant qu'organisation, vous ne devez pas construire une, mais dix 'douves' autour de votre 'château'. »

VARTA Alkaline INDUSTRIAL PRO

VARTA ALKALINE INDUSTRIAL PRO

Est spécialement conçu et produit pour un usage professionnel. Énergie de niveau expert avec une qualité supérieure. Nos batteries haut de gamme sont idéales si vous recherchez une solution de batterie sans tracas pour vos appareils. Des processus de production hautement automatisés garantissent un produit extrêmement fiable et sûr.

- Qualité premium (Fabriqué en Allemagne)
- Durée de conservation jusqu'à 10 ans*
- Technologie anti-fuite
- Conception et emballage du produit respectueux des OEM pour une manipulation facile
- Gamme complète adaptée à de nombreuses applications professionnelles

*AAA, AA, C, D

VARTA

Make reliable

IMPACT

with PanelSeT enclosures

Armoires industrielles d'extérieur PanelSeT HD

Grâce à leur revêtement anticorrosion, nos armoires en acier PanelSeT HD sont spécialement conçues pour résister aux conditions extérieures difficiles.

Life Is On | Schneider Electric

GUIDE DE SÉLECTION « NETWORKS FOR INDUSTRY »

UN PONT ENTRE L'INDUSTRIE ET LES SOLUTIONS DATACOM

La connectivité joue un rôle toujours plus essentiel dans les environnements industriels. Pour répondre à ce besoin croissant, Cebeo étend son expertise en matière de datacom pour le marché tertiaire au secteur industriel. Le nouveau guide de sélection « Networks for Industry », qui paraîtra en 2025, se compose d'un guide pratique et d'un document de travail.

Suite à la page 40

« Offrir une plus-value grâce au partage des connaissances internes et externes »

Florian Delanghe, Product Manager
Datacom & Telecom chez Cebeo

Suite de la page 39

LA RENCONTRE ENTRE INDUSTRIE ET DATACOM

La connectivité de données est une exigence fondamentale pour l'industrie moderne. En effet, les capteurs, les contrôles PLC et les appareils connectés génèrent des données en temps réel permettant de partager, analyser et gérer les processus de production. Cela permet de réduire les coûts, d'accroître la productivité et de réduire les temps d'interruption.

Une connectivité fiable via des câbles en cuivre, en fibre optique ou une connexion sans fil joue donc un rôle crucial pour maintenir le processus de production opérationnel.

« OFFRIR UNE PLUS-VALUE GRÂCE AU PARTAGE DES CONNAISSANCES INTERNES ET EXTERNES »

Florian Delanghe, Product Manager Datacom & Telecom chez Cebeo, souligne l'importance de la synergie entre l'infrastructure passive (comme les câbles et les connecteurs) et les composants actifs (comme les routeurs et les switches) : « Jusqu'il y a peu, les deux domaines de connaissances étaient répartis entre nos départements Cebeo Solutions for Industry et Cebeo Datacom. Étant donné que le chevauchement entre ces deux segments devient de plus en plus important, nous misons sur le partage des connaissances. Cette fertilisation croisée nous permet d'offrir des solutions datacom intégrées plus robustes pour le marché industriel. »

UN GUIDE STRUCTURÉ DE MANIÈRE LOGIQUE

Pour soutenir cette mission, Cebeo lancera en 2025 le guide de sélection « Networks for Industry », un ouvrage de référence clair et polyvalent. Celui-ci permet à l'entreprise de combler le fossé entre la technologie datacom et les applications industrielles.

Le fait de proposer le guide principalement sous forme numérique permettra de le mettre régulièrement à jour. De cette manière, l'offre reste toujours actuelle et pertinente. Cebeo est en plein phase de rédaction, mais il faudra attendre encore un peu avant que le guide ne soit disponible pour les clients.

Les clients industriels qui souhaitent bénéficier d'un soutien supplémentaire peuvent toutefois déjà compter sur les conseils des spécialistes datacom et sectoriels régionaux de Cebeo. Cebeo combine ainsi sa vaste expertise avec des outils pratiques.

QUE PROPOSE LE GUIDE ?

- Un large éventail de solutions proposées par des fournisseurs fiables
- Une structure logique pour une navigation rapide et facile
- Une attention portée à la cybersécurité, y compris les produits conformes à la nouvelle directive NIS2

legrand®

LE NOUVEAU CATALOGUE LEGRAND 2025-2026 EST ARRIVÉ!

DECOUVREZ-LE DANS TOUS LES FILIALES CEBEO OU SUR LEGRAND.BE

EDITION
2025
2026

EMPLOYÉES DU MOIS

DÉCOUVREZ LES ACCESSOIRES STANDARDISÉES POUR TOUS LES CHEMINS DE CÂBLES OBO

- PLUS DE TRANSPARENCE POUR UN CHOIX FACILE
- COMPATIBLES AVEC LES MODÈLES CLASSIQUES À VISSER ET LES MODELES MAGIC
- À INSTALLER PLUS VITE ET FACILEMENT
- OPTIMISATION DE STOCK
- PLUS PRATIQUE ET FLEXIBLE

SCANNEZ-MOI

Building Connections

OBO BETTERMANN

TECHNOLUX

APPLICATIONS TECHNOLUX POUR TOUS LES DÉFIS

PAC-D AI

UN APPAREIL ADAPTÉ AUX ENVIRONNEMENTS CORROSIFS

Le PAC-D AI est un luminaire à LED de grande puissance (jusqu'à 148 lm/W) conçu pour une utilisation professionnelle dans des environnements humides et poussiéreux et dans des zones exposées à des substances corrosives telles que l'ammoniac.
Le couvercle en méthacrylate opale (IK03) est fixé à la base gris clair en polyester renforcé de fibres de verre au moyen de clips en acier inoxydable, ce qui garantit l'étanchéité sur n'importe quelle surface. Grâce à l'indice de protection élevé IP 69K, le luminaire est protégé en permanence contre la pénétration de la poussière et des jets d'eau, ce qui le rend idéal pour une utilisation dans les étables, les industries du bois et du papier et les zones de stockage.
A la page 255 du catalogue TECHNOLUX 16.0, vous trouverez un aperçu des produits chimiques les plus courants et de leur résistance par rapport aux matériaux utilisés.

LZP HT

UN APPAREIL ADAPTÉ À UNE LARGE GAMME DE TEMPÉRATURES (-40°C À +55°C)

L'hermétique en LED LZP HT est un luminaire puissant (jusqu'à 132 lm/W) et robuste pour l'industrie.
Le diffuseur en polycarbonate opale garantit une résistance aux chocs (IK07) et est fixé à la base gris clair en polyester renforcé de fibres de verre au moyen de clips acier inoxydable, ce qui garantit l'étanchéité sur n'importe quelle surface.
Avec une large fourchette de températures allant de -40°C à + 55°C, le luminaire peut être utilisé dans de nombreuses applications.

Les deux luminaires sont développés et fabriqués en Europe, en tenant compte des exigences de durabilité (modules LED remplaçables, matériaux recyclables, conditions de bien-être des animaux, etc.). Les degrés de protection élevés IP 66 et IP 69K permettent d'installer les unités sans protection à l'extérieur et la certification HACCP garantit que les types peuvent être utilisés dans l'industrie alimentaire.

DEMANDEZ VOTRE CATALOGUE TECHNOLUX 16.0
À VOTRE CONTACT OU TÉLÉCHARGEZ-LE SUR
WWW.CEBEO.BE

OPTIMISATION DES PROCESSUS ENTRE VOTRE SERVICE DE CONCEPTION ET LA PRODUCTION

La digitalisation des processus et une production efficace jouent-elles un rôle important dans votre entreprise ? Vous êtes au bon endroit chez Phoenix Contact. En fonction de votre profil client, nous disposons de différentes solutions internes pour optimiser le processus de production sur la base des données disponibles de votre système CAO.

La construction efficace d'un rail DIN avec des composants (également connu sous le nom de rail DIN fonctionnel) n'est pas un secret pour nous. Trop souvent, nous voyons des actions inutiles et manuelles dans le processus de production chez nos clients, ce qui conduit à des erreurs et à une perte d'efficacité.
Pour accompagner nos clients dans cette démarche, nous avons développé le logiciel ClipX ENGINEER.

CLIPX ENGINEER

ClipX ENGINEER est le nouveau logiciel pour la planification efficace des rails DIN fonctionnels, des plaques de montage et même des armoires électriques ! Ce logiciel permet une liaison directe avec votre système CAO. Toutes les données disponibles sont reprises et peuvent être enrichies, par exemple, avec des matériaux de marquage. Votre rail DIN fonctionnel est-il prêt pour la production ? Toutes les informations sur l'article peuvent ensuite être transmises de manière transparente à votre système de commande. Mais cela ne s'arrête pas là : grâce à ce logiciel, vous pouvez immédiatement passer une commande auprès de l'un de nos centres VAC. Ils produisent le rail DIN fonctionnel complet avec tous les composants et marquages de Phoenix Contact. Après quelques jours, nous vous le livrons prêt à l'emploi à votre entreprise.

Êtes-vous en désaccord ou cela ne correspond-il pas à votre processus d'affaires ? Aucun problème ! Notre logiciel « ClipX ENGINEER ASSEMBLE » peut vous aider à construire efficacement votre rail DIN en interne.

CLIPX ENGINEER ASSEMBLE - ADD-ON – LOGICIEL

Le logiciel d'assistance aux employés ClipX ENGINEER ASSEMBLE est un complément intégré du logiciel d'ingénierie ClipX ENGINEER. Il utilise les données du processus d'ingénierie pour générer des instructions étape par étape pour la construction de rails DIN fonctionnels. De plus, ce logiciel est facile à connecter à notre système Pick-by-Light.
Pour chaque instruction à exécuter, une LED s'allume avec les matériaux à utiliser provenant de notre système d'aide à la production de borniers, laissant la recherche de composants au passé.

PHOENIX CONTACT
INSPIRING INNOVATIONS

Principales caractéristiques

- Logiciel de montage pour borniers, incluant le marquage et des instructions étape par étape.
- Application Web compatible avec Edge, Chrome et Firefox.
- Acquisition directe des données à partir du processus d'ingénierie.
- Gain de temps grâce à la reprise directe des données du projet depuis le processus d'ingénierie.
- Représentation simplifiée des projets en production avec des étapes de processus détaillées.
- Minimisation des erreurs de sélection grâce à un système de contrôle Pick-by-Light.

Cordons, câbles Patch et câbles
Des équipements prêts à brancher pour la production au lieu d'assemblages complexes

Choisissez parmi une vaste gamme de câbles préassemblés ou des câbles de signaux individuels pour les capteurs ou des câbles Ethernet pour la transmission de données.

Weidmüller

CAMPUS 2025

VOUS SOUHAITEZ DÉVELOPPER VOS CONNAISSANCES TECHNIQUES EN TANT QUE PROFESSIONNEL ?

Grâce au programme de formation Cebeo Campus, vous resterez informé des dernières innovations en date dans le secteur en 2025. Les spécialistes de Cebeo ou les fabricants dispensent des formations axées sur la pratique à différents niveaux de connaissance et dans divers domaines.

CVC • ÉNERGIE RENOUVELABLE • DOMOTIQUE ET IMMOTIQUE • RÉSEAUX • CONTRÔLE D'ACCÈS ÉCLAIRAGE • SÉCURITÉ • ÉLECTROMÉNAGER • AUTOMATISATION INDUSTRIELLE

Consultez dès à présent nos formations et inscrivez-vous à une formation près de chez vous.
https://www.cebeo.be/fr-be/formations-evenements

cebeo campus

INDUCTIVE SENSORS THAT MAKE PERFECT SENSE.

THIS IS SICK

Sensor Intelligence.

Regardez autour de vous. Nous sommes tous entourés de nombreux objets conçus pour nous faciliter la vie. Dès qu'on les utilise, on se demande parfois comment on a pu s'en passer. C'est le cas des capteurs inductifs de SICK. Dès que vous passez votre commande, les détecteurs vous aident à travailler plus efficacement. Les détecteurs inductifs de SICK sont aussi durables que fiables, ce qui vous permet de vous détendre grâce à une livraison rapide, une installation rapide et une réduction des coûts de maintenance et de remplacement que vous remarquerez vraiment. Une fois installés, ils augmentent votre productivité, vous permettant de mieux utiliser votre temps. C'est ce que nous appelons l'intelligence ! www.sick.com/inductive_sensors

SUNGROW × cebeo A Sonepar Company

Obtenez plus de votre installation avec Sungrow

Découvrez nos solutions d'utilité

La solution ultime pour le contrôle d’accès

La FAAC B680H est la barrière qui combine polyvalence, durabilité et technologie avancée.

Vitesse et précision
Temps d’ouverture et de fermeture réglable entre 1,5 et 6 secondes.

Flexibilité
Jusqu’à 8 m avec des options de bras droits, articulés ou arrondis.

Résistance aux intempéries
Résiste aux conditions extrêmes avec protection IP56 (TÜV).

Technologie hybride
Combinaison moteur hydraulique et sans balais

Durabilité exceptionnelle
Conçue pour plus de 2 millions de cycles intensifs.

Que ce soit pour des parkings extérieurs, des garages souterrains, des sites industriels ou des voies d’accès, cette barrière offre une solution fiable et efficace pour chaque situation.

Découvrez comment la FAAC B680H peut révolutionner votre gestion des accès. Visitez notre site web ou contactez l’un de nos experts pour un devis ou une démonstration gratuite. www.faacbenelux.com