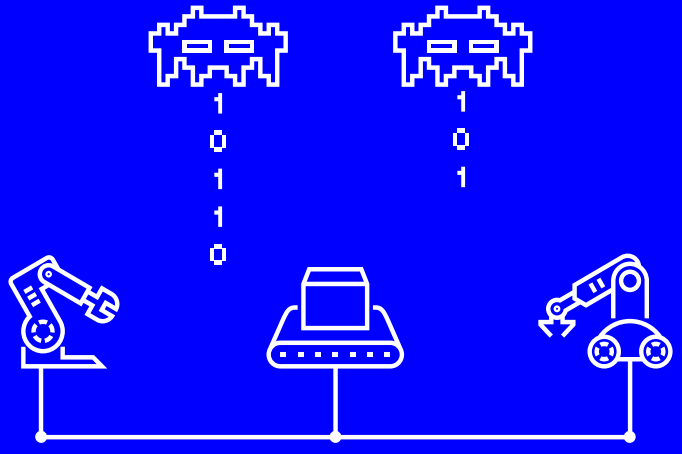
La sécurité industrielle dans l'industrie manufacturière

Quelles entreprises tirent leur épingle du jeu ?

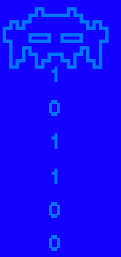


.AGORIA howest UNIVERSITEIT GENT sirris driving industry by technology


1
0
1


1
0
1
0
1


1
0
1


1
0
1
1
0
0


1
0
1
0
1


1
0
1

Table des matières

Avant-propos 05

1 Pourquoi la sécurité industrielle est-elle nécessaire 06

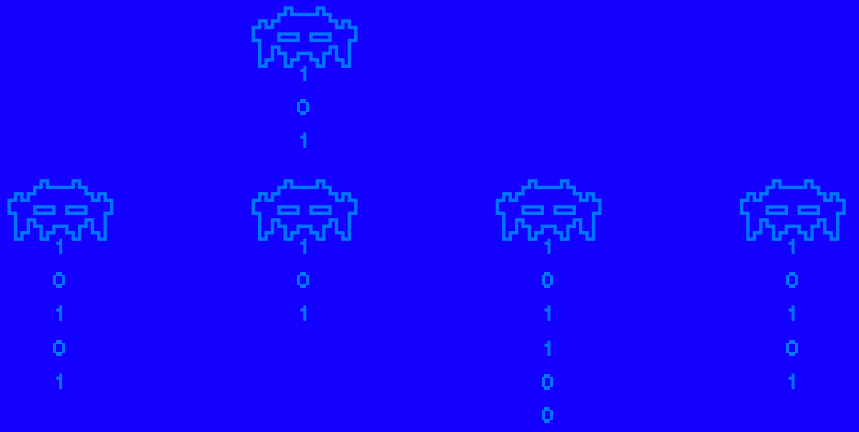
2 Principales conclusions de l'étude 14

3 Agir dans votre entreprise 28

4 Recommandations pour les pouvoirs publics 32

5 Que faisons-nous pour vous ? 36

À propos de cette étude 40



Public cible de l'étude : entreprises manufacturières en Belgique

L'étude d'Agoria a été menée en collaboration avec Howest, UGent Campus Kortrijk et Sirris auprès de 77 entreprises manufacturières belges. Vous en apprendrez davantage sur la composition de l'échantillon au dos de ce livret.

Adopter l'Industrie 4.0 de manière cybersécurisée

La Belgique compte **quelque 5.000 entreprises manufacturières industrielles**. Un peu plus de 60 % d'entre elles ont investi dans leur transformation vers l'industrie 4.0. Les entreprises manufacturières investissent de plus en plus dans les technologies opérationnelles (OT) intelligentes, les machines et robots connectés afin d'améliorer leurs processus de production, mais les cybercriminels montrent un intérêt croissant pour cet internet industriel des objets (IIoT).

Dans une étude internationale réalisée par Fortinet, 58 % des grandes entreprises industrielles indiquent avoir été confrontées à une **brèche de sécurité dans leurs systèmes OT** au cours de l'année écoulée. Où en est la cybersécurité des entreprises manufacturières en Belgique ? Pour le savoir, nous avons mené une étude auprès de 77 entreprises manufacturières belges à la fin de l'année 2020. Nous avons été quelque peu choqués de constater que **30 % des composants matériels critiques et des systèmes d'exploitation associés avaient plus de dix ans**. De plus, les entreprises n'effectuent que rarement des mises à jour. Tout cela laisse l'environnement de production à la merci des cybercriminels. Lorsque les choses tournent mal, seul un répondant sur quatre dispose d'un **bon plan de contingence couvrant à la fois l'environnement IT et OT**.

Isoler l'environnement de production du monde extérieur n'est pas la solution. Un **peloton de tête** formé de 10 % des entreprises interrogées s'est clairement détaché dans notre étude. Ces entreprises montrent l'exemple. Nos experts ont formulé dix recommandations, entre autres sur la base de ces éléments, qui vous aideront à adopter l'Industrie 4.0 de manière cybersécurisée !

Danny Goderis
Chief Digital Officer
Agoria

Kurt Callewaert
Responsable de la recherche
en cybersécurité, Howest

Herman Derache
Managing Director
Sirris


1
1
0
1
1
0
1

Pourquoi la sécurité industrielle est-elle nécessaire dans l'industrie manufacturière ?

L'industrie manufacturière est très présente en Belgique. La transformation digitale de ces entreprises progresse rapidement. L'actuelle pandémie de COVID-19 fait également office d'accélérateur et souligne combien il importe de poursuivre la digitalisation des processus de production et organisationnels.

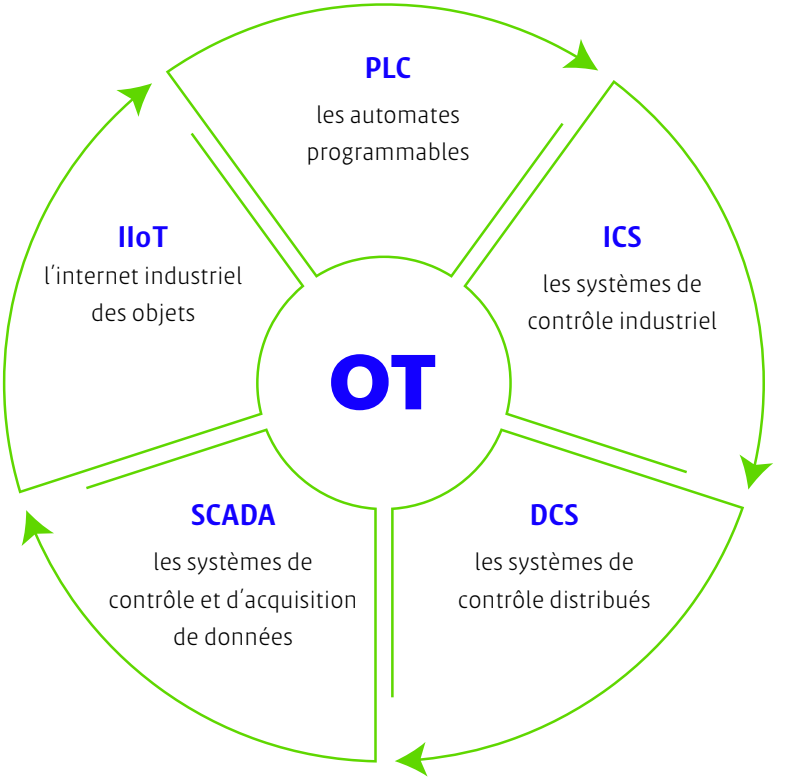
Avec son initiative « The Great Reset », le Forum Économique Mondial (FEM) recommande aux entreprises qui veulent rester compétitives et survivre d'adopter des **business models digitaux** au cœur de leur activité. La digitalisation ne fera donc que s'accélérer dans les entreprises manufacturières. Aujourd'hui, quelque 60 % des entreprises manufacturières belges ont déjà entamé l'une ou l'autre forme de transformation vers l'Industrie 4.0. En donnant plus rapidement priorité à la transformation digitale, les entreprises instaureront des **business models plus intelligents et plus agiles**, libérés de la pensée traditionnelle en silos et alimentés par les données afin de prendre des décisions en temps réel.

Convergence entre IT et OT

Dans les entreprises manufacturières, les réseaux informatiques (IT) et les réseaux industriels de technologies opérationnelles (OT) fusionnent de plus en plus en raison de la transformation digitale. Cette convergence entre IT et OT se produit depuis un certain temps. Elle est essentielle pour que les systèmes de production répondent de manière flexible et intelligente à la variabilité croissante du marché.

Que sont les technologies opérationnelles (OT) ?

Les technologies opérationnelles (OT) comprennent l'ensemble du matériel et des logiciels qui contrôlent et gèrent les équipements et les processus physiques. Parmi les composants et exemples d'OT les plus connus, citons :



Connectivité accrue, besoin accru de cybersécurité

Une convergence accrue implique également une connectivité accrue entre l'IT et l'OT. Les cybercriminels profitent de cette connectivité pour voler, modifier ou détruire des données. Les cyberattaques touchent toutes les entreprises sans exception. Même les **grandes entreprises de production, plus avancées, se retrouvent paralysées**, subissent des pertes de production et des atteintes à leur réputation, et doivent par conséquent souvent faire face à des frais faramineux.

Risque accru d'attaques sur la chaîne d'approvisionnement

De nombreuses entreprises permettent à leurs collaborateurs internes et à leurs clients externes, mais aussi à leurs freelances et à leurs fournisseurs, d'accéder à leur réseau. Le partage de données via les ordinateurs portables, le cloud et les smartphones facilite et accélère la collaboration. De plus, les entreprises utilisent des solutions logicielles développées par des entreprises externes.

Dans quelle mesure la sécurité de ces sous-traitants, partenaires externes et solutions logicielles est-elle solide ? Les cybercriminels mènent des attaques ciblées sur la chaîne d'approvisionnement d'une entreprise en ciblant ses partenaires externes. Ils utilisent un maillon faible de la chaîne d'approvisionnement pour infiltrer le système d'une autre entreprise de la chaîne. Il peut par exemple s'agir d'un fournisseur mal sécurisé qui a accès au réseau de ses clients, lesquels sont ainsi exposés aux risques.

De nos jours, les cybercriminels parviennent à accéder et rester dans votre réseau sur une durée longue, et sans se faire remarquer. Ils mettent ce temps à profit pour en apprendre beaucoup sur votre entreprise. En particulier s'ils ciblent un gain financier, vous pouvez être assuré que lorsqu'ils lanceront effectivement leur attaque – par exemple, le chiffrement de vos appareils – ils le feront au pire moment pour vous.

Karl Mast
Vice President Global Operations, Atlas Copco Airpower

Vous êtes là avec votre entreprise familiale qui existe depuis 35 ans et qui emploie dix personnes… Vous n'avez plus rien. Plus de documents, plus de back-up, plus de données, plus de comptabilité. Tout est chiffré.

Anonyme
CEO d'une entreprise manufacturière belge

L'appel de Paris pour la confiance et la sécurité dans le cyberespace

L'adoption de modèles opérationnels cyberrésilients sont une condition essentielle pour les entreprises. Il s'agit de l'une des recommandations du FEM dans son rapport « The Great Reset » et cela n'a pas échappé à l'Europe. Après « l'appel de Paris » et « Security in Cyberspace », l'Europe préconise désormais la construction d'un cyberbouclier européen et d'un résolveur DNS européen.

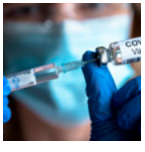
En 2020, **quelques incidents notables** se sont produits chez des fournisseurs de logiciels tels que Microsoft et Solarwinds. Ces incidents pourraient avoir un impact additionnel à long terme sur la sécurité dans les entreprises manufacturières belges et augmenter le risque d'attaques sur la chaîne d'approvisionnement.

Le 24 septembre 2020, des hackers ont volé et publié sur internet le code source de Microsoft Windows XP et Windows Server 2003. Notre étude révèle que de nombreuses entreprises manufacturières belges utilisent toujours et largement ces systèmes d'exploitation dans leurs réseaux industriels. En décembre 2020, le monde a appris que depuis trois ans déjà, des cybercriminels utilisaient le logiciel de monitoring IT de l'entreprise américaine Solarwinds comme cheval de Troie pour s'introduire dans de très nombreuses entreprises, souvent critiques.

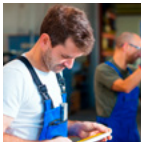
Les hackers ont donc réussi à s'introduire dans la chaîne d'approvisionnement, ce qui leur permet d'attaquer les entreprises qui font partie de cette chaîne. Des attaques ciblant la chaîne d'approvisionnement produisent leurs effets pendant des mois, voire des années. Les criminels utilisent par exemple le code source volé pour identifier et exploiter des vulnérabilités encore inconnues, et pour lesquelles il n'existe donc pas de correctif. Ou ils utilisent les vulnérabilités à fort impact, sans se faire remarquer, pour recueillir des informations sur leurs cibles à grande échelle.

ACTUALITÉS

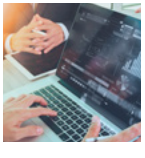
Des usines de Picanol victimes d'une cyberattaque : "Nous ne pouvons plus accéder à notre propre système"
RTBF >



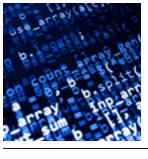
Une cyber-attaque en cours chez l'intégrateur IT belge SPIE ICS
DATANEWS >



1.200 entreprises belges dans le viseur des hackeurs
L'ECHO >



L'Autorité bancaire européenne victime de l'attaque contre la messagerie Microsoft
L'ECHO >



France, Allemagne, Belgique... Les cyber-armées se mettent en ordre de marche
RTBF >

En quoi consiste la cybersécurité pour l'OT ?

La cybersécurité a pour but de garantir **la disponibilité, l'intégrité et la confidentialité** des actifs numériques. Cela se fait par le biais de processus, d'hommes et de technologie, que les entreprises utilisent pour :

1. identifier les risques
2. protéger les actifs
3. détecter les attaques
4. répondre de manière adéquate aux attaques
5. restaurer l'environnement après un incident

Dans sa politique de sécurité, une organisation établit entre autres comment elle réagira de manière prévisible lors de cyberattaques (voir encadré p. 13). La politique de sécurité pour les technologies opérationnelles est très similaire à celle dédiée à la sécurité informatique, l'aspect technologique étant la principale différence. Comme tout système de qualité, une **politique de sécurité** offre la garantie d'une sécurité réussie et durable. Cette politique définit les objectifs, les rôles, les responsabilités et l'approche nécessaires, puis les traduit en processus et directives plus détaillés.

Dans les entreprises qui ont des systèmes IT et OT intégrés, il convient également de combiner la politique de sécurité.

Enquêtes internationales

93%

des entreprises estiment que leur **stratégie de cybersécurité** est insuffisante.

Source : Kaspersky

58%

des entreprises ont été confrontées à un **incident de sécurité** dans leur OT au cours des 12 derniers mois.

Source : Fortinet

61%

des entreprises affirment que des **systèmes OT datés** formaient le principal obstacle à la réduction des cyberrisques.

Source : Ponemon Institute

Les cinq fonctions de la cybersécurité

Identification

Des risques, actifs, menaces, vulnérabilités...

Protection

Antivirus, mises à jour...

Détection

Anomalies dans le trafic, malware, usage abusif...

Réponses

Processus opérationnels et plans de réponse aux incidents

Reprise

À nouveau opérationnel et sans malware

Bron: NIST


2

Principales conclusions de l'étude

Au sein des entreprises manufacturières belges ayant participé à l'étude, la sensibilisation et les connaissances en matière de cybersécurité et en matière de risques liés à la convergence entre IT et OT sont encore insuffisantes. Il n'existe donc que rarement une politique de sécurité OT. Lorsque cette politique est présente, elle n'est généralement pas intégrée dans la politique de sécurité IT ou elle lui est subordonnée.

Dans notre étude, nous avons constaté que l'environnement OT est **très vulnérable**. De plus, beaucoup d'entreprises n'ont pas une bonne visibilité sur les connexions vers et depuis leur environnement OT, ou sur les actifs qui se trouvent dans cet environnement.

D'autre part, le budget alloué à la sécurité OT augmente dans de nombreuses entreprises. Pour les entreprises manufacturières qui forment le peloton de tête de notre étude, la cybersécurité est même une évidence. Toutes ces entreprises ont une **culture de sécurité** et sont familiarisées avec la gestion des risques.

PREMIER CONSTAT

Une politique de cybersécurité intégrant IT et OT fait défaut ou n'est pas alignée par manque de sensibilisation et de connaissances.

Qu'avons-nous constaté ?

1. Il y a trop peu de sensibilisation et de connaissances des cyberrisques dans le domaine de l'OT.
2. Il n'y a généralement pas de politique de sécurité OT.
3. La politique de sécurité OT est rarement intégrée à la politique de sécurité IT et lui est subordonnée.
4. Les équipes OT ne disposent souvent pas des informations de base nécessaires à la mise en œuvre d'une politique de sécurité efficace.

Peu de sensibilisation et de connaissances des cyberrisques

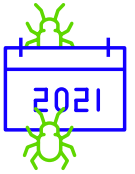
De nombreuses entreprises manufacturières partent du principe que rien ne leur arrivera. Si une cyberattaque se produit malgré tout, elles sont sûres de pouvoir la détecter très rapidement. Néanmoins, les réponses de ces entreprises montrent que la plupart d'entre elles **ne disposent pas des contrôles de cybersécurité de base**. Les connaissances en matière de cybersécurité OT font aussi largement défaut, et ces entreprises organisent en outre peu de formations.

58%

des répondants sont (tout à fait) sûrs d'être en mesure de détecter rapidement une **cyberattaque**.

64%

de ce groupe ont une **politique de sécurité pour l'IT**, mais pas pour l'OT.



50%

des entreprises doutent que leur entreprise soit **victime d'une cyberattaque au cours de l'année à venir**.

Les raisons du manque de sensibilisation aux cyberrisques sont multiples. L'analyse des réponses révèle que les cadres supérieurs **ne comprennent souvent pas suffisamment** la cybersécurité et la considèrent plutôt comme un **coût**. Un des répondants a également indiqué que, contrairement à l'Allemagne, au Royaume-Uni et aux États-Unis, il n'existe en Belgique **pratiquement aucune obligation légale**, pour les entreprises manufacturières, de faire de la cybersécurité une priorité.

Pas de politique structurelle de sécurité OT, et subordonnée à celle de l'IT

La faible sensibilisation aux cyberrisques dans l'OT conduit inévitablement à l'absence d'une **politique de sécurité OT structurée**. Les bonnes politiques de sécurité commencent généralement par une évaluation des risques. La majorité des entreprises manufacturières interrogées n'en avaient jamais réalisé. Une politique de sécurité OT suppose également que quelqu'un soit **responsable** de cette politique, ce qui était rarement le cas.

31%

des répondants n'ont aucune idée de l'âge approximatif des **plus anciens PLC**.

Rendre la cybersécurité visible

Dans ma vie professionnelle, je constate qu'il est difficile de convaincre les gens de quelque chose qui n'est pas visible, comme la cybersécurité. Lorsqu'on déballe par exemple un nouvel appareil, il n'est sûr qu'une fois toutes les mises à jour installées et sa configuration adaptée conformément à vos normes de sécurité. C'est parfois difficile à expliquer, car le danger n'est pas assez tangible. Dans les entreprises plus grandes ou cotées en bourse comme ASSA ABLOY, où je travaille actuellement, cette expertise est présente et, notamment en raison de nos activités, la sécurité fait partie de notre ADN. Il est donc plus facile de traiter la cybersécurité comme une priorité. Néanmoins, nous continuons à rendre la cybersécurité visible via des rapports périodiques assortis de points d'action.

Koen Temmerman

System Engineer ASSA ABLOY Opening Solutions

34%
ont une **politique** qui couvre tant l'IT que l'OT.

55%
des répondants affirment n'utiliser ou n'envisager **aucune norme** relative à la cybersécurité OT.

40%
des entreprises interrogées n'attachent aucune attention à la cybersécurité lors des **achats industriels**.

77%
de ce groupe ne testent jamais la **sécurité OT**.

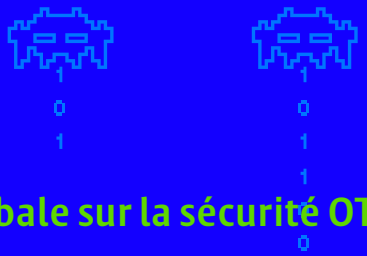
Manque d'informations fondamentales essentielles

Il est impossible de sécuriser efficacement quelque chose si l'on ignore qu'elle existe au sein de notre environnement. Ou si les équipes de terrain ne disposent pas des informations essentielles.

Par le passé, les réseaux OT n'étaient pas connectés au monde extérieur, ce qui laissait croire qu'ils étaient à l'abri des cyberattaques. Seul le besoin de réparation ou de maintenance occasionnelle des pièces incitait les entreprises manufacturières à mieux comprendre leurs réseaux OT. Dans le cadre de notre étude, nous avons creusé cette question en cherchant à savoir si le personnel de terrain avait connaissance d'informations essentielles à la sécurité de l'environnement OT. De nombreuses entreprises ont indiqué ne pas en avoir connaissance.

48%

des répondants affirment ne pas disposer de **connaissances et compétences internes** s'ils devaient être confrontés à une cyberattaque.



Vision globale sur la sécurité OT

Une entreprise confie rarement la responsabilité de l'IT et de l'OT à une seule personne. L'IT est souvent un service ou un centre de services. En revanche, l'OT est un élément essentiel de la production. Mais si les deux systèmes sont interconnectés, il est nécessaire d'avoir une vision globale et un responsable de la sécurité des systèmes IT et OT.

Le directeur IT, le CIO ou le CISO est souvent le candidat évident pour assurer la responsabilité de la sécurité OT. Cela ne signifie pas que l'OT devient tout à coup une partie de l'IT. Des compétences en OT restent essentielles au sein de l'équipe.

Kurt Callewaert

Responsable de la Recherche en Cybersécurité, HOWEST

DEUXIÈME CONSTAT

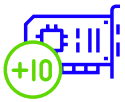
La connectivité, l'âge et l'absence de politique de sécurité rendent l'environnement OT très vulnérable.

Que constatons-nous ?

1. L'environnement OT est très vulnérable sur le plan technologique.
2. Les entreprises manufacturières ne sont généralement pas en mesure de réagir de façon adéquate à un cyberincident OT et de s'en remettre rapidement.

Un environnement vulnérable à cause du long cycle de vie du matériel OT

L'environnement industriel diffère beaucoup d'un environnement IT typique. Les systèmes et les réseaux dans l'industrie contribuent à la production en pilotant et en facilitant les processus physiques. Les entreprises manufacturières belges le font de manière très fiable et efficace. Souvent même pendant des décennies et sans qu'aucune adaptation ne soit nécessaire.



35%

utilisent des **PLC** qui ont dix ans ou plus.

48%

de ce groupe ne procèdent que rarement ou jamais à des **mises à jour**.

32%

des entreprises **scannent leurs réseaux** pour déceler les vulnérabilités.

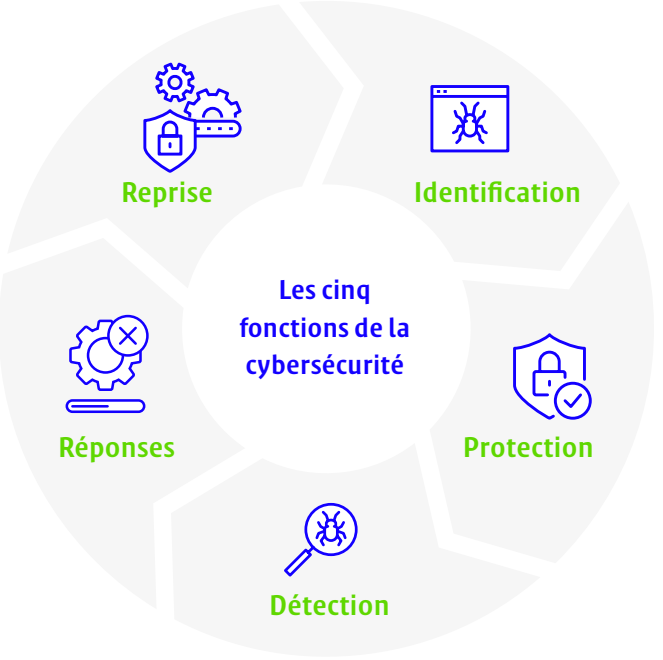
Cependant, ces longs cycles de vie apportent leur lot de défis en termes de cybersécurité.

1. Les composants plus anciens ne contiennent souvent pas de fonctionnalités de sécurité intégrées (security features by design).
2. Les équipements plus récents ne sont pas épargnés par les vulnérabilités et les bugs.

Tout comme l'environnement IT traditionnel, les équipements industriels ont besoin de **mises à jour**. L'étude a également révélé que la plupart des entreprises autorisent l'accès à distance, via internet, aux contrôleurs : la sécurité de cet accès est cruciale pour la sécurité de l'environnement OT.

La sécurité, mise en œuvre et aussitôt oubliée

Les entreprises avec un faible niveau de maturité en matière de cybersécurité considèrent souvent la sécurité comme une mesure à mettre en œuvre 'au début', et n'y prêtent ensuite plus attention. Ces entreprises consacrent uniquement des ressources à **l'identification des risques et la protection** des actifs en fonction. Par contre, la **détection** d'un problème de cybersécurité, la **réaction** appropriée et la **restauration** font généralement défaut dans leur approche. Dans notre étude, nous avons constaté que cette approche se vérifie auprès de nombre d'entreprises manufacturières interrogées.



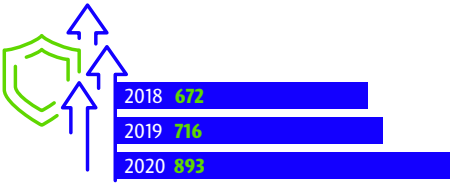
Quel est le système d'exploitation le plus ancien qu'utilisent encore les entreprises manufacturières belges dans la production ?

MS-DOS	3%
Windows 2000	9%
Windows XP	13%
Windows CE	6%
Windows 7	27%
Windows 8	3%
Windows 10	27%

Source : Agoria, « La sécurité industrielle dans l'industrie manufacturière »

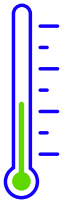
Enquêtes internationales

Le nombre de vulnérabilités détectées dans les équipements OT ne cesse d'augmenter dans le monde



71% des répondants ont une connexion réseau vulnérable aux attaques.

Score de criticité selon le Common Vulnerability Scoring System (CVSS)



48% élevé

22% critique

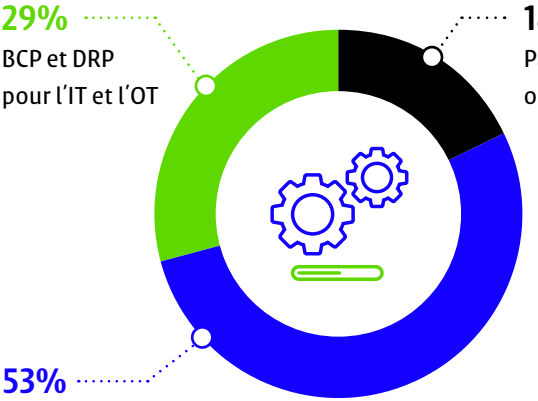
Source : Claroty

Comment aborder les protocoles vulnérables de manière cybersécurisée ?

Dans le réseau de production, les entreprises manufacturières utilisent principalement des protocoles industriels spécifiquement conçus pour l'échange de données (en temps réel). Ces protocoles sont souvent délibérément très ouverts afin de favoriser les intégrations et manquent donc de fonctions de sécurité comme le chiffrement et l'authentification. Ces protocoles très vulnérables conviennent uniquement dans un environnement contrôlé et correctement isolé du reste des réseaux (segmentation).

Combien d'entreprises disposent d'un plan de réponse aux incidents (RI) ?

Combien d'entreprises disposent d'un plan de continuité (BCP) ou d'un plan de reprise d'activité (DRP) ?



38%
ne s'estiment pas en mesure de détecter une **cyberattaque**.

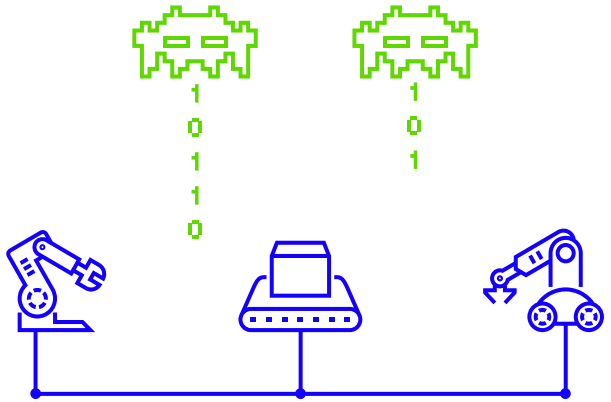
45%
ne restent pas au courant des risques de sécurité via les **recommandations** des équipementiers.

66%
n'utilisent pas ou n'envisagent pas **d'utiliser de normes de l'industrie** relatives à la cybersécurité.

TROISIÈME CONSTAT

10 % des entreprises montrent l'exemple

Un peloton de tête s'est nettement dégagé parmi les entreprises manufacturières interrogées. Qu'est-ce que ces entreprises font de mieux ? Qu'ont-elles en commun ?



Les entreprises manufacturières du peloton de tête :

1. ont une politique de **sécurité pour l'IT et l'OT**
2. **testent régulièrement** leur sécurité
3. **sensibilisent à la sécurité** en organisant des activités au moins une fois par an
4. mettent régulièrement leurs systèmes **à jour**
5. attachent de **l'attention à la cybersécurité** lors de l'acquisition d'équipements industriels
6. pratiquent une forme minimale de **segmentation**
7. disposent en **interne d'une expertise minimale en cybersécurité**, sur laquelle elles peuvent compter en cas de cyberattaque

Qu'avons-nous encore remarqué dans ce peloton de tête ?

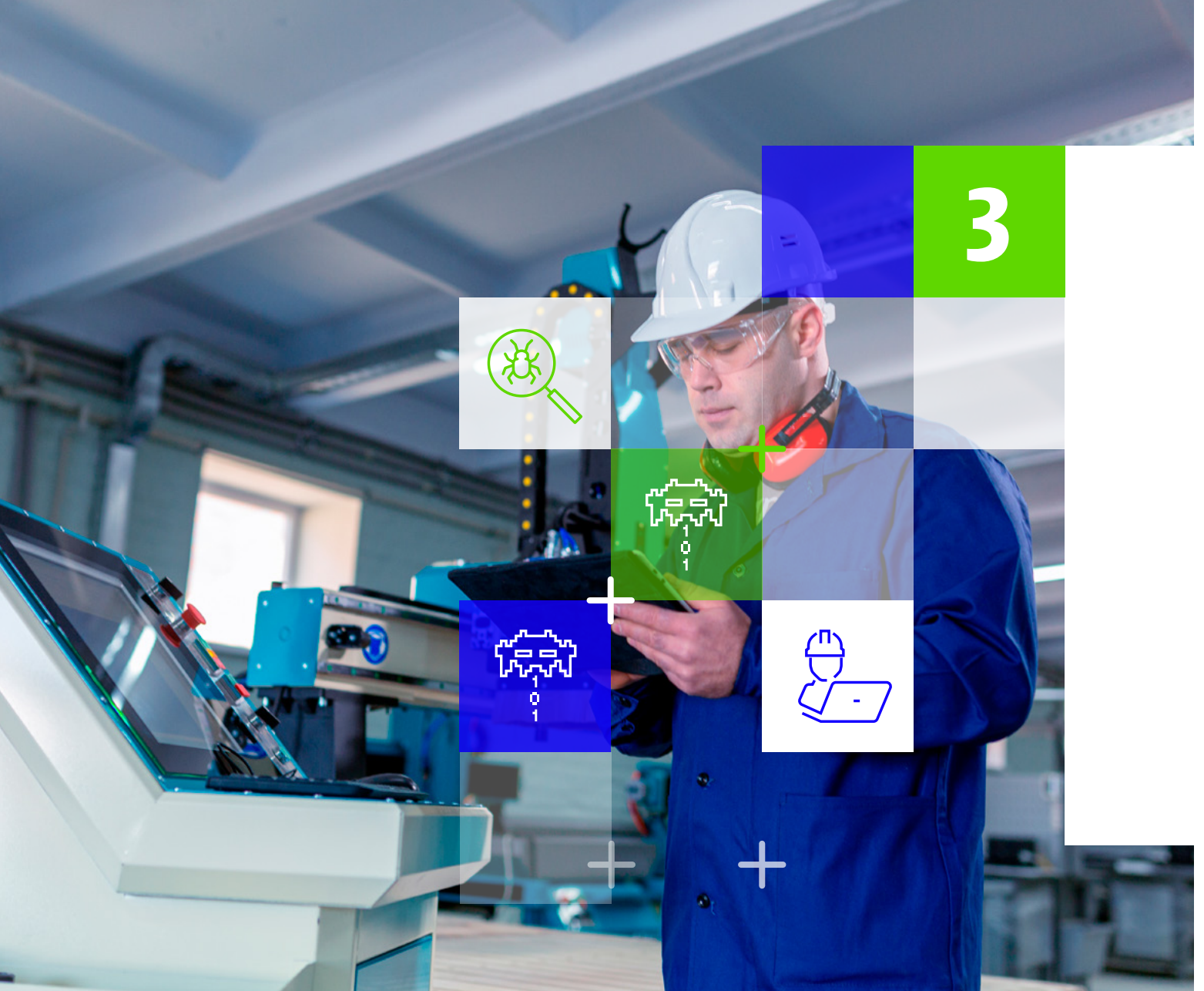
- La moitié de ce groupe d'entreprises fait partie d'un **groupe international** dont le siège se trouve à l'étranger.
- La plupart des entreprises ont **une forte culture de la sécurité**, par exemple parce qu'elles opèrent à l'étranger ou que la sécurité fait partie de leur activité.
- Le peloton de tête se compose d'un mélange de petites et de grandes entreprises. **La taille de l'entreprise n'a donc aucune influence sur la capacité** ou non de mettre en place une bonne politique de sécurité.
- En revanche, les entreprises moins bien classées sont nettement plus petites. En moyenne, **les petites entreprises** manufacturières se positionnent **moins bien** en termes de cybersécurité.
- Le **monitoring des données** sur le réseau industriel et entre l'IT et l'OT est un axe d'amélioration pour presque toutes les entreprises, y compris celles du peloton de tête.

Une culture de « protection ouverte »

Une branche importante d'e-BO est active dans les réseaux offshores. Nous ne faisons aucun compromis en termes de protection ou de sécurité physique de nos collaborateurs ! Alors pourquoi devrions-nous faire des compromis en termes de sécurité industrielle ou de cybersécurité ? Cela a un impact sur toute l'entreprise. Nous avons une culture de « protection ouverte » à partir de laquelle nous établissons formellement le lien avec la cybersécurité industrielle. Et cette culture est importante. Il doit par exemple être possible pour tout le monde, quelle que soit la hiérarchie dans l'entreprise, d'oser signaler quelque chose.

Christophe Dhaene

CEO, e-BO Enterprises.


3

10 RECOMMANDATIONS

Agir dans votre entreprise

Plan de reprise directeur pour l'OT

Réfléchissez ouvertement à la possibilité de mettre en place un plan de reprise directeur uniquement pour votre OT, en supposant que votre IT soit hors service. Dans quel délai pouvez-vous reprendre la production sans IT ? Et pour combien de temps ? Il est facile de dire que plus rien ne fonctionne si l'IT est hors service, mais osez y réfléchir. Par ailleurs, il est important que vous soyez entraîné à exécuter ce plan afin de limiter les risques.

Karl Mast
Vice President Global Operations, Atlas Copco Airpower

10 RECOMMANDATIONS

Agir dans votre entreprise

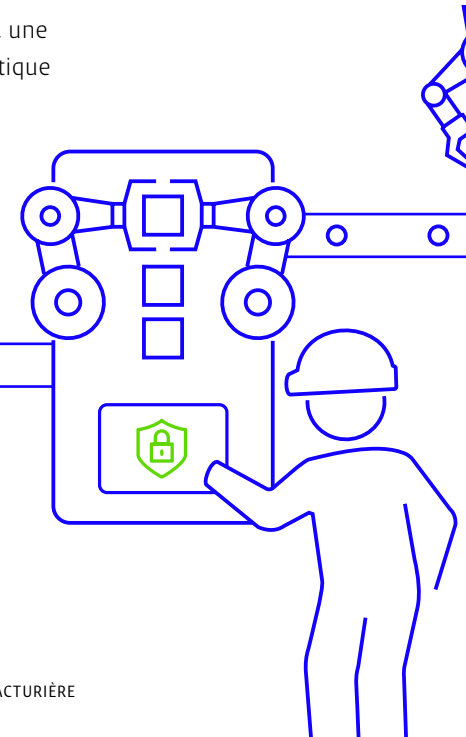
Il n'existe pas de remède miracle pour la cybersécurité industrielle. Chaque entreprise a une infrastructure et un profil de risque différents. De nombreuses recommandations s'appliquent toutefois à une grande majorité d'entreprises.

Mettez en place, du haut vers le bas, une **culture de sécurité** positive et didactique touchant à la sécurité (safety), la cybersécurité et la continuité des activités, de façon systémique et sur base des risques effectifs.

1

2

Augmentez et centralisez la **visibilité** sur tous les actifs à protéger en utilisant les méthodes de gestion des actifs et les techniques de scanning.

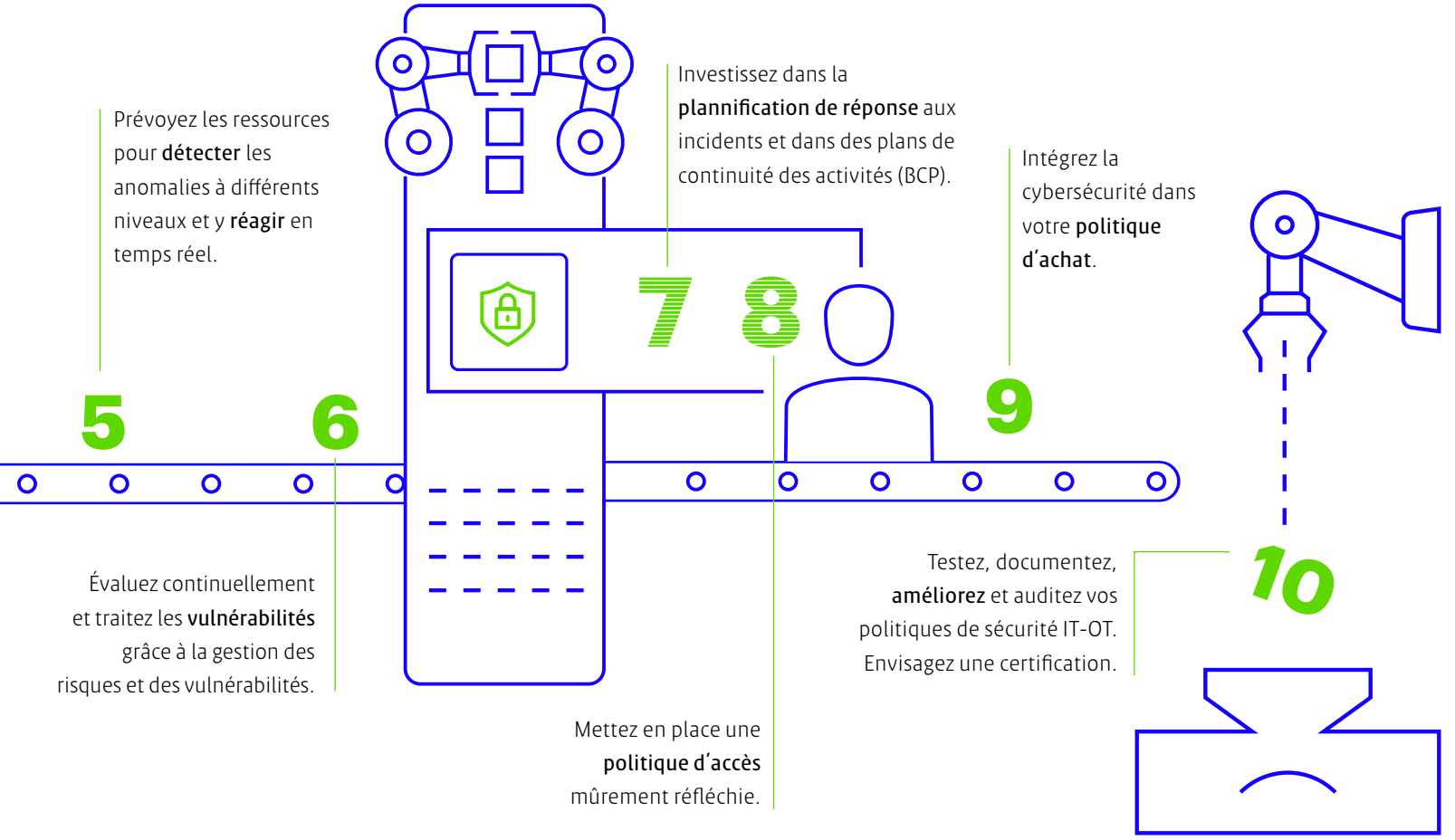


3

Établissez une **politique intégrée** de cybersécurité fondée sur l'évaluation et la gestion formelle des risques pour l'IT et l'OT.

Mettez en place la **ségrégation des réseaux**.

4


Prévoyez les ressources pour **détecter** les anomalies à différents niveaux et y **réagir** en temps réel.
5
Évaluez continuellement et traitez les **vulnérabilités** grâce à la gestion des risques et des vulnérabilités.
6
Investissez dans la **plannification de réponse** aux incidents et dans des plans de continuité des activités (BCP).
7
Mettez en place une **politique d'accès** mûrement réfléchie.
8
Intégrez la cybersécurité dans votre **politique d'achat**.
9
Testez, documentez, **améliorez** et auditez vos politiques de sécurité IT-OT. Envisagez une certification.
10


4
1
0
1

Recommandations pour les pouvoirs publics

Les pouvoirs publics peuvent également soutenir les entreprises en matière de cybersécurité. Comment peuvent-ils y contribuer activement ? Nous avons formulé cinq recommandations à cet effet.

1. Soutenez l'**industrie belge de la cybersécurité** dans son rôle de fournisseur majeur de connaissances et de services pour les pouvoirs publics et les entreprises.

2. Veillez à ce que la cybersécurité fasse partie intégrante et transversale de **toutes les formations d'entreprise**.

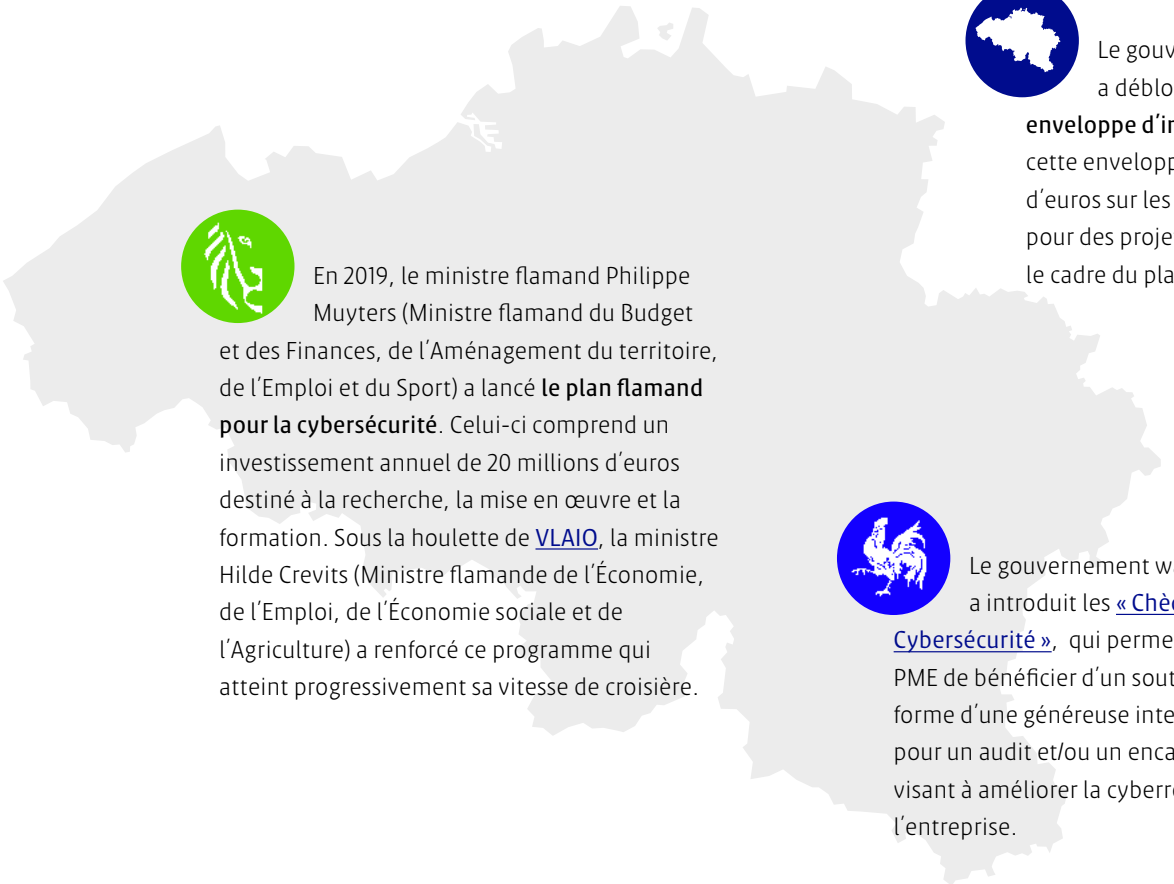
3. Valorisez encore plus la **valeur ajoutée du Center for Cybersecurity Belgium** (CCB), de sorte qu'il puisse mieux mettre ses connaissances internationales à la disposition des entreprises, afin de créer un effet de levier encore plus fort vis-à-vis du monde de l'entreprise.

4. Stimulez la **collaboration entre le monde de l'entreprise, les pouvoirs publics et le monde universitaire** selon le modèle d'innovation « à triple hélice », afin que les connaissances, le talent et les spin-offs atteignent plus facilement l'industrie.

5. Renforcez la cybersécurité et intégrez-la comme une **pierre angulaire de la politique industrielle régionale** avec des ressources appropriées, suffisantes et adéquates, ainsi qu'une stratégie.

Étapes dans la bonne direction

Les pouvoirs publics régionaux et fédéraux ont déjà pris certaines initiatives pour augmenter les ressources destinées aux programmes de cybersécurité. Quelques exemples :



En 2019, le ministre flamand Philippe Muyters (Ministre flamand du Budget et des Finances, de l'Aménagement du territoire, de l'Emploi et du Sport) a lancé **le plan flamand pour la cybersécurité**. Celui-ci comprend un investissement annuel de 20 millions d'euros destiné à la recherche, la mise en œuvre et la formation. Sous la houlette de VLAIO, la ministre Hilde Crevits (Ministre flamande de l'Économie, de l'Emploi, de l'Économie sociale et de l'Agriculture) a renforcé ce programme qui atteint progressivement sa vitesse de croisière.

Le gouvernement fédéral a débloqué une importante **enveloppe d'investissement**. Il utilisera cette enveloppe d'environ 78,8 millions d'euros sur les cinq prochaines années pour des projets de cybersécurité dans le cadre du plan de relance européen.

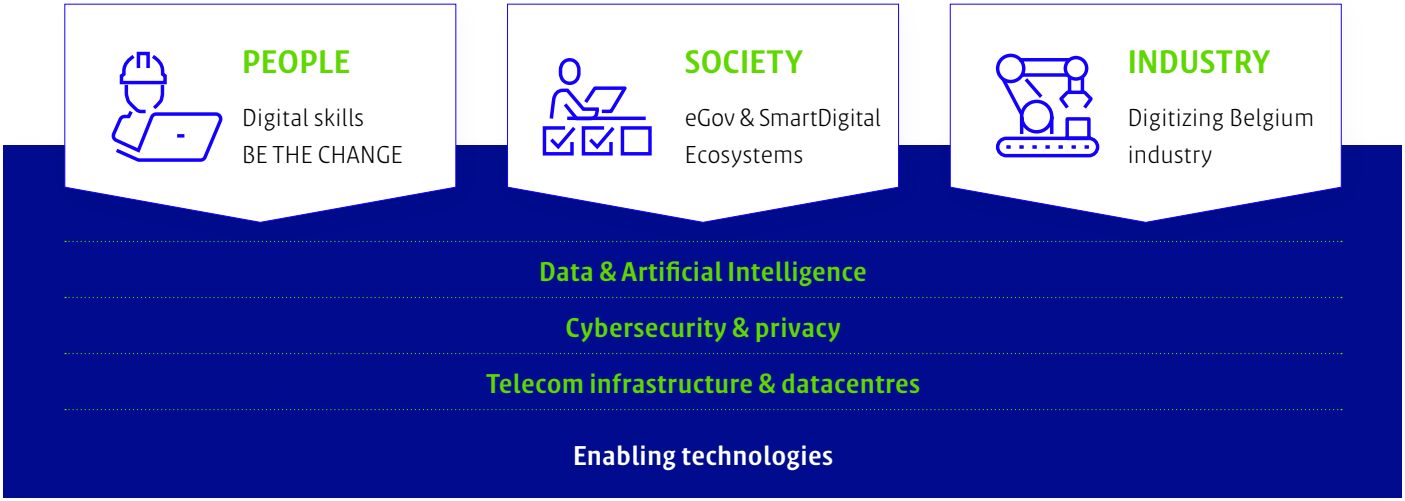
Le gouvernement wallon a introduit les « Chèques Cybersécurité », qui permettent aux PME de bénéficier d'un soutien, sous la forme d'une généreuse intervention, pour un audit et/ou un encadrement visant à améliorer la cyberrésilience de l'entreprise.


5
1
0
1
1
0
1

Que faisons-nous pour vous ?

Agoria, Sirris et Howest soutiennent les entreprises (manufacturières) de diverses manières pour renforcer la cybersécurité dans votre organisation. Nous travaillons toujours sur mesure. Ensemble, nous offrons un très large choix de services allant de l'information, de la sensibilisation, du partage de connaissances et du lobbying à la formation et aux conseils. Voici quelques-unes de nos initiatives.

La cybersécurité est l'un des éléments fondamentaux de notre stratégie :



1 Cyber made in Belgium

Agoria réunit plus de 50 entreprises affiliées actives dans la cybersécurité. Nous sommes de plus en plus considérés comme la voix du « Cyber made in Belgium » et comme une force motrice dans l'écosystème belge. Nous participons entre autre activement aux activités de la **Cybersecurity Coalition (CSC)**, sont proches du **Cyber Centre for Belgium (CCB)** et travaillons en étroite collaboration avec le monde universitaire, comme **Howest**, la **KU Leuven** et le **Centre de l'Agence Spatiale Européenne (ESA) à Redu**.

3 DigiConnect

La plateforme DigiConnect d'Agoria vous met gratuitement et rapidement en contact avec les **partenaires adéquats pour vos projets et écosystèmes digitaux**. Digiconnect fait partie de Digicoach, un vaste programme d'outils, de connaissances et de services pour vous guider de manière optimale dans votre transformation digitale. Nous accordons bien sûr une grande attention à la sécurité.

2 #IndustriePartnerschap mise en place dans le cadre du contrat VLAIO Ambitieus Ondernemen

Agoria et Sirris sont les initiateurs de l'Industrie Partnerschap qui a été mis en place dans le cadre du contrat VLAIO « Ambitieus Ondernemen ». Avec 21 organisations issues de différents secteurs, nos experts proposent une série de services individuels et collectifs (voir p. 35). Nous augmentons ainsi le niveau de connaissance de l'industrie flamande en matière de transformation et d'organisation digitales. Nous améliorons notamment la sensibilisation aux opportunités et aux risques liés à la cybersécurité et montrons comment les entreprises peuvent créer de la valeur avec des produits intelligents et des services digitaux.

4 Post-graduat en cybersécurité industrielle

Vous êtes un expert IT et vous souhaitez approfondir vos connaissances ? Howest et UGent ont récemment lancé une nouvelle formation et ont créé, depuis cette année académique, le post-graduat en cybersécurité industrielle.

Lisez également notre livre blanc avec des recommandations détaillées pour la cybersécurité OT dans les entreprises manufacturières.

Retrouvez l'offre complète et les calendriers de toutes les activités sur nos sites web : www.agoria.be et www.sirris.be

À propos de cette étude

Dans le cadre du laboratoire d'essai Innovatieve Cyberbeveiligingen voor Industrie 4.0 (Cybersécurités innovantes pour l'industrie 4.0), une initiative de VLAIO, Howest et UGent, en collaboration avec Agoria, ont mené une étude auprès d'entreprises manufacturières belges. Sauf mention contraire, les chiffres de l'étude sont issus d'une enquête téléphonique menée du 10 septembre au 14 décembre 2020. Agoria et Sirris ont ensuite élaboré des conclusions et des recommandations, que nous avons soumises pour validation à Howest, à UGent ainsi qu'à des experts chevronnés en cybersécurité OT. Au cours des mois de février et mars 2021, nous avons recontacté certaines entreprises pour leur poser des questions plus approfondies et connaître leurs réactions à nos conclusions et recommandations. C'est la première fois que nous menons une telle étude auprès d'entreprises manufacturières belges. Nous affinerons nos connaissances dans le futur en réitérant cette étude dans les années à venir. **Vous souhaitez être activement impliqué dans cette étude ? Contactez l'un des auteurs.**

ÉTUDE MENÉE FIN 2020

60 questions sur la politique de sécurité IT et OT

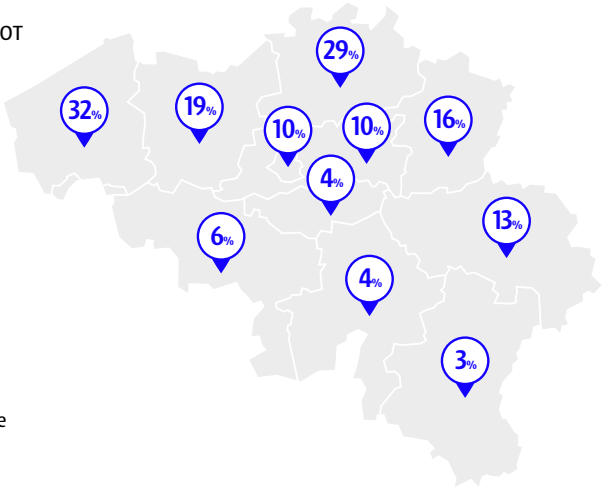
77 entreprises manufacturières belges

SIÈGE SOCIAL

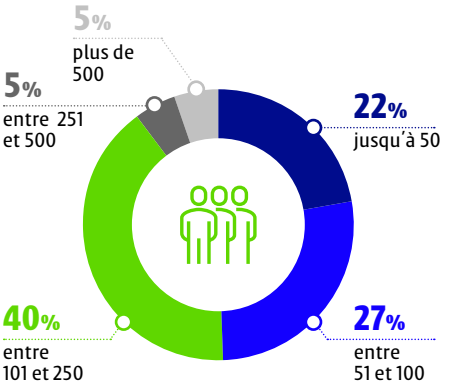
82 % ayant leur siège en Belgique

18 % sont une filiale d'une entreprise étrangère

RÉGION



NOMBRE DE COLLABORATEURS



Auteurs

Patrick Coomans
Agoria en Sirris
+32 477 40 53 09
patrick.coomans@agoria.be

Kurt Callewaert
Howest
+32 473 34 04 65
kurt.callewaert@howest.be

Wim Codenie
Sirris
+32 498 91 94 53
wim.codenie@sirris.be

Yves Schellekens
Agoria
+32 476 98 90 32
yves.schellekens@agoria.be

Avec la contribution de :

Wolker Lemahieu
wolker.lemahieu@agoria.be

Alain Wayenberg
alain.wayenberg@agoria.be

Tijl Atoui
tijl.atoui@howest.be

Johannes Cottyn
johannes.cottyn@ugent.be

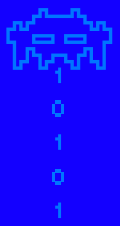
Tijl Deneut
tijl.deneut@howest.be

Hendrik Derre
hendrik.derre@howest.be

Johan Galle
johan.galle@howest.be

Tinus Umans
tinus.umans@ugent.be



À propos d'Agoria

La fédération technologique Agoria ouvre la voie à toutes les entreprises de Belgique que la technologie inspire et qui veulent contribuer au progrès dans le monde grâce au développement ou à la mise en œuvre d'innovations. Ensemble, ces entreprises représentent plus de 310.000 travailleurs. L'organisation regroupe près de 2000 entreprises technologiques, dont 70 % de PME. Agoria compte quelque 200 collaborateurs. Les services et positions d'Agoria portent sur la digitalisation, l'industrie manufacturière de demain, la politique de gestion des talents et la formation, l'évolution des marchés, la réglementation, les infrastructures, le climat, l'environnement et l'énergie. Agoria souhaite mettre en relation tous ceux que la technologie et l'innovation inspirent, accroître le succès des entreprises et façonner un avenir durable.

Pour en savoir plus,
rendez-vous sur www.agoria.be

À propos de Howest et UGent

La Hogeschool West-Vlaanderen (Howest) compte 8.500 étudiants et plus de 800 collaborateurs. Howest propose aux étudiants un éventail diversifié de 24 formations de bachelier et 13 formations de graduat. Howest est la plus grande école supérieure de Flandre dans le domaine de la technologie informatique, de la cybersécurité, des nouveaux médias et des arts & loisirs digitaux (Gaming et 3D). L'UGent est l'une des plus grandes universités de Belgique. Les 11 facultés proposent plus de 200 formations et font de la recherche dans diverses disciplines scientifiques. Le campus de Courtrai propose 3 formations uniques : automatisation des machines et de la production, technologie des bioprocessus circulaires et conception industrielle.

Pour en savoir plus, rendez-vous sur
www.ugent.be et www.howest.be

À propos de Sirris

Fondée en 1949 par Agoria, Sirris est le centre collectif de l'industrie technologique belge. Chaque année, les 150 experts de Sirris aident environ 1.300 entreprises à faire le bon choix technologique et à mener à bien leurs projets d'innovation. En conjuguant experts, infrastructures high-tech exclusives réparties sur tout le territoire et vaste réseau de partenaires (inter)nationaux, Sirris occupe une position privilégiée dans le domaine de l'innovation technologique industrielle en Belgique. Les quelque 2.400 entreprises belges membres de Sirris ont accès à un bouquet étoffé de services et de connaissances.

Pour en savoir plus,
rendez-vous sur www.sirris.be

.AGORIA howest UNIVERSITEIT GENT sirris driving industry by technology