LIÈGE | NOUVELLE DIRECTIVE EUROPÉENNE D'APPLICATION DÈS OCTOBRE

Cybersécurité : 66% des entreprises sondées désarmées face aux mesures à prendre

Dans un contexte où la sécurité numérique est devenue un enjeu majeur, la nouvelle directive NIS-2 représente un tournant décisif. Elle a pour objectif de renforcer la cybersécurité au sein de l'UE et sera d'application dans notre pays dès le mois d'octobre. 2 400 entreprises sont concernées en Belgique. D'après le groupe liégeois B2C Engineering, précurseur en matière de Cybersécurité industrielle, 66% des industriels consultés n'ont aucune idée des implications que cela va représenter pour leur entreprise.

A Liège, en Belgique et à l'échelle de l'Europe, le constat est le même : de nombreuses entreprises sont aujourd'hui confrontées à des infrastructures obsolètes, des systèmes marqués par des vulnérabilités critiques. Cette urgence est d'autant plus accentuée avec l'émergence de l'industrie 4.0 qui repose, entre autres, sur l'interconnexion et la numérisation complète des processus industriels. Dans ce contexte de digitalisation croissante, des équipements initialement non conçus pour un usage externe se retrouvent exposés sur internet, augmentant le risque de pertes de contrôle.

La cybersécurité devient donc une priorité non seulement pour la protection des systèmes, et outils de production, mais aussi pour la sauvegarde des données sensibles des entreprises, de leurs employés et de leurs clients. Face au risque accru de fuites de données, les entreprises doivent se conformer à des normes rigoureuses, pour prévenir toute violation susceptible de les exposer à des risques juridiques et financiers majeurs.

Une réponse à la cybercriminalité pour 2.400 entreprises belges

« Les cybercriminels agissent pour diverses raisons », explique Benjamin Beaurang, administrateur de B2C Engineering implanté à Fexhe-le-Haut-Clocher en région liégeoise mais aussi en France, au Luxembourg et en Suisse. *« L'appât du gain est l'une des principales motivations, notamment par le biais des rançons exigées en échange de la restitution des données volées ou du rétablissement des systèmes informatiques. Pour d'autres, le piratage représente un défi technique et une source de divertissement, une manière de tester et de démontrer leurs compétences. »*

Gregory Putman, Sales Specialist Industrial Networks & Security de SIEMENS, d'ajouter : *« D'autres cybercriminels sont engagés par des entreprises pour saboter la concurrence. Et puis, il existe des motivations terroristes, où les cyberattaques visent à causer des dommages significatifs, comme la modification de la structure de l'eau pour nuire à la population. »*

La nouvelle directive européenne NIS-2 sur la Sécurité des Réseaux et des Systèmes d'Information doit être transposée dans la législation nationale de chaque pays membre de l'Union Européenne avant le 17 octobre 2024. Celle-ci a déjà été votée en Belgique en avril 2024. Elle se veut être une réponse efficace face à la cybercriminalité bien présente en Europe.

La NIS-2 ne se contente pas de poursuivre les efforts initiés précédemment par la NIS-1, à savoir : l'obligation pour les autorités nationales de consacrer davantage de capacité à la cybersécurité, le renforcement de la coopération européenne entre les autorités de cybersécurité ainsi que l'augmentation du nombre d'opérateurs importants et de secteurs critiques de notre société.

Elle innove en promouvant la mise en place de formations, en consolidant les accès et en imposant une responsabilité accrue aux directions d'entreprises. De plus, les sociétés devront adopter des mesures techniques et organisationnelles proportionnées pour gérer les risques.

Quelles sanctions en cas de non application de cette directive par un industriel ? Tout d'abord un avertissement lui sera transmis, et ensuite, si aucune évolution n'est constatée, l'amende peut s'élever jusqu'à 10 millions d'euros ou 2% du chiffre d'affaires total annuel pour les entités essentielles et jusqu'à 7 millions pour les entités importantes. De plus, si une attaque a lieu et que l'entreprise n'est pas conforme à la NIS-2, la responsabilité du ou des dirigeant(s) sera engagée.

Nouveauté : obligation de déclarer chaque cyberattaque

La nouvelle directive s'appliquera désormais à un éventail plus large de sociétés. Elle couvrira ainsi presque toutes les moyennes et grandes entreprises. En Belgique, plus de 2 400 entreprises sont concernées par la mise en application de la directive NIS-2.

« Actuellement, nombreux sont les industriels qui hésitent à déclarer les cyberattaques par crainte de perdre la confiance de leurs clients. Cette réticence les pousse souvent à payer les rançons exigées par les cybercriminels, afin d'éviter une mauvaise publicité et préserver leur image », ajoute Charles Costa, administrateur chez B2C Engineering et référent Cybersécurité.

Avec l'entrée en vigueur de la directive NIS-2 en octobre, les industriels seront désormais obligés de déclarer toute cyberattaque subie. Ce sera la première fois qu'une loi imposera aux entreprises d'informer les autorités de ces incidents, renforçant ainsi la transparence et la sécurité du secteur.

Tous incidents significatifs devront être notifiés en 3 étapes :

- Une alerte précoce dans les 24 heures (si l'incident est susceptible de faire tache d'huile)
- Une notification d'incident complète dans les 72 heures (comme pour le RGPD)
- Un rapport final dans le mois

66% des industriels dans le flou absolu face à la nouvelle directive

Si les équipes de B2C Engineering se positionnent en précurseur dans l'accompagnement des industriels vers la conformité de cette réglementation, le groupe liégeois n'a pas attendu la nouvelle directive européenne pour faire de la cybersécurité une priorité.

B2C Engineering accompagne chaque année une bonne quinzaine d'entreprises en matière de cybersécurité. Soit parce qu'elles ont fait l'objet d'une cyberattaque, soit pour sécuriser leurs données parfois hautement confidentielles comme dans le secteur du pharma. *« Nos clients expriment un besoin croissant en cybersécurité industrielle, un domaine trop longtemps délaissé »*, souligne Charles Costa. «*Nous sommes donc sollicités pour élaborer des stratégies de conformité sur mesure, offrant des solutions avant-gardistes. Mais notre ambition est d'intervenir en amont, prévenant les cyberattaques plutôt que de ne réagir qu'à leurs conséquences. Heureusement, nos clients ne se limitent pas à des situations de crise !* »

En mai dernier, B2C organisait ses Solutions Days 2024, un triple événement organisé à Namur, Valenciennes et Lyon. Un événement réservé aux industriels. Parmi le panel d'intervenants et/ou d'invités, de grands noms comme Arcelormittal, Groupe Spadel, Orange, Siemens, Aveva, Micromedia, Wallix, KEB, Valfrance Semences, BT4DM, UCB, Auvesy, Sonaca, Prayon, SWDE ou GSK.

L'occasion de faire le point sur les dernières innovations technologiques et d'interroger les entreprises sur la nouvelle réglementation européenne. Question posée aux 80 participants : *« À quel point êtes-vous au courant de l'application de la directive NIS-2 en octobre 2024 ? »*. Réponse : 66% des industriels sondés avouent n'en avoir aucune idée ou une connaissance vague du sujet. Un nombre alarmant sachant que la nouvelle directive doit être d'application très prochainement.

« Les cyberattaques, ça n'arrive pas qu'aux autres », met en garde Benjamin Beaurang, administrateur de B2C Group. *« Certains de nos clients ont failli mettre la clé sous le paillasson après avoir perdu toutes leurs sauvegardes. D'autres entreprises se sont retrouvées à l'arrêt durant plusieurs mois ou ont fait l'objet d'une demande de rançon. Heureusement, nos ingénieurs ont pu faire des petits miracles… Mais avec l'adoption de la directive européenne, toutes les entreprises vont désormais être appelées à renforcer leurs mesures de sécurité. »*

Chez B2C, les ingénieurs ont pour mission le design et la sécurisation des réseaux industriels via des pare-feu ou la mise à jour des infrastructures existantes pour éliminer les vulnérabilités. Pour ce faire, ils intègrent des solutions sur-mesure en s'appuyant sur les produits de partenaires tels que Siemens, Stormshield, Auvesy, Wallix, Darktrace. Objectif : répondre aux exigences immédiates, mais également d'envisager les évolutions futures, garantissant ainsi une protection durable et efficace.

B2C Engineering accompagne également les industriels pour la mise en conformité réglementaire :
1. Réalisant l'audit complet en la matière
2. Proposant un plan Multi-Annuel
3. Mettant en place les mesures de mises en conformité y compris les policies et procédures.
4. Restructurant le réseau ainsi que les équipements qui le composent
5. Installant un système de monitoring du réseau.

B2C en 7 chiffres clés :

B2C se distingue par deux entités complémentaires, chacune spécialisée pour proposer un panel de services complets dans le secteur industriel, tant sur le territoire belge qu'à l'international. B2C Engineering se concentre sur le conseil ainsi que l'intégration de solutions innovantes et pérennes. B2C Consulting, quant à elle, rassemble des consultants qualifiés dont la mission est d'accompagner les entreprises dans la concrétisation de leurs projets industriels.

2 Entreprises : B2C Engineering & B2C Consulting

3 Fondateurs : Benjamin Beaurang, Jean-Christophe Bulon & Charles Costa

5 Agences dans 4 pays : Belgique, France (Lyon et Valenciennes), Luxembourg et Suisse

10 Ans d'expertise

70 Collaborateurs au sein du Groupe

300 Projets par an en moyenne

12 000 000 € Chiffre d'affaires annuel

Découvrez le film d'entreprise en vidéo :
https://vimeo.com/921976342/5d062e35dc

Des solutions en cybersécurité :
https://vimeo.com/946128031/8c61f2515c

D'autres vidéos sur la chaine YouTube :
https://www.youtube.com/@b2cengineering/videos

CONTACTS PRESSE/MÉDIAS

François VANHAETSDAELE — Directeur commercial — fvan@b2c-engineering.com — +32 470 62 14 86

Charles COSTA — Administrateur — ccos@b2c-group.com — +32 474 23 49 80

PHOTOS

Photos libres de droits d'auteur :
https://we.tl/t-eDXJepACbZ

CASE STUDY

Refonte du réseau OT d'une usine chimique



Un exemple concret de la démarche de B2C Engineering est le projet d'envergure mené pour un acteur majeur de l'industrie chimique avec des partenaires de renom comme Siemens. Le groupe, grand acteur mondial dans la chimie, est établi en Belgique et partout dans le monde à travers différents sites de production, d'ateliers de fabrication et d'antennes commerciales.

Le projet

Le projet s'inscrit dans un contexte où la cybersécurité industrielle devient une priorité absolue pour les entreprises de tous secteurs confondus. Afin de répondre à ces enjeux, le groupe chimique a d'abord fait réaliser une étude de son réseau via un prestataire externe en cybersécurité IT. B2C Engineering a ensuite été missionné pour challenger le rapport produit par ce prestataire en apportant son expérience OT.

Les attentes

C'est dans ce cadre que B2C a apporté son expertise afin de répondre aux objectifs clairement établis du client :

1. Rendre son réseau OT indépendant du réseau IT pour plus de flexibilité opérationnelle.
2. Répondre aux évolutions technologiques à venir, notamment celles liées à l'industrie 4.0.
3. Se protéger contre d'éventuelles cyberattaques.
4. Gérer le Risk Management pour assurer une continuité des opérations.

Pour atteindre ces objectifs, plusieurs contraintes techniques et normatives étaient à prendre en compte telles que la conformité aux normes IEC-62443 et ISA-99, la connexion sécurisée des PLC et DCS ainsi que le choix du matériel permettant un fonctionnement optimum malgré les distances importantes entre les différentes unités.

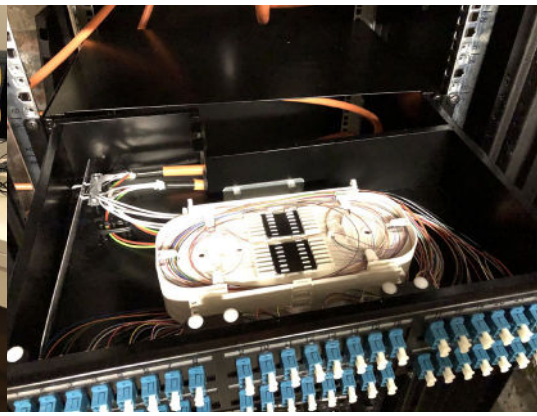
L'étude

B2C Engineering, s'appuyant sur sa maîtrise des normes IEC/ISO11801 et ANSI/ISA62443, a mené une étude détaillée pour ce projet. Cette étude a inclus la rédaction d'un cahier des charges détaillé, le métré des liaisons, la sélection du matériel IT, ainsi que la recommandation de partenaires potentiels pour l'installation sur le site de production.

Pour répondre aux besoins en cybersécurité, B2C a opté pour les produits Siemens. Le client ayant exprimé un besoin spécifique en points d'accès pour le nouveau réseau OT, cela a conduit à l'installation de :

- 14 baies informatiques
- 13 km de fibre optique
- 30 firewalls
- 42 switchs Siemens





« Depuis 7 ans, B2C utilise nos différents produits de manière exponentielle, explique Gregory Putman chez SIEMENS. *C'était donc pour nous une évidence de collaborer avec eux. Notre partenariat a d'ailleurs été renforcé par le projet. Ce que nous avons particulièrement apprécié dans cette collaboration, c'est la polyvalence de B2C, qui excelle dans le domaine de l'automatisation et de la communication industrielle. »*

Depuis la commande du matériel jusqu'à la formation du personnel du client, le projet a duré 12 mois.

Les bénéfices

Les avantages en termes de cybersécurité pour le client sont significatifs. Tout d'abord, il a acquis une indépendance totale dans la gestion de son réseau OT par rapport au réseau IT, avec une capacité d'extension importante, tant au niveau matériel (HW) que logiciel (SW). Le client bénéficie désormais d'un réseau OT entièrement préparé pour l'industrie 4.0, équipé de matériel de pointe, à jour et reconnu pour sa fiabilité, notamment avec la certification ANSSI des solutions. De plus, grâce à la formation sur ces équipements, le personnel du client a développé une solide maîtrise des compétences en cybersécurité. Actuellement, des audits sont en cours sur les autres sites du client pour étendre cette protection à l'ensemble de l'entreprise.

FACILE À LIRE

Ce qu'il faut retenir

5 objectifs de la Directive NIS-2 :

1. **Élargissement de la portée de la législation** pour inclure non seulement les infrastructures critiques traditionnelles, mais aussi d'autres secteurs importants comme les services numériques, les services de communication, les fournisseurs de services cloud, et les infrastructures numériques.
2. **Renforcement des obligations** en imposant des exigences plus strictes en matière de sécurité et de notification des incidents en mettant en œuvre des mesures techniques et organisationnelles adaptées pour gérer les risques liés à la cybersécurité.
3. **Coordination accrue pour renforcer la coopération** entre les États membres de l'UE en partageant les informations sur les menaces et les incidents, dans le respect des règles de confidentialité.
4. **Intensification de la supervision** pour garantir la conformité des entreprises avec la possibilité d'imposer des sanctions significatives en cas de manquement, y compris des amendes lourdes.
5. **Protection des utilisateurs finaux** en exigeant des fournisseurs de services numériques de prendre les mesures nécessaires pour garantir la sécurité de leurs services.

Comment se conformer à la NIS-2 en quelques étapes résumées ?

- **Identification des obligations :** déterminer si l'organisation est concernée et nommer un responsable de la conformité.
- **Évaluation des risques :** réaliser une analyse des risques et cartographier les actifs critiques.
- **Mise en place de mesures de sécurité :** déployer des mesures techniques et organisationnelles ainsi que sécuriser la chaîne d'approvisionnement.
- **Gestion des incidents :** établir des procédures de gestion des incidents et préparer les notifications.
- **Formation et sensibilisation :** former les dirigeants et le personnel tout en promouvant une culture de la sécurité.
- **Surveillance continue et amélioration :** effectuer des audits réguliers et mettre à jour les politiques de sécurité.
- **Collaboration avec les autorités :** établir une coopération avec les autorités et se préparer aux inspections.

En suivant ces procédures, une organisation peut progresser vers la conformité avec la directive NIS-2, réduisant ainsi ses risques de cybersécurité et améliorant sa résilience face aux menaces numériques.