Cyberrisques et cybercriminalité

Comment les entreprises doivent-elles tirer parti de NIS 2 et de l'IA pour renforcer leur sécurité ?

C'est un lieu commun de dire que la transformation numérique s'accompagne d'une augmentation exponentielle des cybermenaces. Les attaques informatiques sont devenues plus fréquentes, sophistiquées et dévastatrices. Selon l'ANSSI, 69 % des cyberattaques en 2023 visaient des entreprises, et 60% des PME européennes victimes d'une cyberattaque font faillite dans les 18 mois qui suivent.

Face à ce constat alarmant et à la montée de l'IA, comment renforcer la résilience des Systèmes d'Information et protéger nos données sensibles ? Quels cadres réglementaires imposer pour réguler le secteur ?

NIS 2 : renforcer le cadre réglementaire, mais à quel prix ?

Adoptée par l'Union européenne, la directive NIS 2 vise à harmoniser et à renforcer la cybersécurité au sein des États membres. Elle étend le champ d'application de la première directive NIS en incluant un plus grand nombre de secteurs critiques : la santé, l'énergie, les transports et les services numériques. Les entreprises concernées seront soumises à des obligations plus strictes en matière de gestion des risques cyber. La date limite de transposition en France est fixée au 17 octobre 2024.
À compter de cette date, les entreprises devront mettre en place des mesures techniques et organisationnelles adaptées pour gérer les risques de sécurité. Les organisations sont dorénavant obligées de notifier les incidents significatifs aux autorités compétentes dans des délais courts. Enfin, NIS 2 encourage une coopération renforcée entre secteur public et privé ; entre les États membres et les organisations pour une résilience collective et mieux organisée. La non-conformité peut entraîner des sanctions sévères, comme des amendes pouvant atteindre 10 000 000€ ou 2 % du chiffre d'affaires mondial annuel.

L'IA : entre menace et opportunité pour la cybersécurité

L'IA n'est pas nouvelle en cybersécurité. Dès les années 2010, les entreprises ont intégré des solutions optimisées par IA pour améliorer leur productivité. Par exemple, un rapport souligne une accélération de 55% en moyenne des enquêtes et du triage d'alertes grâce à l'analyse des risques alimentée par l'IA. Par des algorithmes d'apprentissage automatique (machine learning) et d'apprentissage profond (deep learning), les solutions basées sur l'IA offrent différents avantages de détection et de supervision de l'activité informatique en temps réel et ce en continu.

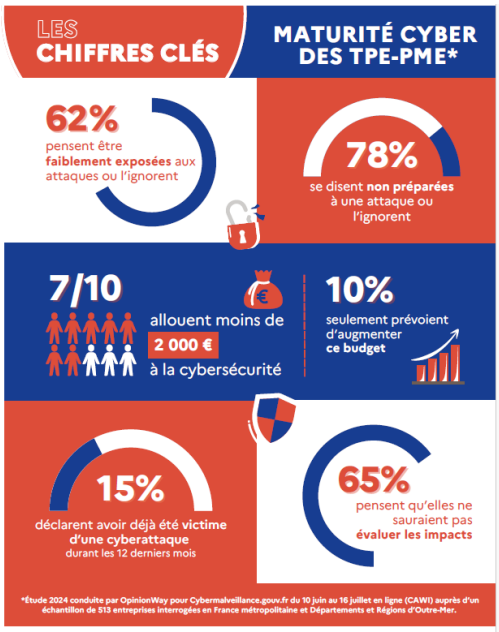
Toutefois, l'Intelligence Artificielle est exploitée par les cybercriminels pour mener des attaques sophistiquées. Dans le cadre de l'hameçonnage (inciter un individu, par un mail ou un SMS frauduleux, à cliquer sur un lien contenant des virus), les hackers peuvent, avec l'aide de Chat GPT, rédiger des e-mails, des SMS sans fautes d'orthographe et de grammaire – jusqu'à lors, l'un des meilleurs moyens pour détecter une tentative d'hameçonnage. L'IA permet également de créer de fausses identités. Par le deepfake notamment. Le 29 janvier 2024, une multinationale à Hong Kong a signalé une perte de 26 millions de dollars suite à une arnaque sophistiquée. Un employé a été dupé lors d'une visioconférence où des deepfakes imitaient ses collègues. Les escrocs ont utilisé l'IA pour créer des avatars convaincants à partir de vidéos YouTube. L'employé a effectué 15 transferts vers 5 comptes bancaires différents sur instruction des faux cadres.

Service de presse
Agence ComCorp
Kelly LEOTARDI
kleotardi@comcorp.fr
+33 7 50 87 76 62
Anne-Claire BERTHOMIEU
acberthomieu@comcorp.fr
+ 33 6 16 53 15 70

Parole d'experts :

« La NIS 2 est un pas en avant nécessaire pour renforcer la cybersécurité mais également la sécurité physique en Europe. Sa mise en œuvre soulève toutefois des questions légitimes, notamment en termes de coûts et de complexité de mise en œuvre. Il est donc crucial d'accompagner les entreprises dans cette transition et de trouver un équilibre entre les exigences réglementaires et les capacités des organisations. À moyen et long terme, les bénéfices de la NIS 2 en termes de résilience, de confiance et de souveraineté européenne sont indéniables. »
Mickael Wajnglas, secrétaire général de SPAC Alliance

« Fuites de données, hameçonnages ou encore rançongiciels, les cyberattaques menacent la survie de milliers de TPE-PME. Avec plus de 4 millions d'entreprises, soit 99% du tissu économique français, elles sont en première ligne. Pourtant, notre étude révèle que 65% d'entre elles ne sont pas préparées à une telle menace. Manque de temps, de connaissances, de budget ou encore du bon interlocuteur sont les principales raisons évoquées. Or, les conséquences peuvent être désastreuses comme l'interruption d'activité, le vol de données, l'altération de l'image de l'entreprise ainsi que des pertes financières pouvant atteindre plusieurs milliers d'euros. Les cyberattaques n'épargnent aucun type d'organisation, quelle que soit leur taille ou leur nature. Face à ce constat alarmant, il est urgent d'agir, de responsabiliser les TPE-PME et de les convaincre de se sécuriser en amont. »*
Gilles Berthelot, Chargé de mission Sensibilisation Cybermalveillance.gouv.fr



**Etude 2024 sur la maturité cyber des TPE-PME conduite par OpinionWay pour Cybermalveillance.gouv*

À RETROUVER SUR EXPOPROTECTION

Zoom sur les conférences

- **« Quel est l'impact de la directive NIS 2 sur la sécurité physique ? »** - *Sébastien Garnault – Fondateur de la CyberTaskForce & Philippe Latombe, Député de la 1re circonscription de Vendée & Arnaud Brouquier, Président de l'Alliance Nationale des Intégrateurs de Technologies (ANITEC) & Philippe Luc, Président d'ANOZRWAY* / mardi 5 novembre de 11h00 à 11h50. Détails en cliquant ici
- **« Face aux cyberattaques, pourquoi attendre pour se sécuriser ?** – *Gilles Berthelot, Chargé de mission Sensibilisation Cybermalveillance.gouv.fr* / mercredi 6 novembre de 16h30 à 17h15. Détails en cliquant ici
- **« Accélération de l'IA en sécurité : quel cadre réglementaire ? » -** *Sébastien Garnault, Fondateur de la CyberTaskForce & Arnaud Latil, Maître de conférences en droit de l'IA à la Sorbonne Université & Général Patrick Perrot, Coordinateur pour l'IA à la Gendarmerie Nationale* / Mercredi 6 novembre de 10h20 à 11h20. Détails en cliquant ici
- **« Encadrement juridique de l'IA : où en est-on ? Que dit la jurisprudence ? Que nous disent les premiers retours d'expérience ? » /** *Oriana Labruyere, Avocate et Fondatrice de* La Robe Numérique *& Quentin Barenne, CEO de* WINTICS *& Thomas Dautieu, Directeur de l'accompagnement juridique à la CNIL* / Jeudi 7 novembre de 14h00 à 14h50. Détails en cliquant ici

Service de presse
Agence ComCorp
Kelly LEOTARDI
kleotardi@comcorp.fr
+33 7 50 87 76 62
Anne-Claire BERTHOMIEU
acberthomieu@comcorp.fr
+ 33 6 16 53 15 70

Salon EXPOPROTECTION 2024

« La gestion du risque 360°dans un environnement instable »

29e édition – Porte de Versailles Hall 1
du 5 au 7 novembre 2024

Pour obtenir votre badge Presse, veuillez renseigner l'onglet dédié aux accréditations :
www.expoprotection.com/fr-fr/register.html

A propos d'Expoprotection :
Fondé dans les années 1960, Expoprotection est le rendez-vous biennal incontournable de la prévention et de la maîtrise des risques. Réunissant près de 650 exposants et autour de 15 000 visiteurs, le salon offre une vision 360° unique en France du marché de la prévention des risques, qu'ils soient professionnels, industriels, climatiques ou liés aux actes malveillants. C'est l'événement idéal pour découvrir les dernières innovations du secteur, rencontrer des experts de haut niveau et faire appel à des fournisseurs de solutions performantes afin de protéger les hommes et les organisations contre l'ensemble des menaces auxquelles ils sont exposés. www.expoprotection.com

Service de presse
Agence ComCorp
Kelly LEOTARDI
kleotardi@comcorp.fr
+33 7 50 87 76 62
Anne-Claire BERTHOMIEU
acberthomieu@comcorp.fr
+ 33 6 16 53 15 70