Live TECH

#7/ Cybersec Europe 2024

« Considérez la conformité comme une partie d'échecs ! »

Ivana Butorac, Cybersec Europe 2024

Secure by Design, c'est -vraiment- parti !

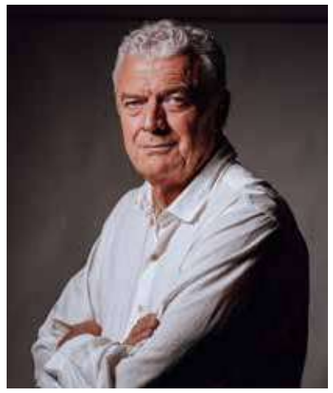
Le concept du Secure by Design n'est pas nouveau. Début mai, 68 « names » de la tech se sont engagés à en promouvoir les principes. Et ça change tout.

DORA ? Pensez « hygiène » !

DORA, de la mise en conformité à une approche par les risques. Explications de Kris Lovejoy, de Kyndryl.

NIS 2, sujet technique ou de management ?

Avec NIS2, la cybersécurité deviendrait-elle l'affaire du top management ? La question mérite d'être posée. Et suppose un changement de paradigme



NIS2, DORA, AI Act...Un vrai tourbillon ! En cette fin du mois de mai, Cybersec Europe 2024 en a été l'amphithéâtre. Autre repère, les six ans du GDPR, introduit en mai 2018. C'est là qu'on voit l'accélération du contexte cyber. De l'ingénierie sociale ciblée à la montée des deepfakes, via l'intelligence artificielle, les cybercriminels utilisent des tactiques de plus en plus sophistiquées pour dérober des informations sensibles.

Avec le recul, le GDPR a mis en lumière l'importance accrue de la réglementation pour aider les entreprises à protéger leurs données. Et, indirectement, la nécessité pour elles de prendre les devants. Aujourd'hui, on voit plus loin. Plus question de se contenter d'être guidés par les différentes formalités ou réglementations gouvernementales. De fait, les enjeux sont trop élevés. L'interruption de l'activité, la perte de clients, l'atteinte à la réputation et la restauration de systèmes qui suivent une violation de données peuvent, en effet, coûter très cher.

A travers les différents articles de ce LiveTech, on comprend mieux comment la cyber-résilience s'impose désormais au cœur même du modèle économique de nos entreprises. Et combien il est essentiel de protéger les informations sensibles et de veiller à ce que l'accès ne soit accordé qu'aux personnes qui en ont absolument besoin..

Alain de Fooz

#7/ Cybersec Europe 2024

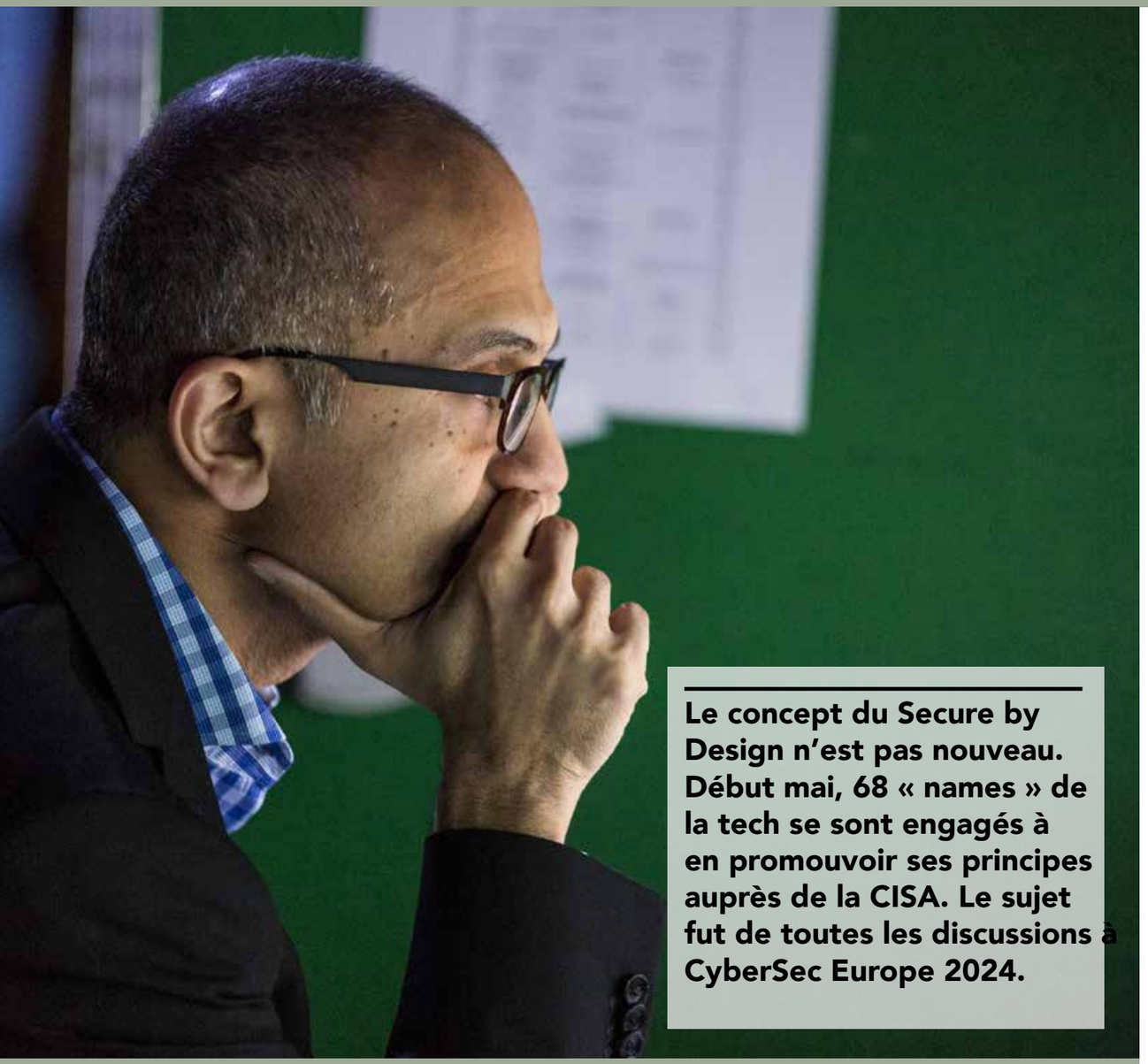
Éditeur responsable:
Alain de Fooz
106, chaussée de Nivelles
1472 Vieux-Genappe
alain@solutions-magazine.com
tél. +32 (0)498 255 118

Stratégie : Axel Cleven
Rédaction: Olivier De Doncker - Marc Husquinet - Nicolas Joannes - Axel Cleven
Photographie: Bénédicte Maindiaux
Sales Information & Media Reservation
André de Woot
tél. +32 (0) 497 41 22 49
adworldsprl@gmail.com

Mise en pages & Production :
Pierre Bertaux
Rédaction, Administration,
Ventes et Abonnements :
106, chaussée de Nivelles
1472 Vieux-Genappe
tél. +32 (0)498 255 118
ING: 310-1568406-02
IBAN: BE32 3101 5684 0602
BIC: BBRUBEBB

dixitcom

Secure by Design, c’est -vraiment- parti !



Le concept du Secure by Design n’est pas nouveau. Début mai, 68 « names » de la tech se sont engagés à en promouvoir ses principes auprès de la CISA. Le sujet fut de toutes les discussions à CyberSec Europe 2024.

AWS, Cisco, Google, IBM, Microsoft… Ils sont 68 à avoir adhéré à un effort dirigé par l’Agence américaine de cybersécurité et d’infrastructure. Tous, au cours de la RSA Conference 2024, ont promis de prendre une série de mesures d’ici un an pour rendre leurs produits plus sécurisés.

Le Secure by Design Pledge de la CISA (Cybersecurity and Infrastructure Security Agency) **est un engagement volontaire** que les éditeurs de logiciels d’entreprise prennent dans un effort de bonne foi pour définir et atteindre certains objectifs axés sur la sécurité, dont le plus fondamental est d’intégrer la cybersécurité dans la conception et la fabrication de produits technologiques.

L’exemple le plus frappant est sans doute l’extension par Microsoft de son initiative SFI (Secure Future Initiative), dans laquelle l’entreprise de Redmond a promis de **donner la priorité à la sécurité dans son organisation et dans le développement de ses produits « avant toute chose »**. Microsoft a annoncé la SFI pour la première fois en novembre dernier, à la suite d’une violation très médiatisée et perpétrée par un acteur étatique chinois.

Dans un billet de blog, Charlie Bell, ExecutiveVP, Microsoft Security, a énoncé **trois principes : la sécurité dès la conception, la sécurité par défaut et la sécurité des opérations.** En ce qui concerne la sécurité dès la conception, Charlie Bell a déclaré : « Désormais, la sécurité passe avant tout lors de la conception d’un produit ou d’un service ».

DE CHATGPT À FRAUDGPT

C’est d’autant plus nécessaire à l’ère de la GenAI. La technologie qui alimente ChatGPTalimente également FraudGPT -une solution de cybercriminalité tout-en-un légitime, qui a déclenché l’alarme auprès des dirigeants d’entreprise. Selon une enquête de Gartner, **57 % des CIO et des CISO sont préoccupés par la fuite de secrets dans le code généré par l'IA.**

« Désormais, la sécurité passe avant tout lors de la conception d’un produit ou d’un service »

Même tendance côté développement, remarque **Devoteam**. *« Les équipes devant accélérer leur fréquence de livraison et les équipes de sécurité faisant face à des menaces de plus en plus sophistiquées et régulières, l’implication de la sécurité dès la conception des applications devient une nécessité. »*

Nous trouvant donc dans un paradigme de développement agile et de déploiement continu, **appliquer la sécurité uniquement à la fin, par un audit de sécurité, n’est plus suffisant ni pratique.** Par ailleurs, corriger une vulnérabilité de sécurité coûte bien plus cher, en temps et argent, quand c’est réalisé en production ou pré-production par rapport aux étapes de conception et de développement.

« C’est tout un changement de paradigme qui implique de se focaliser sur la prévention des attaques et la consolidation des données sécurisées, plutôt que sur la réaction à ces attaques, comme la résolution des problèmes ou la restauration des systèmes », enchaîne **Oodrive**.

DANS LE MOUVEMENT DEVSECOPS

Au niveau des processus de développement, l'approche Secure by Design s'inscrit dans le mouvement DevSecOps. En phase de conception, cela signifie que les différentes options de sécurité sont intégrées dès la phase d'intégration et de test continus. Autrement dit, elles sont implémentées puis testées, afin de ne sélectionner que les meilleures solutions de sécurité pour l'architecture. Ces solutions deviennent en quelque sorte des principes directeurs pour les développeurs. En phase de déploiement, lors du déploiement continu, des tests d'intrusion sont menés pour améliorer toujours plus le niveau de sécurité du logiciel. En phase de livraison, enfin, des tests et audits préventifs continuent d'être lancés pour affiner la solution de sécurité.

« C'est tout un changement de paradigme qui implique de se focaliser sur la prévention des attaques et la consolidation des données sécurisées, plutôt que sur la réaction à ces attaques, comme la résolution des problèmes ou la restauration des systèmes »

Comme il est établi que les failles de sécurité seraient dues, le plus souvent, à un défaut de conception dès l'origine plutôt qu'aux suites d'une attaque informatique, le « by design » s'est progressivement imposé comme le moyen de « penser la conformité » en amont de la conception d'un objet ou d'un système connecté et, ensuite, tout au long de son cycle de vie. Dans le cadre du GDPR, l'approche Secure by Design devient Privacy by Design. L'idée est toujours la même : fournir une protection optimale aux données personnelles dès la conception.

Parfois, le concept de « by design » s'inscrit dans une simple démarche de certification non contraignante. Il en est ainsi du Cyber Security Act, qui incite les fournisseurs ICT à garantir la sécurité des produits dès le stade de la conception et à la prendre en charge tout au long du cycle de vie du produit. Il devrait néanmoins se généraliser, car il fait l'objet d'une proposition de règlement européen, le « cyber resilience act », visant à imposer des règles essentielles relatives à la conception du produit numérique afin de garantir sa cybersécurité.

LE BY-DEFAULT COMPLÉMENTAIRE DU BY-DESIGN

En marge du « by-design », un autre concept, le « by-default », s'est développé. Dans une première déclinaison dite « privacy-by-default », l'opérateur a **l'obligation de garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées.** Le législateur européen a, ici, voulu imposer le plus haut degré de protection, lequel est mis en place par défaut. C'est dans cet objectif que l'utilisateur est seul à pouvoir autoriser de nouveaux traitements -par exemple, en téléchargeant une application sur son smartphone, c'est à l'utilisateur d'autoriser l'accès ou non à l'appareil photo.

Dans une déclinaison « security-by-default », le Cyber Security Act invite les concepteurs à configurer leurs produits, services et processus « de manière à assurer un niveau de sécurité plus élevé ». Ainsi, le premier utilisateur reçoit une configuration par défaut avec les paramétrages les plus sûrs possible, sans avoir à procéder à une quelconque manipulation. Une fois mis à la disposition de l'utilisateur, l'objet ou le système connecté doit être configuré de telle sorte qu'il soit, par défaut, résistant aux techniques d'exploitation les plus répandues, et ce, sans frais supplémentaires.

CULTURE DE LA RÉSILIENCE

Security by Design n'est pas seulement une méthodologie, mais une culture qui nécessite un engagement de tous les acteurs impliqués dans la création et la gestion des systèmes informatiques. En incorporant la sécurité dès le début et tout au long du cycle de vie des systèmes, les organisations peuvent construire des infrastructures plus résilientes face aux menaces croissantes de la cybersécurité.

Il est impératif pour les professionnels de la cybersécurité de continuer à promouvoir et à améliorer les principes de Security by Design afin de protéger l'intégrité, la disponibilité et la confidentialité des systèmes d'information dans un monde de plus en plus interconnecté.

« Nous pensons que la question n'est pas 'pourquoi maintenant ?', conclut **Brandon Wales, Executive Director, CISA.** *La vraie question que nous devrions nous poser est plutôt pourquoi avons-nous mis tant de temps à faire de cette question le véritable enjeu ? Le meilleur moment pour le faire c'est donc tout de suite ! »* ■

Secure Future Initiative, l'engagement de Microsoft

« I want to talk about something critical to our company's future: prioritizing security above all else. »…

Un mémo envoyé aux 200 000 employés du groupe qui fera date. En écho à notre récent article et au rapport lapidaire du CSRB (Cyber Safety Review Board) américain, **Satya Nadella a pris la plume pour redonner un nouvel élan à la culture cybersécurité de son entreprise** et détailler les mesures mises en œuvre par Microsoft pour redorer son image et surtout renforcer sa posture cybersécurité et celle de ses clients.

C'était le 3 mai dernier. En une phrase d'introduction, Satya Nadella résume toutes les clés : **Microsoft joue sa crédibilité, Microsoft veut imposer une nouvelle culture interne qui place la sécurité en premier avec sa Secure Future Initiative,** Microsoft a entendu le CSRB et sa demande de voir le CEO de l'entreprise s'emparer du sujet et en faire sa priorité.

« Si vous devez choisir entre la sécurité et une autre priorité, la réponse est claire : privilégiez la sécurité, précise encore Satya Nadella dans son mémo. Dans certains cas, cela signifie qu'il faut donner la priorité à la sécurité plutôt qu'à d'autres choses, comme le lancement de nouvelles fonctionnalités ou la continuité d'activité de systèmes ancestraux. Il s'agit là d'un élément clé pour faire progresser à la fois la qualité et les capacités de nos plateformes afin de protéger les biens numériques de nos clients et de construire un monde plus sûr pour tous. »

Ivana Butorac

Considérez la conformité comme une partie d'échecs !

Ivana Butorac, oratrice à Cybersec Europe 2024, compare la conformité à une partie d'échecs… Débutons-la ici ! Tout jeu commence par la connaissance de l'adversaire, dit-elle. En l'occurrence, le pouvoir législatif.

Juris non excusat ! L'ignorance de la loi n'excuse personne. Ainsi, une personne qui ne connaît pas la loi ne peut échapper à sa responsabilité en cas de violation de celle-ci. *« Connaître vos obligations et vos droits tels que dictés par la loi influencera de manière significative votre prise de décision en matière d'entreprise et donc de conformité »*, prévient **Ivana Butorac, Data Protection Expert, Sopra Steria.**

Respecter ses obligations et ses droits permettra de plaider en assurant que les clients ont non seulement été protégé contre toute utilisation abusive, mais également que l'entreprise a été protégée contre les atteintes à la réputation et les dommages financiers pouvant résulter d'une non-conformité.

L'exemple du GDPR est révélateur. Les sanctions pour non-respect sont lourdes - parfois des millions d'euros. *« Par facilité, certaines entreprises préfèrent payer. Mais ce n'est pas une solution à long terme.* ***Si vous n'êtes pas perçu comme un fournisseur fiable et digne de confiance, votre réputation sera ternie****. Vos clients commenceront à chercher des alternatives. En d'autres termes, l'ignorance n'exclut personne. »*

CONNAISSEZ VOTRE LOI !

Non, le droit n'est pas une matière aride ! Mieux vaut voir l'utilité des lois, estime Ivana Butorac. En particulier les lois relatives à la technologie. Elles nous livrent de précieux conseils sur la façon dont nous pouvons créer de meilleurs produits et développer de meilleurs services. *« Tant le GDPR que DORA -pour ne citer que ces deux lois- nous aident non seulement à atteindre la conformité, mais également à commercialiser nos produits. Dans la tech, les lois sont si pratiques qu'elles nous disent ce que l'on a à faire ! »*

L'experte en Data Protection chez Sopra Sterianous invite également à réfléchir à l'évolution du marché. Et donc d'investiguer ses perturbations.*« Facebook et Cambridge Analytica ont ébranlé le paysage des lois sur la vie privée et la protection des données, et donc la société d'une manière générale. En tant que citoyens consommateurs, nous sommes sortis du silence ; nous avons commencé à poser des questions et à mettre nos droits au premier plan. La vie privée est l'un de nos droits fondamentaux. Le marché ne pouvait plus ignorer la demande de la société ! »*

Hier, la question de la cybersécurité était taboue. Il était difficile d'en parler. Pour preuve, sa part négligeable dans les investissements. Et pour cause : peu d'organisations estimaient pouvoir être victimes de cyberattaques. *« Le silence façonnait le jeu et créait un grand écart… »* Quant aux lois, pour beaucoup elles existaient, mais elles étaient ignorées. Souvent,à tort, les professionnels considèrent le droit comme quelque chose de très restrictif dans le sens où ce n'est pas lui qui >>>

« Les lois changent, même si elles évoluent assez lentement. Si vous n'en tenez pas compte dès le début, il sera très difficile de revenir en arrière et de refaire vos processus et votre documentation... »

« Connaître vos obligations et vos droits tels que dictés par la loi influencera de manière significative votre prise de décision en matière d'entreprise et donc de conformité »

>>> dirige l'entreprise. De fait. Mais **la sécurité juridique et l'engagement sont les signes d'une attitude commerciale positive**. *« La loi construit la responsabilité ! »*

On peut réfuter que le droit est souvent trop lent à s'adapter au paysage de la tech. Et que, parce que très large, il peut générer un conflit avec celle-ci. Or, on a tout intérêt à fusionner droit et tech. *« Les gens ont du mal à mettre en œuvre les exigences légales d'une loi. L'exemple du GDPR est éloquent. Le texte introduit des principes tels que la minimisation des données, la limitation des finalités, la sécurité et la responsabilité... Vous devrez prendre certaines mesures, comme le cryptage par pseudonymisation. Et adopter une approche basée sur les risques. Réfléchir, aussi, à ce qui peut arriver. Ce n'est qu'à ce moment-là que vous pourrez commencer à élaborer une solution… »*

PLUS DE LOIS, PLUS DE PRÉVENTION

Trop de lois, entend-on. Certes. À entendre Ivana Butorac, c'est très positif. Pour elle, il est important de renforcer la sécurité juridique. Ce sont autant de mesures concrètes pour créer des produits meilleurs et plus sûrs. *« Cette évolution résulte de notre ambition de devenir plus avancé technologiquement. Si nous voulons être innovants, comment, concrètement, atteindre nos objectifs informatiques sans dépasser les limites de la société ? Comment pouvons-nous faire tout cela tout en restant protégés contre les attaques extérieures ? »* La cybersécurité est devenue une priorité. Ce qui veut dire que l'accent est porté sur la prévention. On a compris que **le droit n'est pas là pour restreindre, mais pour nous aider à réfléchir à la manière dont nous pouvons améliorer notre cybersécurité.**

À ce propos, il est intéressant de constater que les législateurs et les régulateurs européens s'intéressent désormais également aux différents marchés et aux différents aspects du monde technologique. *« En fait, nous avons commencé à segmenter la cybersécurité en différents domaines. Ainsi, avec DORA -la loi qui se concentre sur les marchés financiers. Partant que les banques traitent des données hautement confidentielles, elles peuvent vraiment souffrir des cyberattaques. »*

Le volet juridique est un pilier de la résilience. Notamment pour rester compétitif. *« Les lois changent, même si elles évoluent assez lentement. Si vous n'en tenez pas compte dès le début, il sera très difficile de revenir en arrière et de refaire vos processus et votre documentation.* ***Connaître vos obligations, limites et possibilités juridiques contribuera à votre compétitivité sur le marché et à votre résilience d'un point de vue commercial !*** *»*

Établir une gestion et une gouvernance des données efficaces et solides est impérieux. *« Il vous faut connaître la nature des données dont vous disposez. Savoir où vous les stockez. Idem pour leur classification. De manière générale, comprenez la sensibilité de celles-ci. Commencez par faire la différence entre les données personnelles et non-personnelles. Selon la loi, les données personnelles peuvent avoir différents niveaux de sensibilité. Différentes mesures de sécurité sont donc requises... Si vous classez correctement vos données, vous saurez quel type de mesures de sécurité vous devez mettre en œuvre pour rester conforme. Croyez-moi, cela vous évitera bien des soucis ! »*

CONFORMITÉ, TROIS PILIERS

Ivana Butorac conseille également d'adopter une approche des risques basée sur trois piliers plus solides. Pour commencer, évaluer les risques qui pourraient avoir un effet négatif sur le système ou produit. Ensuite, s'intéresser à la tech. Un produit peut, en effet, reposer sur différentes technologies. Ainsi, l'IA. Quels sont les risques liés à l'intelligence artificielle ? Enfin, troisième pilier : une approche du risque fondée sur la société. Le consommateur peut être affecté par l'usage du produit. Ou impacté sur sa vie privée. Bref, on verra dans quelle mesure les droits fondamentaux sont touchés… ou pas. *« Élargir votre approche sur ces trois piliers revient à réduire l'écart. Ce faisant, vous fermerez les portes aux vulnérabilités et aux non-conformités. »*

Enfin, autre conseil : renforcer l'équipe de cybersécurité avec une personne qui a des connaissances très pointues en matière de conformité. *« Votre équipe sera très efficace dans les pratiques de prévention, d'intervention et de détection. D'un point de vue technique,* ***si vous disposez d'un expert en conformité, cela vous aidera à voir ce qui vous manque en dehors de la sécurité que vous devriez mettre en œuvre****. Et cela vous permettra de clôturer cette approche à trois piliers. »* ■

Les sanctions pour non-respect sont lourdes - parfois des millions d'euros. Par facilité, certaines entreprises préfèrent payer. Mais ce n'est pas une solution à long terme. Si vous n'êtes pas perçu comme un fournisseur fiable et digne de confiance, votre réputation sera ternie.

NIS2 : DPO et CISO sont dans un bateau...

De toute évidence, NIS2 pousse à un élargissement du rôle du DPO au-delà du GDPR vers la sécurité. Question : est-il le mieux placé pour mener le projet ?

NIS2 serait dans l'esprit du GDPR, dit-on. Le sujet serait donc, logiquement, l'affaire du DPO. Si le DPO est à la croisée du technique et du juridique, les spécialistes du dossier NIS2 ne sont pas sûrs qu'il soit le meilleur interlocuteur.

« Le GDPR est un sujet juridique, NIS2 un sujet de risk management ! », **estime Stanislas Van Oost, Founder & Managing Director, Easiance.** Pour ce spécialiste de la conformité, on s'éloigne de la vocation première du DPO. *« Pour moi, la protection des données privées n'est qu'un sous-ensemble du sujet. Et donc la gestion de risque brasse plus large. Autant un juriste fera un bon DPO, autant, je pense, il ne pourra faire le job d'un CISO ! »*

CISO ET DPO, UN OBJECTIF COMMUN

Depuis plusieurs années, les DPO sont effectivement en première ligne pour traduire concrètement en interne les évolutions juridiques sur les données -le GDPR bien sûr, mais aussi celles à venir. Qui plus est, **en matière de sécurité de l'information, on rapproche facilement la norme ISO 27001 et le GDPR.** En effet, ces deux textes se recoupent dans leur objectif de renforcer la sécurité de l'information et la protection des données. Bien que leurs approches diffèrent légèrement, les deux initiatives visent à protéger l'information détenue par un organisme. D'un côté, ISO 27001 est axée sur la sécurité de cette information, tandis que le GDPR se concentre spécifiquement sur la protection des données personnelles.

A priori, donc, CISO et DPO partagent un objectif commun : assurer une gouvernance efficace et conforme des données et de la sécurité de l'information au sein des organisations. *« Mais sans plus,* renchérit **Jordan Saint-Ghislain, CybersecurityIncident Response Manager, Redsystem.** *Il n'y a pas que les procédures. Plus que NIS, NIS2 implique de parfois mettre les mains dans le moteur. Et plus souvent qu'on ne l'imagine. Car si vous êtes attaqué, c'est trop tard ! »*

Les CyFun du CCB

Comment se conformer aux exigences de cybersécurité de la Directive NIS2 ? En Belgique, outre la certification à la norme ISO 27001, un nouveau cadre devrait jouer un rôle de présomption de conformité à NIS2 : le cadreCyFun (Cyberfundamentals) créé début 2023 par le CCB (Center for Cyber security in Belgium).

Les CyFun (3 labels) se basent sur la structure du cadre NIST, mais aussi sur les mesures que l'on retrouve dans les normes ISO 27001, IEC 62443 ou les contrôles CIS. Une base solide donc, en cours de test actuellement.

De fait, des questions restent encore sans réponse. Le CyFun améliorera-t-il significativement la cybersécurité ou entraînera-t-il des formalités administratives ? Est-il suffisamment clair ? Quel est le coût de sa mise en œuvre ?

VOIR PLUS LOIN QUE LA QUESTION DE LA CONFIDENTIALITÉ

Autrement dit, si le DPO joue un rôle crucial pour garantir le respect des réglementations en matière de protection des données, il n'est pas toujours le candidat le plus approprié pour diriger des initiatives de cybersécurité plus larges, nuance **Sabika Ishaq, Chief Information Security Officer, Grant Thornton Luxembourg.** L'expertise du DPO se concentre généralement sur les questions liées à la confidentialité et au respect de réglementations telles que le GDPR, plutôt que sur les subtilités techniques de la gestion et de l'atténuation des risques de cybersécurité.

« Au lieu de cela, les organisations peuvent envisager de nommer un CISO ou un responsable de la conformité pour diriger les efforts de cybersécurité. Ces rôles sont spécifiquement dédiés à la supervision de la posture de cybersécurité de l'organisation, y compris l'élaboration et la mise en œuvre de stratégies, politiques et contrôles de cybersécurité. »

Les CISO possèdent l'expertise technique et la vision stratégique nécessaires pour naviguer efficacement dans le paysage complexe des menaces et des vulnérabilités de cybersécurité.

UNE COMPLÉMENTARITÉ DES RÔLES ?

Les organisations peuvent également choisir de créer une équipe ou un département dédié à la cybersécurité, dirigé par un responsable ou un directeur de la cybersécurité. Cette équipe serait chargée de gérer les opérations quotidiennes de cybersécurité, de coordonner les efforts de réponse aux incidents et de mener des initiatives d'amélioration continue dans l'ensemble de l'organisation. *« En centralisant les responsabilités en matière de cybersécurité sous une direction dédiée, les organisations peuvent garantir une approche cohérente et proactive de la gouvernance de la cybersécurité, en l'alignant sur les objectifs commerciaux et les priorités de gestion des risques »,* dit encore Sabika Ishaq.

DPO et CISO dans un même bateau ? On ne peut toutefois écarter la question de la cohabitation de ces postes. Car, quand bien même les discussions s'orientent vers une coopération, un intérêt collectif, une intelligence commune, **un risque demeure : une source de conflit potentiel en termes de gouvernance**.

Pour les organisations qui se dirigent vers une complémentarité des rôles, celle-ci doit se préparer dès maintenant. On imagine facilement qu'avec les développements de l'IA et de l'hyperconnectivité, NIS 3, et encore plus loin, NIS 4 définiront un champ d'intervention, mais aussi d'autres exigences plus pointues pour les entreprises, conclut Stanislas Van Ooost. ■

Kris Lovejoy

DORA ? Pensez « hygiène » !

DORA, de la mise en conformité à une approche par les risques. Le comité exécutif est désormais le principal responsable de la définition de cette stratégie… Explications de Kris Lovejoy, Kyndryl

Entrée en vigueur le 17 octobre 2024 pour NIS2 et le 17 janvier 2025 pour DORA. NIS2 est une directive, là où DORA (Digital Operational Resilience Act) est un règlement. A priori, aucun lien. Bien que. Le souci de résilience est le même.

« Avec DORA, les rapports annuels des sociétés ouvertes devront divulguer leur stratégie et leur gouvernance en matière de risques de cybersécurité, y compris le rôle de leur conseil d'administration dans la gestion des cyber-risques importants ,» stipule d'emblée **Kris Lovejoy, Global Security and ResiliencyLeader, Kyndryl.**

De même, DORA confie aux conseils d'administration de presque toutes les sociétés de services financiers réglementées dans l'Union européenne la responsabilité ultime de la gestion des risques et de la stratégie de résilience opérationnelle pour les technologies de l'information et des communications. En pratique, **cela nécessitera que les conseils d'administration s'approprient davantage la supervision des risques de cybersécurité,** notamment en garantissant le respect des exigences techniques et politiques du règlement.

« Pensez la protection en termes d'hygiène et non pas de course technologique »

SE PRÉPARER AU RÈGLEMENT DORA

Compte tenu de la myriade de menaces, de règles et de mesures de protection, les entreprises peuvent aisément se sentir dépassées lorsqu'elles déploient leur cybersécurité. **« Pensez la protection en termes d'hygiène et non pas de course technologique»**, conseille Kris Lovejoy. Premier conseil : *« savoir précisément quelles technologies ont été déployées, ce qui veut dire recourir à des systèmes d'inventaireperformants. S'assurer, dans la foulée, à ce qu'elles soient à jour, protégées et bien surveillées. Disposer, enfin, d'un mécanisme pour les restaurer en cas de problème. »*

Même si certaines organisations ne prennent pas la cybersécurité aussi au sérieux que d'autres, les entreprises de nombreux secteurs vont devoir s'assurer que leurs normes de sécurité sont prêtes pour les nouvelles législations de l'UE.

A entendre Kris Lovejoy, DORA va inciter les organisations à **envisager les risques de cybersécurité d'une manière holistique.** *« Le règlement va obliger les organisations à mettre en place un cadre garantissant les contrôles adéquats et les investissements nécessaires pour atténuer les risques et assurer leur récupération… ce qui est, en fait, de la cyber-résilience* ! »

CONSIDÉRER LA CHAÎNE D'APPROVISIONNEMENT

DORA prescrit aussi de disposer d'un mécanisme permettant de détecter, de répondre et d'informer les agences concernées d'un incident lorsqu'il

atteint un certain niveau. Les entreprises devront avoir la capacité de mettre en œuvre des contrôles raisonnables pour gérer ce cadre.

De même, les organisations **devront réfléchir à la cybersécurité de la chaîne d'approvisionnement,** ce que Kris Lovejoy décrit comme une *« exigence importante et relativement nouvelle »*, en raison du nombre d'acteurs malveillants qui utilisent les vulnérabilités de la chaîne d'approvisionnement *« essentiellement comme un cheval de Troie »* pour pénétrer dans les organisations.

DORA exige un contrôle renforcé des chaînes d'approvisionnement, incluant les partenaires de sous-traitance comme Kyndryl, qui sont des partenaires essentiels de ces entreprises et organisations, afin de s'assurer qu'ils ne présentent aucun risque. ■

NIS2, DORA… un point commun : la gouvernance

Alors que la directive NIS2 vient homogénéiser le niveau de cybersécurité global à travers les pays de l'UE, le règlement DORA vise à renforcer la résilience opérationnelle numérique du secteur financier.

Son rôle est de s'assurer que les entités financières soient en mesure de résister et continuer à fonctionner même en cas de cyberattaque. Ce sont bien la disponibilité et l'intégrité des services financiers qui sont au cœur du règlement.

Dans la réalité des choses, **les deux textes se complètent bien plus qu'ils ne se font concurrence.** NIS2 vise à renforcer le niveau de cybersécurité global dans l'UE, là où DORA assure que le système financier reste fonctionnel même en cas de cyberattaque.

Qui plus est, ces deux textes partagent **un point commun majeur : l'un et l'autre prévoient l'instauration de sanctions, notamment réputationnelles (name and shame) et établissent, en cas de manquement, la responsabilité pénale des dirigeants de l'entreprise.**

Dans le cas de DORA, ceux-ci ont d'ailleurs l'obligation d'être formés aux risques cyber et à leurs impacts sur la continuité des opérations. Outre l'aiguillon que représente le risque juridique et financier, ceci bouleverse la gestion traditionnelle de la cybersécurité dans l'entreprise et, en particulier, sa gouvernance.

Avec des responsabilités remontées au niveau de la direction, la cybersécurité devient de fait un enjeu d'entreprise, qui sera intégré à la stratégie globale et abordé de façon systématique et transverse, au même titre que d'autres types de risques. Ceci favorisera l'homogénéisation des dispositifs et des pratiques, l'optimisation de l'allocation des ressources, l'intégration de la sécurité dans les processus opérationnels et sa prise en compte « by design » dans les projets et, enfin,le développement d'une culture interne de la cybersécurité.

5 conseils pour anticiper les cybermenaces, s'en protéger, résister à leur impact et restaurer rapidement leurs environnements informatiques critiques

1 **Sensibiliser le conseil d'administration et impliquer l'entreprise dès le départ -** Les réglementations émergentes en matière de cybersécurité exigent un engagement au niveau du conseil d'administration. En conséquence, l'heure n'est plus aux cloisonnements. La cybersécurité n'est pas une question de « niche ». C'est l'affaire de tous, y compris du conseil d'administration et de la direction.

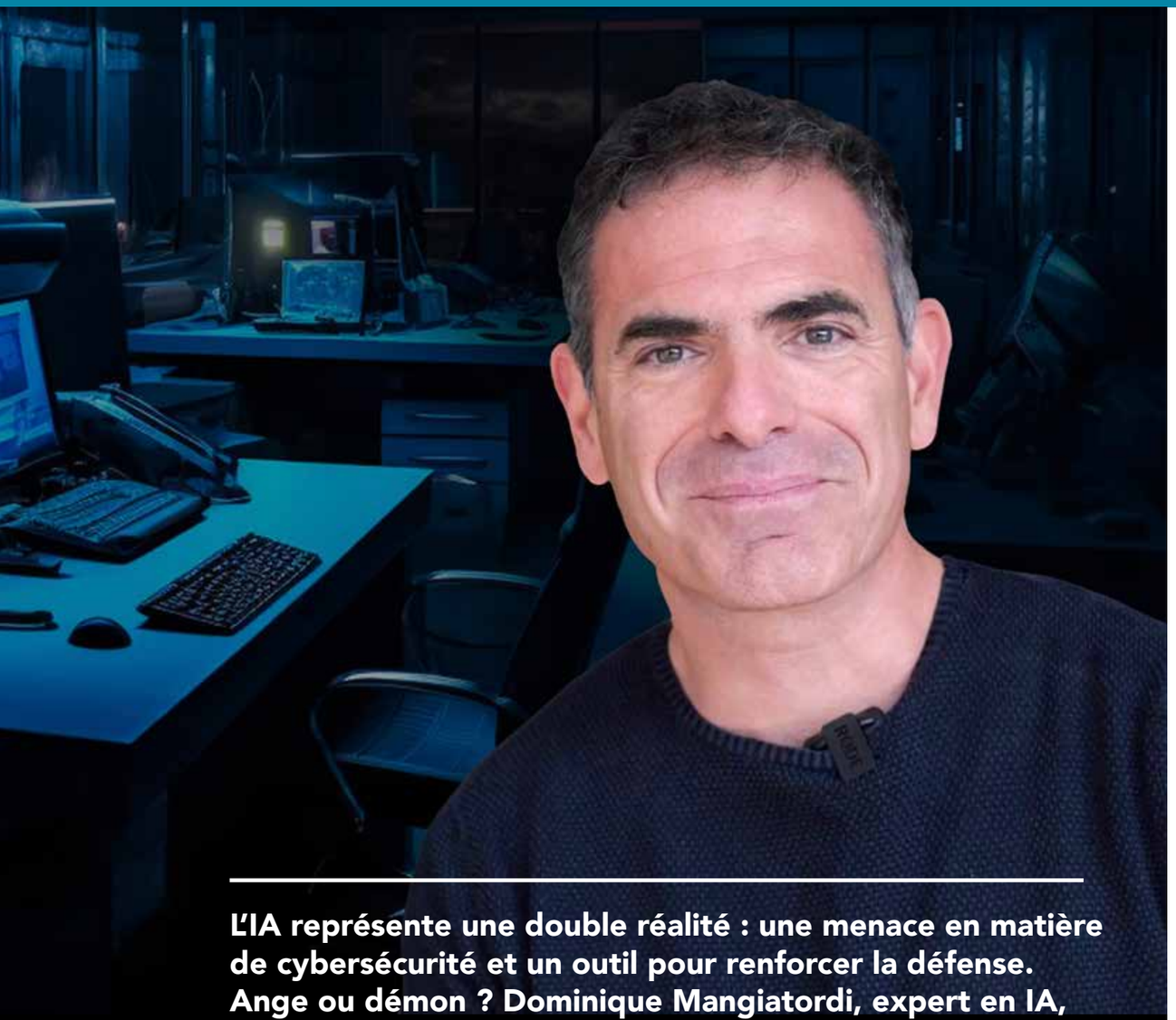
2 **Créer une MVC (Minimum Viable Company**) - L'entreprise minimale viable est définie comme le minimum de services commerciaux dont une organisation a besoin pour maintenir un niveau de fonctionnalité prédéterminé. Une organisation peut disposer de plusieurs dizaines de services métiers, mais il est impératif que seuls ceux définis comme essentiels à sa mission soient inclus dans le MVC. Il est important de développer cette vision de l'entreprise, car elle définira la portée et la complexité de ses efforts de redressement.

3 **Inventorier et déterminer les risques** - Les organisations disposant d'un parc informatique vaste et complexe doivent connaître les actifs dont elles disposent, les mesures dont elles ont besoin pour les protéger et la probabilité de tentative de perturbation en fonction de la fonction. En d'autres termes, identifier et protéger le talon d'Achille de l'organisation.

4 **Élaborer un plan de gestion de crise et des pratiques en cas de perturbation** - L'heure est à l'anticipation et à la préparation pour gérer l'inévitable. Lorsqu'il s'agit de cyberattaques, la question n'est pas de savoir « si », mais quand.

5 **Passer à un cadre Zero Trust et mettre régulièrement à jour la stratégie de cyber-résilience** - La confiance zéro consiste à prendre des décisions d'accès au cas par cas. Chaque utilisateur, application, ordinateur, etc. se voit attribuer le minimum d'accès et d'autorisations nécessaires pour remplir son rôle.

IA et cybersécurité, ange ou démon ?



L'IA représente une double réalité : une menace en matière de cybersécurité et un outil pour renforcer la défense. Ange ou démon ? Dominique Mangiatordi, expert en IA, invité de la prochaine Cyber School, le 19 juin à Living Tomorrow, avance quelques pistes de réflexion.

Nous devons être prudents et en même temps comprendre ***qu'il n'est pas bon de tout avoir dans un laboratoire.*** *Il s'agit d'un produit que nous devons diffuser, mettre en contact avec la réalité* ***et commettre des erreurs tant que les risques sont faibles****. Cela dit, je pense que les gens devraient se réjouir que nous ayons un peu peur de cela. Si je pouvais dire que cela ne me fait pas peur, vous ne devriez pas me faire confiance (...) »* C'était en mars 2023. Sam Altam, fondateur d'OpenAI, exprimait ses craintes sur l'intelligence artificielle générative à ABC News. Plus récemment, à la mi-mai, le même Sam Altam présentait ses excuses à l'actrice Scarlett Johansson, qui l'accusait d'avoir copié sa voix pour Sky, le tout nouveau mode vocal de ChatGPT…

Nous naviguons entre « AI safety » et « AI ethics », deux camps bruyants, diamétralement opposés. Entre les deux, le balancier effectue inlassablement son mouvement. À nous d'en saisir le rythme. Question : l'IA est-elle réellement le nouvel outil indispensable de la cybersécurité aux opportunités multiples, ou bien les risques encourus face à cette nouvelle technologie, pour laquelle nous ne disposons d'aucun recul, sont-ils trop élevés ? *« Si l'IA est utilisée comme facilitateur du quotidien, elle pose de nombreuses interrogations en termes de sécurité »,* reconnaît **Dominique Mangiatordi, expert en IA, invité de la prochaine Cyber School, le 19 juin à Living Tomorrow (Vilvorde).**

UNE MENACE ET UN OUTIL

Ne nous leurrons pas : nous sommes entrés dans l'ère de l'IA offensive. Cette évolution marque un tournant significatif dans la guerre numérique, où les IA deviennent à la fois des cibles et des acteurs majeurs des attaques, comme de la défense. Comme le note

« Désormais, plus besoin d'être un expert en codage et réseau, l'intelligence artificielle offre un réel avantage pour qui souhaite effectuer une cyberattaque»

Dominique Mangiatordi, l'IA représente ainsi une double réalité : ***« une menace en matière de cybersécurité et un outil pour renforcer la défense… »***

Au niveau des menaces les plus prévisibles, il y a naturellement les attaques traditionnelles. Mais dopée à l'IA, elles changent de nature, sans compter de nouvelles menaces qui ne manqueront pas de voir le jour. Les ransomwares ciblés font partie des menaces les plus préoccupantes, car ils visent de plus en plus souvent des organisations abritant des données sensibles tels que les hôpitaux et l'administration publique. Les attaques Zero-Day sont également en hausse. **Avec les Jeux Olympiques de Paris 2024 en ligne de mire, plus de 3 milliards d'attaques sont anticipées !** Côté entreprise, les fournisseurs et partenaires sont devenus des cibles privilégiées, avec une augmentation spectaculaire des attaques de la chaîne d'approvisionnement. Globalement, des attaques en hausse de 600 % l'année dernière !

HACKER ISOLÉ, MAIS ENTOURÉ D'UNE PETITE ARMÉE

« Désormais, plus besoin d'être un expert en codage et réseau, l'intelligence artificielle offre un réel avantage pour qui souhaite effectuer une cyberattaque, poursuit Dominique Mangiatordi. *En maîtrisant les IA, les hackers, souvent isolés, se retrouvent entourés d'une petite armée ! »* **De par la disponibilité et l'accessibilité des techniques d'IA, tout un chacun pourrait s'improviser hacker.** Les phénomènes de ChatGpT et de Codex participent justement à l'émergence de nouveaux outils bien plus accessibles et bien plus rapides.

« L'IA est donc capable de prendre en charge de nombreuses étapes souvent très chronophages dans l'élaboration d'une cyberattaque qui semble presque automatisée.» Cette automatisation permet aussi aux cybercriminels de pouvoir attaquer de façon moins coûteuse qu'auparavant. Grâce aux veilles automatisées, à l'optimisation de leurs capacités d'intrusion avec des techniques de phishing intelligent par exemple, **les cyberattaquants n'ont plus besoin d'autant de ressources qu'avant.** Ce phénomène de transposition du crime terrestre vers le crime cyber grâce aux nouveaux outils ne change pas pour autant la nature de l'acte. L'IA offre de nouvelles opportunités aux criminels qui voient leur récompense augmentée et leur risque d'être repérés diminués (anonymisation par exemple).

IA OFFENSIVES, IA DÉFENSIVES

Côté défensif, l'IA est un outil efficace pour une cybersécurité plus efficace, notamment au regard de la cyberdéfense des organisations aussi bien d'un point de vue organisationnel, pour l'attribution des ressources ou la protection des données, que pour des méthodes plus spécifiques telles que la réponse à incident ou la gestion de la menace cyber.

« L'IA permet de traiter un important volume de données en continu, rappelle Dominique Mangiatordi. *Ainsi, elle peut détecter de nouveaux risques de sécurité, d'autant plus que les algorithmes apprennent au fur et à mesure afin d'éviter les procédures répétitives. Ainsi décuplées, ces capacités permettent d'améliorer certains aspects de la cybersécurité… »*

L'intégration des technologies d'IA et de ML, en particulier, apporte beaucoup. Dans la détection des intrusions, par exemple, les systèmes basés sur l'IA surveillent en temps réel les activités réseau, identifiant tout comportement inhabituel révélateur d'un trafic malveillant. De même, les algorithmes de ML sont utilisés pour créer des modèles de comportement des logiciels malveillants, permettant ainsi une détection proactive des menaces potentielles.

De ce fait, l'IA devient cruciale dans l'analyse des vulnérabilités. Sans elle, il serait beaucoup plus compliqué, voire impossible, de détecter les vulnérabilités Zero-Day. Les IA apprennent et s'adaptent au comportement des attaquants pour mieux anticiper les menaces futures. Il devient alors beaucoup plus difficile, pour les acteurs cyber-malveillants, de les contourner.

DES ATOUTS, MAIS AUSSI DES LIMITES

Plus globalement, l'IA améliore la gestion des risques en anticipant les menaces potentielles. En effet, en assimilant et en analysant des quantités massives d'informations sur les menaces passées et actuelles, les outils d'IA fournissent des solutions de sécurité robustes.

« Face à toutes ces différentes utilisations, qu'elles soient offensives ou défensives, l'intelligence artificielle reste un domaine sur lequel nous avons peu de recul aujourd'hui. Si ces atouts sont évidents, ses limites nous montrent toutes les défaillances qui devront être corrigées afin de pallier les risques d'attaques ou même d'éthique », nuance Dominique Mangiatordi.

PAS SANS INCONVÉNIENTS

Comme la plupart des avancées techniques révolutionnaires, **les avantages de l'intelligence artificielle sont contrebalancés par quelques inconvénients**. Ainsi, le manque de jugement humain. Peu importe à quel point l'IA en matière de cybersécurité devient sophistiquée, les résultats ne sont puissants que proportionnellement par rapport aux données et algorithmes informatiques dont ils découlent. Le fait de s'appuyer sur l'IA laisse entièrement la porte ouverte à des préjugés involontaires et à un manque de responsabilité qui peuvent avoir un impact préjudiciable sur la sécurité et la perception des clients.

Autre souci, **le potentiel de faux positifs**. Cela peut se produire lorsque les systèmes basés sur l'IA font face à de nouveaux problèmes, mais ne disposent pas de l'historique ou du contenu nécessaire pour les analyser correctement. Trop de faux positifs ont le potentiel de submerger les équipes informatiques humaines ou de les amener à rejeter les menaces réelles en leur sein. Les réactions automatisées à des faux positifs peuvent également bloquer les utilisateurs ou les clients inutilement.

QUAND LA SURFACE D'ATTAQUE NE CESSE DE S'AMPLIFIER

Et puis, il n'est pas toujours possible de suivre les nouvelles menaces. Les cybercriminels révisent leurs méthodes tout le temps, avec le potentiel de dépasser les capacités défensives des IA. **En matière de cybersécurité, l'intelligence artificielle nécessite une sensibilisation et des données de formation pour se préparer aux derniers vecteurs d'attaque.** Les pirates informatiques sont en permanence à l'affût de faiblesses, telles que les vulnérabilités Zero-Day qui peuvent être exploitées avant que les systèmes basés sur l'IA ne soient prêts à les résoudre…

« La vraie révolution tient à la vulgarisation des outils d'IA générative aujourd'hui proposés au grand public, ce qui suppose une augmentation de la criminalité », pointe Dominique Mangiatordi. Dans le même temps, la transformation numérique des entreprises est un fait, la dépendance digitale est réelle. Autrement dit, la surface d'attaque ne cesse de s'amplifier. *« Face à ces nouvelles complexités, la maîtrise des risques cyber suppose de gagner une course de vitesse, en accélérant la capacité à anticiper et à identifier la menace, et à reboucler en temps réel les retours d'expérience des crises cyber… »* ■

.

Cyberattaques augmentées, merci l'IA !

L'IA offre de nouvelles opportunités aux criminels qui voient leur récompense augmentée et leur risque d'être repérés diminués. Le sujet de l'IA inquiète autant qu'il interpelle.

Finalement, rien de nouveau. Cela fait plusieurs années que l'IA est utilisée à des fins de malveillance par les cybercriminels. L'usage de l'intelligence artificielle permet d'améliorer des techniques d'attaques déjà utilisées telles que la personnification, le spearphishing, la targetselection ou le persona building.

Connu de tous, le phishing est aujourd'hui de plus en plus efficace grâce aux technologies d'IA disponibles pour générer de façon automatique de fausses informations telles que des vidéos, des articles, des messages ou encore des données personnelles. Cela est possible grâce à une ingénierie sociale qui peut être automatisée en une veille pour identifier les cibles les plus vulnérables à l'aide des données issues des réseaux sociaux. En effet, grâce aux données collectées sur une personne, l'IA peut générer un site web malveillant, mais également des spams personnalisés crédibles donc plus difficilement détectables par les utilisateurs.

D'autres attaques utilisent l'IA pour usurper des identités. S'appuyant sur des injections biométriques, le logiciel de reconnaissance faciale reçoit la donnée corrompue et va la désigner comme authentique. Cette menace est de plus en plus répandue…

DEEPFAKES POUR « PSY-OPS »

Un des exemples les plus répandus d'utilisation de l'IA à des fins malveillantes est celui des deepfakes. Cette technique consiste à utiliser le machine learning pour produire de fausses vidéos les plus réalistes possible. Elle a notamment été utilisée en Ukraine pour des opérations psychologiques (psy-ops) dans le cadre d'une campagne « psy-ops » de désinformation à grande échelle.

Le deep fake est également utilisé pour de l'usurpation d'identité. Cette pratique s'est accentuée pendant la pandémie du Covid19 où les cybercriminels ont eu accès à de nombreuses données biométriques grâce aux visioconférences : une simple photo suffit pour créer une nouvelle photo grâce au « morphing ».

De nouvelles méthodes d'attaques grâce à du « dopage d'IA » ont pu être identifiées. Omniprésente dans notre vie de tous les jours, le machine learning permet d'orienter au mieux les recommandations faites aux internautes grâce aux données recueillies sur nos préférences. Ces robots sont toutefois pris pour cible dans des cyberattaques. En effet, conçu pour altérer les prédictions d'un système de machine learning, l'empoisonnement des données rendu possible grâce aux algorithmes d'intelligence artificielle a pour objectif de corrompre un ensemble de données exploité pour entraîner l'IA.

La dangerosité de l'attaque s'observe dans les possibilités d'influencer l'IA en lui injectant subtilement des scénarios allant dans le sens souhaité. Il est d'ailleurs impossible de remédier à ce type d'attaque lorsque les données corrompues ont été injectées, rendant dès lors le travail de l'IA perdu.

UN OUTIL FACILITATEUR POUR LES CYBERATTAQUANTS

Désormais, plus besoin d'être un expert en codage et réseau, l'IA offre un réel avantage pour quiconque qui souhaite effectuer une cyberattaque. De par la disponibilité et l'accessibilité des techniques, tout un chacun pourrait s'improviser hacker. Les phénomènes de ChatGpT et de Codex participent justement à l'émergence de nouveaux outils bien plus accessibles et bien plus rapides.

Grâce à ces IA, il est possible d'envoyer un mail de phishing contenant un code malveillant en moins de dix minutes avec seulement trois requêtes. Sans utiliser d'IA, la création d'une attaque par phishing peut prendre plusieurs heures à plusieurs jours. S'agissant des étapes techniques d'une attaque, l'outil Codex permet de créer un script shell qui serait inversé sur les machines Windows et qui aurait pour but de détecter des failles SQL, de repérer des exécutions en bac à sable… En somme, cet outil permet de générer du code Python de façon instantanée. L'IA est donc capable de prendre en charge de nombreuses étapes souvent très chronophages dans l'élaboration d'une cyberattaque qui semble presque automatisée.

Nina Schick, auteure, spécialiste de la genAI, au cours de Cybersec Europe 2024

« IA… nous ne sommes pas condamnés à périr ! »

Des craintes… certaines justifiées, d'autres non. Et, en même temps, une nécessité : avancer. Nina Schick, auteure, spécialiste de la genAI, avance quelques pistes de réflexion.

« L'IA n'est pas nouvelle, elle évolue. Comme pour toute nouvelle technologie, viennent d'abord les questions et les réactions négatives, avec ou sans crainte. Une fois cette vague passée, nous considérons le positif, pour la valeur ajoutée, qui sera certainement au rendez-vous… »

Pour Nina Schick, auteure, consultante et conférencière sur la genAI, l'IA est une métatechnologie – la méta fait référence à un composant conceptuel ou fonctionnel actif qui n'est pas visible – qui, pour cette raison, sera utilisée à mauvais escient par de mauvais acteurs. Cela ne fait aucun doute. *« C'est vrai pour toutes technologies, l'IA ne fera pas exception ! »*

Réaliser l'impossible peut faire peur

Si l'on revient à la quête philosophique initiale derrière l'IA, il s'agit toujours de la quête de l'intelligence elle-même. Et l'idée que cela peut être incarné par des entités non biologiques, dotées de systèmes hautement performants, capables de créer et de réaliser des choses que l'on croyait auparavant impossibles, peut faire peur. *« Cela ne signifie pas que l'IA est sensible ou possède une intelligence semblable à celle d'un humain, mais elle peut traiter des informations, prendre des décisions et agir avec des capacités impressionnantes. »*

Il est important de se rappeler que nous concevons et créons ces systèmes. Le récit selon lequel l'IA est une force autonome échappant au contrôle humain est trompeur et supprime notre capacité d'agir, insiste Nina Schick. *« Nous devons piloter l'IA pour créer quelque chose. »*

Et nous n'avons pas le choix. D'ici 2025, 90 % de tous les contenus seront générés par l'IA générative, prédit-elle. Des millions de personnes interagiront avec cette technologie. « *Notre société en sera transformée dans les cinq à dix prochaines années. »*

Une arme… aussi !

Et comme pour tout, il y a des aspects positifs et négatifs. Nina Schick ne doute pas que cette technologie sera utilisée comme une arme.*« Les deep fakes peuvent (re)créer des personnes, qu'il s'agisse de célébrités ou de gens ordinaires. La vie privée et les données deviendront un sujet encore plus controversé. On pourrait s'y perdre... Je prédis une sorte de Far West avant que les décideurs politiques ne s'y mettent et ne réalisent la rapidité et l'impact de cette technologie… »*

Nous ne devons pas, non plus, être trop durs envers nous-mêmes conclut Nina Schick.*« Nous ne savons pas ce que tout cela va apporter, nous ne pouvons donc anticiper, tout anticiper. Cette technologie peut être effrayante pour beaucoup, mais elle apportera tellement d'opportunités… Non, nous ne sommes pas condamnés à périr ! »*

Depuis la Covid-19, les cyberattaques ont augmenté de près de 600%. Ce n'est pas anodin. Cette évolution tient notamment à l'essor de l'IA et aux techniques associées.

L'IA OFFRE DE NOUVELLES OPPORTUNITÉS AUX CRIMINELS

Cette automatisation permet aussi aux cybercriminels de pouvoir attaquer de façon moins coûteuse qu'auparavant. Grâce aux veilles automatisées, à l'optimisation de leurs capacités d'intrusion avec des techniques de phishing intelligent par exemple, les cyberattaquants n'ont plus besoin d'autant de ressources qu'avant. Ce phénomène de transposition du crime terrestre vers le crime cyber grâce aux nouveaux outils ne change pas pour autant la nature de l'acte. L'IA offre de nouvelles opportunités aux criminels qui voient leur récompense augmentée et leur risque d'être repérés diminués -comme l'anonymisation.

Depuis la Covid-19, les cyberattaques ont augmenté de près de 600%. Ce n'est pas anodin. Cette évolution tient notamment à l'essor de l'IA et aux techniques associées. Toutefois, ces dernières sont difficilement quantifiables de par leur nature quasiment indétectable. Il s'agit de facto de « Black figure of crime ».

JUSQU'À POSER DES LIMITES AU DÉVELOPPEMENT DE L'IA...

Face à toutes ces différentes utilisations, qu'elles soient offensives ou défensives, l'IAreste un domaine sur lequel nous avons peu de recul. Si ces atouts sont évidents, ses limites nous montrent toutes les défaillances qui devront être corrigées afin de pallier les risques d'attaques ou même d'éthique.

Actuellement, la gestion des flux informationnels est un atout majeur de l'IA, cette capacité s'insère aussi bien à des fins commerciales que sécuritaires dans des processus techniques de cybersécurité. Cependant, les capacités décuplées des hackers rendent l'IA comparable à une nouvelle arme. Il sera donc question d'équilibrer la place de l'IA dans les processus de cybersécurité mais également pour des questions de réglementations. ■

L'IA explicable, leurre ou réalité ?

À l'heure où les modèles d'IA deviennent de plus en plus complexes, l'IA explicable vise à rendre les résultats de l'intelligence artificielle plus transparents et plus faciles à comprendre.

Certains modèles d'IA de dernière génération sont devenus si complexes dans la façon dont ils décident d'un résultat, que même les experts du domaine ne parviennent pas à comprendre comment ni pourquoi ils prennent ces décisions. C'est ce que l'on appelle souvent le problème de la boîte noire… que l'IA explicable vise à résoudre.

L'IA explicable est un aspect de l'intelligence artificielle qui vise à rendre l'IA plus transparente et compréhensible, ce qui se traduit par une plus grande confiance de la part des équipes bénéficiant de l'IA. Dans un monde parfait, un modèle d'IA robuste peut effectuer des tâches complexes pendant que les utilisateurs observent le processus de décision et auditent toute erreur ou problème.

L'IA EXPLICABLE, BIENTÔT UN ÉLÉMENT ESSENTIEL DES OPÉRATIONS

« L'importance de la compréhensibilité de l'IA augmente, quels que soient l'application et le secteur dans lequel une organisation opère, estime Dynatrace. *L'objectif est de redonner confiance. »* Par exemple, les applications de finance et de santé devront peut-être répondre à des exigences réglementaires impliquant la transparence des outils d'IA. Les préoccupations en matière de sécurité sont au premier plan du développement des véhicules autonomes, et la compréhensibilité du modèle est cruciale pour améliorer et maintenir les fonctionnalités de cette technologie. Plus qu'une question de commodité, l'IA explicable s'imposera comme un élément essentiel des opérations commerciales et des normes de l'industrie.

À mesure que davantage de technologies basées sur l'IA seront développées et adoptées, davantage de réglementations gouvernementales et industrielles seront adoptées. Dans l'UE, par exemple, l'AI Act impose la transparence des algorithmes d'IA, même si sa portée actuelle est limitée. *« L'IA étant un outil si puissant, on s'attend à ce qu'elle continue de gagner en popularité et en sophistication, ce qui entraînera de nouvelles exigences en matière de réglementation et d'explicabilité »*, poursuit Dynatrace.

COMPRENDRE ET MAÎTRISER

On s'inquiète également du biais et de la fiabilité des modèles d'IA. Les hallucinations génératives font beaucoup parler... Mais les modèles d'IA ont une histoire bien établie de biais de production basés sur la race, le sexe, etc. Les outils et pratiques d'IA explicables sont importants pour comprendre et éliminer de tels préjugés afin d'améliorer la précision des résultats et l'efficacité opérationnelle.

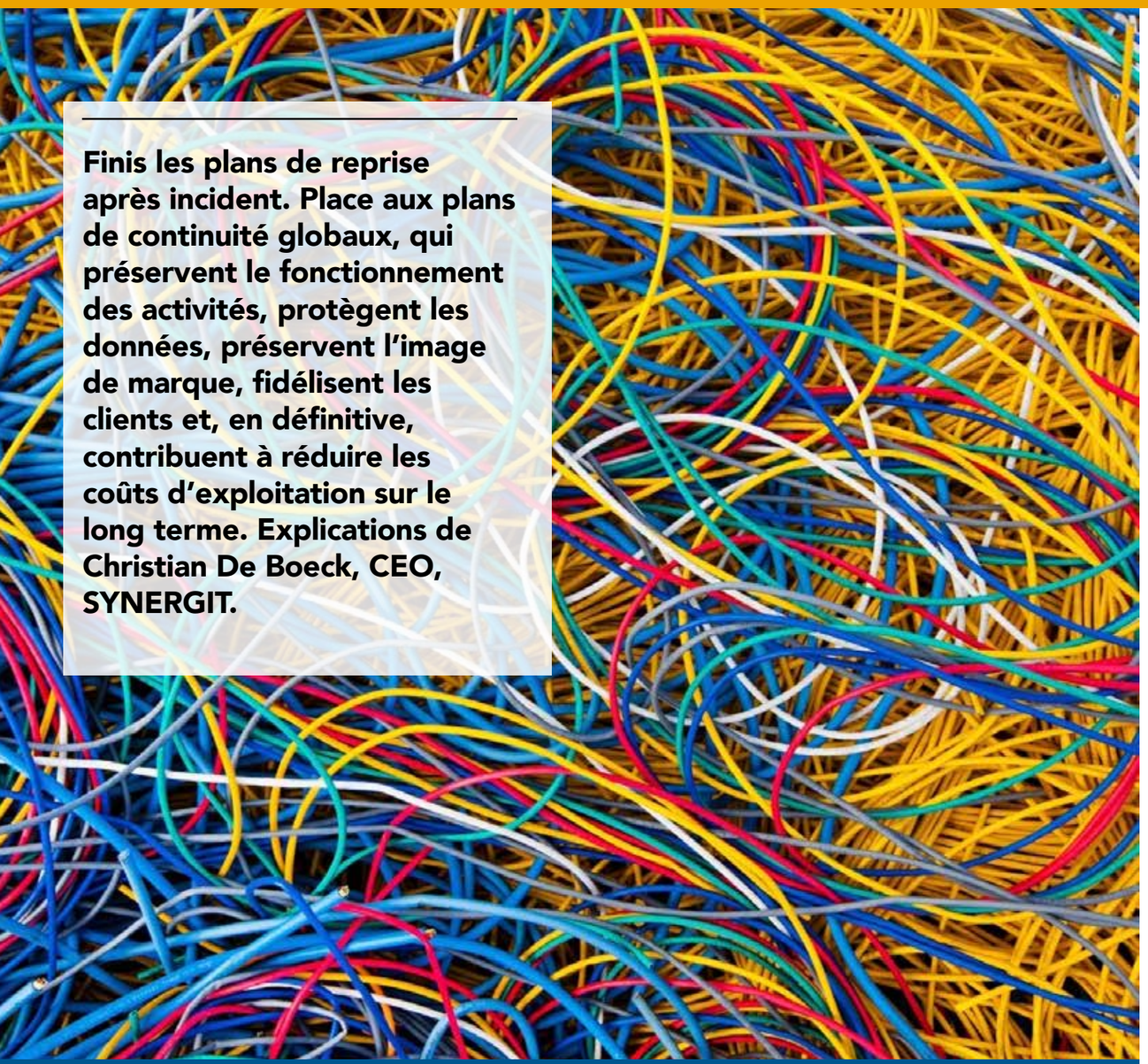
En fin de compte, l'IA explicable consiste à rationaliser et à améliorer les capacités d'une organisation. *« Plus de transparence signifie une meilleure compréhension de la technologie utilisée, un meilleur dépannage et davantage d'opportunités pour affiner les outils d'une organisation »,* ajoute Dynatrace. Par exemple, les applications de finance ou de santé vont peut-être devoir remplir des exigences réglementaires impliquant une transparence des outils d'IA.

CE N'EST QU'UN DÉBUT

À mesure que davantage de technologies basées sur IA seront développées et adoptées, davantage de réglementations gouvernementales et industrielles seront aussi promulguées. L'AI Act impose la transparence des algorithmes d'IA, mais son périmètre reste pour l'instant limité.

En attendant, les méthodologies d'IA explicable en sont toujours à leurs premiers stades de développement. D'ici cinq ans prévoit Dynatrace, de nouveaux outils et de nouvelles méthodes auront fait leur apparition pour comprendre les modèles d'IA complexes, même si ces modèles continuent à progresser et à évoluer.

Un plan de continuité, plus que jamais



Finis les plans de reprise après incident. Place aux plans de continuité globaux, qui préservent le fonctionnement des activités, protègent les données, préservent l'image de marque, fidélisent les clients et, en définitive, contribuent à réduire les coûts d'exploitation sur le long terme. Explications de Christian De Boeck, CEO, SYNERGIT.

Victime d'une cyber-attaque, on le sera. Quand ? Question sans réponse. Aujourd'hui, les entreprises sont de plus en plus conscientes de leur vulnérabilité aux cyberattaques,capables de les paralyser ou de détruire définitivement leurs systèmes informatiques. En outre, la transformation numérique et l'hyperconvergence créent des passerelles imprévues, sources de risques, de vulnérabilités, d'attaques et de défaillances.

Que ce soit à travers l'essor de l'IA ou l'impact de réglementations telles que NIS2, DORA ou bien encore le Cyber Resilience Act, **le plan de continuité n'a jamais été aussi important.** On peut même parler de nouveau statut. Qu'on se rappelle. Les plans de continuité des activités ont fait leur apparition à la suite des plans de reprise après incident, au début des années septante. Dans les années nonante, avec la mondialisation et l'omniprésence de l'accès aux données, les entreprises ont commencé à réfléchir au-delà de la reprise après incident

« Encore trop de campagnes de phishing -développés avec le support d'IA malveillantes- parviennent à ouvrir de larges brèches dans les lignes de défense des entreprises »

et, de manière plus globale, à l'ensemble du processus de continuité des activités.

COMPLEXITÉ NOUVELLE

Désormais, les plans incluent des moyens de se défendre, de protéger les applications et les données critiques et de se remettre d'une violation ou d'une défaillance de façon contrôlée et mesurable. C'est précisément ce qui est demandé avec les nouvelles réglementations. *« Le fait de disposer d'un plan de continuité des opérations réduit les temps d'indisponibilité et permet d'introduire des améliorations durables dans la continuité des opérations, la reprise après incident IT, les capacités de gestion des crises et la conformité aux réglementations »*,**commente Christian de Boeck, CEO, SYNERGYT.**

En même temps, l'élaboration d'une stratégie de plan de continuité est devenue plus complexe. De fait, les systèmes sont de plus en plus intégrés et répartis dans des environnements IThybrides, ce qui crée des vulnérabilités potentielles. L'interconnexion de systèmes stratégiques pour gérer les exigences croissantes complique la planification de la continuité des opérations, ainsi que la reprise après incident, la résilience, la conformité aux réglementations et la sécurité. Lorsqu'un maillon de la chaîne se brise ou est attaqué, l'impact peut se répercuter dans l'ensemble de l'entreprise.

POLITIQUES D'AUDIT ANNUEL ET DE CONTRÔLE RÉGULIER DES RISQUES

Les nouvelles réglementations intègrent des obligations claires. Dans le détail, NIS2 et DORA imposent des exigences accrues. Notamment

la mise en place de **politiques d'audit annuel et de contrôle régulier des risques** pesant sur les systèmes d'information afin d'identifier leurs éventuelles faiblesses, défaillances ou lacunes, et de mettre rapidement en place des mesures correctives. Il s'agira également de produire des **rapports réguliers sur les actifs informatiques,** les audits de sécurité, les incidents cyber survenus, les actions entreprises pour y remédier, etc. Et, bien sûr, établir des plans de reprise après incident ou, mieux, de continuité d'activité.

*« Dès lors, la question du plan de continuité reste un sujet brûlant : la durée moyenne de redémarrage suite à une cyber-attaque est le plus souvent totalement hors délai par rapport aux besoins et aux attentes du business,*constate Christian de Boeck. *Aussi, en marge des plans de redémarrage -basés par exemple sur des sauvegardes off-line et/ou immuable-, il est crucial de constituer des plans de continuité pouvant garantir un redémarrage dégradé des fonctions les plus critiques qui permettront la survie de l'entreprise. »*

La tendance est aux plans de continuité des opérations globaux (ou résilience opérationnelle), qui préservent le fonctionnement des activités, protègent les données, préservent l'image de marque, fidélisent les clients et, en définitive, contribuent à réduire les coûts d'exploitation sur le long terme. *« Ces plans devront faire abstraction des moyens IT 'habituels' reliés et connectés à l'entreprise. Ils seront préparés, documentés et exercés en profondeur pour éviter toute déconvenue lorsqu'une crise éclatera. Ces exercices veilleront à ce que les objectifs attendus soient rencontrés, mais plus encore à ce que chaque intervenant sache exactement que faire le moment venu… »*

COMBINER L'IA ET L'HUMAIN

Il ne faut pas négliger non plus tous les aspects liés à la gestion de crise : ici aussi les attaques peuvent se faire insidieuses et tenter d'orienter les décisions prises par les personnes aux commandes pendant ces périodes critiques dans la direction souhaitée par les attaquants. *« A nouveau, un programme d'entraînement rigoureux permettra de réduire les risques en développant des automatismes et des arbres décisionnels prêts à l'emploi,* continue Christian de Boeck. *Alors, bien sûr, l'IA a ici un grand rôle à jouer, tant pour la détection que l'aide à la décision et aux exercices, mais surtout, combiner l'humain et la machine permettront d'avoir des schémas cognitifs différents qui garantiront une résilience maximale. »*

Naturellement, tout ceci ne sert à rien sans une intégration rigoureuse avec une conscientisation poussée des employés, fournisseurs et partenaires de l'entreprise. *« Encore trop de campagnes de phishing -développés avec le support d'IA malveillantes- parviennent à ouvrir de larges brèches dans les lignes de défense des entreprises. Sur ce plan, rien n'a changé : le facteur humain reste un maillon faible qui doit être régulièrement entraîné contre ce type de manipulation. »* ■

« Le fait de disposer d'un plan de continuité des opérations réduit les temps d'indisponibilité et permet d'introduire des améliorations durables dans la continuité des opérations, la reprise après incident IT, les capacités de gestion des crises et la conformité aux réglementations »

GenAI et cybersécurité, entre opportunités et nouveaux défis

Automatisation des tâches répétitives,productivité accrue, aide à la décision… Les bénéfices de la genAI au profit de la cyber-sécurité sont nombreux. Les défis pour la mettre en œuvre aussi. Explications de Koen Segers, Managing Director BeLux Dell Technologies

La cybersécurité franchit un cap décisif avec l'émergence de l'intelligence artificielle générative.La capacité de la genAI à comprendre, apprendre et mettre en œuvre des connaissances comme le ferait un être humain, représente une assistance précieuse dans la protection des environnements informatiques, mais offre aussi aux cybercriminels de nouveaux vecteurs d'attaque.

« Les défis sont considérables et incitent à se questionner sur les actions à entreprendre pour générer de la valeur de manière responsable, **constate Koen Segers, Managing DirectorBeLux, Dell Technologies.** *Face à cette révolution technologique, il est important de reconnaitre son potentiel, tout en veillant à ce que ces avancées reflètent nos valeurs sociétales. »*

GÉRER LES RISQUES LIÉS À LA genAI

À mesure que les capacités de l'IA générative se développent, la sécurité devient un enjeu prioritaire. Les cybercriminels peuvent exploiter sa rapidité et les avantages liés à l'automatisation, afin de découvrir plus rapidement les vulnérabilités de leurs cibles, faire évoluer les logiciels malveillants en temps réel et créer des emailings de phishing et d'usurpation numérique plus efficaces. Pour cette raison, les systèmes de genAI doivent être accompagnés de mesures de sécurité appropriées pour contrer les tentatives de fraude et les risques de deepfake.

« La sécurisation de la genAI commence par la mise en œuvre d'une infrastructure basée sur la confiance, du edge jusqu'à l'utilisateur en passant par la gestion des données, continue Koen Segers. L'objectif est de mettre en place des mécanismes de contrôle d'accès robustes qui empêchent tout accès préjudiciable et toute utilisation potentielle malveillante du système. Pour sécuriser les données, des fonctionnalités telles que la classification, le chiffrement, ainsi que le stockage et la transmission sécurisés sont nécessaires. »

La contribution humaine joue également un rôle essentiel. Des audits réguliers, des comportements permettant d'identifier les anomalies du système, ainsi que des techniques visant à atténuer les préjugés et à intégrer des

« La clé est de tirer pleinement parti de ces avantages tout en gérant les risques de manière proactive et vigilante. Des mesures de sécurité robustes, une surveillance continue et une approche flexible et constamment adaptée au sujet de la confidentialité des données et de l'éthique sont essentielles. »

« Les défis sont considérables et incitent à se questionner sur les actions à entreprendre pour générer de la valeur de manière responsable. Face à cette révolution technologique, il est important de reconnaitre son potentiel, tout en veillant à ce que ces avancées reflètent nos valeurs sociétales. »

principes éthiques sont fondamentaux pour la prévention des risques.

LA genAI POUR UNE CYBERSÉCURITÉ RENFORCÉE

L'industrie se mobilise pour relever les défis de la genAI, qui offre la perspective de devenir un partenaire incontournable dans le domaine de la cybersécurité, ouvrant ainsi la voie à une protection renforcée contre les menaces informatiques. *« La genAI permet d'analyser d'importantes quantités de données de sécurité spécifiques à une organisation, de formuler des prédictions, et évolue en permanence,* poursuit Koen Segers. *Cela permet aux équipes de cybersécurité de mieux anticiper les menaces, en détectant notamment des anomalies dans le trafic réseau ou du contenu suspect dans les e-mails. De plus, l'IA générative a la capacité de prédire les menaces futures, identifier les vulnérabilités en tirant des enseignements d'incidents passés et de flux de renseignements sur les menaces. »*

L'automatisation peut transformer notre approche de la sécurité, en particulier dans les domaines de la prévention et du contrôle de la détection. En automatisant la détection des menaces, la genAIréduit le temps de découverte et de réponse aux tentatives d'attaque, et en atténue de ce fait les dommages potentiels. L'automatisation des tâches routinières de cybersécurité, comme le reporting d'incidents ou le partage des menaces, permet aux équipes de sécurité de se concentrer sur des tâches plus stratégiques.

Enfin, la création de contenu n'est peut-être pas la première fonctionnalité qui vient à l'esprit lorsque l'on évoque les applications de la genAIpour la cybersécurité, mais il s'agit d'une capacité très utile en matière de formation et sensibilisation des utilisateurs. Utilisée pour personnaliser les modules de formation, la genAI permet de baser les critères de personnalisation sur les rôles des utilisateurs finaux, les comportements passés et les menaces courantes auxquelles ils peuvent être confrontés. *« Ce niveau de personnalisation renforcé de la formation permet de réduire le nombre d'erreurs humaines, qui sont à l'origine de nombreux incidents »*, estime encore Koen, Segers.

UNE VISION PRAGMATIQUE

La genAI engendre de nouveaux défis qui incitent à repenser et à faire évoluer les stratégies de cybersécurité. Elle offre également la perspective d'améliorer la détection et les réponses aux menaces, ainsi que d'apporter des capacités prédictives et une efficacité opérationnelle accrue.

« La clé est de tirer pleinement parti de ces avantages tout en gérant les risques de manière proactive et vigilante, conclut Koen Segers. *Des mesures de sécurité robustes, une surveillance continue et une approche flexible et constamment adaptée au sujet de la confidentialité des données et de l'éthique sont essentielles. Alors que nous entrons pleinement dans l'ère de la genAI, l'évolution de l'IA et de la cybersécurité se poursuivra dans une relation symbiotique. »* ■

Pourquoi partager tant de données personnelles... inutiles ?

Partager des données personnelles avec une entreprise peut paraître innocent. Pour Cindy Wubben, Information Security Officer, VismaBenelux, nous en partageons trop. Beaucoup sont inutiles.

Les cyberattaques et les fuites de données sont quasi quotidiennes. Les scénarios sont souvent les mêmes. Les conséquences aussi. La solution réside non seulement dans la sécurité que les organisations assurent elles-mêmes, mais également dans la manière dont elles traitent les données de leurs clients. A-t-on vraiment besoin de toutes ces données ?

Rarement, pareille question est posée. Et pourtant… Voici quelques mois, une violation de données chez VF Corporation, la société mère de la marque de vêtements The North Face, a touché environ 35 millions de clients. Le butin ? Des données personnelles telles que des adresses e-mail, des noms, des numéros de téléphone et des adresses de livraison. Heureusement, les hackers n'ont pas pu voir les coordonnées bancaires et de carte de crédit des clients. N'empêche.

« Nous entendons de plus en plus souvent ce genre d'histoires, **constate Cindy Wubben, Information Security Officer, Visma Benelux.** *Après tout, les cyberattaquants peuvent gagner beaucoup d'argent grâce au vol de données personnelles. Ils peuvent par exemple vendre les données via le dark web à d'autres cybercriminels, qui, à leur tour, abusent de ces données. »* Cela inclut l'envoi d'e-mails de phishing très réalistes et crédibles. Ou ils peuvent utiliser les données pour accéder à d'autres comptes. Dans le scénario le plus négatif, les pirates peuvent même s'emparer de l'identité ou commander des articles au nom de l'utilisateur.

« Les consommateurs, aussi, doivent être plus critiques et poser davantage de questions sur les informations demandées par une entreprise... »

BEAUCOUP DE DONNÉES PERSONNELLES NE SONT PAS NÉCESSAIRES

À première vue, partager des données personnelles avec une entreprise peut paraître innocent, mais cela peut avoir des conséquences considérables. **Si cette entreprise n'a pas installé la dernière mise à jour de sécurité, il n'est pas si difficile pour les cybercriminels d'accéder à ces données sensibles.**

« Tout d'abord, il est crucial que les entreprises mettent leur sécurité en ordre, afin de ***limiter au maximum le risque de violation de données.*** *Mais elles feraient aussi bien de se demander de quelles données elles ont réellement besoin pour servir un client »,* commente Cindy Wubben.

Surtout dans un environnement en ligne, il est logique que les entreprises aient besoin de demander des informations pour déterminer qui est client. Considérez des données telles que le nom, l'adresse et le lieu de résidence d'un client - ce que l'on appelle les données de nom et d'adresse. *« Or, cela ne s'arrête souvent pas là. Les entreprises demandent davantage d'informations, comme le numéro de téléphone,*

« Après tout, les cyberattaquants peuvent gagner beaucoup d'argent grâce au vol de données personnelles. Ils peuvent par exemple vendre les données via le dark web à d'autres cybercriminels, qui, à leur tour, abusent de ces données. »

le sexe, la profession, la date de naissance ou la nationalité. »

La plupart des informations sont utiles aux entreprises, notamment dans le contexte du marketing. *« Connaitre la date de naissance des clients permettra d'envoyer un e-mail personnalisé le jour de leur anniversaire. Toutefois, ces informations sont loin d'être nécessaires pour garantir un bon service.* ***Pourquoi ne pas se limiter aux informations de base suffisantes pour générer du business ? »***

PENSEZ AUX INFORMATIONS QUE VOUS DEMANDEZ/PARTAGEZ

Les entreprises doivent donc cesser de demander des données personnelles dont elles n'ont pas forcément besoin. Si ces informations finissent à l'extérieur, cela n'est pas seulement gênant pour le consommateur, ça l'est aussi pour les entreprises elles-mêmes qui peuvent voir leur réputation se ternir.

« Les consommateurs, aussi, doivent ***être plus critiques et poser davantage de questions sur les informations demandées*** *par une entreprise,* estime Cindy Wubben. *Par exemple, ne remplissez les champs obligatoires que lors du paiement ou de la création d'un compte. »*

Si nous voulons créer un environnement numérique sain, nous devons **être conscients de nos droits** en matière de confidentialité et faire des choix éclairés concernant les données personnelles que nous partageons. ■

Centre de données, coffre-fort de données

Un centre de données externe et colocalisé rend le concept de coffre-fort de données plus accessible à de nombreuses entreprises. C'est l'idée que défend -avec succès-Digital Realty pour renforcer votre ligne de défense.

Les données sont le carburant de toute organisation moderne. Sans cela, l'activité risque de s'arrêter complètement. Protéger ces données est essentiel, mais il faut aujourd'hui aussi penser à la cyber-reprise. En somme, que peut-on faire pour fonctionner à nouveau le plus rapidement possible après une crise ? **La sauvegarde des données critiques dans un coffre-fort pourrait devenir une nécessité dans les années à venir.** Dans ce cas, estime Digital Realty, un centre de données externe constitue l'emplacement idéal pour intégrer un tel coffre-fort de manière sûre et abordable.

Le nombre de cybermenaces augmente chaque jour. Les dommages causés aux entreprises concernées ne peuvent plus être sous-estimés. Les risques sont connus : des pertes financières vertigineuses aux dommages irréparables à la réputation des clients et partenaires. Et nous ne parlons même pas des amendes que les instances publiques imposent aux entreprises qui ne respectent pas les réglementations les plus récentes. Entre-temps, de nombreuses entreprises réalisent qu'**une cyberattaque n'est qu'une question de temps…**

Sheltered Harbor est une initiative américaine qui aide les organisations disposant de données critiques – comme les entreprises du monde financier ou de la santé – à développer une stratégie solide. Concrètement, le concept s'articule autour de trois principes. Tout d'abord, il doit y avoir un coffre-fort de données où est stockée une sauvegarde de toutes les données importantes. Deuxièmement, les organisations ont besoin d'un plan de cyber-reprise. Ce plan décrit comment ils peuvent rapidement remettre l'entreprise en marche avec les données stockées dans le coffre-fort. Enfin, les entreprises doivent faire réaliser un audit par un organisme indépendant qui peut confirmer qu'elles ont fait tout leur possible pour protéger leurs données.

OÙ PLACER UN COFFRE-FORT DE DONNÉES ?

En raison de l'énorme impact d'une cyberattaque sur le monde des affaires et sur la société en général, la législation n'est pas en reste. Le règlement européen DORA, par exemple, soumet la sécurité des institutions financières à des engagements stricts. NIS2, autre directive européenne, oblige les organisations à atteindre un certain niveau de sécurité. Les dirigeants d'entreprises qui ne s'y conforment pas s'exposent non seulement à des sanctions financières, mais aussi à des peines de prison.

La plupart des législations concernant la sécurité informatique sont conformes à Sheltered Harbor. Cela signifie qu'un coffre-fort de données (ou Cyber Recovery Vault) peut offrir une valeur ajoutée. Actuellement, peu d'entreprises disposent d'un tel système de sécurité pour leurs données. Principalement parce qu'il s'agit d'une entreprise complexe et coûteuse. Concrètement, acheter le matériel nécessaire et l'installer dans un endroit bien sécurisé. **Tout comme une banque offre la possibilité de stocker des bijoux de valeur, un centre de données externe peut faire de même pour les données les plus précieuses.**

SÛR ET ABORDABLE

Pourquoi un centre de données externe ? D'abord parce que c'est, par nature, un lieu sûr.

« La sauvegarde des données critiques dans un coffre-fort pourrait devenir une nécessité dans les années à venir. Dans ce cas, un centre de données externe constitue l'emplacement idéal pour intégrer un tel coffre-fort de manière sûre et abordable. »

Avant de pouvoir accéder à votre coffre-fort à la banque, vous devez passer les contrôles de sécurité. Un centre de données est également une installation dans laquelle vous ne pouvez pas simplement accéder, commente Digital Realty. On peut comparer un centre de données à un hôtel hautement sécurisé pour les données. Avec de nombreuses salles à louer ou faire aménager comme coffre-fort de données.

Comment ça marche exactement ? Tout commence par l'identification des données commerciales et critiques. Quelles données devez-vous récupérer et dans quel ordre ? Les données passent ensuite du centre de données partagé à une « zone de transit » où toutes les données critiques du monde entier sont collectées, puis via un espace d'air jusqu'au coffre-fort numérique. Un tel entrefer est une liaison qui peut être comparée à un pont toujours ouvert et qui n'est abaissé que pour permettre une circulation à sens unique vers la voûte, illustre Digital Realty. Le coffre-fort contrôle le pont et n'est pas connecté au monde extérieur, les pirates ne peuvent donc jamais en prendre le contrôle.

Un autre avantage d'un coffre-fort numérique dans un centre de données est le fait que vous devez acheter moins de matériel vous-même. La plupart des fournisseurs de ce type de technologie ont de nombreux clients qui ont besoin d'une salle de récupération ou d'une salle blanche - un environnement informatique nu dans lequel les entreprises peuvent restaurer des systèmes ou exécuter des tests. Si vous pouvez accueillir des dizaines de clients dans une poignée de salles de réveil, ces entreprises économiseront évidemment beaucoup de coûts.

Un autre espace que vous pouvez partager est la « war room », une pièce aménagée en salle de réunion et connectée au coffre-fort de données pendant le processus de récupération, afin que les spécialistes puissent faire leur travail. L'espace de travail est toujours prêt. On ne perd donc pas de temps à mettre en place des postes de travail à partir desquels l'organisation peut être restaurée. De plus, tout est disposé de manière uniforme. Ce qui fonctionne à Bruxelles s'applique également ailleurs dans le monde.

UN ÉCOSYSTÈME DE PARTENAIRES SOLIDE

Bien sûr, cela implique quelque chose pour l'organisation en question. Outre le matériel et les logiciels, vous avez également besoin de connaissances et d'expertise. Et les profils qui disposent de cela sont généralement rares et coûteux. Heureusement, tous les grands acteurs sont déjà présents dans les centres de données comme ceux de Digital Realty. **Les entreprises bénéficient ainsi d'un écosystème de partenaires puissant et étendu qui peut les aider, afin qu'elles n'aient plus à se soucier que de leurs données.**

Un centre de données externe et colocalisé rend le concept de coffre-fort de données plus accessible à de nombreuses entreprises. Quoi qu'il en soit, les organisations doivent plus que jamais mettre l'accent sur la cyber-reprise. Aucune entreprise ne peut se permettre d'être « down » pendant deux semaines après une cyberattaque. Avec un bon plan de reprise, vous pouvez reprendre vos activités après 48 heures en moyenne. ■

Porsche Club
Belgium

Rejoignez l'un des plus anciens Porsche Club au monde.

Fondé en 1953, le Porsche Club of Belgium est le troisième des Porsche Clubs au monde. Plus qu'une passion pour Porsche, nous valorisons la convivialité, le partage entre passionnés, le fair-play sur route et sur circuit, ainsi que la culture du luxe et de l'exception. Rejoindre notre club, c'est entrer dans la famille Porsche, avec son histoire, ses victoires et son prestige. Notre association accueille tous les passionnés et propriétaires de cette marque légendaire.

Porsche Club of Belgium - Grand Route 395 - 1620 Drogenbos
info@porsche-club-belgium.be - www. porsche-club-belgium.be
porscheclubbelgium - porscheclubbelgium