LES CINQ GRANDES TENDANCES DE LA CYBERSÉCURITÉ DE DEMAIN

MARC DARMON (83)
directeur général adjoint de Thales - Systèmes d'information et de communication sécurisés, président du comité stratégique de filière « Industrie de sécurité »

La multiplication des objets connectés, des interconnexions, la migration vers le cloud sont à la source d'une plus grande fluidité de l'information et d'un traitement toujours plus performant et agile des données, au cœur de la transformation numérique des États et des organisations. Les risques en matière de cybersécurité et la nécessité de protections efficaces n'en sont que plus grands.

Christophe Castaner et Marc Darmon lors des deux signatures du contrat de filière au forum international de cybersécurité le 29 janvier 2020.

On peut ainsi identifier cinq grandes tendances qui posent question en matière de cybersécurité et nous poussent à adapter, automatiser, industrialiser, voire réinventer nos capacités de protection et de défense.

Protection de la vie privée : de la contrainte légale à la proposition de valeur

L'accroissement considérable des données va de pair avec une demande légitime de la part des consommateurs pour plus de contrôle et de traçabilité de leurs données : de mieux en mieux informés de leurs droits, de l'existence du Règlement général sur la protection des données ou d'autres législations du même type (comme PIPEDA au Canada ou PDPA à Singapour), ils questionnent la manière dont les données sont hébergées et traitées, et se demandent qui peut y avoir accès. L'opinion publique

REPÈRES

L'actuelle transformation numérique s'accompagne d'une augmentation importante des risques en matière de cybersécurité : la surface d'attaque s'est considérablement étoffée, et le volume, la valeur et la criticité des données traitées font de ces dernières des cibles de choix. Plus les systèmes d'information collectent et traitent les données, plus ils sont vitaux à notre économie, à notre défense, au bon fonctionnement de nos sociétés, plus ils deviennent attractifs pour les cyberattaquants, que leur origine soit criminelle, terroriste ou étatique. Les cyberattaques sont devenues plus intelligentes, plus coordonnées, plus industrialisées, se rapprochant parfois de véritables opérations militaires dans la planification et l'exécution. Ainsi, garder l'initiative sur des cybermenaces en perpétuelle évolution est une gageure : cela nécessite une connaissance fine et profonde des attaquants et de leurs techniques, une parfaite maîtrise des technologies actuelles et une véritable vision de notre futur numérique. La cybersécurité est ainsi devenue l'oxygène de toute transformation numérique : c'est sur elle que repose le capital-confiance numérique de nos institutions.

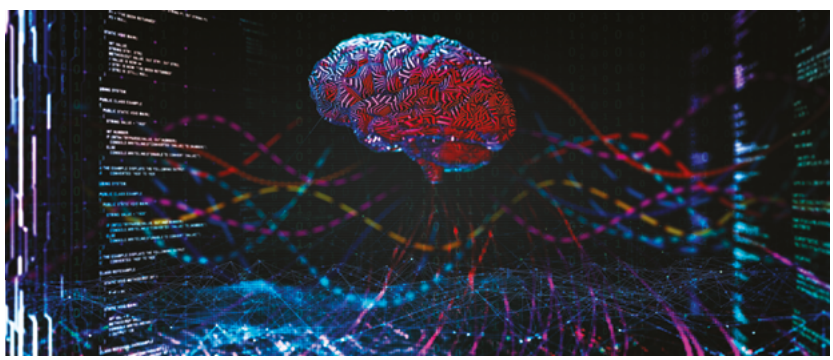
accepte de moins en moins les fuites de données, qui tous les jours font la une des médias. On estime qu'en 2020 le montant des amendes et des dédommagements dépassera trois milliards d'euros, soit le double de 2019. Il ne s'agit pas uniquement d'une affaire de conformité à la législation ou de contrainte légale : la cybersécurité représente désormais une vraie proposition de valeur, pouvant constituer un différenciateur important sur n'importe quel marché, en apportant une garantie de confiance.

Le cloud, plus que jamais

Le *cloud* est devenu, en quelques années, un levier indispensable de la transformation numérique. À l'instar des formations météorologiques traversant les frontières, les solutions de *cloud* sont nombreuses et variées, privées ou publiques, nationales ou étrangères. Le choix de l'environnement utilisé pour le stockage de données se doit d'être directement lié à la valeur et à la criticité de ces dernières, avec un équilibre maîtrisé entre la disponibilité des données, leur sécurité et l'indépendance vis-à-vis du fournisseur. La question de la souveraineté des données critiques est désormais un facteur crucial du choix de *cloud* du fait, notamment, de mesures extraterritoriales comme le *Cloud Act*.

5G et hyperconnectivité

La 5G porte assez mal son nom : en effet, l'évolution technologique qu'elle amène a peu de chose en commun avec les précédentes 2G, 3G ou 4G. En rendant possible la connectivité de tous les réseaux, systèmes, objets et capteurs, elle va permettre le développement considérable de nouveaux services, comme les voitures autonomes, la télémédecine, ou des évolutions majeures dans le domaine de la sécurité publique, de l'industrie, de l'énergie, de la banque, etc. Le développement de la 5G et de technologies associées constitue ainsi une question autant de souveraineté nationale que de stratégie économique. Du fait d'une connectivité sans précédent, la liste des cibles de cyberattaques risque également de s'allonger, avec des attaques capables de se propager plus facilement et plus rapidement, en particulier sur des systèmes critiques. Au-delà de la fiabilité des équipements 5G, nous devrons nous poser la question de la protection de nos systèmes en général et en particulier des objets connectés, dont la sécurisation par conception ne sera pas nécessairement la priorité de tous dans la course à la connectivité.



© MF3d

L'intelligence artificielle (IA), en maîtriser le potentiel

Comme toute technologie, l'intelligence artificielle n'est ni bonne ni mauvaise en soi : seul l'est l'usage qui en est fait. La cybersécurité en est la parfaite illustration. En effet, certains attaquants utilisent désormais l'IA pour sélectionner leurs cibles, déterminer les meilleures failles à exploiter et passer autant que possible sous le radar des systèmes de détection. En contrepartie, l'IA permet d'améliorer les capacités de détection et de réaction, avec une promesse de performance inégalée. En permettant aux humains de se concentrer sur d'autres tâches, elle est aussi une des réponses possibles à la pénurie de talents dans le domaine cyber. Cette utilisation de l'IA doit reposer sur un cadre éthique solide, garantissant en particulier son explicabilité, comme a pu l'entreprendre Thales avec la charte « TrUE AI » (*Transparent / Understandable / Ethical*) lancée en 2019.

Le chiffrement à l'ère quantique

Un des plus grands défis en matière de cybersécurité est très certainement le développement de l'informatique quantique, bientôt capable de résoudre des problèmes mathématiques nécessitant des puissances de calcul inédites. Après l'avance significative réalisée par Google en 2019, avec un problème résolu en trois minutes là où même un supercalculateur aurait mis plus de 10 000 ans, la démocratisation de l'informatique quantique et de son incroyable puissance de calcul n'est plus qu'une question de temps. Avec une conséquence majeure : le risque d'obsolescence des mécanismes de chiffrement ou de signature. C'est pourquoi il est indispensable de travailler, dès maintenant, sur de nouveaux algorithmes « post-quantiques », résistant à ces nouvelles puissances.

Big data, intelligence artificielle, *cloud*, etc. : ces technologies clés sont au cœur des travaux du Comité stratégique de filière (CSF) des industries de sécurité, créé en novembre 2018. Le CSF et le secteur qu'il représente ont un rôle clé à jouer dans la maîtrise du digital et le développement d'une économie numérique de pointe, en France et au-delà des frontières. Nous travaillons sur ces grands défis d'un avenir proche avec un maître mot : la confiance. Et, parce que les cybermenaces ne connaissent pas de frontières, les solutions de sécurité ne peuvent plus se limiter à des acteurs isolés ou aux frontières nationales. Notre vision et nos capacités doivent s'étendre au village planétaire pour devenir *in fine* une vitrine de la France à l'international, capable de fédérer proactivement les autres acteurs de la sécurité au niveau européen.