Stordata

Cybersécurité : atteindre l'équilibre

La sensibilisation à la cybersécurité, un processus en continu

La cybersécurité a changé. Poncif ? Peut-être. Mais est-on bien certain de savoir mesurer toutes les implications de cette étonnante évolution ? Peut-être pas.

Depuis les dernières directives issues de la stratégie européenne de cybersécurité, les RSSI ont enfin obtenu, quasiment du jour au lendemain, l'entière attention de leur direction. Jusqu'ici, ne fallait-il pas se démener pour que le budget cyber soit à la hauteur des menaces ? Pour que les décisions d'achat ou de souscription cessent d'être guidées par les effets de mode ? Évidemment, ce type d'écueils se rencontrent encore. Cela dit, de moins en moins car les professionnels de la cybersécurité d'entreprise sont dorénavant pris très au sérieux.

Si les échanges entre RSSI et métiers sont encore succincts et varient en fonction des organisations et de leur maturité, une synergie entre sécurité (à travers le RSSI) et métiers (business, infrastructure ou encore production) prend forme notamment dans des cadres communs comme le règlement DORA ou l'approche par les risques. Cette écoute attentive et ses effets ne s'exercent pas qu'en interne et rejaillissent sur toute l'activité de conseil et d'intégration de solutions de cybersécurité. Le rôle du RSSI prend de l'épaisseur, sa fonction devient stratégique, son budget s'étoffe suffisamment pour aiguiser son intérêt et son appétit pour plus de préconisations et de nouvelles solutions, plus conformes à l'état de la menace et du risque d'aujourd'hui.

> Les incidents cyber font désormais partie du top 3 des risques d'entreprise avec l'interruption d'activité et les catastrophes naturelles.
>
> Baromètre des risques Allianz

> Pour les PME et les ETI spécifiquement, l'environnement de risques se complexifie et le risque cyber est désormais formellement identifié par une entreprise sur trois.
>
> Rencontres AMRAE 2024 : Baromètre QBE – OpinionWay

La réglementation à l'œuvre

Les moteurs de cette évolution majeure ? Les cyberattaques et leur corollaire, la réglementation. Pour mémoire, les premières mesures majeures en la matière ne datent plus d'hier. Qu'il s'agisse de la loi de programmation militaire LOI n° 2013-1168 du 18 décembre 2013 qui fixait déjà un cadre réglementaire pour protéger les infrastructures critiques contre les cyberattaques ou la directive NIS 1, (directive européenne 2016/1148 Network Information Security) transposée en 2018 dans le droit français, les entreprises ont progressivement été

sensibilisées à la menace, relayant ainsi les appels du pied, de plus en plus insistants, des responsables de la sécurité informatique.

Une course à l'armement cyber

Avec la démocratisation des services en ligne, la valeur croissante de la donnée, l'augmentation des échanges numériques, la massive informatisation de l'entreprise et la dissémination des systèmes d'information, la hausse des incidents de sécurité n'a fait que suivre le cours normal de l'évolution des méthodes de travail. Plus médiatisée également, cette tendance au risque cyber a profondément transformé les équilibres et contribué à répartir autrement l'effort financier dans les organisations.

Conséquence somme toute prévisible de l'augmentation du budget de la direction des systèmes d'information, un empilement de solutions de cybersécurité très hétérogènes contribuant moins à la sécurité globale qu'à une perte de la visibilité des actifs de l'entreprise et une fausse impression de sécurité.

> « C'est un effet ligne Maginot que les entreprises ont vécu et vivent encore sous certains aspects. Cette barrière de sécurité, bien trop fixe, se révèle incapable de soutenir les mutations numériques en cours. La cybersécurité nous parle de stratégie, pas des moyens techniques à mettre en œuvre. »
>
> Simon AMIOT,
> Avant-vente cybersécurité
> STORDATA

Le souhait de la consolidation

Aujourd'hui toutefois, les organisations entrent dans une phase de stabilisation, notamment motivée par une baisse des budgets IT, dans laquelle les RSSI cherchent à rationaliser le parc de solutions de cybersécurité. L'exercice demeure complexe : l'évolution très rapide des usages ne permet pas toujours de différencier l'accessoire de l'indispensable.

L'effort de consolidation se heurte également à l'hyperspécialisation des acteurs de la cybersécurité français et européens.

> « En France, il existe très peu d'éditeurs en mesure d'intervenir sur plusieurs sujets avec la même efficacité. Je n'ai par exemple à l'esprit qu'un seul acteur capable de gérer à la fois l'EDR et la protection du réseau. »
>
> Simon AMIOT

Un seuil d'inefficacite des outils cyber

Au-delà d'une cinquantaine d'outils de cybersécurité, les entreprises réduisent leurs capacités à se défendre. Ce résultat est issu du « Cyber Resilient Organization Report » de IBM de 2020. En 5 ans, les organisations sont parvenues à réduire le nombre de solutions, passant en moyenne de 45 à 32, tous domaines confondus (réseau, cloud, postes de travail, IoT, mobilité, surface d'attaque, etc.). Toutefois, les RSSI témoignent d'une perte de contrôle sur les solutions autonomes en place et regrettent le manque de consolidation.

Naturellement, il reste aux organisations le choix de confier leur cybersécurité à l'un ou l'autre géant de la cyber américain (ou éventuellement israélien), dont la croissance externe, généralement offensive, lui permet de couvrir la quasi-totalité des thématiques considérées. Cela ne résout toutefois pas les problématiques liées à la souveraineté et aux limites budgétaires et renforce considérablement le risque d'enfermement propriétaire que les entreprises cherchent pourtant à fuir autant que possible.

Baromètre du sentiment de sécurité

Une étonnante confiance dans leur cybersécurité !

Les entreprises se font-elles confiance vis-à-vis du risque cyber ? Oui, si l'on en croit les derniers sondages, les entreprises s'estiment plutôt bien préparées à faire face, en amont, aux cyberattaques et en aval à leurs éventuelles conséquences. Ce haut degré de confiance s'explique par la mise en place de sauvegardes régulières et la sensibilisation des collaborateurs.

Par ailleurs, on constate depuis l'année 2023 que le nombre de cyberattaques réussies n'a plus augmenté en France, contrairement aux tentatives (source : Baromètre QBE – OpinionWay). En l'occurrence, la perception des entreprises semble s'aligner avec la réalité. Et de fait, les entreprises croient profondément à l'existence du risque cyber et ont gagné, en réponse, une maturité technique de bon aloi.

Restent la sophistication continue des méthodes d'attaques, l'exploitation de l'intelligence artificielle au service des menaces qui remettent en question, de façon permanente, les mesures de sécurité. Les plans de sauvegarde sont-ils à la hauteur des risques qui pèsent sur les backups de données ? La confiance est chose fragile. Les récents textes européens n'ont de cesse de rappeler que l'évaluation de la solidité des stratégies de cybersécurité est un processus continu.

L'IA demeure perçue comme une menace négligeable

Seules 2 entreprises sur 10 considéreraient l'intelligence artificielle comme une menace pour leur activité.

Encore faut-il déterminer pour quel usage l'on destine l'IA. Mais d'une façon générale, et pour une grande majorité d'entreprises, elles le pensent à raison. Le risque de confier ses données à un outil d'intelligence artificielle n'a pas de conséquences majeures tant que la gouvernance a été correctement effectuée et à ce titre, que les données les plus confidentielles sont bien cantonnées à un usage spécifié. Par ailleurs, et parce qu'il faut savoir combattre à armes égales, les solutions de cybersécurité sont désormais toutes secondées d'intelligence artificielle. Quant à toutes les entreprises dont l'activité même relève d'un intérêt majeur, leur stratégie repose évidemment sur des mesures de sécurité d'un tel niveau que le traitement du risque IA reste incomparable.

La souveraineté est-elle une question de cybersécurité ?

Un débat d'experts s'il en est et tous ne portent évidemment pas le même regard sur la question. De prime abord, le choix d'une solution dite souveraine, à tout le moins européenne, semble relever naturellement de la sphère sécuritaire. Pourtant, tout dépend du point de vue que l'on adopte.

L'association de référence de la cybersécurité en France, le CLUSIF, rappelle par exemple que le cyberscore initié par le gouvernement français ne peut être considéré comme une évaluation en cybersécurité des plateformes numériques dédiées au grand public en ce qu'il prend également en compte la notion de protection et de souveraineté des données.

De son côté, l'ANSSI ne traite pas non plus des questions de dépendance ou de risques géopolitiques des solutions qu'elle préconise et ne s'attache qu'à évaluer l'apport techniques de ces solutions.

« Le risque, c'est précisément ce qu'il faut savoir évaluer » rappelle Simon AMIOT. Quel est le degré de risque qu'un gouvernement étranger ayant accès à mes données, par l'effet de sa propre législation, les transmette à mes concurrents ? Ne dois-je pas plutôt me préoccuper des tentatives d'extorsion et de la prolifération des groupes cybercriminels ? Pour la plupart des entreprises et des collectivités territoriales, la seconde hypothèse est la plus probable ».

Les garanties de plus haute sécurité telles que le référentiel SecNumCloud de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) s'adressent aux hébergeurs de données prestataires de services cloud et valorisent l'aptitude à atteindre un niveau de sécurité élevé.
Pour en bénéficier, les entreprises doivent y consacrer un budget très élevé, d'un niveau équivalent à un SOC PDIS (certifié ANSSI) peu ou prou.
Quand bien même l'on souhaiterait faire profiter son entreprise des mesures de sécurité les plus solides, l'accès à ce type de solution requiert d'en avoir l'extrême nécessité.

Rationaliser, consolider, décommissionner

S'orienter dans le dédale d'une informatique en évolution permanente

Afin de déculpabiliser chacun, précisons qu'en dehors de quelques secteurs sensibilisés et contraints depuis longtemps comme la banque/finance et les grands OIV, la cybersécurité d'entreprise reste un domaine où subsistent beaucoup d'incertitudes, s'additionnant au fil du temps et de la croissance. Un rapprochement de filiales et ce sont de nouvelles solutions de cybersécurité qui s'ajoutent à l'existant, de nouveaux matériels, de nouvelles méthodes avec lesquelles il faut composer.

Dans la pratique, au-delà de quelques convictions générales comme l'urgence de rationaliser, d'atteindre une prédictibilité des coûts et de disposer d'une sécurité efficace et suffisante, l'entreprise se montre rarement en mesure de définir des objectifs plus précis, une feuille de route et encore moins de dresser la liste des outils à conserver.

On le serait à moins. L'exercice du choix éclairé requiert de maîtriser de multiples paramètres, de disposer d'une vaste connaissance de l'offre cyber disponible, de bien connaître le périmètre couvert, et bien sûr le coût réel à engager. La démarche en outre est généralement freinée par les traditionnels silos métiers, que l'on s'efforce d'atténuer et qui semblent prendre un malin plaisir à se reformer dès que l'on a le dos tourné.

Il n'y a pas de choix éclairé sans disposer d'une carte exhaustive. En d'autres termes, le conseil, l'analyse et l'audit externe demeurent des expertises tout à fait bénéfiques, à plus d'un titre.

Par quoi commencer ?

La certification ISO 27001 est le canevas idéal pour prendre le pouls de l'entreprise, évaluer le niveau de risque en fonction de l'activité et du secteur et définir les objectifs.

C'est également un point d'entrée approprié pour tous les collaborateurs puisqu'il énonce l'ensemble des règles d'hygiène cyber, ce socle élémentaire que l'entreprise doit maîtriser.

Au-delà des concepts et des bonnes pratiques partagées, la cybersécurité d'une entreprise est construite sur mesure pour elle, c'est important de s'en souvenir. C'est pourquoi on interrogera le business de l'entreprise, ses objectifs à court et moyen terme, ses prévisions de croissance qui impacteront nécessairement les règles mises en place et qu'il faudra faire évoluer selon un agenda.

ISO 27001 n'est pas, en outre, une certification réservée à quelques-uns. Elle s'adresse à tout type d'entreprise, de la plus petite à la plus grande. Elle prépare avec beaucoup d'efficacité le terrain à

DU MOUVEMENT
dans l'assurance cyber

Après quelques années d'une certaine euphorie, les assureurs ont nettement levé le pied en matière d'assurance cybersécurité, certains choisissant même de ne plus en proposer. Coûteuse pour l'entreprise comme pour l'assureur, l'assurance cyber est cependant en passe de trouver son équilibre grâce aux grands comptes, mieux sécurisés.

Le secteur gagne également en maturité sur la question en passant d'un modèle purement actuariel, basé sur des statistiques généralement incomplètes faute de déclaration d'incident obligatoire à des procédés d'enquêtes et d'expertise. Certains assureurs ont notamment conclu des partenariats avec des éditeurs afin de disposer de résultats probants sur le niveau de sécurité de leurs clients et éventuellement d'exiger certaines mesures supplémentaires.

Quoiqu'il en soit, l'assurance cybersécurité n'est pas un outil de cybersécurité et ne doit jamais être perçue comme une solution suffisante.

d'autres réglementations, comme NIS 2, lesquelles se révèlent nettement moins douloureuses à mettre en œuvre une fois la certification acquise et le processus d'amélioration construit.

Enfin, la certification n'est pas non plus une fin en soi. L'entreprise peut choisir d'en suivre simplement la démarche afin de disposer d'un guide à la mise en place d'une sécurité adaptée à son activité et à son pilotage.

Faire de la place à la simplification

En matière de cybersécurité, le choix de solutions en SaaS ne va pas toujours de soi. L'On Premise continue d'être considéré comme plus sécuritaire. Pourtant, même les grands établissements financiers optent pour le Cloud public pour un grand nombre de leurs workloads.

C'est une question d'analyse risques/avantages et, n'en doutons pas, de psychologie. Si le hardware continue d'être vu comme un élément de cybersécurité, il est aussi très coûteux et manque cruellement de flexibilité. Toutes les organisations en ont fait l'expérience quand elles ont dû, en urgence, multiplier les concentrateurs VPN pour permettre à leurs collaborateurs de poursuivre le travail depuis leur domicile.

Si l'imprévisibilité reste le talon d'Achille de la cybersécurité, les choix historiques et la culture d'entreprise sont aussi à l'œuvre quand il s'agit de faire évoluer les pratiques. Ainsi, le réseau est un exemple courant de résistance à la modernisation vers des solutions as a service. Portées par des éditeurs mutualisant l'expérience sur des milliers de clients, de contextes, de secteurs, ces solutions profitent d'une expérience enrichie au service d'une cybersécurité inatteignable pour une organisation seule.

ISO/CEI 27 001, l'esprit d'amélioration

La certification ISO/CEI 27 001 n'est pas toujours bien comprise des entreprises qui cherchent à l'obtenir. Il ne s'agit pas d'un simple tampon de sécurité. ISO 27 001 garantit que l'entreprise a mis en place un système de cybersécurité doté d'un processus d'amélioration continue.
L'intérêt du processus prend tout son sens avec le sponsoring actif de la direction générale d'une part et l'établissement d'une feuille de route d'autre part.
Il arrive que le souhait de se lancer dans la certification naisse des résultats d'un audit. Les équipes se montrent alors plus vigilantes et identifient mieux les menaces dont elles pouvaient éventuellement se croire à l'abri. Dès lors, s'améliorer devient un enjeu quotidien et la démarche se fait nettement plus volontaire. On constate un vrai sentiment de satisfaction chez les équipes à se voir sur le bon chemin, adopter de meilleures pratiques et se challenger sur de multiples aspects de la sécurité d'entreprise.

« La veille IT est presque un métier en soi. Les administrateurs peuvent tout à fait constater l'évolution des usages, mais la connaissance des solutions disponibles pour y répondre peut leur manquer. Un exemple : qui a entendu parler du SASE ? Le Secure Access Service Edge est un concept de cybersécurité basé sur une convergence des réseaux WAN (et une convergence entre performance et sécurité de ces réseaux), unifiant les réseaux d'entreprises devenus très disparates. C'est déjà un essentiel pour certaines entreprises aujourd'hui et il faut sérieusement s'y intéresser. »

Simon AMIOT

À défaut d'être un expert et d'évoluer dans le secteur concerné, il n'y a aucune raison de ne pas s'équiper d'outils facilitants et dont la sécurité est le métier de l'éditeur. Cela vaut pour le réseau, mais également pour le poste de travail, ou encore le stockage et la sauvegarde.

Stordata, expert conseil en cybersécurité

Audit, analyses de risques, accompagnement à la certification ISO 27 001, conformité réglementaire, intégration et exploitation de solutions cybersécurité, Stordata accompagne les organisations dans toute leur démarche d'amélioration continue de leur cybersécurité.

Le chemin à parcourir pour que toutes les entreprises de France puissent afficher fièrement un système de management de la sécurité de l'information efficace et robuste est encore long, ne nous méprenons pas. Les résultats d'audits montrent que beaucoup d'efforts restent à fournir. Et pourtant, aucune entreprise ne débute de zéro d'une part et toutes se montrent capables d'améliorer significativement leur posture de sécurité d'autre part. C'est précisément ce qu'il faut retenir.

Parce que la cybersécurité one size fits all n'existe pas, la première urgence est d'obtenir une feuille de route aussi claire que possible, conçue pour l'entreprise dans toute sa spécificité et faisant apparaître un ordre de priorité. Au responsable de la sécurité ensuite de faire des choix, éclairés cette fois, au regard des contraintes de son service. La forte sensibilisation du RSSI à l'une ou l'autre mesure de sécurité et selon les contextes orientera sans aucun doute la sélection des actions à venir mais l'essentiel n'est pas là.

L'essentiel, c'est que la maturité de l'entreprise a déjà gagné en ampleur. C'est une graine plantée, qui ne demande qu'à s'épanouir. La cybersécurité reste un domaine récent, dont la jeunesse s'exprime autant dans le chaos d'une offre foisonnante que dans le manque de stratégies solides dans l'entreprise. Il faut y mettre de l'ordre pour continuer de progresser.

Avec l'acquisition de Duonyx, Stordata a hérité du savoir-faire développé par cette entité et a consolidé son expertise en cybersécurité autour des métiers du conseil, de l'intégration et de l'exploitation de solutions éprouvées.
Ses équipes de consultants interviennent dans tous les domaines clés de la cybersécurité : protection des terminaux, sécurité des réseaux (SASE) et des environnements cloud (CSPM), prévention des pertes de données (DLP), mise en œuvre des principes de cybersécurité, sensibilisation des équipes et accompagnement vers la certification.

Stordata

Siège - Versailles
28, rue Saint-Honoré
78000 Versailles
Tél. : +33 1 30 21 42 42

Agence Paris
24, rue Fabert
75007 Paris
Tél. : +33 1 44 18 30 01

Agence Sud-Est
11, Chemin des Anciennes Vignes
69410 Champagne-au-Mont-d'Or
Tél. : +33 4 78 48 09 47

Agence Sud-Ouest
6, rue Maurice Caunes
31200 Toulouse
Tél. : +33 5 34 50 49 00

Agence Méditerranée
Parc de Bellegarde
1 chemin de Borie
34170 Castelnau le Lez
Tél. : +33 5 34 50 49 00

Agence Ouest
34, quai Magellan
44000 Nantes
Tél : +33 2 28 08 09 93

Agence Est
9, rue Icare
67960 Entzheim
Tél. : +33 3 88 76 47 64

www.stordata.fr