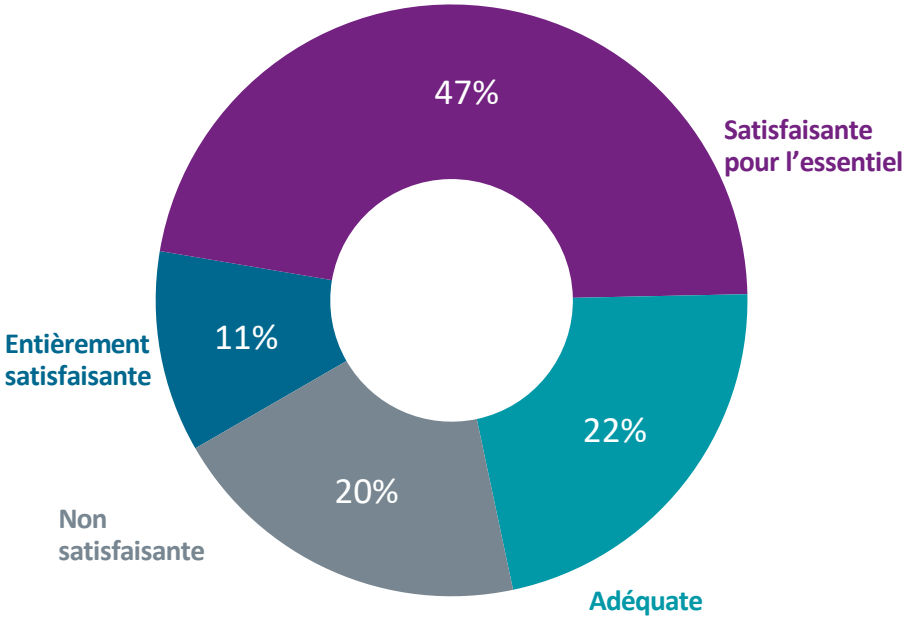
ÉTAT DE LA CYBERSÉCURITÉ 2022 : le Benelux

Au cours de l'année écoulée, le monde des affaires s'est adapté aux enseignements tirés de la pandémie de COVID. Au niveau des effectifs, les entreprises s'efforcent de déterminer les meilleurs moyens d'équilibrer la flexibilité des collaborateurs et la culture d'entreprise. Sur le plan technique, les nombreux avantages d'une architecture « cloud first » sont mis en balance avec les défis de la gestion de la complexité et des coûts dans un environnement multicloud. Il faudra encore des années avant de parvenir à comprendre à quoi ressemble l'équilibre dans un environnement post-pandémique, mais les premiers changements laissent présager une restructuration majeure.

Un autre enseignement important à retenir de la pandémie est que les symptômes sont souvent plus faciles à diagnostiquer et à traiter que les causes profondes. Les implications dépassent évidemment les stratégies d'entreprise, mais le domaine de la cybersécurité est un excellent exemple de ce concept dans le monde des affaires. Les entreprises sont brutalement sensibilisées aux problèmes de cybersécurité défaillante lorsqu'elles sont victimes d'une violation de données, et une analyse a posteriori permet d'identifier les processus ou les outils qui auraient permis d'éviter ou atténué l'attaque. En revanche, cela ne résout peut-être pas les problèmes sous-jacents susceptibles de conduire à un cyberincident différent par la suite.

Le rapport 2022 de CompTIA sur l'état de la cybersécurité examine la déconnexion entre la cause première et les symptômes. La transformation numérique induite par l'adoption du cloud et de la téléphonie mobile impose une nouvelle approche stratégique de la cybersécurité. Cependant, l'adoption complète de cette nouvelle approche pose des défis importants, tant sur le plan tactique que financier. Bien que la cybersécurité demeure l'un des domaines les plus critiques des entreprises modernes, les obstacles qui découlent des considérations héritées de l'informatique et de la mauvaise compréhension des menaces émergentes rendent difficile le respect du traitement prescrit.

Degré de satisfaction quant à la cybersécurité dans l'entreprise



INTÉGRATION D'UNE APPROCHE DE CONFIANCE ZÉRO

À bien des égards, le domaine de la cybersécurité est une réaction à l'évolution de l'informatique d'entreprise. Après tout, le besoin de cybersécurité ne se fait sentir qu'après la mise en œuvre de la technologie. Cette dynamique s'est intensifiée ces dernières années, les entreprises poursuivant activement leur mise à niveau technologique en ayant tendance à traiter la cybersécurité comme un sujet de second plan.

La cybersécurité reflète l'évolution de l'informatique d'entreprise notamment parce que toutes deux sont devenues plus stratégiques. Dans le domaine de l'informatique en général, les entreprises sont habituellement enclines à accepter la transition vers une approche plus stratégique, malgré quelques difficultés croissantes en cours de route. La cybersécurité, en revanche, s'avère un défi bien plus important lorsqu'il s'agit d'adopter un état d'esprit stratégique.

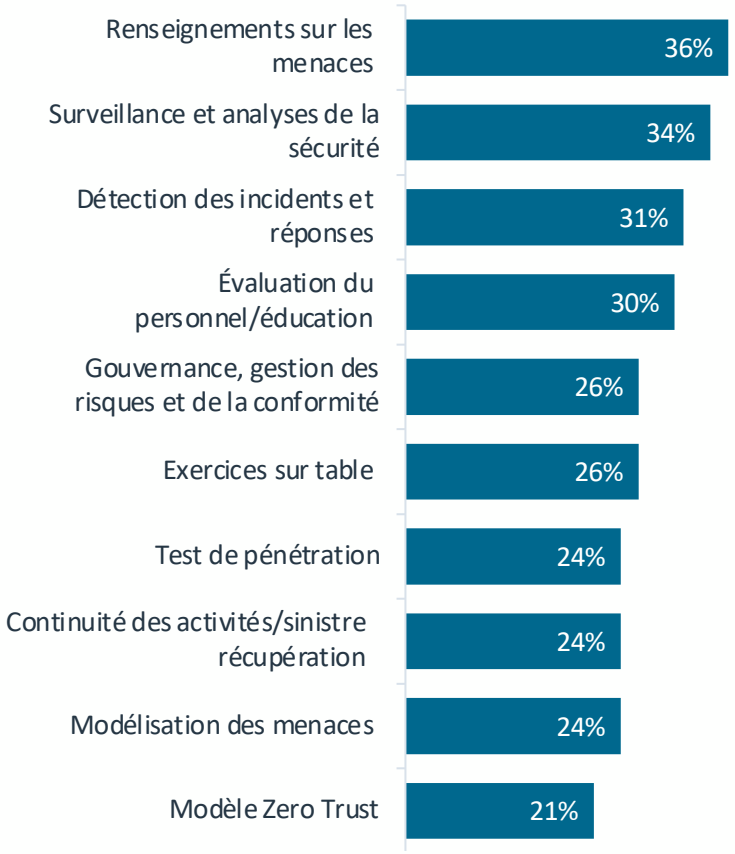
L'un des traits les plus importants d'un mode de pensée stratégique est de reconnaître que la cybersécurité ne se concentre plus principalement sur les événements provenant de l'extérieur. Lorsque l'on examine les problèmes qui ont motivé la cybersécurité, la plupart des principaux enjeux cités sont tournés vers l'extérieur. L'accent mis sur le volume, la variété ou l'ampleur des attaques met en relief les événements extérieurs à l'entreprise. Même les préoccupations concernant la protection de la confidentialité relèvent des attentes externes à l'entreprise. On reconnaît moins que la cybersécurité est liée à la nature changeante des opérations internes à l'entreprise, comme sa dépendance croissante à l'égard des données ou la nécessité de se conformer à l'évolution de la réglementation.

Nous assisterons au cours de la prochaine année à un effort d'intégration de la cybersécurité aux activités commerciales. L'acceptation de la cybersécurité en tant que composante essentielle de la transformation numérique suscitera de nouvelles interrogations et engendrera la mise en place de nouveaux critères pour mesurer le succès dans l'ensemble de l'entreprise. Dans le même temps, l'adoption d'un point de vue holistique permettra de lever bon nombre d'obstacles existants qui empêchent toute modification de l'approche en matière de cybersécurité.

L'introduction de l'informatique dans le cloud et des appareils mobiles a radicalement modifié la notion de périmètre sécurisé qui prévalait depuis des décennies. Alors que les entreprises étaient aux prises avec ce changement de paradigme, une partie de la difficulté résidait dans la définition d'une approche globale qui éclaire un large éventail de décisions en matière de cybersécurité. La Confiance Zéro est apparue comme la réponse à ce dilemme.

Cette année, la Confiance Zéro semble évoluer d'une politique générale à des processus tactiques. L'adoption de la Confiance Zéro n'aura pas lieu du jour au lendemain, et ce pour plusieurs raisons. Tout d'abord, la Confiance Zéro représente une façon radicalement différente de penser la cybersécurité. Plutôt que de considérer la cybersécurité comme l'un des nombreux composants de la fonction informatique et d'investir simplement dans du matériel ou des logiciels, les entreprises doivent désormais considérer la cybersécurité comme un impératif organisationnel dépassant le simple choix de produits technologiques pour éclairer les décisions en matière de flux de travail et de main-d'œuvre.

Pratiques de cybersécurité en place



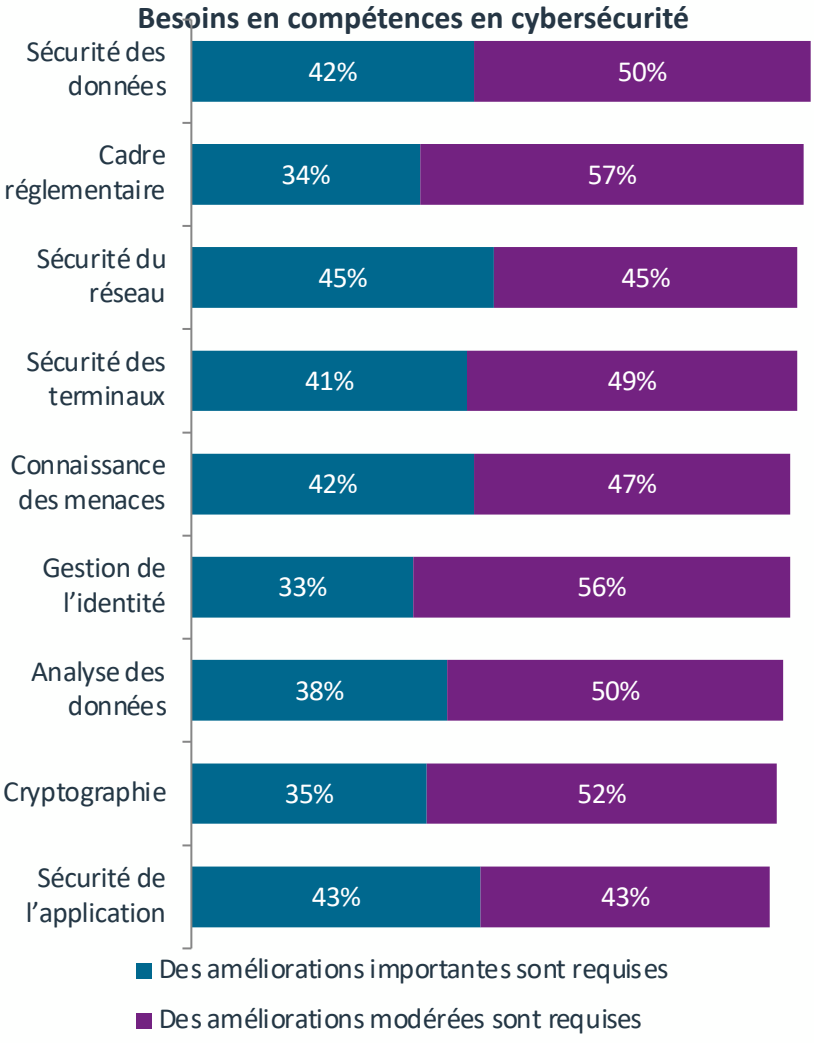
La Confiance Zéro ne dépend pas d'un produit unique ou d'une action ponctuelle ; de nombreux outils et pratiques discrets peuvent faire partie d'une approche de Confiance Zéro. Si l'on examine les éléments qui composent généralement l'approche de la Confiance Zéro, on constate qu'un plus grand nombre d'entreprises prennent en compte chaque partie individuellement plutôt que de considérer le tout collectivement. L'authentification multifacteur, l'un des meilleurs outils pour valider une identité de confiance, est en place dans 29 % des entreprises. La gouvernance de la charge de travail dans le cloud, un processus qui garantit que les ressources du cloud sont utilisées conformément aux règles, est en place dans 26 % des entreprises. D'autres éléments, tels que la micro-segmentation définie par logiciel (33 %) et l'accès au moindre privilège (23 %), dépassent également la sensibilisation au sens large à une politique de Confiance Zéro.

Le principal point à retenir est que la Confiance Zéro est une philosophie autour de la cybersécurité qui permet de poser des questions et oriente les décisions. La meilleure façon d'adopter la Confiance Zéro n'est pas de définir un ensemble de critères permettant de définir un succès total, mais d'élaborer une feuille de route identifiant les meilleures mesures à prendre en fonction du statut de l'entreprise. Ces étapes peuvent inclure un audit complet des données et des flux de travail, la mise en œuvre de produits spécifiques tels qu'un logiciel de gestion des identités et des accès (GIA) ou la création d'un programme de formation continue destiné au personnel. Chaque étape doit répondre à une question précise et avoir des résultats mesurables.

LIER LES PERSONNES ET LE PRODUIT À LA STRATÉGIE

Lorsque les entreprises tentent de s'attaquer à la cause première de leurs lacunes en matière de sécurité, elles découvrent que le problème comporte plusieurs niveaux. Il y a évidemment l'aspect technique, qui a été le point de mire pendant des années et continue d'être une partie substantielle d'une solution de cybersécurité. Il y a aussi l'aspect main-d'œuvre, et de nombreuses entreprises se sont tournées vers la sensibilisation à la cybersécurité pour l'améliorer. Cependant, d'autres aspects traitant des opérations commerciales et des mesures d'entreprise ont probablement reçu moins d'attention ces dernières années.

Alors que les entreprises se concentrent sur la culture de la chaîne de cybersécurité pour inclure tous les aspects organisationnels, les experts techniques n'en restent pas moins un élément essentiel. Après une évaluation approfondie des lacunes en matière de compétences, l'amélioration de ces compétences est le prochain défi. La sécurité du réseau semble parfois être un domaine qui bénéficie d'une expertise approfondie étant donné que cette tâche est effectuée depuis longtemps, mais en réalité, les changements dans le paysage informatique exigent une amélioration constante. D'autres domaines tels que la connaissance des menaces, l'analyse des données et la gestion des identités sont des candidats plus évidents à la croissance des compétences, car ils représentent des tendances plus récentes en matière de cybersécurité.



La liste des produits de cybersécurité commence par des éléments qui existent depuis longtemps. Les pare-feux, les antivirus et les protections contre les logiciels malveillants étaient les principaux composants du périmètre sécurisé, et ils remplissent toujours cette fonction même si le périmètre sécurisé a perdu de son importance. Ces outils sont omniprésents, bien que de nombreux utilisateurs finaux (et peut-être même le personnel informatique) ne les considérer peut-être pas comme faisant partie de l'ensemble de produits du fait tant ils sont courants.

La surveillance du réseau est un autre outil à la longue histoire, un outil qui évolue pour s'adapter à l'époque. Des outils tels que SolarWinds Network Performance Monitor, Datadog Network Monitoring et Auvik offrent des capacités étendues d'observation et d'analyse de l'ensemble d'une architecture réseau. Parmi les fonctionnalités récentes des moniteurs réseau figurent la visibilité sur les composants cloud du réseau et des outils d'analyse pour mieux comprendre le flux de données.

Soulignant l'importance des systèmes cloud, les outils de supervision et de gestion SaaS gagnent rapidement du terrain. L'accélération de l'adoption du cloud a été l'un des changements les plus importants dans les opérations informatiques pendant la pandémie, et les entreprises réagissent maintenant aux effets secondaires de cette activité. En plus des problèmes de cybersécurité, les systèmes cloud s'accompagnent d'un ensemble unique de préoccupations concernant l'utilisation et le coût, et de nouveaux logiciels de gestion sont nécessaires pour administrer, orchestrer et sécuriser correctement l'architecture cloud.

À l'autre extrémité du spectre, il y a des outils qui ont encore un faible taux d'adoption, mais qui devraient être fortement considérés comme des ajouts imminents. Bien que le SaaS soit la forme la plus populaire d'adoption du cloud, le IaaS est également répandu, et peut être plus critique pour une surveillance et une gestion appropriées. Des outils complets de surveillance du réseau sont essentiels pour fournir une vue d'ensemble, mais les analyseurs de paquets et les analyseurs LAN sont des produits ciblés qui peuvent déceler les problèmes difficiles à trouver.

Avec tant d'outils à disposition et autant de contraintes pour le personnel en charge de la cybersécurité, la prochaine étape évidente est l'automatisation. Celle-ci réduit la complexité de l'adoption de produits multiples, mais elle n'élimine pas nécessairement le besoin de spécialistes en cybersécurité. De nouvelles compétences sont nécessaires pour mettre en œuvre correctement l'automatisation et effectuer des ajustements continus au besoin.

Même si l'automatisation ne résout pas complètement le problème des ressources, elle rend la situation plus gérable. L'intégration de la cybersécurité aux opérations commerciales rend la cybersécurité plus critique que jamais, et la mise en œuvre d'une philosophie de Confiance Zéro conduit à une série de nouveaux processus. Une structure organisationnelle dédiée et un ensemble d'outils appropriés sont les premières étapes pour faire face à une complexité accrue. En adoptant une approche équilibrée de l'automatisation, les entreprises peuvent s'attaquer pleinement à leurs difficultés sous-jacentes et évoluer vers une perspective saine de la cybersécurité.