LIVRE BLANC

11 contrôles de sécurité pour réduire les cyber risques

Des solutions pratiques pour renforcer vos défenses, accroître votre cyber résilience et réduire les risques organisationnels.

SOPHOS

Résumé

Dans toute organisation, il est important que les dirigeants comprennent qu'optimiser les contrôles de sécurité ne se limite pas à protéger les données et les systèmes, mais consiste également à réduire les risques organisationnels liés à la réputation de la marque, à la confiance des clients et à la continuité des activités. Les cyberattaques telles que les ransomwares et les attaques par compromission de la messagerie professionnelle (ou attaques BEC, Business Email Compromise) peuvent avoir des conséquences opérationnelles et financières majeures. Selon le Cyber Defense Magazine, la cybercriminalité devrait coûter 1 200 milliards de dollars à l'économie mondiale en 2025[1]. Même lorsqu'elles ont été contrées, les attaques peuvent causer de graves perturbations si les systèmes doivent être mis hors ligne pour être réinitialisés et reconstruits. Certaines organisations ont la capacité de surmonter ce type de situation. D'autres sont contraintes de se poser des questions existentielles auxquelles elles ne s'attendaient pas.

1,2 billion de dollars

En 2025, la cybercriminalité devrait coûter 1,2 billion de dollars américains à l'économie mondiale[1].

Le rôle des contrôles de sécurité dans l'optimisation des cyberdéfenses

Les contrôles de sécurité sont les différents leviers sur lesquels les équipes de cybersécurité peuvent agir pour réduire les risques et protéger l'organisation contre les menaces. S'il en existe de nombreux types, tous ont pour objectif commun soit de prévenir les incidents et les violations, soit de minimiser les dommages lorsque des événements de sécurité se produisent. Certains leviers sont axés sur la prévention, d'autres offrent différents niveaux d'atténuation en matière de prévention, de détection et de réponse aux menaces. Disposer de la bonne combinaison de contrôles de sécurité dans tous les domaines est un élément clé pour mettre en place une stratégie de défense forte.

La mise en place de contrôles de sécurité rigoureux est aussi un élément clé de la gestion des risques via la cyberassurance. Les assureurs évaluent les contrôles mis en place par les organisations pour fixer les primes et les limites de couverture.

Celles-ci couvrent généralement :

Les responsabilités de l'assuré englobent les dommages directs que votre organisation pourrait subir suite à une cyberattaque ou un vol de données. Ceux-ci peuvent inclure les pertes d'exploitation, les coûts de restauration des données, le vol ou les paiements liés aux ransomwares.

Les responsabilités envers des tiers, en général des clients, partenaires, organismes de réglementation ou autres, peuvent inclure des poursuites judiciaires, des demandes d'indemnisation ou des amendes réglementaires imposées par des agences gouvernementales ou des associations professionnelles.

Pourquoi c'est important

De meilleurs contrôles ne permettent pas seulement de protéger vos activités, ils peuvent également réduire vos primes d'assurance et améliorer les indemnités versées en cas d'incident.

Réduisez les cyber risques grâce à ces 11 contrôles de sécurité

Investir dans des contrôles rigoureux permet de réduire les cyber risques et peut contribuer à améliorer l'assurabilité et les conditions de polices d'assurance potentielles. Voici onze contrôles fondamentaux qui renforcent les défenses dans toute une gamme de catégories de prévention et de réduction d'impact.

Correctement mis en œuvre, ces contrôles de sécurité renforcent votre posture de cybersécurité, et vous arment contre les menaces actuelles et futures.

1. Gestion de l'identité et de l'accès
2. Sécurité Endpoint
3. Authentification multifacteur
4. Gestion des vulnérabilités
5. Sécurité des messageries
6. Gestion des sessions privilégiées
7. Gestion des ressources
8. Segmentation et architecture
9. Extended Detection and Response (XDR)
10. Sauvegarde et continuité des activités
11. Sécurité du réseau et contrôle du trafic

1. Gestion de l'identité et de l'accès

La gestion de l'identité et de l'accès (IAM) garantit que seules les personnes autorisées peuvent accéder aux systèmes et aux données. La gestion des accès privilégiés (PAM) limite davantage l'accès à ce dont les utilisateurs ont strictement besoin. Un principe en apparence simple, mais dont l'application peut s'apparenter à un véritable casse-tête, en particulier dans les grandes organisations. Toutes les entreprises ont intérêt à mettre en place des procédures strictes d'onboarding/offboarding, à imposer des règles rigoureuses en matière de mots de passe et à vérifier régulièrement les accès.

Quelle que soit sa taille, toute organisation doit disposer de règles claires pour éliminer les identités obsolètes. Sans cela, les attaquants pourront exploiter les comptes oubliés afin d'augmenter leurs privilèges et de se déplacer dans votre environnement sans se faire repérer.

2. Sécurité Endpoint

Le moindre appareil connecté à votre environnement représente une cible potentielle. Avec le recours croissant au travail hybride, les risques d'exposition n'ont jamais été aussi élevés, rendant la protection des postes de travail plus cruciale que jamais. De nombreuses attaques commencent par des menaces « de base » faciles à détecter et à neutraliser à l'aide d'outils Endpoint puissants. Cependant, les postes non pris en charge ou oubliés finissent souvent par devenir des maillons faibles qui constituent un point d'entrée courant pour les attaques de ransomware distant. Assurez-vous que tous les appareils sont protégés.

3. Authentification multifacteur

L'authentification multifacteur (MFA) valide l'identité d'un utilisateur sur la base de plusieurs facteurs : quelque chose qu'il connaît (par exemple, un mot de passe), qu'il possède (par exemple, un jeton) ou qui lui est propre (par exemple, son empreinte digitale). Dans la mesure où la compromission des identifiants reste l'une des principales causes d'attaques[2], l'authentification multifacteur est un contrôle incontournable pour les organisations modernes. Prévoyez des solutions plus avancées, telles que la géolocalisation et la correspondance numérique, pour renforcer votre capacité de résilience face aux stratégies de contournement des attaquants, tout en veillant à préserver l'équilibre entre l'expérience utilisateur et la confidentialité.

Points à retenir

Les comptes inactifs et les privilèges inutilisés constituent des points d'entrée faciles pour les attaquants. Une fois à l'intérieur, ces derniers peuvent exploiter ces failles pour obtenir un accès privilégié et étendre discrètement la portée de leur attaque.

Le point d'entrée le plus courant est souvent le moins visible. Ne laissez pas les postes obsolètes devenir des portes dérobées.

Implémentez l'authentification MFA pour augmenter la vérification dans les scénarios à haut risque sans créer de friction inutile.

4. Gestion des vulnérabilités

La gestion des vulnérabilités désigne le processus continu consistant à identifier, évaluer et corriger les failles de sécurité dans votre environnement. Elle recouvre des pratiques courantes, telles que l'application de correctifs logiciels et système, les mises à jour de configuration et la surveillance des vulnérabilités récemment divulguées. Il est essentiel de disposer de renseignements sur les menaces fiables pour garder une longueur d'avance sur les risques émergents.

Il est tout aussi indispensable de savoir où se trouvent tous les actifs sur votre réseau pour effectuer une analyse complète. Grâce à cette visibilité, les organisations peuvent adopter une approche basée sur les risques pour prioriser les vulnérabilités, en fonction de leur exposition, de leur probabilité d'exploitation et de leur impact sur l'activité.

5. Sécurité des messageries

Bien qu'il s'agisse d'une technologie plus ancienne, les messageries restent l'un des principaux points d'entrée pour les attaques. Le phishing, en particulier, est un vecteur courant pour les ransomwares et les vols d'identifiants. Les attaques BEC (Business Email Compromise) sont également à l'origine des demandes d'indemnisation les plus fréquentes au titre de la cyberassurance[3]. Une sécurité des messageries renforcée peut empêcher les contenus malveillants de parvenir dans votre boîte de réception, ce qui en fait une première ligne de défense essentielle. À mesure que l'IA générative perfectionne les attaques de phishing en proposant une grammaire et des messages plus pertinents, les solutions de protection doivent évoluer afin de réduire le taux de réussite de ces attaques.

Mais la protection ne devrait pas s'arrêter une fois les emails distribués. Les URL et les pièces jointes qui semblent sûres à première vue peuvent s'avérer malveillantes une fois que l'email est arrivé dans la boîte de réception. Les solutions avancées de sécurité des messageries offrent désormais des fonctionnalités de détection et de remédiation après distribution des emails : elles réanalysent automatiquement le contenu, retirent les emails malveillants et neutralisent les liens si leur profil de risque change. Ces contrôles permettent de repérer les menaces qui parviennent à contourner les défenses initiales et de réduire au minimum la durée pendant laquelle les messages nuisibles séjournent dans les boîtes de réception des utilisateurs.

Points à retenir

Recherchez les vulnérabilités dans vos applications tierces et vos services Cloud, pas seulement dans vos systèmes centraux.

Un seul clic suffit. La meilleure façon de bloquer le phishing est de s'assurer que les utilisateurs ne voient jamais l'appât, même après sa distribution.

6. Gestion des sessions privilégiées

Les comptes administratifs offrent aux acteurs malveillants le plus grand pouvoir, tout particulièrement lorsque ces privilèges incluent l'accès aux systèmes d'identité, aux contrôles de configuration et aux outils de sécurité. Dès qu'il a accès aux privilèges admin, un attaquant est en mesure de désactiver les défenses et de déployer un ransomware à grande échelle.

Pour réduire ce risque, les organisations ont tout intérêt à mettre en place un modèle à plusieurs niveaux pour les accès privilégiés et à surveiller activement l'utilisation de ces comptes. La gestion des sessions privilégiées (PSM) assure une surveillance en loggant, en enregistrant et, dans certains cas, en contrôlant les sessions administratives en temps réel, ce qui permet de détecter les activités suspectes, de prévenir les utilisations abusives et d'assurer la conformité.

7. Gestion des ressources

Il est impossible de protéger ce dont on ignore l'existence. Les organisations devraient tenir à jour un inventaire à la fois de leurs actifs matériels et de leurs données. En cas d'incident, il est essentiel de savoir où sont stockées les données sensibles, afin de pouvoir investiguer rapidement et efficacement, établir des rapports précis et contenir au plus vite la menace. Une bonne gestion des actifs facilite les investigations approfondies, contribue à rationaliser les responsabilités et réduit l'impact d'une violation.

8. Segmentation et architecture

Une fois qu'un acteur malveillant a réussi à s'introduire dans votre environnement, sa prochaine action consiste généralement à effectuer un déplacement latéral afin d'élever ses privilèges, d'accéder à des systèmes sensibles ou de déployer un ransomware. Une segmentation du réseau et une conception architecturale solides peuvent grandement entraver ce mouvement. En créant des frictions et en forçant les attaquants à faire davantage de « bruit », la segmentation augmente vos chances de les détecter plus tôt dans la chaîne d'attaque.

L'architecture de votre système doit reposer sur les principes de confidentialité, d'intégrité, de disponibilité et de résilience. Pour ce faire, il faut notamment limiter l'accès entre systèmes et entre utilisateurs et systèmes grâce à un modèle « Zero Trust », dans lequel chaque transaction est vérifiée en fonction de l'identité, de l'appareil et des autorisations de l'utilisateur.

Points à retenir

Êtes-vous en mesure de savoir qui a accédé à votre interface administrateur mardi dernier et ce qu'il a fait exactement ? Si tel n'est pas le cas, il est temps de renforcer la surveillance.

Conserver des documents non nécessaires peut entraîner une augmentation des coûts d'assurance et aggraver les dommages causés à la réputation en cas de violation.

Segmentez le réseau pour isoler les systèmes critiques des points d'accès courants.

9. Extended Detection and Response (XDR)

Jongler avec des dizaines d'outils distincts peut fragmenter les alertes, ralentir le triage et masquer les activités malveillantes. Les fonctionnalités XDR (Extended Detection and Response) viennent remédier à cela en offrant une vue unifiée des activités sur les postes, pare-feux, réseaux, messageries, identités, sauvegardes et systèmes de sécurité du Cloud, ce qui réduit le nombre d'alertes inutiles et permet une prise de décision plus rapide et plus sûre. Cela permet d'éliminer le scénario de type « chaise pivotante » dans lequel les analystes sont contraints de passer d'un outil cloisonné à l'autre pour investiguer et répondre aux menaces.

Les systèmes XDR plus robustes se basent également sur des analyses avancées, la détection priorisée par l'IA, la recherche profonde des données, ainsi que la corrélation et l'escalade automatisées des alertes. Cette convergence des capacités améliore la précision de la détection, accélère les investigations et aide les équipes de cybersécurité à se concentrer sur les menaces les plus graves sans être ralenties par des problèmes liés aux outils.

10. Sauvegarde et continuité des activités

Lorsqu'un cyber incident perturbe les opérations ou endommage les systèmes, des sauvegardes bien préparées et un plan de continuité des activités solide peuvent faire la différence entre une reprise rapide et une interruption de service prolongée. Cela dit, toutes les sauvegardes ne sont pas identiques. Pour être efficaces, les sauvegardes doivent être validées, testées régulièrement et capables de restaurer les systèmes et les données en toute intégrité.

Mais souvent, la configuration des sauvegardes est défaillante. Nombre d'organisations découvrent trop tard que leurs sauvegardes ne restaurent que partiellement les systèmes ou omettent des données critiques ; et ce qui aurait dû être une panne de courte durée devient une situation très difficile de plusieurs semaines.

Il est tout aussi important que les sauvegardes soient protégées par une authentification hors bande. Sans ce rempart, un acteur malveillant disposant d'un accès étendu pourrait tenter de désactiver ou de supprimer les données de sauvegarde dans le cadre de son attaque.

Points à retenir

Les fonctionnalités XDR transforment les alertes isolées en actions décisives, accélérant ainsi les investigations et améliorant les résultats de la réponse aux menaces.

Dans la mesure du possible, conservez les sauvegardes segmentées et hors ligne. Votre rétablissement ne doit jamais reposer sur un seul canal.

11. Sécurité du réseau et contrôle du trafic

Le réseau n'est pas seulement une couche de connexion, c'est aussi un point de contrôle stratégique pour l'inspection, le filtrage et la gestion du trafic dans votre environnement. Les pare-feux, les systèmes de prévention des intrusions (IPS), le filtrage DNS et les passerelles Web sécurisées constituent la base d'une mise en œuvre multicouche.

Mais tous les pare-feux ne se valent pas. Les solutions anciennes, mal configurées ou sous-utilisées, peuvent créer des failles de sécurité exploitables. C'est pourquoi il est essentiel de maintenir votre capacité de résilience en évaluant régulièrement vos défenses, en les corrigeant et en les mettant à jour, et en les adaptant au panorama actuel des menaces.

Les contrôles modernes, tels que l'accès réseau Zero Trust (ZTNA), garantissent un suivi des accès plus granulaire et plus sensible au contexte. Associées à des protections traditionnelles, ces solutions contribuent à réduire la surface d'attaque, à prévenir les mouvements latéraux et à empêcher l'exfiltration dans les environnements hybrides et Cloud.

Points à retenir

Intégrez la télémétrie du réseau à votre pile de détection de manière à améliorer la visibilité, à accélérer les investigations et à signaler les activités anormales, en particulier les mouvements latéraux et le trafic C&C (Command and Control).

D'une vision globale à une approche globale

La cybersécurité ne se résume pas à déployer les bons outils : il s'agit d'adopter une stratégie qui allie expertise, processus et technologies. Ces 11 contrôles, lorsqu'ils sont implémentés de manière réfléchie et cohérente, peuvent réduire considérablement l'exposition de votre organisation aux risques.

Pour assurer une résilience à long terme, il est indispensable de se doter d'un programme de cybersécurité solide, reproductible, adaptable et reposant sur une répartition claire des responsabilités. La technologie est puissante, mais elle ne sert à rien en l'absence d'équipes qualifiées et de processus structurés garantissant sa bonne utilisation.

Les menaces sont vouées à se transformer, les technologies à en suivre le rythme et votre entreprise à évoluer. Pour garder une longueur d'avance, il faut adopter une approche globale, s'adapter en permanence et instaurer une culture où la sécurité ne se limite pas à une liste à cocher, mais constitue un facteur clé de la réussite de l'entreprise.

[1] Cyber Defense Magazine : The True Cost of Cybercrime : Why Global Damages Could Reach $1.2-$1.5 Trillion by End of Year 2025
[2] Édition 2025 du rapport annuel Sophos sur les menaces
[3] Dark Reading, « Email-Based Attacks Top Cyber-Insurance Claims », 8 mai 2025

Êtes-vous prêt à évaluer votre programme de cybersécurité ?

Discutez avec un expert Sophos dès aujourd'hui.

Sophos France
Tél. : +33 1 34 34 80 00
Email : info@sophos.fr