

MANUEL

La cyber- assurance décryptée



Des contrôles de sécurité qui contribuent à réduire
les risques et les primes de cyber-assurance

Index

Introduction	1
Qu'est-ce que la cyber-assurance ?	2
Qui a besoin d'une cyber-assurance ?	3
Les petites entreprises ont-elles besoin d'une cyber-assurance ?	4
Qu'est-ce qui est couvert par la cyber-assurance ?	5
Qu'est-ce qui n'est pas couvert par une cyber-assurance ?	6
Comment réduire les primes de cyber-assurance : Une analogie.	7
Contrôles minimaux pouvant être mis en œuvre	8
Authentification multi-facteurs	8
Stratégies en matière de mots de passe	9
Analyse du comportement de l'utilisateur	9
Audit des changements	10
Surveillance du courrier électronique	10
Sauvegarde et récupération	11
Contrôle d'accès basé sur les rôles	11
Conformité	12



Introduction

Les pratiques de cybersécurité que vous avez mises en place sont-elles suffisantes pour protéger les données de votre organisation ? Même après des décennies d'étude des personnes, des processus et des technologies, cette question est toujours présente dans les esprits des responsables de la sécurité des organisations du monde entier. Malgré tous les efforts déployés, des pirates continuent à s'infiltrer dans les contrôles de sécurité et à perturber les processus opérationnels. La perte, la compromission ou le vol de données électroniques ont un impact négatif sur les entreprises, et celles-ci sont également responsables des dommages résultant du vol de données de tiers. La cyber-assurance est importante pour protéger les entreprises contre le risque de événements cybernétiques, y compris ceux liés au terrorisme.

Dans cet e-book, nous mettons en évidence les paramètres de sécurité essentiels qui aident votre entreprise à satisfaire aux contrôles minimums spécifiés par les souscripteurs. Le respect de ces contrôles de base se traduira par des primes d'assurance intéressantes et améliorera la cyberhygiène de votre environnement de travail.



L'assurance cybersécurité, également connue sous le nom d'assurance de cyber-responsabilité ou de cyber-assurance, est une police qui peut être souscrite pour aider à réduire les risques financiers liés aux activités en ligne en échange d'une cotisation mensuelle ou trimestrielle. La cyber-assurance trouve son origine dans l'assurance erreurs et omissions (E&O), une forme d'assurance qui protège contre les fautes et les défauts dans les services fournis par une entreprise.



Qui a besoin d'une cyber-assurance ?

Les organisations qui créent, stockent et gèrent des données électroniques en ligne, telles que les contacts des clients, les numéros de cartes de crédit et autres informations personnelles identifiables, peuvent bénéficier d'une cyber-assurance. Les temps d'arrêt dus aux cyber-incidents pouvant entraîner une perte de ventes et de clients, les entreprises de commerce électronique peuvent également bénéficier d'une cyber-assurance.



Les petites entreprises ont-elles besoin d'une cyber-assurance ?

Selon le [DBIR de Verizon](#), parmi les 5 258 violations de données confirmées, 263 ont été signalées par des petites entreprises comptant de 1 à 1 000 employés et 307 par des grandes entreprises comptant plus de 1 000 employés. Nous ne savons pas combien de petites industries sont concernées par les 4 688 autres violations de données. Toutefois, il ressort clairement de ces données qu'une organisation de toute taille peut être victime d'une violation de données. Cela dépend en grande partie du type d'infrastructure sur lequel une organisation s'appuie et du type de données qu'elle traite. Le réflexe le plus prudent est de souscrire une cyber-assurance si vous traitez des données de clients et des biens numériques, tels que des vlogs et des livres électroniques.



Les polices de cyber-assurance aident à couvrir les pertes financières qui résultent de cyber-événements et d'incidents. En outre, la couverture du cyber-risque aide à couvrir les dépenses associées à la réparation, y compris le paiement de l'assistance juridique, des enquêteurs, des communicateurs de crise et des crédits ou remboursements aux clients. Les dépenses comprennent généralement les coûts associés aux éléments suivants :

- ✔ Répondre aux demandes d'extorsion d'une attaque par ransomware.
- ✔ Informer les clients lorsqu'une violation de la sécurité s'est produite.
- ✔ Payer les frais de justice liés à la violation de la vie privée.
- ✔ Faire appel à des experts en informatique légale pour récupérer les données compromises.
- ✔ Rétablir l'identité des clients dont les informations personnelles identifiables (PII) ont été compromises.
- ✔ Récupérer les données qui ont été modifiées ou volées.
- ✔ Réparer ou remplacer des systèmes informatiques endommagés ou compromis.

En fonction du type de police et du fournisseur, certains assureurs commencent à proposer des polices qui couvrent également les pertes de responsabilité civile.



Qu'est-ce qui n'est pas couvert par une cyber-assurance ?

De nombreuses stratégies de cybersécurité excluent les problèmes de sécurité évitables causés par des personnes, tels qu'une mauvaise gestion des configurations ou une mauvaise manipulation des ressources numériques. Parmi les autres problèmes exclus par les stratégies de cybersécurité, citons :

- ✔ Violations ou cyber-événements préexistants ou antérieurs, tels que des incidents survenus avant la souscription de la police.
- ✔ Cyber-événements initiés et causés par des employés ou des internes.
- ✔ Pannes d'infrastructures non causées par une cyberattaque délibérée
- ✔ Non-correction d'une vulnérabilité connue
- ✔ Le coût de l'amélioration des systèmes technologiques, y compris le renforcement de la sécurité des systèmes ou des applications.



Comment réduire les primes de cyber-assurance : Une analogie

La cyber-assurance est similaire à l'assurance maladie. Si vous avez un problème de santé au moment où vous souscrivez une assurance, ou si vous avez une mauvaise habitude qui pourrait affecter votre santé, vous risquez de ne pas pouvoir vous assurer ou votre prime d'assurance sera élevée. Les assureurs s'attendent à ce que les acheteurs d'assurance soient en bonne santé, sans complications majeures, et aient des habitudes de vie saines.

De même, les souscripteurs de cyber-assurance s'attendent à ce que certains contrôles minimums soient en place dans votre organisation. Le cryptage de bout en bout, l'authentification multifactorielle (MFA) et la conformité aux stratégies réglementaires en sont quelques exemples. En fonction des mesures de sécurité prises par l'organisation, les primes d'assurance varieront. Par exemple, une maison équipée d'alarmes anti-vol et de systèmes de détection d'incendie bénéficie généralement d'une prime plus abordable que celle qui n'en est pas équipée. Non pas que la compagnie d'assurance s'attende à ce qu'une maison soit cambriolée, mais les assurés s'attendent à ce que certains contrôles minimums soient en place en cas d'urgence.



Contrôles minimaux pouvant être mis en œuvre

Dans cette section, nous avons regroupé quelques contrôles de sécurité qui permettent de déjouer les cyberattaques connues et décrivons comment AD360, la solution IAM de ManageEngine, vous aide à les mettre en œuvre efficacement.

Authentification multi-facteurs



Selon [Verizon](#), 61 % des failles de sécurité connues impliquaient des informations d'identification. Protégez votre organisation contre les attaques basées sur les mots de passe, telles que les attaques par force brute, les tentatives de piratage de mots de passe et les attaques par dictionnaire, grâce à MFA. Qu'il s'agisse d'une application ou d'un terminal, l'activation de l'AMF est nécessaire pour aider à protéger votre infrastructure informatique.



Comment nous vous aidons: Avec ManageEngine AD360, vous pouvez configurer le MFA pour les applications sur site et dans le cloud, ainsi que pour les terminaux de votre réseau. Il peut sécuriser les tentatives de connexion locales et à distance aux machines des serveurs et des utilisateurs, prévenir les menaces basées sur les informations d'identification et aider à répondre aux exigences de conformité.

Stratégies de mot de passe

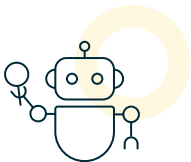


Les mots de passe faibles permettent aux pirates de s'introduire dans un réseau. Selon une étude récente, 68 % des personnes utilisent le même mot de passe pour différents comptes sur différentes plateformes. Cela signifie qu'une fois qu'un compte utilisateur est compromis, tous les comptes ayant le même mot de passe en sont également victimes. Dans ces cas-là, les pirates se contentent de se connecter plutôt que de s'introduire.



Comment nous aidons: Le Password Policy Enforcer d'AD360 est doté de restrictions uniques en matière de mots de passe que l'on ne trouve pas dans les applications de base d'Active Directory (AD) et de cloud computing. Vous pouvez configurer des stratégies qui peuvent être appliquées à des unités organisationnelles spécifiques, rejeter les mots de passe avec répétition consécutive du même caractère, restreindre l'utilisation de palindromes et de mots du dictionnaire comme mots de passe, spécifier le nombre de fois qu'un caractère particulier peut être utilisé, et plus encore.

Analyse du comportement des utilisateurs



Il est presque impossible de parcourir les journaux d'audit et de détecter les menaces. Un outil doté d'une fonction d'analyse du comportement de l'utilisateur (UBA) analysera les journaux d'audit et vous avertira en cas d'activité malveillante ou suspecte.



Comment nous aidons: AD360 vous alerte lorsqu'un serveur est consulté en dehors des heures de bureau, qu'un compte dormant devient actif, qu'un nombre inhabituel d'activités de gestion des utilisateurs est détecté, que quelqu'un tente de supprimer des données, qu'un processus inhabituel s'exécute dans la machine, et plus encore.

Audit des changements



L'audit est à la fois nécessaire et obligatoire lorsqu'il s'agit de la sécurité d'une organisation. Il sert à la fois de mesure réactive et proactive pour répondre aux menaces. Les journaux d'audit permettent d'analyser la surface d'attaque et un outil performant alertera les administrateurs informatiques lorsque les choses semblent suspectes.



Comment nous aidons: Avec l'auditeur de changement piloté par UBA d'AD360, auditez, AD, les serveurs de fichiers, les serveurs Windows et les postes de travail Windows en temps réel. Avec ce seul outil, vous pouvez également auditer une configuration hybride d'Exchange, Azure AD, Microsoft Teams et d'autres services principaux de Microsoft 365.

Surveillance des e-mails



L'hameçonnage est la principale technique utilisée par les pirates informatiques au cours des trois dernières années pour réaliser des failles de sécurité. Il est donc important de surveiller les e-mails ainsi que les serveurs et les machines des utilisateurs.



Comment nous vous aidons: Grâce à la fonction de recherche de contenu d'AD360, vous pouvez identifier les e-mails qui contiennent des informations permettant d'identifier une personne, des pièces jointes d'une taille inhabituelle, des liens suspects et d'autres mots-clés spécifiés qui peuvent indiquer la présence de liens suspects. La surveillance du trafic des e-mails entrants et sortants vous aide à détecter les e-mails en gros qui sont généralement le signe d'une attaque de hameçonnage.

Sauvegarde et récupération



Selon une recherche récente, la fréquence des ransomwares a doublé depuis 2021. Dans cette attaque, les acteurs de la menace exfiltrent des données critiques, les chiffrent et menacent l'organisation d'exposer les données publiquement afin de percevoir une rançon. Si les organisations n'ont pas mis en place une solution de sauvegarde et de récupération appropriée, leur réputation et leurs finances pourraient souffrir.



Comment nous aidons: Le module de sauvegarde et de récupération d'AD360 permet de prendre des sauvegardes progressives de AD sur site, Azure AD, Microsoft Office 365, Google workspace et Exchange sur site. En cas de perte de données due à une attaque par ransomware ou à une erreur humaine, restaurez tous les fichiers, dossiers, attributs utilisateur, objets AD, boîtes aux lettres, calendriers, contacts et toute autre entité de votre espace de travail en un seul clic.

Contrôle d'accès basé sur les rôles



L'abus de privilèges est l'action la plus courante des pirates informatiques impliqués dans les fraudes financières et l'espionnage. L'une des techniques de prévention les plus recommandées pour empêcher l'abus de privilèges est l'utilisation de contrôles d'accès basés sur les rôles. Grâce à cette stratégie, les techniciens n'ont accès qu'aux modules sur lesquels ils doivent travailler, au lieu de disposer de tous les privilèges d'administrateur.



Comment nous aidons: AD360 vous permet de créer des rôles de service d'assistance personnalisés qui peuvent être attribués aux techniciens sans fournir de privilèges d'administrateur. Les rôles personnalisés peuvent être créés pour AD sur site et Microsoft 365 à l'aide d'AD360, et il n'y a aucune restriction quant au nombre de rôles qui peuvent être créés.

Conformité



Se conformer aux mandats industriels est à la fois obligatoire et nécessaire pour la sécurité de l'organisation. La non-conformité affecte la réputation de l'organisation ainsi que ses finances.



Comment nous aidons: Les rapports d'audit granulaires et les capacités de gestion d'AD360 aident à se conformer aux normes SOX, HIPAA, RGPD, PCI DSS, GLBA, FISMA, ISO 27001 et plus encore.

Conclusion

La liste des contrôles minimaux requis ne reste pas toujours la même. Après chaque violation majeure de la sécurité, les souscripteurs d'assurance ajoutent sans cesse de nouveaux contrôles de sécurité à la liste. Au moment de l'achat, les acheteurs sont censés les avoir mis en œuvre.

Les assureurs insistent souvent sur les contrôles anti-hameçonnage, le cryptage des données, la segmentation du réseau et d'autres pratiques d'hygiène de base du réseau pour que les organisations obtiennent un coût décent pour leurs polices. Bien que la cyber-assurance soit un secteur nouveau, avec l'évolution continue vers les services en cloud, l'obtention d'une cyber-assurance sera bientôt inévitable.

ManageEngine AD360

AD360 est une solution intégrée de gestion des identités et des accès (IAM) permettant de gérer les identités des utilisateurs, de régir l'accès aux ressources, de renforcer la sécurité et de garantir la conformité. Du provisionnement des utilisateurs, de la gestion des mots de passe en libre-service et de la surveillance des modifications d'Active Directory à l'authentification unique (SSO) pour les applications d'entreprise, AD360 vous aide à effectuer toutes vos tâches IAM avec une interface simple et conviviale.

Avec AD360, il vous suffit de choisir les composants dont vous avez besoin et de commencer à relever les défis de l'IAM dans les environnements sur site, en cloud et hybrides à partir d'une seule console.

💰 [Obtenir un devis](#)

⬇️ [Télécharger](#)