GoSecure

RAPPORT

GoSecure

CYBERSÉCURITÉ EN ENTREPRISE: PERCEPTIONS, DÉCALAGES ET RÉALITÉ

INTRODUCTION

Des organisations de tous types et de toutes tailles sont continuellement attaquées. Malgré cela, un écart persiste entre les perceptions et pratiques des défenseurs[1] et la réalité actuelle des cybermenaces, ou, plus précisément, les vecteurs d'attaques couramment utilisés par les testeurs d'intrusion lors de leurs exercices de simulations de menaces.

Pour étudier cette différence, nous avons élaboré une enquête sur les perceptions et les pratiques des professionnels de la cybersécurité, en collaboration avec Serene-risc, un réseau canadien de mobilisation des connaissances en matière de cybersécurité. L'enquête visait à comprendre la perception et les pratiques des défenseurs quant à des mesures de sécurité spécifiques ainsi que les mises en œuvre de ces mesures au sein de leurs organisations respectives. En combinant les résultats de l'enquête et notre expérience de tests d'intrusion, nous avons été en mesure de confronter deux perspectives : celle des défenseurs et celle des testeurs d'intrusion, ces derniers étant les mandataires de véritables attaquants. Ce rapport met en lumière les principales conclusions de l'étude et fournit plusieurs conseils pratiques pour aider à remédier certaines disparités identifiées au cours de l'étude.

Le rapport débute avec un aperçu général de la population sondée au cours de l'étude. Ensuite, la première section présente les principaux résultats de l'enquête et les compare avec l'expérience de nos testeurs d'intrusion. C'est au cours de cette analyse que nous avons découvert une disparité entre les attaquants et les défenseurs. La deuxième section creuse davantage cette découverte en croisant les perceptions des défenseurs avec leurs actions rapportées à travers un modèle statistique. Les résultats de celui-ci sont ensuite comparés aux vecteurs d'attaques les plus couramment exploités par les testeurs d'intrusion. C'est avec cet amalgame d'analyses que nous mettons en évidence des biais potentiels chez les défenseurs.

Finalement, à travers des conseils pratiques, cette étude propose des solutions concrètes afin de surmonter ces biais et renforcer les pratiques de cybersécurité des défenseurs, et ce, afin d'améliorer les postures de sécurité des entreprises. Ce faisant, il est probable de croire que les attaquants réels seront plus fréquemment déjoués.

APERÇU GÉNÉRAL DES DONNÉES

À des fins de transparence, une description de la population sondée, de l'équipe d'intrusion de GoSecure ainsi que de l'échantillon des rapports de tests d'intrusion utilisés sont présentées ci-dessous. Aussi, les microdonnées de l'enquête sont disponibles en ligne: https://www.serene-risc.ca/fr/enquete-perception-vs-realite

POPULATION SONDÉE

Au total, 120 personnes ont répondu à l'enquête. Parmi les répondants, il y a un bon éventail de titres représentant des postes de direction et des professions de terrain, tels qu'analyste en sécurité, administrateur de réseau ou administrateur de système. Comme le montre la figure 1, 50,8% des répondants occupent un poste de direction. Ainsi, une grande partie des répondants de l'échantillon représente des personnes ayant des capacités décisionnelles au sein de leur organisation.

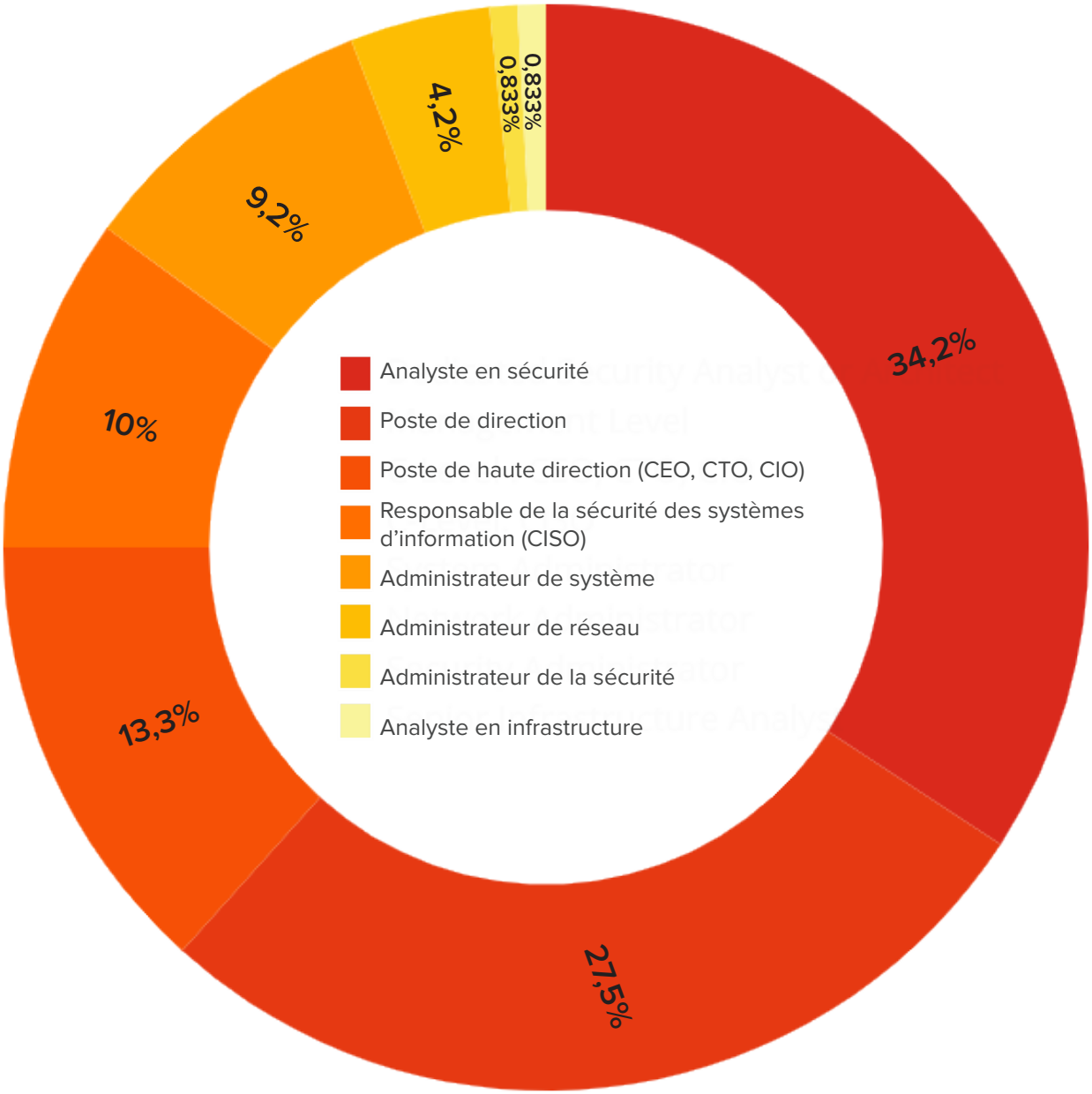


Figure 1– Position occupée par les répondants de l'enquête au sein de leur organisation

La figure 2 illustre qu'en termes d'expérience, 49,2% ont déclaré avoir plus de 10 années d'expérience, 25% entre 5 et 10 ans et 25,8% moins de 5 ans.

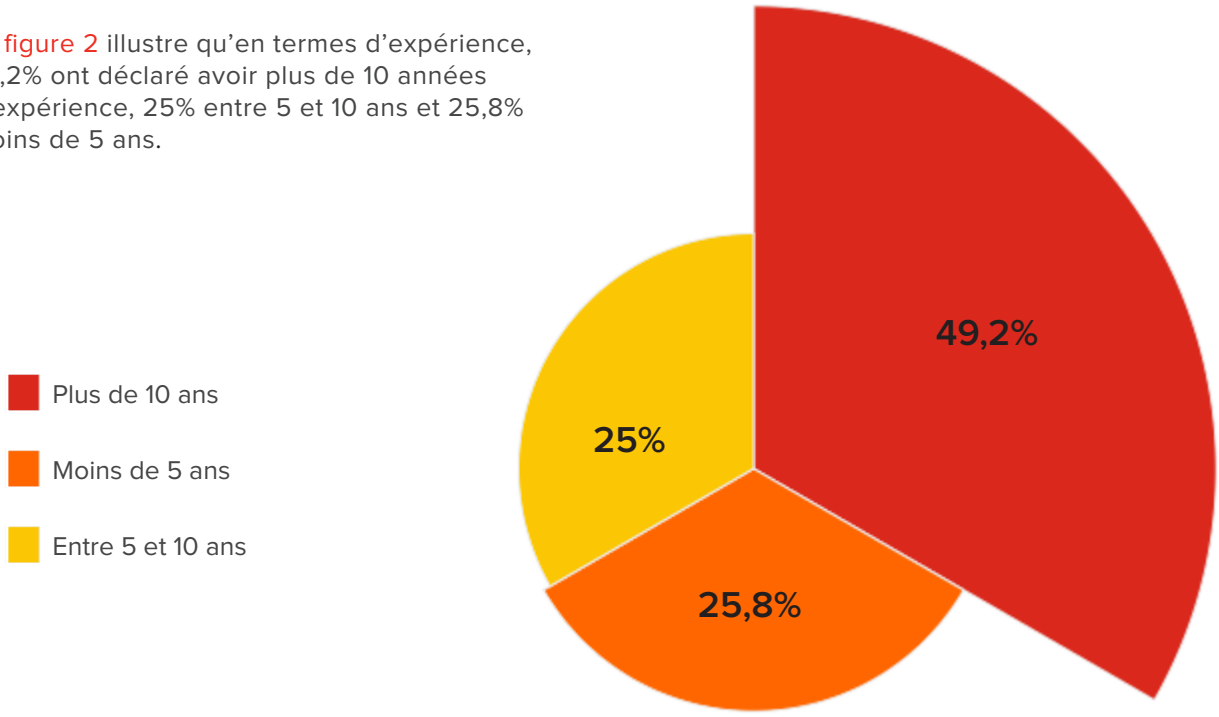


Figure 2 - Années d'expérience des répondants

Au total, 64,1% des répondants ont également déclaré être employés dans une organisation comptant plus de 500 salariés et 84,8% étaient basés au Canada ou aux États-Unis.

Pour les personnes souhaitant approfondir les résultats, les microdonnées de l'enquête sont disponibles en ligne.

EXPÉRIENCE EN MATIÈRE DE TESTS D'INTRUSION

Grâce aux centaines de tests réalisés chaque année à travers l'Amérique du Nord, GoSecure possède une vaste expérience dans la réalisation de tests d'intrusion interne, externe et d'applications Web, les tests d'ingénierie sociale, ainsi que dans les mandats de simulation d'adversaires ou de simulation de menaces, appelé « Red Team ». Les clients testés opèrent dans divers secteurs, tels que les banques, le transport, la vente au détail et l'aviation. La taille de ces clients varie de petites et moyennes organisations à des organisations d'envergure internationale. Les statistiques, concernant les résultats des tests d'intrusion présentés à la section 2.2, comprennent 65 rapports (type de mandats : interne, externe, applications Web) pour lesquelles 182 observations ont été extraites.

PARTIE 1:
ATTAQUE ET DÉFENSE : DISSONANCES FONDAMENTALES

L'enquête visait à évaluer les perceptions et les pratiques des professionnels de la cybersécurité à l'égard de différents aspects de la posture de sécurité de leur organisation. Dans cette section, nous présentons les principaux résultats concernant l'authentification à facteurs multiples, les politiques de mots de passe, les mesures de sécurité spécifiques, la gestion des mises à jour, les fonctionnalités de produits activées par défaut, les inventaires d'actifs et la surveillance des actifs (« endpoint visibility »). Chaque sous-section propose une comparaison entre les résultats de l'enquête auprès des défenseurs et l'expérience de nos testeurs d'intrusion. Des conseils pratiques sont également présentés à la fin de chaque sous-section afin de remédier aux disparités détectées entre les perceptions et les pratiques des défenseurs et l'expérience de nos testeurs d'intrusion.

1 - AUTHENTIFICATION À FACTEURS MULTIPLES

Les répondants ont d'abord été interrogés sur l'authentification à facteurs multiples, une mesure de sécurité exigeant qu'un utilisateur présente au moins deux facteurs, tels que « quelque chose qu'il connaît » et « quelque chose qu'il possède », avant de se voir accorder l'accès à un système. Sur une échelle de 1 (peu important) à 5 (très important), 93,3% des personnes interrogées ont répondu que l'authentification à facteurs multiples est importante ou très importante pour la sécurité de leur organisation.

Lorsque nous leur avons demandé si une telle mesure était implantée sur le réseau externe de leur organisation, 45% ont répondu oui, 41,7% partiellement et 13,3% non, conformément à ce qui est illustré dans la figure 3. Nous leur avons ensuite demandé si l'authentification à facteurs multiples avait été implantée sur leur réseau interne, mesure qui pourrait empêcher un attaquant ayant ouvert une brèche dans le système de pivoter à l'interne vers des actifs de plus grande valeur. À cette question, la distribution des réponses a été plus conservatrice, comme le montre la figure 4. En effet, au total 23,3% des répondants ont indiqué qu'ils avaient mis en application l'authentification à facteurs multiples dans son intégralité sur le réseau interne, 40,8% partiellement et 35,8% ont déclaré qu'ils n'avaient pas implanté cette mesure de sécurité.

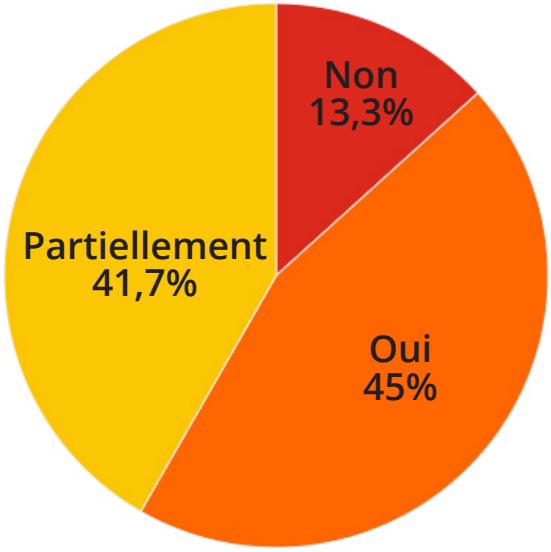


Figure 3 - Authentification à facteurs multiples sur le périmètre externe

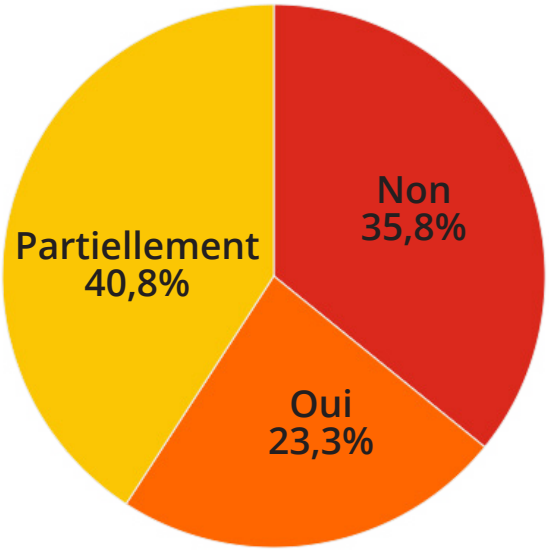


Figure 4 - Authentification à facteurs multiples sur le périmètre interne

EXPÉRIENCE DES TESTEURS D'INTRUSION

Les résultats des tests d'intrusion ont démontré que l'authentification à facteurs multiples s'avère très efficace pour bloquer les attaquants. Toutefois, une telle mesure ne doit pas seulement être implantée sur le service de courrier électronique, endroit où l'authentification à multiples facteurs est la plus couramment appliquée, mais doit également être mise en œuvre sur tous les services externes exposés. De plus, il est important de noter qu'une question secrète n'est pas considérée comme un second facteur, puisqu'un mot de passe et une question secrète sont tous deux basés sur la connaissance de l'utilisateur. Chaque facteur doit provenir d'un vecteur d'authentification différent : par exemple, un mot de passe renvoie à quelque chose que l'on connaît, tandis qu'un numéro RSA OTP (« One Time Password ») renvoie à quelque chose que l'on possède.

De même, les testeurs d'intrusion de GoSecure ont été surpris de constater que 23% des personnes interrogées avaient déclaré avoir mis en place une authentification à facteurs multiples sur leur réseau interne, puisqu'ils ont rarement été confrontés à de telles mesures de sécurité dans les organisations. Ils ont également mentionné que, même si les services essentiels disposent de l'authentification à facteurs multiples, les activités quotidiennes telles que les accès à distance aux serveurs (par exemple via RDP) ou l'accès au partage de fichiers sont généralement non sécurisées.

CONSEILS PRATIQUES POUR L'AUTHENTIFICATION À FACTEURS MULTIPLES

- Appliquer l'authentification à facteurs multiples sur tous les services exposés de l'organisation (VPN, courrier électronique, RDP, etc.);
- L'authentification à facteurs multiples par SMS s'avère plus efficace que l'authentification à facteur unique;

  Gardez en tête que pour les services essentiels qui pourraient être ciblés par des attaquants très motivés, l'authentification à facteurs multiples par SMS pourrait être contournée en utilisant une technique appelée « SIM Swapping ».
- L'utilisation de jetons logiciels constitue une solution d'authentification à facteurs multiples abordable. Ceux-ci fonctionnent à partir d'une application sur votre téléphone ou sur un ordinateur plutôt que de s'appuyer sur un jeton physique comme une clé RSA. C'est l'un des cas où des logiciels en code source ouvert existent, mais leur gestion et leur intégration sont relativement complexes. L'utilisation d'une solution commerciale peut éventuellement être envisagée si la facilité de mise en œuvre de la mesure est un élément qui vous préoccupe.

  Sachez que les informations envoyées à l'utilisateur pour inscrire le jeton peuvent parfois être réutilisées par un attaquant si celui-ci y a accès. Il est donc important d'encourager les utilisateurs à détruire le fichier ou le courrier électronique une fois qu'ils ont enregistré leur jeton logiciel.

2 - POLITIQUES DE MOTS DE PASSE

L'importance d'avoir une bonne politique de mots de passe est bien connue en cybersécurité. Lorsque nous avons demandé aux répondants de choisir quelles étaient les exigences minimales d'une politique de mots de passe adéquate, 56,3% ont indiqué que les mots de passe devaient comporter un minimum de six caractères et 74,8% ont déclaré que les mots de passe doivent être un mélange de lettres, de chiffres et de caractères spéciaux. Aussi, 83,1% des personnes interrogées s'accordent pour dire que la réutilisation des mots de passe devrait être interdite, 81,5% sont d'accord pour dire que les mots de passe populaires devraient également être interdits et 62,2% ont déclaré que les mots du dictionnaire devraient tout simplement être prohibés.

De plus, nous avons remarqué deux tendances intéressantes dans les données concernant les changements de mots de passe : 43,7% des personnes interrogées ont convenu que des changements de mot de passe réguliers (par exemple, tous les 90 jours) devaient être une exigence minimale, tandis que 43,7% ont déclaré le contraire, c'est-à-dire aucun ou peu de changement de mot de passe (une ou deux fois par an ou en cas de compromission présumée du mot de passe). Certaines personnes ont également choisi les deux options.

Cette divergence dans les résultats peut s'expliquer par l'idée que le changement de mot de passe obligatoire est une arme à double tranchant : il peut atténuer les risques lorsqu'un mot de passe est potentiellement compromis, mais semble également être une méthode qui déplait aux utilisateurs, qui finissent par trouver des mots de passe plus simples ou par simplement contourner cette politique de sécurité en ajoutant un numéro à leurs mots de passe précédents. L'acceptation d'une mesure de sécurité par les utilisateurs est essentielle pour que celle-ci soit efficace. Lorsque les utilisateurs n'adhèrent pas à ce contrôle, ils trouveront toujours un moyen de le contourner. Vous trouverez ci-dessous une bonne, et malheureusement vraie, histoire racontée par un de nos testeurs d'intrusion sur la manière dont un utilisateur a réussi à contourner un dispositif de sécurité :

« La politique en matière de mots de passe qui avait été mise en place empêchait les utilisateurs de choisir les six derniers mots de passe qu'ils avaient préalablement utilisés. Dans l'optique de contourner cette politique, les utilisateurs pouvaient changer leurs mots de passe six fois de suite dans une courte période de temps et revenir à leur mot de passe préféré. C'est notamment ce que faisait une personne, tous les trois mois, afin que son mot de passe soit toujours le nom de son chat. »

Les répondants ont également été questionnés à savoir si l'organisation pour laquelle ils travaillent, en tant que spécialistes de la sécurité, répond aux exigences minimales de la politique de mots de passe qu'ils venaient de choisir. La répartition des réponses est illustrée dans la figure 5 et montre que 17,2% ont répondu non, 23,3% ont répondu partiellement et 59,5% ont répondu oui. Bien qu'assez optimiste, la section ci-dessous démontre que ces résultats vont toutefois à l'encontre de l'expérience de nos testeurs d'intrusion.

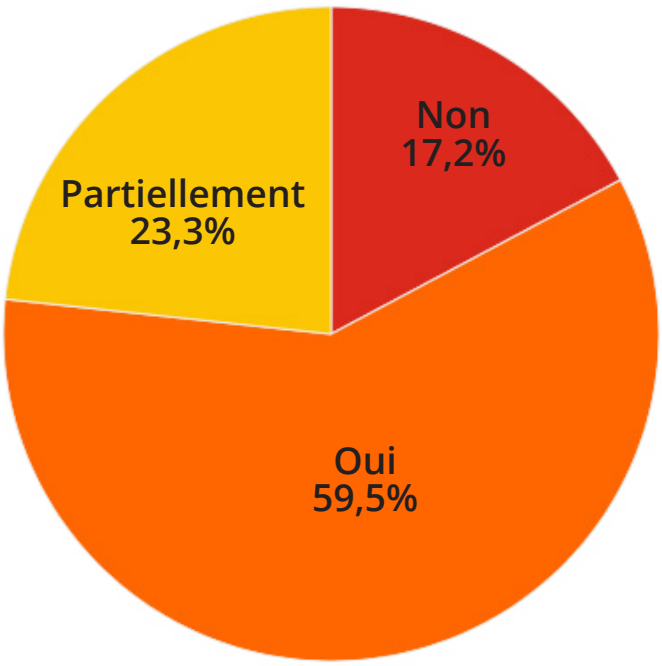


Figure 5 - Organisation répondant aux exigences minimales fixées par les répondants en matière de politique de mots de passe

EXPÉRIENCE DES TESTEURS D'INTRUSION

Les testeurs d'intrusion utilisent souvent deux techniques pour compromettre les systèmes avec des mots de passe : la pulvérisation de mots de passe et les attaques par dictionnaire. La pulvérisation de mots de passe consiste à essayer un mot de passe populaire sur un grand nombre de comptes et à trouver le maillon faible : le compte avec LE mot de passe devinable. Généralement, lors de telles attaques, les testeurs d'intrusion disposent d'une liste de mots de passe vedettes. Cette liste comprend des mots de passe simples tels que « Password123 », « Welcome1 »,

« Letmein1 », SaisonAnnée (ex. Hiver2020) et NomDeCompagnie123 (ex. GoSecure123). En utilisant l'attaque de pulvérisation de mots de passe, les testeurs d'intrusion ont déclaré avoir réussi, en moyenne, dans 25% des cas. L'attaque par dictionnaire, en revanche, exige que les testeurs d'intrusion aient accès à une liste de mots de passe codés/hachés (ce qui est possible grâce à diverses attaques, telles que l'usurpation ARP) et essaient de trouver le mot de passe en texte clair en codant/hachant une liste connue de mots de passe et en les testant par rapport à la liste compromise. Dans une telle situation, les testeurs d'intrusion trouvent, dans 20% des cas, des mots de passe contenant : un nom et quatre chiffres, comme Julia1984, dans 4 à 5% des cas, des mots de passe contenant des mots vulgaires (vous pouvez probablement deviner des exemples) et dans 4 à 5% des cas, des mots de passe contenant des mots de vacances, comme BeachCuba1. Lors de l'attaque par dictionnaire, les testeurs d'intrusion ont déclaré avoir réussi à trouver, dans la plupart du temps, au moins un mot de passe.

De plus, lors des audits de mots de passe où les testeurs d'intrusion tentent de «cracker» les hachés de mots de passe d'une base de données de comptes d'utilisateurs, généralement trouvés lors d'un test d'intrusion, ceux-ci ont déclaré avoir pu récupérer jusqu'à 98,3% des mots de passe d'une organisation.

Ainsi, lorsque 60% des personnes interrogées déclarent que leur organisation satisfait les exigences minimales d'une bonne politique de mots de passe, il semble que cela ne corresponde pas à l'expérience de nos testeurs d'intrusion. Cela peut s'expliquer par le fait que des mots de passe, tels que NomDeCompagnie2019*, répondent aux exigences d'une bonne politique de base de mots de passe, mais les testeurs d'intrusion sont conscients de ces différentes variations et les utilisent comme levier lors de leurs tests. De plus, la probabilité qu'un seul utilisateur possède ce genre de mot de passe augmente considérablement avec le nombre d'utilisateurs

CONSEILS PRATIQUES SUR LES POLITIQUES DE MOTS DE PASSE

- Bloquez tous les mots reliés à l'organisation (par exemple, avec un filtre de mot de passe), même si des caractères spéciaux ou des chiffres sont ajoutés aux mots de passe. Si nécessaire, vous pouvez utiliser la fonction de filtrage des mots de passe de Microsoft;
- Mentionnez aux employés que les mots de passe ne doivent pas être liés à des informations publiquement disponibles à leur sujet sur les réseaux sociaux, tels que Facebook, LinkedIn ou Instagram. Les testeurs d'intrusion utilisent souvent ces informations lors des tests;
- Lorsqu'un incident de sécurité se produit ou qu'une personne externe accède à la base de données des utilisateurs, vous devez imposer un changement de mots de passe sur l'ensemble du réseau, y compris les comptes de service et, surtout, le compte krbtgt, le compte de service le plus puissant d'« Active Directory »;
- Des activités continues d'audit de mots de passe peuvent être réalisées afin d'identifier de manière proactive tout mot de passe potentiellement faible. Par exemple, l'extraction périodique de la base de données des utilisateurs pour tenter de «cracker» les hachés de mots de passe et forcer les changements de mots de passe pour tous les comptes « crackés» représente une pratique supplémentaire efficace.

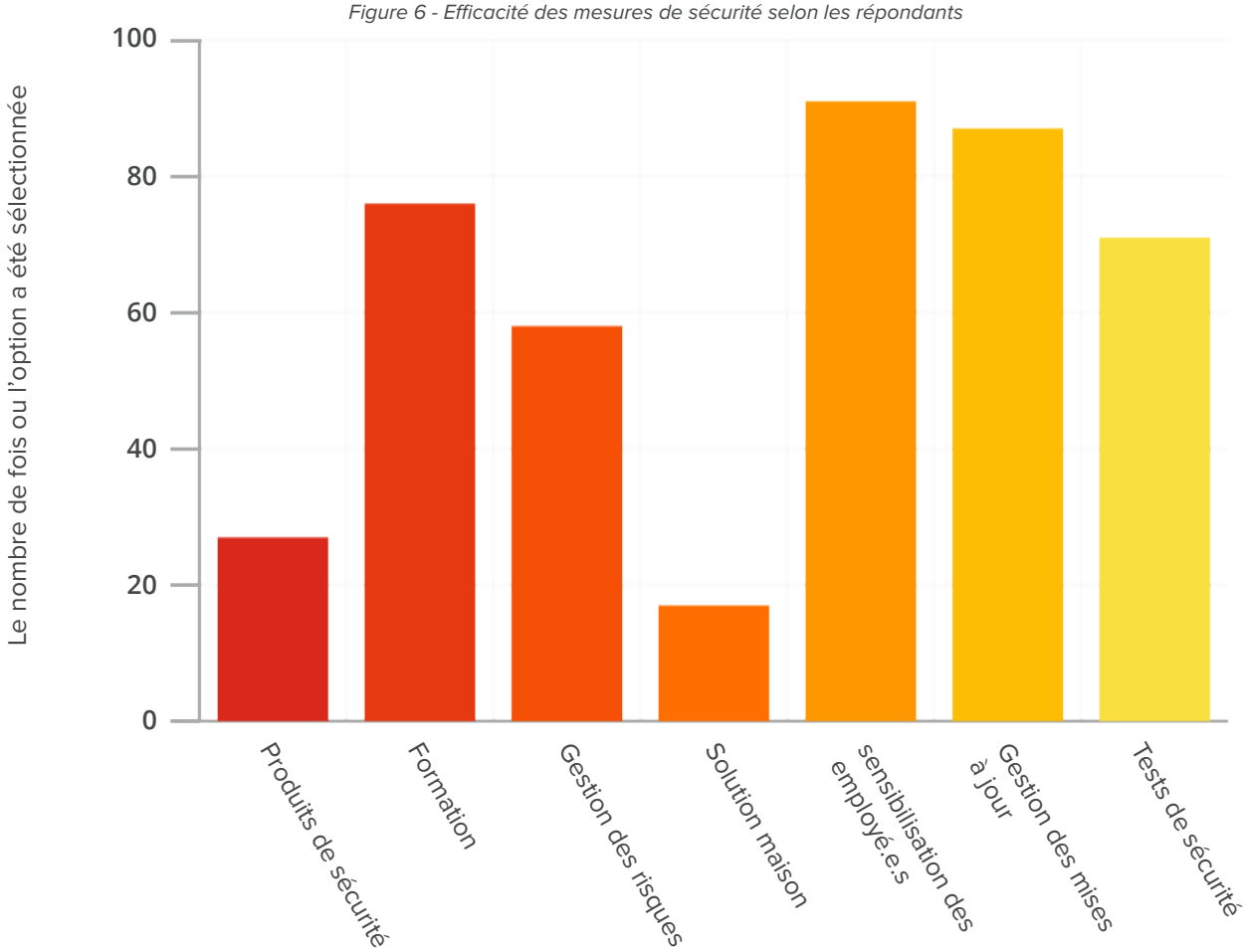
3 - LES MESURES DE SÉCURITÉ

Nous avons demandé aux répondants quelles mesures de sécurité (basées sur un ensemble de mesures prédéterminées) permettraient d'accroître la posture de sécurité de leur organisation. Ils pouvaient choisir plus d'une mesure parmi celles-ci :

- De meilleurs produits de sécurité (par exemple, antivirus/pare-feu/WAF);
- Une meilleure formation pour les employés TI;
- Une meilleure gestion des risques et de meilleures politiques de sécurité de l'information;
- Un développement à l'interne de solutions de sécurité (solution maison);
- L'éducation et la sensibilisation des employés;
- Une meilleure gestion des mises à jour ;
- Davantage d'évaluations et/ou de tests de sécurité.

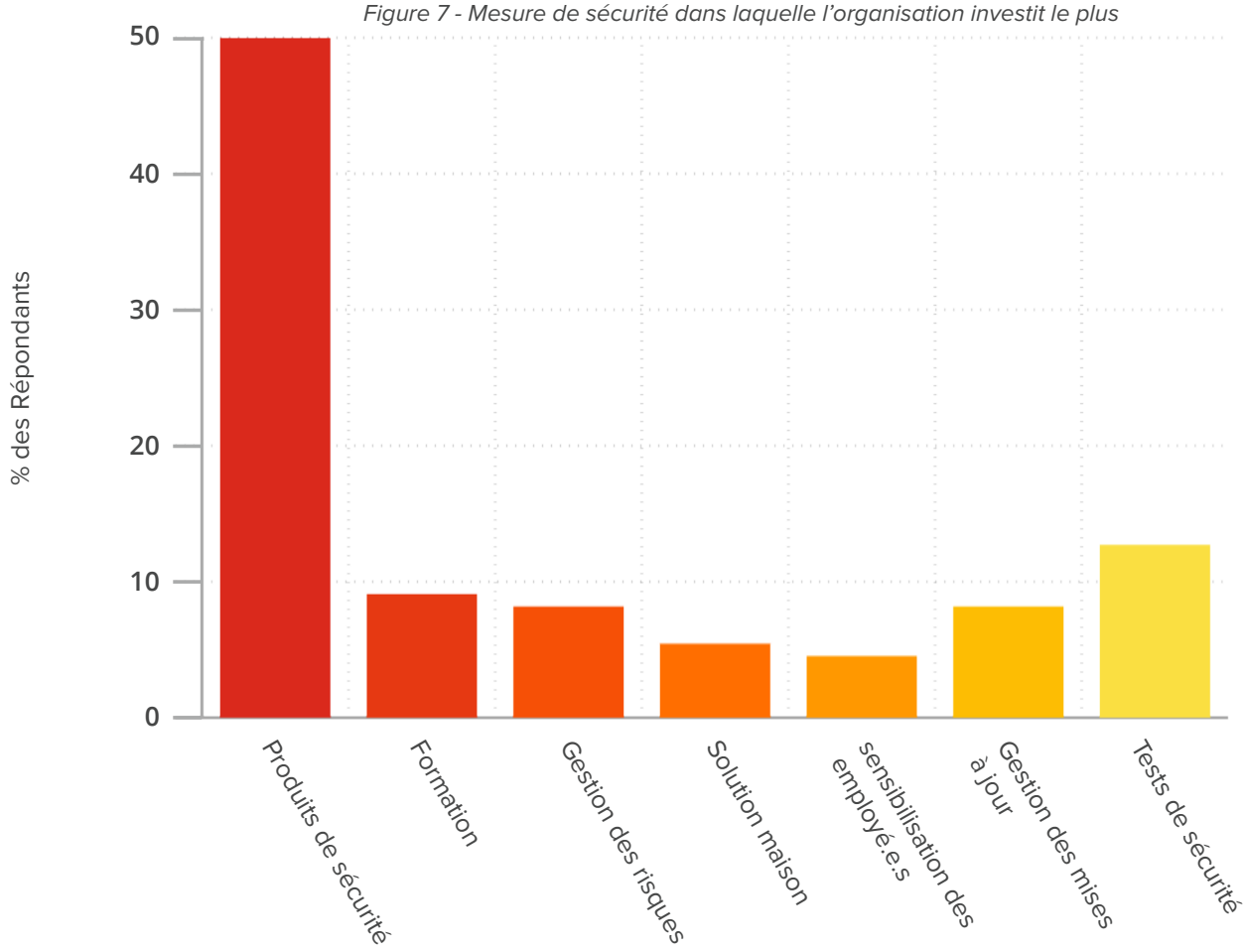
La répartition des réponses est présentée à la figure 6. Nous pouvons observer que l'éducation et la sensibilisation des employés est en tête, suivie par une meilleure gestion des mises à jour, la formation des employés TI et davantage d'évaluations et/ou de tests de sécurité. Ces mesures sont donc considérées efficaces par les répondants pour renforcer la sécurité de leur organisation. Les produits de sécurité (par exemple, antivirus/pare-feu/WAF) et les solutions de sécurité « maison », en revanche, ne semblent pas être des mesures populaires parmi ceux-ci.

Figure 6 - Efficacité des mesures de sécurité selon les répondants



Les répondants ont ensuite été invités à sélectionner la mesure de sécurité dans laquelle leur organisation a le plus investi, les résultats sont présentés dans la figure 7. Selon près de 50% des répondants, les produits de sécurité (par exemple, antivirus/pare-feu/WAF) correspondent à la mesure de sécurité dans laquelle leur organisation a investi le plus.

Figure 7 - Mesure de sécurité dans laquelle l'organisation investit le plus



EXPÉRIENCE DES TESTEURS D'INTRUSION

Les testeurs d'intrusion conviennent que la sensibilisation des employés est importante, mais soulignent qu'elle n'est pas une panacée. En effet, la formation visant à la sensibilisation des employés est souvent mal ciblée, limitée dans le temps et, la plupart du temps, présente des acteurs et des scénarios de menaces désuets (tels que les princes nigériens ayant besoin d'argent). Somme toute, l'éducation et la sensibilisation des employés à la sécurité représente une mesure qui n'est pas nécessairement inefficace, mais de nombreux facteurs empêchent qu'elle devienne une solution réellement viable.

Plutôt que d'éduquer et de sensibiliser la majorité des employés à la sécurité, les testeurs d'intrusion de GoSecure ont constaté qu'une formation continue des employés TI est une mesure beaucoup plus efficace pour contrer les attaques. En effet, le travail des testeurs est beaucoup plus difficile lorsque les professionnels TI savent comment renforcer les serveurs et bloquer les maillons faibles, en plus d'être continuellement conscients des nouvelles menaces et des nouvelles techniques publiées en ligne.

De plus, les testeurs d'intrusion de GoSecure n'ont pas été surpris que les produits de sécurité soient la mesure dans laquelle les organisations investissent le plus. Lors des conférences sur la cybersécurité, les participants sont bombardés de messages vantant les dernières technologies garantissant la résolution de tous les problèmes de sécurité. Cependant, même si la plupart des clients sur lesquels les testeurs d'intrusion ont enquêté disposent d'un excellent antivirus, d'un pare-feu ou d'un WAF sur le périmètre externe, ils n'en ont généralement aucun sur le réseau interne. Ainsi, les testeurs mentionnent que dès qu'ils s'introduisent dans un système, le pivotement à l'interne est d'une facilité choquante

CONSEILS PRATIQUES SUR LES INVESTISSEMENTS DANS LES MESURES DE SÉCURITÉ

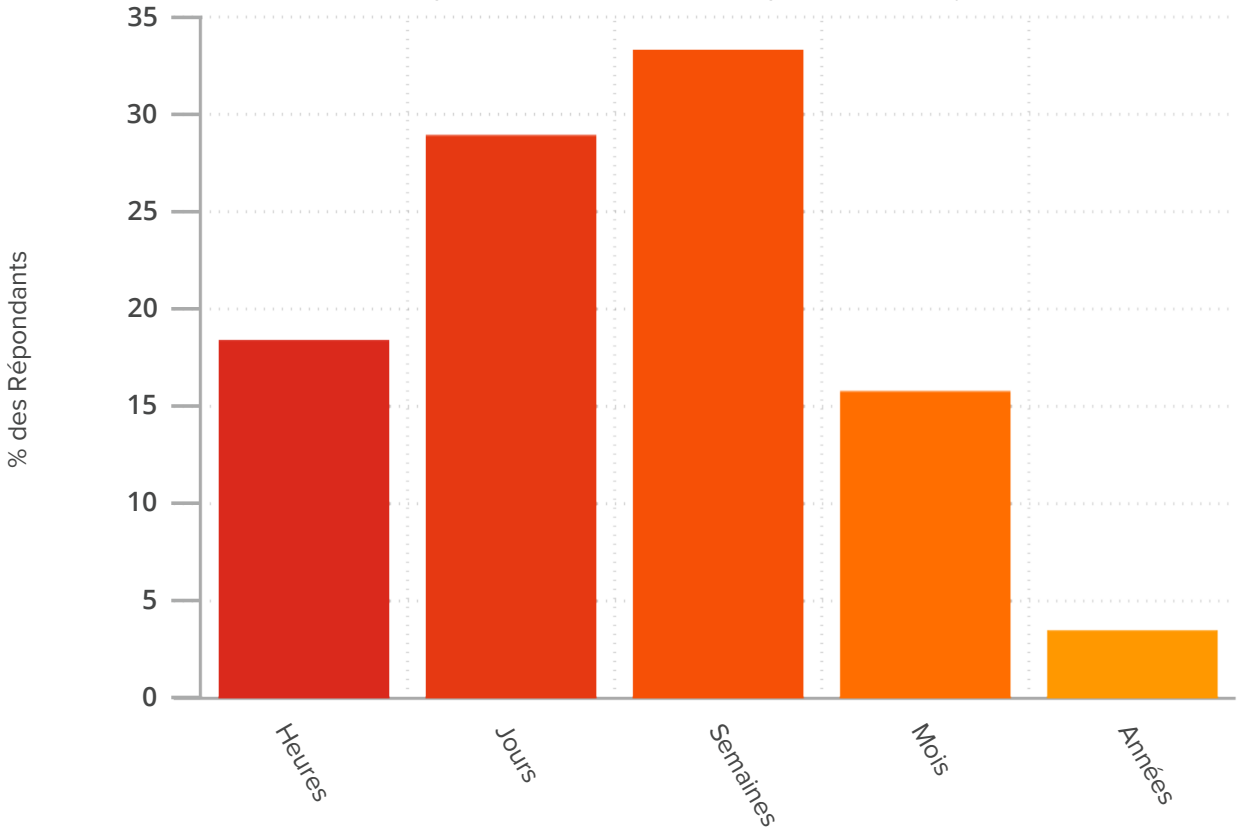
- Lorsque vous planifiez la mise en œuvre de mesures de sécurité, prenez d'abord en considération la maturité de la posture de sécurité de votre organisation ainsi que les technologies actuellement implantées;
- Investissez dans la formation continue de votre personnel TI.

4 - GESTION DES MISES À JOUR

Au cours des dernières années, la gestion des mises à jour est LA mesure de sécurité au centre du discours de l'industrie en matière de cybersécurité. Il est évident qu'avec de nouvelles vulnérabilités divulguées chaque jour, un conseil tel que : Assurez-vous que vos systèmes soient mis à jour! est régulièrement mentionné par les partisans du domaine.

Ainsi, lorsque nous avons demandé aux personnes interrogées quelle était l'importance de la gestion des mises à jour pour la sécurité de leurs systèmes, plus de 90% ont déclaré qu'elle était importante ou très importante. Les résultats deviennent intéressants lorsque nous leur avons demandé « Combien de temps est-il nécessaire à votre organisation pour appliquer une mise à jour de sécurité, une fois qu'elle est disponible? ». Comme le démontre la figure 8, 18,42% ont répondu en quelques heures, 28,95% en quelques jours, 33,33% en quelques semaines, 15,79% en quelques mois et 3,51% en quelques années. Avec plus de 52% des répondants qui disent qu'il faut des semaines, voire plus, pour appliquer les mises à jour, il n'est pas étonnant que les rançongiciels, exploitant des vulnérabilités connues, soient autant utilisés par les attaquants.

Figure 8 - Temps nécessaire avant la gestion des mises à jour



EXPÉRIENCE DES TESTEURS D'INTRUSION

Sans grande surprise, les testeurs d'intrusion de GoSecure ont indiqué que les résultats exprimés ci-dessus sont conformes à leurs expériences (bien qu'ils n'aient jamais eu connaissance d'un service informatique répondant dans les heures qui suivent à une nouvelle mise à jour de sécurité). Aussi, ils ont souligné que la plupart des organisations testées avaient une bonne politique de gestion des mises à jour en ce qui concerne Windows. Cependant, certaines applications considérées comme cruciales sont généralement moins bien maintenues, c'est le cas notamment de Java, Flash ou Firefox. De ce fait, lorsque ces applications ne sont pas mises à jour, elles peuvent créer des vulnérabilités majeures; vulnérabilités avec lesquelles les testeurs sont familiers et prêts à exploiter.

De plus, les testeurs découvrent encore des vulnérabilités critiques telles qu' « EternalBlue » (MS17-010), sur certains des systèmes qu'ils testent, alors qu'un correctif a été publié par Microsoft en 2017. Avant d'effectuer un test d'intrusion, il est donc recommandé de procéder à un examen approfondi de toutes les mises à jour disponibles (y compris les mises à jour autre que celles de Windows) et d'en effectuer le plus possible dans votre organisation.

CONSEILS PRATIQUES POUR LA GESTION DES MISES À JOUR

- Envisagez la standardisation des outils utilisés par vos employés. Par exemple, si vos employés utilisent Chrome, Firefox, Edge et Opera, il sera difficile de mettre à jour tous ces navigateurs. Ainsi, dans cette situation, limiter l'accessibilité des utilisateurs à un seul navigateur pourrait faciliter le processus de gestion des mises à jour;
- Développez un processus de gestion des vulnérabilités qui permet, en autres, d'identifier les mises à jour manquantes et les problèmes de configuration;
- Afin de minimiser les risques d'interruption de service causés par des mises à jour problématiques, procédez à un déploiement progressif. Dans la terminologie de Microsoft, cela correspond à un « déploiement par phase »;
- Utilisez un outil de balayage de vulnérabilités pour identifier les vulnérabilités présentes sur le réseau de l'organisation. Si nécessaire, vous pouvez utiliser « OpenVAS », un logiciel en code source ouvert.

5 - LES FONCTIONNALITÉS ACTIVÉES PAR DÉFAUT DANS LES PRODUITS

De nombreuses fonctionnalités dans les produits sont vulnérables par défaut et leur exploitation facilite grandement la vie d'un testeur d'intrusion. Les répondants ont été invités, sur la base de leur expérience, à indiquer dans quelle mesure les produits propriétaires (par exemple, Windows ou SAP), utilisés par la plupart des organisations, sont sécuritaires lorsqu'ils sont à jour. Au total, 57,3% ont répondu « sécuritaire » ou « extrêmement sécuritaire », 35,4% « moyennement sécuritaire » et 7,69% « pas du tout sécuritaire » ou « très limité ». Nous leur avons ensuite demandé si leur organisation enquêtait sur ces produits pour identifier et désactiver les paramètres de sécurité qui pourraient représenter un risque. Comme le démontre la figure 9, 64,1% des répondants ont déclaré avoir validé les paramètres de sécurité, tandis que 28,2% ont répondu non et 7,69% ne le savaient pas.

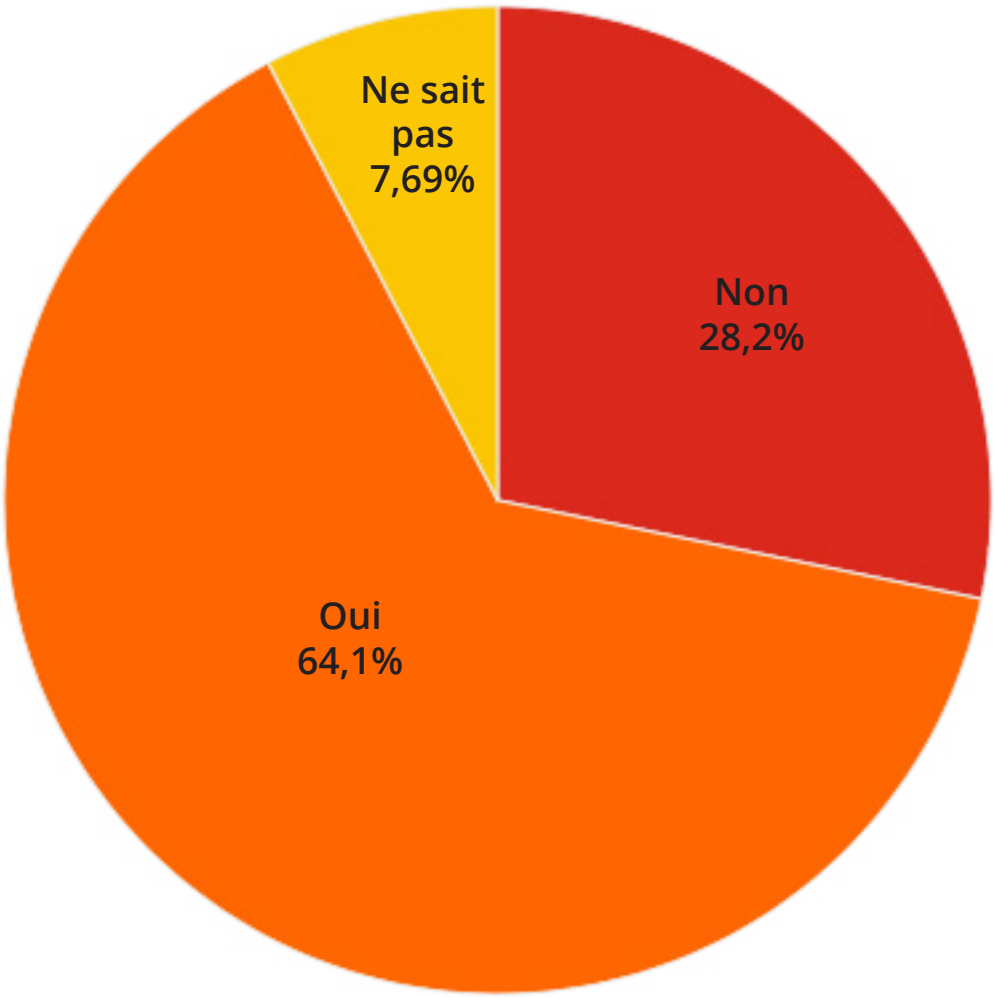


Figure 9 -Enquête faite sur la configuration par défauts des logiciels

EXPÉRIENCE DES TESTEURS D'INTRUSION

Les fonctionnalités vulnérables par défaut dans les produits représentent soit une vulnérabilité (un testeur d'intrusion peut exploiter la fonctionnalité pour accéder aux systèmes), soit un contrôle manquant (une fonctionnalité supplémentaire qui aide les testeurs dans leur processus d'attaque). Les testeurs de GoSecure estiment que, dans environ 80% des tests d'intrusion, ces vecteurs d'attaque sont exploités. Par exemple, les protocoles NetBIOS et LLMNR, qui permettent la capture de plusieurs formes d'identifiants encodés, sont rarement désactivées et représente une fonctionnalité vulnérable cruciale. Les mots de passe par défaut, les identifiants Windows stockés en mémoire, les zones DNS non sécurisées, IPv6 activé par défaut et l'usurpation fonctionnelle du protocole ARP sont d'autres exemples de fonctionnalités vulnérables par défaut.

Les testeurs d'intrusion ont donc été surpris de constater que 64% des répondants ont déclaré avoir mitigé ce risque. Peut-être ont-ils accepté les risques associés à ces fonctionnalités? Cependant, les organisations ont peut-être aussi simplement enquêté sur la sécurité d'un produit en demandant un test de sécurité ou un audit avant leur déploiement. Le produit peut sembler très sécuritaire dans les rapports de sécurité, mais son déploiement dans l'environnement de l'organisation peut être très différent de l'environnement dans lequel il a été testé pour la première fois. En effet, l'état de la sécurité dans le laboratoire d'un fournisseur et l'état de la sécurité dans un environnement corporatif sont très différents

CONSEILS PRATIQUES SUR LA CONFIGURATION DES PRODUITS

- Si votre organisation utilise le système d'exploitation Windows et que vous ne disposez pas de systèmes d'exploitation désuets (tels que Windows NT) dans votre environnement, la désactivation des protocoles NetBIOS et LLMNR est une solution simple et rapide pour augmenter la sécurité de votre réseau interne;
- Si NetBIOS est nécessaire dans l'environnement, isolez les actifs qui le nécessitent du réseau principal de l'organisation, mettez en place un serveur WINS pour la résolution du nom NetBIOS et configurez ces ordinateurs pour qu'ils utilisent le serveur WINS en appliquant la clé de registre correspondante via une politique de groupe (GPO). De plus, compte tenu de l'importance de ce vecteur d'attaque pour les testeurs d'intrusion, il convient de mettre fortement l'accent sur la désactivation des fonctionnalités vulnérables par défaut dans les produits. Malheureusement, il n'est pas possible de dresser une liste explicative, car il y a tout simplement trop de produits à énumérer;
- À long terme, établir un standard de configuration de sécurité pour les différents types de systèmes existant dans l'organisation. Le « Center for Internet Security » (CIS), avec ses « CIS benchmarks », offre une norme mondialement reconnue proposant des directives de configuration détaillées pour différentes technologies.

6 - INVENTAIRE DES ACTIFS

Par la suite, nous avons demandé aux répondants s'ils tenaient un inventaire complet de leurs actifs externes (adresses IP et domaines) et internes (adresses IP, serveurs et domaines). Comme le montre la figure 10, la plupart des répondants, soit 77,1%, ont déclaré qu'ils tenaient un inventaire complet de leurs actifs, tandis que 17,8% ont répondu non et que 5,08% ne le savaient pas. Bien qu'il soit très encourageant de constater qu'un si grand nombre d'organisations tiennent un inventaire de leurs actifs, c'est notamment l'exactitude de cet inventaire qui est remise en question lors d'un test d'intrusion.

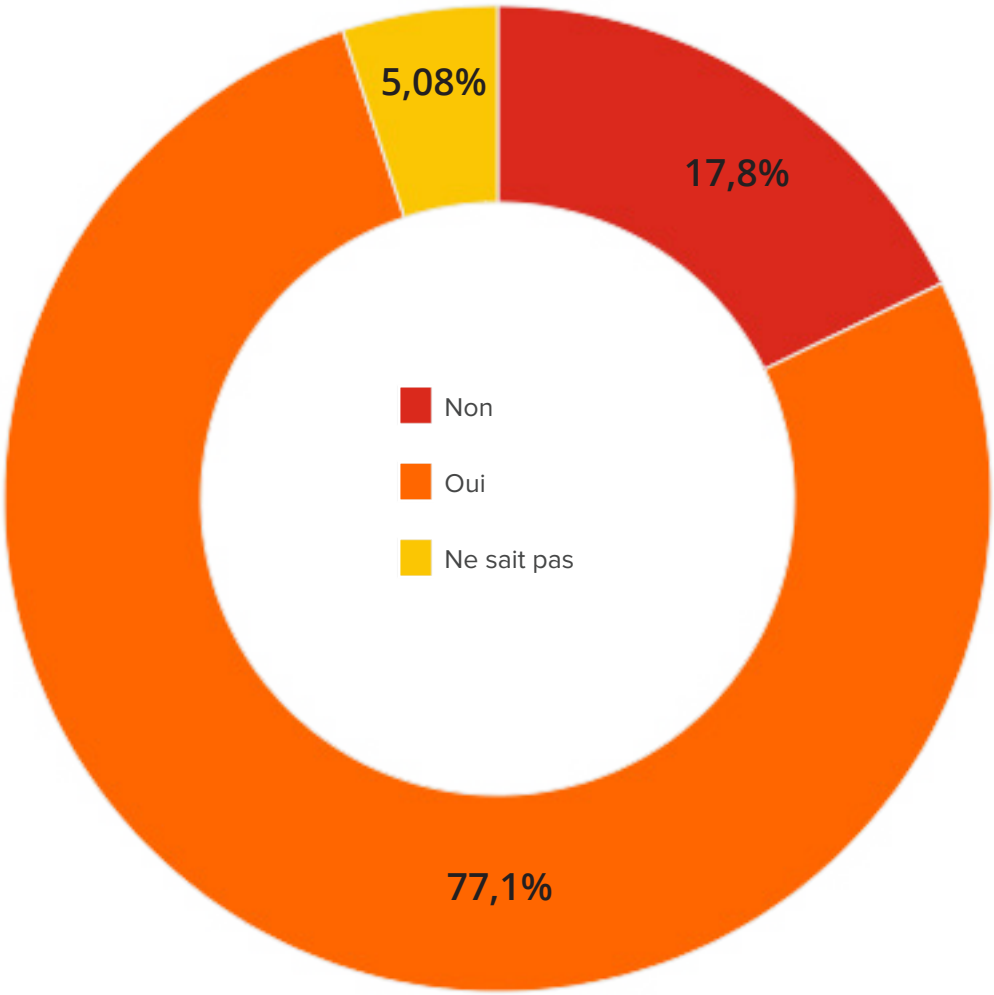


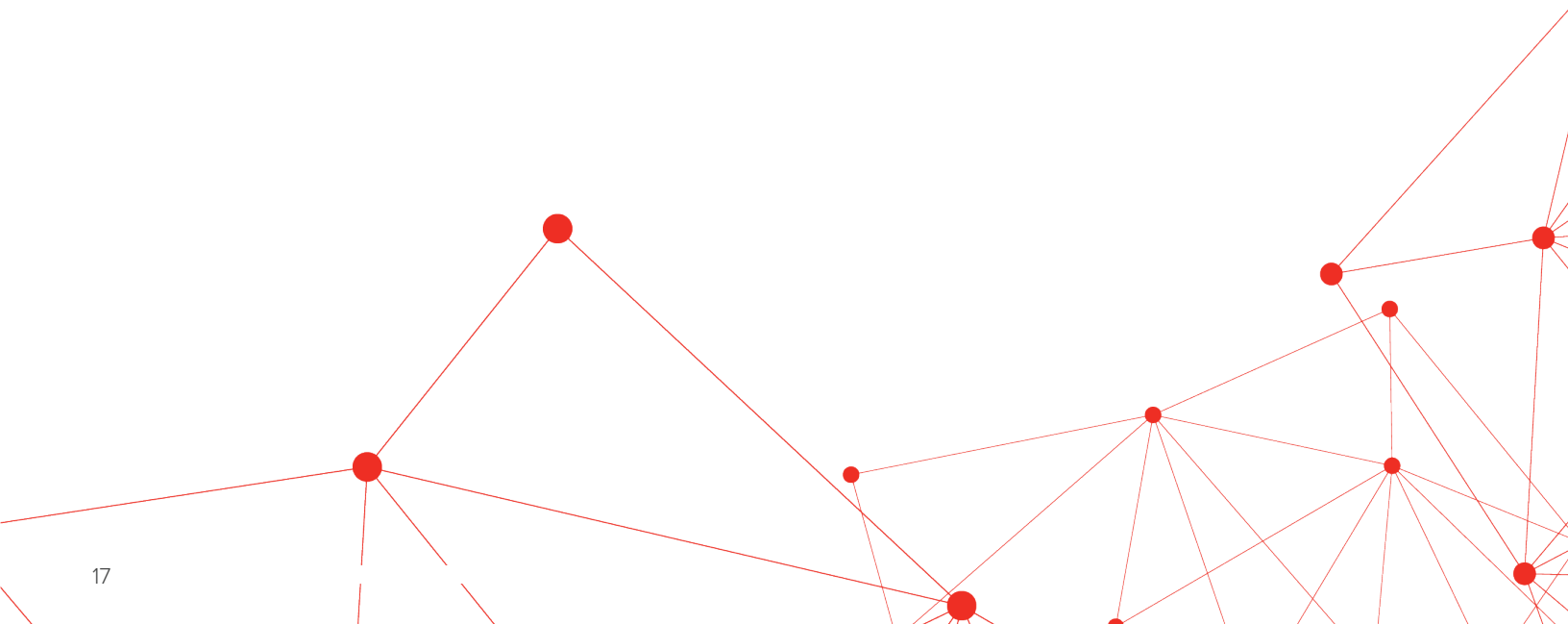
Figure 10 - Inventaire des actifs

EXPÉRIENCE DES TESTEURS D'INTRUSION

Dans l'ensemble, les testeurs d'intrusion de GoSecure ont mentionné que la plupart des organisations testées maintenaient un inventaire d'actifs. Cependant, la plupart du temps, l'inventaire est dans un état incertain ou n'est pas entièrement à jour. Lors de tests d'intrusion, par exemple, les testeurs ont réussi à exploiter des serveurs oubliés pour s'introduire dans des réseaux. Ils ont même mentionné le vol d'ordinateurs portables pendant des mandats réalisés par l'équipe de « Red Team ». Fréquemment, lors de ces « Red Teams », les employés n'ont pas remarqué qu'un appareil était manquant.

CONSEILS PRATIQUES SUR L'INVENTAIRE DES ACTIFS

- Assurez-vous que votre inventaire actuel d'actifs informatiques est mis à jour et qu'un processus est en place afin de le maintenir. Le NIST dispose de nombreuses ressources sur ce sujet (en anglais);
- Envisagez l'utilisation des outils de sécurité offensifs pour évaluer votre inventaire d'actifs. Des outils dont le code source est disponible, tels que BloodHound (Cette présentation à DerbyCon montre comment utiliser BloodHound avec une perspective de défense) ou ADRecon, permettent d'avoir la « vue de l'attaquant » sur les actifs. Cela peut changer la perception de l'équipe TI sur les actifs, tout en permettant d'en découvrir certains qui ne figuraient pas dans l'inventaire officiel;
- À long terme, établir une stratégie globale pour la gestion des actifs tout au long de leur cycle de vie. Les processus de sécurité définis subséquemment, tels que la gestion des risques, la gestion des mises à jour et la reprise après compromission devraient suivre cette stratégie globale.



7 - SURVEILLANCE DES ACTIFS

La surveillance des actifs (« endpoint visibility ») représente la visibilité sur tous les appareils hébergés sur un réseau, tels que les ordinateurs portables, les ordinateurs de bureau, les téléphones mobiles, les tablettes électroniques, etc. Nous avons demandé aux répondants quel était le degré de surveillance des actifs sur l'ensemble de leur organisation. Tel qu'illustré par la figure 11, 68,4% ont déclaré avoir une surveillance élevée ou très élevée, 23,9% une surveillance modérée et 7,69% ont dit avoir une surveillance nulle ou faible.

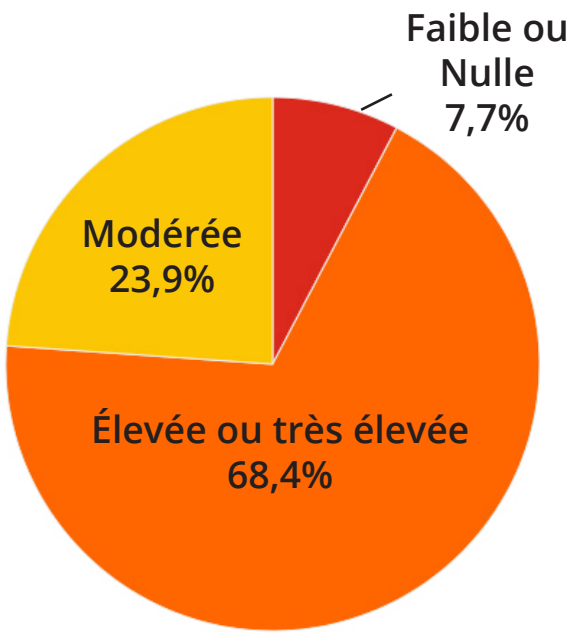


Figure 11 - Surveillance des actifs

EXPÉRIENCE DES TESTEURS D'INTRUSION

Le fait que 68% des personnes interrogées aient déclaré avoir un niveau élevé de surveillance sur leurs actifs a surpris les testeurs d'intrusion. Ils ont mentionné que l'écart pouvait s'expliquer par l'idée que la surveillance des actifs perçue par les personnes interrogées est basée sur des menaces plus traditionnelles plutôt que sur des techniques plus récentes, comme l'utilisation des charges utiles (« payload ») en mémoire ou l'utilisation malicieuse des fonctionnalités des systèmes d'exploitation. De plus, sur la base de l'expérience en tests d'intrusion et en considérant des cadres de tactiques, de techniques et de procédures (TTP), comme le cadriciel (« framework ») Att&ck du Mitre, la surveillance des actifs des clients ne couvre généralement qu'une fraction des stratégies et des techniques connues.

CONSEILS PRATIQUES SUR LA SURVEILLANCE DES ACTIFS (« ENDPOINT VISIBILITY »)

- Envisager un fournisseur de détection et de réponse sur les actifs (« Endpoint Detection and Response » ou « EDR ») pour améliorer la surveillance sur ces derniers et prévenir les attaques sophistiquées;
- Il existe également des outils gratuits comme Sysmon et « Windows Event Forwarding » (WEF) / « Windows Event Collector » (WEC) qui, lorsqu'ils sont bien configurés, constituent un bon remplacement, complément ou ajout à une solution EDR.

PARTIE 2:
LES DÉRAPAGES COGNITIFS EN CYBERSÉCURITÉ

Après avoir constaté des incohérences dans les résultats de l'enquête par rapport à l'expérience des testeurs d'intrusion, nous avons procédé à une comparaison entre les perceptions et les pratiques des défenseurs. Pour ce faire, nous avons choisi une question qui évaluait la perception des répondants face à la maturité de la posture de sécurité de leur organisation et, à l'aide d'un modèle statistique, nous avons examiné si la maturité perçue correspondait avec les mesures de sécurité mentionnées comme étant mises en place (ou non) dans l'organisation du répondant. Par la suite, nous avons compilé les 10 principales vulnérabilités/contrôles manquants relevés dans 65 rapports de tests d'intrusion. Ces observations sont présentées dans la sous-section « Les vecteurs d'attaque les plus courants » et sont accompagnées de conseils pratiques pour les nouveaux vecteurs d'attaque non mentionnés ci-dessus. Les dérapages cognitifs décelés à travers ces deux analyses sont par la suite abordés dans la sous-section « Que se passe-t-il ? ».

MATURITÉ PERÇUE EN MATIÈRE DE SÉCURITÉ, COMPTE TENU DES MESURES DE SÉCURITÉ MISES EN ŒUVRE

L'enquête a débuté en questionnant les répondants quant à leur perception sur la maturité globale de leur organisation en matière de sécurité.

«Sur une échelle de 1 à 5, quel est, selon vous, le degré de maturité de la posture de sécurité de votre organisation?»

Comme le montre la figure 12, moins de 4% ont répondu 1, ce qui représente une faible maturité en matière de sécurité, 20% ont répondu 2, 32% ont répondu 3, 31% ont répondu 4 et environ 13% ont répondu 5, ce qui représente une grande maturité en matière de sécurité. **Cette question nous a permis d'évaluer si la posture de sécurité perçue par les répondants à propos de leur organisation correspond, en moyenne, à l'implémentation -ou non- des sept mesures discutées dans la section 1.**

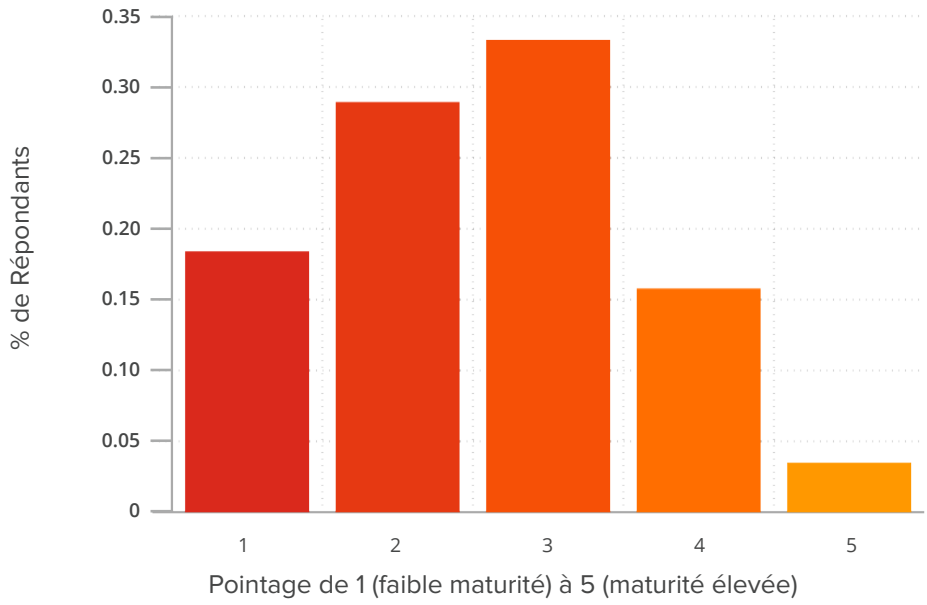


Figure 12 - Perception des répondants sur la maturité globale de leur organisation en matière de sécurité

Pour estimer s'il existe des relations entre la perception de maturité dans la posture de sécurité d'une organisation et si les sept mesures de sécurité sont implantées dans ladite organisation, nous avons calculé un modèle statistique appelé la méthode des moindres carrés ordinaires (MCO)[2]. Pour les lecteurs désireux d'en savoir plus, le modèle et les résultats sont expliqués plus en détail dans l'annexe du rapport.

Le modèle montre que cinq mesures de sécurité, déclarées comme ayant été mises en œuvre, présentent une corrélation significative et positive avec la perception qu'ont les répondants en ce qui concerne la maturité de leur organisation en matière de sécurité. En résumé, plus les répondants déclarent avoir mis en œuvre ces cinq mesures, plus ils perçoivent la maturité de leur organisation en matière de sécurité comme élevée.

- Authentification à facteurs multiples sur les actifs externes;
- Authentification à facteurs multiples sur les actifs internes;
- Gestion des mises à jour;
- Inventaire des actifs;
- Surveillance des actifs.

Toutefois, les points importants à retenir du modèle ne sont pas les relations significatives, mais plutôt les relations non significatives. En effet, le modèle a permis de constater qu'il n'y avait pas de relation significative entre la maturité perçue en matière de sécurité et deux mesures :

- Exigences minimales en matière de mot de passe;
- Enquêter les produits pour identifier et désactiver les fonctionnalités qui représentent un risque.

Cela signifie qu'en moyenne, la perception de la maturité de sécurité d'une organisation n'est pas corrélée avec la mise en œuvre de ces deux mesures.

Bien que les résultats du modèle soient basés sur les perceptions des répondants (et ne déduisent rien quant aux mesures de sécurité réellement mises en œuvre), ils indiquent qu'il pourrait y avoir des biais potentiels chez les défenseurs quant aux mesures de sécurité à considérer. Plus précisément, lorsque les résultats sont mis en corrélation avec les données des tests d'intrusion présentées ci-dessous, d'importantes disparités en matière d'information sur les vecteurs potentiels d'attaque sont mises en évidence.

LES VECTEURS D'ATTAQUE LES PLUS COURANTS

Nous avons examiné 65 rapports de tests d'intrusion (interne, externe et applications Web) et avons extrait un total de 182 observations. Le tableau 1 présente les 10 observations les plus fréquemment trouvées dans ces 65 rapports. Ces observations représentent soit une vulnérabilité ou un contrôle manquant classé de sévérité moyenne à élevée. **Ces dix observations pourraient faire office de liste de contrôle pour tout professionnel de la cybersécurité souhaitant sécuriser les vecteurs d'attaque les plus courants utilisés par les testeurs d'intrusion. Pour des raisons d'efficacité, ces vecteurs pourraient être validés et mitigés avant même de recourir à des services de tests d'intrusion.** Cela permettrait d'établir une base de sécurité et d'imposer aux testeurs d'intrusion à innover et trouver de nouveaux moyens d'entrée dans les réseaux. Veuillez noter que pour la liste des « vecteurs d'attaque les plus courants », nous avons mélangé les différents types de mandats (interne, externe, et applications Web) puisque les résultats étaient intéressants. Cependant, nous reconnaissons que la présence de NetBIOS/LLMNR et les attaques d'injection de script (« Cross-Site Scripting ») sont deux observations qui ne proviennent pas du même contexte. Ainsi, de futures recherches pourraient s'intéresser à extraire de grandes tendances sur les vecteurs d'attaque selon les types de mandats.

Cela étant dit, nous présentons ci-dessous les dix principales observations et, à la suite de chacune d'elles, nous proposons des conseils pratiques supplémentaires, lorsqu'opportun.

Table 1 – Conclusions les plus courantes présentent dans les rapports de tests d'intrusion

Conclusion	Nombre de rapports	Percentage total
Politique mots de passe problématique	35	55%
Services organisationnels à facteur d'authentification unique	23	36%
Identifiants Windows stockés en mémoire	21	33%
Réutilisation des mots de passe	21	33%
Présence de NetBIOS/LLMNR	21	33%
Processus de gestion de mises à jour inadéquat	19	30%
«HTTP Strict Transport Security (HSTS)» manquant	17	27%
Contrôleurs de domaines ou de serveurs avec accès à Internet	15	23%
«Cross-Site Scripting (XSS)»	14	22%
Stockage des informations sensibles inadéquat	14	22%

Avoir une politique de mots de passe problématique, comme le montre le tableau 1, est l'observation la plus fréquente dans nos rapports. Un mot de passe faible peut être un mot de passe court ou commun, un mot de passe par défaut, ou un mot de passe pouvant être obtenu facilement en exécutant une attaque par force brute. Une telle attaque utilise un sous-ensemble de tous les mots de passe possibles, tels que des mots du dictionnaire, des noms propres, des mots basés sur le nom d'utilisateur, ou des variations courantes de ces thèmes. Cette observation est souvent l'origine d'une première compromission. Pour obtenir des conseils pratiques afin d'améliorer la politique des mots de passe, veuillez-vous référer à la section 1.2.

Les services organisationnels à facteur d'authentification unique représentent la deuxième observation la plus fréquente. Elle représente un processus de sécurité qui exige soit quelque chose que l'utilisateur connaît, quelque chose qu'il possède ou quelque chose qu'il «est» afin de confirmer son identité. L'utilisation d'un mot de passe est la méthode la plus populaire pour l'authentification à facteur unique, et ce, même si les utilisateurs sont souvent reconnus pour utiliser des mots de passe faibles ou pour réutiliser le même mot de passe sur plusieurs sites Web. En outre, les systèmes qui reposent sur des mots de passe comme seul facteur d'authentification peuvent exposer le réseau de l'organisation à des attaques par force brute ou par pulvérisation de mots de passe. Ces attaques sont inefficaces lorsqu'une authentification à facteurs multiples est activée. Pour obtenir des conseils pratiques sur la mise en œuvre de l'authentification à facteurs multiples, veuillez-vous référer à la section 1.1.

Les identifiants Windows stockés en mémoiret la troisième observation la plus courante. Plusieurs des protocoles d'authentification activés par défaut sur Windows stockent les identifiants des utilisateurs et des services dans des zones de mémoire restreintes, sous la protection du compte SYSTEM. Ces informations peuvent être récupérées en texte clair en utilisant les privilèges administratifs locaux. Nous présentons ci-dessous deux conseils pratiques qui peuvent aider à prévenir une exfiltration des identifiants Windows stockés en mémoire.

CONSEILS PRATIQUES POUR PRÉVENIR L'EXFILTRATION DES IDENTIFIANTS WINDOWS STOCKÉS EN MÉMOIRE

- Pour éviter l'exfiltration des identifiants Windows stockés en mémoire, les nouvelles versions de Windows offrent une fonction appelée « Credential Guard ». Cette fonction est extrêmement efficace pour mitiger cette vulnérabilité, mais nécessite tout de même des configurations spécifiques;
- Une autre mesure consiste à isoler le processus en charge de l'authentification dans Windows (lsass) avec une clé de registre appelé « RunAsPPL ».

La réutilisation des mots de passe est la quatrième observation la plus fréquente et est liée à la réutilisation de mots de passe pour des comptes d'utilisateurs locaux ou si un utilisateur du domaine utilise un mot de passe unique pour plusieurs comptes avec divers niveaux d'accès. Pour éviter la réutilisation des mots de passe des comptes d'administrateurs locaux, consultez le conseil pratique ci-dessous.

CONSEIL PRATIQUE POUR ÉVITER LA RÉUTILISATION DES MOTS DE PASSE

- Assurez-vous que tous les comptes d'administrateurs locaux ont des mots de passe uniques. Cette vérification est possible grâce à Microsoft LAPS, une solution gratuite qui assigne les mots de passe des administrateurs locaux de manière aléatoire tout en permettant une gestion facile.

Les protocoles NetBIOS/LLMNR, désormais considérés comme obsolètes, représentent la cinquième observation la plus courante. Ces protocoles sont généralement utilisés dans le processus de résolution des noms d'hôtes sous la forme de multidiffusion, mais n'offrent aucun mécanisme d'authentification. Cela les rend vulnérables à de multiples attaques d'usurpation d'identité au niveau du réseau. Veuillez-vous référer à la section 1.5 pour obtenir des conseils pratique afin de mitiger les risques associés à ces protocoles désuets.

Le processus de gestion de mises à jour inadéquat, la sixième observation, est la pratique cyclique d'identification, de classification, de remédiation ou de mitigation des vulnérabilités, et ce, en particulier pour les systèmes d'exploitation et les applications. Les processus de gestion des vulnérabilités (mises à jour) sont considérés comme inadéquats lorsque de nombreux systèmes en production ne sont pas mis à jour et fonctionnent avec des versions de logiciels obsolètes. La section 1.4 présente des conseils pratiques sur la gestion des mises à jour.

« HTTP Strict Transport Security (HSTS) » manquant est la septième observation et représente un contrôle manquant plutôt qu'une vulnérabilité comme telle. Il s'agit d'un dispositif de sécurité mis en œuvre dans les navigateurs pour stocker localement le certificat numérique des sites Web HTTPS visités et les associer à leur nom de domaine respectif. Chaque visite ultérieure d'un site Web protégé est automatiquement redirigée vers la variante sécurisée (HTTPS) et déclenche une validation du certificat présenté par le serveur Web par rapport à celui qui était précédemment enregistré. Si les certificats ne correspondent pas, le navigateur limitera l'accès au site Web puisqu'il détectera une activité malveillante en cours. Les navigateurs n'utiliseront cette fonction que si un site Web envoie l'entête HTTP HSTS. Sachez que la gestion adéquate de l'entête HSTS nécessite un processus de gestion des certificats bien défini afin d'éviter tout impact potentiel sur les utilisateurs. Le conseil ci-dessous résume la manière d'activer le HSTS.

CONSEIL PRATIQUE POUR ACTIVER HSTS

- Activez HSTS en ajoutant un entête de réponse portant le nom « Strict-Transport-Security » et la valeur « max-age=expireTime », où « expireTime » représente le temps (en seconde) pendant lequel les navigateurs se souviendront que le site devrait être accessible via HTTPS. Pensez également à ajouter le drapeau « includeSubDomains » si nécessaire.

Les contrôleurs de domaine ou de serveurs avec accès à Internet représentent la huitième observation la plus fréquente et signifie que des contrôleurs de domaine ainsi que des serveurs du réseau de l'organisation permettent un accès réseau à des actifs hébergés sur Internet. Les normes de sécurité et les meilleures pratiques actuelles déconseillent cette pratique. Le conseil pratique ci-dessous résume de quelle manière ce contrôle manquant pourrait être mitigé.

CONSEIL PRATIQUE POUR MITIGER LES EFFETS DES CONTRÔLEURS DE DOMAINE OU DES SERVEURS AYANT ACCÈS À INTERNET

- Restreindre l'accès à Internet pour tous les systèmes essentiels de l'organisation, tels que les contrôleurs de domaine et les serveurs internes. Dans la mesure où l'accès à Internet est nécessaire pour répondre à des exigences professionnelles documentées, les communications doivent être limitées aux hôtes, aux services et aux ports appropriés.

« Cross-Site Scripting », la neuvième observation la plus fréquente, est une vulnérabilité commune des applications Web. Une application est vulnérable au Cross-Site Scripting (XSS) lorsque les données saisies par l'utilisateur sont réutilisées telles quelles dans la page de réponse. Nous fournissons ci-dessous deux conseils pratiques pour vous aider dans la mitigation des attaques XSS.

CONSEILS PRATIQUES POUR MITIGER LES EFFETS DU XSS

- Valider l'ensemble des entrées des utilisateurs;
- L'utilisation d'une liste d'inclusion (« allow list ») avec des expressions régulières strictes sur les entrées de l'application est, de loin, la stratégie la plus efficace pour mitiger les attaques XSS.

La dernière observation la plus courante est **le stockage des informations sensibles inadéquat**, qui fait référence aux méthodes utilisées pour protéger les informations sensibles, telles que les informations personnelles sur les clients ou les employés, les mots de passe, les informations bancaires ou toute information susceptible de causer un préjudice si elle est connue par une personne malveillante. Le stockage de ces informations sans chiffrement dans un document, sur un poste de travail ou sur un réseau partagé est une pratique risquée. Vous trouverez ci-dessous deux conseils pratiques pour atténuer les risques liés au stockage de mots de passe en texte clair.

CONSEILS PRATIQUES POUR RÉDUIRE LES RISQUES DE STOCKAGE DES MOTS DE PASSE EN CLAIR

- Aucun fichier de mots de passe en clair ne doit être toléré sur le réseau. Pour éviter cela, utilisez un gestionnaire de mots de passe comme Keepass ou une solution de gestion des mots de passe au niveau de l'organisation;
- Une mesure supplémentaire intéressante consiste à effectuer une recherche périodique des termes « mots de passe » ou « password » dans les fichiers partagés (cette méthode est souvent utilisée par les testeurs d'intrusion).

QUE SE PASSE-T-IL?

Ce qui est le plus frappant dans les résultats qui sont présentés ci-dessus, c'est que les deux mesures de sécurité qui ne sont pas associées à la perception de sécurité des répondants sont directement liées aux principaux vecteurs d'attaques exploités lors de tests d'intrusion. Ces deux mesures de sécurité sont : 1) répondre aux exigences minimales en matière de mots de passe et 2) l'enquête des produits pour identifier et désactiver les fonctionnalités qui représentent un risque. Les principaux vecteurs d'attaque exploitées lors des tests d'intrusion et intimement liés à ces mesures sont les exigences inadéquates en matière de mots de passe, la réutilisation de mots de passe, les identifiants Windows stockés en mémoire et la présence des protocoles désuets NetBIOS/LLMNR.

En effet, lorsque les exigences minimales en matière de mots de passe ne sont pas respectées, il devient simple pour les testeurs d'exploiter cette faiblesse et de s'introduire dans un réseau grâce à des attaques par force brute ou par pulvérisation de mots de passe. Pire encore, si plusieurs postes de travail partagent les mêmes informations d'identification, les testeurs d'intrusion peuvent exploiter cette réutilisation de mots de passe pour compromettre de nouveaux appareils et pivoter dans le réseau sans être détectés.

De plus, les identifiants Windows stockés en mémoire et la présence de NetBIOS/LLMNR sont deux fonctionnalités activées par défaut dans le produit Windows et représentent une vulnérabilité. Ces fonctionnalités sont exploitées en permanence par les testeurs d'intrusion. Investiguer les fonctionnalités activées par défaut dans les produits pour désactiver celles qui représentent une vulnérabilité devrait être une priorité pour les défenseurs, car même le pare-feu le plus robuste ne peut mitiger ce vecteur d'attaque qui expose l'organisation à un risque élevé.

Ainsi, en croisant les résultats du modèle statistique avec les 10 principales vulnérabilités/contrôles manquants trouvés dans 65 rapports de tests d'intrusion, **nous concluons qu'il existe un décalage ou une disparité d'information entre les défenseurs et les attaquants au niveau des éléments clefs à considérer en cybersécurité**. En effet, les principaux vecteurs d'attaque trouvés par les testeurs d'intrusion ne semblent pas être perçus comme des éléments essentiels contribuant à la maturité de sécurité d'une organisation chez les défenseurs. Il est nécessaire de modifier cette asymétrie d'information afin de sécuriser les maillons faibles actuellement présents dans de nombreuses organisations.

Il est évident qu'il reste beaucoup de travail à faire pour sécuriser les systèmes au niveau technique. Cependant, cette recherche met en lumière que le défi n'est pas seulement technique, mais également humain. L'analyse des perceptions qu'ont les défenseurs sur la cybersécurité nous a mené à reconnaître que toutes les mesures de sécurité ne sont pas perçues et classées de la même façon par ceux-ci et qu'il y a encore des mesures de sécurité importantes qui ne sont pas prises en compte.

Les recherches futures pourraient s'intéresser à cette disparité et examiner pourquoi il en est ainsi, par exemple, en interrogeant des professionnels de la cybersécurité sur le sujet. Il est nécessaire de comprendre le processus décisionnel des défenseurs et la manière dont ils font face à cette tâche complexe. Les facteurs qui influencent leur processus de réflexion et les biais potentiels qui orientent leurs jugements doivent également être décelés et analysés. Par exemple, en n'enquêtant pas les produits pour identifier et désactiver les paramètres de sécurité qui représentent un risque, les défenseurs semblent implicitement faire confiance à ce qu'ils achètent, un problème qui rappelle celui du « passager clandestin » (« Free-rider problem »). En effet, des chercheurs, tels qu'Anderson et Moore (2007)[3], ont constaté que la sécurité de l'information dépend de la somme de tous les efforts individuels et que « lorsqu'elle dépend de la somme des efforts individuels, la charge aura tendance à être supportée par les agents ayant le rapport coûts-avantages le plus élevés, tandis que les autres sont des passagers clandestins » (traduction de l'anglais, p.72), profitant ainsi de l'investissement des pairs.

Ainsi, l'étude du processus décisionnel des défenseurs pourrait aider à résoudre le dilemme dans lequel nous nous trouvons actuellement. Une approche considérant ce facteur humain pourrait potentiellement conduire à de nouvelles méthodes de sécurisation des systèmes; des méthodes qui prendraient en compte les biais cognitifs des défenseurs, leurs pratiques quotidiennes ainsi que la tâche complexe qui leur est imposée.

CONCLUSION

Dans l'ensemble, nous constatons qu'il existe une asymétrie d'information entre les attaquants et les défenseurs. En effet, les mesures de sécurité qui ne sont pas associées à la perception de sécurité des défenseurs sont reliées à des techniques d'attaque souvent exploitées par les testeurs d'intrusion pour compromettre des systèmes. Ces résultats montrent que, bien que de réels efforts soient déployés dans le secteur pour protéger les systèmes informatiques, de l'information cruciale quant aux principaux vecteurs d'attaques n'est toujours prise en compte par les défenseurs. Cette dissonance doit être rectifiée afin de contrer les vrais attaquants potentiels.

En conclusion, cette recherche illustre qu'avec une perspective de données croisées entre les attaquants et les défenseurs, nous avons pu mettre en lumière des tendances problématiques en cybersécurité. De futures recherches pourraient s'intéresser à cette dissonance humaine, et ce, afin de démystifier ce qui influence les professionnels de la cybersécurité à penser et à se comporter comme ils le font face à la sécurité de leur organisation.

Auteurs

Masarah Paquet-Clouston (chercheure en cybersécurité chez GoSecure),
Laurent Desaulniers (directeur des services de tests d'intrusion chez GoSecure),
Maxime Nadeau (testeur d'intrusion chez GoSecure)

Collaborateurs

Michael Joyce (co-directeur général chez Serene-risc),
Benoît Dupont (directeur scientifique chez Serene-risc)

Remerciements

Nous remercions tous les participants d'avoir pris le temps de répondre à l'enquête. Nous voudrions également remercier Olivier Bilodeau et Alexandre Beaulieu pour leurs précieux commentaires tout au long de la rédaction, ainsi que Pascal Fortin pour son aide dans le cadre de l'enquête et de l'angle de recherche initial.

À PROPOS DE GOSECURE

GoSecure est reconnu comme étant un leader et un innovateur en ce qui a trait aux solutions de cybersécurité. L'organisation est la première – et la seule – à intégrer la détection de menaces pour les terminaux, les réseaux et les services messagerie au sein d'un seul service de détection et réponse gérées. La plateforme de détection et réponse livre une détection prédictive multi-vecteurs, une prévention et une réponse en appliquant une combinaison unique d'analyse comportement, d'investigation « forensics » de mémoire, d'apprentissage automatique et de techniques de réputation pour contrer les menaces les plus avancées. Nos services MDR sont dirigés par des niveaux de services agressifs pour une réponse rapide et des services de mitigation active qui touchent directement les réseaux et terminaux de nos clients. Ensemble, ces capacités offrent la meilleure réponse face à l'augmentation accrue de la sophistication et de l'évolution des logiciels malveillants et des employés malicieux qui ciblent les personnes, les processus et les systèmes. En mettant l'accent sur l'innovation, la qualité, le respect et l'intégrité, GoSecure est devenu un fournisseur de produits et services de cybersécurité reconnu pour des organisations de toutes tailles et évoluant dans tout type d'industrie.

ANNEXE

Modèle statistique des MCO sur la maturité perçue de la posture de sécurité et les mesures mises en œuvre

Avec la question : « Sur une échelle de 1 à 5, quel est, selon vous, le degré de maturité de la posture de sécurité de votre organisation? », nous avons évalué si la sécurité perçue par les répondants correspondait, en moyenne, aux sept mesures qu'ils ont déclaré avoir mises en œuvre, ou non, dans leur organisation en calculant une régression des moindres carrés ordinaires (MCO). Un modèle de régression MCO est une méthode d'analyse statistique qui estime la relation entre une ou plusieurs variables explicatives (appelées variables indépendantes) et une variable de résultat (appelée variable dépendante) en minimisant la somme des carrés des résidus. La formulation du modèle est présentée dans l'équation 1..

$$SecMaturity_i = \beta_0 + \beta_1 MFAInternal_i + \beta_2 MFAExternal_i + \beta_3\ MinPassword_i +$$

$$\beta_4\ PatchMan_i + \beta_5\ ProprietaryInv_i + \beta_{6i} *\ AssetInv_i + \beta_7 *\ EndPointVis_i + \varepsilon_i \quad (eq.1)$$

SecMaturity représente l'échelle à laquelle un répondant i considère la maturité de la sécurité de son organisation (de 1, faible sécurité, à 5, haute sécurité), β_0 est l'ordonnée à l'origine du modèle (la constante), MFAInternal représente si l'authentification à facteurs multiples a été déclarée comme mise en œuvre au niveau interne alors que MFAExternal est au niveau externe. MinPassword indique si la personne interrogée a déclaré que les exigences minimales en matière de mot de passe sont respectées dans son organisation, PatchMan indique le temps nécessaire à l'organisation pour appliquer une mise à jour sur une échelle de 1 (heures) à 5 (années) lorsqu'une nouvelle vulnérabilité est révélée, selon la personne interrogée. ProprietaryInv indique si le répondant a déclaré que son organisation étudie les produits pour des fonctionnalités spécifiques représentant des vecteurs d'entrée potentiels et AssetInv indique si le répondant a déclaré que son organisation tient un inventaire complet de ses actifs[4]. Enfin, EndPointVis examine si le répondant a déclaré faire une surveillance de ses actifs (« Endpoint visibility ») dans son organisation. Étant donné que la distribution de chaque variable explicative a déjà été présentée dans la section 1, nous ne les présentons pas à nouveau dans cette section.

Spécificités du modèle

Même si la variable de résultat (maturité perçue en matière de sécurité) est échelonnée d'un à cinq, comme le montre la figure 12, nous constatons que les données correspondent à un modèle de régression linéaire. De plus, comme le montre la figure 12, la distribution de la variable de résultat suit une distribution normale, même si la méthode d'échantillonnage impose des valeurs discrètes. Pour confirmer que notre modèle suit les hypothèses des MCO, nous avons d'abord calculé le test de Durbin-Watson et constaté qu'il n'y avait pas d'autocorrélation dans les termes d'erreur. Ensuite, nous avons calculé le test de Breush-Pagan, qui a montré qu'il n'y avait pas non plus d'hétéroscédasticité dans les termes d'erreur. Nous avons finalement calculé les « variance inflation factors » (VIFs) pour évaluer les problèmes potentiels de multicolinéarité, et tous les VIFs étaient inférieurs à 1,6 illustrant qu'il n'y a pas de problème de multicolinéarité avec les variables explicatives.

Résultats du modèle

Les résultats du modèle sont présentés dans le tableau 1. Le coefficient de chaque variable explicative n'est pas normalisé, ce qui signifie que le coefficient représente un changement de la variable de résultat (sécurité perçue) lorsqu'une unité d'augmentation est ajoutée à la variable

explicative. L'écart type estime l'écart du coefficient : plus il est petit, plus le coefficient est précis. La valeur p détermine la signification des résultats : une valeur p inférieure à 0,05 indique qu'il existe une relation significative entre les variables explicatives et la variable de résultat. Nous avons ajouté une colonne pour indiquer si la relation est significative. Enfin, le R2 du tableau 1 indique la proportion de la variance de la variable de résultat qui peut être expliquée par les variables explicatives.

Table 1 – Résultats du modèle

	Coefficient	Écart type	P-Value	Variable Significante
L'ordonnée à l'origine (la constante)	1.01	0.49	0.04	oui
Authentification à facteurs multiples sur les actifs internes	0.24	0.12	0.01	oui
Authentification à facteurs multiples sur les actifs externes	0.31	0.12	0.05	oui
Exigences minimales en matière de mots de passe	0.09	0.10	0.40	non
Gestion des mises à jour	- 0.15	0.08	0.05	oui
Enquête sur les fonctionnalités des produits	0.17	0.17	0.31	non
Inventaire des actifs	0.47	0.18	0.01	oui
Surveillance des actifs (endpoint visibility)	0.38	0.10	0.00	oui
R^2	0.51			

Comme le montre le tableau 1, l'ordonnée à l'origine et cinq des sept variables explicatives sont significatives : l'authentification à facteurs multiples aux périmètres interne et externe, la gestion des mises à jour, l'inventaire des actifs et la surveillance des actifs (« endpoint visibility »).

Pour l'authentification à facteurs multiples sur les actifs internes, une augmentation d'un point de la déclaration d'avoir mis en œuvre la fonctionnalité (de non (0) à partiellement (1) ou de partiellement (1) à oui (2)) entraîne une augmentation de 0,24 (écart type 0,12) point de la maturité de sécurité perçue par les répondants. Pour l'authentification à facteurs multiples sur les actifs externes, une augmentation d'un point de la déclaration d'avoir mis en œuvre la fonctionnalité (de non (0) à partiellement (1) ou de partiellement (1) à oui (2)) représente une augmentation de 0,31 (écart type 0,12) point de la maturité de la sécurité perçue chez les répondants. En termes de la gestion des mises à jour, une augmentation d'un point (sur une échelle de 5 points allant de quelques heures (1) à quelques jours (2), ou de quelques jours (2) à quelques semaines (3), ou de quelques semaines (3) à quelques mois (4), ou de quelques mois (4) à quelques années (5)) entraîne une diminution de 0,15 (écart type 0,08) point de la maturité perçue en matière de sécurité. Une augmentation d'un point de la déclaration d'avoir un inventaire des actifs (de l'absence d'inventaire (0) à l'existence d'un inventaire (1)) entraîne une augmentation de 0,47 (écart type 0,18) point de la maturité perçue en matière de sécurité et enfin, une augmentation d'un point de la déclaration d'avoir de la surveillance d'actif (« endpoint visibility ») (de 1 à 5, où 1 représente une faible visibilité et 5 une forte visibilité) entraîne une augmentation de 0,38 (écart type 0,10) point de la maturité perçue en matière

de sécurité. Les deux variables restantes, à savoir les exigences minimales en matière de mot de passe et l'enquête sur les produits pour des fonctionnalités représentant des vecteurs d'entrés, ne sont pas significatives dans le modèle. Ainsi, le respect des exigences minimales en matière de mot de passe et l'enquête des produits sont deux variables qui ne sont pas corrélées à la maturité perçue de la posture de sécurité chez les répondants.

Enfin, comme le montre le tableau 1, la proportion de la variance de la variable de résultat qui peut être expliquée par les variables explicatives est de 38%. Cela signifie qu'un important pourcentage de la variance de la variable de résultat est expliqué par d'autres variables explicatives (non incluses dans le modèle). Une enquête plus approfondie sur la question sera donc nécessaire dans un futur rapproché.

1 - Dans le présent document, le masculin est utilisé dans le seul but d'alléger le texte, et ce, sans préjudice pour la forme féminine.

2 - La méthode des moindres carrés ordinaires est une méthode d'analyse statistique qui estime la relation entre une ou plusieurs variables explicatives (appelées variables indépendantes) et une variable de résultat (appelée variable dépendante) en minimisant la somme des carrés des résidus.

3 - Anderson, R., and T. Moore. "Information Security Economics – And Beyond." In Proceedings of the Annual International Cryptology Conference, 68–91. Springer, Berlin, Allemagne, 68–91, 2007.

4 - Nous avons recodé comme "non" lorsque les personnes interrogées ont déclaré qu'elles ne savaient pas si leur organisation enquêtait sur des produits ou tenait un inventaire actualisé des actifs.