CESIN : Les instantanés 2021

Le CESIN a mis en place depuis maintenant plus de trois ans, un dispositif d'enquête hebdomadaire, appelé « la question de la semaine ». Ces enquêtes flash permettent, en 2 à 3 clics de recueillir la position de nos membres sur un point précis, qu'il concerne leurs démarches de cybersécurité, un point d'actualité, une tendance ou un sujet de fond. Fort de ses 700 membres (en 2021), de leur diversité et du nombre de répondants à chaque question, le CESIN peut proposer une vision transverse, représentative de la réalité des entreprises. Comme le club l'avait déjà fait pour les exercices 2019 et 2020, il semblait naturel de partager ces enseignements, au-delà des membres du Clubs membres, à l'ensemble de la « communauté cybersécurité ».

Cette synthèse de l'année 2021 s'appuie sur les 21 questions qui ont été proposées aux membres du CESIN. Les panels de répondants, sont représentatifs, de 106 à 212 et la moyenne s'établit à 163.

Le choix des sujets abordés a été, encore une fois, éclectique. L'actualité a également été prise en compte. Celle-ci était riche en ce début d'année 2021 suite aux révélations concernant les attaques via la supply chain logicielle **[Q48]**. Celles-ci mettant en évidence à la fois le **risque de la supply-chain logicielle** en lui-même et celui de **fuite d'outils offensifs** (dans ce cas précis, ceux de FireEye)… Si ces attaques, et les risques associés, ont, bien sûr, été pris en compte en priorité par les organisations utilisatrices des solutions Solarwind, elles marquent également une évolution de posture. En effet, 65% des répondants considèrent que cette attaque massive, visant les leaders de l'édition logicielle constitue un précédent et 91% prédisent que ce type d'attaques va se multiplier, renforçant la nécessité de processus plus réactif de gestion des vulnérabilités.

Une autre typologie d'attaque a fait l'actualité début 2021, il s'agit du **Credential Stuffing [Q54]** , technique qui consiste à accéder à un service en ligne via des crédentiels volés sur un autre site (ou achetés sur le Darkweb). Outre la généralisation de ce type d'attaque, la préoccupation autour de celle-ci s'est trouvée renforcée après que la CNIL ait prononcé une amende de 150 000 € (et 75 000 pour son sous-traitant) à l'encontre d'un responsable de traitement. Celui-ci, suite à plusieurs vols de données consécutifs à des attaques par Credential Stuffing n'étant pas jugé assez réactif dans sa mise en place de mesures efficaces de réduction de risque. Lorsque la décision de la CNIL a été rendue publique, 35% des membres du CESIN considéraient que leurs entreprises n'était pas exposées aux attaques par Credential Stuffing (ce qui peut s'expliquer pour une entreprise qui ne propose pas de services transactionnels en ligne ou qui protège ceux-ci par une authentification multi facteurs), 34 % étaient concernées mais sans notifier ces attaques à la CNIL ni déposer plainte. Ces notifications et dépôts de plainte ne sont, pour ce type d'attaque, systématisés que pour moins de 3% des entreprises.

La prise en compte des risques d'attaques de la supply chain logicielle s'insère, pour partie, dans la démarche de **sécurité des tiers.** La part de celle-ci dans les démarches de sécurité tend à se renforcer, se formaliser et s'outiller. La prise en

compte contractuelle de la cybersécurité devient alors incontournable et se décline via l'élaboration de **Plan d'Assurance Sécurité [Q65]**. Ceux-ci sont mis en œuvre par plus des ¾ des répondants à cette question hebdomadaire. Les disparités sont néanmoins assez marquées puisque 32% ne mettent en place des PAS que pour les fournisseurs les plus critiques alors que 13% l'ont, non seulement systématisé, mais l'utilisent pour piloter opérationnellement la sécurité du service rendu par leurs fournisseurs.

L'évolution des usages peut, elle aussi, être porteuse de nouveaux risques ou, pour le moins, d'évolution de la cartographie des risques d'une organisation. L'utilisation des **réseaux sociaux**, s'est ainsi généralisée en entreprise comme outil de communication, de promotion, de marketing, de recrutement, … 29% des répondants à cette question ont pris en compte la nécessité de **gérer les accès** à ces nouveaux outils **[Q51]** et, pour 10% d'entre eux, cette gestion des accès aux réseaux sociaux utilisés par l'entreprise est entièrement intégrée aux processus transverses d'IAM. Parmi l'offre très large de réseaux sociaux, l'usage de l'un d'entre eux préoccupe plus les RSSI : **WhatsApp [Q47]**. Les usages professionnels et personnels s'y mélangent allègrement. De plus, en ce début 2021, l'annonce du partage de données entre WhatsApp et sa maison-mère Facebook (pas encore devenue Meta – projet abandonné depuis) a de quoi préoccuper, voire inquiéter les professionnels de la sécurité. Néanmoins, l'usage de WhatsApp sur les téléphones mis à disposition par l'organisation n'est interdit que pour 17% des répondants (dont 14% en recherche de solutions alternatives). A l'opposé, l'usage de WhatsApp est autorisé sans restriction pour 46 % de répondants dont uniquement 20% sont en recherche de solutions alternatives.

Outre ces sujets d'actualité, d'émergence de nouveaux risques ou de renforcement de risques connus, les questions hebdomadaires de 2021 ont porté sur les pratiques de cybersécurité des membres du club. De la mise en place des fondamentaux jusqu'aux dispositifs émergents, les sujets traités ont été variés.

Le premier des fondamentaux est, pour bien se protéger, de bien se connaitre et en priorité de bien **connaitre son exposition publique [Q57]**, la première qui sera éprouvée par les cybercriminels. Pour ce faire, 47% des entreprises estiment disposer d'une vision précise de cette exposition et y appliquent un monitoring régulier. Ce monitoring n'est pas continu pour 24% des répondants qui disposent néanmoins d'un inventaire précis alors que la visibilité sur ces zones d'exposition demeure à renforcer pour 31% des entreprises. Certes l'évolution vers les cloud rend ces inventaires plus difficiles à maîtriser mais Il est préoccupant qu'une entreprise sur trois n'ait pas une vision claire de ses actifs immédiatement visibles par des attaquants.

Autre basique de sécurité incontournable, les dispositifs d'authentification. Les nombreuses faiblesses et contraintes des mots de passe, combinées aux difficultés d'évolution vers un autre mode d'authentification en font un thème régulier de débat. Les promesses de dispositifs d'authentification multifacteurs simples d'utilisation, voire « passwordless » tendent néanmoins à devenir plus concrètes. Par ailleurs, en terme de protocole d'authentification, Microsoft, à l'automne 2021, a annoncé la **fin du protocole d'authentification basique dans Exchange online [Q64]** sous un an. Les membres du CESIN n'avaient pas attendu la contrainte de Microsoft pour réaliser cette évolution vers de la « modern authentication » dans la messagerie Exchange. L'évolution était

effectivement finalisée pour 25 % d'entre eux et en cours pour 17%. Il est également à noter que 35 % des entreprises ne sont pas concernées puisque n'utilisant pas Exchange online.

Une autre problématique de l'authentification par mot de passe est celle des **mots de passe par défaut** **[Q61]**. Nous sommes encore trop souvent confrontés à leur découverte et exploitation par des auditeurs et pentesters… quand ce n'est pas par des attaquants. Malgré ce risque important et cette exposition à un défaut élémentaire, la problématique des mots de passe par défaut n'est pas particulièrement prise en considération par 28% des entreprises, 33% ont édicté des règles dont l'application n'est pas contrôlée et seules 5% d'entre elles ont mis en place un dispositif de contrôle systématique et continu.

La robustesse des dispositifs d'authentification n'est pas exclusivement dépendante de la qualité de dispositifs techniques mais également de l'usage qui en est fait et de la mise en application de bonnes pratiques. Le facteur humain est donc prépondérant dans toute démarche de cybersécurité qui doit intégrer des mesures de sensibilisation adaptées. Parmi celles-ci les **campagnes de phishing à visée pédagogique** **[Q50]** sont un outil en plein essor, utilisé par près de 80% de nos membres. Ces campagnes permettent d'allier des mises en situation à la communication de supports pédagogiques, souvent sous forme de vidéos. Elles permettent également de mettre en place des indicateurs qui, s'ils ne sont pas nécessairement révélateurs du niveaux de sensibilisation global des collaborateurs ou de l'efficacité de la démarche de sensibilisation, permettent de mesurer une progression de l'acquisition de bons réflexes face au phishing. Si en cas d'attaque, il suffit qu'un seul utilisateur se fasse piéger par les cybercriminels, les **taux de clics** constatés en 2021 demeurent préoccupants puisqu'ils ne sont inférieurs à 10% que pour 25% des répondants et dépassent les 20% pour 22% des répondants. Ces campagnes de phishing sont nécessaires à l'entraînement à la vigilance vis-à-vis des mails, mais elles ne sont sûrement pas suffisantes pour changer profondément les comportements dans une proportion plus satisfaisante. La sensibilisation sur les risques liés aux emails reste un challenge sur lequel il reste sans doute à inventer de nouveaux procédés, car le phishing est un vecteur d'attaque qui risque d'être encore largement utilisé par les cybercriminels.

Ce constat pousse légitimement à continuer à renforcer les dispositifs techniques de protection du trafic web, notamment pour se prémunir contre des liens dangereux sur lesquels les utilisateurs cliquent, dans le cadre de campagnes réelles de phishing. Parmi ceux-ci, **le déchiffrement SSL** **[Q46]** semble de plus en plus nécessaire alors que le pourcentage de flux Internet chiffré ne cesse d'augmenter (estimé à 85% en 2021), rendant les dispositifs de filtrage et d'analyse de flux inefficaces. Néanmoins, le déchiffrement SSL pose la question du maintien de la confidentialité des sessions web des utilisateurs internes, dans le cadre de la tolérance à l'utilisation des outils mis à disposition à des fins personnelles. La complexité du sujet se reflète parfaitement dans la répartition des réponses des membres du club qui déchiffrent tout ou partie des flux SSL en informant ou non leurs utilisateurs. Il se dégage cependant une tendance marquée de déchiffrement SSL partiel, excluant, certaines catégories de sites gérées par le proxy et de l'information des utilisateurs de cette pratique (34 %). Mais les chiffres les plus révélateurs de cette question sont peut-être l'absence de filtrage proxy pour 5% des répondants et l'absence de déchiffrement SSL pour

41%. Ces entreprises sont de fait moins armées contre la fuite de données et les connexions à des URL malveillantes.

L'authentification de la source des emails est un complément à la protection de la messagerie. Il s'agit de mettre en œuvre, sur ses domaines de messagerie, le **standard DMARC** (Domain-based Message Authentication, Reporting and Conformance) **[Q53]** qui permet de réduire le risque d'usurpation de nom de domaine. C'est un dispositif collaboratif car si toutes les entreprises appliquent le protocole DMARC en mode « reject », le taux de domaines de messagerie usurpés diminuera sensiblement, chacune garantissant à ses interlocuteurs de leur écrire seulement avec des noms de domaine vérifiés. 59% des organisation des 161 RSSI ayant répondu à cette question ont effectivement mis en œuvre DMARC (et le projet est en cours pour 20 %). Cette mise en œuvre n'est cependant pas sans potentiels effets de bord métiers. Ainsi DMARC est configuré en mode « supervision » uniquement, pour 21% des répondants où le projet est donc potentiellement toujours en cours. Les e-mails ne passant pas les contrôles sont mis en quarantaine par 11% des organisations et bloqués par les 28% les plus matures.

Une population, dans les entreprises, est particulièrement visée par les attaquants, quelles que soient leurs motivations. Il s'agit des administrateurs du système d'information. Plusieurs pratiques de cybersécurité permettent de réduire les risques inhérents à leurs accès très larges. Parmi celles-ci, les dispositifs de **Privilege Access Management – PAM** **[Q56]**, permettant une gestion centralisée des accès à risques, une authentification renforcée, une traçabilité, … tendent à se généraliser (69 % des entreprises ayant contribué à cette question). Néanmoins, la mise en œuvre de ce type de solution de « bastion » pose des questions de responsabilisation, le **propriétaire du PAM** devenant une sorte de « super administrateur » de l'ensemble du SI, en charge de la définition des stratégies d'accès à risques, de la gestion des exceptions, de la supervision du PAM et de la réaction à des comportements suspicieux. Ainsi, dans près de 25% des organisations, cette responsabilité est confiée à l'équipe RSSI, en position de « gardien du temple », mais dans 44% des entreprises cette responsabilité demeure aux sein des équipes techniques et/ou de production, intégrant ainsi le domaine de la sécurité opérationnelle et permettant potentiellement une gestion opérationnelle plus agile.

Une autre bonne pratique de cybersécurité visant à réduire l'exposition aux risques des administrateurs est de leur dédier un poste de travail spécifique à leurs activités à risques, en complément d'un poste standard. Ce **second poste d'administration** **[Q58]** est, le plus souvent, équipé d'un OS durci, isolé sur un réseau d'administration et ne permet ni de surfer sur Internet, ni de consulter ses e-mails. Si la pratique est en place dans 70% des entreprises, la pandémie et la généralisation du télétravail ont nécessité de s'adapter. Seules 19% des entreprises ont conservé un poste d'administration physique, différent du poste standard, y compris en situation de télétravail. Pour près de 51% des entreprises, le poste d'administration est un poste virtuel auquel les administrateurs accèdent via un dispositif de rebond, depuis leur poste standard, au bureau ou en situation de travail à distance.

Toujours dans l'objectif de réduire la surface d'attaque, une autre bonne pratique de cybersécurité consiste à **séparer les différents environnements**

techniques **[Q66]** de développement, tests/recette/qualification et production, voire pré-production/intégration. Mais cette bonne pratique à un coût, tant d'investissement matériel et logiciel que de maintien en conditions opérationnelles. C'est certainement ce qui explique que, de façon pragmatique, 52% des organisations ne séparent leurs environnements que pour une majorité et non l'intégralité de leurs systèmes, vraisemblablement les plus critiques. Cette séparation d'environnement est systématisée à l'ensemble des systèmes de 39% des organisations et est peu ou pas en place uniquement pour 8% d'entre elles.

Les approches de prévention cybersécurité évoluent régulièrement, voyant naitre ou évoluer de nouveaux concepts. Parmi ceux-ci, 2021 à été l'année où a vraiment commencé la promotion du **Secure Access Service Edge – SASE** **[Q60]**. Ce concept voit la convergence de différentes fonctions de réseau et de sécurité (proxy web avec inspection SSL, Zero Trust, CASB, DLP, firewall, SD-WAN, authentification des devices et des utilisateurs, MFA) dans un service cloud unique. L'objectif est de permettre aux utilisateurs, de plus en plus mobiles, d'accéder, depuis n'importe quelle localisation, de façon dynamique et sécurisée, aux applications et données dans le cloud. Si la promesse semble intéressante, 67% des répondants à cette question n'ont pas encore appréhendé ce nouveau modèle, 20% l'ont inscrit dans leur roadmap et seuls 13% ont franchi le pas et engagé un projet dont 3% sont bien avancés.

Au-delà de cet arsenal de prévention et de réduction de la surface d'attaque, les entreprises n'ont d'autres choix que de renforcer leurs capacités à détecter des attaques et à y faire face. La mise en place d'un **SOC** **[Q59]** est un projet prioritaire pour 20% des organisations, quand ce service n'est pas déjà mis en place (72%). Dans ce cas, en fonction de la taille de l'entreprise, de son secteur d'activité, de son exposition aux risques, des moyens consacrés à la cybersécurité, … se pose la question de l'externalisation totale ou partielle du SOC. Le mode hybride où les ressources et/ou activités internes collaborent avec des services et ressources externalisés, est le modèle le plus couramment déployé (37%). Le SOC exclusivement interne demeure le choix de 19% des organisations, probablement celles de plus grande taille alors que le SOC n'est entièrement externalisé que par 16% des entreprises. Enfin, 8,5% d'entreprises de disposent pas de SOC et n'ont pas en projet d'en mettre un en place. Ce dernier chiffre potentiellement à moduler du taux de déploiement des EDR où le service de supervision peut être inclus à l'offre ce qui, in fine, dote les entreprises les plus modestes d'un premier niveau de SOC intégré.

En cas d'attaque détectée par le SOC, une des premières étapes de réaction nécessitera de réagir face aux tentatives de **latéralisation** **[Q63]** de l'attaquant. Celles-ci ayant pour objectif d'étendre la compromission du point d'entrée initiale à de nouveaux systèmes, potentiellement plus « attractifs » ainsi que d'initier la persistance de l'attaque. Pour limiter la latéralisation, plusieurs dispositifs techniques peuvent être employés. 10% des entreprises s'appuient sur les capacités de mise en quarantaine du firewall local et/ou de l'antivirus alors que 23% s'appuient sur les capacités de mise en quarantaine automatisée par d'EDR. 15% ont fait le choix, non pas de s'appuyer sur les mécanismes endpoints mais sur des capacités d'isolation réseau mettant notamment en jeu les firewalls ou routeurs filtrants. 39% des répondants ont une approche combinant les mécanismes orientés endpoint et les mécanismes réseau. Enfin, 12% des

répondants ne mettent pas en œuvre de dispositif particulier afin de limiter les latéralisations.

Malgré l'évolution de la mise en œuvre des dispositifs de prévention, détection et réaction, force est de constater que le nombre d'attaques destructrices, de type ransomware, ne cessent d'augmenter. Il devient donc nécessaire, pour les entreprises, de prendre en compte que « cela peut arriver » et que certaines attaques réussies nécessiteront une phase de reconstruction afin, par exemple de **repartir après un ransomware [Q55].** La capacité de reconstruction nécessite des mesures de prévention qui, si elles ne sont pas spécifiques sont, à minima des mesures adaptées, comme par exemple, l'isolation de sauvegardes, ne pouvant être altérées par un logiciel malveillant. La phase de reconstruction nécessite également d'être formalisée dans des procédures, éventuellement au sein d'un dispositif de PCA. En Mars 2021 15% des 210 membres du CESIN ayant répondu à cette question s'estiment matures sur le sujet, qui est massivement en projet pour 68% d'entre eux, alors que 17% se concentrent sur les mesures de prévention.

La limitation de l'impact d'une attaque réussie peut également consister à mettre en œuvre une assurance dédiée aux sinistres de type cyber. Bien qu'étant un « produit » d'assurance assez récent, le taux d'équipement progresse rapidement puisque 72% des organisations disposent, en 2021, d'une couverture de **cyber assurance [Q62]** et que la souscription de celle-ci est un projet à court (12%) ou moyen (4%) terme pour de nombreuses autres. Seules 11,5% des organisation n'envisagent pas de souscrire. Parmi la majorité des entreprises couvertes, 57% le sont depuis plus de deux ans et envisagent de renouveler leurs contrats, tout comme celles ayant souscrit un contrat plus récemment. Seule une très petite frange (0,68%) d'entreprises n'envisagent pas de renouveler leur contrat.

Au-delà de ce panorama, assez large et éclectique des mesures de sécurité mises en œuvre par les membres, les questions hebdomadaires permettent également de faire un focus sur certains points d'organisation permettant le pilotage de la démarche. En particulier, face à l'omniprésence des menaces et la nécessité d'être en capacité de détecter et de réagir très rapidement en cas d'attaque, se pose la question de **l'organisation en 24/7 des équipes sécurité [Q49]**. Le dispositif est le plus souvent complexe à mettre en œuvre de façon efficace et coûte cher. C'est certainement ce qui explique qu'il ne soit pleinement mis en œuvre que par 13% des organisations. 8% ont entièrement externalisé ce service 24/7, ce qui induit potentiellement quelques limitations de prises de décisions en cas d'attaque importante en heure non ouvrées. Encore une fois, le pragmatisme l'emporte puisque la capacité minimale de détection et réaction en 24/7 s'appuie sur un mécanisme d'astreinte pour 33% des entreprises, alors que 45% ont fait le choix d'un service en horaires ouvrés uniquement.

Qui dit organisation de cybersécurité dit aussi ressources humaines et, depuis plusieurs années, pénuries de compétences et difficultés de recrutement. Pour faire face à cette situation, les entreprises ont recours à des **ressources humaines externes [Q52]**. Néanmoins, celles-ci restent majoritairement stables au sein des équipes (51%) et ne sont en hausse que pour 16% d'entre elles. Les 31% d'organisations pour lesquelles ce recours à des ressources

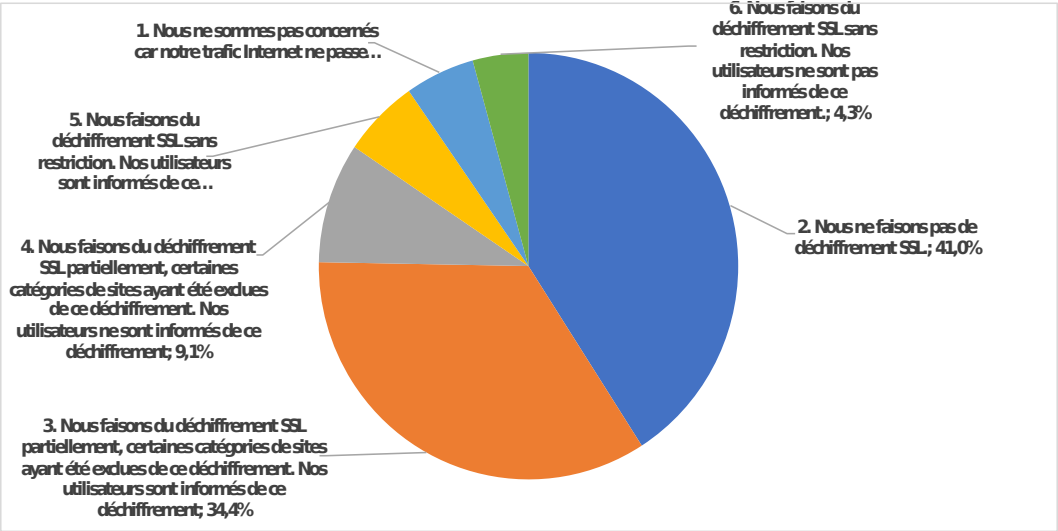
externes est en baisse sont potentiellement engagées dans un processus d'internalisation… ou de réduction des coûts.

ANNEXE

QUESTION DE LA SEMAINE : DETAIL DES RESULTATS

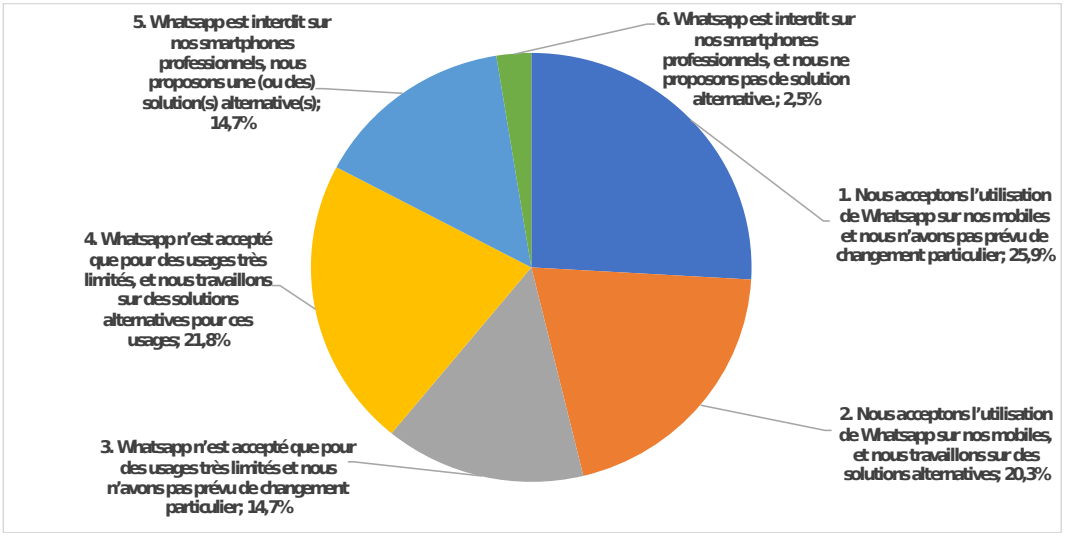
[Q46] Déchiffrement SSL

Les accès Internet passent généralement par un proxy qui assure un filtrage d'URL selon des catégories, des blacklists et des whitelists. Mais en pratique la quasi-totalité des accès à Internet se font en https. Pour que le proxy puisse être pleinement efficace, il est alors intéressant qu'il puisse déchiffrer le trafic, l'analyser, puis le rechiffrer. Le déchiffrement SSL pose bien sûr des questions de rupture de la confidentialité, notamment sur des accès Internet dans le cadre d'un usage personnel « toléré ». Quelle position avez-vous adoptée sur le déchiffrement SSL par votre proxy ?



[Q47] WhatsApp

WhatsApp est une application principalement à usage personnel (la version pro s'est peu développée) qui a pourtant une certaine pénétration dans les entreprises souvent en mode Shadow It .Où en êtes-vous vis-à-vis de cette application et que comptez-vous faire, au vu des nouvelles conditions d'utilisation de WhatsApp, qui annoncent le partage de données personnelles avec la maison-mère Facebook (pour les utilisateurs résidant en dehors de l'Union Européenne), conditions qui devront être acceptées avant le 8 février sous peine de se voir refuser l'accès au service ?

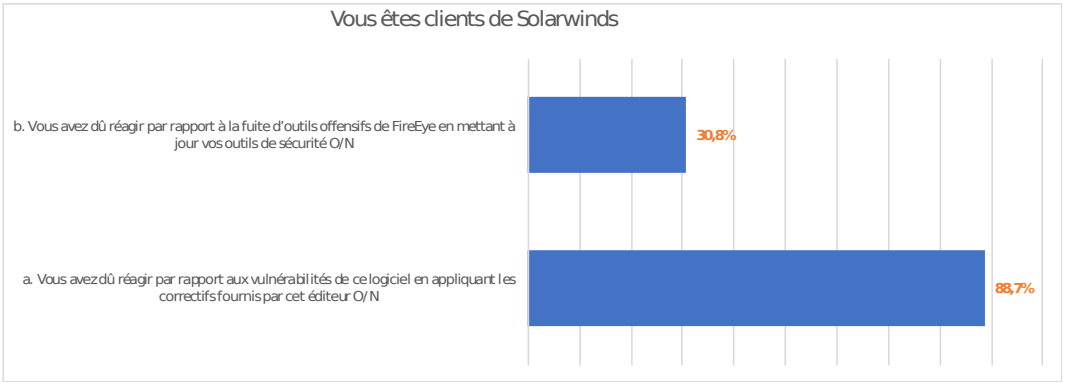


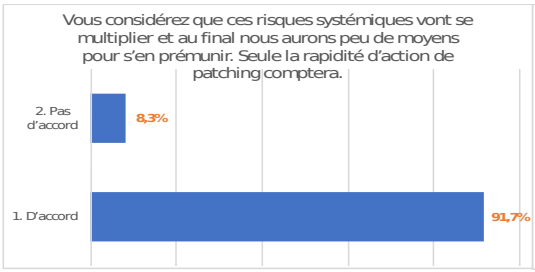
[Q48] Solarwind

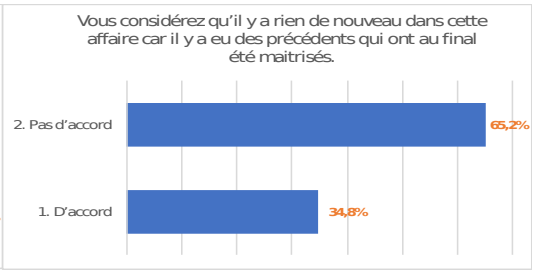
Fireye a découvert fin 2020 qu'elle était victime d'une cyberattaque. Les attaquants ont pu notamment exfiltrer un certain nombre d'outils de red team que Fireeye utilisait dans le cadre de de ses activités. Après des investigations menées par Fireye, Microsoft et le FBI, il a été identifié que cette cyberattaque s'était appuyée sur la modification par les attaquants du logiciel Orion de Solarwinds. Microsoft, Cisco et bien d'autres entreprises ont ainsi réalisé être également victimes de cette attaque car utilisateurs du logiciel compromis. On parle de 18000 victimes. Cette attaque a mis en évidence 2 risques :

- Le risque dit de la « supply chain logicielle » d'atteinte à l'intégrité du code sur des applications, et notamment des applications largement diffusées (ex : Solarwinds dans le cas présent)
- Le risque sur la fuite d'outils offensifs quand des organisations développant ces d'outils sont-elles mêmes victimes d'une cyber attaque (ex : Fireeye dans le cas présent)

Comment appréhendez-vous ce nouvel épisode de cyberattaque ?

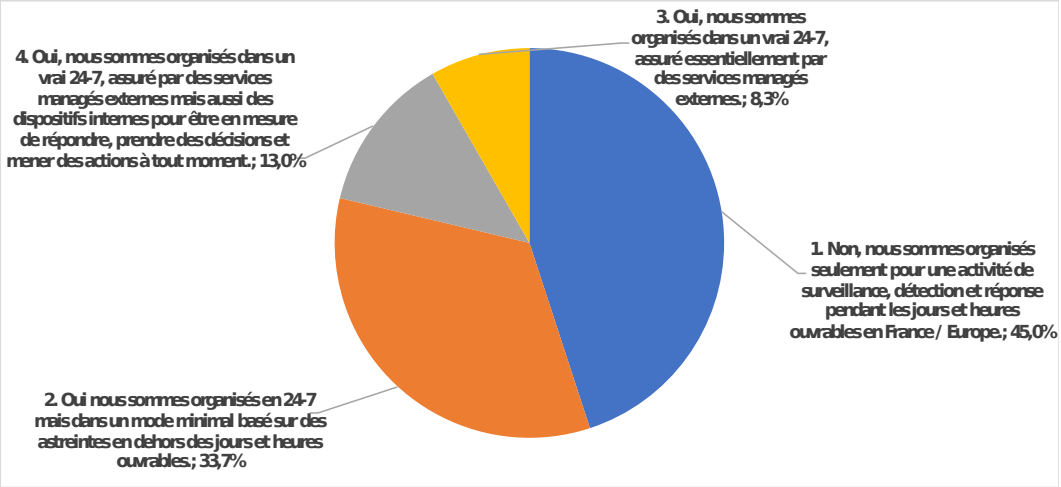






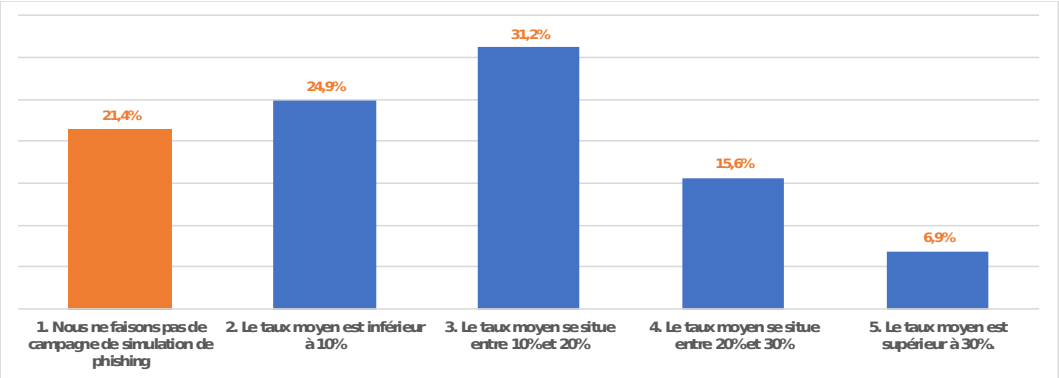
[Q49] Une cybersécurité 24/7

Notre métier compte de plus en plus sur les processus de détection et de réponse à incidents pour traiter les nouvelles menaces. Le temps de réaction à une attaque est déterminant pour en limiter l'impact. Avez-vous organisé vos processus de surveillance, de détection et de réponse pour qu'ils soient 24-7 sur toutes vos sites et régions du monde ?



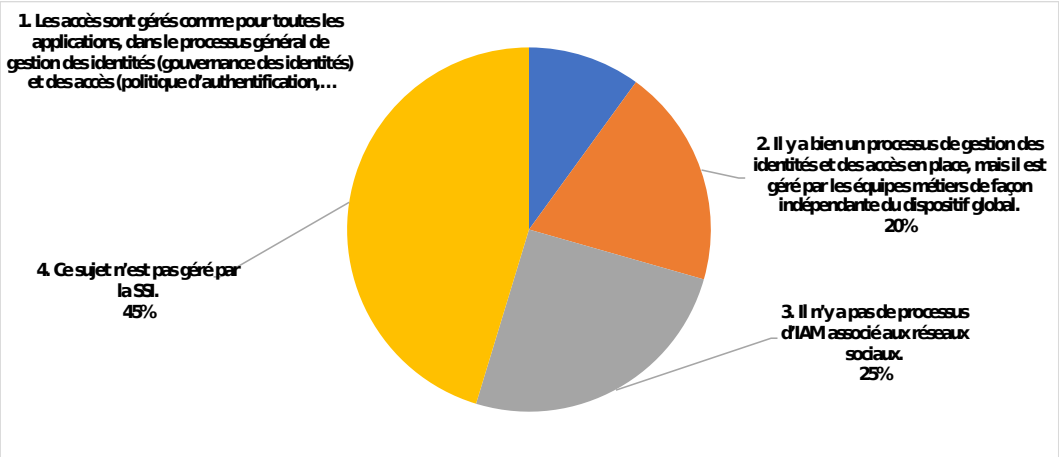
[Q50] Simulation de phishing

Le phishing reste le moyen d'attaque le plus fréquemment utilisé par les cybercriminels. Peut-être faites-vous des campagnes de simulation de phishing pour habituer vos utilisateurs à être vigilants face à cette menace. Les indicateurs clés pour ces campagnes sont le taux de clic sur les URL ou d'ouverture des pièces jointes, le taux de saisie de credentials, et le taux de signalement de mails « suspects ». Même si toutes les campagnes ne présentent pas le même niveau de difficulté pour les utilisateurs, et si l'on considère le premier indicateur : Quel taux de clic ou d'ouverture de pièce jointe observez-vous en moyenne ?



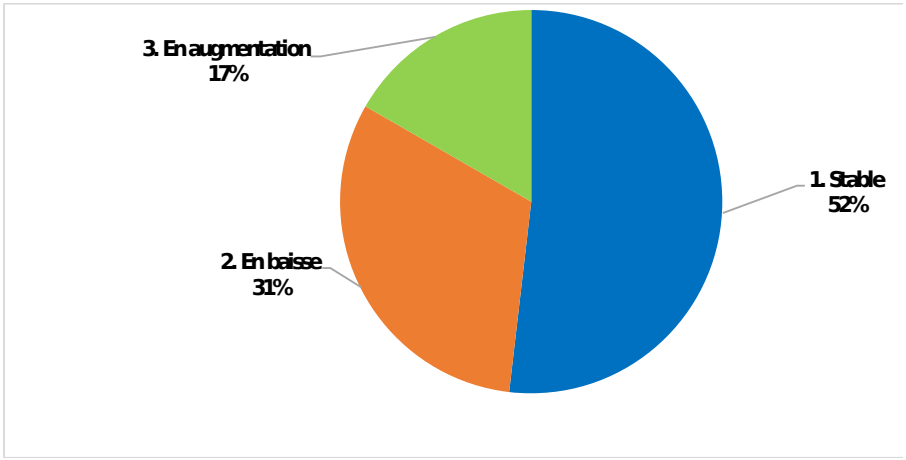
[Q51] Réseaux sociaux

Votre entreprise utilise les réseaux sociaux pour gérer des pages, poster des contenus, mettre en ligne des publicités. Comment gérez-vous l'accès à ces médias ?



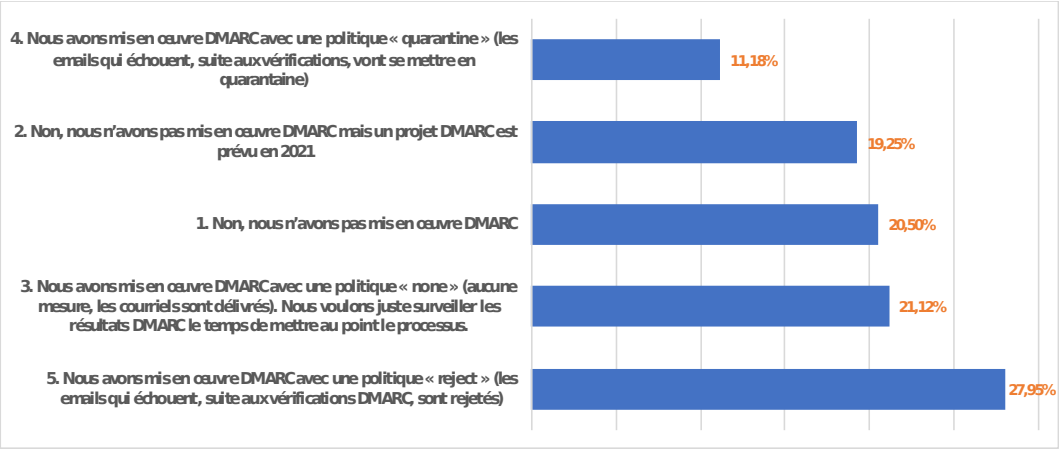
[Q52] Ressources humaines externes dans les équipes de cybersécurité

La question de cette semaine se porte sur les ressources humaines externes au sein de vos équipes : la part des ressources externes (ETP) par rapport aux ressources totales consacrées à la cybersécurité dans votre entreprise est-elle ?



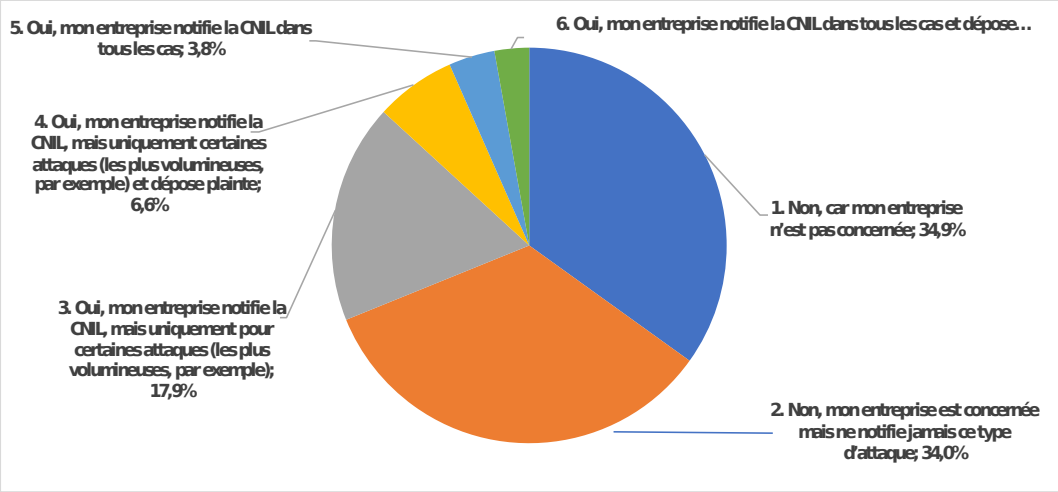
[Q53] DMARC

Le standard DMARC (Domain-based Message Authentication, Reporting and Conformance) est une stratégie d'authentification des emails pour assurer la protection contre l'usurpation des domaines de messagerie. La mise en place de DMARC s'est développée ces trois dernières années, face à la croissance très forte du phishing. Avez-vous mis en place le DMARC au sein de votre organisation, et si oui en appliquant quelle politique au niveau de l'enregistrement DNS de vos noms de domaine ?



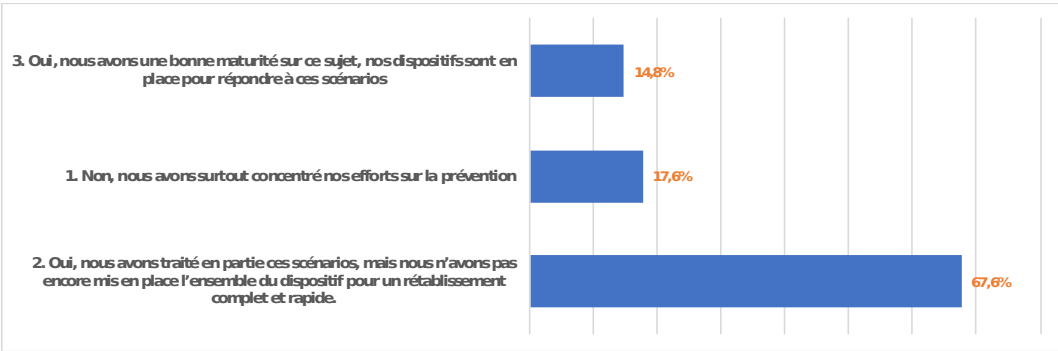
[Q54] Credential stuffing

Le credential stuffing est une attaque généralement exécutée à l'aide de robots, qui se sert typiquement de listes de credentials acquises ou disponibles sur le dark web par exemple (sites compromis, phishing…) et qui les utilise pour tenter de se connecter sur d'autres sites. Ainsi vous pouvez avoir des attaquants qui viennent sur votre site, arrivent à s'y connecter et vous voler des données, simplement parce que certains de vos clients ont utilisés les mêmes mots de passe sur différents sites dont le vôtre. Et vous êtes dans la situation d'une intrusion sur votre site alors qu'à la base, il y a eu d'abord une faille de sécurité ailleurs que chez vous. La CNIL vient de sanctionner un responsable de traitement pour lequel il y a eu plusieurs dizaines de notifications de violation de données : https://www.cnil.fr/fr/credential-stuffing-la-cnil-sanctionne-un-responsable-de-traitement-et-son-sous-traitant. Est-ce que vous notifiez à la CNIL les attaques de credential stuffing que vous subissez ?



[Q55] Repartir après un ransomware

Malgré les mesures de prévention, le nombre d'attaques destructrices qui réussissent, que ce soit des cryptolockers ou d'autre types d'attaques, a sensiblement augmenté depuis 1 à 2 ans. Il est essentiel de réduire les impacts de ces attaques en ayant la capacité à reconstruire ses systèmes et données endommagés. Cela veut dire des sauvegardes protégées pour qu'elles ne soient pas détruites elles aussi, mais aussi des procédures et dispositifs de reconstruction rapide de serveurs et de postes de travail. Et plus généralement des plans de continuité et de reprise d'activité qui intègrent le scénario du ransomware. Avez-vous travaillé sur ces questions ?

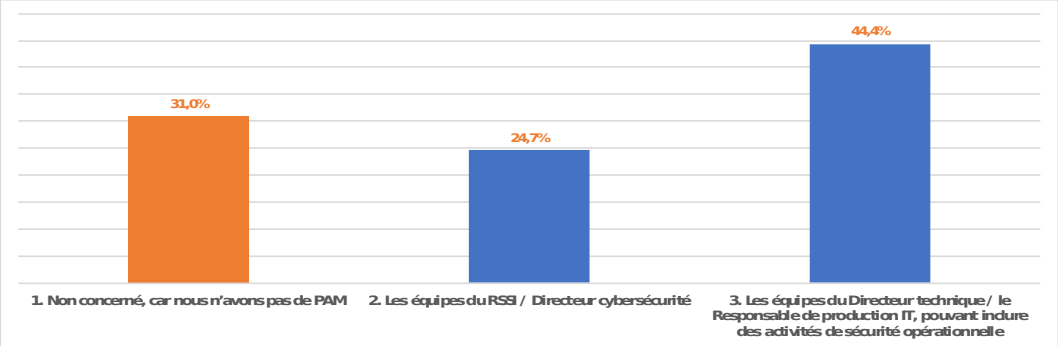


[Q56] Gouvernance PAM

La sécurisation des comptes à privilèges passe de plus en plus fréquemment par la mise en œuvre d'une solution de PAM (Privilege Access Management), qui assure, pour ces comptes, des fonctions d'authentification, de « proxy » avec rupture de connexion, de vault, de traçabilité, etc. Les acteurs autour du PAM sont :

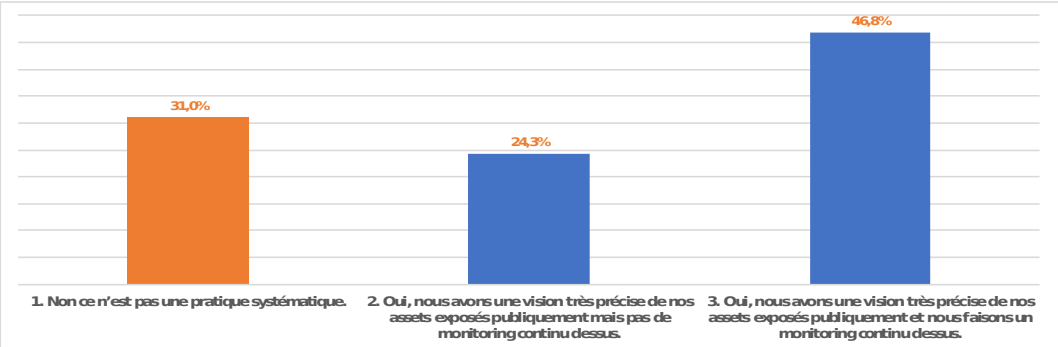
- Les utilisateurs de ces solutions qui sont des administrateurs IT internes et/ou des prestataires.
- Les personnes en charge du maintien en condition opérationnelle du PAM qui sont en général les équipes opérationnelles IT. Le responsable (propriétaire et super administrateur) de ces « bastions », qui est responsable des stratégies de connexion aux systèmes cibles, de la gestion des exceptions, du (ou des) super compte(s) « bris des glace » et a en charge l'analyse des logs et la levée de doute en cas de comportement suspect.

Dans quelle équipe se situe le responsable du PAM dans votre organisation ?



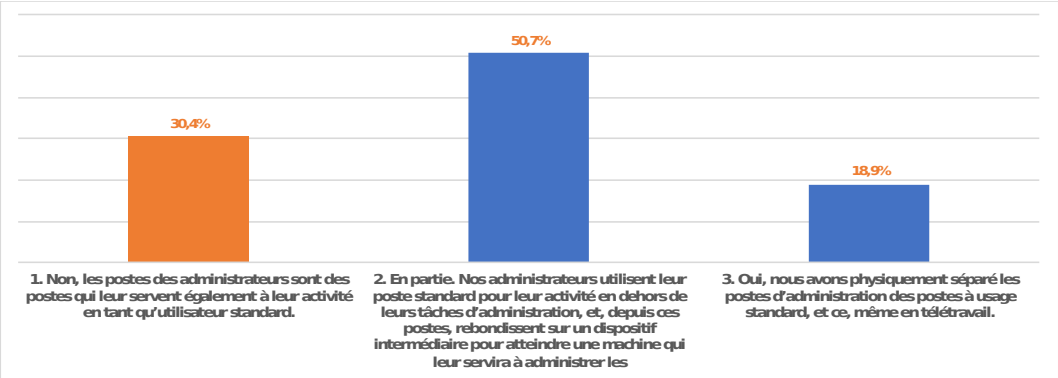
[Q57] Détection périmétrique

Un pourcentage élevé de cyberattaques arrive à entrer via du phishing, mais il y a aussi des attaques qui profitent d'IP publiques mal protégées. Pour éviter de subir une attaque via le second scénario, il faut d'une part bien connaître son exposition publique depuis des datacenters classiques ou depuis ses environnements cloud, et d'autre part il faut scanner ces assets pour vérifier qu'il n'y a pas de ports anormalement exposés. Réalisez-vous un inventaire / une découverte de votre périmètre et un monitoring de votre exposition publique ?



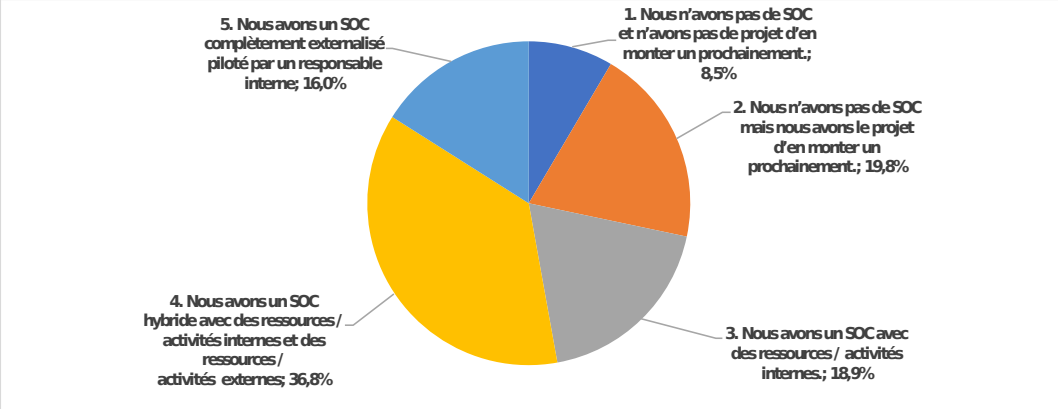
[Q58] Postes dédiés à l'administration

Il est recommandé de dédier les postes servant à l'administration de systèmes sensibles, de façon à limiter la surface d'exposition de ces postes. Ces postes sont supposés être durcis, isolés dans des sous-réseaux dédiés, sans accès à Internet et ne jamais être utilisés pour consulter des emails. Dans l'écosystème Microsoft, ce type de poste d'administration s'appelle des PAW. Avez-vous appliqué ce type de recommandation ?



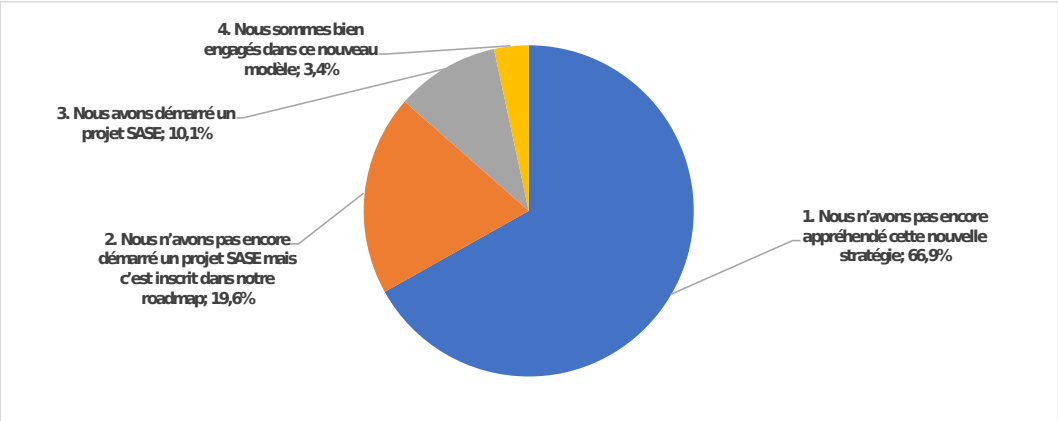
[Q59] SOC

Les SOC deviennent des dispositifs essentiels pour la cyberdéfense de nos organisations. Leur développement est très important. Où en êtes-vous avec ce dispositif ?



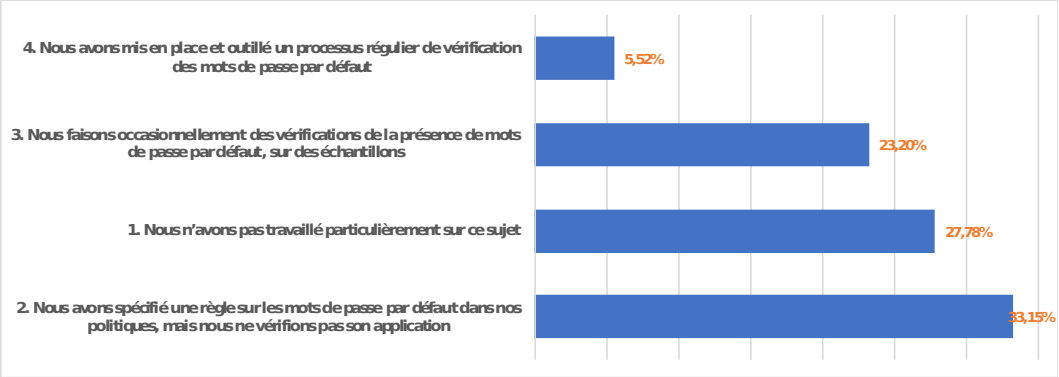
[Q60] SASE

Le SASE (Secure Access Service Edge) est un nouveau modèle qui combine et fait converger différentes fonctions de réseau et de sécurité (proxy web avec inspection SSL, zero trust, CASB, DLP, firewall, SD-WAN, authentification des devices, utilisateurs authentifiés avec du MFA) dans un service cloud unique pour permettre aux utilisateurs d'accéder, depuis n'importe quelle localisation, de façon dynamique et sécurisée, aux applications et données dans le cloud. Le SASE s'inscrit dans un contexte où l'utilisateur est de plus en plus mobile et non à l'intérieur d'un périmètre et que les données essentielles de l'entreprise sont dans le cloud.



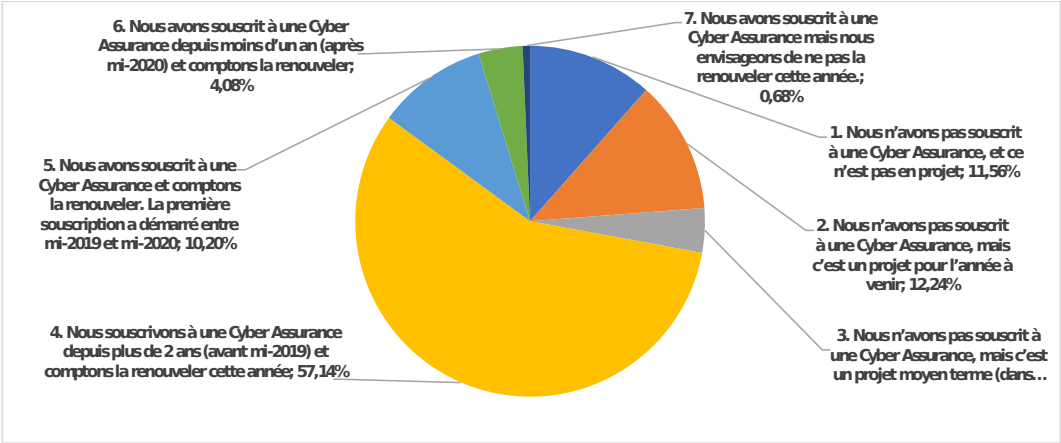
[Q61] Mots de passe par défaut

Les questions autour des mots de passe sont nombreuses. On peut parler de MFA, de passwordless et de diverses stratégies pour renforcer et tester les mots de passe. Ou s'interroger sur le cas particulier des mots de passe par défaut. Qui n'a pas constaté, à l'occasion d'un audit, que le pen testeur a exploité un mot de passe par défaut dans tel ou tel serveur Tomcat, équipement de réseau ou tout autre composant.



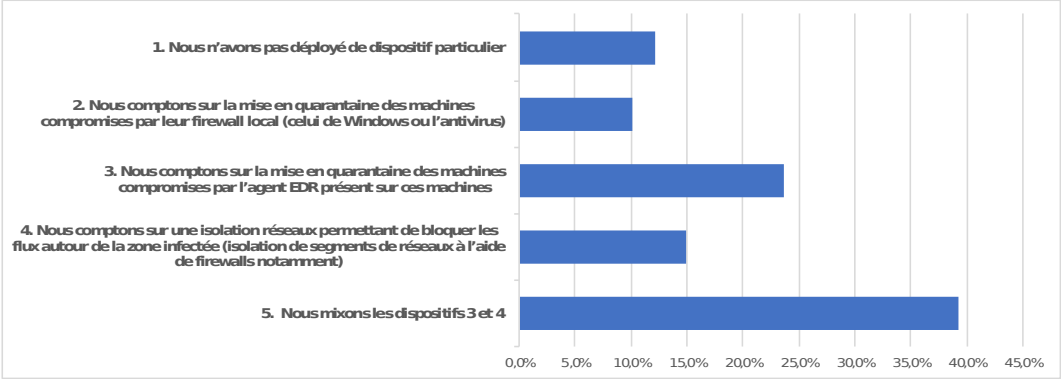
[Q62] Cyber Assurance

Le nombre d'attaques ayant des impacts financiers élevés est en constante augmentation. Les cas de ransomwares en sont une illustration. Depuis 3 ou 4 ans, la progression des souscriptions à des contrats de cyber assurance est elle aussi en croissance. Quelle est votre situation vis-à-vis de cette approche assurantielle ?



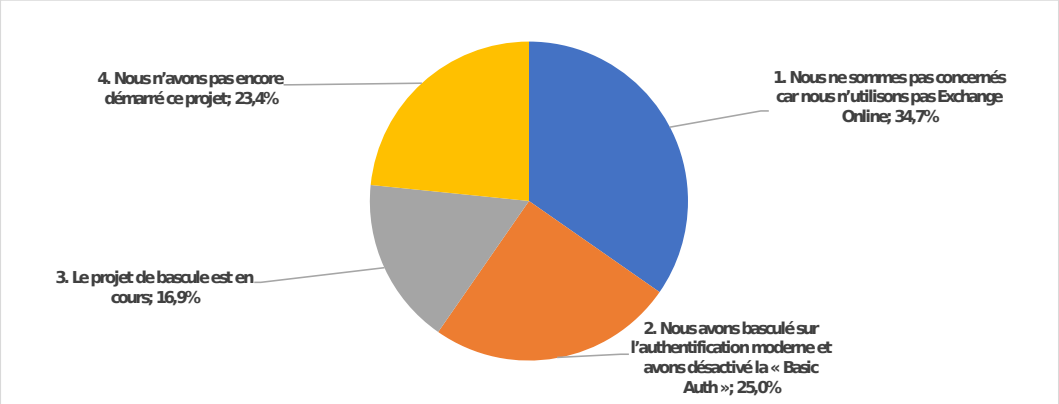
[Q63] Latéralisation

Lorsqu'une attaque a une capacité à se latéraliser rapidement, il est nécessaire d'une part de bloquer le point d'entrée de l'attaque et les connexions vers des sites malveillants, mais il est bien sûr urgent de stopper les mouvements latéraux pour limiter l'impact de l'attaque. Pour cela il s'agit d'isoler les systèmes infectés ou les réseaux dans lesquels ces systèmes se trouvent. Quelle stratégie d'isolation avez-vous prévue, mise en place et éventuellement utilisée dans ce cadre ?



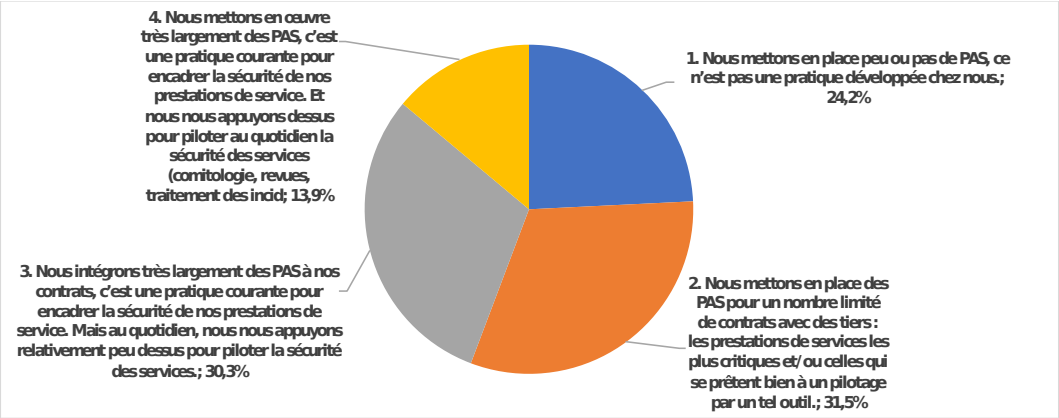
[Q64] Authentification basique Microsoft

Microsoft vient d'annoncer la date de fin de l'authentification basique (basic auth) pour le 1er Octobre 2022. Cette date limite a fluctué ces derniers mois, elle vient d'être confirmée. Cela concerne les utilisateurs d'Exchange Online. Le passage à la « Modern Auth » va améliorer sensiblement la sécurité des tenants O365. Où en êtes-vous de cette implémentation ?



[Q65] Plan d'Assurance Sécurité

Un Plan d'Assurance Sécurité est un outil contractuel qui permet de définir comment les politiques d'un tiers et nos politiques vont être mises en œuvre et s'articuler concrètement dans le cas d'une prestation donnée et la façon dont on va en contrôler et piloter l'exécution. Quel usage avez-vous des Plan d'Assurance Sécurité ?



[Q66] Séparation des environnements

Assurez-vous une séparation des environnements de développement, de qualification et de production ?