CESIN

LES INSTANTANÉS

1er Semestre 2023

2023

Le CESIN a mis en place depuis l'automne 2019, un dispositif d'enquête hebdomadaire appelé « la question de la semaine ». Ces enquêtes flash permettent, en 2 à 3 clics de recueillir la position des membres du Club sur un point précis, qu'il concerne leurs démarches de cybersécurité, un sujet d'actualité, une tendance ou une question de fond. Depuis novembre 2022, pour 900 membres interrogés, grandes entreprises, administrations et ETI, le CESIN à introduit à ses résultats une répartition des répondants par taille d'entreprise et secteur d'activité.

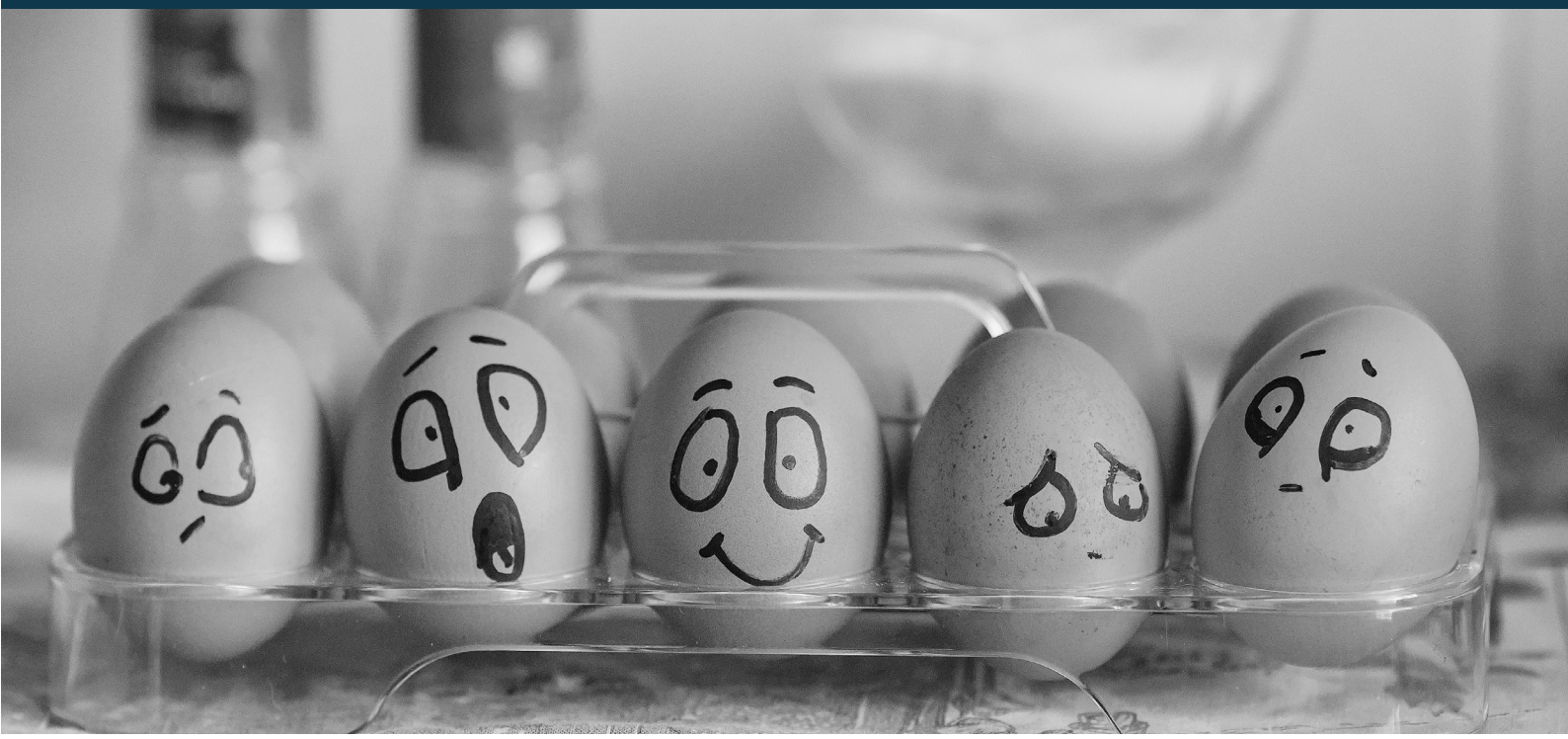
Cette synthèse analyse un florilège du premier semestre 2023 et s'appuie sur 27 questions.

Comme nous avions commencé à le dessiner lors de la présentation des instantanés 2022, les sujets sont divers et variés. Nous les regroupons selon 4 catégories : les sujets d'actualité, les mesures de sécurité, l'organisation / la gouvernance et les sujets innovants.

Les annexes comportent les métriques brutes liées aux résultats de ces sondages.

Sommaire

Les sujets d'actualité



Bilan de l'année 2022 et état d'esprit début 2023

En bilan de l'année 2022, vous avez été plus de 218 à nous partager votre avis sur vos principales préoccupations [Q95] durant l'année écoulée parmi :

- vous avez été **39%** à avoir eu pour principale préoccupation «la recherche de nouveaux talents et le maintien de vos experts dans votre équipe Cyber Sécurité.» ;
- **36%** d'entre vous ont pensé au sujet de la recherche de signes avant-coureurs d'un déploiement de Ransomware dans son organisation, face aux multiples attaques survenues durant l'année ;

la batailles des budgets – guerre perpétuelle dans toutes les organisations, quelles que soient leur taille et leur secteur d'activité – reste une préoccupation pour **20%** d'entre vous ;

- enfin, **5%** d'entre vous sont préoccupés par le sujet que l'on voit venir petit à petit durant cette année 2023 : les nouvelles conditions d'application et de souscription de la Cyber Assurance.

Ces préoccupations nous ont donnés l'occasion de vous interroger également, en tout début d'année sur votre **état d'esprit du moment** [Q97]. Vous avez été 225 à avoir répondu au sondage : près de **57%** d'entre vous affirment se sentir plutôt bien dont **29%** affirment se sentir dans un état d'esprit «normal» et **28%** affirment même être boostés avec un moral au beau fixe. Enfin, vous avez été **42%** à vous sentir dans un état d'esprit négatif, minés par le budget et/ou une charge de travail augmentée. On peut bien sûr s'interroger sur l'état de stress des RSSI au sein de la communauté et de manière générale, la profession en elle-même. Au second trimestre 2021, Advens et le CESIN se sont engagés dans la réalisation d'une étude sur le stress des métiers de Responsable en Cybersécurité, recouvrant principalement les fonctions de Directeur Cybersécurité et de Responsable de la Sécurité des Systèmes d'Information (RSSI). Cette étude a montré des niveaux de stress préoccupants au sein de la profession. Nous vous invitons à lire ce rapport intitulé « Apprivoiser le stress cyber pour apaiser un métier haut en couleur », mettant en lumière certaines prochaines étapes à mettre en œuvre pour diminuer ce risque (encore un !).

La veille Cybersécurité

La veille en cybersécurité consiste à rester à l'affût des menaces émergentes et des vulnérabilités potentielles. Cela implique la surveillance constante des activités malveillantes, la collecte d'informations sur les nouvelles techniques d'attaque et l'analyse des tendances de la cybersécurité.

Les chercheurs en cybersécurité, les analystes et les professionnels du domaine jouent un rôle essentiel dans cette phase de découverte.

Ses intérêts sont quadruples :

- **détecter les menaces :** la cybersécurité évolue rapidement, et les nouvelles attaques peuvent apparaître à tout moment. Avec une veille active, on peut identifier les tendances émergentes, les méthodes d'attaque et les vecteurs d'exploitation avant qu'ils ne deviennent répandus ;

- **réduire le temps de réaction :** la rapidité de réaction est essentielle en cybersécurité. La veille permet d'alerter les équipes sécurité dès qu'une menace potentielle est détectée, ce qui permet de prendre des mesures immédiates pour limiter les dégâts ;

- **limiter les pertes financières et de réputation :** les cyberattaques peuvent avoir des conséquences financières et sur la réputation non négligeable pour les entreprises et les organisations. En surveillant de près les activités malveillantes, la veille en cybersécurité permet de prévenir les incidents avant qu'ils ne causent des dommages irréparables.

- **améliorer la posture de sécurité :** les informations recueillies par la veille permettent aux organisations de mieux comprendre leurs vulnérabilités et de renforcer leur posture de sécurité. Cela inclut la mise en œuvre de correctifs, l'application de meilleures pratiques de sécurité et la sensibilisation des employés aux menaces potentielles.

Dans la profession de RSSI, la veille est une activité essentielle et partie intégrante des compétences clés recherchées chez un RSSI. Durant cette question de la semaine **[Q99]**, nous avons voulu savoir quelle veille vous et votre équipe pratiquez et comment. Vous avez été 228 à répondre à ce sujet essentiel. Diverses méthodes et sources existent pour assurer une veille riche et variée :

- **Surveillance des sources d'informations :** La veille en cybersécurité implique la surveillance continue des sources d'informations (dont les bulletins et veilles mensuelles du CESIN et vous êtes **75%** à utiliser les éléments de veille fournis par le club), les bulletins de sécurité (dont ceux de l'ANSSI, dont **70%** d'entre vous suivent les éléments fournis par l'agence), les forums de hackers, les rapports d'incidents et les flux de renseignements sur les menaces (Cyber Threat Intelligence - CTI) ;

    - **Presse en ligne spécialisée :** les médias spécialisés dans la cybersécurité fournissent des informations sur les dernières menaces, les vulnérabilités découvertes, les piratages notables et les meilleures pratiques de sécurité. Les professionnels de la cybersécurité et les entreprises peuvent s'abonner à ces sources pour rester informés des développements dans le domaine. **57%** d'entre vous affirment lire assidûment la presse en ligne spécialisée ;

    - **Événements :** les conférences, les webinaires sur la cybersécurité offrent une excellente opportunité de se tenir au courant des dernières tendances et des nouvelles technologies de sécurité. Ces événements rassemblent souvent des experts qui partagent leur expertise et leurs connaissances en matière de cybersécurité.

- **Collaboration entre les acteurs de la cybersécurité :** La veille en cybersécurité est renforcée par une collaboration active entre les équipes de sécurité, les agences gouvernementales, les fournisseurs de solutions de sécurité et d'autres parties prenantes, permettant un partage d'informations essentielles sur les menaces. De ce fait, **58%** d'entre vous exploitent le networking ;

- **Service de veille externe :** Certaines organisations optent pour des services de veille en cybersécurité fournis par des sociétés spécialisées / prestataires externes (cela représente **37%** des répondants). Ces services surveillent activement les infrastructures de leurs clients, analysent les comportements suspects et alertent les équipes de sécurité en cas de menace ;

    - Cas particuliers des Centres opérationnels de sécurité (SOC) : les SOC sont des unités spécialisées au sein d'une organisation chargée de détecter, d'analyser et de répondre aux incidents de sécurité en temps réel. Ils jouent un rôle crucial dans la veille en cybersécurité en surveillant continuellement les activités malveillantes et en prenant des mesures pour contrer les menaces. Vous êtes **38%** à bénéficier de la veille de votre prestataire SOC.

- **Utilisation de technologies d'analyse avancées (plutôt des acteurs CTI) :** Les outils d'analyse automatisée aident à trier les données massives collectées et à identifier rapidement les modèles et les comportements suspects (représentant **11%** parmi les répondants pour la catégorie « Autres » (Canal de veille CISA, activité de veille de CIX-A (+ une plateforme de CTI), du CESIN et de l'ECSO, abonnement à des groupes spécialisés, activité de veille par le CERT interne, salons, CEST du groupe, veille du CLUSIF, tweeter, suivi de feed)).

A noter : parmi toutes ces méthodes, **36%** d'entre vous affirment croiser les différentes sources.

En conclusion, la veille en cybersécurité est un élément essentiel dans la protection des systèmes et des données contre les attaques informatiques de plus en plus sophistiquées et variées. En anticipant les menaces, en réduisant le temps de réaction et en améliorant la posture de sécurité, la veille permet aux organisations de faire face aux défis des cybermenaces avec une meilleure préparation.

TikTok

On ne peut pas parler de veille sans sujet d'actualité autour de TikTok **[Q101]**. Vous avez été 193 répondants à nous donner votre avis sur votre posture sécurité vis-à-vis de cette application. TikTok permet aux utilisateurs de créer des vidéos courtes accompagnées de musique, de 3 à 180 secondes. TikTok devient le principal service de ce type en Asie, et l'application est au début des années 2020 considérée comme celle ayant la plus forte croissance tous pays confondus (depuis dépassée par ChatGPT). Cependant, cette popularité n'est pas sans soulever des problématiques en matière de sécurité, de confidentialité des données et de conformité aux réglementations.

En quoi Tik tok est problématique ? Le réseau social d'origine chinoise est accusé par de nombreux pays occidentaux de faire peser une menace en matière de protection des données et de cybersécurité.

Depuis le début de l'année, TikTok est dans le collimateur de nombreux pays occidentaux qui l'accusent de faire peser un risque inacceptable pour la vie privée et la sécurité de ses utilisateurs. Aussi, la Commission européenne a demandé à ses salariés de supprimer l'application au plus vite et les Etats-Unis et le Canada ont déjà interdit l'application chinoise sur les appareils gouvernementaux en raison de risques supposés d'espionnage.

Que dit la règlementation européenne ?

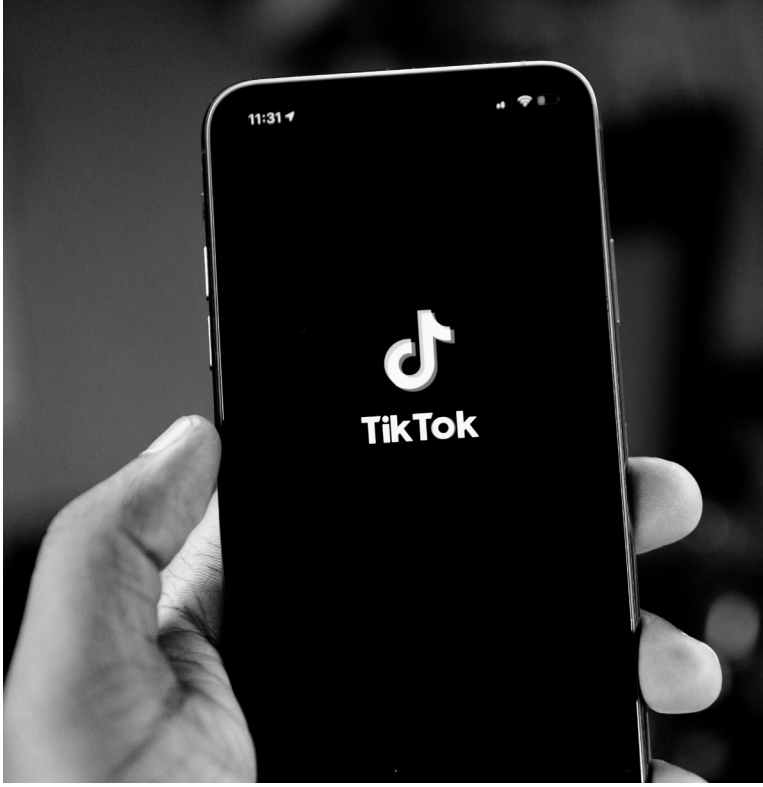
Jusqu'au 25 août pour se mettre en conformité DSA (Digital Services Act)

Ce règlement historique (DSA) est entré en vigueur mi-novembre 2022 (et sera appliqué en 2024) mais les entreprises ont jusqu'au 25 août pour se mettre en conformité. Parmi ces entreprises, dix-neuf très grandes plateformes en ligne, incluant Twitter, TikTok et les principaux services d'Amazon, Apple, Google, Meta et Microsoft, seront soumises à des contrôles renforcés. Les résultats du «test» de conformité qui avait été mené au siège européen du groupe à Dublin montrent que «des efforts supplémentaires sont nécessaires afin d'être totalement prêt» pour le 25 août, a commenté Thierry Breton, chargé de la régulation du numérique au sein de l'exécutif européen.

Les contraintes imposées aux entreprises par le DSA incluent l'obligation de procéder à une analyse des risques liés à leurs services en matière de contenus illégaux, d'atteinte à la vie privée ou à la liberté d'expression, mais aussi en matière de sécurité publique. A ce jour, l'ANSSI n'a pas publié d'étude sur les risques cyber liés à l'usage de TikTok. Des moyens adéquats, notamment dans la modération de contenus, doivent être mis en œuvre pour atténuer ces risques, et un accès aux algorithmes devra être accordé aux experts de Bruxelles. Le DSA comprend aussi des interdictions, comme celles d'exploiter les données « sensibles » des utilisateurs (genre, tendance politique, appartenance religieuse) pour de la publicité ciblée et des obligations de transparence, comme la publication des principaux paramètres utilisés par les systèmes de recommandation.

Pour le moment suite aux interdictions de TikTok dans d'autres pays européens, "le gouvernement a décidé d'interdire désormais le téléchargement et l'installation d'applications récréatives sur les téléphones professionnels remis aux fonctionnaires", a indiqué le ministère.

Du côté des Etats Unis le gouverneur du Montana a promulgué, mercredi 17 mai 2023, une loi qui bannit l'application TikTok dans cet Etat américain.



Conclusion

L'utilisation de TikTok soulève des préoccupations importantes en matière de sécurité, de confidentialité des données et de conformité aux réglementations. Pour assurer une utilisation responsable et sûre de TikTok, il est essentiel que les organisations mettent en place des mécanismes de protection liés à son usage (et dans son utilisation personnelle, s'intéresser au cas des mineurs), une modération de contenu efficace et une gestion responsable des données personnelles des utilisateurs.

En tant qu'utilisateurs, il est également important de prendre conscience des risques pour toute utilisation de réseau social et d'être attentifs à la confidentialité de données personnelles postées ou partagées tout en respectant les droits d'auteur et les droits des autres utilisateurs. Une étude et des décisions au cas par cas dans chaque organisation doivent être prises sur l'utilisation de TikTok. A ce stade, le principe de précaution demeure une bonne pratique : vous avez été **75%** à ne pas avoir pris de position, **15%** ont techniquement interdit l'application sur les smartphones professionnels et **10%** d'entre vous recommandent de ne pas l'utiliser sur les smartphones professionnels.

Surf Internet et conservation des données

Dans la même suite logique, l'utilisation d'Internet a révolutionné la manière dont nous accédons à l'information, communiquons et interagissons. Cette révolution numérique s'accompagne également de questions complexes concernant la protection des données et la vie privée. Dans ce contexte, la loi nous contraint à conserver un an ***tout le surf de nos employés sur Internet*** ainsi que le surf de nos clients pour ceux qui proposent des hotspots ouverts. Il s'avère que le volume des données à conserver est considérable finalement.

La Commission nationale de l'informatique et des libertés (CNIL) joue un rôle crucial en établissant des directives et des règles pour garantir que les données des utilisateurs soient traitées de manière éthique et conforme à la loi. Un document de la CNIL met en lumière l'importance de la conservation des « données de trafic » dans le cadre de l'utilisation d'Internet.

Les données de trafic

Les données de trafic se réfèrent aux informations qui sont générées lors de l'utilisation des réseaux de communication (e.g. Internet). Cela inclut des éléments tels que l'adresse IP du poste, la date, l'heure et la durée de connexion, ainsi que des détails permettant d'identifier le destinataire d'une communication. Ces données sont cruciales pour assurer le fonctionnement fluide d'Internet et sont essentielles pour les enquêtes criminelles et la sécurité en ligne.

En principe, ces informations devraient être effacées ou rendues anonymes pour protéger la vie privée des utilisateurs. Cependant, il existe des dispositions légales et réglementaires qui permettent de conserver ces données dans le but de faciliter la recherche et la poursuite des infractions pénales.

Dans le sujet de la question de la semaine **[Q113]**, nous avons interrogé les membres sur la manière dont ce **sujet du surf internet et de la conservation des données** est traité dans leur entreprise respective. Vous avez été 158 répondants dont **61%** à être en accord avec la loi.

Conservation des données par les employeurs

Lorsque les employeurs offrent un accès Internet à leurs employés, ils ne sont pas soumis à l'obligation de conservation des données de trafic selon la CNIL. Cependant, les employeurs ont le droit de surveiller l'activité en ligne de leurs employés, mais cette surveillance doit être effectuée dans le respect de certaines garanties, notamment l'information des employés sur le système de surveillance mis en place et la déclaration préalable du dispositif à la CNIL. En ce qui concerne nos membre, **26%** ont réduit la durée de conservation pour des questions de volume et de coût. Parmi ces derniers, vous êtes :

- **13%** à l'avoir réduit sur 6 mois ou plus ;
- **11%** à l'avoir réduit sur 3 mois ou plus ;
- **2%** à l'avoir réduit sur 1 mois ou plus ;
- **1%** à l'avoir réduit sur une période inférieure à 1 mois.

En conclusion, la conservation des données de trafic dans le contexte de l'utilisation d'Internet est une question complexe qui nécessite un équilibre entre la protection de la vie privée des utilisateurs et les besoins en matière de sécurité et d'application de la loi. Le document de la CNIL fournit des directives essentielles pour les établissements offrant un accès Internet public, ainsi que pour les utilisateurs individuels, afin de garantir que les données sont traitées de manière responsable et conforme à la loi : 2% d'entre vous ont une autre manière de traiter ce sujet.

Systèmes de communication / collaboration en cas de crise d'origine Cyber

La gestion de crise a également été un sujet d'actualité durant ce premier semestre. Vous avez été 193 à répondre à la question concernant les systèmes de communication et de collaboration en cas de crise d'origine cyber [Q114]. De plus en plus d'organisations sont confrontées à des cyberattaques sophistiquées et potentiellement dévastatrices pouvant entraîner le déclenchement d'une crise d'origine cyber. Lors d'une crise cyber par ransomware, il est possible que la solution principale de communication et de collaboration de l'entreprise soit rendue indisponible (Office 365, Google Workspace, etc.). Il semble donc sage de prévoir ce cas de figure afin de ne pas consommer trop de temps à organiser un système de fortune. Vous avez été **45%** à n'avoir rien prévu pour le moment et **20%** d'entre vous ont prévu de basculer sur une solutions grand public réduite. Par ailleurs, **23%** d'entre vous affirment avoir souscrit : soit une offre complète supplémentaire (9%), soit une offre sécurisée éventuellement souveraine réduite (14%). Il est noté que **12%** d'entre vous ont une autre manière de traiter ce sujet.

Événements et réunions Cybersécurité

Enfin, dans le dernier sujet d'actualité, nous avons remarqué que depuis quelques années, le ***nombre d'évènements et réunions cyber se multiplient***, et l'année 2023 s'annonce bien chargée. Ces différents évènements n'ont pas tous les mêmes objectifs, le même format et/ou le même visitorat. Ils n'apportent pas tous le même service ou la même valeur. Nous avons voulu avoir votre avis sur cette question de la semaine [Q104] et vous avez été 222 répondants.

Les événements et réunions cyber occupent une place importante dans le façonnement de la technologie, de la sécurité et des tendances émergentes : **6%** d'entre vous affirment participer librement à un maximum d'évènements tant ils sont source d'inspiration et riches d'enseignement.

En effet, ces rassemblements sont des opportunités pour les professionnels de la cybersécurité, les chercheurs, les développeurs et les entreprises de partager leurs découvertes, leurs retours d'expérience et d'explorer les nouvelles opportunités et risques qui se présentent à eux. Face à leur nombre grandissant, **84%** d'entre vous font le tri et participent à un nombre limité d'évènements car vous estimez que le calendrier des rencontres cyber est trop chargé par rapport au temps que vous pouvez libérer mais **47%** d'entre vous ont trouvé que ces différents évènements traitent souvent des mêmes sujets dans l'année et vous faites le tri pour éviter les répétitions.

Au fil des ans, ces événements ont été le théâtre de découvertes majeures. Des chercheurs ont mis en avant des vulnérabilités critiques dans des logiciels fortement utilisés, permettant aux entreprises et aux utilisateurs finaux de prendre des mesures correctives pour renforcer leur sécurité. Dans certaines conférences comme la DEF CON, des experts en sécurité exposent des failles critiques dans des systèmes d'exploitation couramment utilisés, offrant la possibilité de prendre le contrôle total des appareils des utilisateurs. Ces découvertes déclenchent une action rapide pour la mise en place de correctifs et a suscité une sensibilisation quant à l'importance des mises à jour régulières pour contrer ces menaces : **53%** d'entre vous participent à ces évènements pour concentrer votre veille des produits et services sur quelques jours dans l'année. Cependant, **39%** d'entre vous limitent fortement votre participation car vous trouvez que la pression commerciale y est trop forte.

Malgré tout, certains rassemblements sont importants et permettent de favoriser le partage d'expérience entre les professionnels de la cybersécurité : **63%** d'entre vous y vous pour rencontrer vos pairs et faire du networking. Ces échanges d'informations permettent aux acteurs du secteur d'apprendre des erreurs passées et d'améliorer leurs stratégies de défense : **15%** d'entre vous sont contributeurs actifs et prennent volontiers la parole lors de ces évènements mais **11%** participent à ces évènements mais sans s'exprimer car vous n'êtes pas autorisé(e) à communiquer durant ce type d'évènement alors que **7%** d'entre vous souhaitent prendre la parole dans une table ronde ou faire une présentation lors de l'un de ces évènements mais l'occasion ne s'est jamais présentée.

De plus, ces événements offrent un aperçu des nouvelles tendances émergentes dans le domaine de la cybersécurité. Ces tendances peuvent englober des évolutions dans les méthodes d'attaque utilisées par les cybercriminels, les nouvelles réglementations en matière de protection des données ou l'émergence de nouvelles technologies de sécurité, entre autres. Il est à noter tout de même que **14%** affirment être réticents à participer à certains de ces évènements, sur fond de loi Sapin 2.

Les mesures de sécurité

Les questions hebdomadaires soumises aux membres du CESIN traitent tout à la fois de processus et procédures que de mesures techniques. Elles ne sont pas ordonnées ici selon un quelconque ordre de priorité, ni par chronologie.

Répartition du Cloud dans le SI

Suite à la question posée lors du dernier baromètre au sujet de la part du Cloud dans votre SI, nous souhaitions affiner vos réponses car l'adoption du Cloud est sans doute différente en fonction du mode utilisé. L'idée était de connaître la répartition de votre SI (en %) **[Q102]**. Vous avez été 129 répondants et les résultats ont été les suivants : **56%** de vos SI sont hors cloud (on premises), **22%** en mode IAAS/PAAS et **25%** en mode SAAS.

Les services informatiques en nuage ont transformé la façon dont les entreprises déploient, gèrent et exploitent leurs infrastructures et applications. Le modèle du « cloud computing » offre divers services tels que le Software as a Service (SaaS), l'Infrastructure as a Service (IaaS) et le Platform as a Service (PaaS), chacun ayant ses avantages et ses cas d'utilisation spécifiques.

Sauvegarde des données hébergées

Les grandes solutions ***Cloud en mode SAAS*** garantissent un certain niveau de disponibilité de leurs services. Vous utilisez un service de « Digital Workplace » type Google / Microsoft office ou autre. La question de la semaine **[Q109]** consistait à savoir comment les membres assurent la sauvegarde des données hébergées et véhiculées par ces services. Vous avez été 134 répondants et **40%** affirment ne pas avoir de dispositif de sauvegarde et faire confiance au service.

À mesure que de plus en plus d'entreprises adoptent des services Cloud en mode SaaS tels que Google Workspace, Microsoft Office 365, Salesforce, et bien d'autres, la sauvegarde des données devient une préoccupation vitale pour garantir la disponibilité, la sécurité et la continuité des opérations.

Responsabilités partagées

Il est impératif de comprendre la notion de "responsabilités partagées" pour assurer une sauvegarde efficace des données dans un environnement Cloud / SaaS.

De nombreuses entreprises, à tort, estiment que leur fournisseur de services Cloud assume l'entière responsabilité de la sécurité de leurs données. Il est crucial de réaliser que la sécurité des données est une responsabilité partagée, comme l'exige par exemple le RGPD. Cette notion de "responsabilité partagée" signifie que le "responsable du traitement des données" (l'entreprise) et les "sous-traitants" (les fournisseurs de services Cloud) partagent des devoirs en matière de sécurité des données vis-à-vis des clients et des autorités de contrôle des données.

Les fournisseurs Cloud assurent la disponibilité de la plateforme, mais la gestion et la sauvegarde des données relèvent de la responsabilité des utilisateurs. Cette distinction est cruciale pour mettre en place une stratégie de sauvegarde efficace.

Sauvegarde tierce

Pour garantir une protection robuste des données, des solutions de sauvegarde tierces spécifiquement conçues pour les environnements SaaS peuvent être utilisées et vous êtes **34%** à avoir souscrit à l'offre de sauvegarde en ligne associée à ces services ainsi que **23%** d'entre vous font une copie à des fins de sauvegarde chez un autre fournisseur. Ces solutions automatisent les sauvegardes, offrent une flexibilité accrue, et peuvent prendre en charge simultanément plusieurs services SaaS, simplifiant ainsi la gestion des données. Des fonctionnalités de sauvegarde intégrées permettent aux utilisateurs de restaurer des données supprimées accidentellement ou de revenir à des versions antérieures de fichiers.

Il est recommandé d'établir un calendrier régulier pour la sauvegarde des données en fonction de leur criticité. Il est également primordial de conserver des copies de sauvegarde dans un lieu sécurisé et hors site pour une protection optimale (principe de la sauvegarde 3-2-1) : vous êtes **23%** à faire une copie on-premises à des fins de sauvegarde, respectant ce principe. Parallèlement, la gestion des autorisations est essentielle pour garantir que seules les personnes autorisées ont accès aux données sensibles et aux outils de sauvegarde.

Les racines des noms de domaine Google

Depuis le 10 mai 2023, 8 nouvelles racines de noms de domaine (.dad, .phd, .prof, .esq, .foo, .zip, .mov et .nexus) ont été publiées par Google. Les extensions .ZIP et .MOV au grand public, suscitant à la fois de l'enthousiasme et des inquiétudes parmi les utilisateurs et les professionnels de la cybersécurité. Ces deux TLD sont accusés de pouvoir être utilisés à des fins malveillantes. La question **[Q112]** de la semaine consistait à savoir les mesures que vous avez prises pour vous prémunir de ces risques. Vous avez été 130 à répondre à ce questionnaire et **67%** d'entre vous affirment n'avoir mis en place aucune mesure, ces 8 TLD sont accessibles à l'ensemble de vos collaborateurs et à n'avoir mis aucune mesure de mitigation en place.

Risque accrue pour le phishing

Si le .ZIP est communément utilisé pour l'archivage et la compression de fichiers, il est également largement exploité par les cybercriminels dans des campagnes de phishing. Ces attaques de phishing exploitent la similitude entre les noms de domaine .ZIP et les fichiers d'archives .zip pour tromper les utilisateurs et les inciter à télécharger des fichiers malveillants.

Des exemples tels que microsoft-office.zip et microsoft-office365.zip ont été mis en évidence, illustrant comment ces noms de domaine peuvent sembler parfaitement légitimes pour les utilisateurs qui cherchent à accéder aux services Microsoft Office ou Office 365. Cependant, en cliquant sur de tels liens, les utilisateurs risquent de divulguer leurs informations d'identification à des acteurs malveillants.

De plus, un chercheur en sécurité (Bobby Rauch) a mis en évidence des techniques sophistiquées de camouflage des liens malfaisants dans les URLs en .ZIP, rendant la distinction entre sites légitimes et malveillants plus difficile pour les utilisateurs. Cette situation a suscité des inquiétudes quant à la vulnérabilité des internautes face à de telles attaques.

Exemple :

- https://github.com/kubernetes/kubernetes/archive/refs/tags/v1.27.1.zip
- https://github.com/kubernetes/kubernetes/archive/refs/tags/@v1271.zip

Alors que la première mène bien au téléchargement du dossier compressé attendu, la seconde mène en fait vers un site, **https://v1271.zip**, qui pourrait être utilisé à de mauvaises fins.

Les questions de sécurité

Google s'est défendu en affirmant qu'il surveille de près l'utilisation des noms de domaine en .ZIP et qu'il dispose d'un système de sécurité intégré appelé Google Safe Browsing, qui protège les utilisateurs contre l'accès à des sites web malveillants. Cependant, malgré ces mesures, les professionnels de la cybersécurité demeurent préoccupés quant à la capacité des acteurs malveillants à exploiter ces nouvelles extensions.

Stratégies de protection et de gestion des noms de domaine

Pour les organisations soucieuses de protéger leur marque et leurs utilisateurs, des mesures préventives sont nécessaires. Certaines grandes entreprises ont déjà procédé à des enregistrements préventifs de noms de domaine en .ZIP pour éviter tout abus potentiel. Cependant, cette stratégie peut être coûteuse et ne garantit pas une protection totale contre les cybermenaces. De ce fait, **20%** d'entre vous affirment avoir bloqué un sous-ensemble (qui contient .zip et .mov) et **1%** à avoir bloqué les 8 TLD.

Surveillance des noms de domaine et réaction proactive

Une surveillance efficace des noms de domaine est également essentielle pour détecter rapidement les abus potentiels. **4%** d'entre vous ont ajouté des règles de surveillance de l'usage de ces nouveaux TLD. Cette surveillance peut être réalisée en utilisant des solutions de sécurité et des services d'EDR (Endpoint Detection Response). Les entreprises peuvent également s'appuyer sur leur SIEM (Security Information and Event Management) pour suivre les journaux DNS et identifier toute activité suspecte. L'utilisation d'outils de filtrage et de blocage des publicités (comme AdGuard, etc.) peut également être une solution et offre également des fonctionnalités de filtrage de contenu malveillant, y compris les domaines suspects.

La commercialisation des extensions .ZIP et .MOV par Google a suscité un débat sur la sécurité en ligne et la protection des utilisateurs. Alors que ces nouveaux noms de domaines offrent des possibilités intéressantes pour les marques et les services en ligne, elles peuvent également être exploitées par des acteurs malveillants pour des activités illicites. Les entreprises doivent donc mettre en place des stratégies de protection et de surveillance pour atténuer les risques liés à ces nouvelles extensions et garantir la sécurité de leurs utilisateurs en ligne. Face à ce débat, **8%** d'entre vous affirment avoir mis en place d'autres mesures.

Sécurisation des systèmes industriels

Les systèmes industriels sont de plus en plus connectés et interdépendants, ce qui augmente les risques liés à la sécurité des informations et des processus. La mise en place d'un programme de sécurisation efficace peut être un défi de taille pour de nombreuses entreprises. La question de la semaine **[Q107]** consistait à connaître les difficultés que vous rencontrez pour piloter la mise en œuvre de votre programme de sécurisation des systèmes industriels. Sur les 79 répondants - faible participation démontrant que "la prise de conscience de l'informatique industrielle n'est pas réservée qu'aux industriels » est encore faible – **67%** indiquent que la difficulté tient du cycle de vie plus long de certains équipements industriels et **33%** d'entre vous ont répondu que le programme est rendu difficile par l'inadaptation des offres de sécurité à évoluer dans un milieu de production industrielle à forte contrainte.

La sécurité des systèmes industriels est un sujet crucial en raison de l'augmentation des cybermenaces visant les infrastructures critiques industriels. Les systèmes industriels, tels que les SCADA (Systèmes de Contrôle et d'Acquisition de Données) et les ICS (Systèmes de Contrôle Industriel), sont utilisés dans des secteurs vitaux tels que l'énergie, l'eau, le transport et la production industrielle. Pour éviter les conséquences potentiellement désastreuses des attaques sur ces systèmes, les différentes organisations doivent mettre en œuvre des mesures de sécurisation appropriées. 56% d'entre vous pointent la responsabilité et les budgets délocalisés au sein de chaque entité industrielle ce qui ne favorise ni la standardisation ni la discipline de mise en œuvre et 18% ont priorisé et ne sécurisent que le(s) site(s) vitrine(s) de son organisation ou ceux classés OIV/OSE.

Malgré tout cela, **52%** d'entre vous notent un manque de maturité dans la perception du risque cyber des SI industriels et **48%** d'entre vous font face à une frilosité des responsables du SI industriels à perturber la production de votre organisation. En mettant en œuvre des évaluations de risques approfondies, en séparant les réseaux, en maintenant les systèmes à jour, en contrôlant strictement l'accès, en surveillant en continu et en sensibilisant les employés, les organisations renforcent leur posture de sécurité face aux menaces croissantes qui ciblent les systèmes industriels dans le cadre de programmes pluriannuels. Cela reste un vaste sujet à la fois technique et organisationnel, où **22%** d'entre vous considèrent que le chantier est très vaste et complexe et vous ne savez pas par quoi commencer ni comment l'organiser. Enfin, si le sujet est porté à un échelon stratégique de l'organisation, les tensions et difficultés peuvent être amoindries. Ceci est valable pour **6%** d'entre vous ayant affirmé que le pilotage est facilité car la DSI a repris la responsabilité des SI industriels.

DMARC et consors

Nous avions déjà abordé la ***question du DMARC*** lors d'une question de la semaine . Un post récent mentionnait que les acteurs du CAC40 sont passés de 15% à 35% de REJECT sur DMARC. Vous avez été 155 à avoir répondu à ce questionnaire **[Q94]**. L'idée était de savoir si vous aviez mis en œuvre le DMARC au sein de votre organisation, et si oui, quelle politique au niveau de l'enregistrement DNS de vos noms de domaine avez-vous appliqué ?

Le DMARC (Domain-based Message Authentication, Reporting, and Conformance) est un protocole d'authentification du courrier électronique devenu une mesure de sécurité essentielle dans la lutte contre les attaques d'usurpation d'identité, notamment le phishing. Il s'appuie sur :

- SPF (Sender Policy Framework), un protocole de vérification d'emails qui permet aux propriétaires de domaines d'indiquer les serveurs de messagerie autorisés à envoyer des emails en leur nom
- DKIM (DomainKeys Identified Mail), un mécanisme d'authentification des emails qui utilise des signatures numériques pour vérifier l'intégrité et l'origine du message

Le DMARC permet de garantir la fiabilité de l'en-tête from du domaine expéditeur, renforçant ainsi la confiance dans les communications électroniques.

Vous êtes **30%** à ne pas avoir mis en œuvre DMARC dont **14%** en ont le projet pour 2023.

Le phishing et l'usurpation d'identité sont des menaces grandissantes sur Internet. Grâce à DMARC, les propriétaires de domaines peuvent contrer ces attaques malveillantes qui exploitent la confiance des utilisateurs. DMARC offre une méthode éprouvée pour protéger les marques, les clients et les destinataires contre les conséquences de ces tentatives d'usurpation.

Protection contre des menaces

Le DMARC joue un rôle (important) pour empêcher diverses formes d'attaques malveillantes, dont :

- **Usurpation de domaine :** Les cybercriminels usurpent l'apparence des domaines d'entreprises légitimes pour créer des emails frauduleux qui trompent les destinataires.
- **Usurpation d'adresse électronique :** Les attaquants se font passer pour des adresses électroniques légitimes, induisant en erreur les destinataires quant à l'expéditeur réel.
- **Business Email Compromise (BEC) :** Les escrocs se font passer pour des hauts responsables d'entreprises pour tenter de détourner des fonds ou de voler des informations sensibles.

- **Email de phishing :** Les emails de phishing cherchent à inciter les destinataires à divulguer leurs informations d'identification ou à installer des logiciels malveillants en se faisant passer pour des marques légitimes.

Avantages supplémentaires

En plus de protéger contre les attaques, DMARC offre également des fonctionnalités de création de rapports détaillés. Les propriétaires de domaines peuvent recevoir des rapports sur l'activité d'authentification des emails, leur permettant ainsi d'analyser les messages acceptés ou refusés et de connaître leur origine.

La gestion efficace de DMARC implique une configuration et une maintenance continues des politiques pour un domaine. Une surveillance attentive des activités d'authentification des emails et une capacité à ajuster les politiques DMARC en fonction des besoins sont essentielles pour maintenir une protection solide.

Vous êtes **70%** à avoir déjà mis en œuvre cette mesure de sécurité avec :

- une politique « none » pour **23%** ;
- une politique « quarantine » pour **19%** ;
- une politique « reject » pour **28%**.

On peut noter **une augmentation de 10%** de la mise en œuvre DMARC par rapport à 2021.

Passwordless

La multiplication des mots de passe pour nos utilisateurs, rend la sécurité fragile : réutilisation du même mot de passe, utilisation de base de mot de passe trop facile à deviner…Et que dire du célèbre 2022 remplacé par 2023 dans un mot de passe ! Le ***passwordless*** combine identité de l'utilisateur avec des méthodes de validation de celui-ci par du biométrique ou des clés de sécurité ou encore du MFA. L'idée de cette question de la semaine était de savoir si vous aviez engagé des études sur la mise en œuvre du passwordless dans votre organisation **[Q111]**. Vous avez été 186 répondants et **39%** à penser vous pencher sur le sujet dans les 2 ans qui arrivent, **21%** à étudier le passwordless pour un déploiement à court terme.

Le Passwordless est un concept visant à éliminer l'utilisation des mots de passe pour les services en ligne. Il utilise des méthodes d'authentification telles que la biométrie, les clés de sécurité ou les codes à usage unique. Les mots de passe sont souvent vulnérables aux attaques, et l'authentification multi facteur n'est pas parfaite. Les mots de passe entraînent également des problèmes d'expérience utilisateur et des coûts élevés. C'est pourquoi, **4%** d'entre vous ont répondu que le passwordless est déjà déployé partout dans votre organisation.

Cette solution a également ses inconvénients à ce jour :

1. **Dépendance technologique** : le Passwordless repose sur des technologies avancées telles que la biométrie ou les clés de sécurité. Si ces technologies rencontrent des problèmes techniques ou sont compromises l'accès aux services en ligne peut être bloqué.

2. **Coûts initiaux :** la mise en œuvre du Passwordless peut nécessiter des investissements initiaux importants pour l'acquisition et la mise en place des technologies nécessaires.

3. **Interopérabilité :** l'adoption généralisée du Passwordless nécessite une compatibilité et une interopérabilité étendues entre les différentes plates-formes, système d'exploitation, d'infrastructure et fournisseurs de services. De ce fait, **20%** d'entre vous considèrent que leur infrastructure n'est pas du tout prête pour ça;

4. **Confidentialité des données biométriques :** l'utilisation de la biométrie dans le cadre du Passwordless soulève des questions concernant la confidentialité et la protection des données biométriques des utilisateurs. les préoccupations concernent principalement la manière dont ces données sont stockées, traitées et protégées contre les violations de sécurité ou les utilisations abusives.

5. **Utilisation limitée sur certains appareils :** certaines méthodes d'authentification sans mot de passe, telles que la biométrie ou les clés de sécurité, peuvent ne pas être largement prises en charge sur tous les types d'appareils ou dans tous les environnements.

Compte tenu de ces inconvénients, **7%** indiquent que vos utilisateurs ne sont pas prêts pour le passwordless et **9%** d'entre vous ont répondu autrement : déploiement partiel, pas convaincu, solutions pas assez matures, etc.

Windows HELLO

Dans la continuité du sujet, les avis ont toujours été partagés sur la biométrie, même stockée localement, entre la simplicité d'usage et les questions de privacy. Vous avez été 242 répondants **[Q98]** concernant l'utilisation de ***Windows Hello, une fonctionnalité de Microsoft introduite avec Windows 10,*** qui permet aux utilisateurs d' s'authentifier de manière sécurisée sur leurs appareils Windows à aide de la biométrie ou d'autres méthodes d'identification. Windows Hello propose plusieurs options d'authentification, notamment la reconnaissance faciale, la reconnaissance d'empreintes digitales et la reconnaissance de l'iris. Vous êtes près de **80%** à ne pas l'utiliser et ce indépendamment de la taille de vos entreprises.

Pour aller plus loin et comprendre les **20%** d'utilisateurs de cette technologie, notons que cette dernière vise à remplacer les mots de passe traditionnels, considérés comme moins sécurisés, offrant des méthodes d'authentification plus fiables et pratiques. En utilisant des caractéristiques biométriques uniques (empreinte digitale ou reconnaissance faciale) à chaque individu, Windows Hello permet de renforcer la sécurité des appareils et des comptes utilisateurs.

Windows Hello utilise des capteurs matériels spécifiques pour capturer et comparer les données biométriques, garantissant une protection avancée contre les attaques de contrefaçon ou d'usurpation d'identité. Les informations biométriques sont stockées localement sur l'appareil et ne sont pas transmises via Internet, évitant ainsi que le secret ne soit propagé sur la toile.

Windows Hello tend vers une approche "Passwordless" (sans mot de passe) en matière de sécurité informatique. Cette technologie offre une alternative intéressante en proposant une authentification forte et pratique, basée sur des méthodes biométriques.

Les **20%** qui l'utilisent sont répartis comme suit :

- **7%** partiellement pour des raisons de compatibilité matériel ;
- **7%** en laissant le code pin à 6 chiffres ;
- **6%** en durcissant la complexité du code pin (pour réduire les risques de shoulder surfing).

Conclusion

Windows Hello offre une authentification biométrique avancée, sécurisée et pratique, permettant de remplacer les mots de passe traditionnels. Son adoption contribue à renforcer la sécurité tout en simplifiant l'expérience utilisateur. Toutefois, il est essentiel de prendre des mesures pour contrer les éventuelles vulnérabilités et d'être conforme au RGPD pour protéger la vie privée de ces utilisateurs

Politique des mots de passe

Pour finir dans le cycle des mesures sur les mots de passe, la question **[Q110]** visait à connaître votre choix entre ***l'ergonomie liée à l'habitude des utilisateurs de gérer des changements à 8 caractères et le renforcement de la sécurité sur la politique des mots de passe***. Vous avez été 215 répondants.

La sécurité des données et des systèmes d'information est un enjeu crucial pour toute entreprise. Une des premières lignes de défense contre les attaques informatiques est la mise en place d'une Politique de Gestion des Mots de Passe (PGMP) solides L'ANSSI et le National Institute of Standards and Technology (NIST) fournissent des directives essentielles pour créer et maintenir des mots de passe sécurisés, ainsi que pour sensibiliser les employés aux meilleures pratiques en matière de sécurité informatique.

Recommandation de mot de passe

L'un des piliers d'une PGMP efficace est la création de mots de passe solides. L'ANSSI et le NIST préconisent des approches similaires :

- Opter pour des mots de passe d'une longueur minimale de 12 caractères (pour l'ANSSI) et 8 caractères (pour le NIST) : **29%** d'entre vous sont passés à 12 caractères en allongeant la durée de vie du mot de passe et **24%** à être passé à 12 caractères sans changer les autres critères de sa PGMP ;
- Intégrer une combinaison de caractères spéciaux, de chiffres, de majuscules et de minuscules en combinant avec le MFA pour renforcer la complexité : **25%** à avoir choisi d'autres solutions (10, 14 ou 16 caractères + MFA, politique adaptée pour les applications critiques,etc.) et **54%** d'entre vous ont mis en place du MFA ou équivalent pour les accès les plus critiques et où la longueur du mot de passe a moins d'incidence sur votre sécurité ;
- Éviter l'utilisation d'informations personnelles (date de naissance, lieu de résidence)
- Activer le renouvellement automatique des mots de passe, en particulier pour les comptes sensibles

Il est noté que **17%** d'entre vous ont une PGMP imposant 8 caractères et déclarent n'avoir rien changé.

Conclusion

Il est difficile de se baser uniquement sur les recommandations des organismes, malgré leur convergence en matière de sécurité l'ANSSI et le NIST ne partagent pas toujours des recommandations identiques concernant la gestion des mots de passe. Ces dernières sont d'ailleurs très vastes et difficiles à mettre en pratique.

Certains prônent l'utilisation de mots de passe générés à partir de termes du dictionnaire, tandis que d'autres privilégient des séquences de caractères aléatoires.

Cette divergence met en lumière la complexité du paysage de la cybersécurité et souligne la nécessité pour chaque entreprise d'adapter sa PGMP en fonction de ses besoins spécifiques, de son environnement et selon la criticité de ses actifs. Il est impératif de se mettre à la place de l'utilisateur, de comprendre les ressources nécessaires et les compétences requises pour maintenir ces mots de passe à un niveau de sécurité élevé et équilibré, en prenant en compte les besoins spécifiques en matière de sécurité. Il est important de noter qu'une politique de mot de passe trop contraignante pourrait devenir inutilisable, entraînant une perte d'efficacité en matière de sécurité pour les utilisateurs.

L'établissement d'une PGMP robuste demeure un élément fondamental de la sécurité informatique moderne ou dans certains cas, se tourner vers des solutions alternatives : SSO, Passwordless, etc.

La gouvernance / l'organisation

La sensibilisation : test de faux phishing

Les questions hebdomadaires portants sur la gouvernance se sont intéressées à certains piliers de celles-ci, à commencer par le sujet far de la ***sensibilisation*** [Q96], avec les campagnes de sensibilisation qui reposent sur plusieurs types d'action. L'une d'entre elles consiste à organiser des tests de faux phishing auprès des collaborateurs afin de mesurer leur niveau de vigilance et de préparer une formation adaptée. Vous avez été 280 à répondre à cette question de la semaine.

Ces tests sont réalisés sous forme d'envois d'e-mails conçus pour ressembler à des communications légitimes et incitent les destinataires à cliquer sur des liens malveillants, ouvrir des pièces jointes ou à divulguer des informations sensibles.

Pourquoi le phishing est-il tant privilégié par les hackers ?

Le phishing est un choix de prédilection pour les hackers, car même un fraudeur novice peut facilement créer un e-mail d'hameçonnage basique. De plus, l'aspect le plus important est que le "pare-feu humain" est couramment exploité par les pirates informatiques.

Selon vous, les attaques par phishing demeurent les plus fréquentes subies par les entreprises (représentant près de 80% des attaques), suivies de près par la fraude au président.

Se protéger contre le phishing

L'objectif principal de ces tests ou campagnes est de sensibiliser les utilisateurs aux techniques utilisées par les cybercriminels et de les éduquer sur la manière de reconnaître et d'éviter les attaques de phishing. De plus en plus de fournisseurs proposent des solutions de tests de faux phishing et de sensibilisation associée, offrant une variété de scénarios et d'e-mails personnalisables. Ces outils permettent aux RSSI de planifier, d'exécuter et d'analyser les résultats des campagnes de sensibilisation au phishing, en fournissant des rapports détaillés sur les taux de clics, les erreurs courantes et les progrès réalisés dans la formation des utilisateurs.

Mener une campagne de sensibilisation à la cybersécurité, et plus particulièrement à l'hameçonnage, nécessite :

- l'animation de séances de formation et de sensibilisation à la sécurité, en présentiel et/ou en e-learning ;
- la programmation de l'envoi régulier d'e-mails de phishing fictifs aux collaborateurs ;
- l'investissement en temps pour la production, le déploiement, la mise en œuvre, le suivi et les indicateurs de performance et d'efficacité de la sensibilisation.

Cette approche proactive en matière de sensibilisation à la sécurité informatique est devenue essentielle, car les attaques de phishing continuent d'évoluer et sont passives. Vous êtes **89%** à faire des tests de faux phishing auprès de vos collaborateurs : 19% d'entre vous les réalisent de manière mensuelle, 50% programment ces campagnes plusieurs fois par an et au moins une fois par an pour 21% d'entre vous.

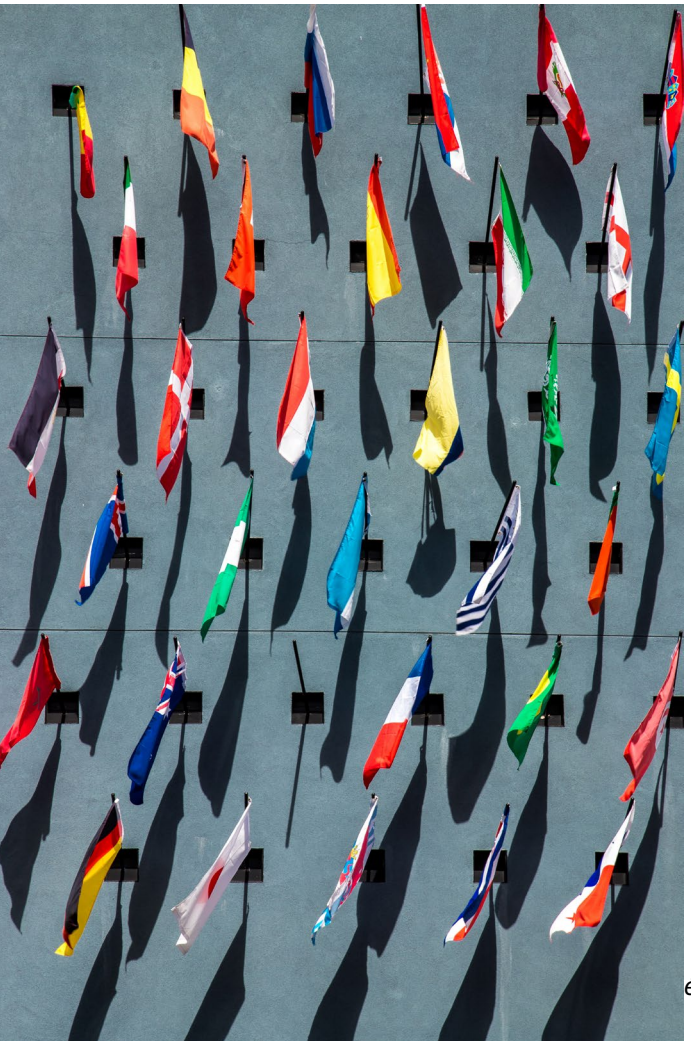
Conclusion

La sensibilisation au phishing et la réalisation de tests de faux phishing sont des mesures organisationnelles essentielles pour renforcer la sécurité des organisations face aux cyberattaques. Le phishing reste une méthode de choix pour les hackers en raison de sa simplicité et de l'exploitation (abusée) du pare-feu humain. Renforcer la vigilance les collaborateurs et instaurer une culture quotidienne de cybersécurité permet de réduire les risques liés aux attaques de phishing et de protéger l'organisation contre les pertes économiques, les dysfonctionnements du système, les retards dans les activités et la dégradation de l'image. Vous avez été **11%** à affirmer ne jamais réaliser de campagnes de faux phishing.

Nationalité des solutions de sécurité

Durant la 100ème question de la semaine, nous nous sommes penchés ***sur la nationalité des solutions de sécurité*** **[Q100]** que vous utilisez dans vos entreprises. Selon vos réponses à notre dernier baromètre, vous utilisez, en moyenne 15 solutions de sécurité. Nous vous avons demandé de considérer la liste (pour certains ce sera moins que 15 solutions, pour d'autres ça peut être plus voire beaucoup plus) et de répartir ces solutions selon leur nationalité. L'objet de la question était de mieux cerner le marché des solutions de cybersécurité déployées en France. Vous avez été 173 répondants. La majorité d'entre vous utilisent des solutions américaines (70%) tandis que **30%** utilisent des solutions de nationalité européenne, dont 20% sont françaises.

La question de la nationalité des fournisseurs des solutions de sécurité suscite de plus en plus d'attention en ces temps d'instabilités politiques. Cela avait été un vrai débat lors du début du conflit entre la Russie et l'Ukraine. La nationalité d'un fournisseur de sécurité peut avoir des implications sur la confidentialité des données, la souveraineté nationale, la sécurité nationale et la confiance dans les technologies utilisées



La nationalité des fournisseurs de solutions de sécurité est devenue une question importante pour les entreprises et les gouvernements à l'ère de la transformation numérique. Il est essentiel que les organisations considèrent ces aspects dans leur processus d'achat et prennent des décisions éclairées en fonction de leur situation spécifique. La transparence, la sécurité, et la conformité aux réglementations sont des éléments clés pour établir une relation de confiance entre les fournisseurs de sécurité et leurs clients. Il est noté que **6%** d'entre vous utilisent des solutions de nationalité israélienne et enfin **5%** d'entre elles proviennent d'autres pays.

Au-delà des enjeux de scalabilité, de conformité réglementaire et de proximité/disponibilité du support, il serait intéressant de s'interroger sur le facteur lié à la « qualité » (réelle ou supposée) des différentes solutions utilisées. Il s'agit d'un argument revenant souvent dans les discussions et idées reçues autour de ce sujet, sans qu'il soit néanmoins véritablement objectivé, selon le cabinet du Ministre délégué chargé du Numérique.

Agences de notation

Un autre sujet organisationnel a suscité les inquiétudes de la part du club : l'image de la notation financière et à l'heure où le fait cyber ne cesse de se développer, ***les pratiques de notation cyber*** (cyber rating) se développent que ce soit dans le cadre de contrats d'assurance, de contrats de sous-traitance ou tout simplement pour mesurer son niveau d'exposition publique. L'idée de cette question **[Q105]** était de savoir comment vous utilisiez ce type de service au sein de votre organisation. Vous avez été 179 à répondre à cette question de la semaine, **45%** d'entre vous n'utilisent pas les services des agences de notation et **7%** d'entre vous affirment avoir d'autres usages de ces services.

Le rôle des Agences de Notation Cyber

1. Évaluation de la posture de sécurité : les agences de notation cyber évaluent les pratiques de sécurité informatique d'une entreprise, en prenant en compte ses politiques, procédures, technologies et mesures de protection contre les Cybermenaces.

2. Mesure de l'exposition publique et préservation de l'image : ces agences évaluent également l'exposition publique d'une entreprise envers les risques de cyberattaques, notamment en évaluant la présence en ligne, les vulnérabilités potentielles et les fuites de données. **39%** d'entre vous utilisent ces services comme l'un des moyens de surveiller votre exposition publique et détecter vos défauts de sécurité pour y remédier au plus tôt et **34%** affirment utiliser ces services pour des questions d'image, de benchmark et de réputation de votre entreprise vis-à-vis de tiers.

3. Aide à la prise de décision : les notations cyber aident les entreprises à prendre des décisions éclairées concernant leur stratégie de sécurité, leurs investissements technologiques et leur choix de partenaires commerciaux. A cet effet, **17%** d'entre vous affirment utiliser ces services pour faire réagir les dirigeants de votre entreprise.

4. Sensibilisation et incitation à l'amélioration : les notations cyber peuvent aider à sensibiliser les entreprises sur l'importance de la sécurité informatique et les inciter à améliorer leur posture de sécurité pour protéger leurs données et leur réputation.

Impact sur les Contrats d'Assurance et de Sous-traitance

1. Assurance cyber : les agences de notation cyber peuvent jouer un rôle dans la tarification des polices d'assurance cyber, en fonction du niveau de sécurité et de résilience de l'entreprise évaluée. De ce fait, **23%** d'entre vous utilisent ces services dans le cadre de la négociation de votre police de cyber assurance.

2. Contrats de sous-traitance : dans le cadre de contrats de sous-traitance, les notations cyber peuvent être utilisées comme critère pour évaluer la capacité d'un fournisseur à protéger les données et les actifs de l'entreprise cliente (gestion des tiers / 3rd parties). Vous êtes 16% à utiliser ces services dans ce cadre.

3. Due diligence : les notations cyber sont devenues un élément clé de la due diligence pour les fusions et acquisitions, car elles aident à évaluer le niveau de risque associé à l'opération.

Conclusion

Les agences de notation par leur contribution à l'amélioration de la posture de sécurité, leur impact sur les contrats d'assurance et de sous-traitance, ainsi que leur rôle de sensibilisation et de mesure de l'exposition publique renforcent la résilience des entreprises face aux Cybermenaces.

Cependant, comme précisé dans le communiqué de presse du 19 juin 2023 (Les acteurs du cyber rating suscitent la controverse au sein du CESIN), « si le marché est en demande de visibilité, ces acteurs sont-ils en capacité de créditer les entreprises de manière impartiale ? Quelle fiabilité des méthodes d'évaluation, pour quels impacts sur les entreprises ? ». « Le CESIN suggère, afin d'éviter un certain nombre de dérives, la mise en œuvre d'un référentiel pour soutenir l'émergence de notations claires et transparentes, sur la base de méthodes et critères reflétant fidèlement et de façon reproductible le niveau de maturité des organisations. De sorte à garantir la compétence des analystes et l'application du principe d'amélioration de la cybersécurité en continue. Enfin, il suggère la mise en œuvre de normes et mesures standardisées, de manière à rationaliser la communication auprès des Comités Exécutifs et Conseils d'Administration, et en vue de favoriser le développement de sociétés de cyber rating en Europe. »

Relation avec vos tiers

La gestion des tiers, la question de la semaine **[Q106]** consistait à connaître quelles relations vous entretenez avec vos tiers essentiels. Vous avez été 158 répondants et **25%** d'entre vous avez affirmé ne rien faire de particulier avec vos tiers essentiels.

Les tiers essentiels sont des entités extérieures à votre organisation qui ont un impact critique sur votre entreprise. Ils peuvent être des fournisseurs, des sous-traitants, des partenaires commerciaux ou des prestataires de services essentiels. Dans une économie mondialisée et interconnectée, la plupart des entreprises dépendent de tiers pour une variété de services, allant de l'hébergement web à la logistique en passant par le traitement des paiements. Cette dépendance crée une toile complexe de relations qui peuvent représenter des vulnérabilités potentielles en matière de cybersécurité.

Quelques risques liés aux tiers essentiels

1. **Les failles de sécurité chez les tiers :** si un de vos fournisseurs subit une violation de sécurité, vos données et informations peuvent être exposées.
2. **La disponibilité des services :** si un fournisseur critique subit une panne due à une attaque, cela peut perturber vos opérations commerciales et donc votre business.
3. **Les pratiques de sécurité déficientes chez les tiers** : les pratiques de cybersécurité insuffisantes chez un tiers peuvent créer des vulnérabilités qui peuvent être exploitées pour cibler votre organisation.
4. **La confidentialité des données :** les tiers peuvent avoir accès à vos données sensibles. Vous devez vous assurer qu'ils les protègent de manière adéquate.

Renforcer la relation avec les tiers

Pour renforcer vos relations avec les tiers essentiels en matière de cybersécurité, voici quelques étapes clés à suivre :

1. **Évaluation des risques :** Identifiez les tiers qui ont accès à des informations sensibles ou qui ont un impact critique sur vos opérations. Évaluez les risques potentiels associés à chaque tiers, surtout quand ils sont identifiés comme tiers critiques ou essentiels pour l'organisation : 46% d'entre vous ont mis en place un PAS avec vos tiers essentiels et **37%** d'entre vous ont demandé à avoir un correspondant sécurité chez chacun de ses tiers essentiels.
2. **Normes de sécurité :** Établissez des normes, référentiels ou standards de sécurité claires que vous attendez de vos partenaires commerciaux. Assurez-vous qu'ils respectent ces normes.
3. **Audit de sécurité :** Réalisez régulièrement des audits de sécurité chez vos tiers essentiels pour vous assurer qu'ils sont conformes à vos normes de sécurité : **24%** d'entre vous effectuent des évaluations régulières (tests d'intrusions, audit SMSI, etc.) avec vos tiers essentiels.
4. **Formation et sensibilisation :** Fournissez une formation sur la cybersécurité à vos tiers essentiels pour les sensibiliser aux meilleures pratiques de sécurité.
5. **Plan d'intervention en cas d'incident :** Élaborez un plan d'intervention en cas d'incident de sécurité (pour éviter les attaques par rebond) qui inclut des dispositions pour les tiers essentiels : **34%** d'entre vous ont mis en place un processus de notification en cas d'incident de sécurité survenant chez le tiers
6. **Intégration des parties prenantes :** l'intégration des parties prenantes et des tiers essentiels dans une organisation est également gage de maturité cybersécurité : **23%** d'entre vous organisent un Comité Sécurité régulier avec vos tiers essentiels et **18%** d'entre vous ont mis en place un tableau d'indicateurs techniques avec vos tiers essentiels.

Conclusion

Les relations avec les tiers essentiels sont un maillon essentiel de votre posture en matière de cybersécurité. En travaillant en étroite collaboration avec vos partenaires commerciaux et fournisseurs pour renforcer la cybersécurité, vous réduirez les risques externes et renforcerez la protection de votre organisation dans un paysage numérique de plus en plus complexe et dangereux.

Être responsable cyber aujourd'hui

Enfin, pour mettre en lien avec un atelier de l'université d'Été 2023 sur la maturité du responsable Cyber, la question de la semaine sur ***le métier de responsable cyber*** aujourd'hui a permis de mettre en lumière votre regard sur ce métier **[Q108]**. Vous avez été 234 répondants.

Au fil du temps, le métier de RSSI a connu un changement et une évolution significative. Il requiert une combinaison unique de compétences techniques et de connaissances en gouvernance et conformité liées à la sécurité des systèmes d'information. Les RSSI jouent un rôle crucial dans la protection des données, la préservation de la confidentialité et la continuité des activités des organisations.

En synthèse, voici votre regard sur le métier, par ordre d'importance :

1. Une appétence particulière pour la gouvernance dans la protection des SI
2. Parce que c'est un métier de challenges et d'innovations constantes
3. Une appétence particulière pour l'aspect technique de la protection des SI
4. La possibilité de tisser des relations avec les métiers et les instances dirigeantes de votre organisation
5. Une filière transverse pour découvrir tout le spectre des SI dans une organisation
6. Parce qu'il y a une dimension motivante autour de la protection
7. Une opportunité qui s'est présentée à vous et vous avez pris goût à la matière
8. Parce que c'est un métier jeune, moderne et en devenir

L'évolution des risques

Les responsable Cyber doivent constamment s'adapter aux nouvelles menaces, mettre à jour leurs compétences techniques et développer leur compréhension de la gouvernance et de la conformité.

Les exemples d'attaques majeures, telles que les ransomwares ciblant des entreprises de toutes tailles, soulignent l'importance cruciale pour un responsable cyber d'être constamment vigilant, en sachant que l'utilisateur reste souvent malheureusement le dernier rempart lors de la défaillance voire l'absence de solutions cyber. Les cyberattaques peuvent avoir un impact dévastateur sur la réputation des entreprises, la confiance des clients et la santé financière.

Améliorer la posture cyber

En analysant les incidents passés et en tirant des enseignements des expériences, les responsables Cyber peuvent identifier les points faibles dans leurs défenses, les erreurs commises et les mesures efficaces prises pour contrer les attaques. Le partage d'informations sur les incidents est également crucial pour renforcer la collaboration entre les entreprises et les organisations, permettant ainsi une meilleure résilience face aux cybermenaces. Les conférences et les interviews sont de précieux moyens pour encourager ce partage d'informations.

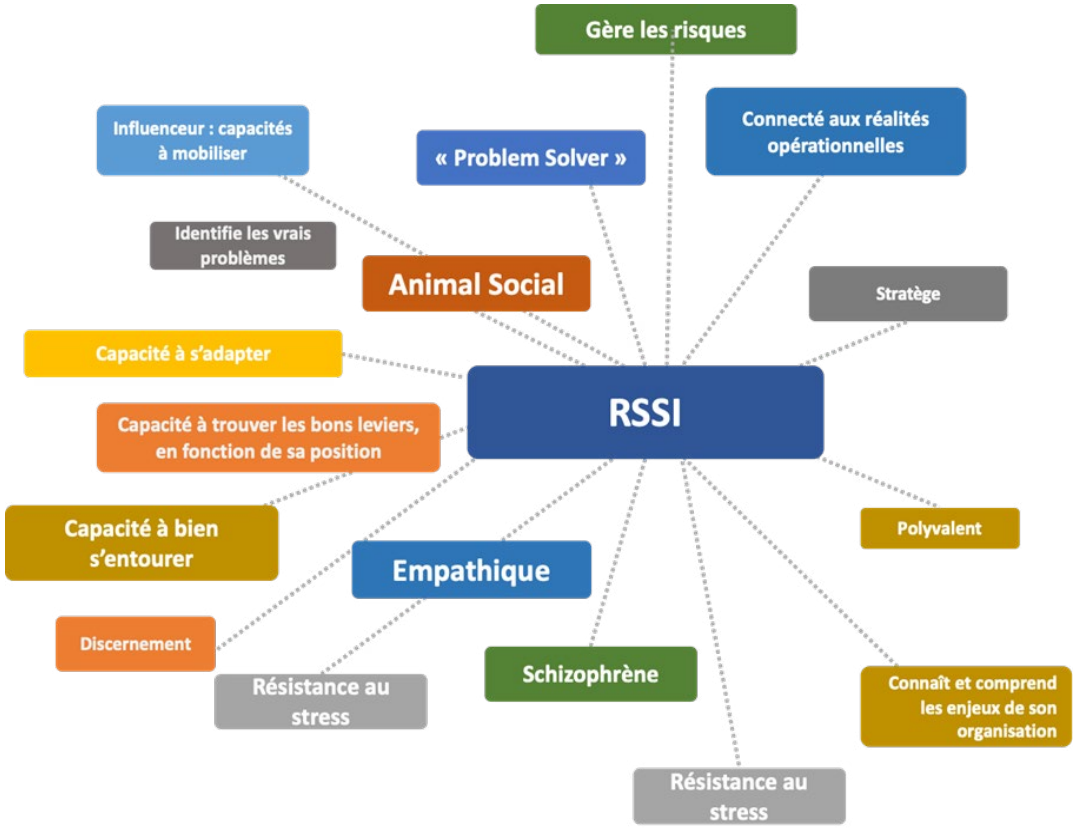
Les compétences essentielles pour un RSSI efficace

La responsabilité en matière de cybersécurité ne se limite plus à la sécurisation des composants informatique. Les responsables cyber encouragent désormais une culture de sécurité à tous les niveaux de l'entreprise, impliquant chaque employé. La sensibilisation à la cybersécurité est devenue un aspect fondamental pour renforcer la posture de sécurité globale de l'organisation. Des formations régulières et des simulations d'attaques aident les employés à reconnaître les tentatives de phishing et autres menaces, favorisant ainsi une meilleure compréhension des meilleures pratiques en matière de sécurité.

Outre la visibilité externe, la posture vis-à-vis de ses interlocuteurs et de son environnement, l'adéquation et l'efficacité du responsable Cyber dans sa structure et ses enjeux métiers, l'atelier de l'université d'été 2023 a proposé quelques critères clés à retenir pour évaluer la maturité d'un responsable Cyber, restant encore fonction des situations et des enjeux parmi :

- Capacité de séduction, de communication, de conviction, d'empathie et stratégie
- Un « animal social », « schizophrène »
- Lucide sur sa situation, ses besoins humains et choix de ses combats
- La maturité n'est pas liée à la séniorité
- La maturité VS compétence/légitimité
- Capacité à prendre de la hauteur

En résumé :



Les sujets innovants

ChatGPT

Face aux nombreuses actualités et aux besoins de sécurisation (nous parlons toujours de fondamentaux et de bonnes pratiques), les sujets innovants ont été un peu laissés de côté durant ce semestre. Cependant, le sujet ***ChatGPT (Generative Pre-trained Transformer)*** reste non seulement innovant et toujours d'actualité : certains de nos membres s'interrogent sur l'usage de ce dernier. C'est une innovation qu'il va falloir mieux comprendre dans ce qu'elle apporte en termes de valeur mais aussi de risques. Certains d'entre vous se sont peut-être déjà engagés sur le plan de la cyber en réaction à ces annonces. Dans la question concernant ce sujet **[Q103]**, vous avez été plus de 200 répondants mettant en lien l'importance et la prise en compte de ce sujet au sein de votre organisation et pour commencer, **56%** d'entre vous n'ont pris aucune mesure particulière quant à son utilisation et **12%** à l'avoir autorisé san autre questionnement.

Chat GPT est une technologie basée sur le modèle GPT-3.5, développée par OpenAI. Ce système de traitement du langage naturel présente des capacités avancées de génération de texte et d'interaction avec les utilisateurs. Bien que cette technologie offre de nombreuses opportunités pour améliorer l'efficacité et l'expérience utilisateur dans divers domaines, son utilisation soulève également des problématiques importantes en matière de sécurité, de confidentialité et de réglementation. De ce fait, **5%** d'entre vous affirment l'avoir interdit et contrôlé.

Quelles sont les problématiques liées à son utilisation ?

Le règlement prévoit d'encadrer des systèmes dits "à haut risque", tels que ChatGPT, ou sa nouvelle version encore plus performante GPT-4. Il est également question de modèles d'intelligence artificielle utilisés dans la reconnaissance faciale, ou encore dans les transports et l'éducation.

Afin de sécuriser au maximum leur usage, les intelligences artificielles devraient faire face à des essais préalables à leur mise sur le marché. L'Europe insiste sur le besoin d'identifier les potentiels risques d'un système et d'assurer une bonne gestion des données. (voir également l'article suivant : Intelligence artificielle: une règlementation fait son chemin, la CNIL mobilisée)

De nombreuses entreprises européennes dont (en France) Airbus, Dassault Systèmes, Orange et Renault craignent qu'un excès de réglementation sur l'IA ne fasse échouer les efforts visant à faire de l'Europe l'un des principaux acteurs de son développement. Et que cela leur demande aussi trop d'efforts et cela concerne 1% d'entre vous qui l'ont interdit sans avoir mis en place de contrôle.

Quelle est la réponse d'OpenAI ?

Le PDG d'OpenAI, Sam Altman, a annoncé qu'OpenAI pourrait cesser d'opérer dans l'Union européenne si elle n'arrive pas à se conformer à la nouvelle législation en préparation sur l'intelligence artificielle. Altman, qui effectue une tournée dans plusieurs pays européens, a mentionné qu'il a eu des discussions avec les régulateurs de l'UE concernant la loi sur l'IA, tout en critiquant la façon dont elle est actuellement rédigée.

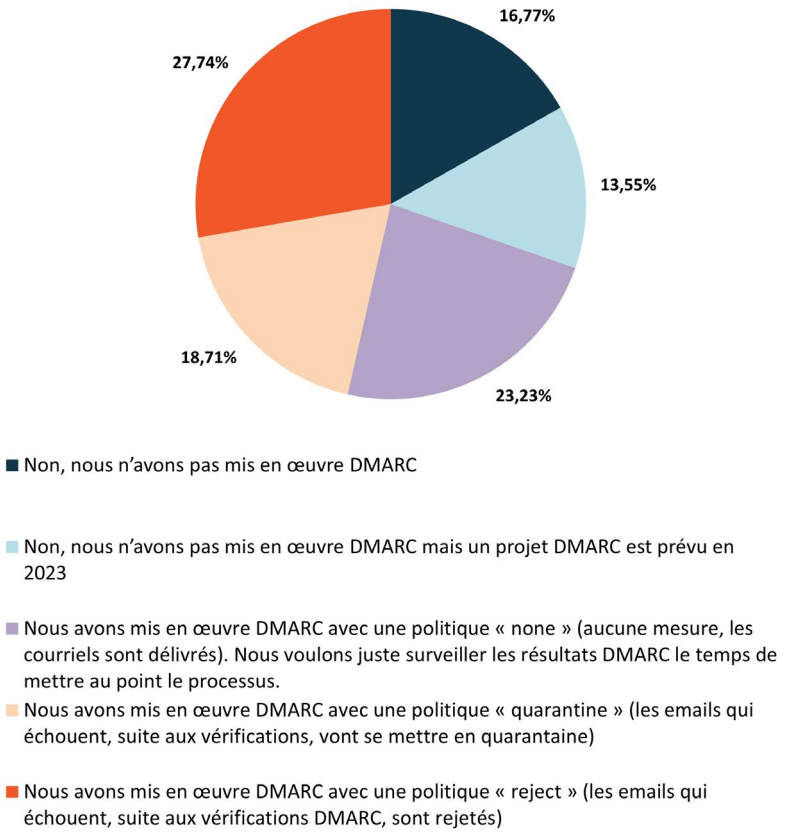
Conclusion

Les décideurs doivent être conscients des problématiques liées au biais, à la désinformation et à la confidentialité, tout en s'assurant de mettre en œuvre des politiques de sécurité et de protection des données appropriées. En respectant ces principes, Chat GPT peut être utilisé de manière bénéfique et responsable dans divers domaines, ouvrant ainsi la voie à de nouvelles opportunités dans le monde de l'intelligence artificielle et du traitement du langage naturel. C'est pourquoi, 25% des membres l'ont autorisé avec une recommandation de ne pas l'utiliser pour des sujets sensibles.

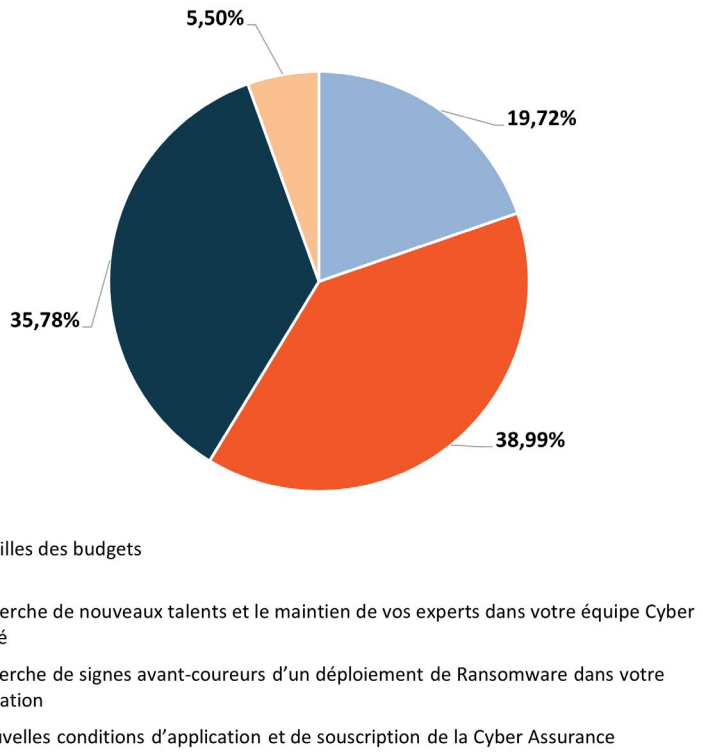
Annexes

Questions de la semaine : détails des résultats

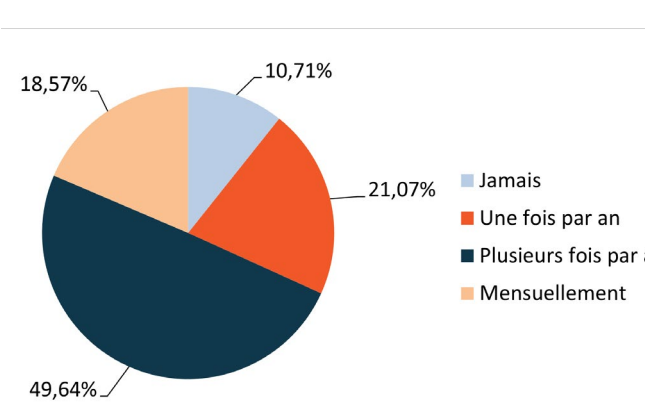
[Q94] DMARC - Avez-vous mis en place le DMARC au sein de votre organisation, et si oui en appliquant quelle politique au niveau de l'enregistrement DNS de vos noms de domaine ?

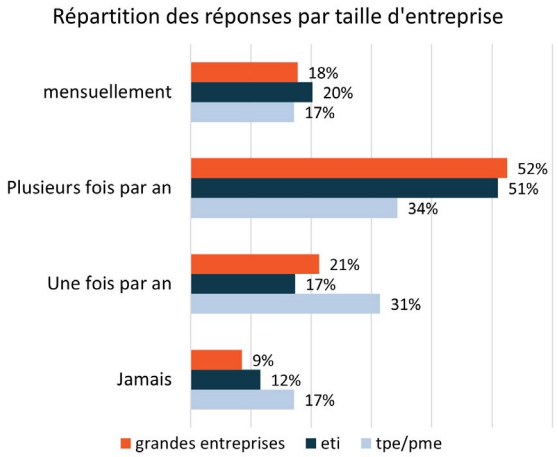


[Q95] Bilan 2022 - En bilan de cette année 2022, quelles ont été vos principales préoccupations durant l'année écoulée ?



[Q96] Sensibilisation : tests de faux phising - Faites-vous ce type de tests et si oui à quelle fréquence ?





Pour qu'une campagne d'hameçonnage soit efficace, elle doit :

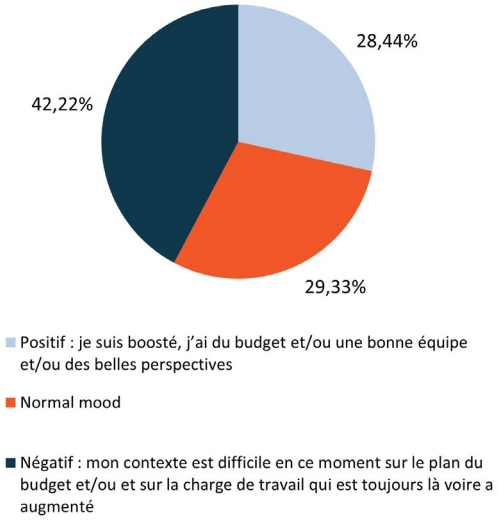
- apprendre à l'utilisateur à devenir vigilant et à prendre un rôle actif dans sa cybersécurité quotidienne ;
- être adaptée à chaque individu ou groupes d'individus et prendre en compte les différences d'apprentissage de chacun ;
- accompagner le collaborateur dans son développement de compétences face aux attaques par phishing, sans se contenter de souligner ses erreurs, ce qui serait peu constructif (non-stigmatisation et droit à l'erreur) ;
- favoriser l'autonomie de chacun ;
- être maintenue sur le long terme sans nécessiter d'intervention continue.

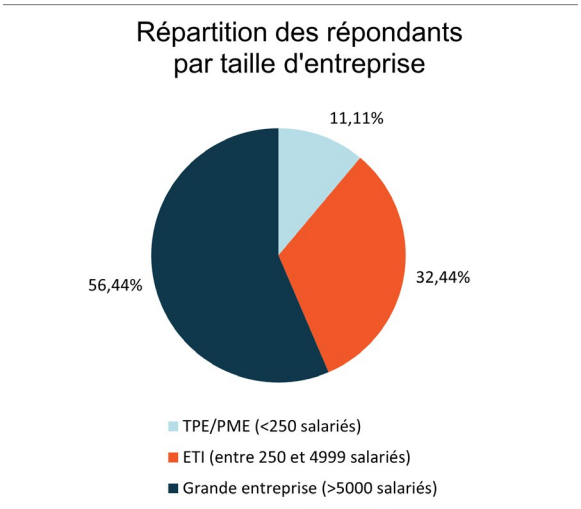
Outils (liste non exhaustive)

Quelques outils (classés de manière aléatoire) qui proposent de la sensibilisation et des simulations d'attaques de phishing : Proofpoint, KnowBe4, Sophos Phish Threat, Hoxhunt, Cyber Guru, TryRiot, Kamaé, NINJIO, SANS Security Awareness, Avant De Cliquer, etc.

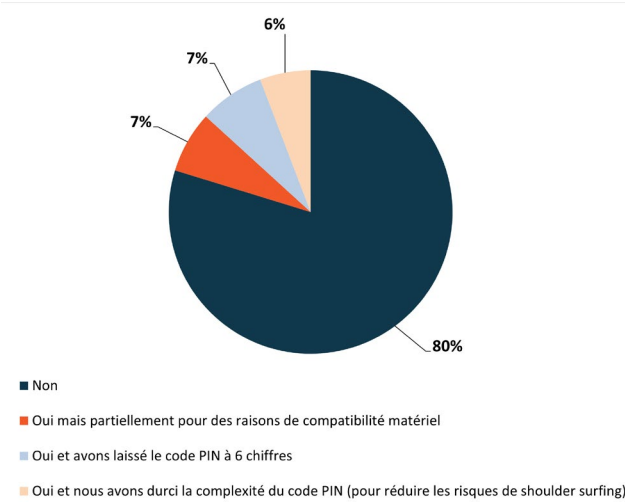
Source : Gartner Magic Quadrant for Security Awareness Computer-Based Training - July 2019

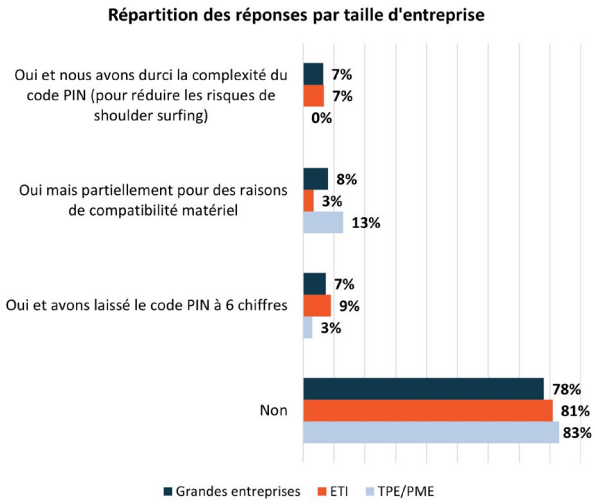
[Q97] État d'esprit du moment - Quel est votre état d'esprit du moment ?





[Q98] Windows Hello - Utilisez-vous Windows Hello?





Avantages

L'utilisation de Windows Hello offre plusieurs avantages pour les entreprises et les utilisateurs finaux. Elle simplifie le processus d'authentification en éliminant la nécessité de retenir et de saisir des mots de passe complexes. De plus, les méthodes biométriques offrent une expérience d'utilisation plus fluide et plus rapide, tout en réduisant les risques de vol de mots de passe ou d'accès non autorisés.

L'intérêt pour une entrepris' d'adopter Windows Hello réside principalement dans l'amélioration de la sécurité et de la convivialité d' l'authentification des utilisateurs. Voici quelques avantages spécifiques de sa mise en œuvre pour une organisation :

1. **Sécurité renforcée :** Windows Hello utilise des méthodes qui sont considérées comme plus sûres que les mots de passe traditionnels. Cela réduit les risques de piratage ou d'accès non autorisés aux appareils et aux comptes utilisateur.

2. **Simplification d' l'expérience utilisateur :** Avec Windows Hello, les employés n'ont plus besoin de se souvenir de mots de passe complexes et de les saisir à chaque fois. Ils peuvent simplement utiliser leurs caractéristiques biométriques pour s'authentifier rapidement et facilement, ce qui améliore l'expérience globale d' l'utilisateur.

3. Réduction des coûts liés à la gestion des mots de passe : Les mots de passe oubliés ou perdus peuvent entraîner des coûts significatifs en termes de support technique et de réinitialisation des comptes utilisateur. Avec Windows Hello, les entreprises peuvent réduire ces coûts en éliminant en grande partie la dépendance aux mots de passe.

Cependant, il existe également certains risques à prendre en compte lors du déploiement de Windows Hello :

1. Compatibilité matérielle : Windows Hello nécessite des appareils prenant en charge les fonctionnalités biométriques. Tous les appareils existants ne sont pas équipés de ces fonctionnalités, ce qui peut nécessiter des investissements supplémentaires pour mettre à niveau le matériel existant ou acheter de nouveaux appareils compatibles.

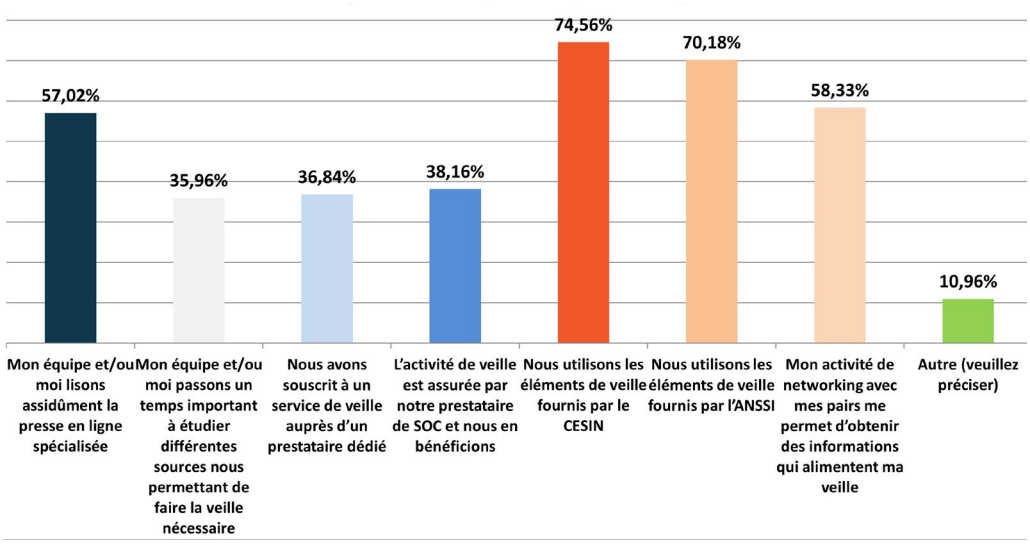
2. Vulnérabilités potentielles : Bien que les méthodes biométriques offrent une sécurité accrue par rapport aux mots de passe, elles ne sont pas infaillibles. Il est possible, bien que peu probable, que des attaquants puissent contourner ou falsifier les données biométriques pour accéder à un appareil ou à un compte. Les entreprises doivent prendre des mesures pour atténuer ces risques en appliquant des politiques de sécurité appropriées et en combinant Windows Hello ave' d'autres mesures de sécurité, telles qu' l'authentification à deux facteurs.

3. Stockage et protection des informations biométriques : Windows Hello propose deux options de stockage : en local su' l'appareil ou avec l'offre Entreprise, sur un serveur d'entreprise (au choix : site, hybride, cloud). Cette approche permet aux entreprises de mieux gérer (information centralisée, mesure de sécurité globale et contrôler l'authentification et la sécurité des données. Pour assurer la sécurité de ces informations, Windows Hello utilise une approche où une nouvelle paire de clés publique-privée est générée su' l'appareil. La clé privée est ensuite protégée par le TPM (Trusted Platform Module). Dans les cas où l'appareil ne possède pas de TPM, la clé privée est chiffrée et stockée dans le logiciel. La conformité au règlement « biométrie sur les lieux de travail » reflète la volonté de la CNIL d' s'assurer de la protection des données biométriques dans un contexte professionnel.

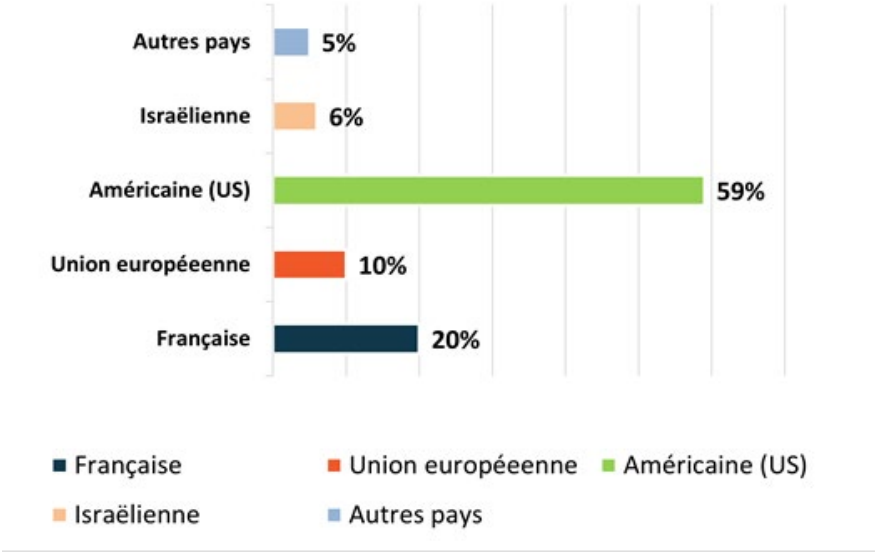
Déploiement et intégration

Le déploiement de Windows Hello peut varier en fonction de l'infrastructure informatique existante de l'entreprise. Dans certains cas, il peut nécessiter des mises à jour matérielles et logicielles pour prendre en charge les fonctionnalités biométriques et garantir la compatibilité avec les appareils utilisés. Cependant, Windows Hello est généralement conçu pour être facile à configurer et à déployer, notamment grâce à l'interface utilisateur intuitive de Windows 10.

[Q99] Veille - Quelle veille vous et votre étquipe pratiquez et comment ?



[Q100] Nationalité - Comment ventilez-vous vos solutions de sécurité selon leur nationalité?



Quelles sont les problématiques liées à la nationalité des solutions de sécurité ?

1. Accès aux données sensibles : si un fournisseur de sécurité est basé dans un pays donné, les lois et réglementations de ce pays peuvent lui permettre d'accéder aux données sensibles de ses clients, ce qui soulève des inquiétudes en matière de confidentialité et de protection des données.

2. Souveraineté nationale : les gouvernements peuvent être préoccupés par l'utilisation de solutions de sécurité fournies par des entreprises étrangères, craignant une perte de contrôle sur les infrastructures critiques et la sécurité nationale.

3. Risque de cyberespionnage : la nationalité d'un fournisseur peut être liée à des activités de cyberespionnage potentielles, ce qui accroît la méfiance envers les fournisseurs étrangers.

4. Dépendance technologique : les entreprises et les gouvernements peuvent être inquiets de devenir trop dépendants de fournisseurs étrangers pour leurs besoins en sécurité, ce qui pourrait les exposer à des risques géopolitiques ou économiques.

5. Conformité réglementaire : certaines réglementations ou politiques gouvernementales peuvent exiger l'utilisation de solutions de sécurité fournies par des entreprises nationales, ce qui peut compliquer les choix technologiques.

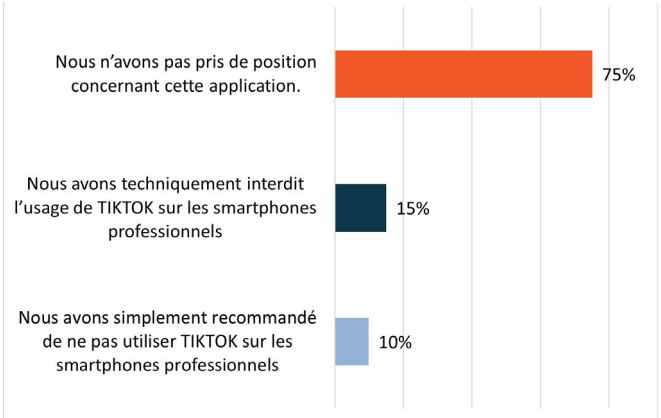
Implications sur la sécurité et la conformité

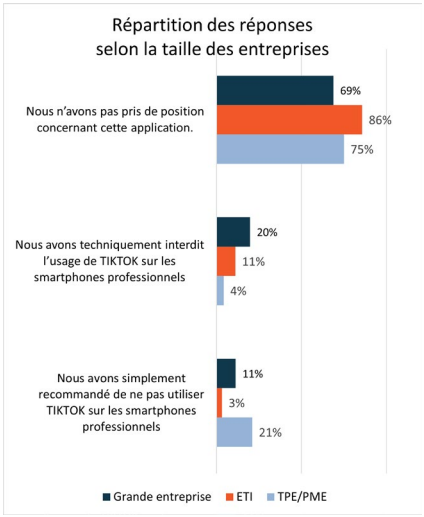
1. Confidentialité des données : la nationalité d'un fournisseur de sécurité peut impacter le niveau de confidentialité des données stockées et traitées par leurs solutions. Des évaluations de risques spécifiques sont nécessaires pour déterminer si les données peuvent être exposées à des acteurs non autorisés.

2. Localisation des données : certains pays imposent des restrictions sur la localisation géographique des données sensibles. Les solutions de sécurité doivent se conformer à ces exigences pour éviter les problèmes de conformité.

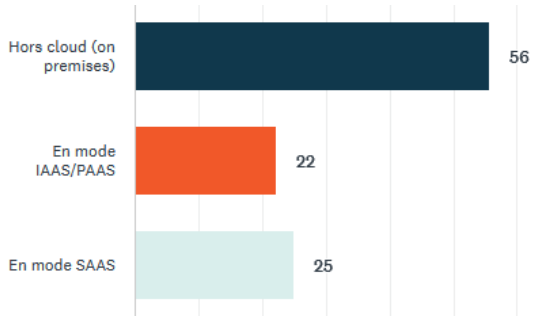
3. Audits de sécurité : les organisations doivent être en mesure de réaliser des audits indépendants des solutions de sécurité pour garantir leur fiabilité. La localisation du fournisseur peut influencer la facilité d'accès pour de tels audits.

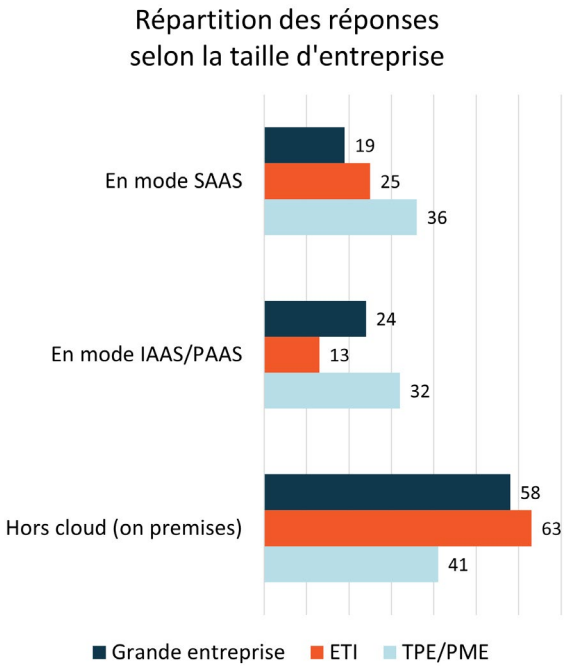
[Q101] Tiktok - Quelle posture avez-vous prise dans votre entreprise vis-à-vis de cette application?





[Q102] Cloud et répartition SI - Comment se répartit votre SI aujourd'hui (en poucentage)?





Évolutions du Cloud et usages

1. Adoption croissante du Cloud : le cloud est devenu incontournable pour les entreprises de toutes taill
L'adoption de services Cloud publics, privés ou hybrides continue de croître en raison des avantages
flexibilité, de réduction des coûts et de facilité de mise en œuvre.

2. Vers une approche multi-Cloud : les entreprises optent de plus en plus pour une approche mu
Cloud, en utilisant plusieurs fournisseurs Cloud pour diversifier les risques, éviter la dépendance à un s
fournisseur et optimiser la performance.

3**. Sécurité et confidentialité** : la sécurité des données dans le Cloud reste une préoccupation majeu
pour les entreprises. Les fournisseurs Cloud investissent massivement dans des mesures de sécur
avancées pour renforcer la confiance des utilisateurs.

4. Edge Computing : avec la croissance des dispositifs IoT (Internet of Things), le Edge Computing gag
en importance, amenant les ressources de calcul et de traitement plus près des sources de données,
qui a un impact sur la façon dont les services Cloud sont distribués.

5. Hybride et Multi-Cloud : les entreprises optent de plus en plus pour des environnements hybrid
combinant des solutions Cloud publiques et privées, ainsi que des déploiements multi-cloud pour évi
la dépendance à un seul fournisseur et améliorer la résilience.

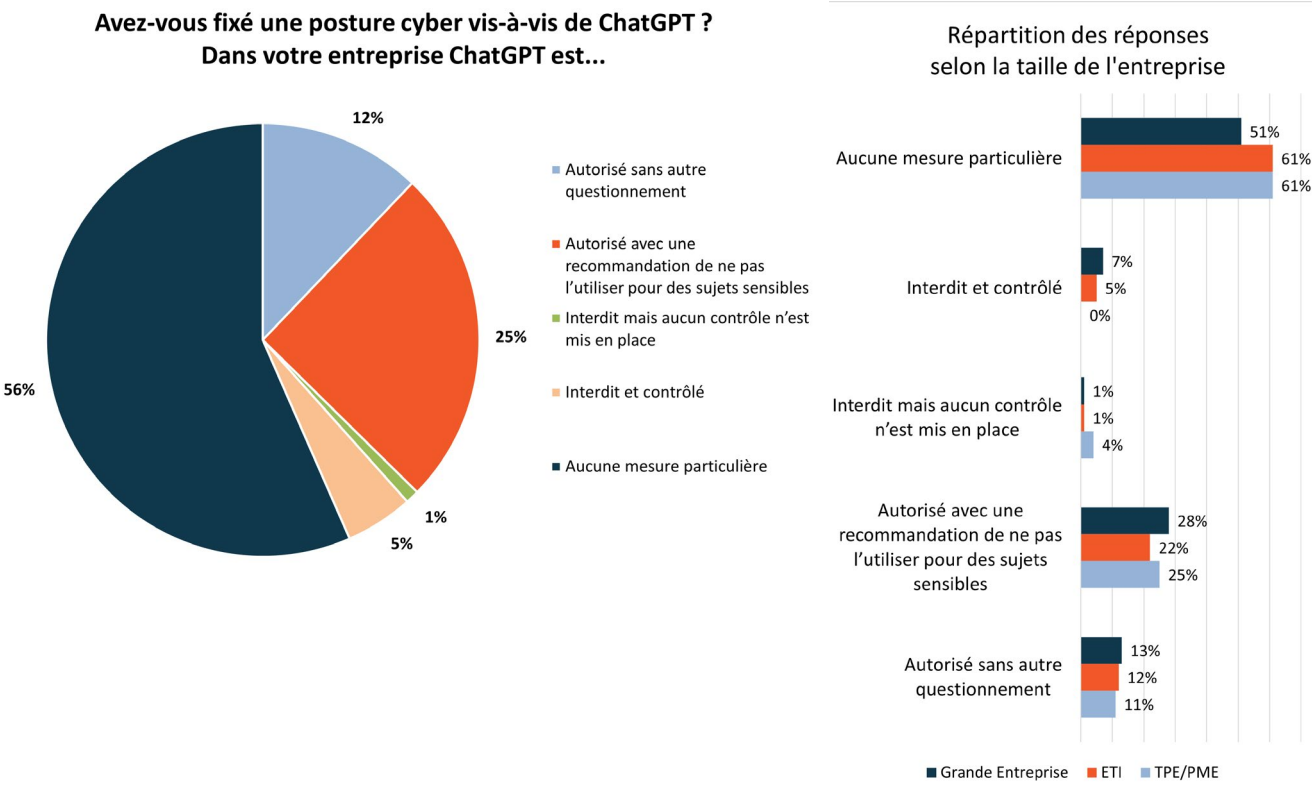
6. Serverless Computing : cette approche permet aux développeurs de se concentrer uniquement s
le code de l'application sans se soucier de la gestion de l'infrastructure sous-jacente. Les ressources so
allouées automatiquement en réponse aux demandes, ce qui permet de réduire les coûts et d'amélio
l'efficacité.

7. IA et Machine Learning intégrés : de nombreux fournisseurs de services Cloud intègrent désorm
des fonctionnalités d'intelligence artificielle (IA) et d'apprentissage automatique (Machine Learnir
dans leurs offres. Cela permet aux entreprises d'exploiter ces technologies sans avoir à gérer tou
l'infrastructure nécessaire.

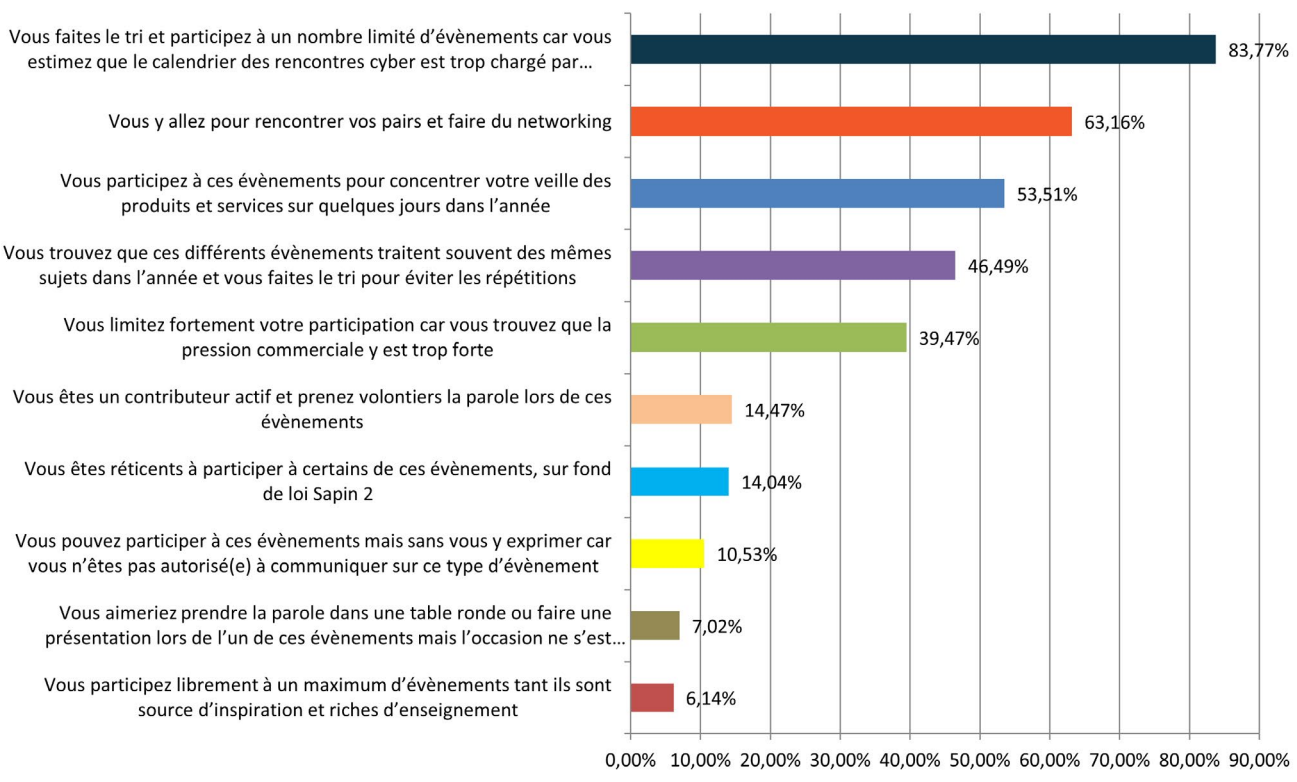
8. Containers et Kubernetes : L'utilisation de conteneurs et de plateformes d'orchestration comm
Kubernetes gagne en popularité pour faciliter le déploiement d'applications indépendamment
l'infrastructure sous-jacente.

L'évolution constante des modèles de Cloud Computing montre que les entreprises continuent d'explorer
d'adopter divers services Cloud pour répondre à leurs besoins spécifiques. Le choix entre SaaS, IaaS et Pa
dépend des exigences de l'entreprise en matière de fonctionnalité, de contrôle et de flexibilité. Les tendanc
émergentes telles que l'Edge Computing et l'adoption de conteneurs continueront de façonner la manièr
dont les services Cloud sont répartis et utilisés à l'avenir.

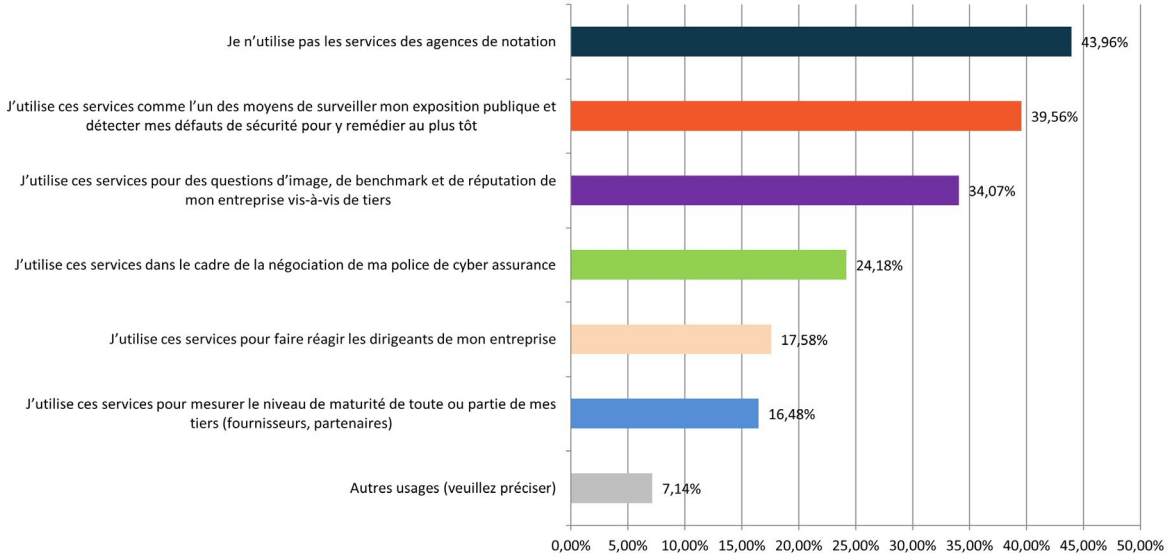
[Q103] ChatGPT - Avez-vous fixé une posture vis-à-vis de ChatGPT?



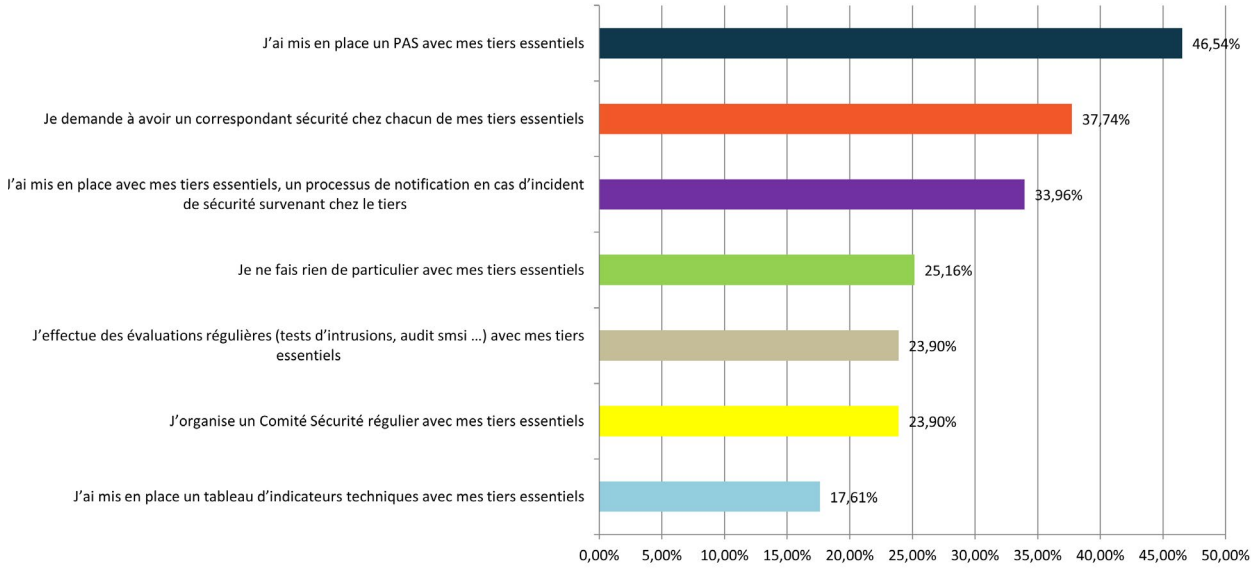
[Q104] Événements et réunions Cyber - Quelle est votre position vis-à-vis de ces événements, de façon générale ?



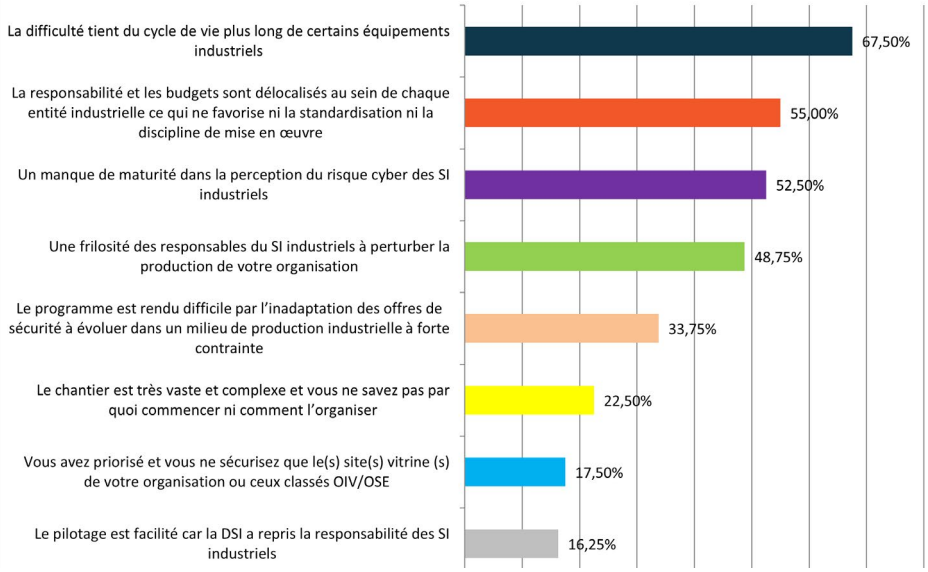
[Q105] Agences de notation - Comment utilisez-vous ce type de services ?



[Q106] Interactions avec vos tiers - Quelles relations entretenez-vous avec vos tiers essentiels?



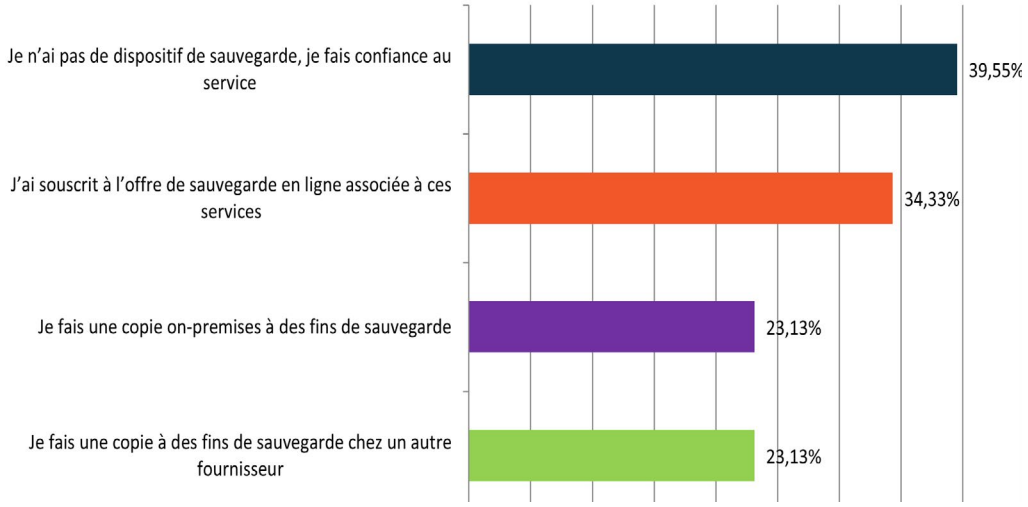
[Q107] Sécurisation des systèmes industriels - Quelles difficultés rencontrez-vous pour piloter la mise en oeuvre de votre programme de sécurisation des systèmes industriels ?



[Q108] Être responsable cyber aujourd'hui - Pour vous c'est…

1. Une appétence particulière pour la gouvernance dans la protection des SI;
2. Parce que c'est un métier de challenges et d'innovations constantes;
3. Une appétence particulière pour l'aspect technique de la protection des SI;
4. La possibilité de tisser des relations avec les métiers et les instances dirigeantes de votre organisation;
5. Une filière transverse pour découvrir tout le spectre des SI dans une organisation;
6. Parce q'uil y a une dimension motivante autour de la protection;
7. Une opportunité qui s'est présentée à vous et vous avez pris goût à la matière;
8. Parce que c'est un métier jeune, moderne et en devenir.

[Q109] Sauvegarde des données hébergées - Comment assurez-vous la sauvegarde des données hébergées et véhiculées par ces services ?



Pour aller plus loin, plusieurs aspects liés à la sécurité des données et la sauvegarde doivent être pris en compte :

- **Chiffrement des données :** toutes les données, qu'elles soient stockées ou en transit, doivent être chiffrées. L'absence de chiffrement des données expose à un risque potentiel de violation de données.

- **Authentification à multi-facteurs :** l'authentification à multi-facteurs est essentielle pour garantir la sécurité des données. Les mots de passe, même robustes, peuvent être vulnérables aux attaques de phishing, aux enregistreurs de frappe et aux logiciels malveillants. L'authentification à multi-facteurs bloque efficacement 99,9 % des violations.

- **Emplacement des centres de données (sauvegardes) :** l'emplacement physique des centres de données revêt une importance capitale pour la conformité. Les données sont soumises à la juridiction du pays où elles sont collectées ou traitées, et elles doivent y demeurer. Par exemple, le RGPD exige que les données des citoyens européens soient stockées dans l'UE ou dans un pays offrant un niveau de protection équivalent.

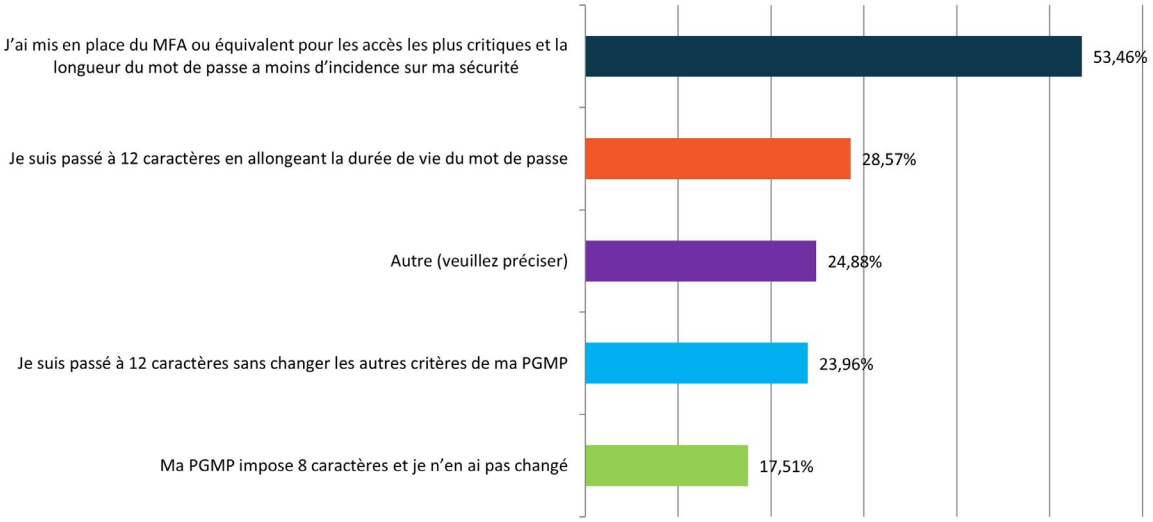
- **Connectivité, accès aux données et sécurité :** le choix de l'emplacement du centre de données peut influer sur la connectivité, la sécurité et la rapidité d'accès aux données. Les fournisseurs de services Cloud de l'UE doivent permettre aux utilisateurs d'accéder à leurs données ou de les

supprimer, ce qui nécessite de vérifier la facilité d'accessibilité des données.

▪ **Test de récupération et surveillance :** ma mise en place de procédures de test de récupération régulières est essentielle pour s'assurer que les données peuvent être restaurées efficacement en cas de besoin.

▪ **Sensibilisation des employés :** il est crucial de sensibiliser les employés à l'importance de la sauvegarde des données et de leur fournir des directives sur la gestion appropriée des données dans l'environnement SaaS. Il convient également d'établir des politiques de gestion du cycle de vie des données afin de déterminer la durée de conservation de certaines données et le moment opportun pour les supprimer en toute sécurité.

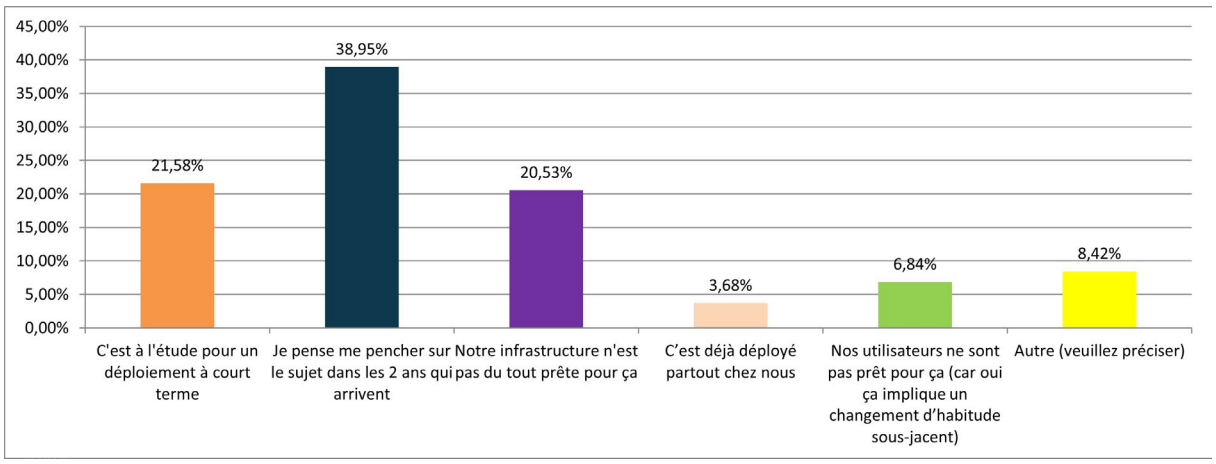
[Q110] Politique de Gestion des Mots de Passe (PGMP) - Entre l'ergonomie liée à l'habitude des utilisateurs de gérer des changements à 8 caractères et le renforcement de la sécurité, quel a été votre choix ?



Pour aller plus loin, la préservation de la confidentialité des mots de passe est un élément clé pour prévenir les cyberattaques. Suivez ces conseils pour une sécurité renforcée :

- Ne jamais partager vos mots de passe, même avec des personnes de confiance
- Éviter de faire appel à d'autres personnes pour générer vos mots de passe
- Changer immédiatement les mots de passe par défaut attribués par les systèmes
- Éviter toute communication de mots de passe par des moyens non sécurisés, comme l'e-mail ou le SMS.
- Ne pas enregistrer vos identifiants sur papier ou dans des fichiers numériques exposés.
- Opter pour des mots de passe différents pour chaque compte, minimisant ainsi les risques en cas de compromission.
- Implémenter la double authentification dès que possible pour une sécurité accrue.
- Utiliser des outils de gestion de mots de passe pour stocker et sécuriser vos informations sensibles (1password, Keepaas, etc.).

[Q111]Passwordless - Le passwordless est-il une solution à l'étude dans vos entreprises?



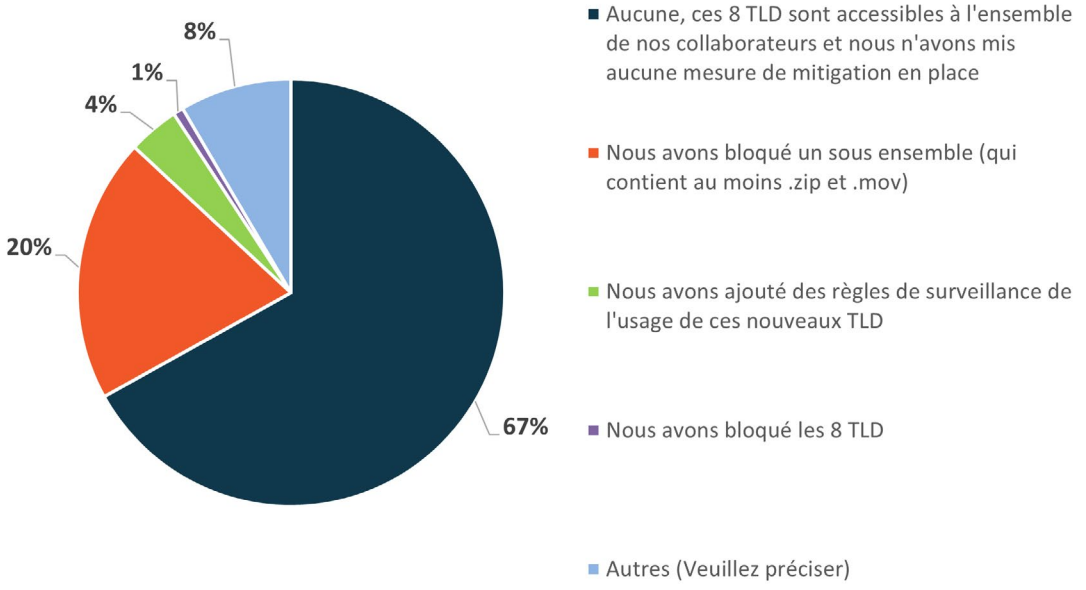
Pour aller plus loin, les méthodes d'authentification sans mot de passe peut être les suivantes :

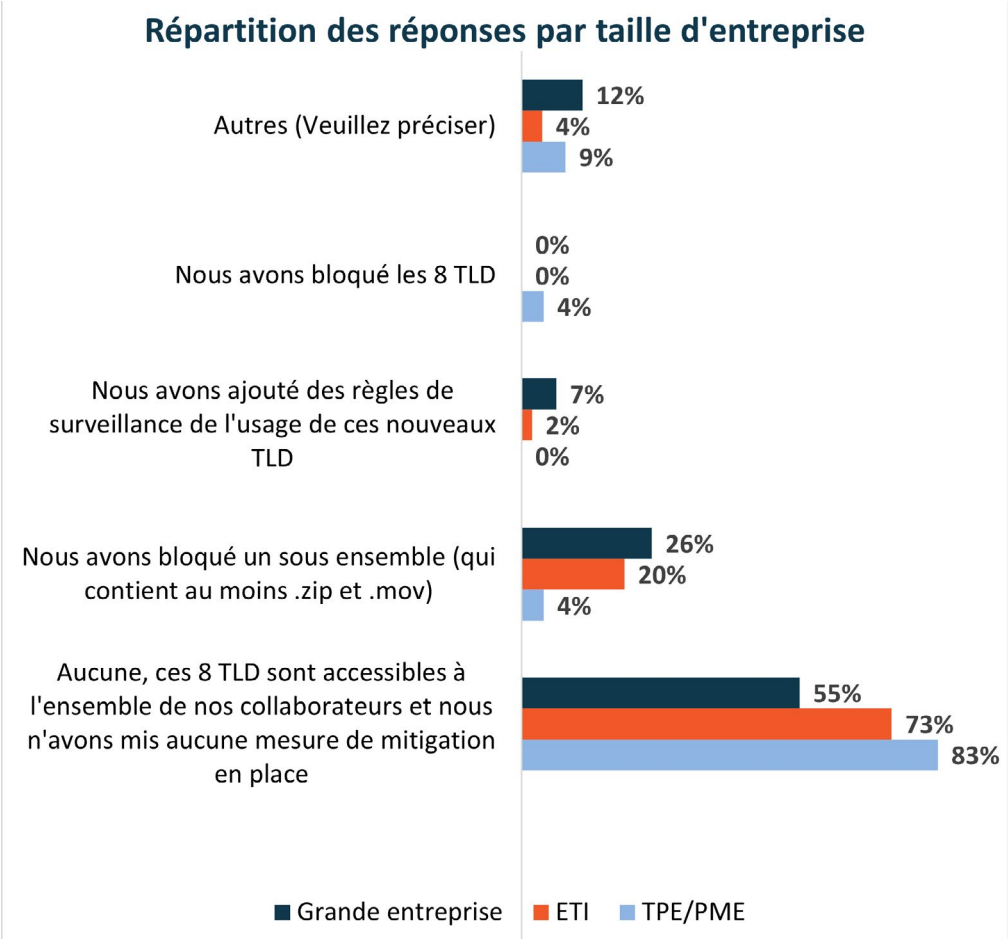
1. Biométrie : La biométrie permet d'authentifier les utilisateurs en se basant sur des caractéristiques physiques uniques, telles que les empreintes digitales, les iris ou les caractéristiques faciales. Ces informations biométriques sont utilisées pour vérifier l'identité de l'utilisateur, rendant les systèmes passwordless plus sécurisés et pratiques.

2. Clés de sécurité : Les clés de sécurité sont des appareils physiques qui se connectent aux ordinateurs ou aux appareils mobiles via USB, NFC ou Bluetooth. Ces clés génèrent des codes d'authentification uniques qui sont utilisés pour valides l'identité de l'utilisateur. Les clés de sécurité sont difficiles à pirater et offrent un niveau de sécurité élevé.

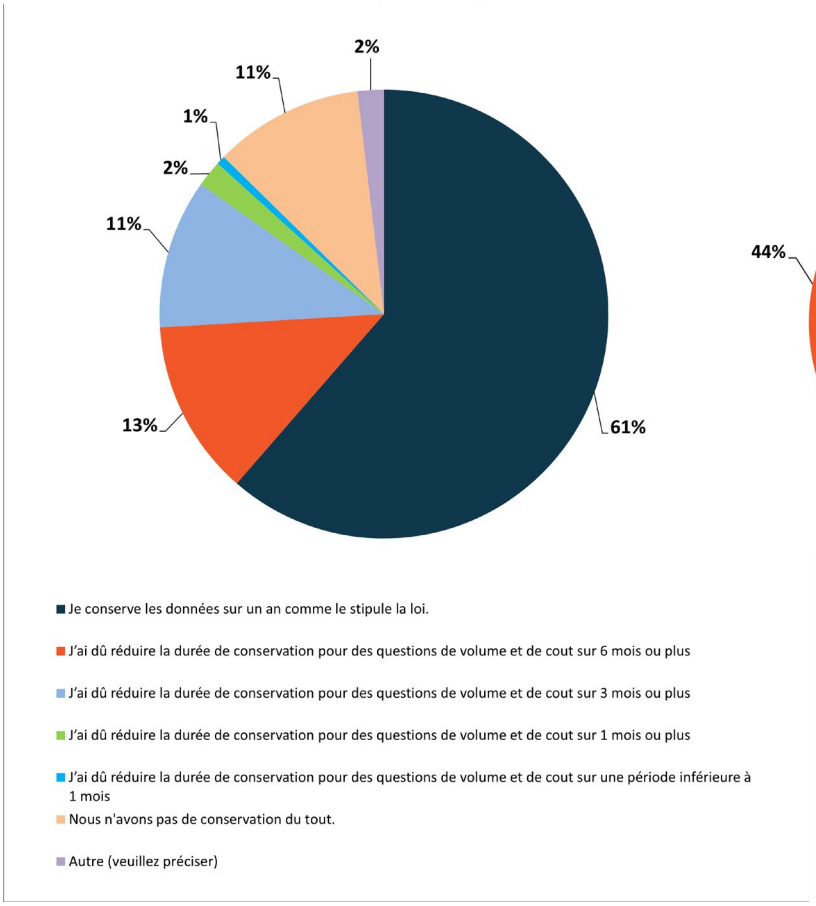
3. Codes à usage unique : Les codes à usage unique sont des combinaisons de chiffres générées dynamiquement et envoyées aux utilisateurs via des canaux sécurisés, tels que les applications mobiles ou les messages texte. Ces codes doivent être utilisés dans un délai limité pour s'authentifier sur un service en ligne. Cette méthode est largement utilisée dans les processus de double authentification (2FA) et offre une sécurité accrue par rapport aux mots de passe traditionnels.

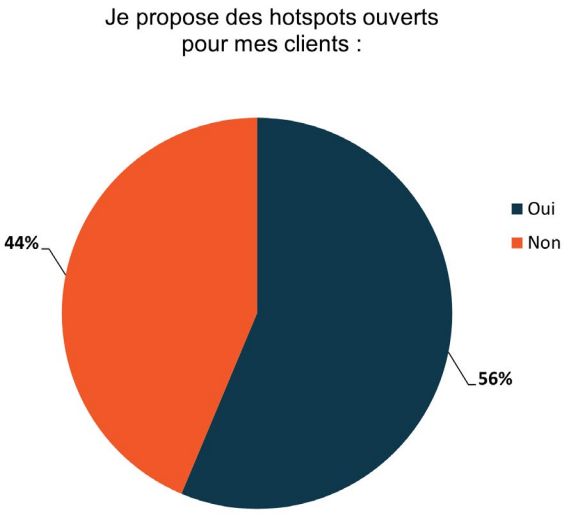
[Q112] Les racines de noms de domaine Google - Quelle mesure votre organisation a-t-elle prise ?



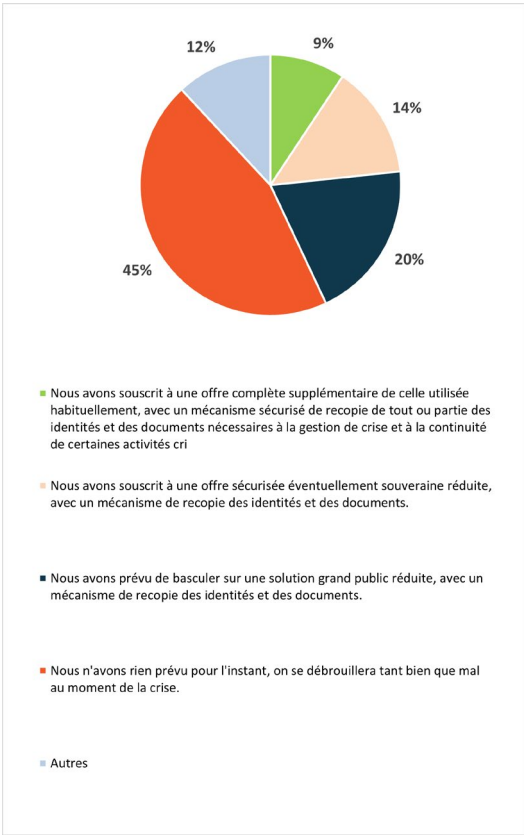


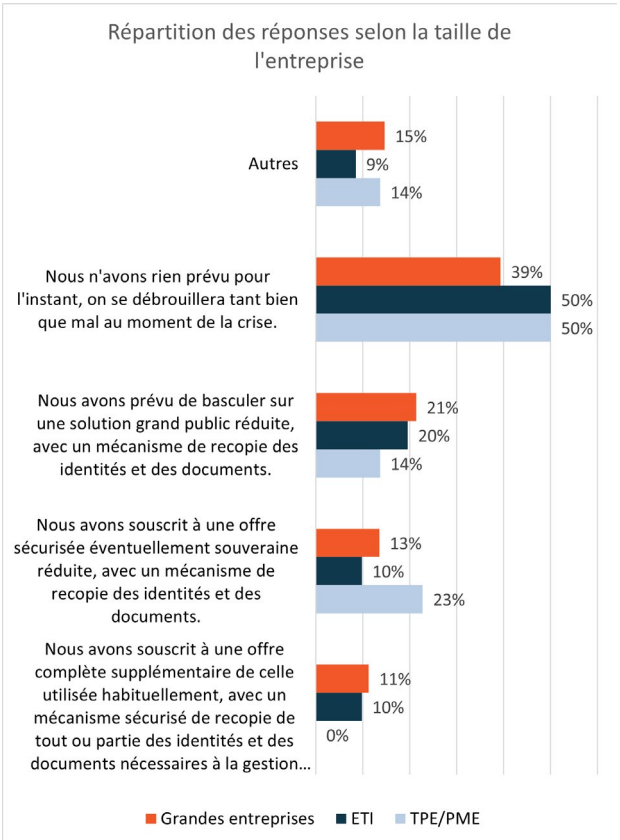
[Q113] Surf internet et conservation des données - Comment est traité ce sujet dans vos entreprises respectives ?





[Q114] Système de communication / Collaboration et crise cyber - Comment ce sujet est-il traité dans votre entreprise ?





Pour aller plus loin dans la gestion de crise cyber, une communication et une collaboration efficaces entre les parties prenantes internes et externes sont essentielles pour atténuer les conséquences de l'attaque et rétablir les opérations normales. Pour aider les organisations à faire face à ces situations critiques, l'ANSSI a émis des recommandations spécifiques concernant le système de communication et de collaboration lors d'une crise cyber, sans énoncer de produits ou de solutions de gestion de crise :

1. Mise en œuvre d'une cellule de crise cyber : regroupe des membres clés de différentes équipes opérationnelles de l'organisation, y compris les responsables de la sécurité informatique, des opérations, des communications, des ressources humaines et de la direction. Cette cellule doit assurer la coordination des actions, la prise de décision rapide et la communication efficace.

2. Rôles et Responsabilités définis : chaque membre de la Cellule de Crise Cyber doit avoir des rôles et des responsabilités clairement définis. L'ANSSI recommande d'identifier à l'avance les personnes qui seront impliquées dans la gestion de la crise et de leur attribuer des tâches spécifiques pour assurer une réponse rapide et coordonnée.

3. Communication interne : la communication interne est cruciale pour informer rapidement tous les employés de la situation en cours, des mesures prises pour atténuer l'incident et des actions à entreprendre. L'ANSSI recommande l'utilisation de canaux de communication internes sécurisés pour éviter la propagation de fausses informations et de directives contradictoires.

4. Communication externe : une communication transparente avec les parties prenantes externes est essentielle pour maintenir la confiance et minimiser les dommages à la réputation de l'organisation. La liste des contacts clés avec les autorités compétentes, les fournisseurs, les clients et les partenaires, afin de les informer rapidement en cas de crise cyber doit être établie.

5. Gestion des médias : désigner des porte-paroles officiels pour gérer les relations avec les médias et le public. Ces porte-paroles doivent être formés pour s'exprimer de manière cohérente, précise et rassurante tout en évitant de divulguer des informations sensibles qui pourraient être exploitées par les attaquants.

6. Réaliser des entraînements réguliers : pour garantir une réaction efficace lors d'une crise cyber, les organisations de réaliser régulièrement des exercices et des simulations de gestion de crise. Ces entraînements permettent aux membres de la Cellule de Crise Cyber de se familiariser avec les procédures et d'identifier les domaines d'amélioration.

La gestion d'une crise cyber exige une préparation minutieuse, une communication claire et une collaboration efficace entre les parties prenantes internes et externes, avec des outillages efficaces et faciles à mettre en œuvre. La veille constante et l'adaptation aux nouvelles menaces sont également essentielles pour maintenir une posture de sécurité solide face à l'évolution du paysage cybernétique.

CONTACT PRESSE

Véronique LOQUET
AL'X Communication
E-mail : vloquet(at)alx-communication.com
Téléphone : 06 68 42 79 68