Menaces informatiques et pratiques de sécurité en France

Édition 2016

- Les entreprises de plus de 200 salariés
- Les Collectivités Territoriales
- Les particuliers internautes

Club de la Sécurité de l'Information Français

Remerciements

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de cette étude, tout particulièrement :

Les responsables du groupe de travail

M. MOURER Lionel	ATEXIO	Responsable de l'étude et de la partie Entreprises
M. HENNIART Thierry	RÉGION HAUTS-DE-FRANCE	Responsable Collectivités Territoriales
M. FREYSSINET Éric	MINISTÈRE DE L'INTÉRIEUR	Responsable Internautes

Les membres du Comité d'Experts

M. ALEXANDRE Damien	SYNDICAT MIXTE SOLURIS
M. ARDOUIN Philippe	SYNDICAT DES EAUX DE CHARENTE MARITIME
M. BARRIAL Pierre	ACADÉMIE DE LILLE
M. BEELMEON Richard	ALTRAN
M. BLUM Patrick	ESSEC
M. BUSNEL Étienne	GIE INFO 2
Mme. BUTEL Annie	BNP PARIBAS F.D.G
M. CEVAËR Christian	CCI DE PARIS
M. DELPHIN Bruno	VEOLIA ENVIRONNEMENT
M. CHARBONNEAU François	ALTRAN TECHNOLOGIES
Mme. DIALLO Mariama	CONIX
M. FOUCAULT Jacques	CABINET DE CONSEIL JACQUES FOUCAULT
M. LIS Pierre-Marc	VILLE ET COMMUNAUTÉ D'AGGLOMÉRATION DE SAINTES
M. MARLIANGEAS Claude	VILLE DE CHATELAILLON-PLAGE
M. MINASSIAN Vazrik	ADENIUM SAS
M. MOISAN Noël	IT LINK
M. PAÏS Henri	ESI GROUP
M. REBILLARD Jean-Philippe	COMMUNAUTÉ D'AGGLOMÉRATION DE LA ROCHELLE
M. THIERRY Éric	MANUTAN
M. VERMOT Denis	COMMUNAUTÉ D'AGGLOMÉRATION DE LA ROCHELLE
M. VITU Jean-Christophe	CYBER ARK
M. WURSTHEISER Philippe	HUAWEI

Le CLUSIF remercie également vivement les représentants des entreprises et collectivités territoriales ainsi que les internautes qui ont bien voulu participer à cette enquête.

Enquête statistique réalisée pour le CLUSIF par le cabinet GMV Conseil et Survey Sampling International.

Avant-propos

Vous êtes en possession de l'édition 2016 de notre rapport MIPS (Menaces informatiques et pratiques de sécurité en France).

Si vous avez lu nos rapports précédents vous ne serez dépaysé ni par la forme, ni par une bonne partie de nos questions. Vous trouverez toujours une enquête exhaustive des menaces informatiques et pratiques de sécurité vues par les entreprises en France, les internautes de notre pays et, cette année, les collectivités territoriales - puisque comme vous le savez ou devez le savoir, l'enquête MIPS du Clusif alterne à chaque édition (c'est-à-dire chaque deux ans) entre collectivités territoriales et hôpitaux.

Cette édition est aussi le premier pas d'une stratégie d'évolution adoptée par le CA et le GT MIPS, dont l'objectif est d'adapter au mieux le contenu de cette enquête aux besoins de nos lecteurs, qu'ils soient professionnels de la SSI ou simples lecteurs concernés par le sujet.

Ce travail, incontournable dans un domaine où les menaces et les pratiques évoluent aussi rapidement, doit être mené par le Clusif avec beaucoup d'attention : il serait en effet irresponsable de notre part de tout bouleverser car cela impliquerait la perte d'éléments permettant de comparer les résultats obtenus d'une enquête à l'autre.

Nous avons donc décidé de conserver une grande partie de notre questionnaire et d'introduire les nouvelles problématiques par petites touches. Ainsi, nos expert (et vous, lecteur), détiendrons les éléments de comparaison nécessaires pour une mise en perspective de ces dernières.

Le second objectif, que nous essayerons de mettre en place lors des prochaines éditions, sera d'avoir des points de contact entre notre étude MIPS et notre Panorama de la Cybercriminalité, car ces deux initiatives ne sont finalement que deux photographies d'une même réalité : si MIPS permet de voir l'état de la SSI vu des menaces et des pratiques, le Panorama permet quant à lui de percevoir les « signaux fables » des menaces, celles qui font l'actualité mais qui, de manière générales, restent encore rares.

Enfin, si l'objectif de chaque initiative du CLUSIF (ouvrage ou conférence) est d'alimenter la réflexion autour de la SSI, l'étude MIPS reste de ce point de vue la plus aboutie de toutes : non seulement vous pouvez consulter les résultats des analyses réalisées par nos experts, mais vous avez également accès aux données de l'enquête afin de vous former votre propre opinion, fût-elle contraire à celle d'un des experts.

Alimenter la réflexion des professionnels de la Sécurité du Système d'Information est depuis toujours l'objectif majeur du CLUSIF. Ce rapport, en complémentarité avec notre Panorama de la Cybercriminalité, en est l'un des objectifs clefs.

Les tendances émergentes du Panorama deviennent ainsi, à court ou moyen terme, des tendances dans MIPS.

Finalement, et comme je l'ai promis en 2014, je réaffirme encore une fois notre vision de l'usage de ce rapport :

- Pour le Responsable ou Fonctionnaire de la Sécurité des Systèmes d'Information ou pour un chef d'entreprise, c'est le moyen de mettre en perspective sa propre politique de sécurité ou d'identifier les freins rencontrés par des entreprises tierces,
- Pour un Offreur de biens ou un Prestataire de services en Sécurité des Systèmes d'Information, c'est mieux apprécier la nature du marché, le déploiement des offres et/ou les attentes et besoins à combler,
- Pour nos services institutionnels et ceux en charge d'une mission de veille, qu'elle soit technique, réglementaire ou sociétale, c'est l'opportunité de détecter des phénomènes émergents ou représentatifs d'une volumétrie, voir sa contraposée si on considère par exemple la réticence toujours forte à évoquer les fraudes financières et les malveillances internes.

Je vous souhaite donc bonne lecture, et espère que les efforts que nous faisons et allons continuer à faire pour faire évoluer MIPS saurons vous satisfaire.

Et je vous souhaite bonnes lectures, au pluriel cette fois, puisque MIPS est un ouvrage de lecture, certes, mais surtout de consultation à chaque fois que vous devrez vous situer dans un domaine ou une problématique.

Lazaro Pejsachowicz
Président du CLUSIF

Synthèse de l'étude

Au travers de l'édition 2016 de son enquête sur les menaces informatiques et les pratiques de sécurité (MIPS), le CLUSIF réalise, comme tous les 2 ans, un bilan approfondi des usages en matière de sécurité de l'information en France.

Cette enquête se veut être une référence de par la taille et la représentativité des échantillons d'entreprises (334 ont répondu) et des collectivités territoriales (203 ont répondu) interrogés. Par ailleurs, elle se veut relativement exhaustive, en prenant, pour la première fois cette année, l'ensemble des 14 thèmes de la norme ISO 27002:2013, relative à la sécurité des Systèmes d'Information.

Enfin, cette année comme depuis 2008, l'étude reprend le volet très complet consacré aux pratiques des particuliers utilisateurs d'Internet à domicile (1 008 répondants), en constante évolution au regard des nouveaux usages.

Cette synthèse reprend l'une après l'autre chacune des thématiques abordées et en précise les tendances les plus remarquables.

Entreprises : les attaques sont toujours bien présentes, mais… où est la gestion des incidents de sécurité ?

Point positif : le nombre d'acteurs de la SSI au travers de la mise en place d'organisations et de structures évolue toujours positivement… Pour autant, la « maturité SSI » elle stagne, principalement du fait 1] du manque de budget attribué à la SSI (42% des répondants), et 2] des contraintes organisationnelles.

Côté budget, on constate une légère reprise, pondérée par le fait que le poste ayant eu la plus grosse augmentation, cette année encore, est la mise en place de solution, avec 31%. On reste toujours dans la technique : ainsi pour beaucoup la sécurité reste une histoire de mise en place de solution technique…

Après une stagnation depuis 2010, le nombre d'entreprises ayant formalisé leur PSI reprend la bonne pente à 69% (+ 5 points vs 2014). La DSI tient une part prépondérante dans la formalisation de la PSI (63% vs 54% en 2014), alors que le RSSI stagne (39% vs 38% en 2014).

La fonction de Responsable de la Sécurité des Systèmes d'Information (RSSI ou RSI) est de plus en plus clairement identifiée et attribuée au sein des entreprises (67%), soit + 181% en 8 ans ! En grande majorité, les RSSI sont rattachés à la DSI (42%), ce qui pose encore la question de son « pouvoir » d'arbitrage… Mais ne vaut mieux-t-il pas un RSSI mal rattaché que pas de RSSI du tout ? : la question est toujours ouverte…

Concernant les ressources humaines, les chartes sont maintenant bien déployées et la sensibilisation de subit pas de grand mouvement en dehors de celle des VIP en net recul (elle passe de 31% en 2014 à 20% en 2016 : la fin de l'effet Prism ?…).

Point négatif : 47% des entreprises déclarent encore n'avoir pas classifiées leurs informations sensibles et seules 50% réalisent des analyses de risques sur tout ou partie de leur SI !

La cryptographie est encore peu utilisée (34% en font l'usage) et lorsqu'elle l'est, c'est la DSI qui en a largement le contrôle (76%).

Du côté des technologies de protection, certains outils commencent à être un peu plus généralisés. Par exemple : le chiffrement sur PC portables passe de 33% en 2014 à 43% en 2016, les IPS et IDS passent respectivement à 53% et 64% (vs 40% et 49% en 2014).

La formalisation des procédures opérationnelles de déploiement des correctifs de sécurité (patch management) est, en 2016, en régression (59% vs 65% en 2014).

Les PDA, tablettes et smartphones fournis par l'entreprise connaissent encore une augmentation de leur usage (27% ne les autorisent pas vs 34% en 2014). Et l'usage des équipements personnels (BYOD – *Bring Your Own Device*) recule encore pour arriver 71% d'interdiction (66% en 2014 et 38% en 2012) !…

La sécurité dans le cycle de développement régresse et de fait reste toujours trop insuffisante (prise en compte à 17%, - 7 points vs 2014) !… Pourtant, il n'est plus à démontrer que nombreux sont les piratages qui utilisent des failles applicatives liées au développement (injection, XSS, etc.).

44% des entreprises ont placé leur SI en tout ou partie sous infogérance (7% en totalité, - 2 points vs 2014) et quand c'est le cas, 30% ne mettent pas en place d'indicateurs de sécurité et 40% ne réalisent aucun audit sur cette infogérance !… Après une augmentation vertigineuse entre 2012 et 2014 (+24 points) ; l'utilisation du Cloud augmente encore un peu cette année (+ 4 points à 42%), même s'il représente que 42% des entreprises.

Ces deux dernières années marquent un retour des incidents « logiques » par malveillance : infections par virus (en tête avec 44%, + 14 points), fraudes informatiques et télécoms (11%), chantage ou extorsion informatique (11%), attaques logiques ciblées (7%)… Malgré cela, 49% des entreprises ne disposent toujours pas d'une cellule de collecte et de traitement des incidents de sécurité de l'information…

Près d'un tiers (30%) des entreprises ne prennent pas en compte la continuité d'activité… Sans surprise, l'indisponibilité des 'systèmes informatiques de gestion' représente le scénario le plus couvert (58%). Le BIA (Bilan d'Impact sur l'Activité), prenant en compte les attentes des « métiers » régresse légèrement (51%, - 4 points vs 2014). Et pour ceux qui en dispose, 25% des plans « utilisateurs » et 23% des plans « IT » ne sont jamais testés : alors, sont-ils réellement efficients ?…

Le RSSI n'intervient que pour 11% dans les déclarations « CNIL », en 5ème position après le Service Juridique (15%), le Service RH (17%), le CIL (19%) et le DSI (26%).

Sur une période de deux ans, 68% (- 3 point vs 2014) des entreprises interrogées ont réalisé au moins un audit ou contrôle de sécurité du Système d'Information. Ces audits sont motivés principalement par le respect de la PSSI (57%), des exigences contractuelles ou règlementaires (35%) ou des exigences externes, comme les assurances ou les clients (29%).

Enfin, les tableaux de bord de la sécurité de l'information (TBSSI) stagnent, restant à 25% ! Pourtant, le TBSSI reste un moyen simple et efficace, pour autant que l'on ait choisi les bons indicateurs, de 'piloter' la sécurité de l'information au sein de son entreprise…

Au final, bien que le nombre de RSSI croisse (ce qui est bien), la maturité des entreprises stagne (ce qui l'est moins)…

Les Collectivités Territoriales au tournant de la numérisation de la relation « citoyen ». Des efforts à maintenir pour assurer la sécurité de leur système d'information et des informations qui leur sont confiées…

En 4 ans, l'écosystème des Collectivités Territoriales a évolué : renforcement des intercommunalités dans des agglomérations de 20 000 habitants *minimum*, multiplication des services dématérialisés à la population ou entre entités publiques, cadre budgétaire de plus en plus contraignant…

Les Collectivités Territoriales perçoivent nettement que leurs activités ont une dépendance croissante vis-à-vis de l'informatique et du numérique, +10% en 4 ans.

L'étude montre que la sécurité du système d'information est efficiente dès lors que les moyens organisationnels, humains et financiers sont clairement attribués et que la politique de sécurité est portée par les instances dirigeantes.

Près de 50% des Collectivités Territoriales interrogées se plaignent d'un manque cruel de personnel qualifié susceptible d'intégrer la fonction publique territoriale. Le recours à de la prestation externe se heurte au manque de moyen financier.

Cette année encore, l'étude montre une grand disparité des moyens et des pratiques de sécurité, avec en queue de peloton, les Communautés de Communes qui n'ont pas, malgré la réforme territoriale, atteint la taille critique et le niveau de maturité pour s'investir dans la sécurité de leurs systèmes d'information.

Les investissements dans la sécurité physique et logique portent leurs fruits : nous notons un taux moyen de 30% des contrôles d'accès physique par badge (plus de 70% pour les « grandes » Collectivités), une augmentation significative de l'authentification par certificat électronique sur support matériel (+57%) et une industrialisation de la gestion des droits d'accès (+20% pour les modèles par habilitations).

Les Collectivités sont confrontées aux mêmes menaces que les Entreprises, les infections virales reprenant la tête du hitparade.

L'entrée en vigueur de la réforme SVA/SVE : « Silence Vaut Acceptation » exigeant des Collectivités qu'elles répondent sous deux mois aux « Saisines par Voies Electronique », impactera sans nul doute les exigences

de disponibilité et d'intégrité des systèmes d'information. Pour éviter les risques de contentieux, les directions informatiques devront, dans les mois et les années à venir, mettre en œuvre de nouveaux moyens et de nouvelles pratiques de sécurité.

En période de restriction budgétaire, les arbitrages nécessiteront de prendre en compte ces éléments et allouer une part plus grande à la sécurité !

Internautes plutôt en sécurité, mais encore mal à l'aise avec certains outils

L'échantillon d'internautes consulté est constitué de façon à être représentatif de la population française. L'accès à Internet se fait de plus en plus sur des terminaux mobiles et les connexions Wifi sont toujours en progrès (utilisées par 85% des personnes interrogées). Sur le plan des usages, l'économie collaborative intéresse de plus en plus d'internautes (16%), tandis que l'on note un léger tassement (– 2 points) de l'utilisation des moyens personnels dans un cadre professionnel (ou même – 4 points pour ce qui est de l'usage d'équipements professionnels dans un cadre personnel).

Dans ce contexte, les internautes se sentent globalement en sécurité sur Internet, et ce dans des proportions stables par rapport à 2014. C'est manifestement lié à une appréhension plus aigüe des risques, certainement parce qu'ils s'informent beaucoup et qu'ils maîtrisent de mieux en mieux les outils et les comportements de sécurité en ligne. Toutefois, la variété des pratiques et des outils de sécurité à mettre en œuvre les mettent parfois en difficulté.

Il faut souligner que l'augmentation des menaces sur les systèmes mobiles est nettement perçue par les utilisateurs, leur confiance ayant baissé.

Enfin, l'appréhension des nouveaux outils de sécurité ou de nouveaux comportements de sécurité peuvent varier en particulier en fonction des tranches d'âge. Il paraît donc important que l'ergonomie de ces outils (tels que les logiciels et systèmes de gestion de mots de passe) s'adapte à tous les types d'utilisateurs et que l'offre d'outils de sécurité pour les terminaux mobiles se développe.

Pour conclure…

La menace est toujours bien présente et notre enquête montre de nouveau que les malveillances et les incidents de sécurité ne faiblissent pas !

Le temps des politiques de sécurité « parapluie », que l'on formalise pour se donner bonne conscience, est globalement terminé. Il n'en reste pas moins que les organisations doivent encore (et toujours) évoluer pour atteindre un niveau de maturité suffisant en matière de sécurité de l'information. Il y va de leur survie, au regard des enjeux qu'elles portent et des données dont elles ont la responsabilité…

Alors, « au travail » et n'oublions pas « Si vous pensez que seule la technologie peut résoudre vos problèmes de sécurité, alors vous n'avez rien compris à la technologie, ni à vos problèmes…[1]. » !

Pour les plus courageux d'entre vous, l'étude détaillée et argumentée vous attend dans le reste de ce document…

Bonne lecture !

Lionel MOURER

Pour le Groupe de Travail « Enquête sur les menaces informatiques et les pratiques de sécurité »

[1] Bruce SCHNEIER (1963 -).

Sommaire

Liste des figures

Méthodologie

L'enquête du CLUSIF sur les menaces informatiques et les pratiques de sécurité en France en 2016 a été réalisée de début janvier à mi-mars 2016, en collaboration avec le cabinet spécialisé GMV Conseil, sur la base de questionnaires d'enquête élaborés par le CLUSIF. Trois cibles ont été retenues pour cette enquête :

- les entreprises de plus de 200 salariés : 334 entreprises de cette catégorie ont répondu à cette enquête,
- les collectivités territoriales : 203 d'entre eux ont accepté de répondre,
- les particuliers internautes (de 15 ans et plus) : 1008 personnes, issues du panel d'internautes de l'institut spécialisé Lightspeed GMI, ont répondu à cette enquête via Internet.

Pour les deux premières cibles, le questionnaire utilisé a été construit en reprenant les thèmes de la norme ISO 27002 :2013 décrivant les différents items à couvrir dans le domaine de la sécurité de l'information. L'objectif était de mesurer de manière assez complète le niveau actuel d'implémentation des meilleures pratiques de ce domaine. Ces différents thèmes, numérotés dans la norme de 5 à 18, sont les suivants :

- thème 5 : Politique de sécurité de l'information,
- thème 6 : Organisation de la sécurité de l'information,
- thème 7 : Sécurité des ressources humaines,
- thème 8 : Gestion des actifs,
- thème 9 : Contrôle d'accès,
- thème 10 : Cryptographie,
- thème 11 : Sécurité physique et environnementale,
- thème 12 : Sécurité liée à l'exploitation,
- thème 13 : Sécurité des communications,
- thème 14 : Acquisition, développement et maintenance des Systèmes d'Information,
- thème 15 : Relations avec les fournisseurs,
- thème 16 : Gestion des incidents liés à la sécurité de l'information,
- thème 17 : Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité,
- thème 18 : Conformité.

Pour ce qui concerne les particuliers internautes, les thèmes suivants ont été abordés :

- caractérisation socioprofessionnelle des personnes interrogées et identification de leurs outils informatiques (ordinateurs et smartphones),
- usages de l'informatique et d'Internet à domicile,
- perception de la menace informatique, sensibilité aux risques et à la sécurité, incidents rencontrés,
- pratiques de sécurité mises œuvre (moyens et comportement).

Les réponses aux questions ont été consolidées par GMV Conseil en préservant un total anonymat des informations, puis ont été analysées par un groupe d'experts du CLUSIF, spécialistes du domaine de la sécurité de l'information.

Afin de simplifier la compréhension du document, le choix a été fait de ne citer que les années de publication des rapports, à savoir 2016, 2014, 2012, 2010 et 2008. Les enquêtes ont été réalisées sur le premier trimestre de l'année de publication et les chiffres cités portent donc sur l'année précédente, respectivement 2015, 2013, 2011, 2009 et 2007.

Enfin, le groupe d'experts tient également à préciser que toute enquête de ce type contient nécessairement des réponses discordantes dues à la subjectivité de l'observation sur des domaines difficilement quantifiables ou, dans le cas du domaine spécifique de la sécurité du SI, de la « culture » et de la maturité de chaque entreprise, collectivité publique ou internaute.

Entreprises

- Présentation de l'échantillon
- Dépendance à l'informatique des entreprises de plus de 200 salariés
- Moyens consacrés à la sécurité de l'information par les entreprises
- Thème 5 : Politique de sécurité de l'information
- Thème 6 : Organisation de la sécurité de l'information
- Thème 7 : Sécurité des ressources humaines
- Thème 8 : Gestion des actifs
- Thème 9 : Contrôle d'accès
- Thème 10 : Cryptographie
- Thème 11 : Sécurité physique et environnementale
- Thème 12 : Sécurité liée à l'exploitation
- Thème 13 : Sécurité des communications
- Thème 14 : Acquisition, développement et maintenance des Systèmes d'Information
- Thème 15 : Relations avec les fournisseurs
- Thème 16 : Gestion des incidents liés à la sécurité de l'information
- Thème 17 : Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité
- Thème 18 : Conformité

Les Entreprises

Présentation de l'échantillon

Pour l'édition 2016 de son enquête, le CLUSIF a conservé les types d'entreprises tels qu'en 2014 afin de pouvoir comparer les progrès ou les éventuelles régressions. Ainsi, la cible est constituée des entreprises de plus de 200 salariés des secteurs d'activité suivants :

- Banque – Assurances,
- Commerce,
- Industrie - BTP,
- Services,
- Transport – Télécoms.

334 entreprises ont répondu à la sollicitation du CLUSIF (entretien de 27 minutes en moyenne), avec un taux d'acceptation d'environ 8% (- 2 points par rapport à 2014) : sur 100 entreprises contactées, seulement 8 ont accepté de répondre à nos questions, ce qui a impliqué d'appeler plus de 4 000 personnes !

L'échantillon est construit selon la méthode des quotas avec 2 critères – l'effectif et le secteur d'activité des entreprises – pour obtenir les résultats les plus représentatifs de la population des entreprises.

Cet échantillon est ensuite redressé sur le secteur d'activité et les tranches d'effectif pour se rapprocher de la réalité des entreprises françaises, sur la base des données INSEE.

Entreprise Taille / Secteur	200-499 salariés	500-999 salariés	1 000 et plus	Total	Total en %		Données INSEE
Banque - Assurance	13	5	6	**24**	**7,2%**	→	**6,7%**
Commerce	21	3	5	**29**	**8,7%**	→	**19,6%**
Industrie - BTP	115	37	14	**166**	**49,7%**	→	**37,8%**
Services	55	16	11	**82**	**24,6%**	→	**22,1%**
Transport – Télécoms	19	8	6	**33**	**9,9%**	→	**13,8%**
Total	**223**	**69**	**42**	**334**	**100,0%**		**100,0%**
Total en %	**66,8%**	**20,7%**	**12,6%**	**100,0%**		↑ Redressement	
Redressement →	↓	↓	↓				
Données INSEE	**65,0%**	**19,0%**	**16,0%**	**100,0%**			

Au sein de chaque entreprise, nous avons cherché à interroger en priorité le Responsable de la Sécurité des Systèmes d'Information (RSSI). Celui-ci a répondu pour 34% (35% en 2014) des entreprises interrogées, mais plus de 55% dans les plus de 1 000 salariés (53% en 2014).

Toutes tailles et secteurs confondus, les personnes sondées sont à plus de 87% des DSI (Directeur des Systèmes d'Information), des Directeurs ou Responsables informatiques ou des RSSI (91% en 2014).

Moyens consacrés à la sécurité de l'information par les entreprises

En préambule, toutes les entreprises, tous secteurs confondus et quelle que soit leur taille, confirment cette année encore que l'informatique est perçue comme stratégique. La question ne se pose plus…

Un budget sécurité dont le périmètre est mieux cerné

Les RSSI ont moins de mal que les années précédentes à cerner le budget qui leur est attribué par rapport au budget informatique total (15% de NSP cette année contre 25% en 2014).

Lorsque le budget est clairement identifié (32% des cas) la répartition reste hétérogène.

Quel pourcentage représente le budget sécurité par rapport au budget informatique ?

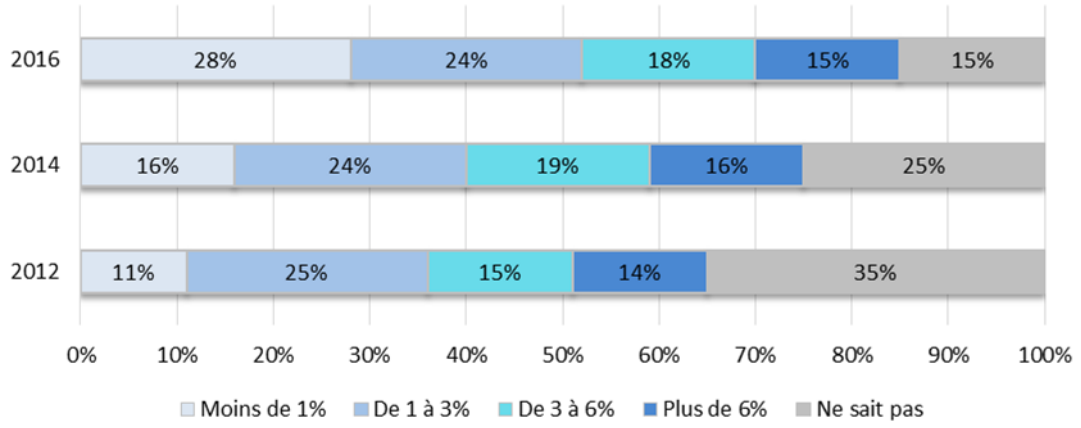


Figure 1 – Part du budget informatique alloué à la sécurité dans les entreprises

Une légère reprise des budgets sécurité

Globalement, le pourcentage des budgets « constants » augmente (67% contre 54% en 2014) tandis que les budgets « en augmentation » diminuent (18% contre 27% en 2014).

En 2015, quelle a été l'évolution du budget sécurité de l'information par rapport à l'année précédente ?

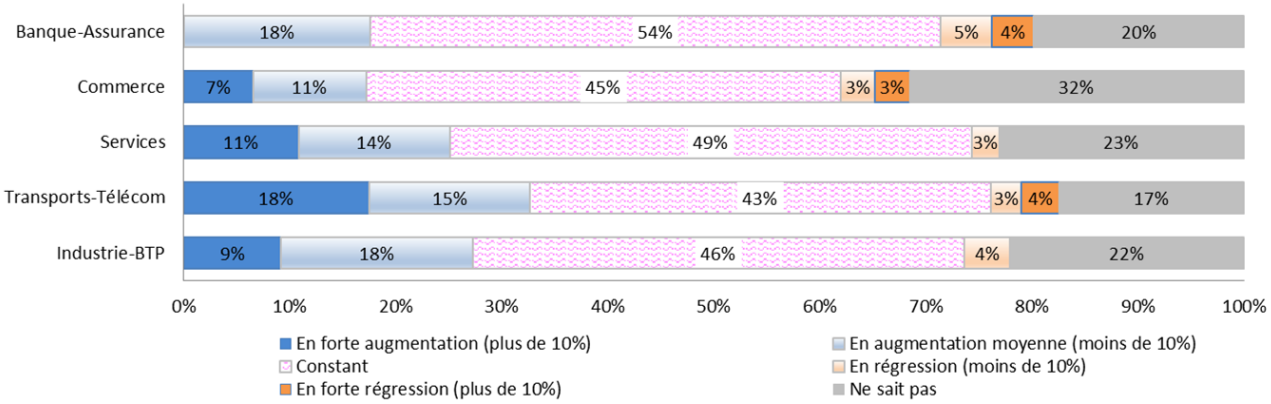


Figure 2 – Évolution du budget sécurité selon les secteurs d'activités

Par ailleurs, les postes ayant eu la plus grosse augmentation sont la « Mise en place d'éléments organisationnels » (+ 4 points à 16%) et la « Formation \ Sensibilisation » (+ 3 points à 12%). Toutefois, pour beaucoup d'entreprises, la sécurité reste encore une histoire de mise en place de solutions techniques…

Les contraintes organisationnelles et le budget freinent encore le RSSI

Enfin, lorsque l'on cherche à connaître les freins à la conduite des missions de sécurité dans leur entreprise, les RSSI citent les points présentés à la figure suivante.

Citez les principaux freins à la conduite des missions de sécurité de l'information ?

Figure 3 – Principaux freins à la conduite des missions de sécurité de l'information

Les deux freins principaux restent comme en 2014 le manque de moyens budgétaires et les contraintes organisationnelles, en hausse sensible par rapport à 2014 (respectivement + 8 points et + 15 points). C'est un signe négatif, particulièrement important pour le premier critère (manque de budget).

La réticence de la Direction Générale passe de 19% (2014) à 24% (2016) ! Il reste du chemin à faire auprès de nombreuses DG… Les DSI, quant à eux, sont plutôt convaincus de l'utilité de la SSI (5% de réticents)…

En fin, le manque de personnel qualifié remonte de deux crans, signe d'une continuelle difficulté à recruter dans le secteur de la SSI…

Thème 5 : Politique de sécurité de l'Information (PSI)

Croissance de la formalisation et perception plus forte de son importance

Le nombre d'entreprises ayant formalisé leur PSI, après avoir stagné pendant 4 ans à 64%, progresse de 5 points pour atteindre 69%. Cette augmentation s'explique par la prise de conscience progressive des risques à ne pas adresser les sujets de sécurité.

Cette formalisation est plus importante dans les services (100% pour la Banque-Assurance) que dans les secteurs traditionnels (65% dans le BTP, 62% dans les Transports-Télécom).

La PSI est actualisée chaque année pour une majorité d'entreprise (65%).

Lorsque la PSI est formalisée, le soutien de la Direction Générale est de 90% ; il n'est que de 52% dans le cas contraire (PSI non formalisée).

Élaboration de la PSI

On constate une implication de plus en plus importante des différentes fonctions de l'entreprise dans l'élaboration de la PSI.

Quelles sont les entités de votre entreprise qui se sont impliquées dans l'élaboration de la Politique de Sécurité de l'Information (PSI) ?

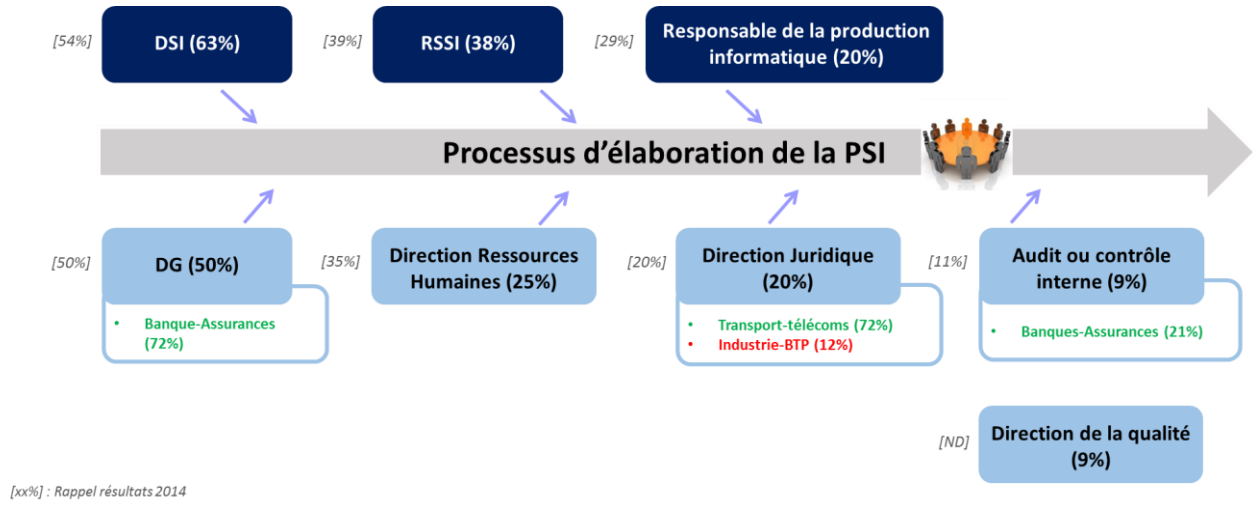


Figure 4 - Implication dans la PSI des différentes entités de l'entreprise

Néanmoins on constate une implication beaucoup plus forte de la Direction Générale et de la DSI dans les petites et moyennes entreprises que dans les grandes. La plus grande proximité avec les équipes opérationnelles contribue probablement à l'identification plus aisée du risque. D'autre part, les PMEs sont souvent dépendantes d'un petit nombre de grands clients qui exercent une pression de plus en plus importante sur leurs fournisseurs quant à la maîtrise de la sécurité de l'information.

Quelles sont les entités de votre entreprise qui se sont impliquées dans l'élaboration de la Politique de Sécurité de l'Information (PSI) ?

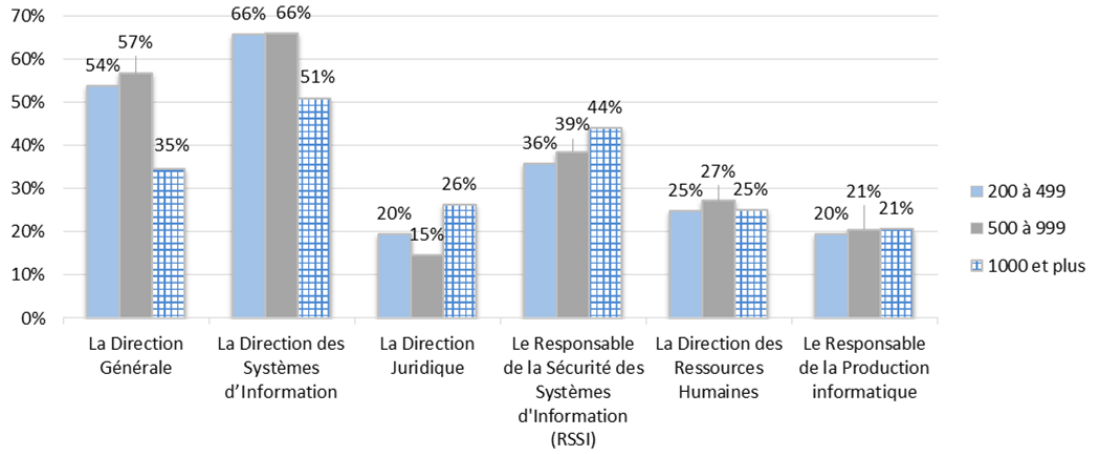


Figure 5 - Implication des fonctions de l'entreprise dans la PSI (en fonction de leur taille)

Communication de la PSI

À contrario la communication de celle-ci, à l'exception des banques et assurances qui ont un programme de formation dédié, n'est globalement pas industrialisée. La conséquence est que sa connaissance et son adoption ne sont ni complètes ni homogènes ce qui limite son application et son efficacité.

La Politique de Sécurité de l'Information (PSI) de votre entreprise est-elle communiquée à tous les acteurs du SI ?

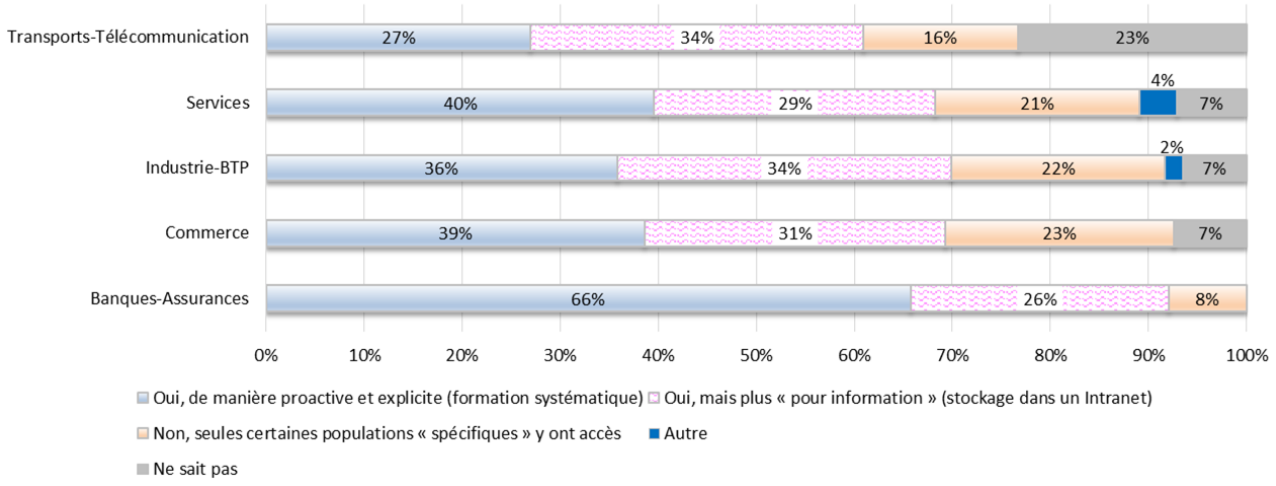


Figure 6 - Communication proactive et explicite de la PSI (formation systématique)

54% des entreprises appuient leur PSI sur des référentiels officiels et à peine plus (59%) partagent celles-ci avec les partenaires extérieurs.

La Politique de Sécurité de l'Information (PSI) de votre entreprise s'appuie-t-elle sur des référentiels de sécurité ? Est-elle communiquée à tous les acteurs du SI ? Est-elle partagée avec des partenaires extérieurs de l'entreprise concernés par le SI ?

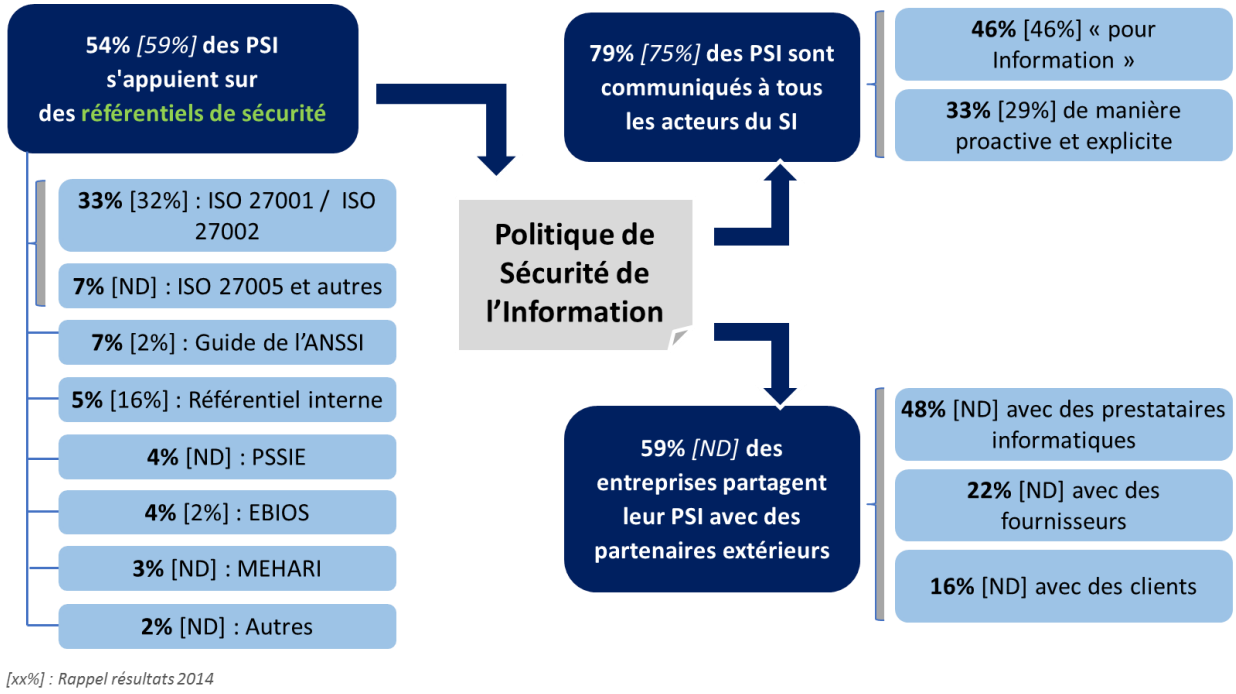


Figure 7 - Référentiels utilisés pour la formalisation de la PSI

Il sera intéressant d'observer cette évolution avec la croissance des infrastructures cloud.

Thème 6 : Organisation de la sécurité de l'information

Une fonction RSSI qui continue de croître

La fonction de Responsable de la Sécurité des Systèmes d'Information (RSSI ou RSI) continue sa progression au sein des entreprises, ce qui va dans le sens de l'histoire… La croissance est remarquable, passant de 37% (en 2008) à 67% (2016), soit une croissance de 181% en 8 ans !

La fonction de Responsable de la Sécurité des Systèmes d'Information (RSSI) est-elle clairement identifiée et attribuée ?

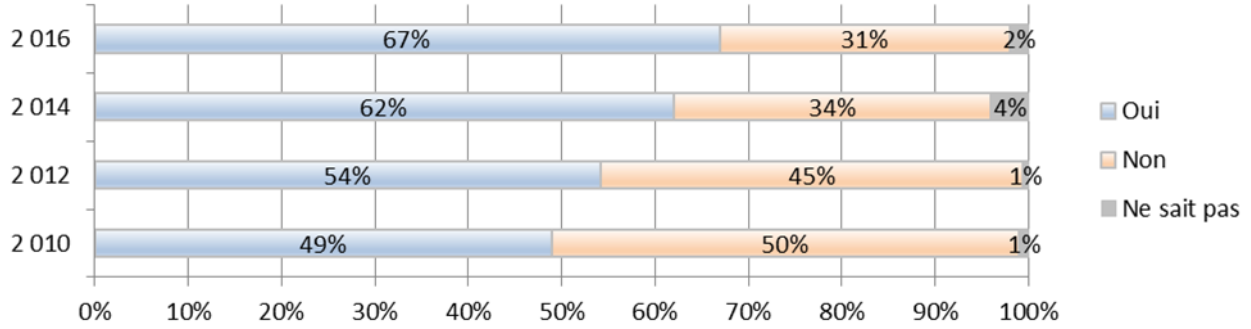


Figure 8 - Attribution de la fonction RSSI

52% des RSSI sont dédiés à cette tâche à temps plein (vs 47% en 2012), avec des disparités qui se tassent en fonction des secteurs d'activités (64% dans les Services pour plus de 80% dans la Banque – Assurance).

Lorsque le RSSI n'existe pas, cette mission reste fortement attachée à la Direction des Systèmes d'Information (40% des cas).

Un rattachement encore en perpétuelle évolution…

Le RSI ou RSSI est soit rattaché à la DSI (42% contre 46% en 2014), soit à la Direction Générale (30% (+3 points vs 2014), où, en troisième position à la Direction Administrative et Financière (DAF) (7%) ou directement des entreprises interviewées. Ceci s'explique encore par les arrivées plus nombreuses de RSSI au sein d'entreprises de tailles moyennes, provenant très souvent de la DSI et ayant un niveau de maturité en Sécurité des SI moyen, voire faible.

Quel est le rattachement hiérarchique du RSSI au sein de votre entreprise ?

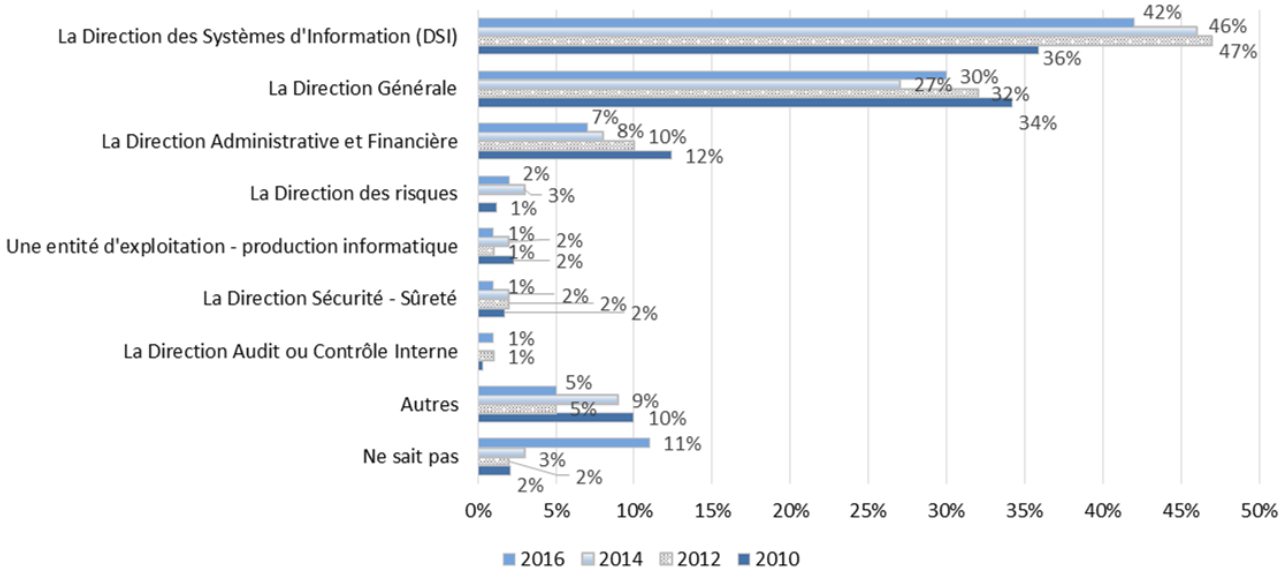


Figure 9 - Rattachement hiérarchique du RSSI au sein de l'entreprise

Globalement, la répartition des tâches du RSSI n'a que très peu évolué depuis 2010. On note toutefois que l'aspect 'juridique' diminue sensiblement, lié certainement à la prise en compte des aspects CNIL par des CIL (ou équivalents) plus nombreux…

Dans le cadre des missions du RSSI, quel pourcentage représente les temps consacré…

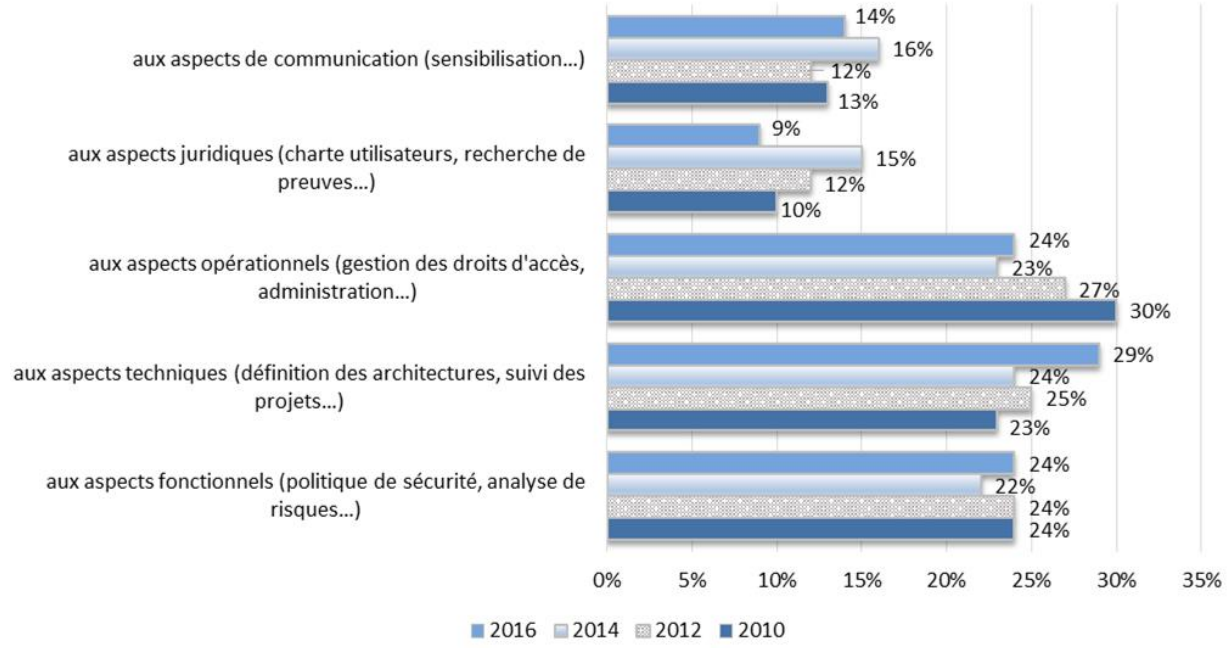
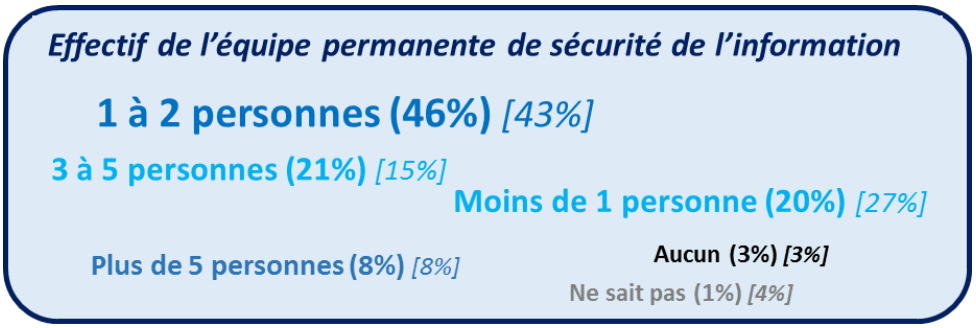


Figure 10 - Répartition des missions du RSSI

95% des entreprises ont en permanence une équipe sécurité (-2 points vs 2014). Toutefois, dans 47% le RSSI (ou son équivalent) est 'partagé' et dans 46% des cas il est encore un homme ou une femme seul(e) ou en binôme seulement !

Quel est l'effectif total de l'équipe sécurité de l'information permanente au sein de votre entreprise ?



[xx%] : Rappel résultats 2014

Figure 11 - Effectif total de l'équipe sécurité permanente au sein de l'entreprise

Thème 7 : Sécurité des ressources humaines

L'étude 2016 nous révèle que 4 entreprises sur 5 ont une charte d'usage ou d'utilisation du SI. Les entreprises du secteur Banque-Assurances avec un taux à 100% ont systématisé cet usage. Nous noterons que près d'un quart des industries du BTP (26%) et des entreprises des secteurs Transports – Telecom (23%) n'ont pas de telle charte.

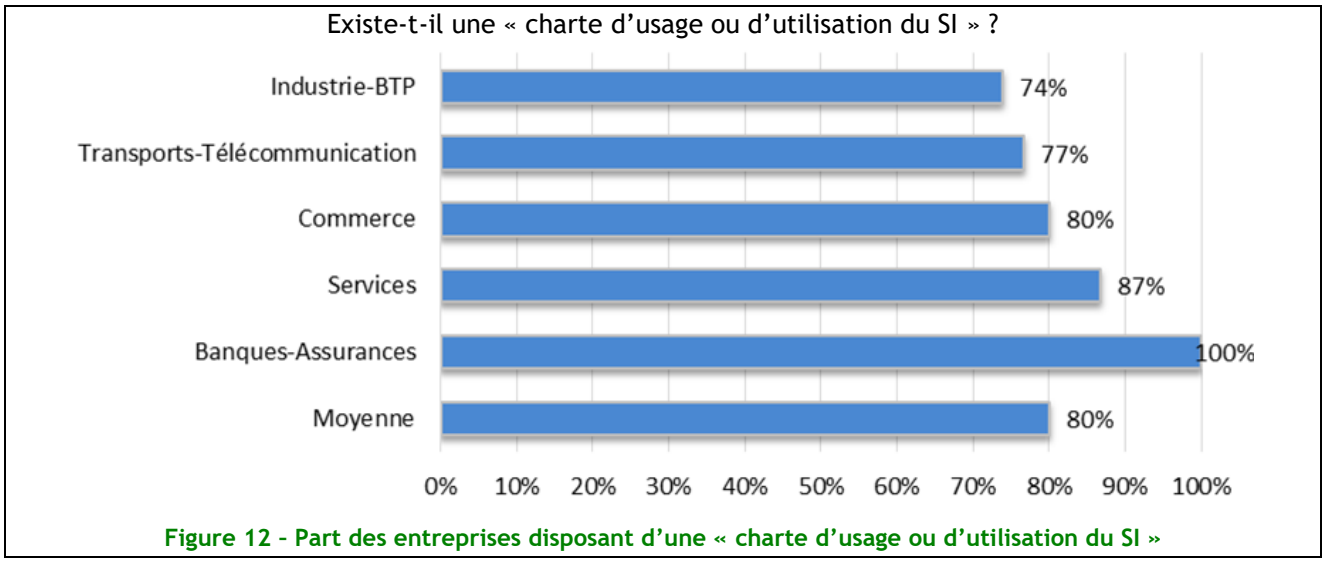


Figure 12 – Part des entreprises disposant d'une « charte d'usage ou d'utilisation du SI »

La part des entreprises dédiant cette charte à leur personnel ne cesse de croitre depuis 2012 pour atteindre un taux de 96% en 2015. Le pourcentage des entreprises étant en cours d'élaboration d'une charte à destination de leur personnel passant de 18% en 2012 à 3% en 2016. Cela illustre le travail effectué par l'ensemble des acteurs depuis ces dernières années.

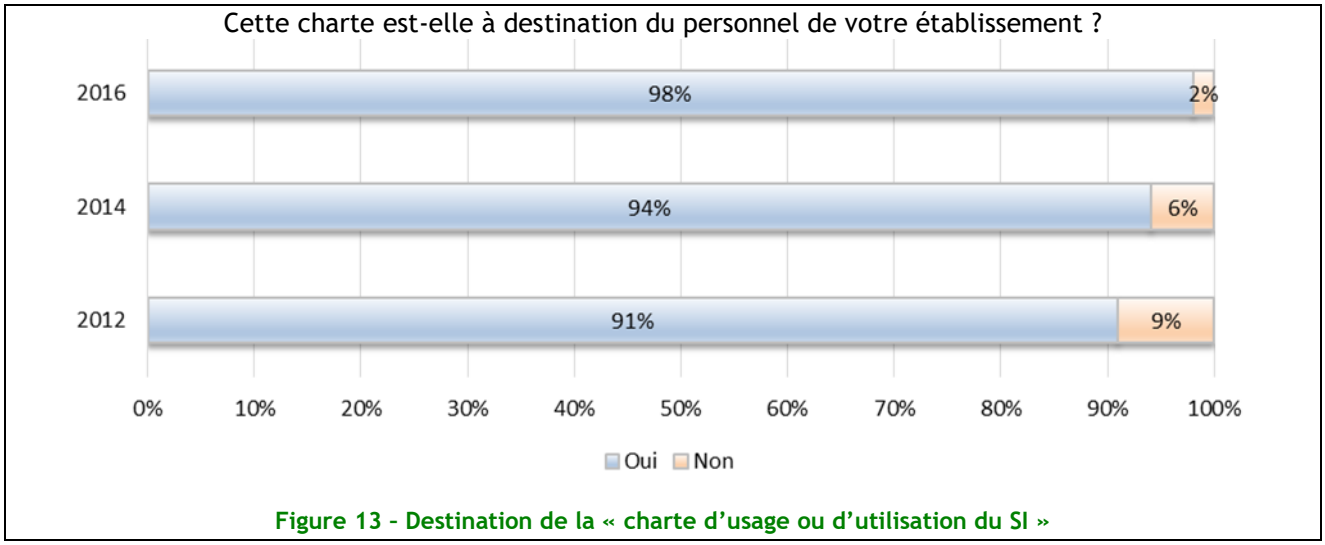


Figure 13 – Destination de la « charte d'usage ou d'utilisation du SI »

La part des entreprises ayant une charte spécialement destinée aux personnels externes (prestataires / fournisseurs) augmente légèrement depuis 2014 (+7 points). Près de la moitié d'entre elles (51% en 2014 et 47% en 2016) n'ont toujours pas de telle charte.

Les moyens utilisés par les entreprises pour assurer la sensibilisation se centrent principalement sur la publication à l'ensemble des personnels. Cette étude 2016 montre par ailleurs que la part des actions de sensibilisation dédiées auprès de certaines catégories des personnels de l'entreprise est moins forte que les années précédentes.

Quels sont les moyens utilisés pour assurer la sensibilisation ?

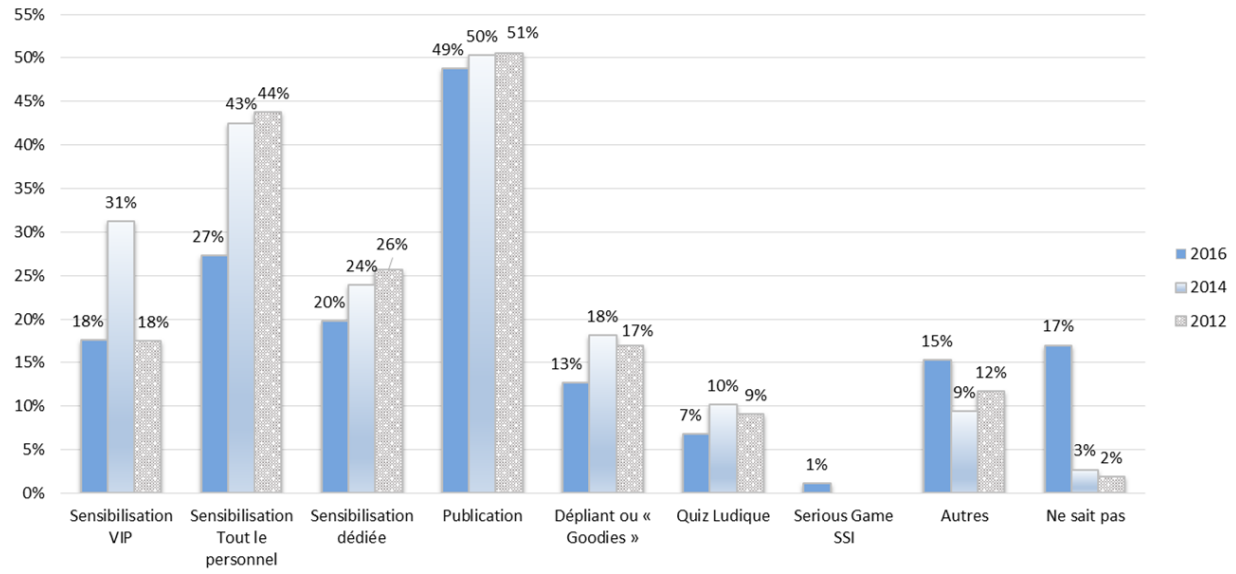


Figure 14 - Moyens utilisés pour assurer la sensibilisation

Paradoxalement, face aux efforts mis en œuvre par les entreprises pour sensibiliser leur personnel, peu d'entre elles en mesurent les impacts (32%).

Enfin, bien que les entreprises, quel que soit leur secteur d'activité, aient systématisé les procédures de suppression des droits d'accès et de restitution du matériel lors des départs des collaborateurs, le taux de celles n'en disposant pas est en augmentation de 4 points entre 2014 et 2016.

Les secteurs les plus concernés par cette dégradation sont Transports-Télécommunication (+8 points), Commerce (+5 points) et Services (+4 points). Ceci est certainement dû au fait que les RSSI dernièrement arrivés le sont au sein d'entreprises de tailles moyennes, provenant très souvent de la DSI et ayant un niveau de maturité en Sécurité des SI moyen, voire faible.

Existe-t-il une procédure pour gérer, en cas de départ ou mutation des collaborateurs, la suppression de tous les droits d'accès et la restituation de tout le matériel ?

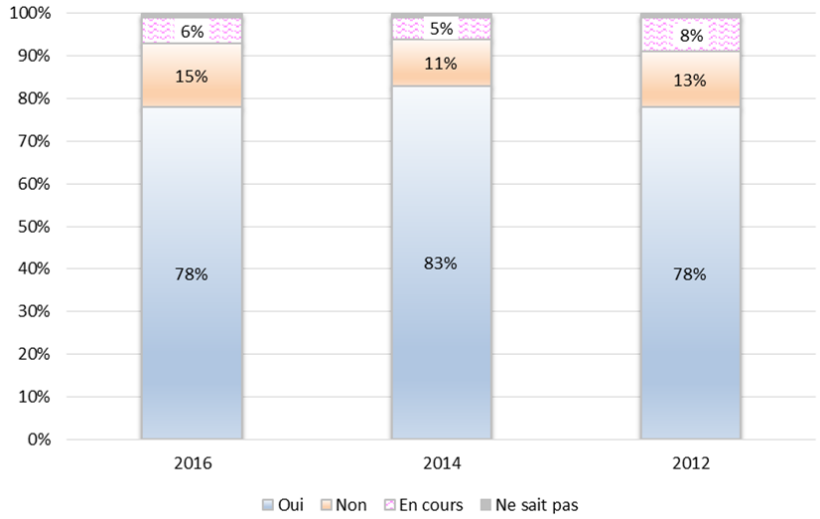


Figure 15 - Existence d'une procédure de gestion des droits d'accès et de restitution du matériel

Thème 8 : Gestion des actifs

Inventaire et classification : un bilan en demi-teinte

La croissance constatée depuis plusieurs années sur l'identification des informations sensibles se poursuit avec un écart notable pour le secteur « Commerce » (84% contre 74% en moyenne). Les fuites de données personnelles qui sont été particulièrement médiatisées dans le secteur du commerce ont peut-être contribué à le sensibiliser plus particulièrement.

Avez-vous inventorié toutes les informations (et leurs supports) de votre entreprise et leur avez-vous attribué un propriétaire ?

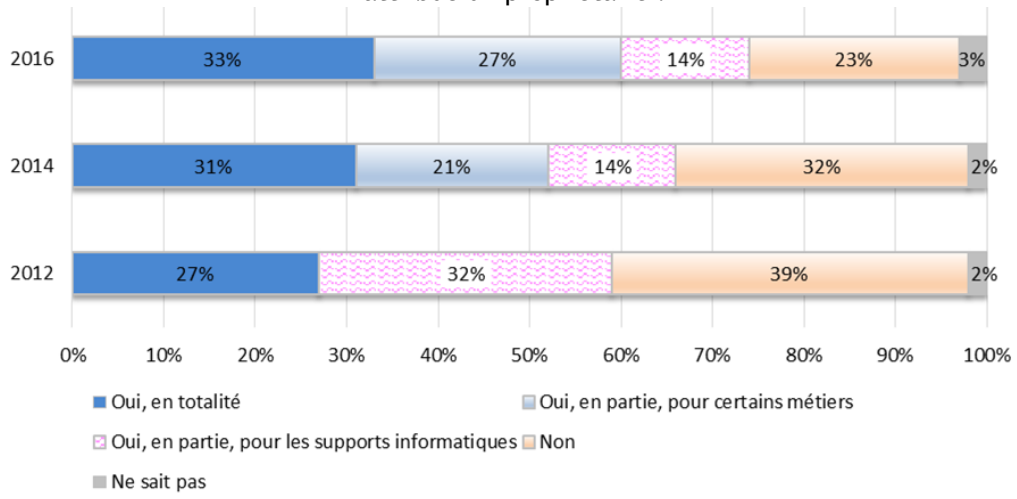


Figure 16 – Inventaire des informations de l'entreprise

Cette progression se constate essentiellement dans la partie « Oui, en partie pour certains métiers » qui passe de 21% en 2014 à 27%.

En revanche, à l'inverse, la hausse qui avait été constatée concernant la classification des informations a ralenti (52% contre 66% en 2014). Ces évolutions « inverses » sont étonnantes dans la mesure où les deux activités (identification et classification) sont souvent traitées ensemble. Il faut cependant noter que le processus de classification est plus « lourd » et demande un investissement conséquent que les grandes entreprises (> 1000 salariés) sont plus enclins à faire (33% ont fait la classification complètement contre 22% en moyenne).

En dehors du secteur « Banques Assurances » qui pour des raisons réglementaires et culturelles est en avance sur ce sujet (seules 33% des entreprises du secteur n'ont pas classifiées leurs informations sensibles), les entreprises restent globalement peu matures : en moyenne, 47% d'entre elles déclarent n'avoir pas classifiées leurs informations sensibles.

Avez-vous formalisé une classification des données de votre entreprise ?

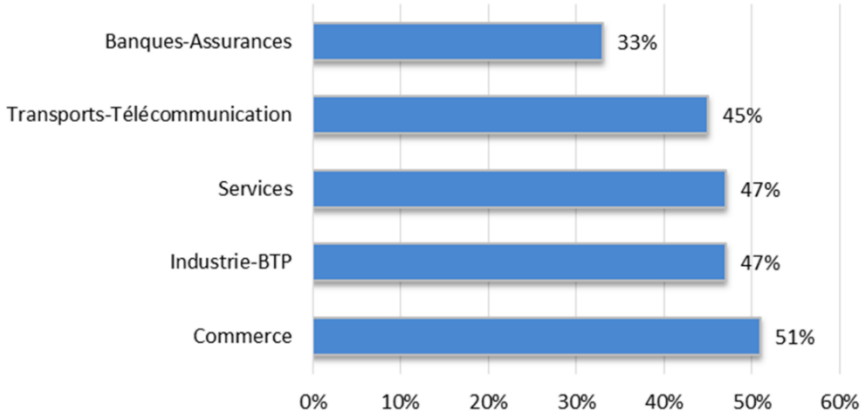


Figure 17 - Entreprises n'ayant pas lancé de démarche de classification

Dans les cas où la démarche n'a pas été engagée, la question se pose de savoir sur quelle base sont décidés les axes prioritaires d'actions sur la sécurité des SI. De même, on peut également s'interroger sur l'identification « partielle » des informations sensibles soit « pour certains métiers », soit « pour les supports informatiques ».

Le nombre de niveaux de sensibilité définis par les entreprises se situe en moyenne autour de 3,3.

Des analyses de risques qui ne progressent pas

Une entreprise sur deux réalise une analyse de risque formelle et seulement 15% réalisent cette analyse en totalité. Le pourcentage est d'ailleurs en légère baisse par rapport aux années précédentes. Cette activité ne devrait pas être négligée d'autant plus que la PSI de l'entreprise repose essentiellement sur l'analyse de risques.

Comme précédemment, les grandes entreprises réalisent ces analyses de façon plus systématique : elles ne sont que 27% à n'avoir pas réalisé cette analyse de risque formelle contre 51% en moyenne.

Cette analyse de risque réalisée essentiellement par le RSSI/RSI (62%) devrait impliquer davantage les autres acteurs de l'entreprise, notamment le Risk Manager qui n'est concerné que dans 8% des entreprises interrogées.

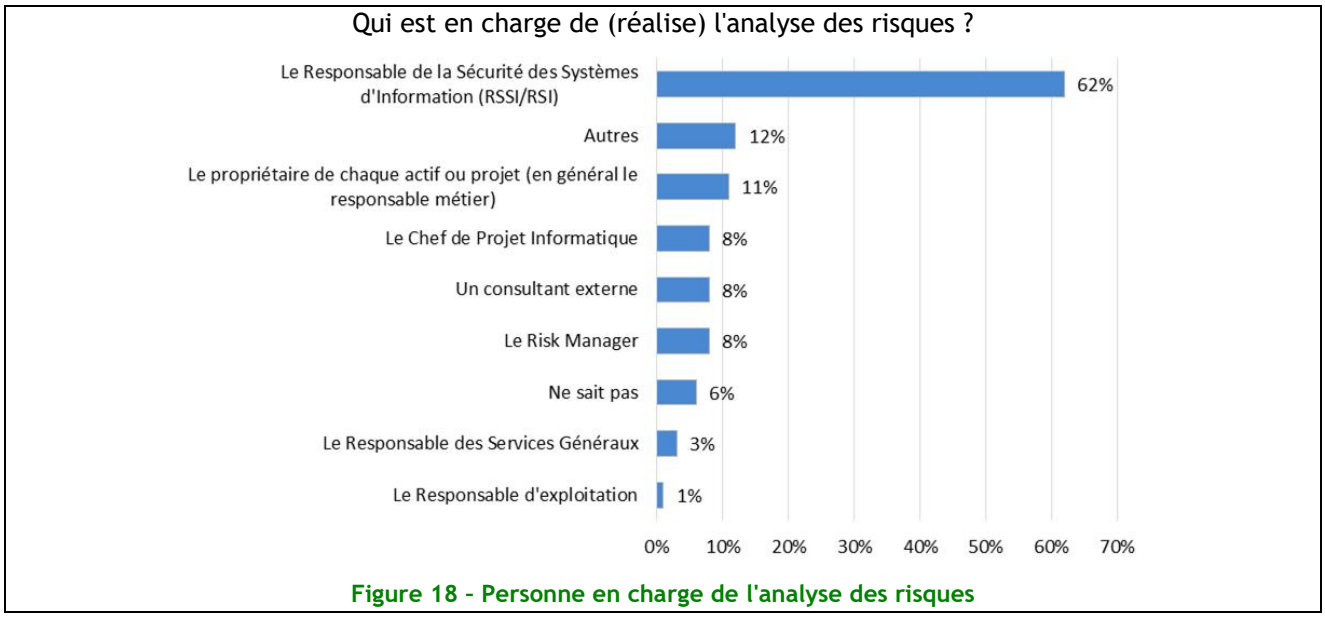


Figure 18 – Personne en charge de l'analyse des risques

Les méthodes d'analyse de risques utilisées sont variables mais étonnamment, dans 43% des cas les méthodes utilisées sont inconnues – le chiffre monte à 74% dans le secteur du Commerce). Cela traduit un manque de maturité et surtout le manque d'implication des acteurs du SI ou du métier dans la gestion des risques.

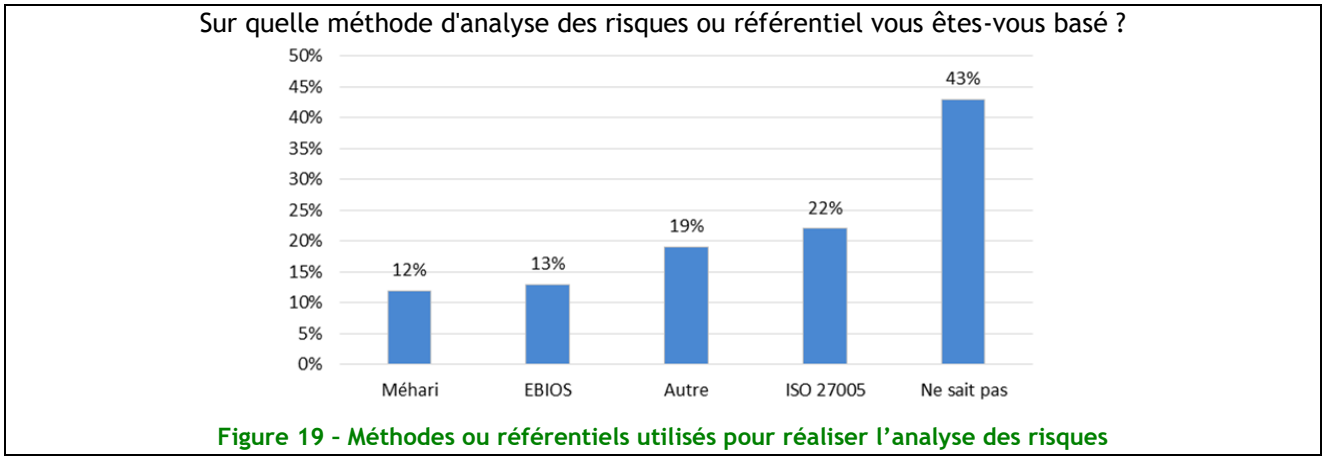


Figure 19 – Méthodes ou référentiels utilisés pour réaliser l'analyse des risques

En moyenne, 70% des entreprises ont défini et argumenté le plan d'action d'amélioration de la sécurité de l'information de leur société en fonction de cette analyse et le taux monte 79% chez les Industries-BTP. Ce chiffre est en régression par rapport à 2014 où ils étaient 83% à avoir défini ce plan d'actions.

Thème 9 : Contrôle d'accès

Une gestion des identités en forte progression

On remarque une forte progression de la mise œuvre de matrices d'habilitations basées sur des rôles et profils : 60% des entreprises interrogées les utilisent désormais contre 41% en 2014. De même l'utilisation de workflows d'approbation et de mécanismes de provisionning automatiques augmente dans une moindre mesure (le provisionning étant présent désormais dans les deux tiers des entreprises de plus de 1 000 employés).

Ces résultats traduisent une prise de conscience des entreprises quant à l'importance d'adapter finement les droits au rôle de chaque utilisateur. En effet, la mise en œuvre de ces chantiers nécessite une forte implication du management et des métiers au cours de projets consommateurs en temps et en ressources.

Les mécanismes d'authentification forte de type OTP (One Time Password), certificat matériel ou logiciel progressent également. On note que l'utilisation de la biométrie reste faible. Ce faible niveau d'adoption pourrait s'expliquer par la complexité rencontrée lors des chantiers de déploiement.

Les taux d'utilisations des solutions de Single Sign On restent stable par rapport à 2014, quelle que soit la technologie (SSO ou Web SSO).

Quelles sont les technologies / approches de sécurisation utilisées dans votre entreprise en matière de contrôle d'accès logique ?

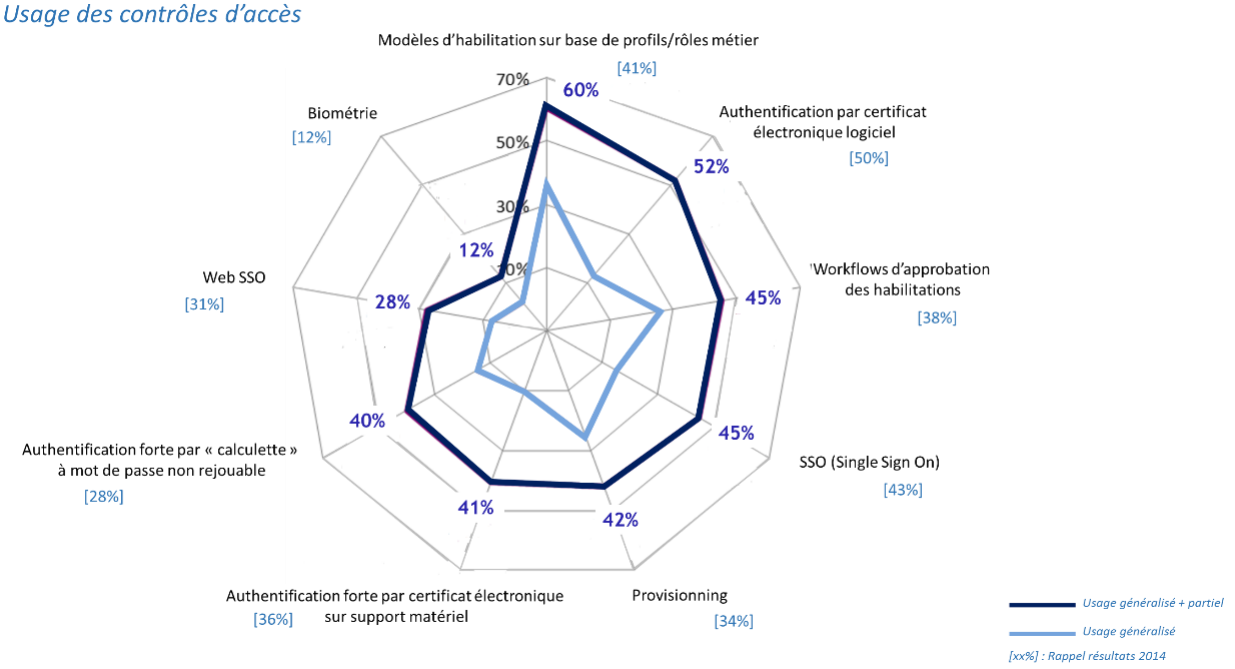


Figure 20 - Technologies / approches de sécurisation en matière de contrôle d'accès logique

L'utilisation de ces différentes solutions n'est pas homogène en fonction du secteur d'activité. La Banque-Assurance est par exemple largement plus avancée dans l'utilisation des profils et rôles (88% des entreprises de ce secteurs ayant mis en œuvre ces mécanismes) et du provisionning que les autres secteurs d'activités.

Quelles sont les technologies / approches de sécurisation utilisées dans votre entreprise en matière de contrôle d'accès logique ?

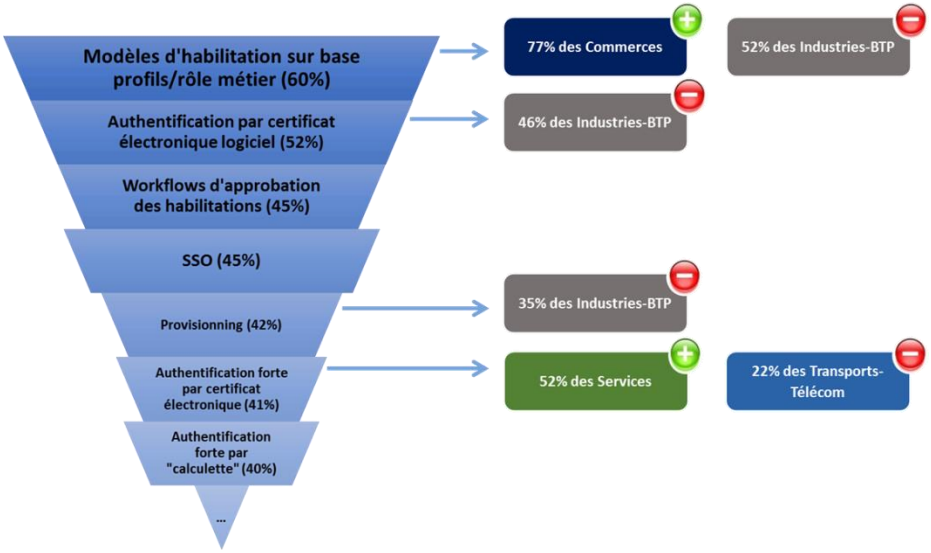


Figure 21 - Technologies / approches de sécurisation en matière de contrôle d'accès logique (détail par secteur d'activité)

Le palier dans les procédures de gestion des accès se confirme

Pas d'évolution dans la formalisation des processus de gestion du cycle de vie des comptes avec toujours environ 2/3 des entreprises ayant ce processus entièrement formalisé et ce de façon homogène quel que soit le secteur d'activité.

On retrouve également une stabilité dans le nombre d'entreprises disposant d'une procédure de gestion du cycle de vie des administrateurs. Cette proportion est paradoxalement plus faible que celle associée à la gestion des comptes standards alors que la criticité et la sensibilité des accès administrateurs est bien plus importante.

De même, le nombre d'entreprises disposant de politique de complexité et d'expiration des mots de passe reste stable.

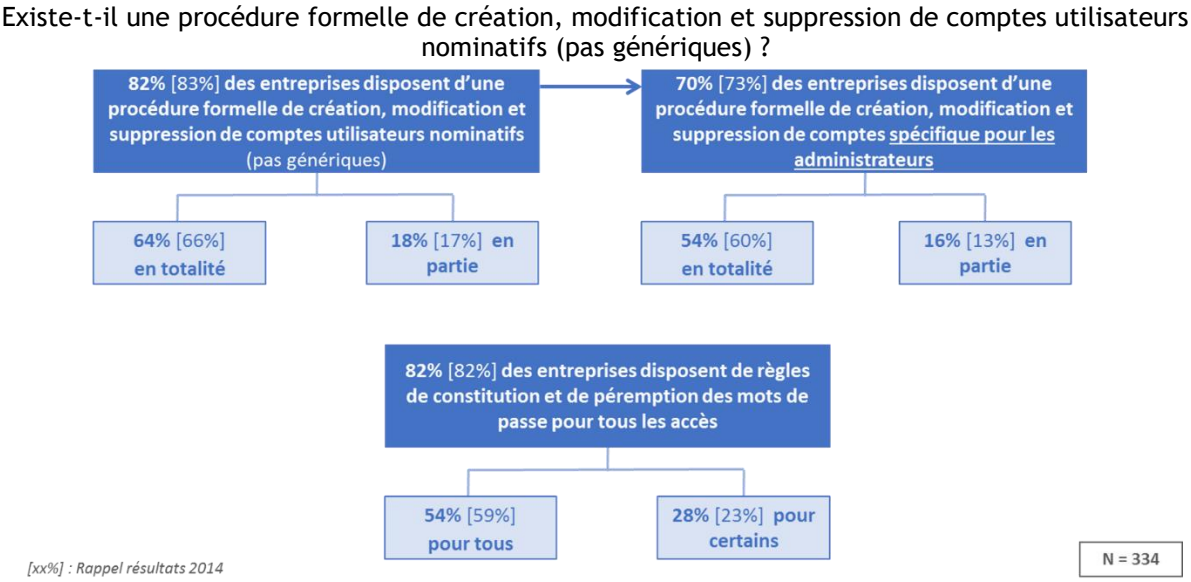


Figure 22 - Procédures de gestion des accès logiques

À nouveau, l'analyse détaillée de ces résultats fait apparaître une existence de ces politiques et procédures dans une plus forte proportion dans le secteur de la Banque-Assurance.

Thème 10 : Cryptographie

Globalement, la cryptographie reste peu utilisée (34% en moyenne tous secteurs confondus). La Banque-Assurance est largement majoritaire avec 51% d'utilisation : bien entendu ceci est lié au métier mais également aux nombreux règlements, lois, etc. qui lui incombe.

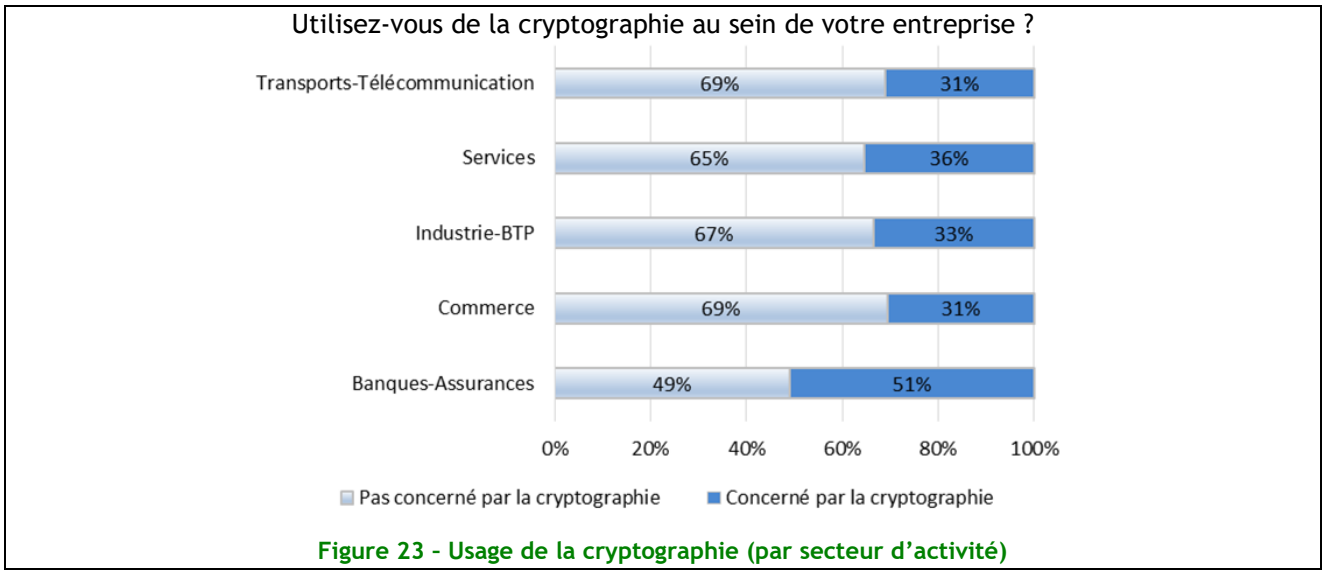


Figure 23 - Usage de la cryptographie (par secteur d'activité)

Lorsqu'elle est utilisée, c'est très largement (à 76%) la DSI qui porte la responsabilité de la gestion des moyens cryptographiques (attribution, révocation, destruction des clés). Ce point, identifié (parfois à tort) comme « technique » lui revient naturellement…

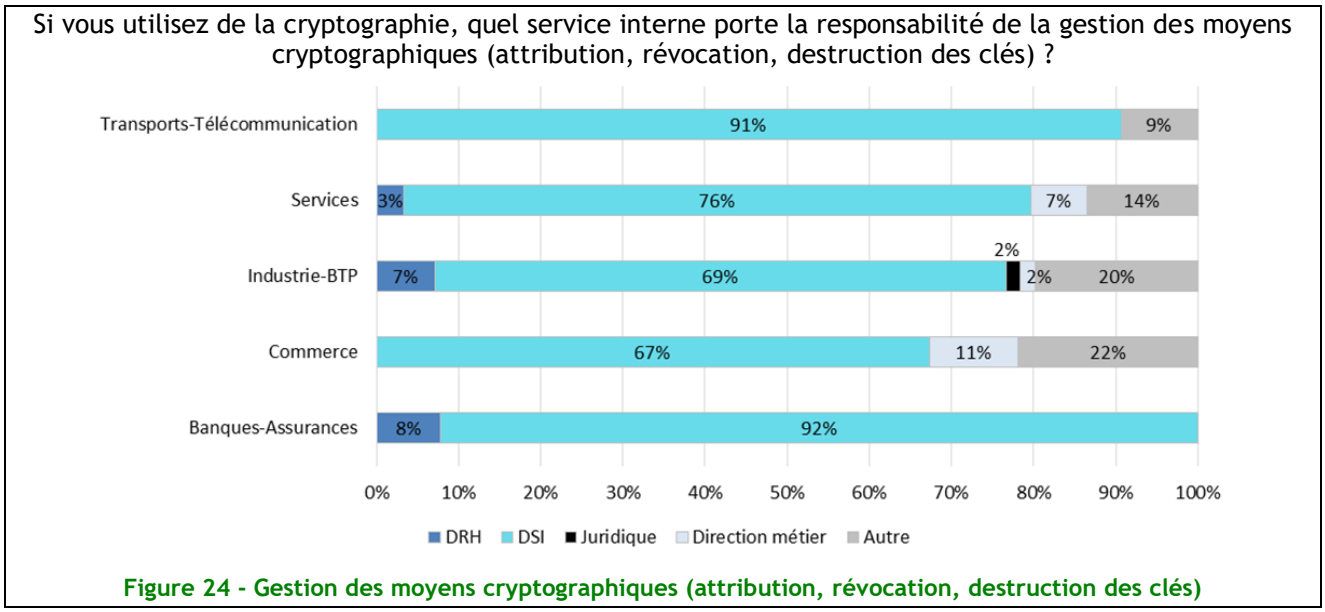


Figure 24 - Gestion des moyens cryptographiques (attribution, révocation, destruction des clés)

Thème 11 : Sécurité physique et environnementale

Le pourcentage des entreprises qui veillent à la protection des supports physiques (bandes, CD, papiers, etc.) dans le cadre de leur PSSI a baissé par rapport à 2014. Ce pourcentage passe de 70% en 2014 à 66% cette année. Cette baisse peut être justifiée par l'absence d'utilisation de plus en plus accentuée de ces supports physiques.

Une disparité des pratiques est toujours constatée entre les différents secteurs d'entreprises, mais cette année, les Banques-Assurances se démarquent de loin et gèrent de manière plus efficace la protection de leurs données sur supports physiques. Elles affichent un pourcentage de 88% contre une moyenne de 66%.

La protection des données sur supports physique (bandes, CD, papiers, etc.) est-elle prise en compte dans la PSSI ?

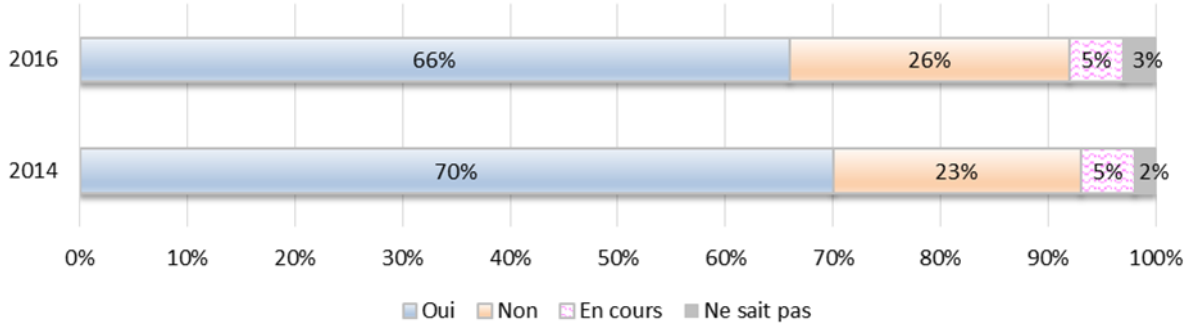


Figure 25 - Entreprises prenant en compte la protection des données sur supports physique dans la PSSI

Par ailleurs, les dispositifs de sécurité physique implémentés ont largement augmenté par rapport à l'année dernière. On peut constater une grande prise de conscience et un souci de renforcer d'avantage cette sécurité physique, ce qui est une bonne chose. La mise en place de ces dispositifs est plus accentuée chez les entreprises de 1 000 personnes et plus.

Les dispositifs de contrôle d'accès physique sont utilisés dans 65 % des cas, valeur qui a fortement progressé par rapport à 2014 (44%). Deux entreprises sur trois sont équipées de détecteurs d'incendie (66%) et de contrôles d'accès par badge (65%).

Des dispositifs de sécurité physique sont-ils implémentés pour sécuriser l'accès et/ou les salles machines dans votre entreprise ?

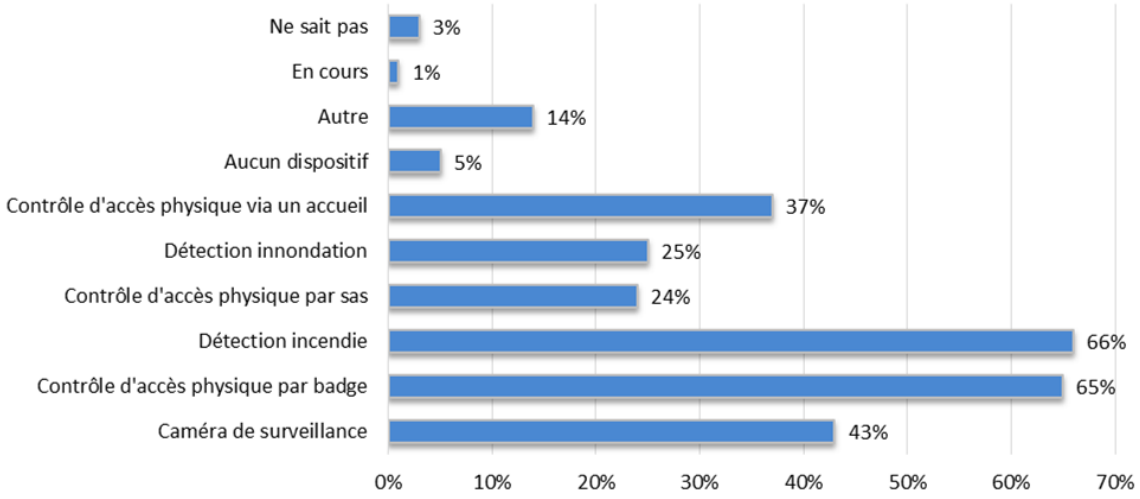


Figure 26 - Dispositifs de sécurité physique pour sécuriser l'accès et/ou les salles machines

Par ailleurs, la sensibilité à la mise en œuvre de mesures de sécurité physique des entreprises Industries-BTP et des effectifs entre 200 et 500 personnes est très faible… Certaines des fabrications de ces activités peuvent pourtant relever d'une sensibilité importante. Ce secteur mériterait une sensibilisation plus ciblée sur la sécurité physique et ses dispositifs spécifiques.

Thème 12 : Sécurité liée à l'exploitation

Les entreprises partagent sans ambiguïté le constat d'une augmentation constante des menaces et des attaques qui tirent parti des vulnérabilités existantes. Un arsenal d'outils est à leur disposition, mais certains seulement semblent faire l'adhésion de tous. Si aucune technique n'émerge véritablement, certaines progressent et certains composants du Système d'Information font maintenant l'objet d'une attention plus soutenue.

Les vulnérabilités sont un vrai talon d'Achille. Les entreprises y font face en s'appuyant sur diverses sources, cependant l'effort semble s'effriter quelque peu…

Un arsenal de protection

Globalement, les protections peuvent se classer dans 2 catégories :

- les outils classiques, relativement simples et unanimement adoptés :
  - les solutions antivirus et antimalware qui interdisent à toute attaque connue d'être active,
  - l'anti-spam qui prévient toute diffusion des attaques via la messagerie,
  - le pare-feu (firewall) qui va bloquer les flux suspects, bloquant ainsi l'effet de certaines attaques,
- des outils plus spécifiques et relativement complexes :
  - le SIEM pour corréler les évènements du SI afin d'établir tout comportement suspect,
  - le Data Leak Protection qui interdira à certains types de données de quitter l'entreprise,
  - les outils de détection et de protection du réseau,
  - le Network Access Control pour interdire à tout matériel sans identification préalable de se connecter au réseau.

Quelles protections contre les logiciels malveillants avez-vous mis en œuvre dans votre entreprise ?

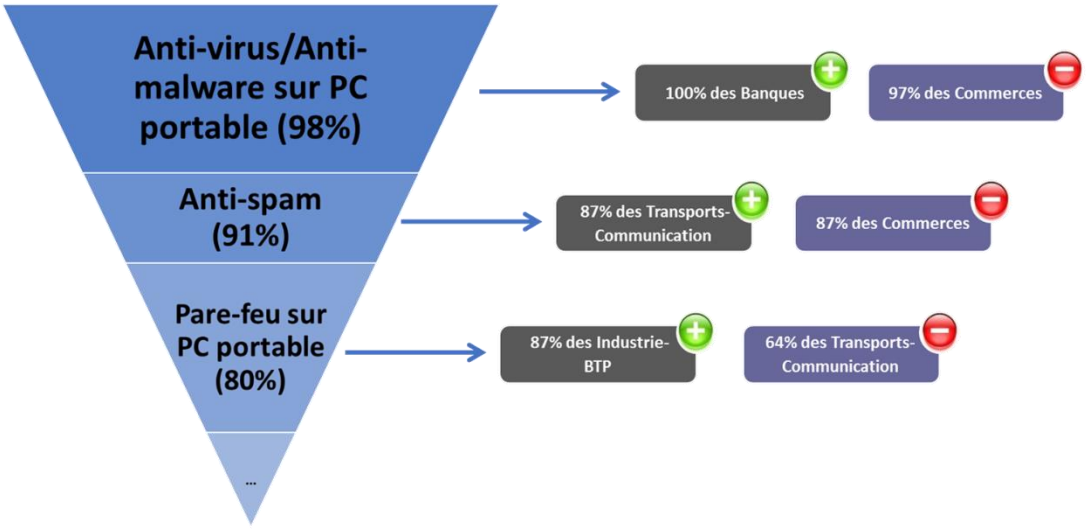


Figure 27 - Top 3 des outils de protection contre les logiciels malveillants

Ces outils classiques sont aujourd'hui bien maitrisés, considérés comme indispensables d'où leur déploiement quasi systématique. On note cependant que s'ils sont tous présents, chaque entreprise met en particulier l'action sur l'un d'entre eux, les « bons » et « mauvais » élèves par métier varient selon l'outil, impliquant une répartition non homogène de ces outils.

Le coût de mise en œuvre, la complexité restent des facteurs de blocage qui empêchent les outils plus spécifiques, plus riches de trouver un écho grandissant.

Quelles protections contre les logiciels malveillants avez-vous mis en œuvre dans votre entreprise ?

Technologies de sécurité

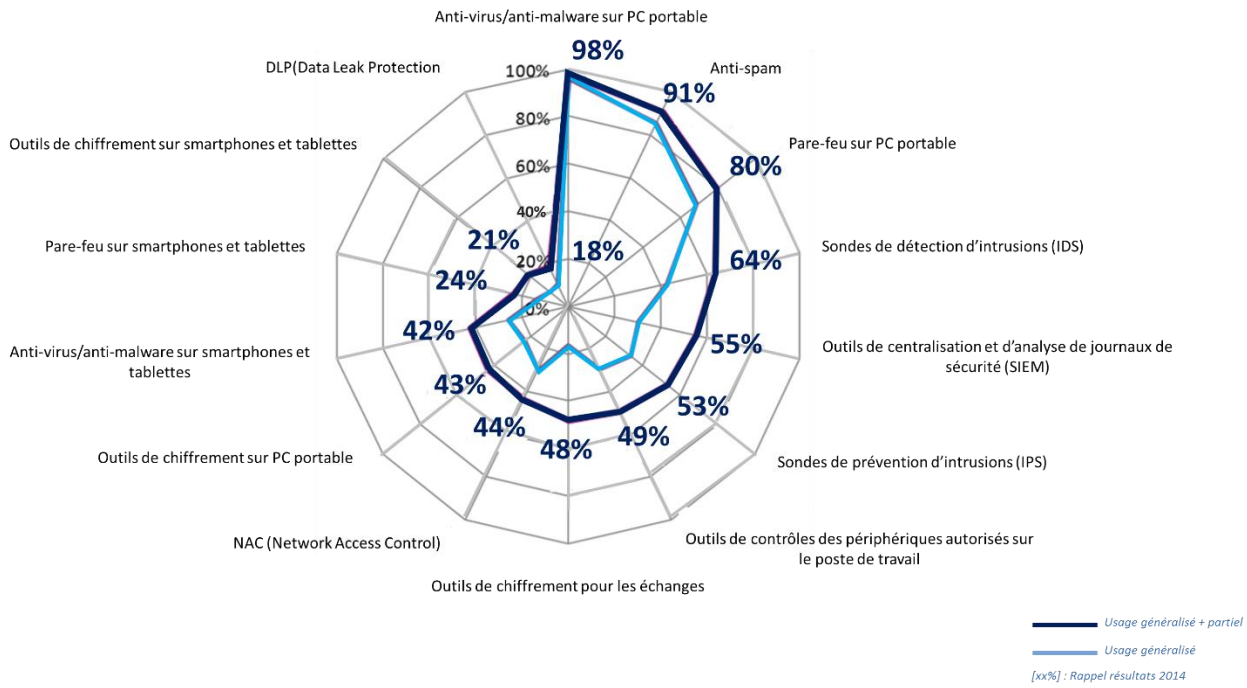


Figure 28 - Arsenal de solutions de sécurité à la disposition des entreprises

Certaines solutions cependant trouvent leur place, très orientées autour du poste utilisateur :

- le déploiement de NAC : +9 points (par rapport à 2014),
- les outils de contrôles des périphériques des PC/portables : +8 points,
- le chiffrement des équipements : +6 points.

On note avec intérêt que l'effort de mise en place de ces solutions se déplace aussi vers les nouveaux équipements qui sont devenus incontournables : les smartphones et tablettes. Ils sont maintenant couverts par des dispositifs similaires aux PC :

- antivirus / antimalware : +19 points,
- pare-feu : +7 points,
- chiffrement des données : +6 points.

Si la sécurité du SI innove peu, elle devient clairement plus globale. Il reste donc à identifier les freins au déploiement des solutions plus complexes qui sont des briques nécessaires à une protection efficace des matériels et des données.

Les vulnérabilités

Aucune solution n'est hélas sans faille et l'informatique n'échappe pas à cette règle… Les logiciels, les matériels, contiennent des défauts qui sont utilisés, « exploités » par des tiers pour voler des données, en tirer un profit financier ou tout simplement nuire.

Certes les traces laissées par ces attaquants, leurs signatures sont, avec le temps, découvertes et les technologies de sécurité citées plus haut, les traiteront, cependant qu'une nouvelle déclinaison de

l'exploitation d'une vulnérabilité laissera encore le SI exposé. La véritable réponse est donc bien d'identifier et de pallier ces vulnérabilités et ce dans les meilleurs délais.

Pour y parvenir les entreprises s'appuient sur une « veille technologique » : 61% des entreprises en réalise adopté cette démarche et sans surprise les banques de manière importante (79%).

Cependant on note une forte régression dans le recours à ce dispositif, -17 points en deux ans… Cumulé au non déploiement des solutions complexes de protection, cela laisse entendre une plus grande exposition aux attaques pour les entreprises.

L'impact est immédiat sur la formalisation, la documentation des procédures de gestion des vulnérabilités, des risques. On consacre moins de temps à la veille et donc on documente moins la manière de traiter : 59% des entreprises ont formalisé et documenté les procédures de correction des vulnérabilités (en recul de 6 points).

Pourtant des acteurs se positionnent en offre de service pour aider les DSI dans cet effort. Ils sont loin d'avoir fait l'unanimité, d'autres sources restent majoritaires pour diffuser l'information nécessaire.

Réalisez-vous une veille permanente en vulnérabilités et en solutions de sécurité de l'information ?

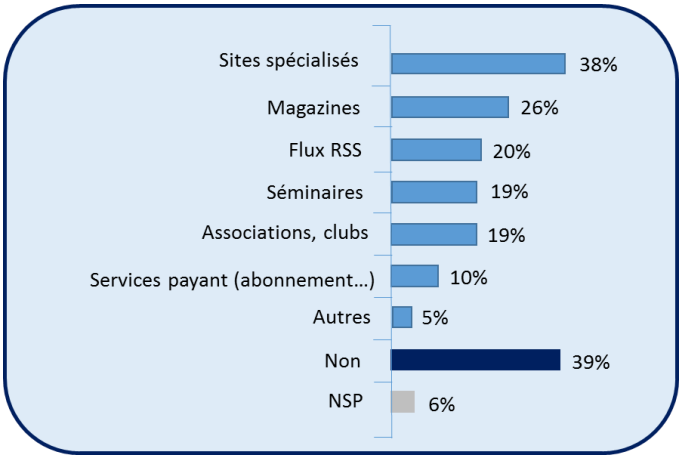


Figure 29 - Sources d'information de la veille en vulnérabilités et en solutions de sécurité

Mais le résultat le plus explicite qui démontre une stagnation si ce n'est un recul dans la mise en place des protections c'est la réactivité des entreprises qui ne s'est hélas pas améliorée…

En cas de menace grave, en moyenne quel délai est nécessaire pour déployer les correctifs ?

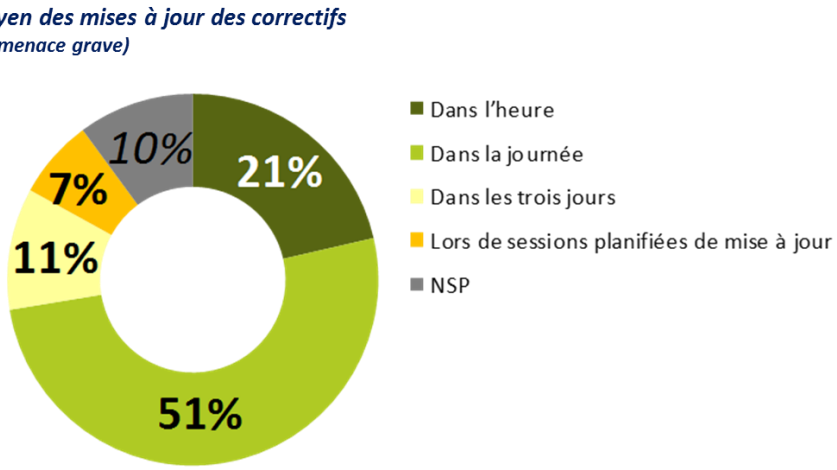


Figure 30 - Réactivité dans l'application des correctifs

Les moyens pour améliorer la sécurité liée à l'exploitation sont bien présents, sans toutefois être complétement déployés… Parfois même, l'effort fait dans leur utilisation est à la baisse.

Parmi les explications que l'on peut identifier, on retrouve : une charge de travail plus importante pour les RSSI, des efforts budgétaires qui limitent l'investissement dans ce domaine, une affectation des budgets aux outils au détriment des moyens humains…

Thème 13 : Sécurité des communications

La position des politiques de sécurité concernant l'accès au SI par des postes non maîtrisés a été rendue plus stricte depuis deux ans. 68% des entreprises interdisent l'accès contre 59% en 2014, la différence se faisant au niveau de l'autorisation sous condition (29% cette année contre 39% en 2014).

On note une évolution en faveur de l'accès par un réseau wifi privé au sein de l'entreprise de manière contrôlée (60% contre 52%) et une baisse de l'interdiction d'accès (28% contre 35%), ce qui confirme la tendance vue entre 2014 et 2012. Sur ce point, le secteur des commerces autorise un accès sous condition dans 70% des cas, tandis que le secteur des Transports-Telecom ne le fait que dans 46% des cas.

On constate une baisse de l'interdiction d'accès via des tablettes et smartphones fournis par l'entreprise (27% contre 34%) répercutée sur une autorisation d'accès contrôlée ou non. Le même type d'appareils mais personnels (BYOD) se voit plus souvent interdit qu'en 2014 (71% contre 66%).

La position concernant la voix sur IP ou la téléphonie IP n'a que très peu évolué.

Les messageries instantanées externes sont mieux acceptées lorsqu'elles sont contrôlées qu'en 2014 (environ 7%) ce qui confirme la tendance vu entre 2012 et 2014 (environ 10%), de même que l'utilisation des réseaux sociaux dans des proportions légèrement moins importantes.

L'accès à l'Internet est majoritairement filtré, et ce dans les mêmes proportions qu'en 2014. Concernant ce point, le secteur des Transports-Telecom est plus restrictif (88% d'interdiction d'accès) tandis que le secteur des Services est plus permissif (64% d'interdiction d'accès).

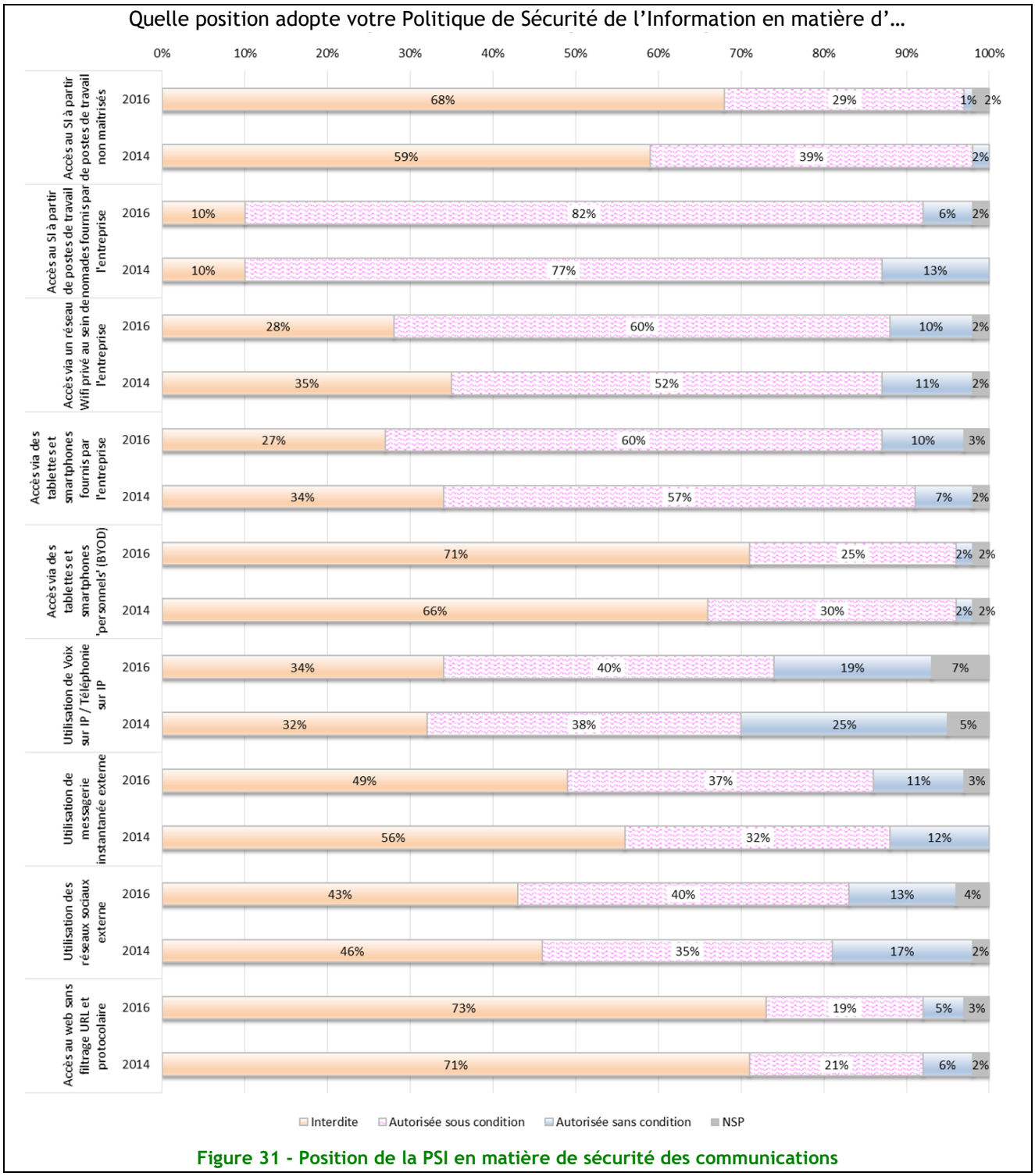


Figure 31 - Position de la PSI en matière de sécurité des communications

Thème 14 : Acquisition, développement et maintenance des Systèmes d'Information

Diminution importante de la mise en place de processus de développement sécurisés

Le nombre d'entreprises utilisant un processus de développement sécurisé à fortement chuté depuis deux ans, passant de 24% à 17% !

Avez-vous mis en place des cycles de développement sécurisés ?

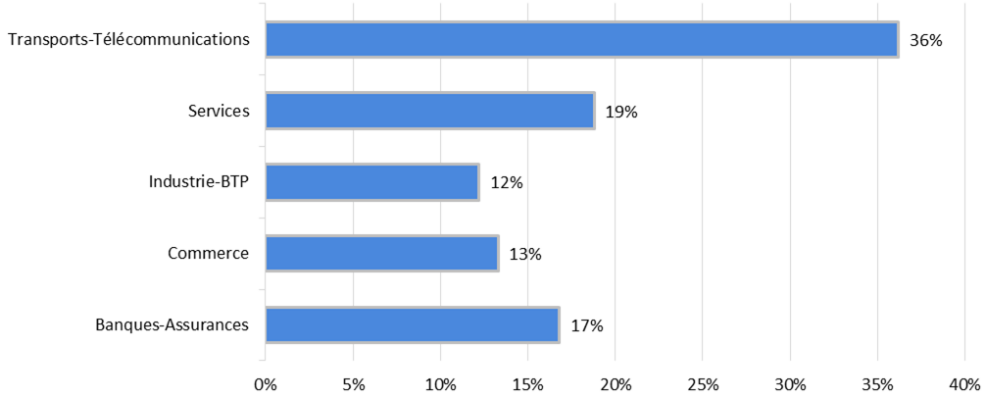


Figure 32 – Entreprises utilisant un processus de développement sécurisé (par secteur d'activité)

Alors que près de la moitié des entreprises (49%) avaient mis en place des bonnes pratiques pragmatiques, elles ne sont plus que 38%.

Il est probable que cette diminution est le miroir de l'augmentation des audits de code et des tests de sécurité (tests de pénétration, test d'intrusion) qui sont pratiqués dans les entreprises. D'autre part, il est à craindre que l'accélération de la digitalisation qui vise à compresser sans cesse le temps de cycle de mise en ligne des nouveaux services soit prioritaire pour les DSI et les métiers par rapport à la prise en compte de la sécurité dans les développements qui est considérée souvent comme un facteur de ralentissement des projets.

L'utilisation de Microsoft SDLC reste stable à 31%.

On constate un fort développement d'OWASP CLASP, passant de 7% à 18% en deux ans, alors que Cigital SDL (1%) et Incas (0%) ont vécu.

Il reste 12% des entreprises qui utilisent d'autres approches, chiffre stable.

Si vous avez mis en place des cycles de développement sécurisés, quelle approche utilisez-vous ?

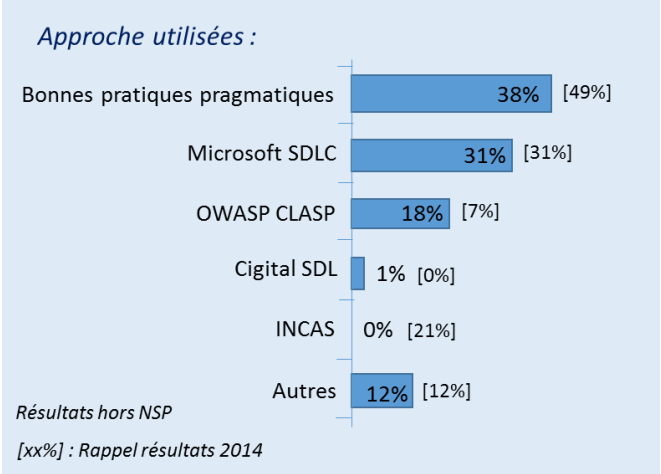


Figure 33 - Mise en place de cycles de développement sécurisés : approches utilisées

Si l'on observe les approches les plus populaires par secteur d'activité, parmi les entreprises qui ont mis en place un processus de développement sécurisé, on trouve :

- pour le secteur banque-assurance, OWASP CLASP à 53%,
- pour le secteur du commerce, 25% utilisent Microsoft SDLC et 25% d'autres approches,
- le BTP utilise des bonnes pratiques pragmatiques à 46%, ainsi que les services à 44%,
- le secteur du transport utilise Microsoft SDLC à 26%.

Thème 15 : Relations avec les fournisseurs

Un recours à l'infogérance stable et un suivi en progression

La part du recours à l'infogérance reste stable depuis 2014, un peu moins de la moitié des entreprises ayant recours à ces prestations. Les grandes entreprises sont plus consommatrices de service d'infogérance, et ce, quel que soit leur secteur d'activité.

Avez-vous placé tout ou partie de votre Système d'Information sous contrat d'infogérance ?

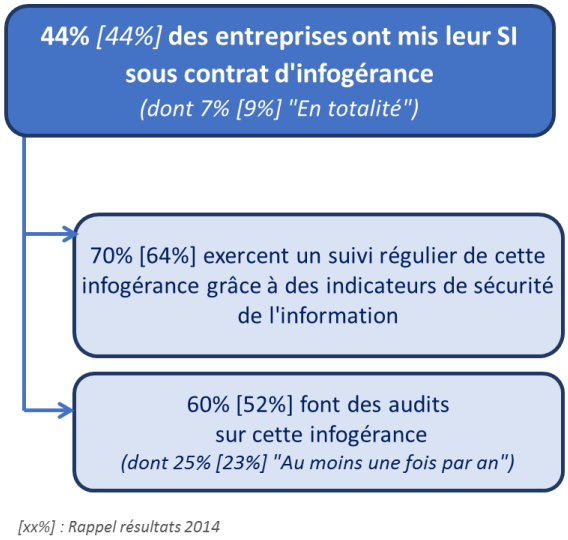


Figure 34 - Mise en infogérance (totale ou partielle) du Système d'Information

Si cette utilisation de l'infogérance reste stable, il est positif de noter une progression dans le suivi de ces activités : désormais 70% des entreprises exercent un suivi régulier et 60% effectuent des audits sur cette infogérance. Il est rassurant de constater qu'une bonne gestion de la relation avec son fournisseur d'infogérance inclut dorénavant un contrôle du niveau de sécurité de la prestation. Ces contrôles ne sont cependant pas effectués de façon homogène dans tous les secteurs d'activité, 41% des entreprises de la Banque-Assurance effectuent par exemple un audit au moins une fois par an contre 13% des sociétés de Transport-Télécommunications.

Le cloud est stable mais son adoption est variable en fonction des entreprises

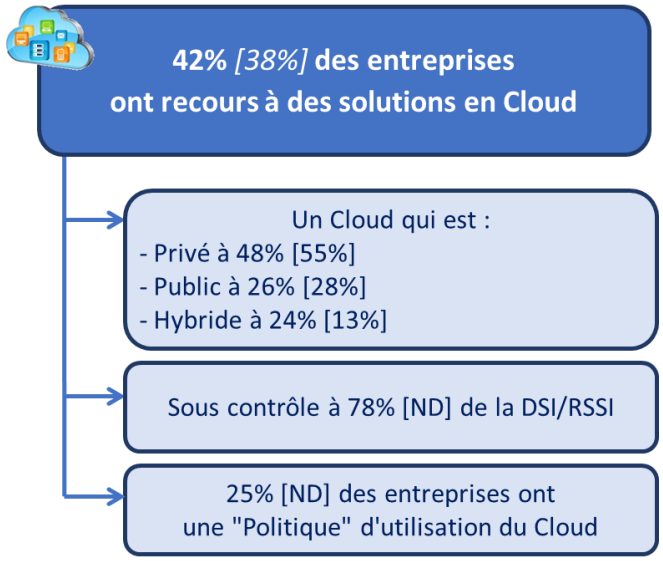
Le taux d'utilisation du Cloud augmente faiblement passant de 38% en 2014 à 42% en 2016, le Cloud privé étant toujours le plus répandu, devant le Cloud public. Le Cloud hybride voit son usage reculer fortement depuis 2014 (passant de 24 à 13%). Peut-être paie-t-il sa réputation d'environnement complexe et coûteux ?

Il est intéressant de constater une diversité dans l'adoption du Cloud en fonction de la taille de l'entreprise (la moitié des grandes entreprises ayant recours à ces services contre à peine plus d'un tiers des entreprises de moins de 500 salariés).

Des différences de maturités quant à l'adoption du cloud sont également identifiées selon les secteurs d'activité : le commerce et les services sont, de loin, les plus gros consommateurs de services Cloud.

Même si la grande majorité des entreprises assure que le Cloud est sous le contrôle de la DSI ou du RSSI, seul un quart des sociétés interrogées dispose actuellement de politique formalisée concernant les règles d'utilisation du Cloud.

Les Directions métiers et/ou les utilisateurs ont-ils recours à des services en Cloud ?



[xx%] : Rappel résultats 2014

Figure 35 - Utilisation des services en Cloud

Thème 16 : Gestion des incidents liés à la sécurité de l'information

Existence d'une cellule de collecte et de traitement des incidents de sécurité

49% des entreprises ne disposent pas d'une cellule de collecte et de traitement des incidents. Cette valeur, en augmentation par rapport à 2014 (45%) montre que la sensibilité à la mise en place d'une procédure de gestion des incidents de sécurité n'est pas encore très mature dans nombre d'entreprises. Seulement 24% des cellules de collecte sont dédiées et 23% sont partagées avec d'autres fonctions.

De façon assez logique, plus l'entreprise est grande, plus elle est organisée pour traiter les incidents (68% des entreprises de plus de 1 000 salariés, contre 46% en moyenne). Dans la même logique ce sont les entreprises de type Banque-Assurance et de Transport-Télécommunication qui sont les mieux dotées ; rien d'étonnant à cela au regard des lois (de type LPM) qui « pèsent » sur elles…

Existe-t-il une cellule de collecte et de traitement des incidents de sécurité de l'information ?

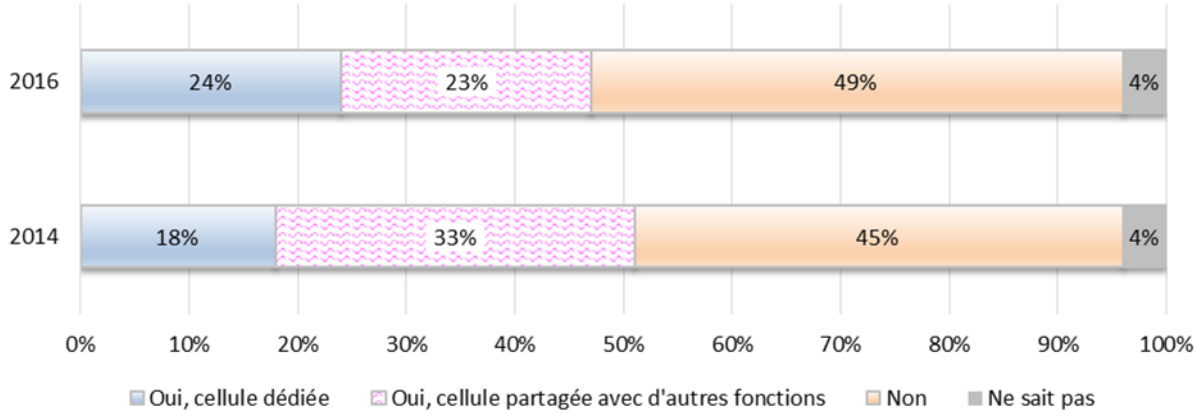


Figure 36 - Organisation de la gestion des incidents

Types d'incidents de sécurité collectés par la cellule

L'informatique de gestion reste en tête des types d'incidents de sécurité les plus collectés même si la proportion diminue cette année 79% contre 82% en 2014.

Durée maximale de résolution d'un incident ayant généré l'arrêt de service le plus long

Les entreprises sont assez réactives dans la réponse des incidents de sécurité de l'information dont ils sont victimes. Les incidents sont résolus dans 58% des cas en moins de 24h ou entre 24h et trois jours dans 12% des cas.

Si vous avez subit des incidents de sécurité de l'information, quelle a été la durée maximale de l'incident ayant généré l'arrêt de service le plus long ?

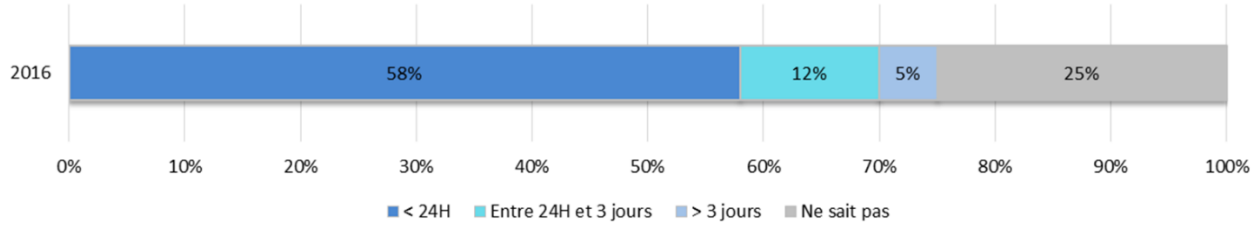


Figure 37 - Durée d'arrêt de service après un incident

Les services et transports-télécommunication comptent la durée maximale de l'incident ayant généré l'arrêt de service le plus long inférieure à 24h avec respectivement 64% et 61%.

Dans 25% des cas, les entreprises ne savent pas estimer la durée d'arrêt de service après un incident. Cela reste une valeur assez conséquente compte tenu des circonstances et on pourrait se demander comment elles font…

Dépôt de plainte suite à des incidents liés à la sécurité de l'information

Même constat que les années précédentes, le dépôt de plainte suite à des incidents de sécurité reste encore très faible, 14% cette année. On peut également noter que seules 4% des Banques-Assurances, pourtant les plus concernées, ont déposé plainte.

Cela peut signifier que les conséquences subies à l'issu de ces incidents ne sont peut-être pas si importantes ou nuisibles pour l'activité.

Les infections par virus en tête des incidents de sécurité

Pour la première fois depuis longtemps, les infections par virus informatiques sont en tête des incidents de sécurité signalés par les entreprises, tandis que vols de matériels et pertes de services essentiels sont en net recul.

La présence de systèmes de détection anti-virus étant stable depuis longtemps et généralisée, il est possible que cette évolution de la perception des incidents soit liée aux vagues importantes de rançongiciels – très visibles par nature – qui frappent de plus en plus les entreprises et pas uniquement les particuliers, notamment les cryptolockers.

Au cours de l'année 2015, votre organisme a-t-il subi des incidents de sécurité de l'information consécutifs à…

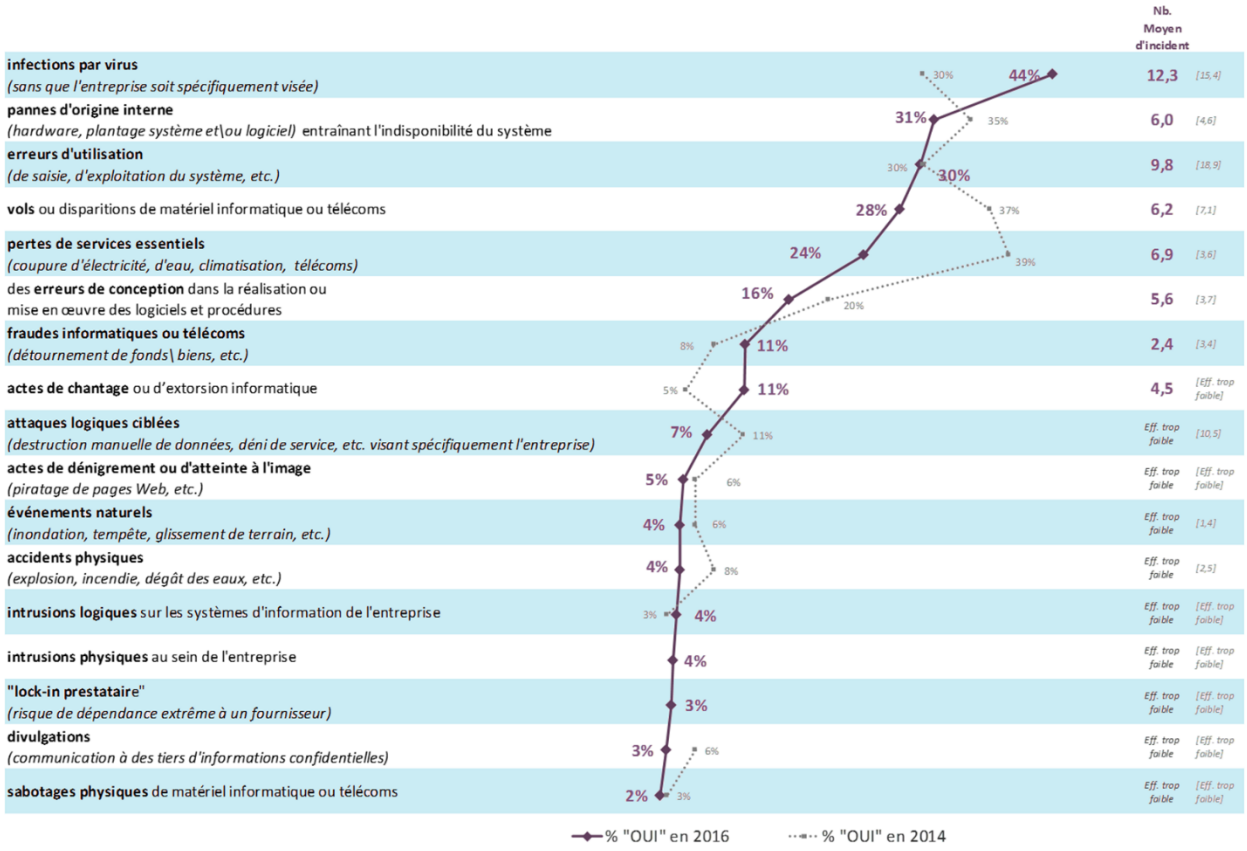


Figure 38 – Recensement des incidents de sécurité par les entreprises

Les entreprises ont été confrontées cette année à une nouvelle question, permettant de mesurer leur exposition aux risques évoqués lors du dernier Panorama de la Cybercriminalité présenté par le CLUSIF en janvier 2016. Ainsi, au cours de l'année 2015, le hameçonnage (phishing) concerne 42% des entreprises, viennent ensuite les rançons et fraudes au président (26%) et les fraudes aux moyens de paiement (23%). Toutefois, même si elles y sont beaucoup confrontées, pour beaucoup d'entre elles ces incidents n'ont pas entraîné de conséquences notables car elles y sont préparées.

Une progression de l'activation des polices d'assurance

Parmi les entreprises qui ont subi un incident et en ont évalué le préjudice financier, le nombre de celles qui fait appel à sa police d'assurance a doublé par rapport à 2014 (passant de 6 à 12%), tandis que le recours à la trésorerie est en net recul (passant de 33 à 18%). 26% des entreprises consultées ont une police d'assurance prenant en compte la valeur des informations altérées, perdues ou volées (34% parmi les banques et assurances).

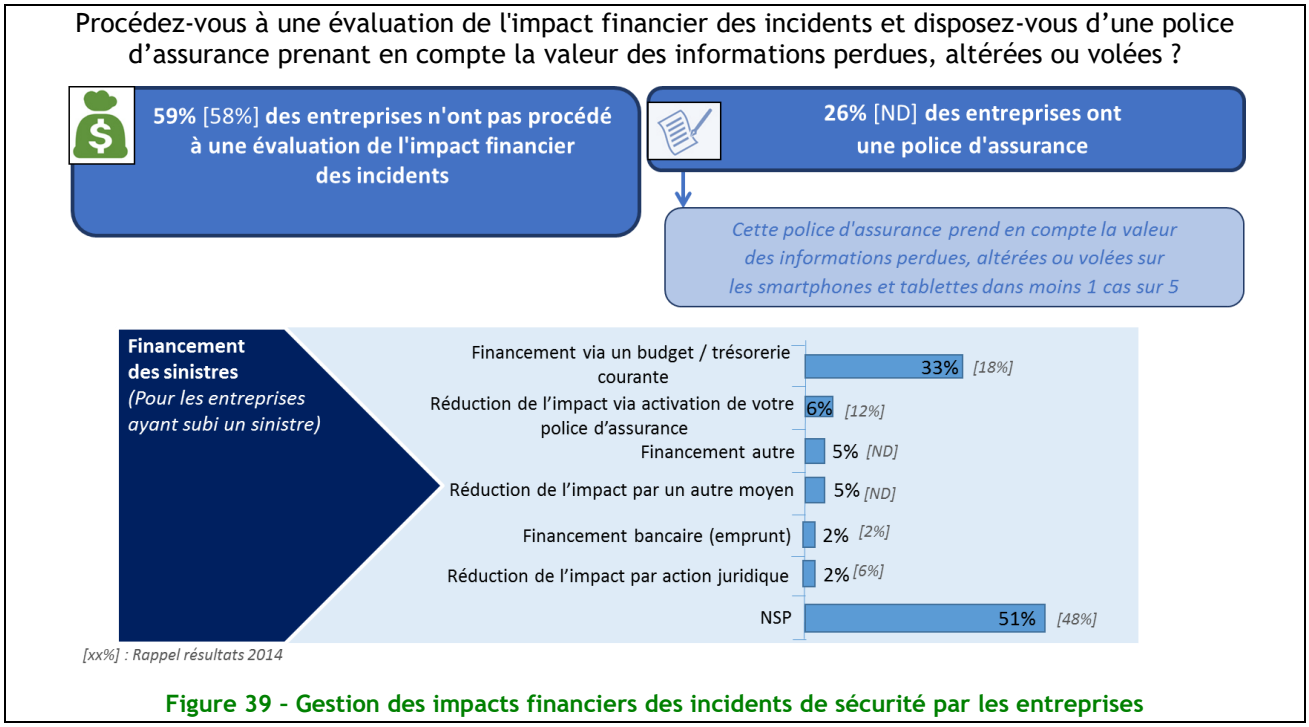


Figure 39 – Gestion des impacts financiers des incidents de sécurité par les entreprises

Thème 17 : Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité

Le nombre d'entreprises qui ont un processus de Continuité d'Activité diminue légèrement, passant de 73% en 2014 à 70% en 2016, mais cela reste dans la tendance si l'on se fonde sur les études depuis 2012 (69%).

Concernant les systèmes informatiques de gestion, le secteur des Services est celui prenant le plus en compte leur indisponibilité (69%) tandis que les Transports-Telecom les délaissent sensiblement plus (41%).

On constate une grande différence de traitement de l'indisponibilité des locaux entre le secteur des Banques-Assurances (70%) et le secteur Transports-Telecom (29%).

Par ailleurs, il est à noter que les entreprises semblent plus se préoccuper de l'indisponibilité d'un fournisseur essentiel dont la couverture passe en 2 ans de 18% à 25%, rétablissant le score observé en 2012 (26%). Sur ce point, le secteur des Industries-BTP se trouve en retrait, seules 18% d'entre elles s'en préoccupent.

On note une baisse relative de la couverture de l'indisponibilité de l'informatique industrielle, passant de 32% à 28%.

La gestion de la continuité d'activité dans votre entreprise couvre-t-elle les scénarios suivants ?

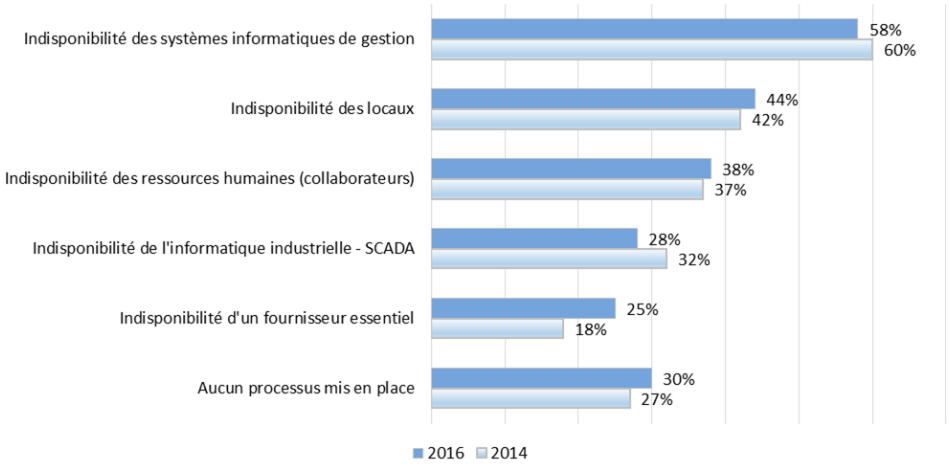


Figure 40 - Scénarios couverts par la gestion de la continuité d'activité

On constate une baisse importante de la prise en compte des exigences « Métiers ». La chute est de 5 points (60% en 2016 contre 65% en 2014 et 37% n'ayant rien réalisé contre 30%) ce qui vient dégrader la bonne progression observée en 2014 (progression de 12 points). Le secteur des Banques-Assurances reçoit la palme d'or, 80% d'entre-elles ayant évalué les exigences « Métiers ».

Avez-vous évalué les exigences « Métiers » en termes de Délai Maximal d'Interruption Admissible (DMIA ou RTO) et de Perte de Données Maximale Admissible (PDMA ou RPO) dans le cadre d'un BIA (Bilan d'Impact sur l'Activité) formel ?

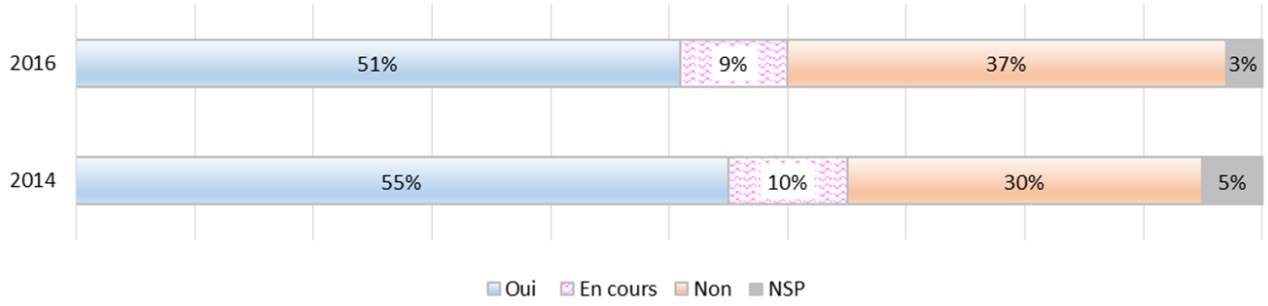


Figure 41 - Identification des RTO / RTO au travers d'un BIA

Les exercices utilisateurs sont globalement en très légère baisse (notamment dans les exercices annuels). Encore un quart des entreprises n'en font jamais (même proportion qu'en 2014 et 2012). Sur ce dernier point, on constate un écart important entre le secteur des Transports-Telecom où 32% ne font jamais de tests et le secteur des Banques-Assurances où seulement 11% n'en font jamais.

À quelle fréquence les plans de continuité d'activité sont-ils testés par les utilisateurs désignés dans le cadre de l'activation du PCA ?

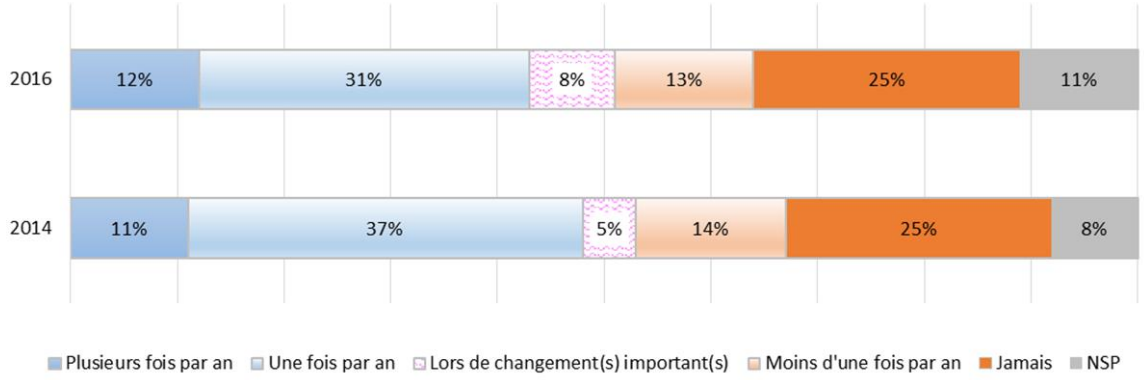


Figure 42 - Fréquence de réalisation des tests par les utilisateurs désignés dans le cadre de l'activation du PCA ?

On constate une stabilisation de la fréquence de tests des plans de continuité/reprise d'activité informatiques. Le secteur des Banques-Assurances étant là encore le bon élève du groupe avec seulement 4% d'entre eux qui ne les testent jamais contre une moyenne générale de 23%.

À quelle fréquence les plans de continuité / reprise d'activité informatiques sont-ils testés ?

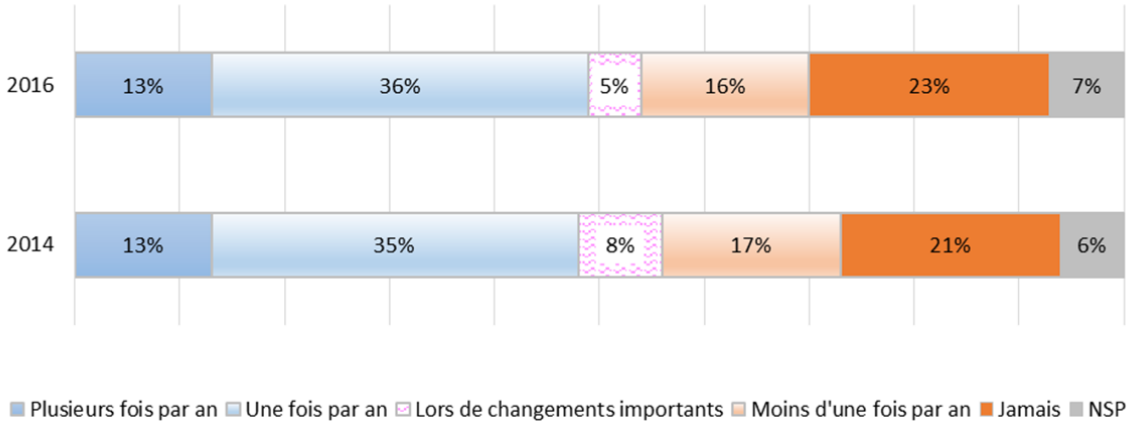


Figure 43 - Fréquence de réalisation des tests des plans de continuité / reprise d'activité informatiques

Cette année encore, 59% des entreprises couvrent par des tests de 75 à 100% de leurs solutions mises en œuvre ce qui est très positif d'autant que l'on constate une progression concernant le taux de couverture à 100% (27% en 2016 contre 19% en 2014). Le secteur du Commerce, en très forte progression, est devenu le bon élève avec 43% d'entre eux couvrant 100% des solutions en place, au contraire des Industries-BTP (seulement 18%).

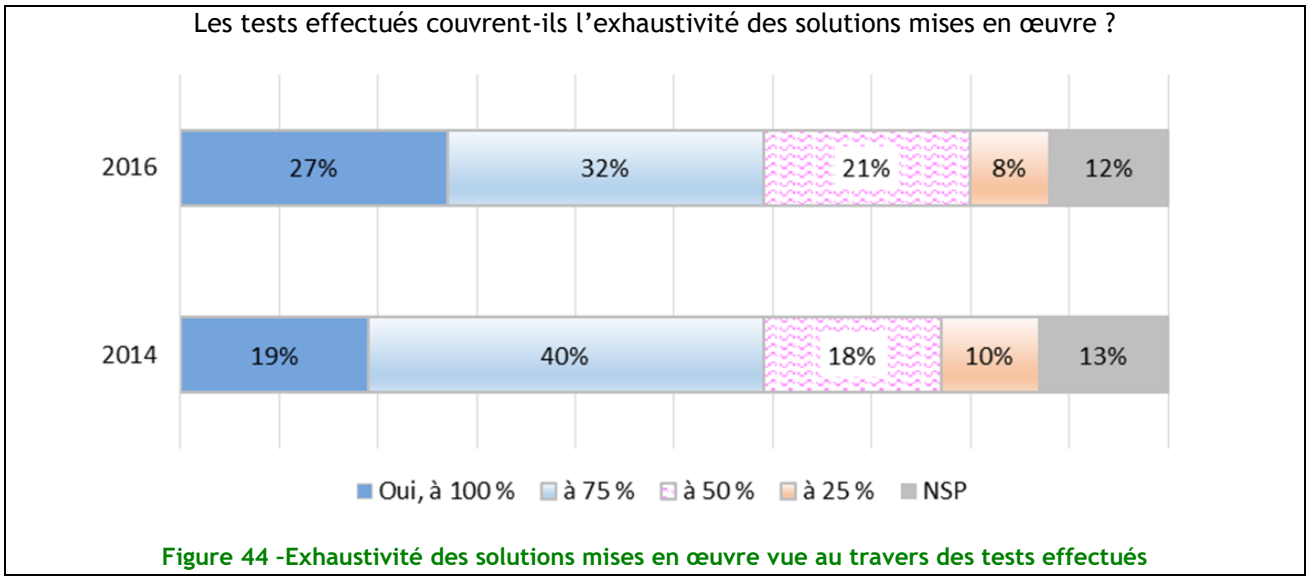


Figure 44 -Exhaustivité des solutions mises en œuvre vue au travers des tests effectués

Au niveau de la gestion de crise, bien que l'on constate une légère augmentation des différents dispositifs mis en place (notamment la salle de gestion de crise équipée : 21% contre 14%), seulement 56% des entreprises possèdent une gestion de crise formalisée, ce qui reste faible malgré, là aussi, une augmentation par rapport aux données de 2014.

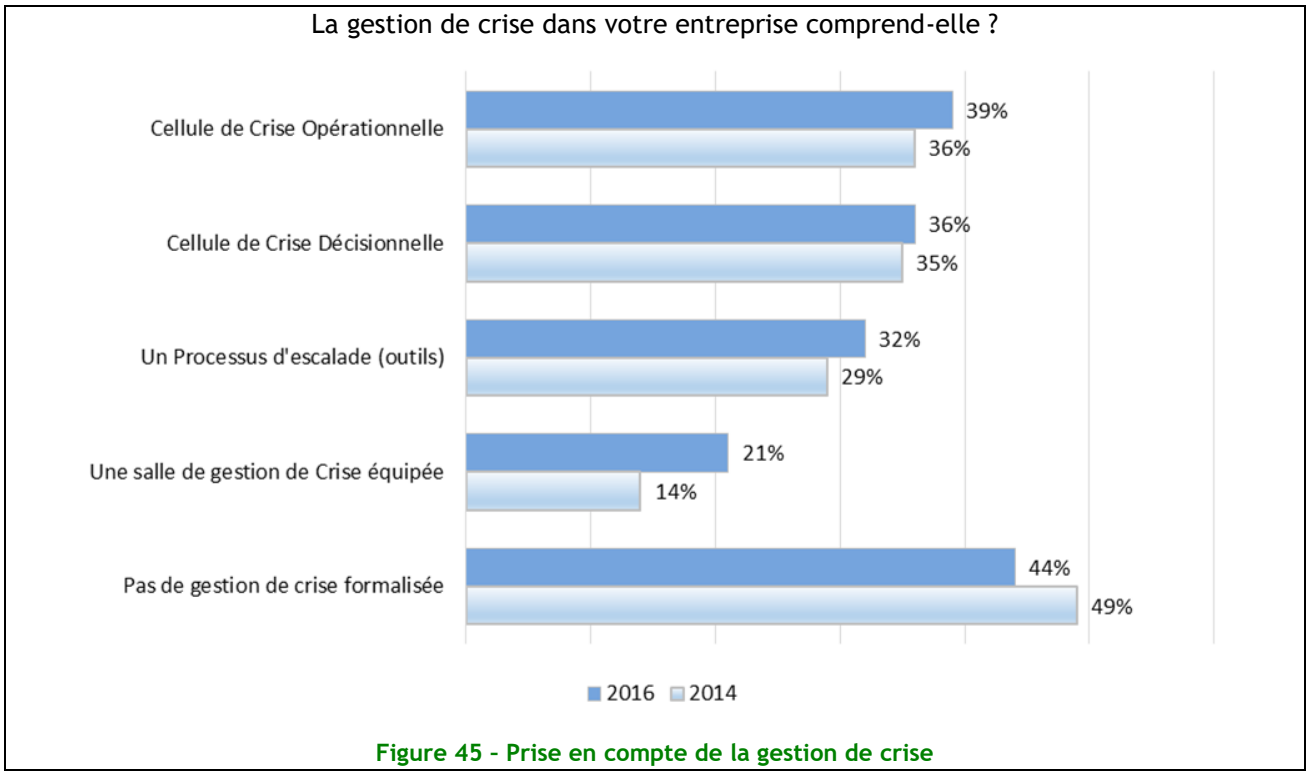


Figure 45 - Prise en compte de la gestion de crise

Thème 18 : Conformité

Ce thème aborde les éléments liés à la conformité sous trois aspects :

- la conformité avec la Loi Informatique et Libertés,
- les audits de sécurité,
- l'utilisation de tableaux de bord.

Conformité avec la Loi Informatique et Libertés

La déclaration des traitements à la CNIL est toujours assurée en majorité par le DSI (26%), puis de manière presque équivalente, par le CIL (19%), le service RH (17%) et le service juridique (15%).

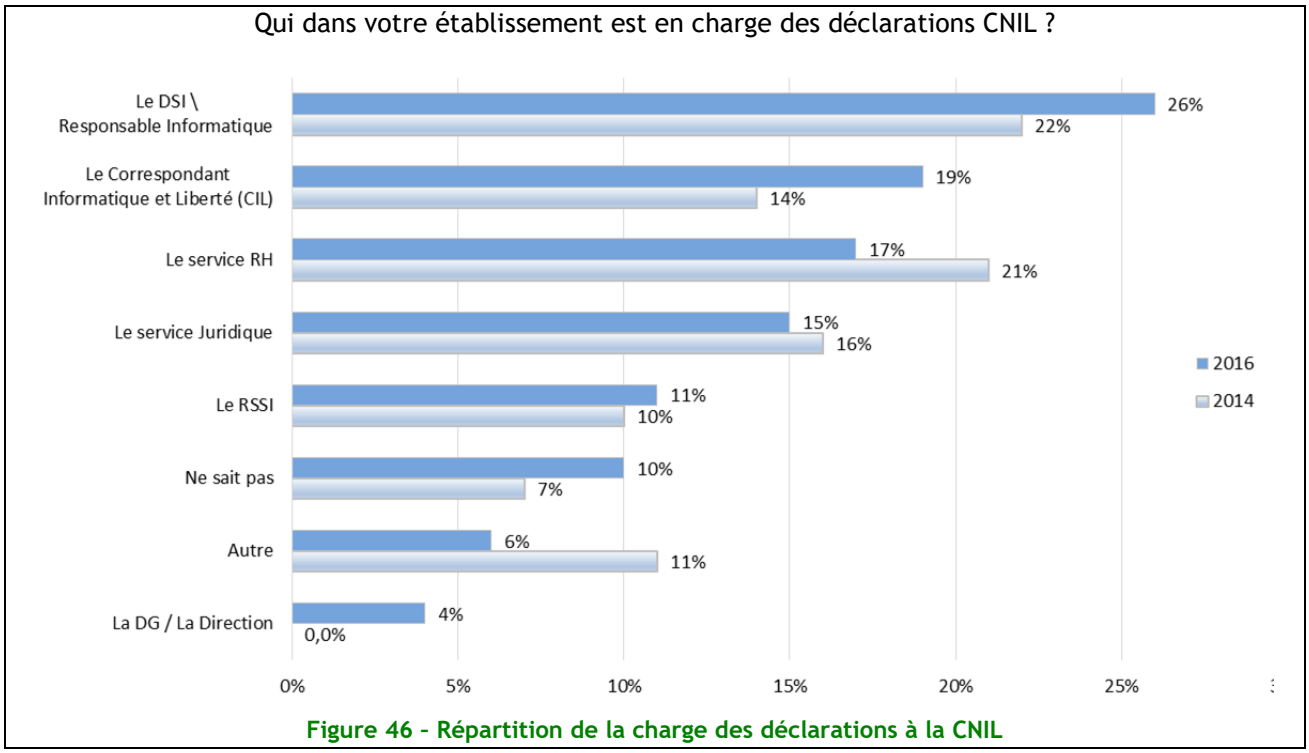


Figure 46 – Répartition de la charge des déclarations à la CNIL

On note toujours des disparités importantes selon les secteurs d'activité, par exemple pour le CIL (38% dans la Banque-Assurance mais seulement 14% dans le secteur Industrie-BTP et 11% dans le commerce).

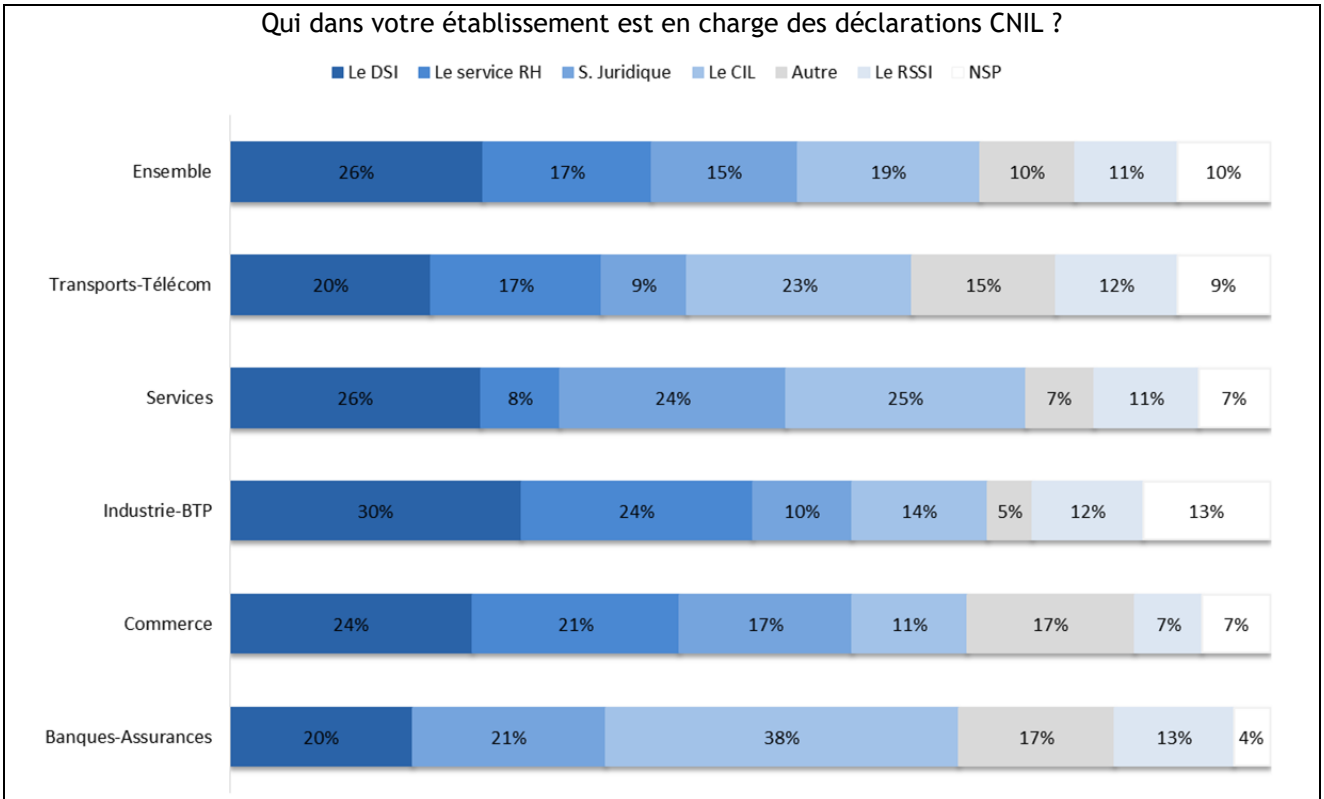


Figure 47 – Répartition de la charge des déclarations à la CNIL selon le secteur d'activité

La différence est d'ailleurs surtout liée à la taille des entreprises, le CIL étant cité à 45% pour les entreprises de plus de 1 000 salariés, contre 20% entre 500 et 1 000 personnes, et seulement 12% en dessous de 500. Dans les petites structures, où il n'y a souvent pas de CIL, c'est le DSI qui se charge des déclarations (31%).

Dans les grandes entreprises, il reste toutefois surprenant que le CIL ne soit pas cité plus souvent, d'autant plus que le Règlement Européen sur la protection des données personnelles va rendre cette fonction obligatoire dans de nombreuses entreprises à partir du 25 mai 2018.

Les audits de sécurité

Près des deux-tiers des entreprises ont réalisé un audit de sécurité au cours des deux dernières années, reflétant une relative stabilité dans le temps.

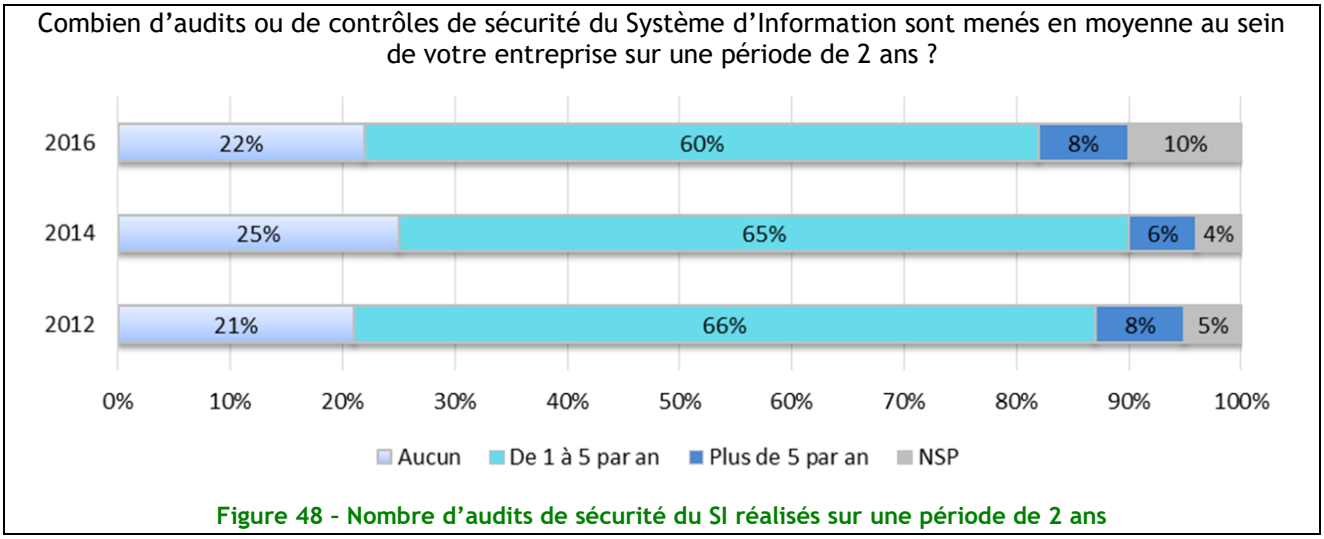


Figure 48 – Nombre d'audits de sécurité du SI réalisés sur une période de 2 ans

Les grandes entreprises pratiquent les audits de façon quasi systématique (84% contre 68% en moyenne). Le secteur Banques-Assurances est également le plus consommateur de ce type de prestation (79%).

Les audits réalisés portent essentiellement sur les tests d'intrusion (42%) et l'architecture (41%). Viennent ensuite les audits organisationnels (34%) et les audits de configuration (31%), puis les audits physiques (27%) et les audits de continuité d'activité (26%).

En ce qui concerne les motivations de ces audits, on observe une évolution sensible par rapport aux enquêtes de 2014 et 2012. De manière surprenante, 30% des personnes interrogées « ne savent pas » quelle est la motivation des audits, alors qu'elles n'étaient que 9% lors des précédentes enquêtes.

Parmi celles qui ont répondu, le respect de la PSSI augmente sensiblement (57%) au détriment des audits externes (29%) et des projets sensibles (17%). Les exigences contractuelles ou règlementaires restent la seconde motivation (35%).

Chez les grandes entreprises, c'est le respect de la PSSI qui est la motivation majeure (72%), bien plus que dans les entreprises de moins de 500 salariés (51%).

En revanche, dans le secteur des Banques-Assurances, ce sont les exigences règlementaires qui motivent majoritairement les audits (70%).

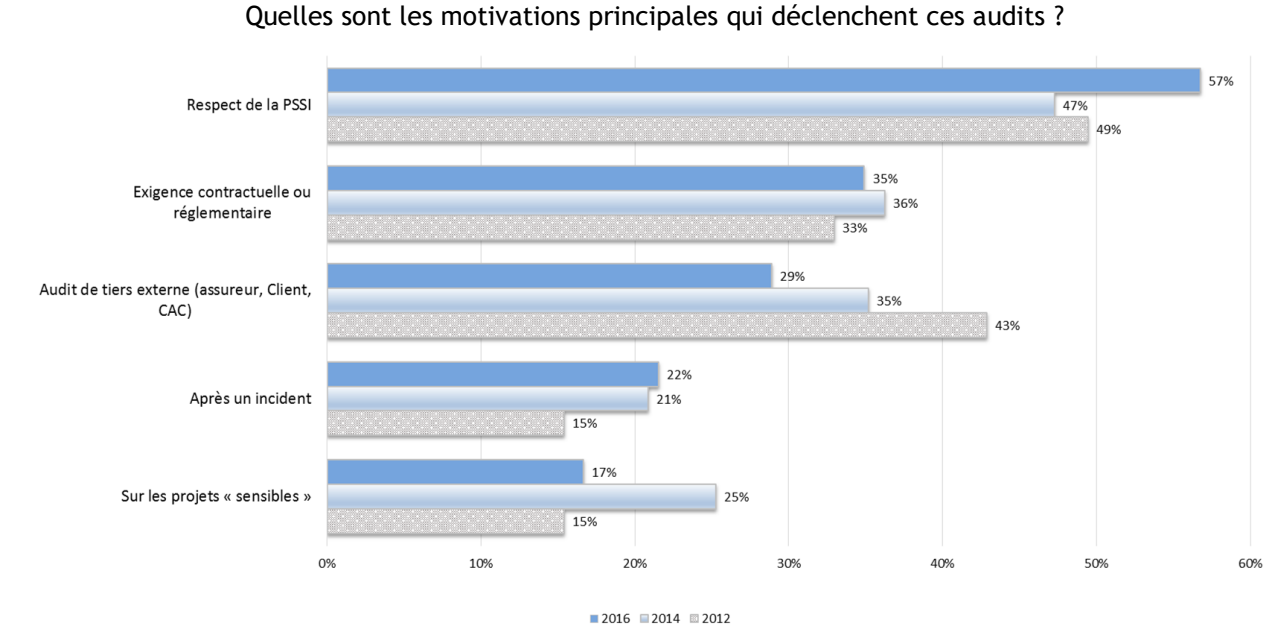


Figure 49 – Motivations déclenchant les audits de sécurité

Utilisation de tableaux de bord de sécurité

L'utilisation de tableaux de bord reste très largement absente, une majorité d'entreprises (67%) indiquant ne pas en avoir mis en place. Si cette pratique avait sensiblement augmenté en 2014 (25% contre 15% en 2012), l'enquête de cette année ne montre pas d'évolution.

Votre entreprise a-t-elle mis en place des indicateurs et/ou un tableau de bord de la sécurité de l'information (TBSSI) ?

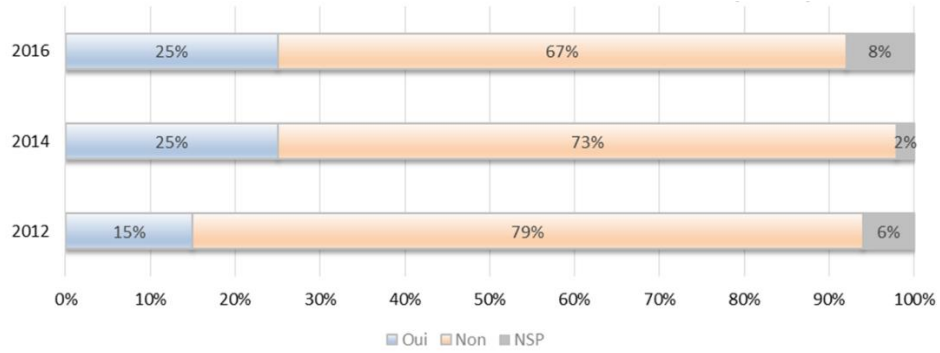


Figure 50 – Mise en place de tableaux de bord de la sécurité de l'information

Les entreprises qui ont mis en place des tableaux de bord, suivent en moyenne 5 indicateurs.

On note cette année une augmentation sensible du rôle de pilotage des indicateurs pour la SSI (43%) tandis que leur vocation opérationnelle reste la motivation principale (62%). L'intérêt des Directions Générales ne représente que 20% de l'usage des tableaux de bord, en net retrait par rapport à 2012 où il était cité par 37% des entreprises.

Quels sont les types d'indicateurs et/ou de tableau de bord de la sécurité de l'information (TBSSI) ?

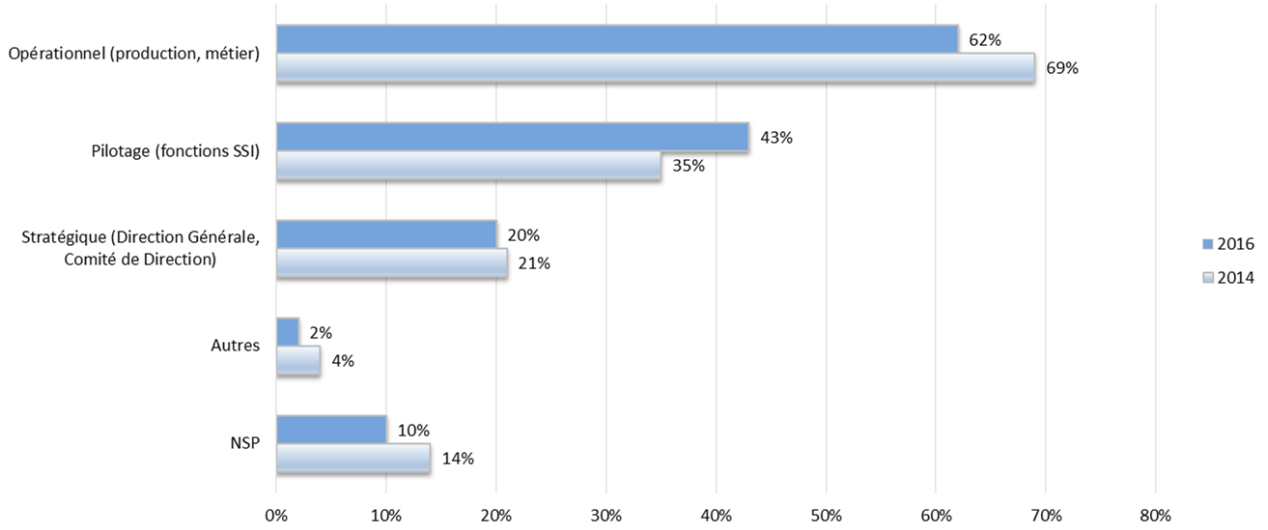


Figure 51 – Types d'indicateurs ou de tableaux de bord

Comme cela était déjà souligné en 2012 puis en 2014, les RSSI doivent certainement considérer que l'information des Directions Générales exige d'être fortement améliorée.

Comme par le passé, les indicateurs de nature technique sont cités en priorité (taux de disponibilité, incidents, vulnérabilités détectées, taux de mise à jour). Les indicateurs d'organisation restent importants, mais en baisse sensible par rapport à 2014 : avancement des projets de sécurisation (en baisse de 50% à 39%), conformité avec la PSI (en baisse de 50% à 38%),

Quels sont les types d'indicateurs que vous suivez dans ce tableau de bord ?

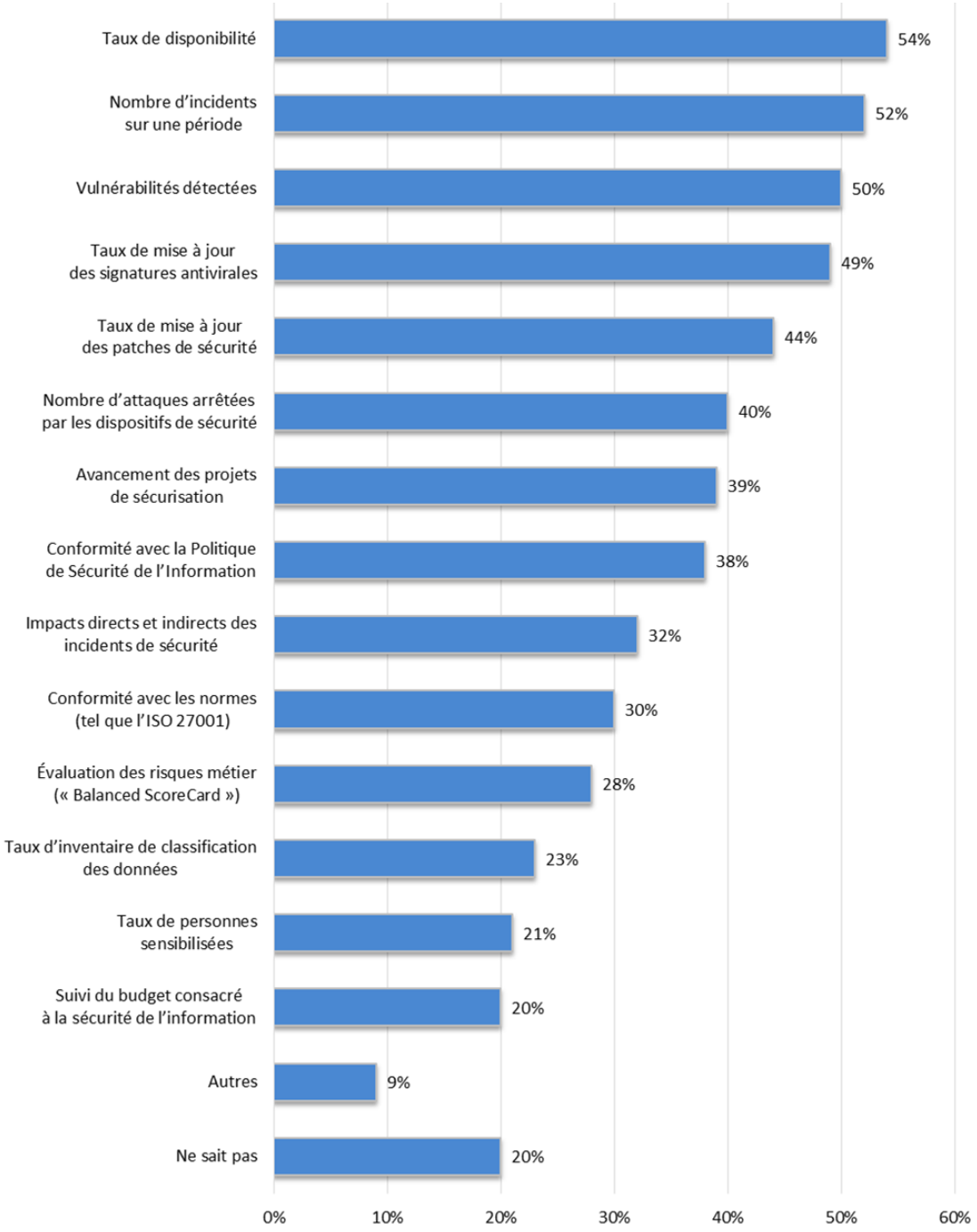


Figure 52 – Indicateurs suivis dans le tableau de bord

Collectivités Territoriales

- Présentation de l'échantillon
- Dépendance à l'informatique des collectivités territoriales
- Moyens consacrés à la sécurité de l'information par les collectivités territoriales
- Thème 5 : Politique de sécurité de l'information
- Thème 6 : Organisation de la sécurité de l'information
- Thème 7 : Sécurité des ressources humaines
- Thème 8 : Gestion des actifs
- Thème 9 : Contrôle d'accès
- Thème 10 : Cryptographie
- Thème 11 : Sécurité physique et environnementale
- Thème 12 : Sécurité liée à l'exploitation
- Thème 13 : Sécurité des communications
- Thème 14 : Acquisition, développement et maintenance des Systèmes d'Information
- Thème 15 : Relations avec les fournisseurs
- Thème 16 : Gestion des incidents liés à la sécurité de l'information
- Thème 17 : Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité
- Thème 18 : Conformité

Les Collectivités Territoriales

Présentation de l'échantillon

Une analyse globale qui doit toujours être relativisée par des disparités de pratiques entre les différents profils de collectivités.

La cible de l'enquête 2012 a été reprise pour comparer les progrès ou les éventuelles régressions en termes de sécurité de l'information au sein des Collectivités Territoriales. Depuis la dernière enquête, un certain nombre de réformes ont légèrement changé la structure des intercommunalités – changement de seuil des Communautés de Communes ou d'Agglomération, élargissement du nombre de Communautés Urbaines et création de Métropole. Les Conseils Départementaux et Régionaux ont été regroupés sous le terme plus générique de Conseils Territoriaux, le poids de Région dans l'échantillon étant amené à diminuer avec la réforme mise en place en janvier 2016.

La cible est constituée des Collectivités Territoriales suivantes :

- les communes de plus de 30 000 habitants,
- les intercommunalités, à savoir :
  - les Communautés de Communes de plus de 10 000 habitants,
  - les Communautés d'Agglomération, Communautés Urbaines et les Métropoles,
- les Conseils Territoriaux, qui regroupent les Régions et les Départements.

Sur plus de 1260 collectivités de France métropolitaine interrogées, 203 ont répondu à la sollicitation du CLUSIF, soit un taux d'acceptation d'environ 16 %. Ce résultat est satisfaisant et nous permet de considérer que l'échantillon de la cible est représentatif.

Pour construire l'échantillon interrogé, la méthode des quotas a été utilisée. Un redressement a été effectué de manière à ce que la répartition par catégorie des répondants corresponde avec la réalité des collectivités françaises.

En 2012, les données des Communautés de Communes, des Communautés d'Agglomération et Urbaines étaient regroupées en une seule catégorie dénommée « Communautés ». Quand cela était pertinent pour permettre la comparaison, les données 2016 ont été agglomérées sur cette même catégorie. Le découpage 2016 permet de mettre en exergue une disparité des réponses entre les Communautés de Communes et les autres formes de Communauté. Il est important de considérer que les Communes et les Communautés de Communes les plus petites délèguent la gestion de leur informatique à des structures départementales dans des syndicats informatiques.

	Echantillon CLUSIF	%	Redressement	Données nationales
Communes de plus de 30 000 habitants	63	31 %	⇨	15 %
Communautés de communes de plus de 10 000 habitants	77	38 %	⇨	62 %
Communautés d'agglomération, urbaines et métropoles	41	20 %	⇨	16 %
Conseils territoriaux (Départements & Régions)	22	11 %	⇨	7 %
Total	**203**	**100 %**	⇨	**100 %**

Au sein de chaque Collectivité, nous avons cherché à interroger en priorité le Responsable de la Sécurité des Systèmes d'Information (RSSI). Celui-ci a répondu pour 20 % en moyenne, c'est un chiffre légèrement

supérieur à la précédente enquête. Dans près d'un cas sur 2, le répondant est attaché à la Direction Informatique.

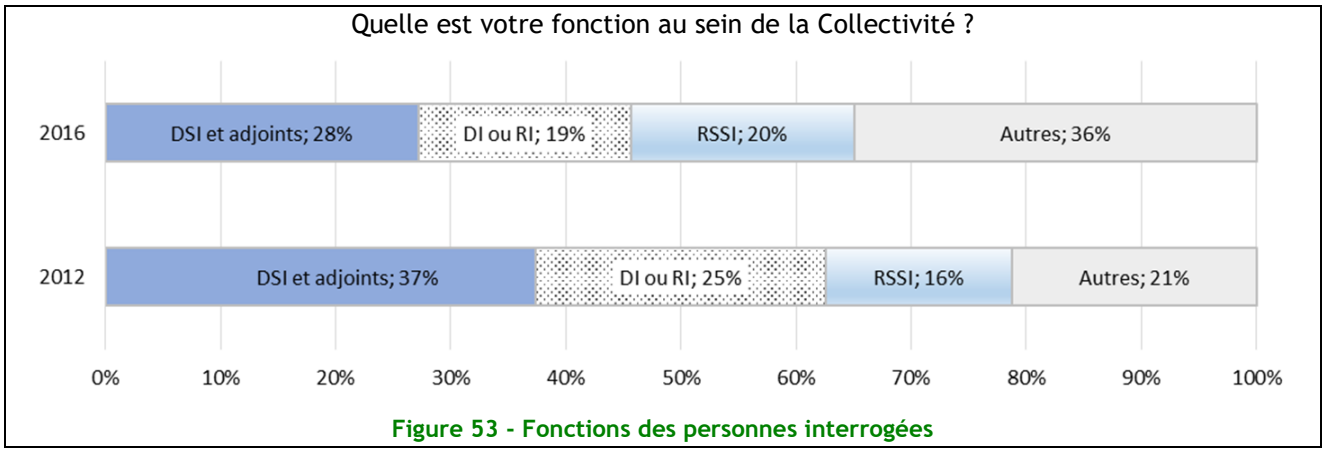


Figure 53 - Fonctions des personnes interrogées

Cette année encore, l'analyse détaillée des réponses fait apparaître des pratiques inégales entre les différents profils de Collectivités. Ainsi, si le répondant est un RSSI dans 40% des cas pour les Conseils Territoriaux, ce chiffre descend à 15% pour les Villes et les Communautés de Communes.

Sentiment de dépendance à l'informatique

Une perception de la dépendance à l'informatique et au numérique qui s'accroit de plus de 7 points depuis 2012

Les Collectivités Territoriales ont pris le virage du numérique avec la dématérialisation des échanges avec les citoyens et avec leurs partenaires (flux comptables, marchés dématérialisés, contrôle de légalité). La conscience d'une dépendance à l'informatique est encore plus marquée pour les Conseils Territoriaux, passant de 60% à plus de 82%.

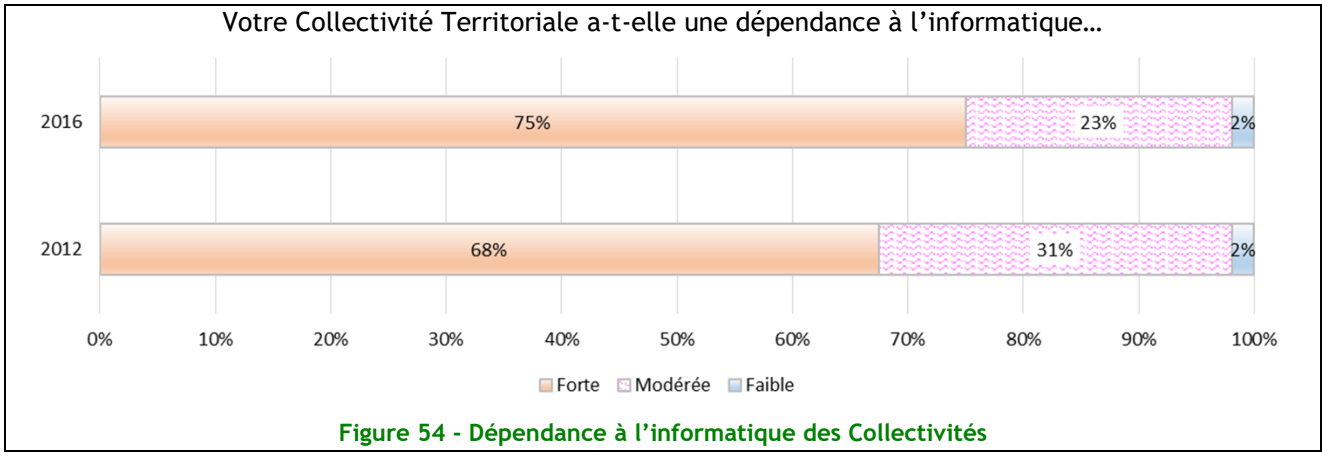


Figure 54 - Dépendance à l'informatique des Collectivités

Moyens consacrés à la sécurité de l'information par les collectivités

Des budgets très disparates en fonction de la taille et des compétences attribuées aux collectivités

66% des collectivités ont accepté de révéler le montant de leur budget informatique. Comme les années précédentes, **les budgets sont d'une très grande disparité et varient d'un rapport 1 à 100** : en moyenne 5,8 M€ pour les Conseils Territoriaux, 1 M€ pour les Communautés d'Agglomération/Urbaines et Métropoles, 800 K€ pour les Villes et moins de 60 K€ pour les Communautés de Communes.

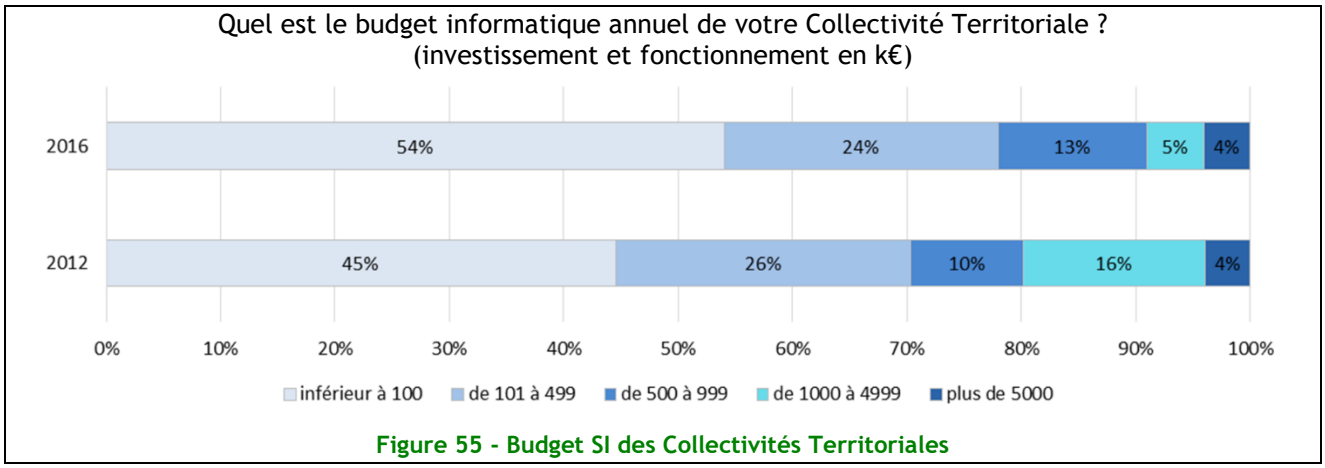


Figure 55 - Budget SI des Collectivités Territoriales

Un budget informatique qui participe moins à la sécurité

Le budget sécurité reste difficile à évaluer. Sur le nombre de Collectivité qui ont identifié une ligne budgétaire propre à la sécurité de l'information, sa part dans le budget informatique diminue assez fortement.

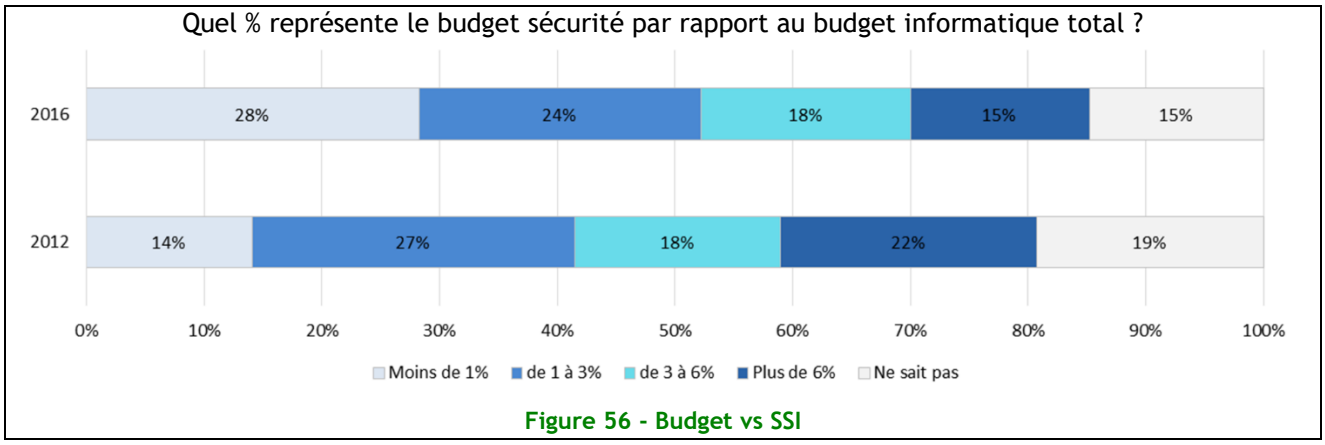


Figure 56 - Budget vs SSI

La sécurité, un budget en régression depuis 2012

Globalement, les **difficultés budgétaires touchent également les Collectivités**. Ainsi, seul 18% des collectivités interrogées voient leur budget dédié à la sécurité progresser (-10% pt) ; dans le même temps pour une grande majorité (67%) la part alloué à la sécurité reste « constante ».

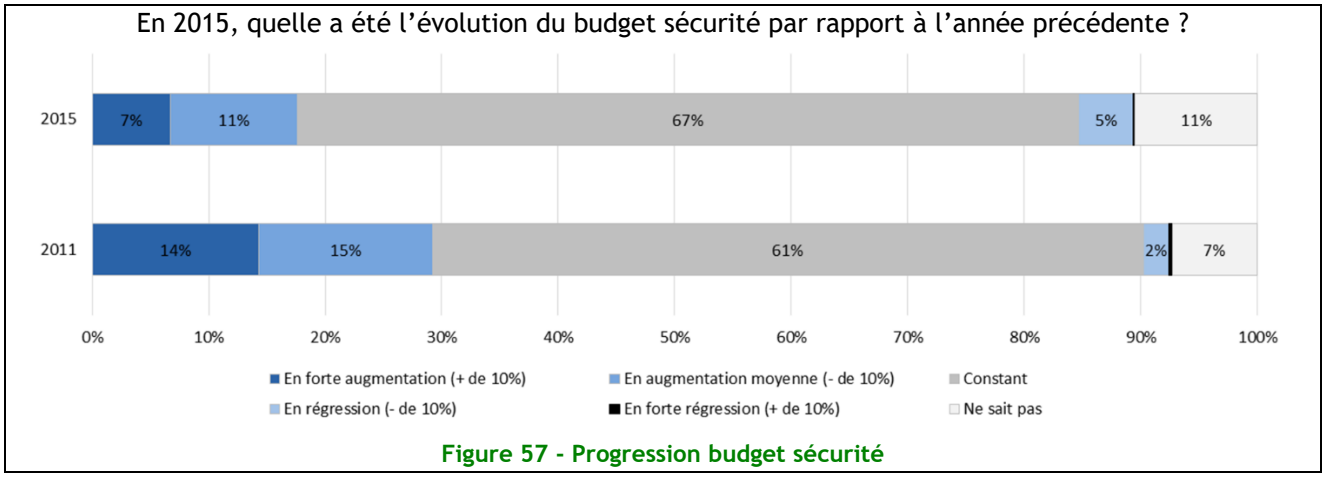


Figure 57 - Progression budget sécurité

Le poste budgétaire pour la mise en place de solutions toujours en première place.

Corolaire du tarissement des budgets, les principaux postes budgétaires augmentent moins qu'il y a 4 ans. **La hiérarchie des investissements ne change pas pour autant**. Le principal poste reste pour la mise en place de solutions. Il est satisfaisant de constater que les efforts en termes organisationnels et de sensibilisation restent proportionnellement importants.

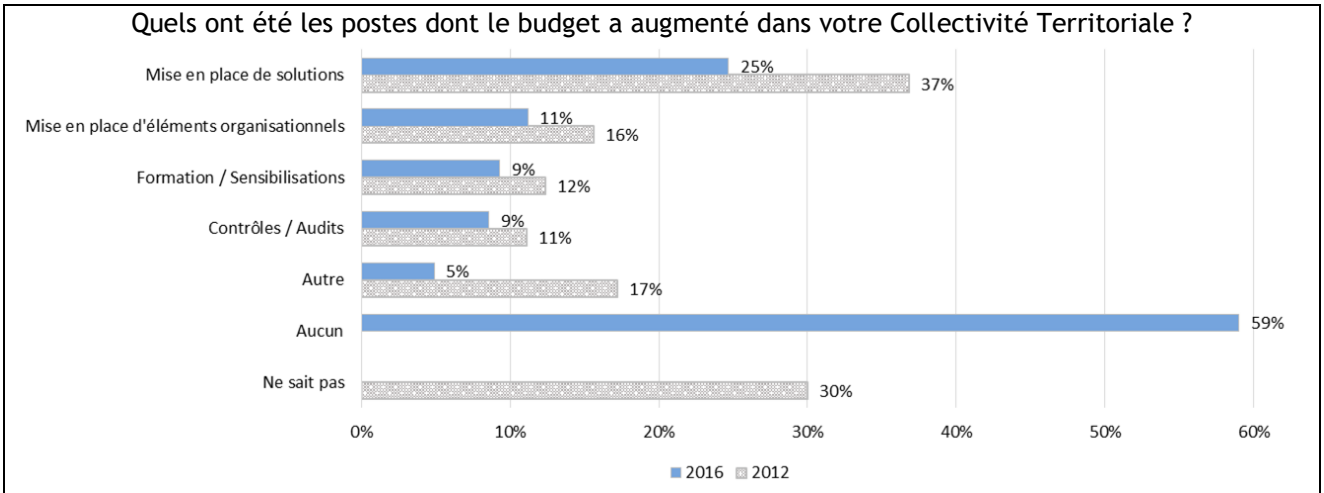


Figure 58 - Evolution du budget en fonction des postes

Principal frein à la conduite des missions de sécurité : le manque de personnel qualifié

En 2016, le principal frein reste **le manque de personnel qualifié**, même si le manque de budget se fait durement ressentir puisqu'il vient juste derrière à 2 points.

Si le manque de budget est globalement partagé, le manque de personnel qualifié et de connaissance se font particulièrement ressentir dans les Communautés de Communes.

Près d'une personne interrogée sur 3 se plaint de contraintes organisationnelles et près d'une sur 4 doit faire face aux réticences de la Direction Général, des métiers ou des utilisateurs. Ces freins sont moindres dans les Communautés de Communes (respectivement 22% et 17%) qui ont majoritairement des organisations moins verticales.

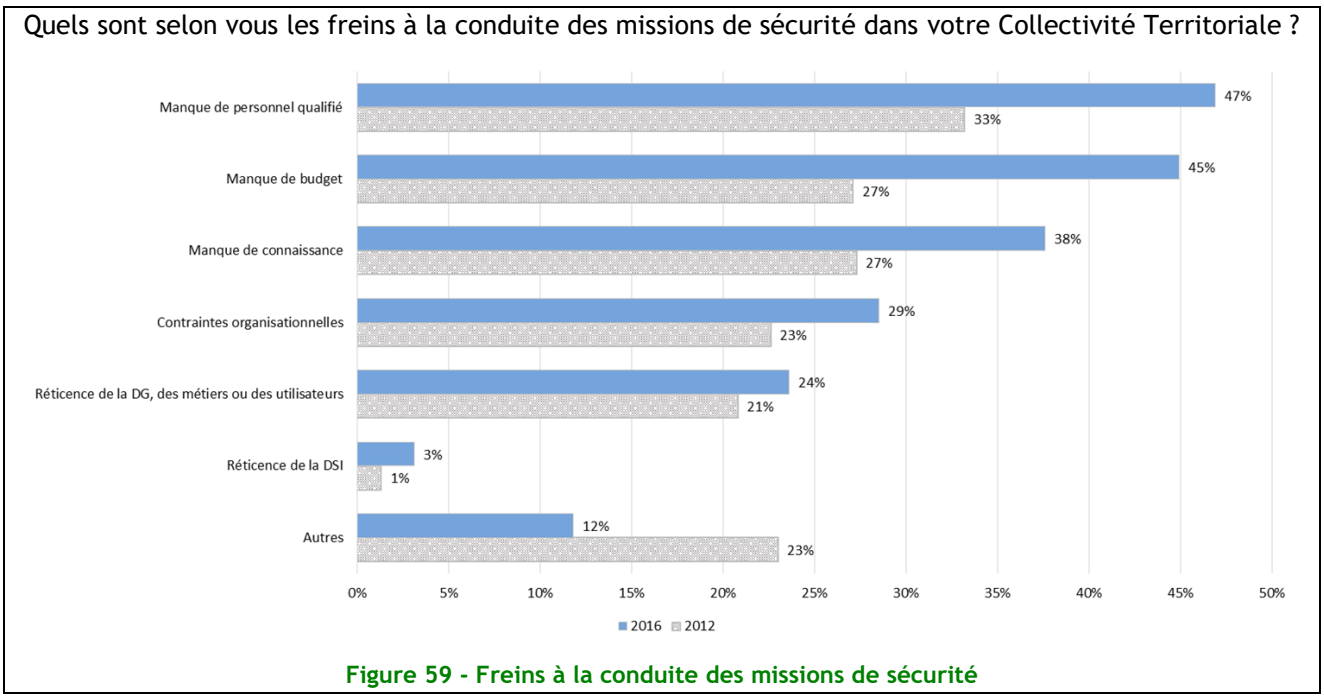


Figure 59 - Freins à la conduite des missions de sécurité

Thème 5 : Politique de sécurité de l'information

La formalisation de la politique de sécurité (PSI) progresse… sauf dans les Communautés

Bien que la moyenne n'ait pas progressé depuis 2012, cela n'est qu'une apparence due au fort poids des Communautés de Communes dans l'échantillon. Un peu plus de 2 Communautés de Communes sur 10 et un peu moins de 4 Communautés d'Agglomération, Urbaines ou Métropoles sur 10 ont formalisé une PSI. Plus de la moitié des Villes et des Conseils Territoriaux ont aujourd'hui formalisé une PSI. Quand elle est formalisée, **cette PSI est soutenue à 90% par la Direction Générale**. Pour pratiquement 6 Collectivités sur 10, la PSI a été conçues ou mise à jours depuis moins d'un an et 2 sur 10 depuis moins de 3 ans.

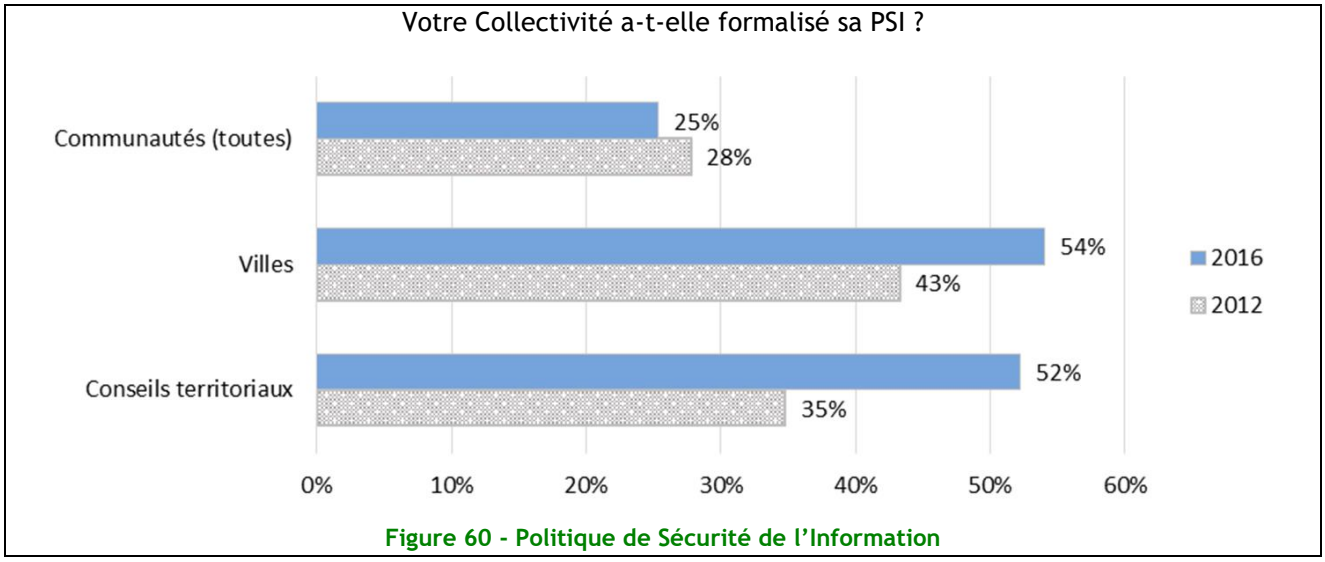


Figure 60 - Politique de Sécurité de l'Information

Un lien étroit entre la formalisation de la PSSI et l'existence d'un RSSI au sein de la collectivité

Quel que soit le profil de Collectivité, il semblerait qu'il existe un lien étroit entre la présence d'un RSSI/RSI et la formalisation de la PSSI. Nommer un RSSI serait donc une condition *sine qua non* pour disposer d'une PSSI ou *a minima*, la première mission du RSSI serait de rédiger la PSSI.

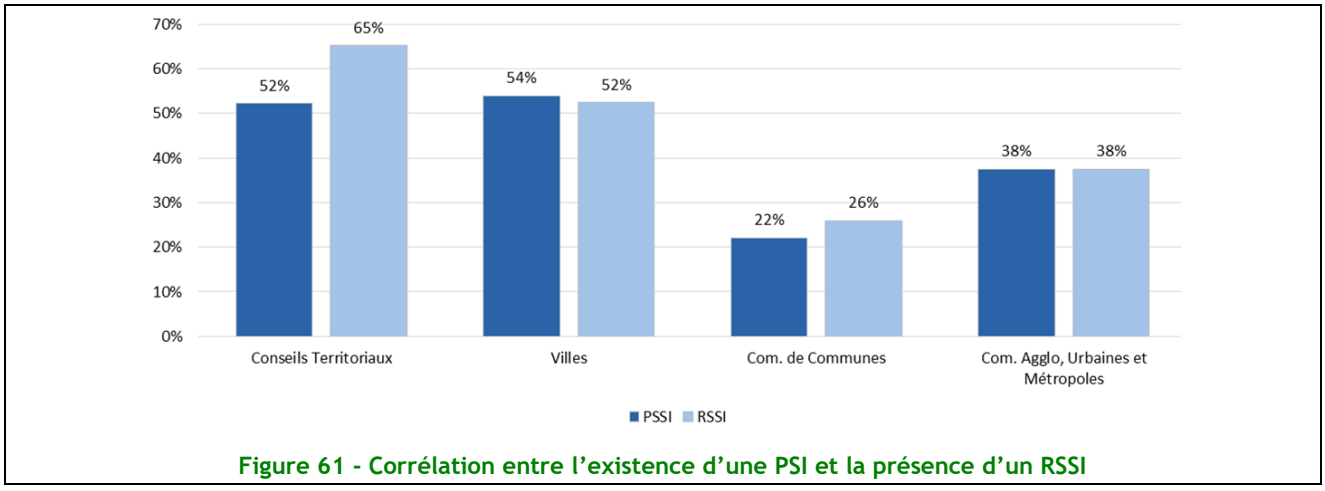


Figure 61 - Corrélation entre l'existence d'une PSI et la présence d'un RSSI

Une Direction Générale moins impliquée dans la PSI.

Si les Directions Générales des Services restent concernées par la PSI, elles seraient moins fortement impliquées en 2016. **Celle-ci est aujourd'hui prise en main par les Directions des Systèmes d'Information**. L'implication des élus et des fonctions supports (Juridique et Ressources Humaines) reste forte. Les métiers semblent s'écarter du processus de construction de la PSI.

Quelles sont les entités de votre Collectivité qui ont participé à l'élaboration de la PSI ?

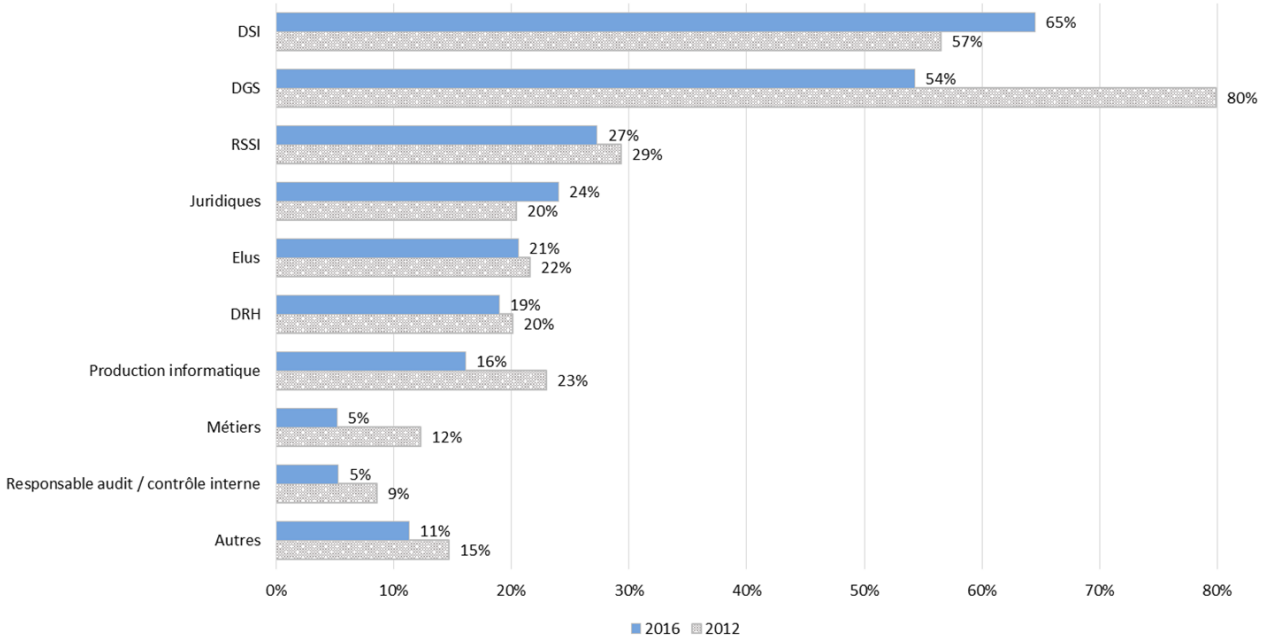


Figure 62 - Entités participant à l'élaboration de la PSI

Une PSI qui voit son cadre méthodologique progresser modestement

L'appropriation de référentiel progresse dans les Collectivités Territoriales. Si les Collectivités les plus structurées comme les Conseils Territoriaux et les Communautés d'Agglomération, Urbaines et Métropoles plébiscitent les normes 27000 (75% pour les Conseils Territoriaux) les Villes et les Communautés de Communes ont tendances à avoir plusieurs référentiels qu'elles personnalisent en interne. Les référentiels nationaux sont néanmoins cités dans 26% des Collectivités (Guide ANSSI, PSSI Etat, EBIOS)

La PSI de votre Collectivité s'appuie-t-elle sur des référentiels de sécurité ? (si oui, lesquels ?)

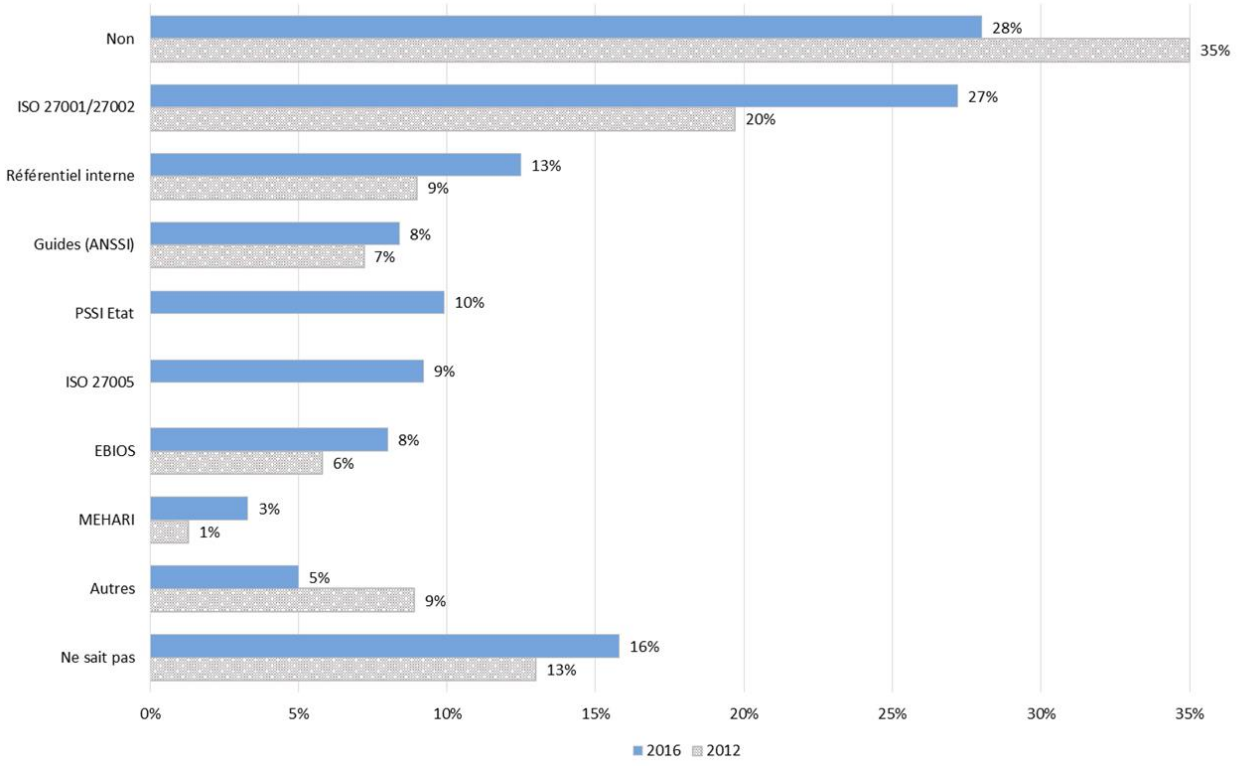


Figure 63 - Référentiels et PSI

Quand elle est formalisée, la PSI est communiquée de manière proactive et explicite dans un peu moins d'un cas sur 3. Quand elle est communiquée en interne, elle l'est rarement – une fois sur deux - aux partenaires externes et principalement aux prestataires informatiques qui interviennent sur le système d'information.

La PSI de votre Collectivité est-elle partagée avec des partenaires extérieurs ?

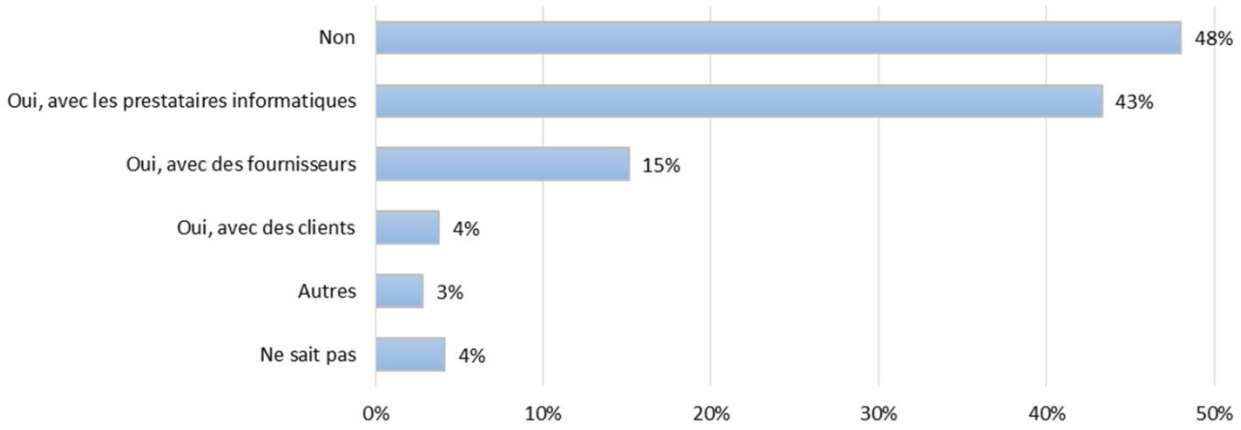


Figure 64 - PSI et partenaires extérieurs

Thème 6 : Organisation de la sécurité et moyens

Le RSSI : un poste métier en stagnation

Depuis 2012, la fonction de RSSI ou de RSI ne progresse en moyenne que de 3 points pour passer à 35%. Il faut noter une forte progression dans les Villes qui en 2012 déclaraient avoir désigné un RSSI pour 35% d'entre-elles. Ce taux passe à 52% en 2016.

Le RSSI voit sa mission légèrement se diluer. En 2012, les personnes affectées à cette mission étaient dédiés à 46%. Ce taux passe à 40% en 2016. L'augmentation du taux dans les Communautés est due à une désignation d'un RSSI dédié dans les Communautés d'Agglomération, Urbaines et Métropoles (67% des cas en 2016).

Il faut s'interroger sur les raisons de cette régression : manque de profil spécialisée, réduction des effectifs ou, le RSSI en Collectivité n'aurait-il pas su convaincre de l'utilité de sa mission ?

La fonction de RSSI ou de RSI, lorsqu'elle est attribuée, est-elle dédiée à la sécurité de l'information ?

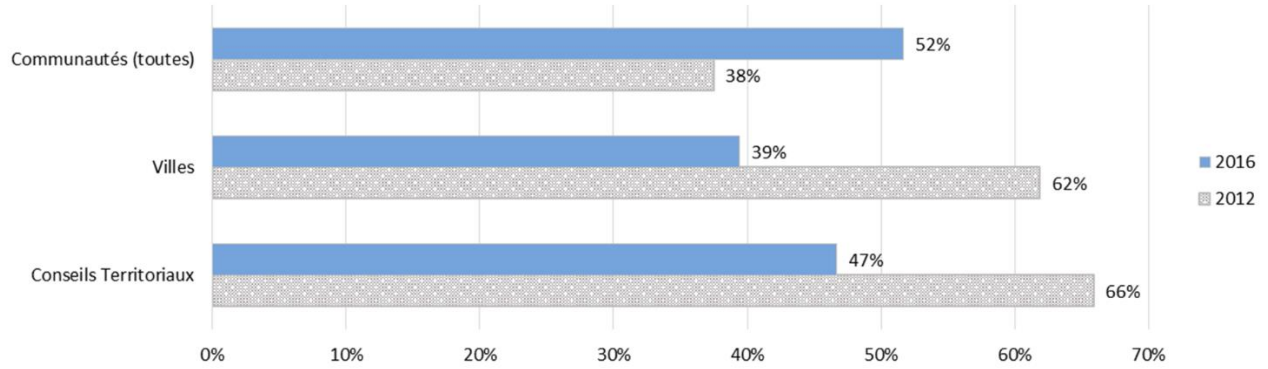


Figure 65 - Part des RSSI dédié à la fonction

Le rattachement du RSSI est étroitement lié à la taille de la collectivité

Plus la collectivité est petite et plus les fonctions sont cumulées par le comité de direction. Ainsi, dans les Communautés, la fonction sécurité est souvent portée par un Directeur (DGA), directement rattaché au Directeur Général des Services (DGS). Dans les structures plus conséquentes, ce n'est pas par défaut mais plutôt dans un souci de séparation des rôles et responsabilités que la fonction RSSI est en prise directe avec le DGS.

Quel est le rattachement hiérarchique du RSSI/RSI au sein de votre collectivité ?

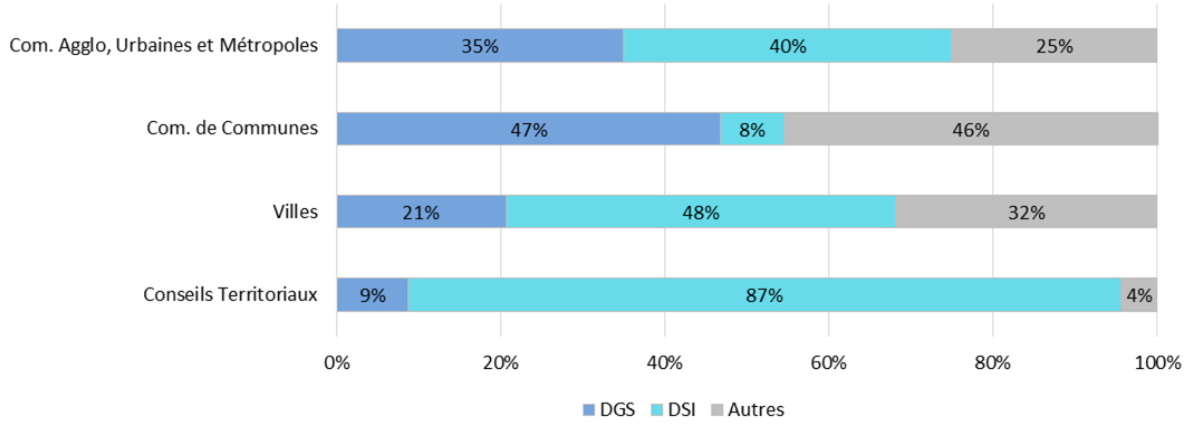


Figure 66 - Rattachement du RSSI

Entre 2012 et 2016, la répartition du temps consacrés aux différents aspects de la mission du RSSI n'a pas significativement évoluée. (+3 points en technique et opérationnel, -4 points en juridique)

Dans le cadre des missions du RSSI, quel % représente le temps consacré aux aspects…

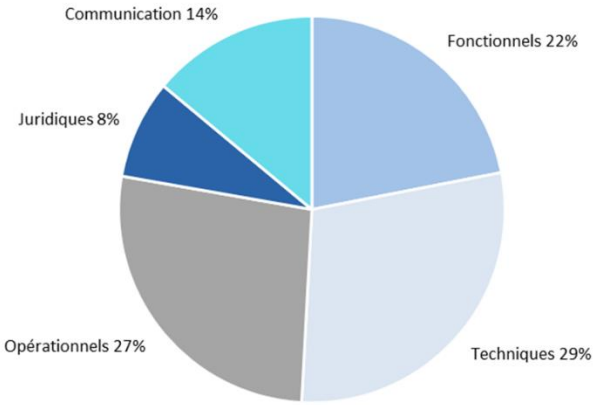


Figure 67 - Activités du RSSI

Une fonction sécurité qui souffre d'un manque de transversalité.

Seules 12% des collectivités disposent d'un comité transversal. Cette transversalité s'appuie en général sur des structures existantes de correspondants système d'information ou référents applicatifs.

Thème 7 : Sécurité des ressources humaines

La charte d'usage du système d'information (SI), référence réglementaire pour la protection du SI, n'est pas adoptée pour toutes les populations d'usager.

Lorsque la technologie n'est pas en mesure de limiter ou de contrôler l'usage du système d'information, la charte reste le meilleur moyen pour cadrer les pratiques sur le SI. Elle est également une obligation réglementaire pour l'information des usagers. Encore faiblement adoptée par les Communautés (38%), elle **marque une progression notable de 8 points pour l'ensemble des Collectivités (49%)**.

Cependant le public visé par la charte n'encadre pas systématiquement l'ensemble des acteurs accédant au SI.

Lorsqu'une « charte d'usage ou d'utilisation du SI » existe, à qui est-elle destinée ?

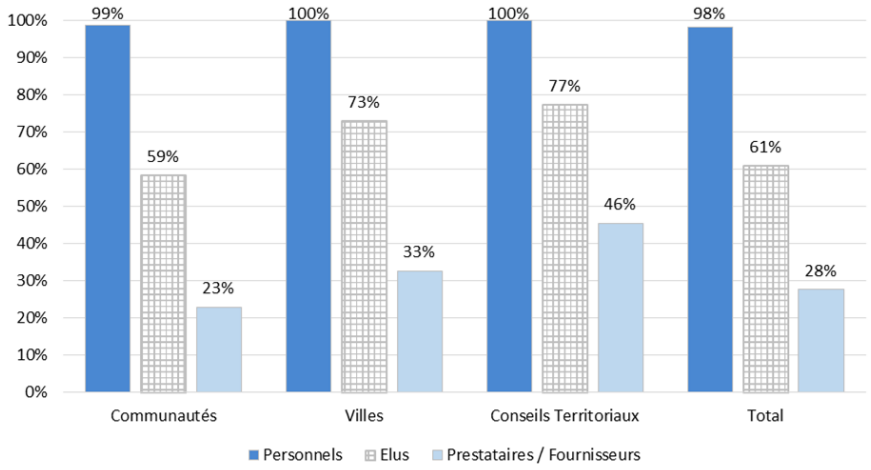


Figure 68 - Populations visées par la charte d'usage du SI

Une sensibilisation au cœur des actions RH.

En plus d'une communication de la charte d'usage du système d'information, la sensibilisation des usagers permet de leur faire prendre conscience de la nécessité d'adopter une posture éthique et responsable au sein du SI. L'implication des élus et la mise en œuvre d'un programme de sensibilisation en SSI sont fortement liées. **De ce fait, plus les élus sont impliqués comme destinataires ou comme approbateurs de la charte d'usage du SI, plus les actions de sensibilisation sont fortes et variées.**

Quels sont les moyens utilisés pour assurer la sensibilisation ?

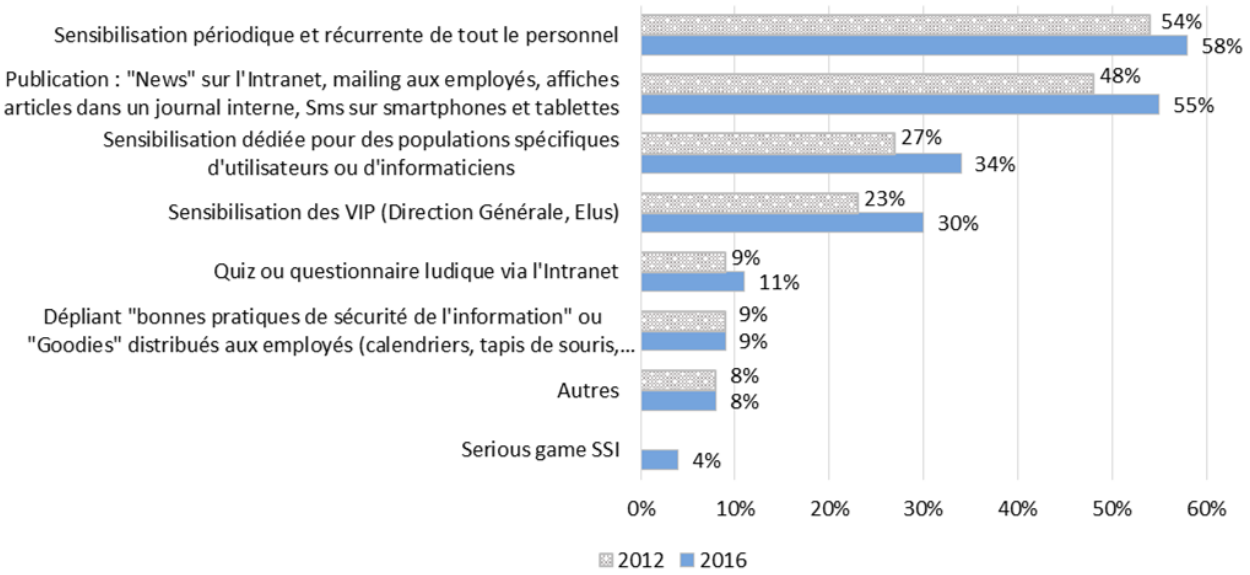


Figure 69 - Les moyens utilisés pour assurer la sensibilisation

Une gestion des départs difficilement maîtrisable

Si majoritairement les Directions Informatiques se disent informées de l'arrivée d'un nouvel agent, **50% d'entre elles ne sont pas tenu au courant des changements de postes et des départs**. Le cycle de vie de l'habilitation est un des points essentiels pour garantir la maîtrise des accès au SI. La fin de vie d'une habilitation est l'un des challenges dans les années à venir pour les collectivités. Preuve de sa complexité, sa mise en œuvre stagne globalement depuis 2012. Elle reste un point délicat pour les structures comme les Communautés et une source de risque sérieuse par la présence de nombreux comptes dormants.

Existe-t-il une procédure pour gérer, en cas de départ ou mutation des collaborateurs, la suppression de tous les droits d'accès et la restitution de tout le matériel ?

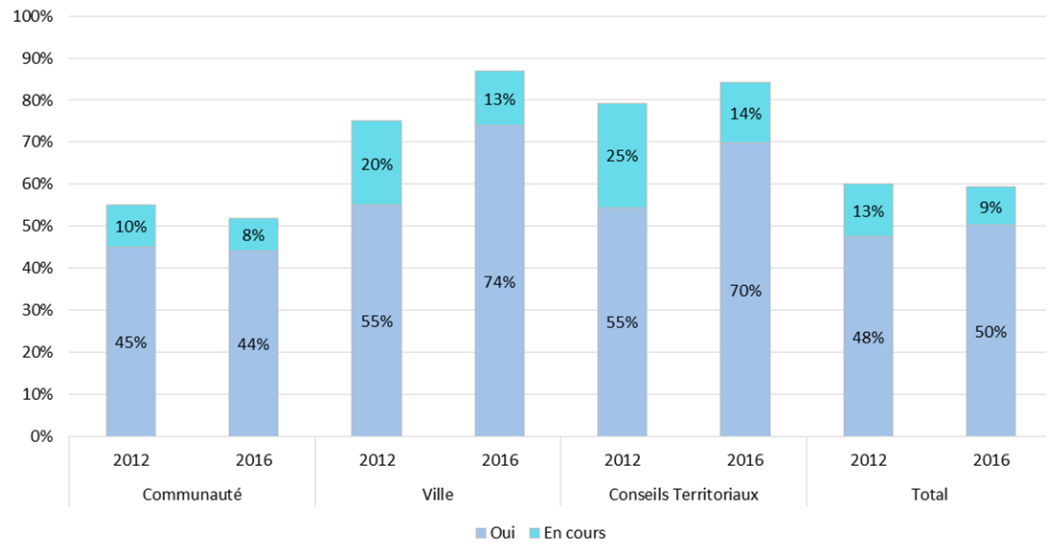


Figure 70 - Procédure de suppression des droits d'accès et de restitution du matériel

Thème 8 : Gestion des actifs

Pas ou peu de progrès dans la gestion des actifs

Excepté pour les Communautés de Communes, l'étude 2016 révèle que l'inventaire des informations et de leurs supports aurait légèrement progressé depuis 2012 : 54% (- 1 points).

Avez-vous inventorié toutes les informations (et leurs supports) de votre Collectivité et leur avez-vous attribué un propriétaire ?

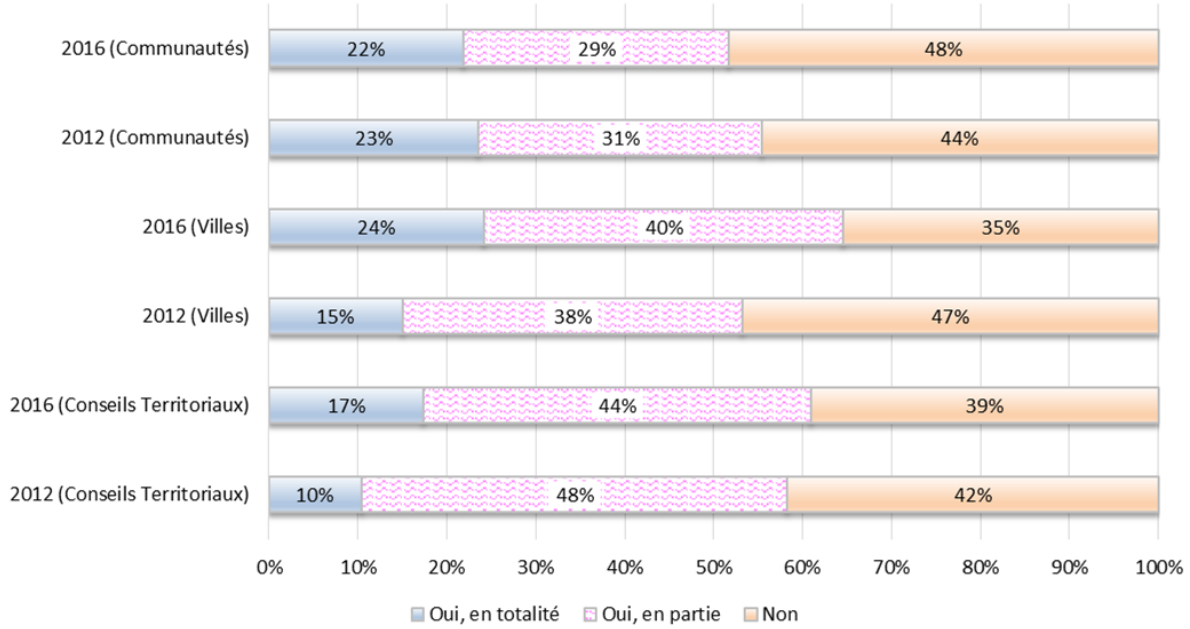


Figure 71 - Inventaire de données et attribution de propriétaire

La classification des informations est en très net recul : 25% des Collectivités ont réalisé une classification de manière exhaustive alors qu'elles étaient 40% en 2012.

Avez-vous classifié les informations, pour indiquer le besoin, les priorités et le degré souhaité de protection ?

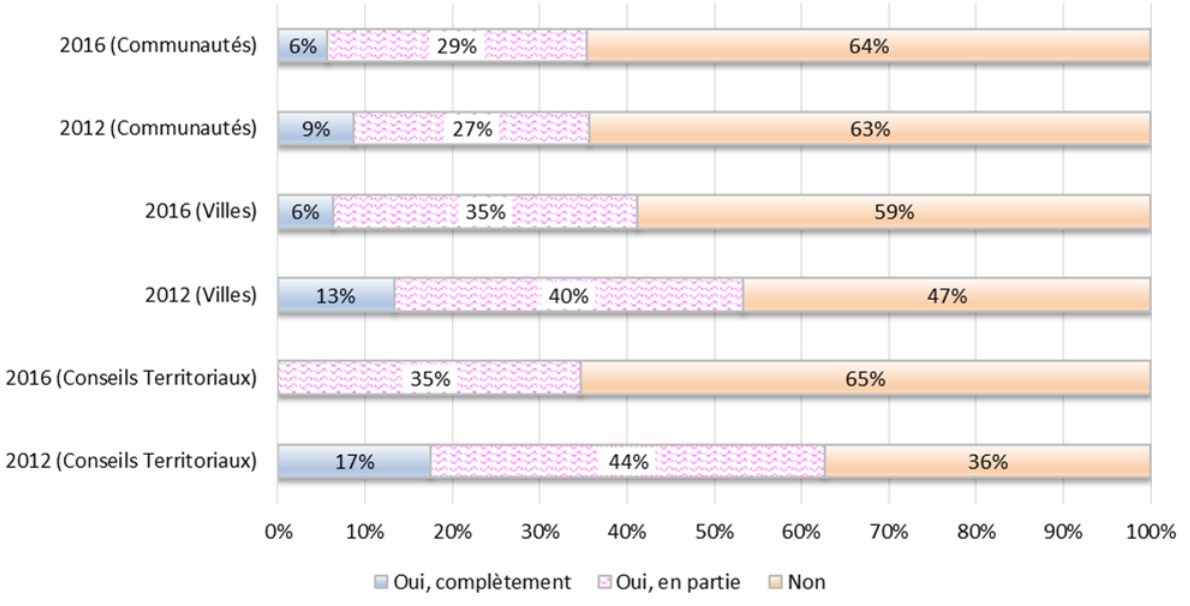


Figure 72 - Classification des données

La part des collectivités ayant réalisé une analyse de risque est en diminution, passant de 33% en 2012 à 27% en 2016. Une analyse plus fine des données collectées révèlent que ce n'est pas le cas pour les Villes (36% en 2012, 48% en 2016).

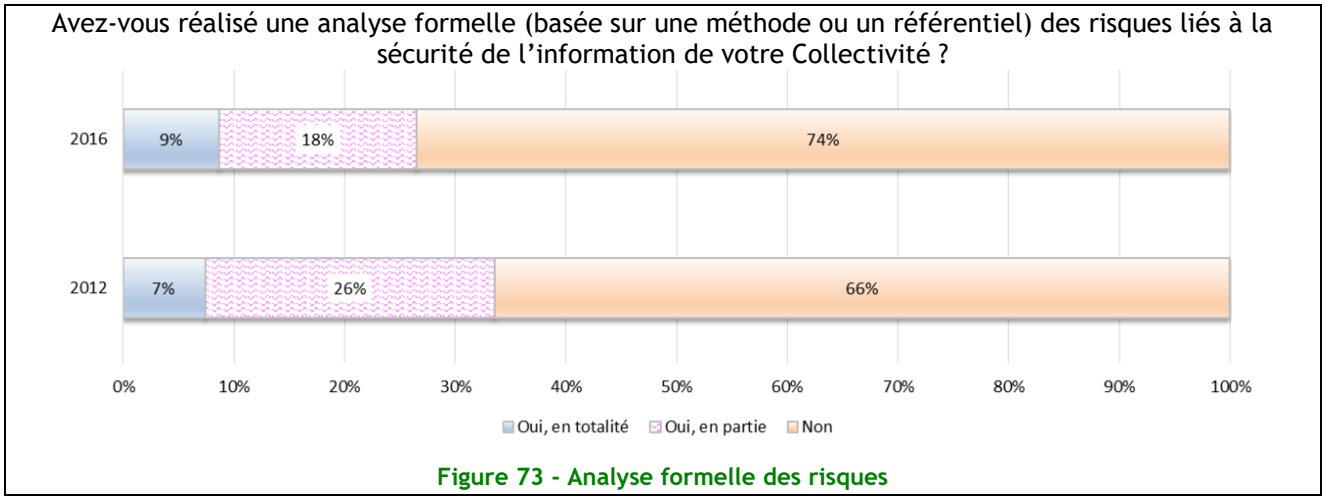


Figure 73 - Analyse formelle des risques

Dans 60% des cas, l'analyse est réalisée par le RSSI qui en porte la responsabilité. Selon certains d'entre eux, il serait fréquent qu'ils se fassent assister par un consultant externe, l'exercice demandant une bonne maîtrise des méthodes d'analyse.

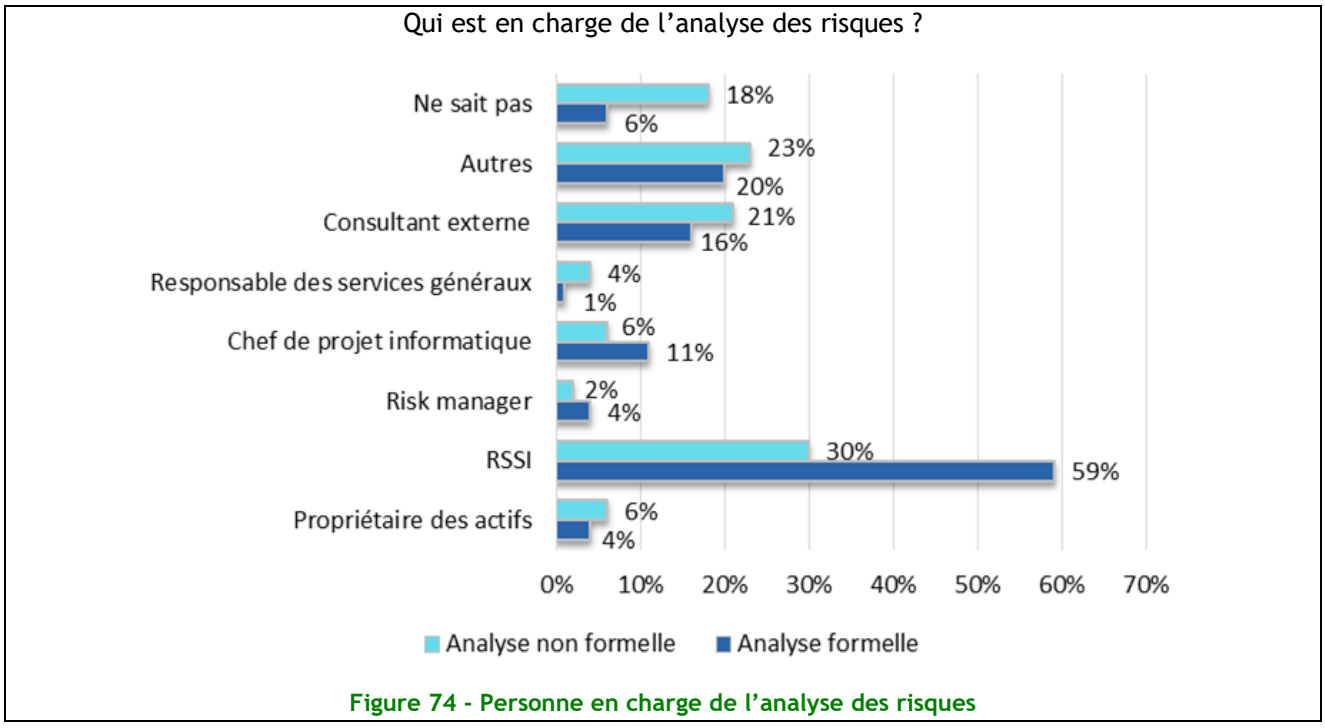


Figure 74 - Personne en charge de l'analyse des risques

Les méthodes EBIOS et ISO 27005 restent les référentiels les plus utilisées pour l'analyse de risque : 45% des collectivités interrogées les pratiquent. On note un progrès de 10% pour la méthode EBIOS probablement parce qu'elle est fortement recommandée par l'ANSSI ou les organismes de tutelles.

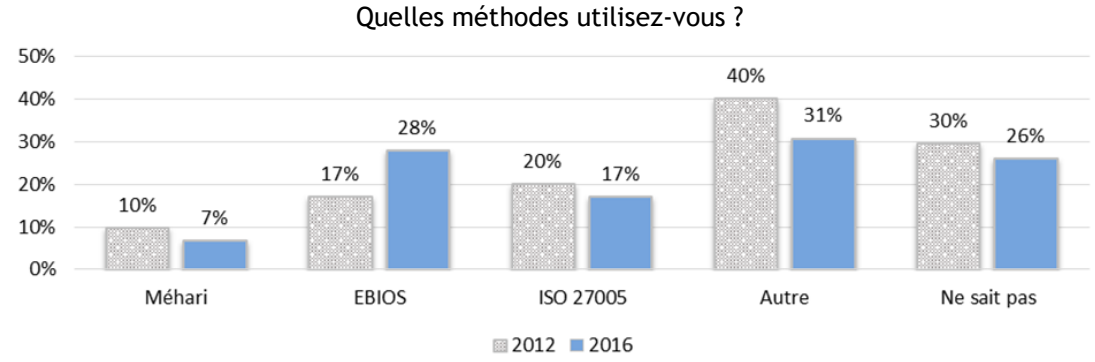


Figure 75 - Méthode d'analyse des risques

Thème 9 : Contrôle d'accès

Une augmentation significative des moyens de contrôle d'accès.

L'authentification forte par certificat électronique sur support matériel (58%) et l'authentification par certificat électronique logiciel (56%) **se confirment** et restent les deux types de contrôle d'accès les plus couramment utilisés en 2016.

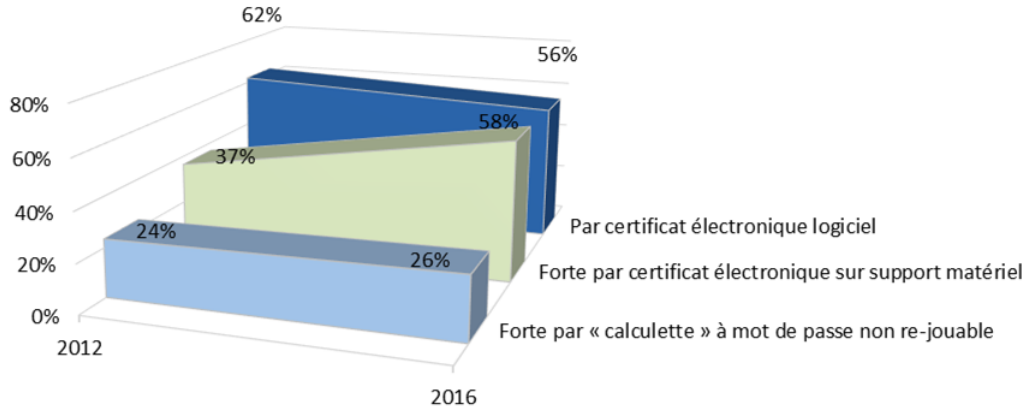


Figure 76 - Technologie/approche de sécurisation par type d'authentification

Un deuxième zoom basé sur un angle d'analyse « technologique » met en exergue la progression des approches « SSO ». Selon certains, la protection de la vie privée expliquerait la faible adhésion des collectivités à la biométrie.

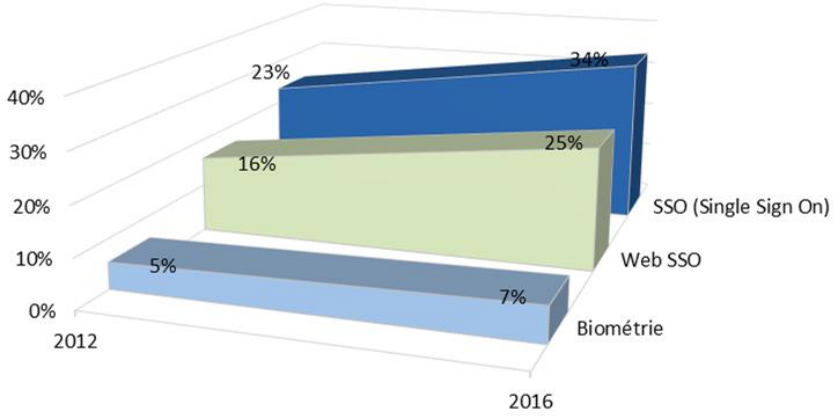


Figure 77 - Authentification - Zoom sur les approches technologiques

Une meilleure gestion des droits d'accès par l'automatisation des taches.

Les approches de sécurisation basées sur des modèles d'habilitation sur base de profils / rôle métier progressent de 7 points en 4 ans. De même, le provisionning avec 24% progresse de 4 points.

Il est intéressant de noter la concomitance de l'évolution des modèles d'habilitation sur base de profils / rôle métier avec les workflows d'approbation des habilitations qui permettent de faciliter leurs gestions.

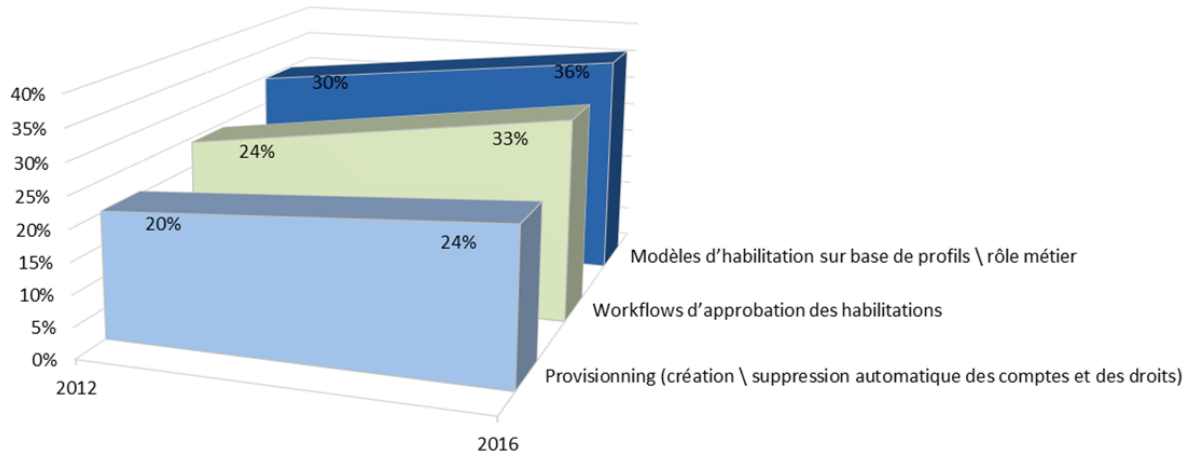


Figure 78 - Authentification - Zoom sur les modèles par habilitations/droits

Plus d'automatisme, moins de formalisme dans les procédures

En contradiction avec le point précédent, **la part des Collectivités déclarant avoir une procédure formelle de création, modification et suppression de comptes utilisateurs nominatifs est en nette diminution**. Cette baisse est encore plus marquée lorsque l'on s'intéresse à la population sensible des « administrateurs ». Les Collectivités pensent-elles qu'une fois que les automatismes tels que les workflows d'approbation et les modèles d'habilitation en place, le formalisme n'est plus de mise ?

Existe-t-il une procédure formelle de création, modification, et suppression de comptes utilisateurs nominatifs ?

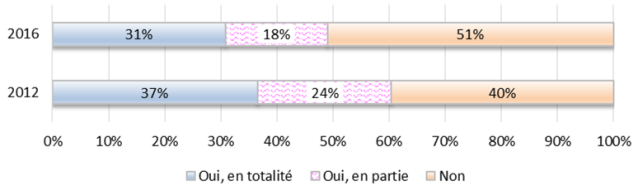


Figure 79 - Procédure formelle de création, modification, et suppression de comptes utilisateurs

Cette même procédure existe-t-elle spécifiquement pour les administrateurs ?

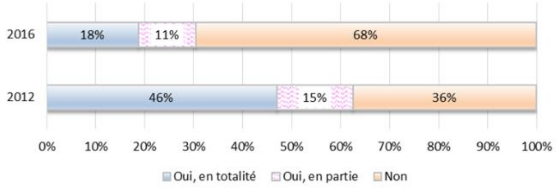


Figure 80 - Procédure spécifique pour les administrateurs ?

L'analyse par type de Collectivités sur la population des administrateurs met en évidence une très forte baisse sur les Communautés (-32 points entre 2012 et 2016) et les Conseils Territoriaux (-42 points entre 2012 et 2016). Deux hypothèses pourraient expliquer cette baisse : l'absence de procédure spécifique aux administrateurs, les procédures existantes étant suffisantes ou, pire, une absence totale de procédure de gestion.

L'existence de règles de constitution et de péremption des mots de passe progresse passant de 53% en 2012 à 58% en 2016 (cumul des catégories « Oui, pour tous » et « Oui, pour certains »).

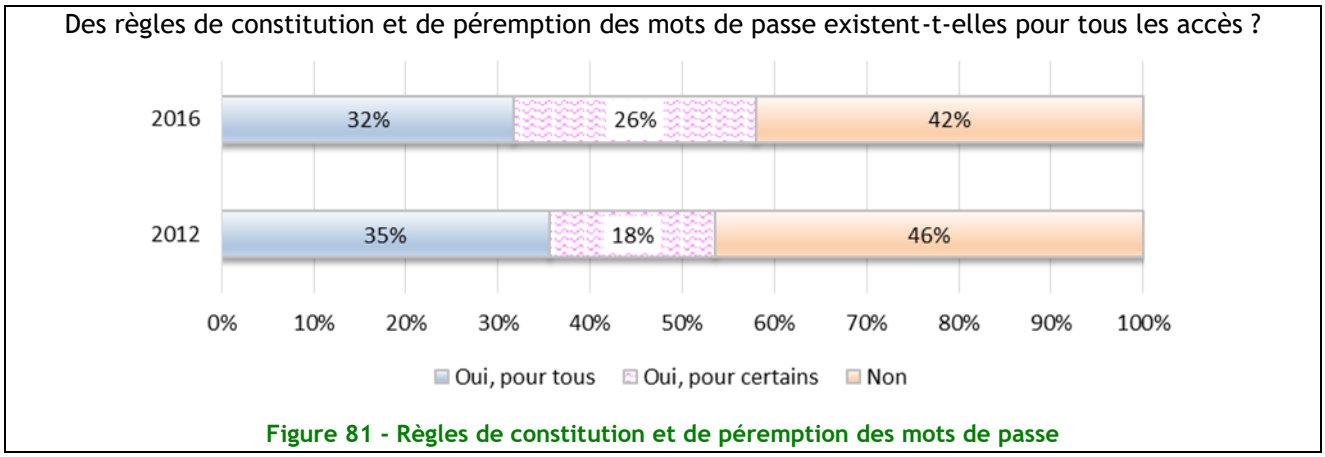


Figure 81 - Règles de constitution et de péremption des mots de passe

Avec respectivement une diminution de la part du « Non » de 6 points et de 9 points les Communautés et les Conseils Territoriaux ont participé à cette amélioration. Les Villes sont les seules à voir la part du « Non » augmenté entre 2012 et 2016 (+5 points).

Thème 10 : Cryptographie

Une méconnaissance de l'utilisation des moyens cryptographiques par les collectivités territoriales

Le Référentiel Général de Sécurité (RGS) préconise les moyens cryptographiques pour répondre aux exigences de sécurité. Moins de 2 collectivités sur 5 déclarent les utiliser. Ces fonctions de sécurité sont souvent intégrées dans un même certificat. Elles sont désormais obligatoires pour la dématérialisation de la chaîne comptable (PES v2) et du contrôle de légalité (ACTES). Il est possible que les collectivités interrogées n'aient pas considéré les usages précédents dans les réponses qu'elles nous ont fournies.

Quand elles les exploitent, c'est quasiment à part égale pour des fonctions d'authentification (24%), d'authenticité de l'information par signature (23%) ou pour le chiffrement des données (19%). Les moyens cryptographiques ne sont pratiquement pas exploités pour la non-répudiation d'une action (5%).

Thème 11 : Sécurité physique et environnementale

La plupart des Collectivités Territoriales n'aurait pas encore déployé de moyens contre les accidents physiques et l'accès non-autorisé

Elles seraient 29% dans ce cas. Dans notre échantillon, les Communautés de Communes seraient les plus démunies avec plus de 40% d'entre elles qui indiquent ne pas encore avoir déployé de moyens spécifiques.

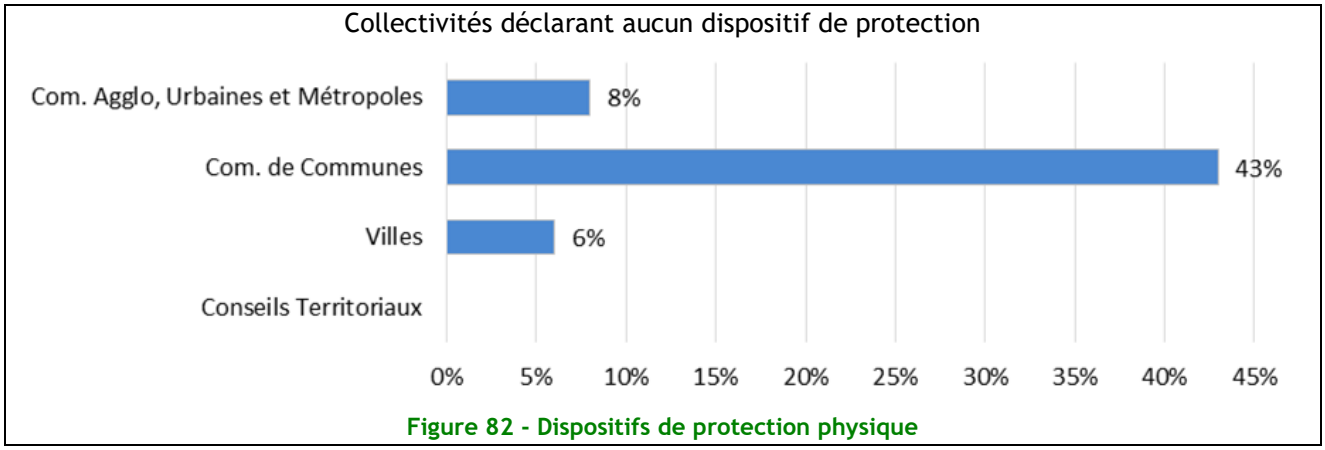


Figure 82 - Dispositifs de protection physique

Pour les autres, un système de détection incendie serait installé dans 48% des cas. Les collectivités seraient semble-t-il moins vulnérables aux inondations, 11% se protégeraient contre une fuite d'eau, une infiltration ou encore une montée des eaux. Dans un cas comme dans l'autre, on observe des pratiques moins soutenues dans les Communautés de Communes.

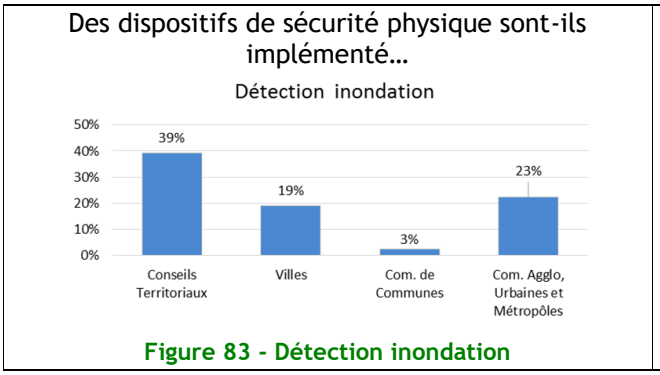


Figure 83 - Détection inondation

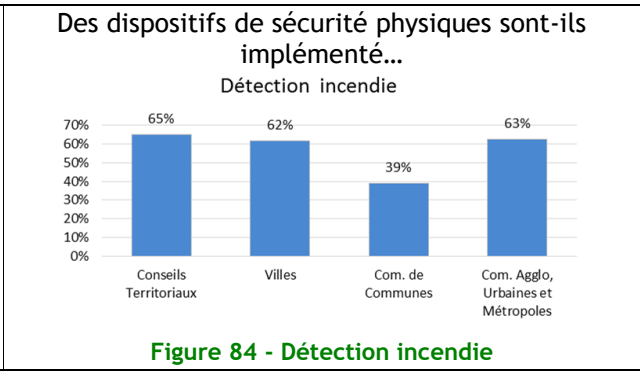


Figure 84 - Détection incendie

Le contrôle d'accès par badge est le plus utilisé et serait souvent renforcé par des caméras de surveillance.

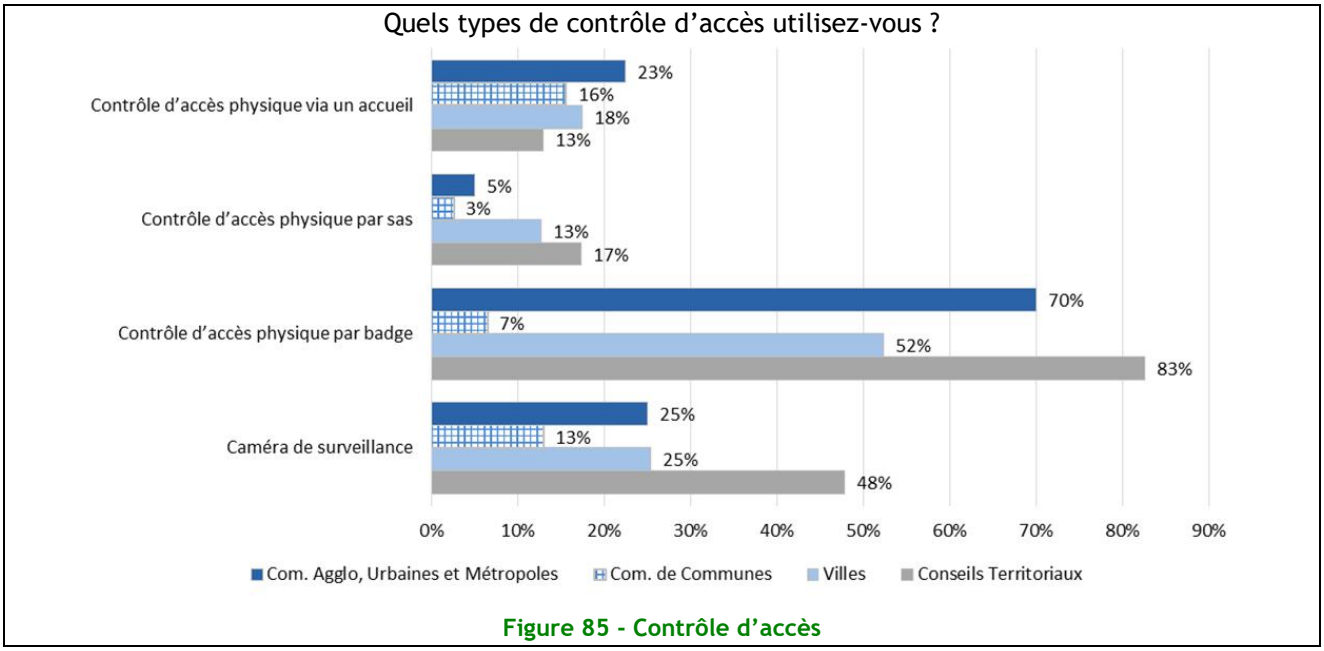


Figure 85 - Contrôle d'accès

La protection des données sur supports physiques parfois pris en compte dans la PSSI

Ce sont les Conseils Territoriaux qui seraient les plus impliqués, 70% déclarent l'avoir intégré. Les pratiques les plus citées concerneraient **la protection des bandes de sauvegarde** et l'utilisation de **broyeurs** pour détruire les documents sensibles.

La protection des données sur support physique (bandes, CD, papiers, etc.) est-elle prise en compte dans la PSSI ?

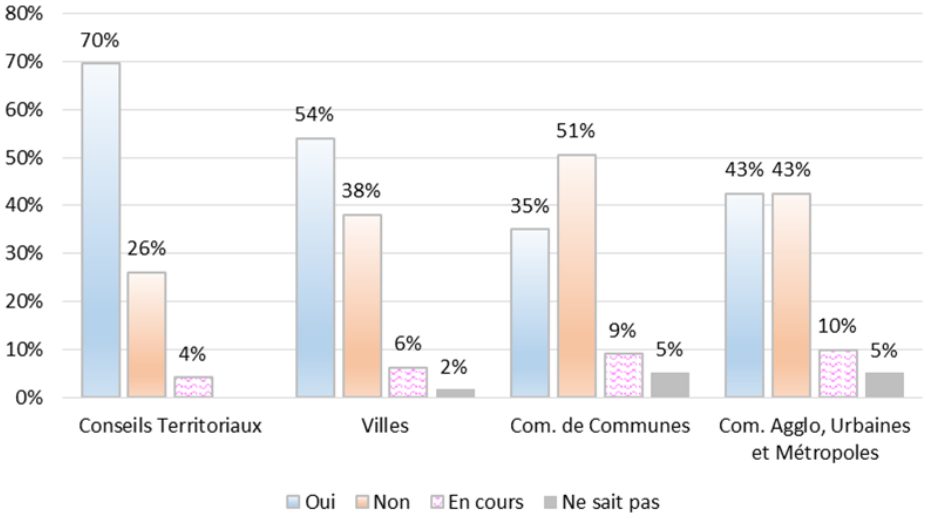


Figure 86 - Protection des données sur support physique

Thème 12 : Sécurité liée à l'exploitation

Logiciels malveillants : Une stratégie inchangée pour lutter contre de nouveaux types d'attaques

L'utilisation de solutions anti-virus, anti-spam et de pare-feu sur les postes des utilisateurs reste généralisée au sein des différentes collectivités, atteignant un **niveau comparable à celui rencontré au sein des entreprises.**

Protection contre les logiciels malveillants…

Technologie de sécurité

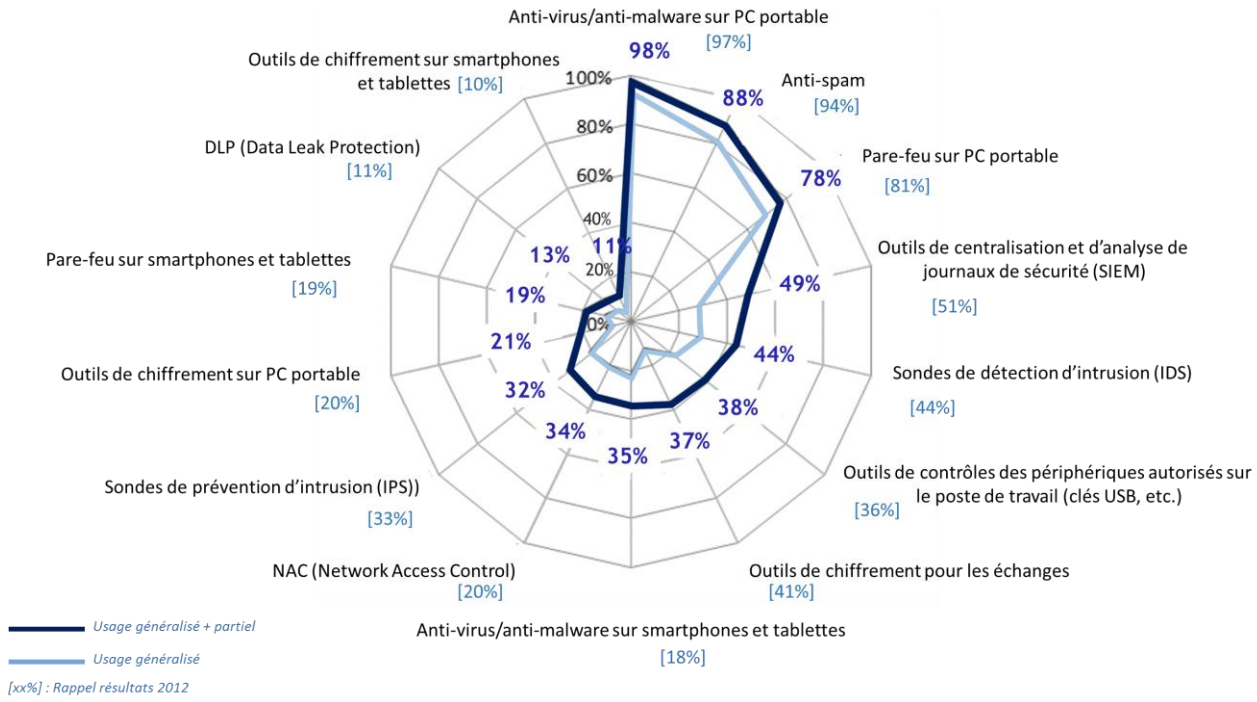


Figure 87 - Technologies de sécurité

Ces bonnes pratiques permettent de garantir un niveau de sécurité de base sur les postes de travail, mais ne sont **pas généralisées sur les terminaux mobiles de type smartphones et tablettes, bien qu'en progression** (l'utilisation d'anti-virus et anti-malware sur ces terminaux ayant quasiment doublé en 4 ans, passant de 18% à 35% et se rapprochant ainsi du niveau des entreprises).

Le chiffrement des postes de travail et des terminaux mobiles est nettement moins répandu qu'en entreprise (21% contre 43% pour les PC, 11% contre 21% pour les terminaux mobiles). De même, les taux d'utilisation des outils de DLP (contrôles de fuites des données) et de contrôle des périphériques autorisés restent stables depuis 2012 et inférieurs à ceux rencontrés en entreprise (13% contre 18% pour le DLP, 38% contre 49% pour le contrôle des périphériques). Ces écarts peuvent potentiellement s'expliquer par une moindre présence de données jugées confidentielles au sein des Collectivités.

La sécurisation des réseaux continue à reposer principalement sur les pare-feux même si l'adoption des technologies de NAC (contrôle d'accès au niveau réseau) est en progression significative depuis 4 ans, passant de 20% à 34%.

L'utilisation de solutions de types IPS/IDS (détection et prévention d'intrusions) reste partielle. Ce taux utilisation est bien inférieur à celui rencontré au sein des entreprises (32% contre 53% pour les IPS, 44% contre 64% pour les IDS), qui considèrent ces solutions comme partie intégrante de l'outillage nécessaire à la détection et au contingentement des attaques.

Les solutions de collectes et d'analyses de logs de type SIEM sont utilisées à un niveau comparable à celui des entreprises. Ces solutions nécessitent cependant des ressources et de l'expertise afin d'en tirer profit et la question est posée quant à la capacité à mettre en œuvre une véritable analyse basée sur de la corrélation des logs ou uniquement une collecte et un stockage centralisé des journaux.

En 4 ans, les Collectivités ont ainsi peu fait évoluer les solutions techniques utilisées, reposant sur les classiques anti-virus / anti-malware, pare-feux et anti-spam. L'utilisation d'autres solutions reste toujours bien moins importante qu'en entreprise, ce retard étant encore plus présent au sein des Communautés de Communes. Dans le même temps, les types de menaces et d'attaques ont fortement évolués et ciblent désormais également les Collectivités, que ce soit à des fins idéologiques (défiguration de sites web à des fins de propagande) ou lucratives (utilisation de rançongiciel comme LOCKY qui aurait, selon la presse, touché de nombreuses collectivités). Face à cette évolution, il convient de s'interroger sur l'adéquation des technologies mises en œuvre au sein des Collectivités pour prévenir et détecter ces différentes attaques.

Vulnérabilités techniques : Une veille des vulnérabilités en recul, avec de fortes disparités

Réalisez-vous une veille permanente en vulnérabilités et en solutions de SSI ?

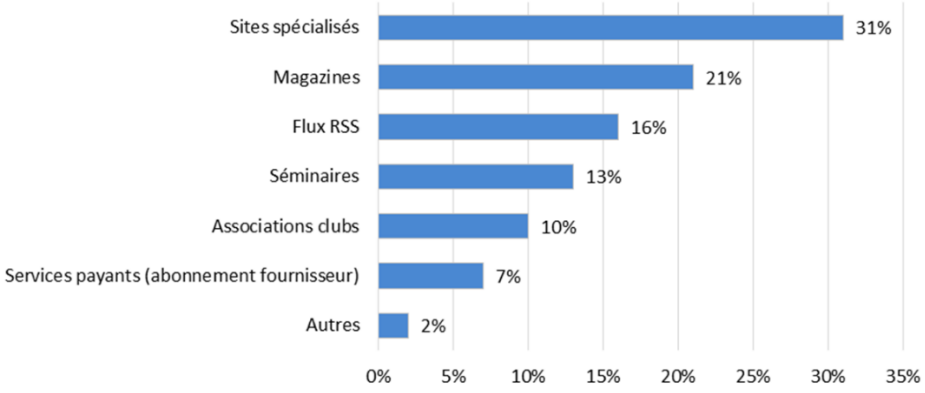


Figure 88 - Veille sécurité

Il apparait que **les processus de veille en vulnérabilité sont moins systématiquement implémentés au sein des Collectivités qu'en 2012** avec à peine une collectivité sur deux (49%) effectuant cette veille actuellement pour deux collectivités sur 3 (65%) il y a 4 ans. Ce résultat peut être considéré comme représentatif d'une forte disparité du niveau de maturité entre les différents types de collectivités : à peine 34 % des Communautés de Communes mettent en place des procédures là où 68% des Villes et 63% des

Communautés d'Agglomération font cet effort, ce qui correspond globalement aux résultats relevés il y a 4 ans.

Cette veille est empirique et basée majoritairement sur la collecte d'information sur sites spécialisés, des magazines et des flux RSS.

La gestion des correctifs est stable mais à nouveau avec de fortes disparités

34 % des Collectivités ont formalisé des mécanismes d'application de patchs et de correctif qui reste globalement identique comparé à 2012, cependant on dénote à nouveau un très fort écart entre les différents types de Collectivités avec uniquement 17% des Communautés de Communes ayant effectué ce travaille de formalisation alors que les Communautés d'Agglomération, Urbaines et Métropoles sont à 60%, les Villes à 62% et les Conseils Territoriaux à 70%.

Des délais de correction en améliorations

En cas de menace grave, en moyenne quel délai est nécessaire pour déployer les correctifs ?

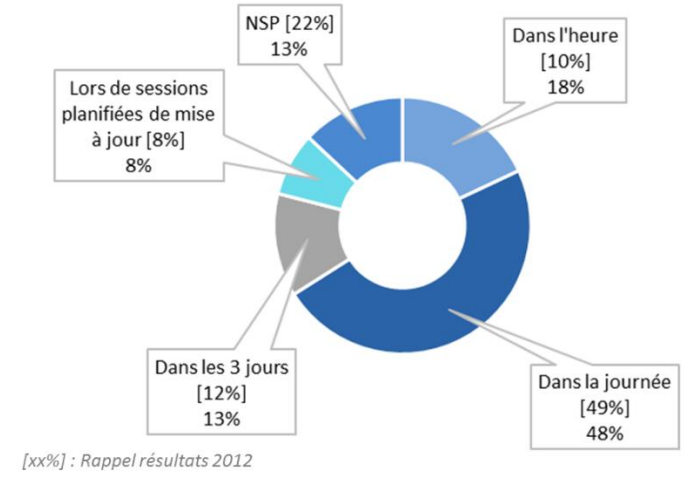


Figure 89 - Délai moyen de déploiement de correctifs

Les délais d'applications de correctifs en cas de menace grave se sont réduit et le nombre de collectivités indiquant être à même de réagir dans l'heure a quasiment doublé (passant de 10% à 18%). **Une progression du nombre de collectivités en capacité de réagir dans la journée est également constatée**.

Thème 13 : Sécurité des communications

Des SI accessibles depuis des moyens maîtrisés par les collectivités.

Depuis la précédente enquête les Collectivités ont **poursuivi leurs efforts de cadrage pour proposer des solutions de connexion à leurs SI**. Ainsi, les accès externes autorisés sous condition depuis des postes de travail fournis par les Collectivités sont en hausse (de 57% à 65%) et les accès depuis des postes non maîtrisés sont principalement interdits.

La mobilité se développant, elles autorisent plus largement (de 20 % à 43%) l'accès externe depuis un Wifi privé mais ils restent soumis à conditions.

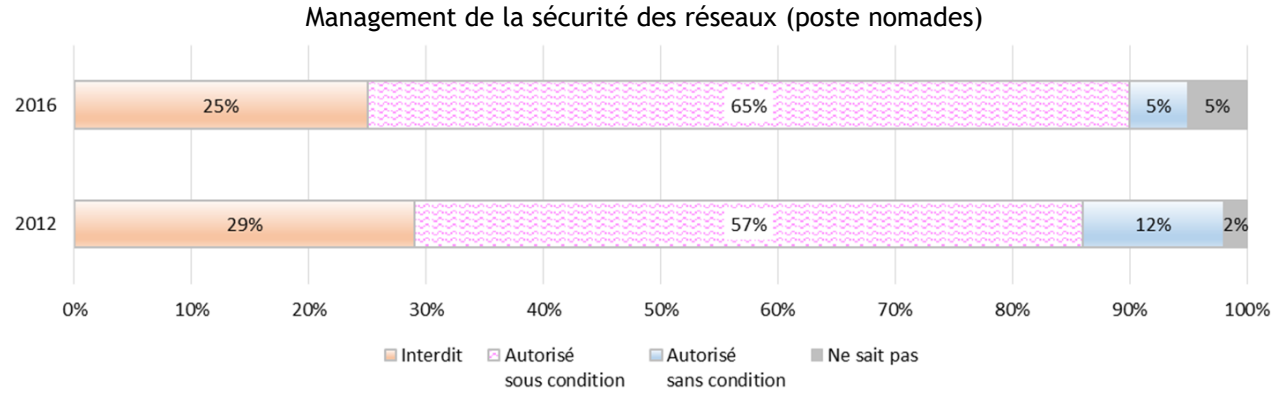


Figure 90 - Accès depuis l'extérieur à partir de postes de travail nomades fournis par la collectivité

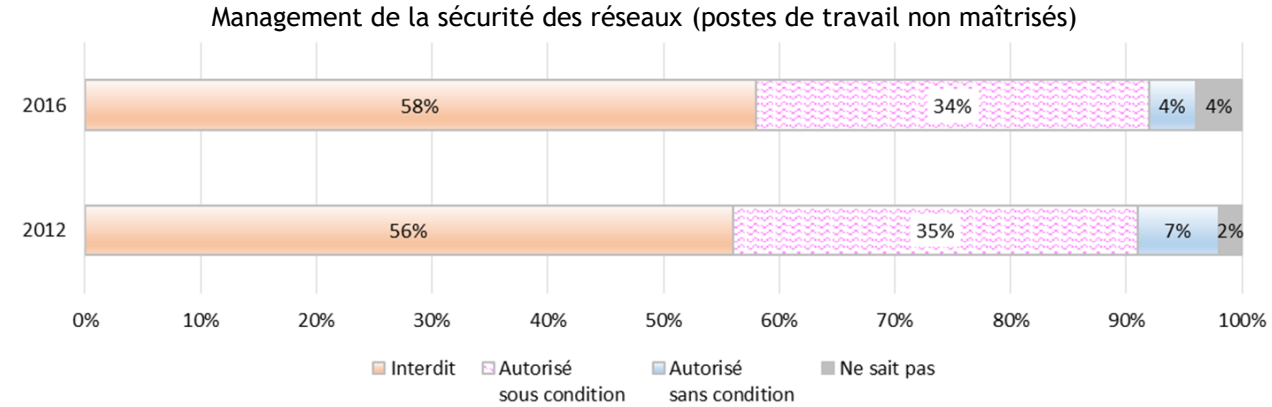


Figure 91 - Accès depuis l'extérieur à partir de postes de travail non maîtrisés (Cyber café, poste de travail personnel, etc.)

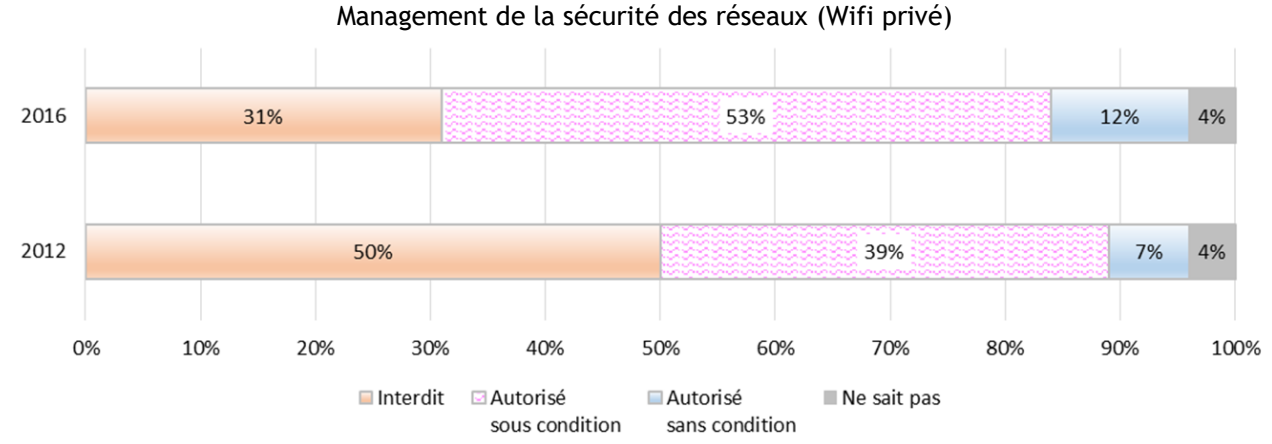


Figure 92 - Accès via un réseau Wifi privé au sein de la collectivité

Tablettes et smartphones, le BYOD un risque reconnu.

Si les tablettes et smartphones fournis par la collectivité peuvent bénéficier d'un accès au SI sous condition à hauteur de 47%, les équipements personnels sont interdit par la moitié d'entre elles. Le taux des restrictions monte à 87% en incluant les autorisations sous condition démontrant que **les collectivités ont pleinement conscience des risques associés à ces terminaux mais n'ont pas toutes mis en œuvre les moyens techniques** nécessaires à leur prise en charge.

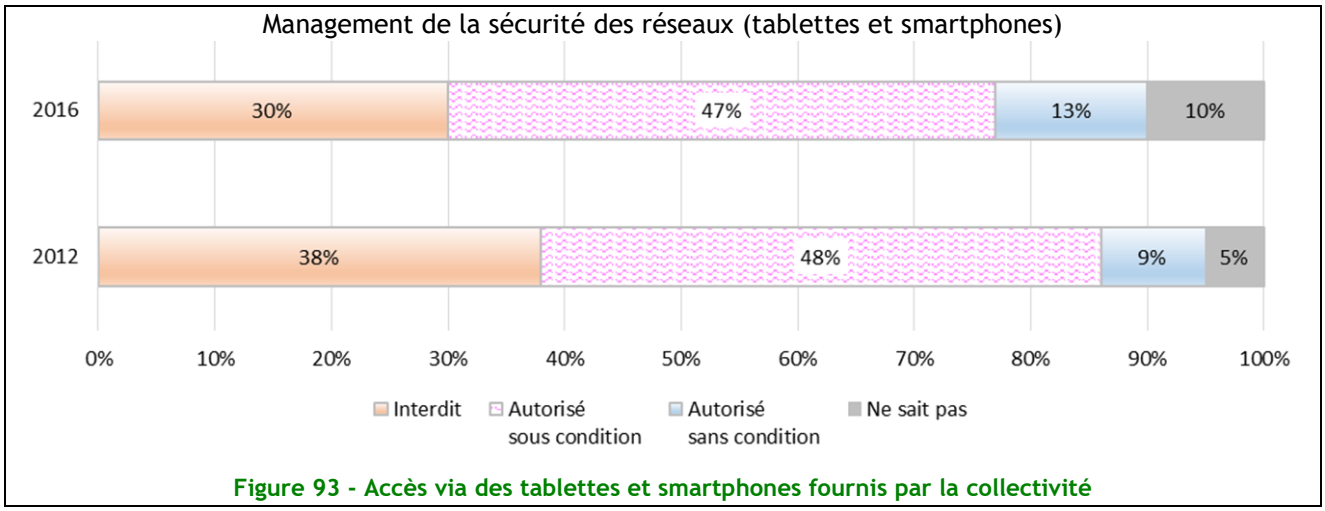


Figure 93 - Accès via des tablettes et smartphones fournis par la collectivité

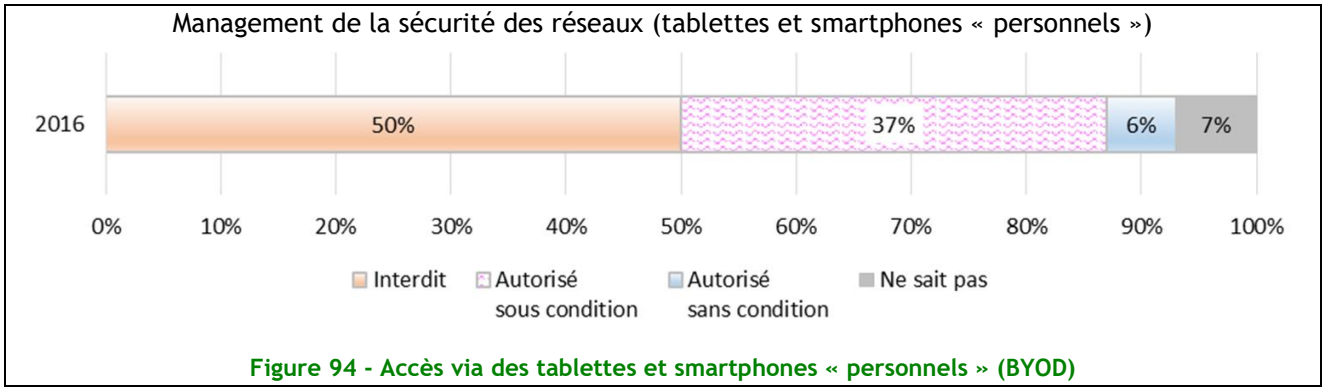


Figure 94 - Accès via des tablettes et smartphones « personnels » (BYOD)

Le web sous contrôle.

Inversion de tendance forte entre 2012 et 2016, les accès au web sans filtrage sont désormais majoritairement non autorisés à l'image des Conseils Territoriaux qui n'étaient que 10% à interdire ces accès en 2012 contre 78% aujourd'hui. Cela s'expliquerait, d'une part, par le renforcement des exigences règlementaires et légales (HADOPI, anti-terrorisme), et d'autre part, par une baisse importante du coût des outils de filtrage qui, selon certaines analyses, aurait été divisé par 5 ces 4 dernières années. Les Communautés de Communes restent cependant en retrait où seules 52 % d'entre elles l'interdisent et 21% l'autorisant même sans condition.

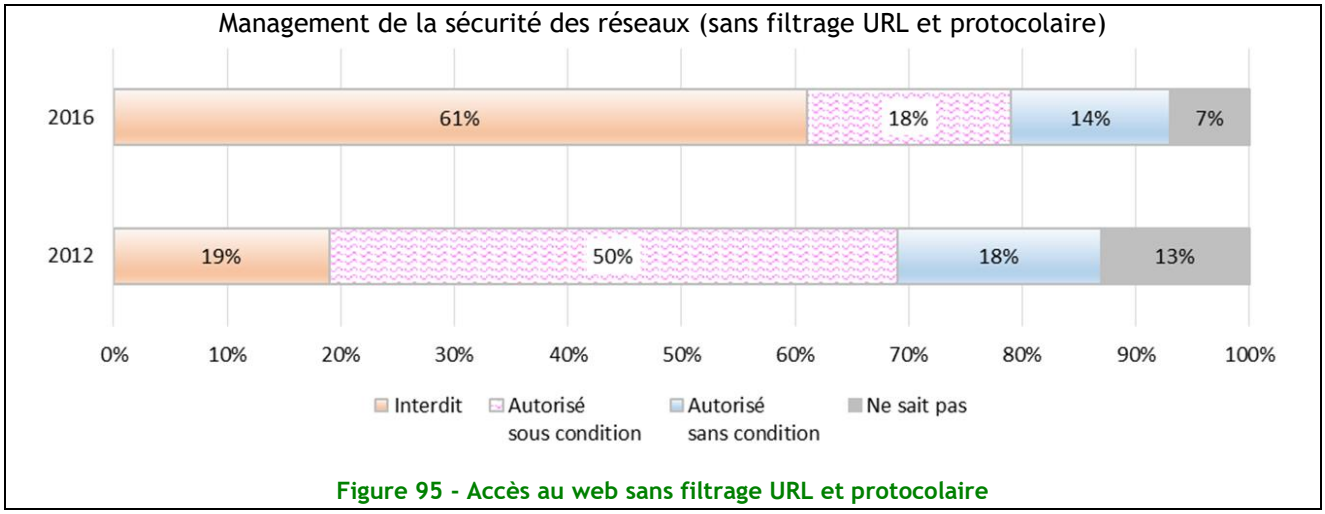


Figure 95 - Accès au web sans filtrage URL et protocolaire

VoIP et ToIP, quels risques ?

L'usage de la voix sur IP et téléphonie sur IP est **un peu plus réglementé que par le passé** même si les interdictions et autorisations sous condition ne représentent que 67% des réponses contre 63% en 2012. Les risques en découlant ne sont sans doute pas clairement connus.

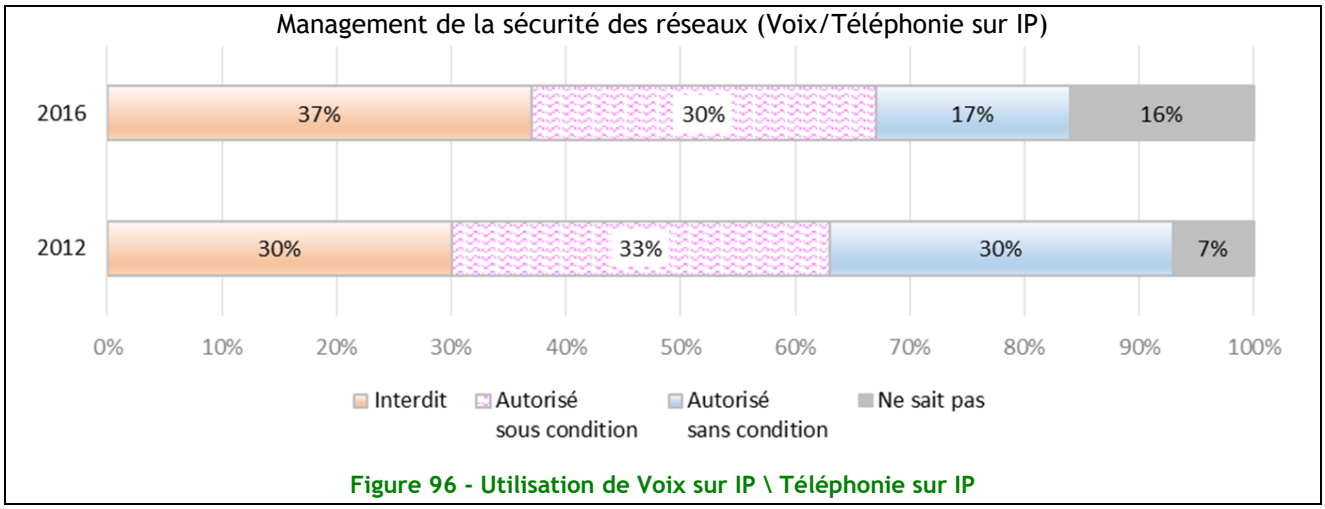


Figure 96 - Utilisation de Voix sur IP \ Téléphonie sur IP

Des réseaux sociaux mieux encadrés.

Véritables vecteurs de communications des collectivités, les **réseaux sociaux voient leurs utilisations plus encadrés**, mais ce sont les Communautés d'Agglomération et Métropoles qui portent majoritairement cette évolution avec 78% d'autorisation sous condition.

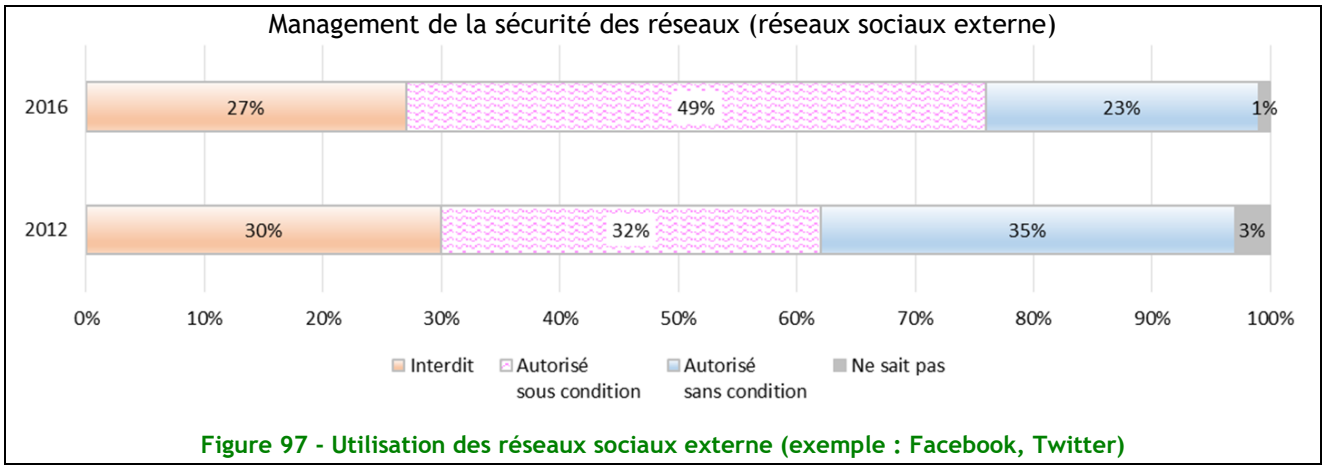


Figure 97 - Utilisation des réseaux sociaux externe (exemple : Facebook, Twitter)

Les messageries instantanées portées par la transformation digitale.

La transformation digitale amène de nouvelles pratiques de communication au travers des réseaux sociaux mais aussi par l'usage des messageries instantanées. Ces messageries viennent concurrencer la messagerie traditionnelle autant dans la sphère professionnelle que personnelle. **Leur interdiction devient délicate et oblige les collectivités à ériger des règles d'usage.**

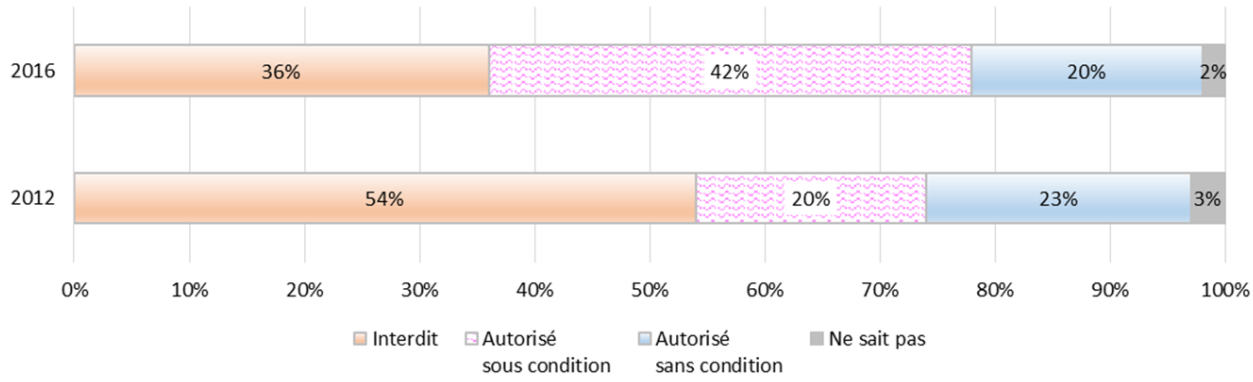


Figure 98 - Utilisation de messagerie instantanée externe

Thème 14 : Acquisition – Développement et maintenance du SI

Une activité de développement, marginale, qui ne motive pas la mise en place de cycles sécurisés

En première lecture nous pourrions nous étonner de l'absence de cycles de développement sécurisés dans les Collectivités. Ce chiffre est à relativiser au regard de leurs activités de développement. Depuis plusieurs années, l'ensemble des collectivités privilégie le progiciel, raréfiant ainsi le développement d'outils et par voie de conséquence, l'opportunité de mettre en œuvre des cycles sécurisés.

Ce peu d'engagement dans une démarche de développement sécurisé n'est pas de bon augure concernant les exigences spécifiques des Collectivités Territoriales auprès des éditeurs de leurs progiciels.

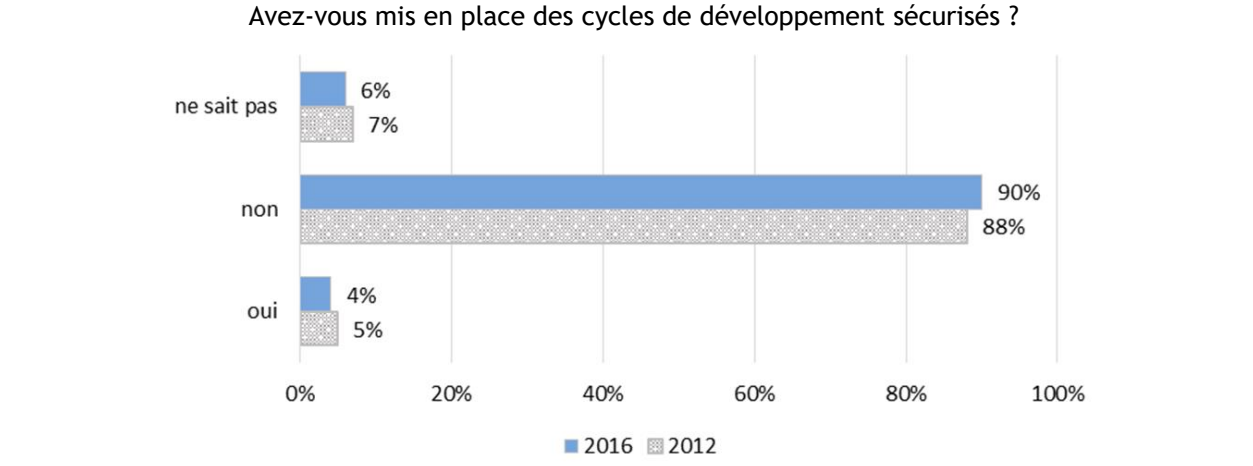


Figure 99 - Cycles de développement sécurisés

Thème 15 : Relations avec les fournisseurs

Vers une réinternalisation des systèmes d'information ?

70% des Collectivités ne font pas appel à l'infogérance pour prendre en charge leur système d'information. C'est le même taux qu'en 2008 mais c'est 10 points de plus qu'en 2012.

S'il y a quasiment deux fois moins de Collectivités qui déclarent avoir placé en totalité leur système d'information sous contrat d'infogérance qu'en 2012, ce chiffre est principalement lié au recul dans les plus petites collectivités. Bien qu'à un niveau très faible, 4% des Conseils Territoriaux et 3% des Villes ont franchi le pas. Cela représente une progression, respectivement de 60% et 88% en 4 ans.

L'appel à l'infogérance partielle est plus mitigé, puisque le taux passe de 26% à 21%. Seules les Villes ont une pratique en augmentation (+30%).

La baisse constatée des services infogérés s'accompagne néanmoins d'une progression significative de la maturité et des pratiques vis-à-vis des tiers. Désormais, 61% (+11 points) des collectivités suivent cette infogérance par des indicateurs de sécurité.

Les services infogérés continuent à être audités au même niveau qu'en 2012, mais d'une manière légèrement moins systématique.

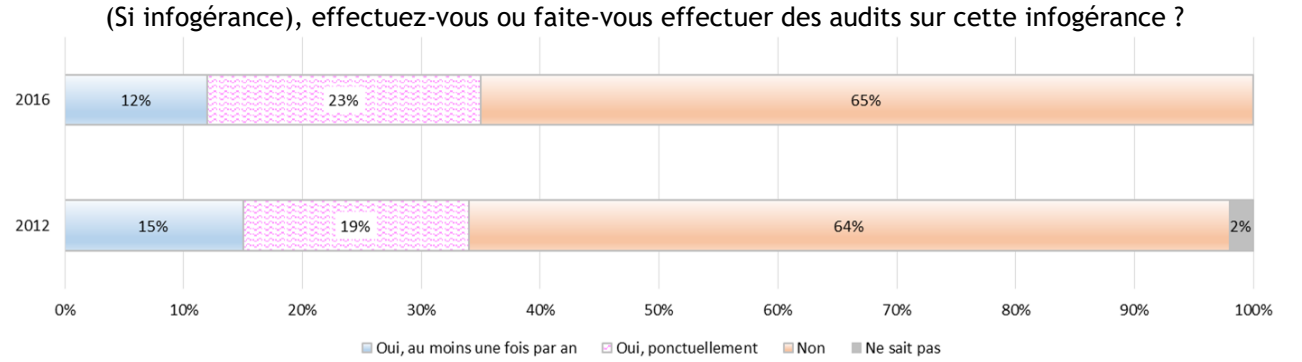


Figure 100 - Audits infogérés

L'informatique dans le nuage (cloud), un usage en forte progression dans les Collectivités

L'usage de l'informatique dans le nuage (cloud) **progresse de plus de 120%** depuis 2012

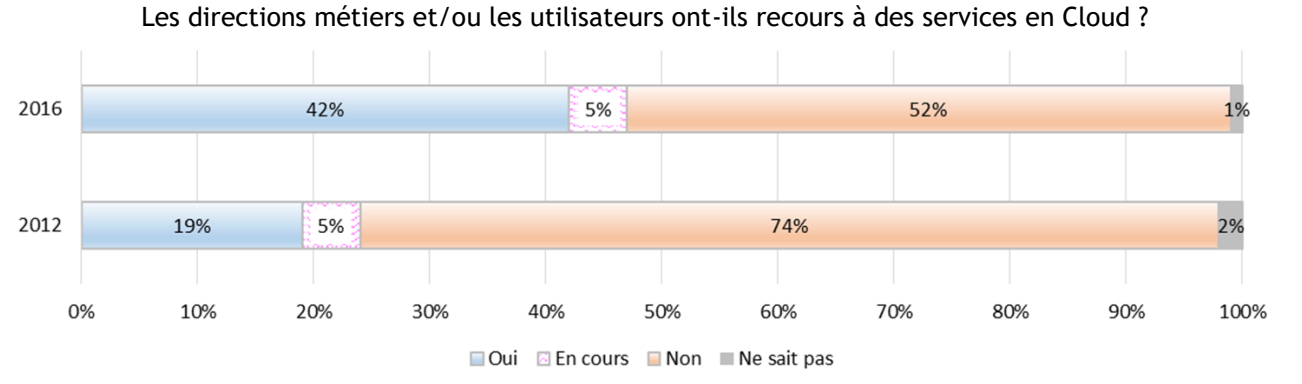


Figure 101 - Services en Cloud

Même si cela reste majoritairement du cloud privé, la part de cloud public ou de cloud hybride augmente significativement (+50% pour le public, +38% pour l'hybride).

Est-ce le reflet de l'utilisation de ce type de service amené par les agents au sein des Collectivités ?

L'usage du cloud reste sous contrôle de la DSI ou du RSSI pour 72% des sondés. Toutefois, dans ce cas, seulement 10% ont formalisé une politique expliquant ce qui est autorisé ou pas (5% sont en cours de formalisation).

On peut raisonnablement penser que l'informatique dans le nuage est source de perte de contrôle d'une partie du système d'information par les directions informatiques, ainsi près de 25% des collectivités n'a pas la main sur l'usage du cloud fait par ses agents.

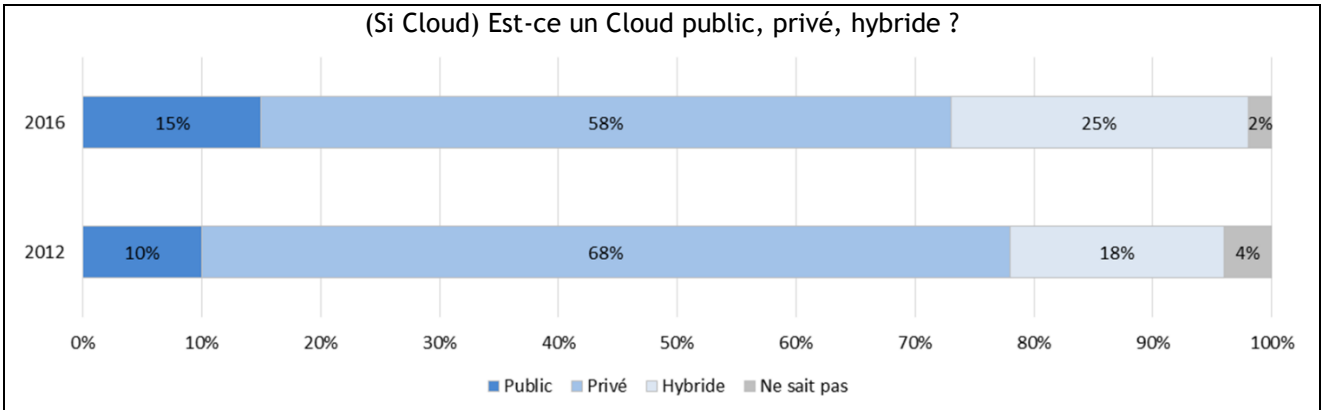


Figure 102 - Type de Cloud

Thème 16 : Gestion des incidents SSI

Survenue des incidents : Une sinistralité en mutation

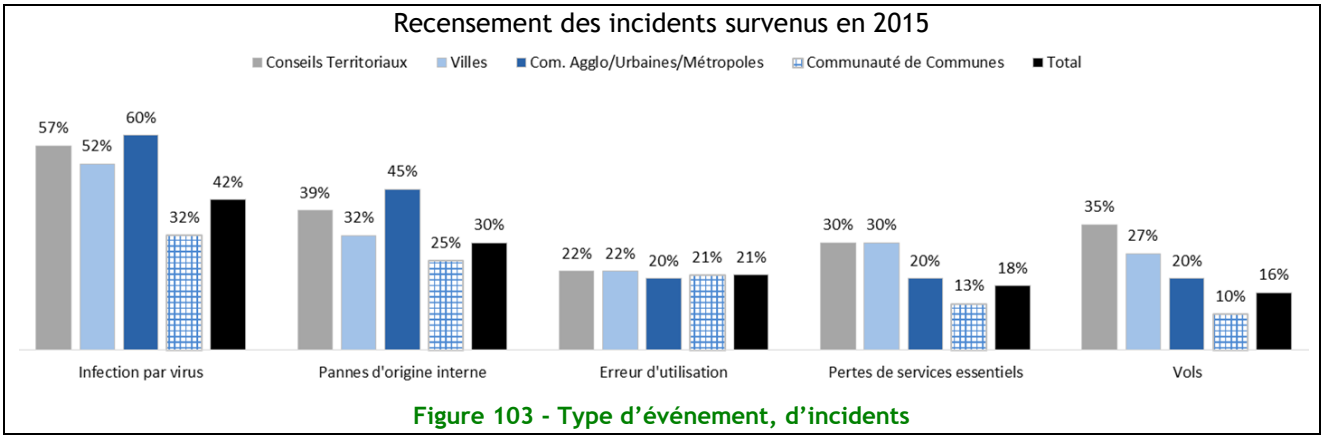


Figure 103 - Type d'événement, d'incidents

Les pertes de services essentiels sont en recul constant depuis 2008 : elles représentaient 44% en 2008, 27% en 2012 pour atteindre 18% en 2016.

Les sinistres les plus fréquemment observés sont désormais les infections par virus, les pannes d'origine interne et les erreurs d'utilisation, avec une très forte augmentation des attaques virales (progressant de 25% en 2012 à 42% en 2016). Ces proportions sont comparables à celles rencontrées au sein des entreprises.

Le phishing est le vecteur d'attaque le plus utilisé et près d'une Collectivité Territoriale sur trois s'est trouvée confrontée à une campagne de ce type. Cela souligne la nécessité de conduire des campagnes régulières de sensibilisation à destination des utilisateurs finaux. Cependant, l'impact de ces incidents est encore jugé majoritairement non significatif même si une grande majorité (82%) des Collectivités n'évalue pas les conséquences financières réelles lors de la survenue d'incidents.

L'impact financier pourrait augmenter si la tendance constatée en entreprise se vérifie au sein des Collectivités : seules 4% des Collectivités ont été confrontées à des attaques de types rançons ou fraudes aux présidents contre 26% des entreprises, mais les techniques nécessaires à l'exécution de ces attaques (de type malware de chiffrement par exemple) se démocratisent, rendant ces attaques simples et rapidement lucratives. Les Collectivités Territoriales sont peut-être mieux protégées des « fraudes aux présidents » par les procédures de contrôle de la comptabilité publique. Ces procédures ne les protègent pas pour autant des conséquences d'une infection virale d'un rançongiciel.

Une gestion de la sinistralité en stagnation

Nous notons **un léger recul depuis 2012 dans l'appréhension des incidents de sécurité** dans les collectivités territoriales. Depuis 2012 , les organisations ont sans doute évolué, d'un RSSI qui s'occupait seul de la collecte des incidents, nous sommes passés à un partage des tâches avec les équipes opérationnelles qui font une première analyse, le RSSI se positionnant en deuxième niveau. Cette gestion est toutefois accompagnée par un meilleur ciblage des incidents associés à l'informatique de gestion (81%, +9 points)

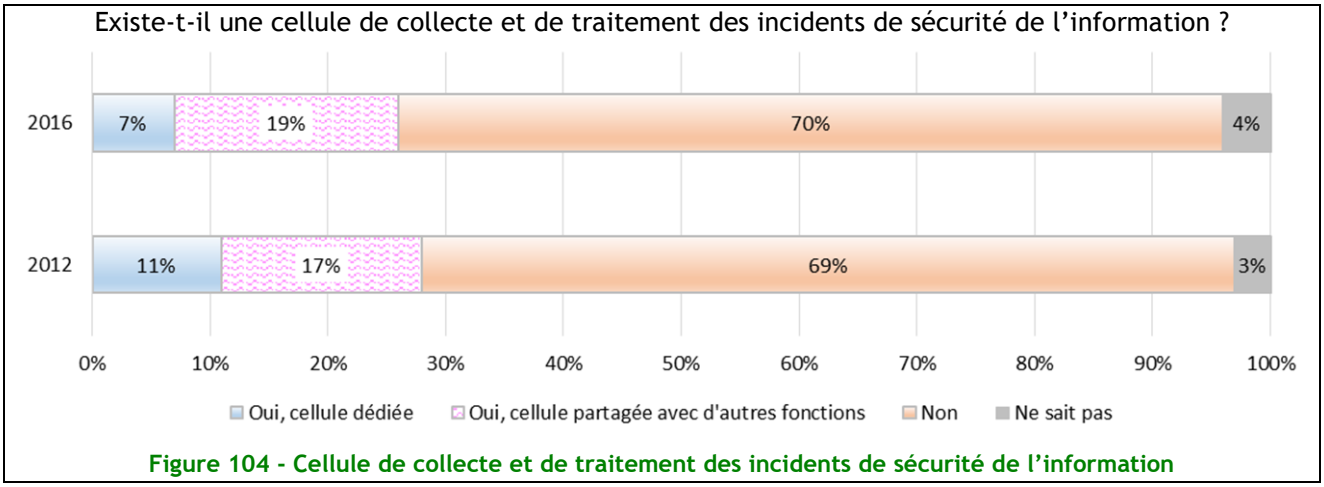


Figure 104 - Cellule de collecte et de traitement des incidents de sécurité de l'information

Si une collectivité sur 3 ne connait pas la durée maximale des incidents qu'elle a subi, 39% la mesure à moins d'une journée et seulement 6% à plus de 3 jours.

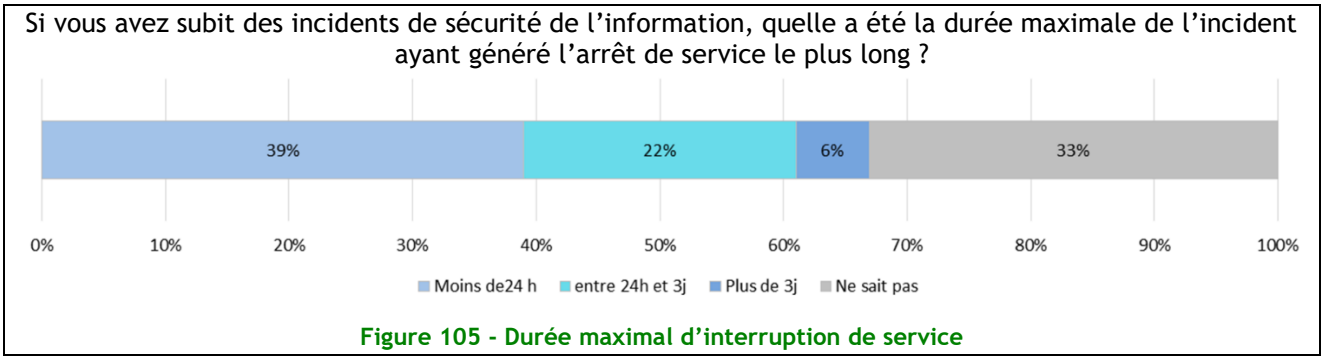


Figure 105 - Durée maximal d'interruption de service

Quand elles subissent des incidents, les Collectivités sont 3 fois plus nombreuses qu'en 2012 à déposer plaintes. Ce chiffre reste toutefois faible, autour de 13%, malgré les efforts des autorités pour faciliter les procédures de déclaration et la mise à disposition de services spécialisés.

Thème 17 : Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité

Les Collectivités en progrès en matière de continuité de l'activité

Grâce à une belle amélioration depuis 2012 (+8 points), on constate **que 54% des Collectivités disposent de processus de gestion de la Continuité d'Activité**. Sur ce point, les Communautés de Communes sont en queue de peloton (47% d'entre-elles ont des processus en place) et les Conseils Territoriaux sont, à contrario, sur la bonne voie (74%).

Globalement, on constate une meilleure prise en compte de l'indisponibilité des locaux et des ressources humaines mais une baisse dans la prise en compte des systèmes informatiques de gestion, ce qui est relativement surprenant.

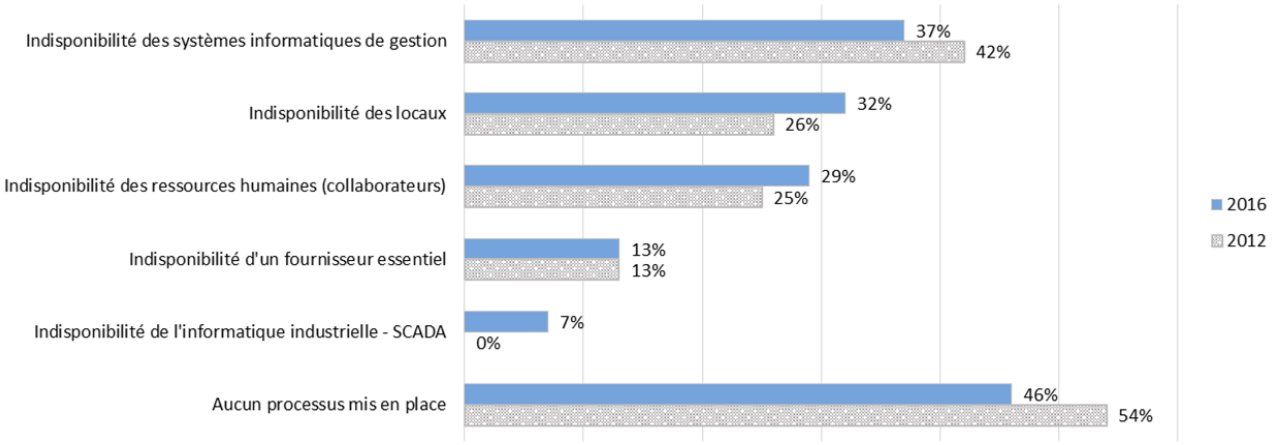


Figure 106 - La gestion de la continuité d'activité

Par rapport à 2012, quasiment la moitié des Collectivités testent leur plan de continuité d'activité, ce qui constitue une légère amélioration. Les Communautés de Communes sont une nouvelle fois en retrait sur ce point (62% ne teste jamais leur PCA) et les Villes sont en meilleure position (35%).

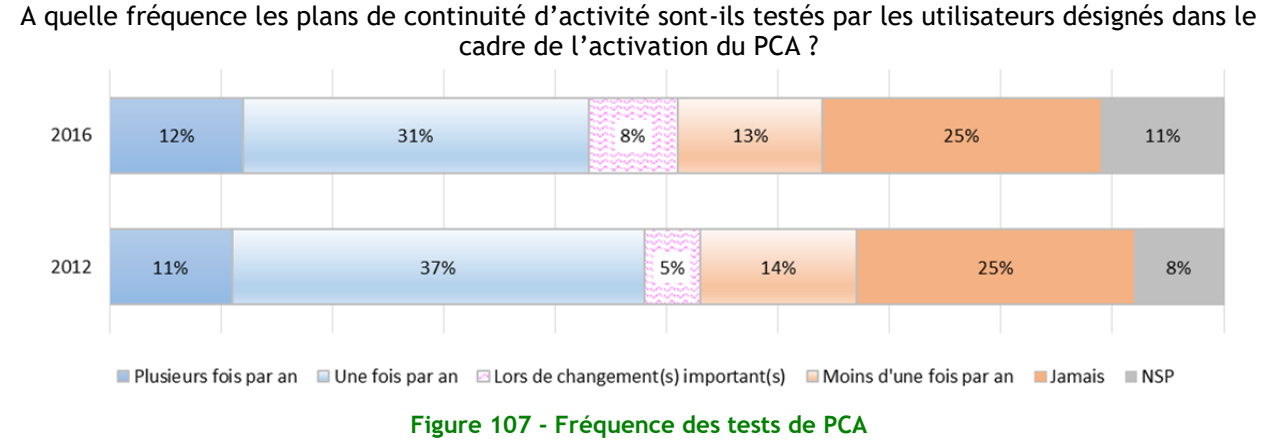


Figure 107 - Fréquence des tests de PCA

On constate une légère augmentation des tests de plans de continuité/reprise d'activité informatiques, quasiment la moitié des Collectivités étant concernées. Là encore, les Communautés de Communes sont en retrait sur ce point (61% ne testent jamais leur PCI) et les Villes sont, elles, en meilleure position (30%).

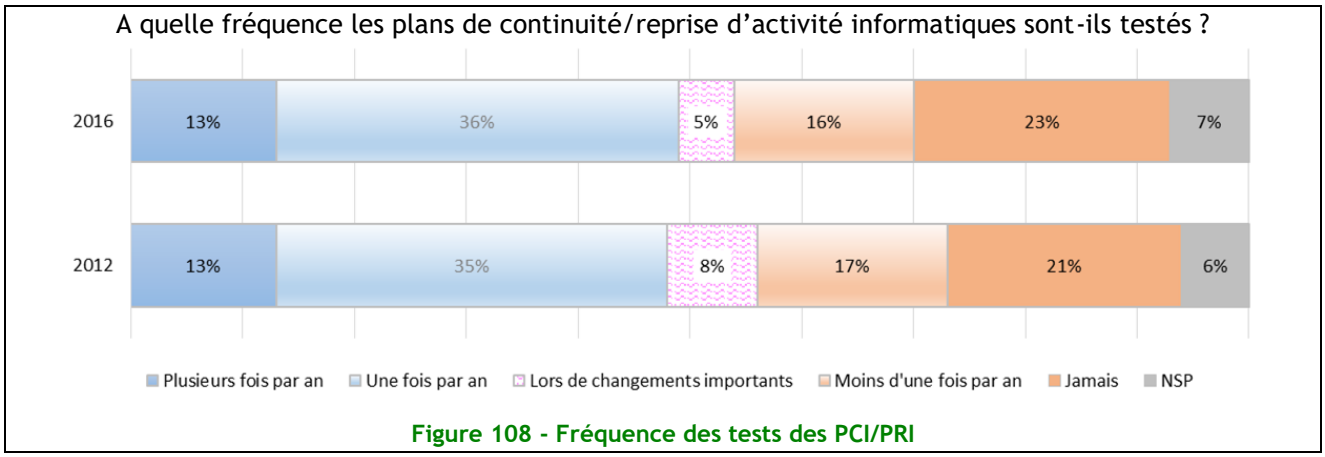


Figure 108 - Fréquence des tests des PCI/PRI

Là où 59% des Entreprises couvrent, via des tests, 75 à 100% des solutions mises en place, seules 43% des Collectivités le font, confirmant les disparités visibles entre les deux secteurs dans les différents tests pouvant être effectués.

Une nouvelle fois les Villes se démarquent, elles sont 55% à tester à 75% les solutions mises en place.

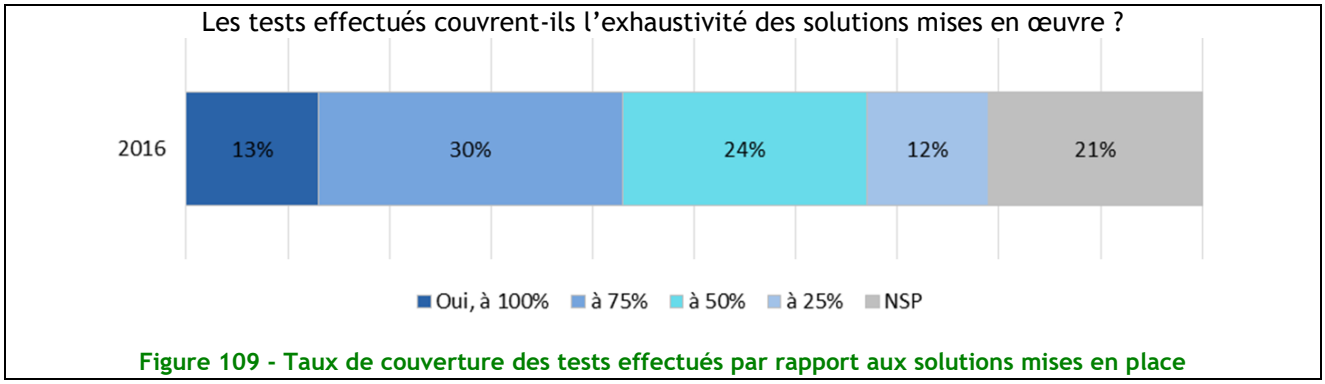


Figure 109 - Taux de couverture des tests effectués par rapport aux solutions mises en place

Dernier aspect important à souligner, plus d'un quart des Collectivités seulement ont une gestion de crise formalisée. A noter que les Communautés de Communes font largement pencher la balance : représentant 62% des sondés, elles sont 12% à avoir une gestion de crise formalisée. Les autres catégories de sondés tournant plutôt autour de 52%, chiffre qui se rapproche de ce que l'on peut trouver concernant les Entreprises.

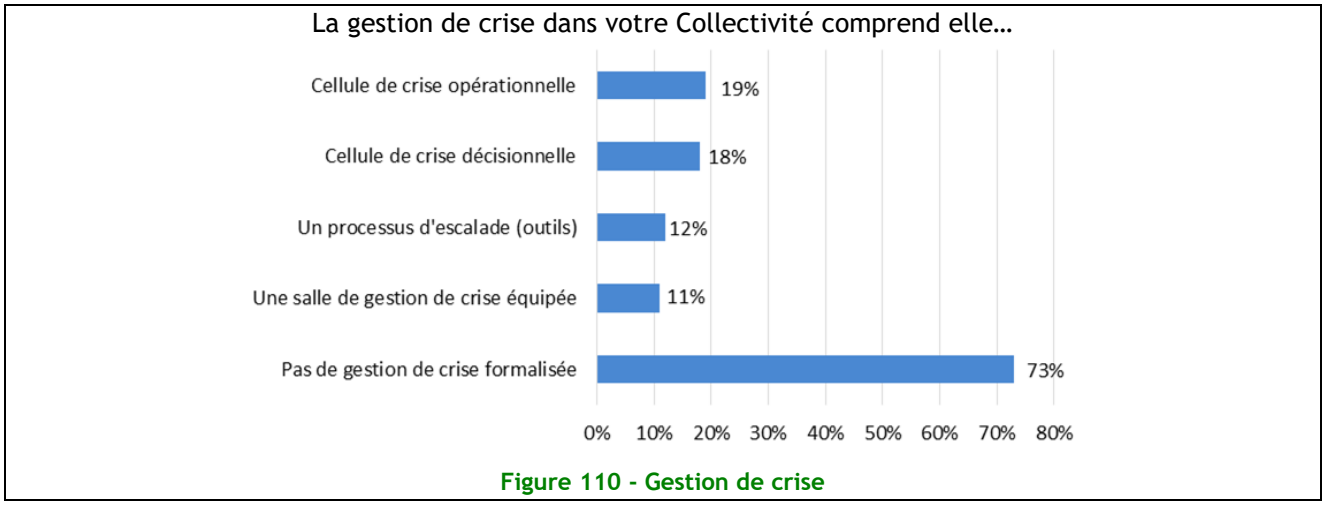


Figure 110 - Gestion de crise

Thème 18 – Conformité

Conformité aux obligations légales et réglementaires loin d'être complète

La conformité aux obligations de la CNIL est globalement stable comparée à l'étude précédente. La légère évolution des chiffres montre une meilleure prise en compte de ces obligations. Notons que le Règlement Européen voté en avril de cette année donne 2 ans aux Collectivités pour ce mettre en totale conformité, avec des règles plus contraignantes.

A votre avis, votre Collectivité est-elle en conformité avec les obligations de la CNIL ?

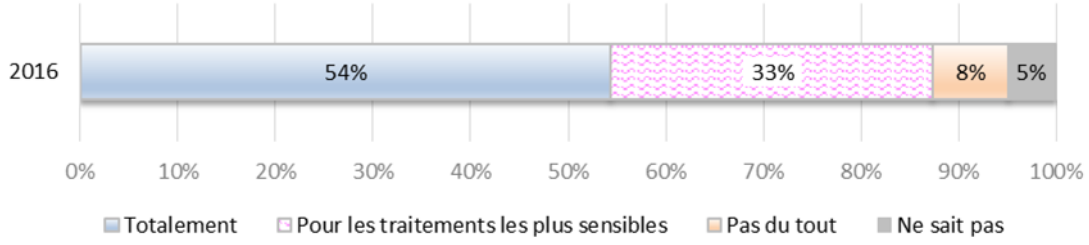


Figure 111 - Obligations de la CNIL et conformité

Le taux de Correspondant Informatique et Liberté (CIL) nommés continue de progresser pour passer de 31% en 2012 à 38% en 2016. Le nombre de nominations prévues (4%) ou à l'étude (8%) est plus faible qu'en 2012. Le nombre de collectivités sans CIL reste important (46%) principalement dans les Communautés de Communes (56%) et les Communautés d'Agglomération (38%).

Votre Collectivité a-t-elle désigné un Correspondant Informatique et Liberté (CIL) tel que défini par la CNIL ?

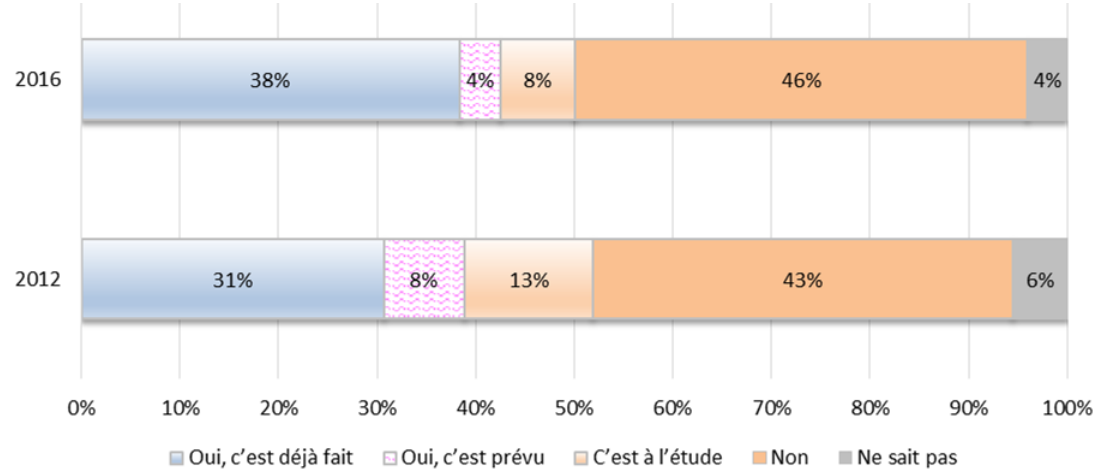


Figure 112 - Désignation d'un CIL

L'existence ou non du CIL peut être très nettement reliée au niveau de connaissance des Collectivités vis-à-vis des lois et/ou règlementations spécifiques en matière de sécurité de l'information. Comme en 2012, les Conseils Territoriaux témoignent d'une plus grande connaissance de leurs obligations légales (61%)

Le Règlement Européen sur la protection des données personnelles a été adopté le 27 avril 2016 et publié au Journal Officiel le 4 mai 2016 – après notre enquête. Cette réforme globale doit permettre à l'Europe de s'adapter aux nouvelles réalités du numérique. Immédiatement applicable en France, les entreprises et les Collectivités devront être en totale conformité pour 2018. Nous prêterons une attention particulière aux impacts de cette nouvelle réglementation lors de notre prochaine enquête.

La conformité RGS (Référentiel Général de Sécurité) progresse sensiblement (44% contre 37% en 2012). Là encore, une forte disparité existe entre les Communautés de Communes (26%) et les autres Collectivités Territoriales qui sont conformes à plus de 70%.

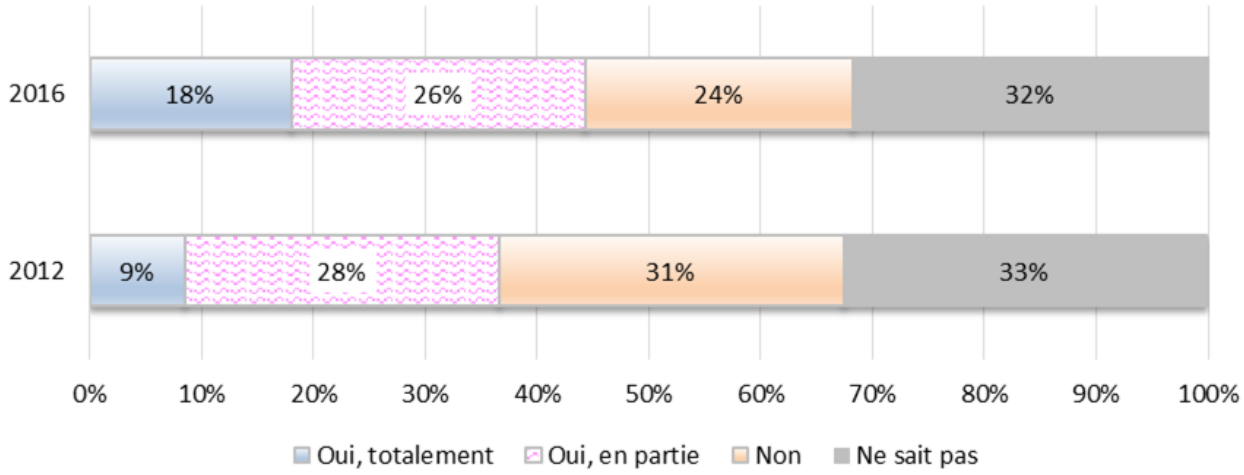


Figure 113 - Conformité au RGS ?

Tableaux de bord : un faible niveau de suivi

Près de 9 collectivités sur 10 ne mettent pas en place des tableaux de bord relatifs à la sécurité de l'information. Le taux de mise en place des tableaux de bord progresse uniquement de 2 points depuis 2012. Ils existent surtout dans les Villes (22%) et les Communautés d'Agglomération, Urbaines et Métropoles (28%).

Sur le panel qui se trouve de fait limité, les indicateurs mis en place ont essentiellement un intérêt opérationnel (76%) ou de pilotage des fonctions SSI (30%). Dans 21% des cas, ils ont également un intérêt stratégique et sont exploités par les directions générales.

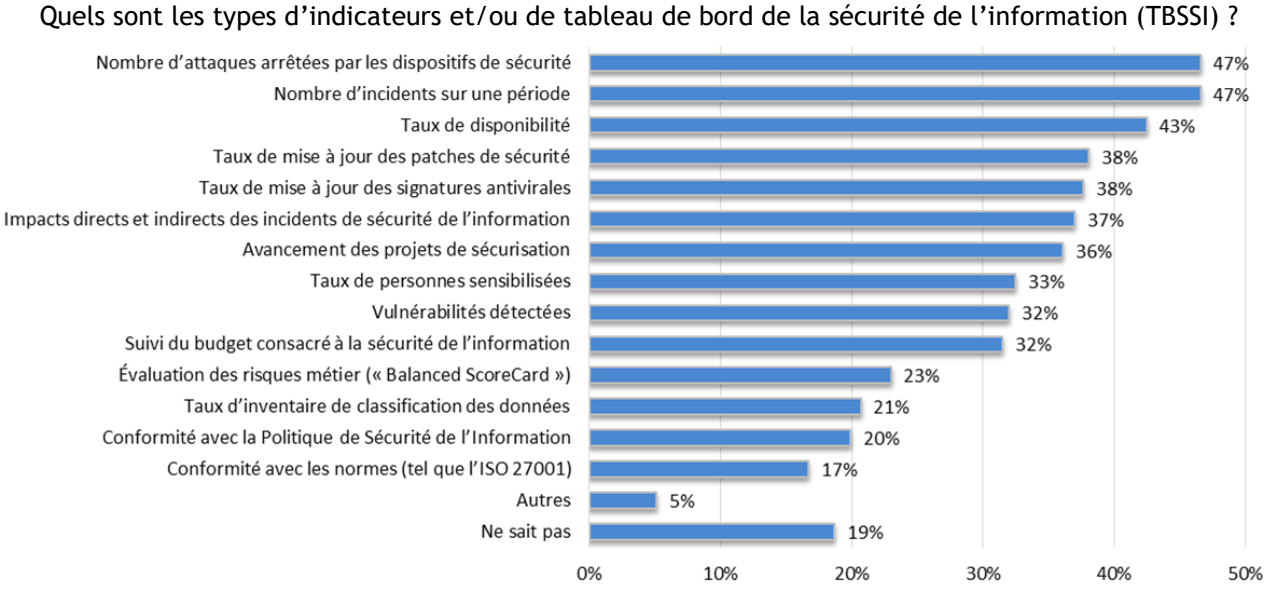


Figure 114 - Types d'indicateurs et/ou de tableau de bord de la SSI

Audit des systèmes d'information, peu de contrôle effectif

43% des collectivités interrogées effectuent des audits, alors que près de **53% n'en effectuent aucun** sur une année. D'après les personnes interrogées, la tarification des tests d'intrusion serait encore très onéreuse.

Combien d'audits ou de contrôles de sécurité du Système d'Information sont menés en moyenne au sein de votre Collectivité sur une période de 2 ans ?

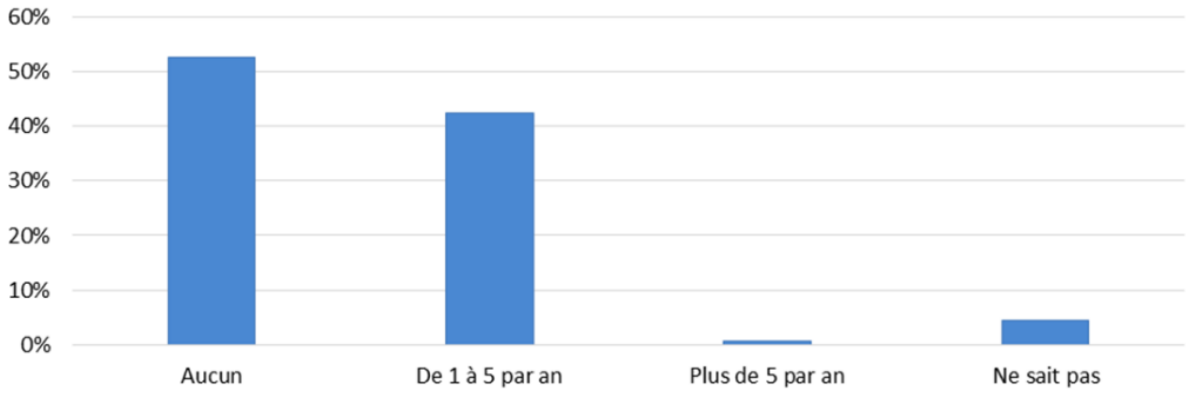


Figure 115 - Audits et contrôles de SSI sur une période de 2 ans

Les audits sont principalement techniques (architecture, intrusion, configuration). L'absence de réponse sur la classification des audits relève principalement des Communautés de Communes (41%) alors que les autres Collectivités semblent mieux maîtriser ce type de processus.

Quels types d'audit ou de contrôles de sécurité du Système d'Information sont menés au sein de votre Collectivité ?

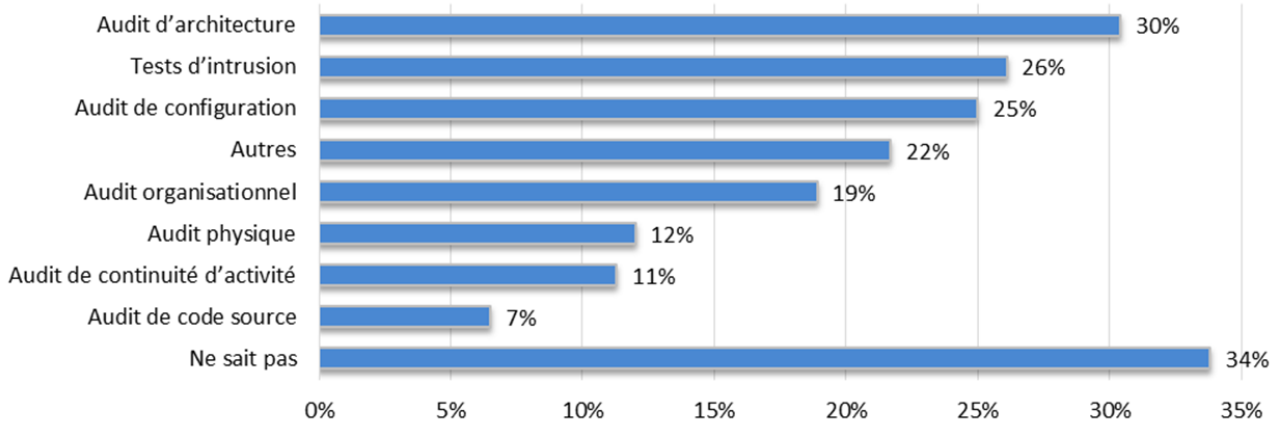


Figure 116 - Types d'audit et de contrôles de sécurité du SI

La motivation des audits est nettement moins marquée qu'en 2012. Néanmoins, la PSSI et les incidents restent les principaux facteurs déclenchant, surtout pour les Conseils Territoriaux (61% et 30% respectivement). Les exigences contractuelles et réglementaires sont également décisives dans une moindre mesure, tout en se situant au-delà de 23% pour les Conseils Territoriaux et les Villes.

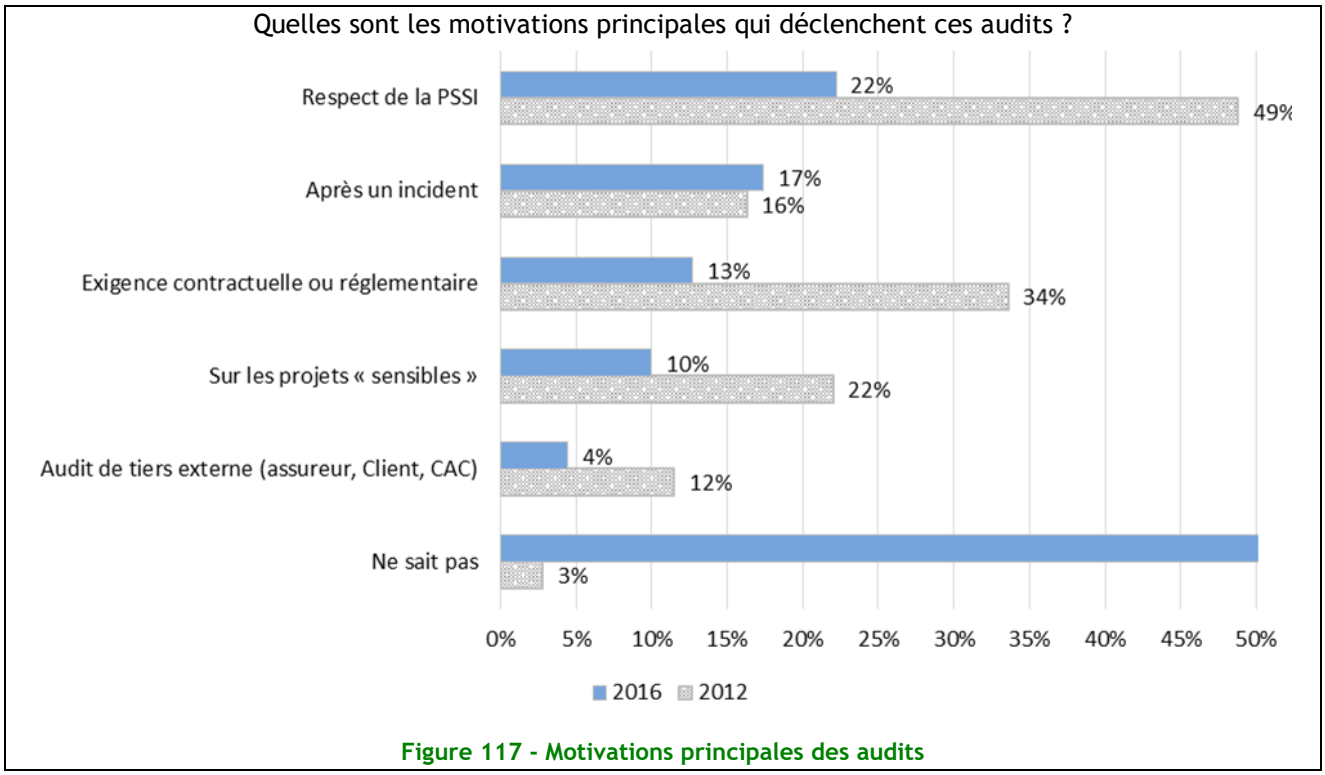


Figure 117 - Motivations principales des audits

Internautes

- Identification et inventaire ordinateur et smartphone
- Usage de l'internaute
- Perception de la menace et sensibilité de l'utilisateur aux risques et à la sécurité de l'Information
- Moyens et comportements de sécurité mis en œuvre par l'internaute

Les internautes

Présentation de l'échantillon

Le CLUSIF s'est efforcé cette année encore de mesurer les perceptions et les comportements des internautes quant aux enjeux de sécurité du numérique. Ainsi, l'échantillon d'internautes de cette année 2016 est très semblable à celui étudié il y a deux ans, avec 1008 personnes de 15 ans et plus ayant répondu à l'étude et se répartissant de la façon suivante :

- 49% d'hommes et 51% de femmes,
- 45% ont moins de 45 ans, 30% ont plus de 60 ans,
- 55% d'actifs, 45% d'inactifs (étudiants, sans emploi ou retraités),
- 40% ont des enfants à la maison (en couple ou parents isolés).

Les statistiques issues de cette enquête ont été réalisées par le cabinet spécialisé GMV Conseil s'appuyant sur un panel d'internautes de GMI, leader mondial et plus gros Access Panel en France.

L'échantillon final a fait l'objet, comme lors des études précédentes, d'un redressement sur les données de signalétique et par rapport aux données connues sur le plan national : sexe, âge, région, type d'agglomération, FAI, pratique d'Internet, etc.

Partie I – Identification et inventaire ordinateur et smartphone

Une consultation de l'Internet via des équipements mobiles…

En 2016 l'ordinateur portable se maintient comme mode de connexion le plus utilisé pour accéder à l'Internet suivi de très près par le smartphone. Le smartphone détrône l'ordinateur fixe sur la 3e marche du podium.

Quels équipeemnts (professionnels ou personnels) utilisez-vous pour vous connecter à Internet à votre domicile ?

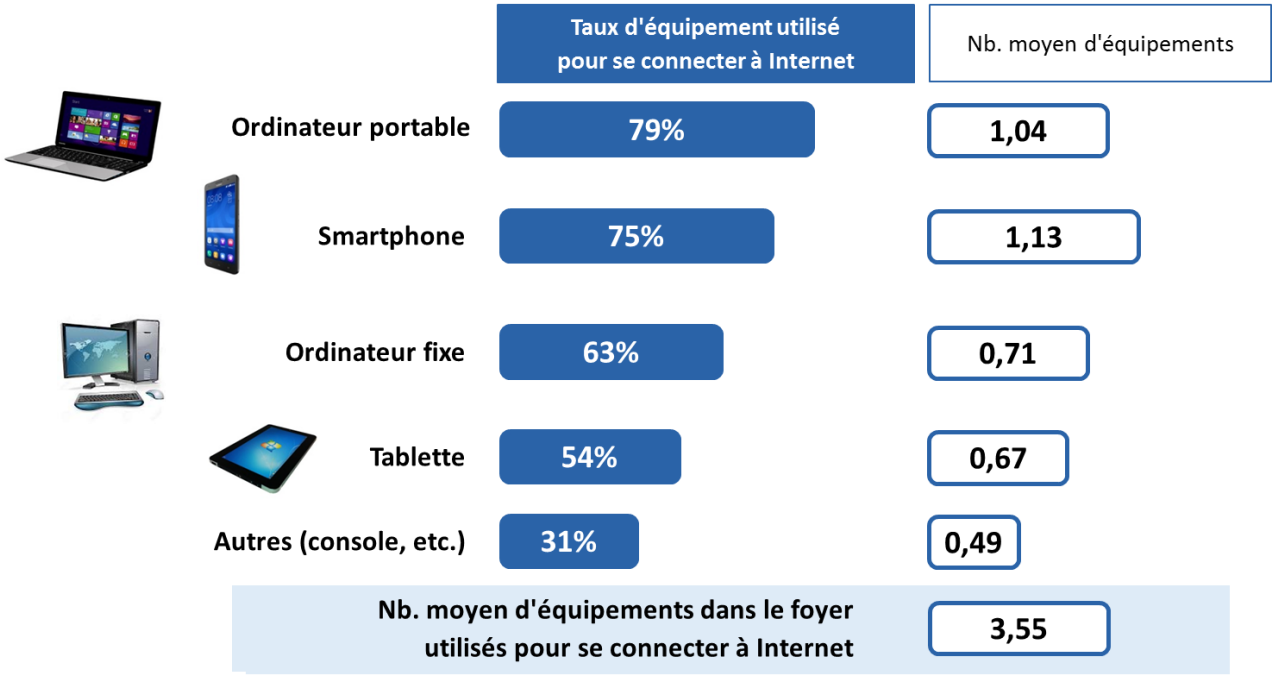


Figure 118 - Équipements utilisés pour se connecter à Internet

L'utilisation de la tablette pour accéder à l'Internet progresse également de manière conséquente (+15 points) confirmant la tendance à l'usage des objets mobiles comme mode de connexion privilégié par les Internautes.

Il est surprenant de constater une baisse du nombre moyen d'équipements par foyer (3,55 en 2016 contre 4,6 en 2014) capables de se connecter à l'Internet. L'explication possible est un non renouvellement des équipements historiques comme les ordinateurs fixes, au profit des smartphones et tablettes et de leur versatilité, associés aux services de stockage dans le nuage.

En dehors de votre domicile, vous connectez-vous à Internet avec un ou plusieurs équipements mobiles (ordinateur portable, tablette, smartphone) ?

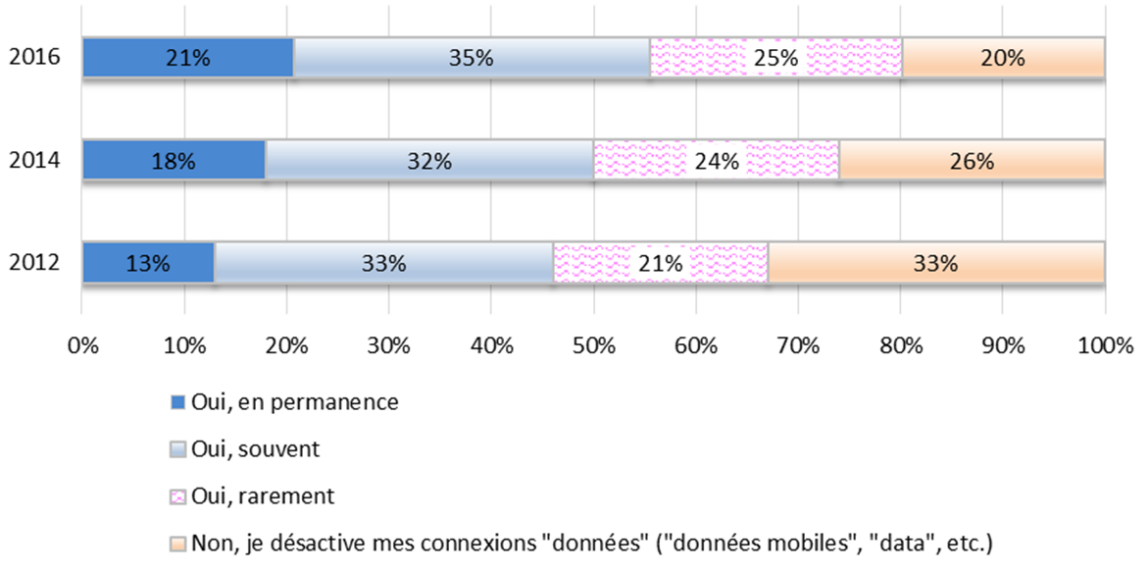


Figure 119 – Taux de connexion permanente à Internet sur les terminaux mobiles

Pour ce qui est de la mobilité, le nombre de français toujours connectés ou souvent connectés à l'Internet en dehors de leur domicile, suit une hausse régulière sur la période 2014 à 2016 comparativement à celle constatée entre 2012 et 2014 (de l'ordre de 5 points). Dans le même temps, le nombre de ceux qui ne se connectent jamais à l'aide de leur équipement mobile recule également selon une pente constante de 7 points. Ceci peut s'expliquer par la forte baisse des tarifs des forfaits mobiles, l'augmentation du parc de smartphones et la généralisation de la 4G apportant un réel confort de navigation.

Objets connectés dans les foyers en stagnation

Mis à part une hausse continue du nombre de téléviseurs connectés (+7 points), le nombre des autres types d'objets connectés se maintiennent ou connaissent un léger recul, contrairement à la période 2012 – 2014.

Parmi les objets suivants, qu'est ce qui est connecté à Internet chez vous ou dans votre sphère personnelle ?

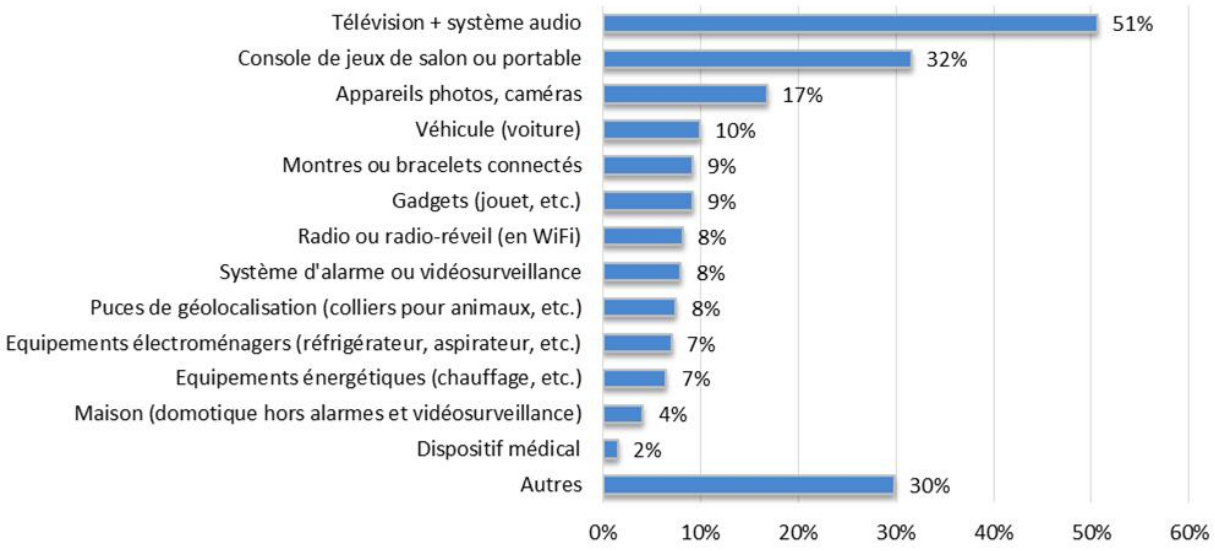


Figure 120 - Connexion à Internet dans votre sphère personnelle

La moyenne par foyer d'objets connectés se stabilise donc à 2. Et ce, malgré l'apparition de nouvelles catégories d'objets connectés comme les montres ou bracelets et les appareils photos.

Partie II - Usages de l'internaute

Le Wifi toujours plébiscité

En 2016 ce n'est pas moins de 85% d'internautes qui optent pour la connexion à l'Internet via Wifi.

Cette progression de 6 points sur la période 2014-2016 peut s'expliquer par la progression du parc d'ordinateurs portables, de tablettes et smartphones, équipements embarquant tous en natif des modules Wifi. Cette impression se confirme par la forte baisse du pourcentage de l'explication « mon équipement est dépourvu de capacité Wifi » comme raison de la non utilisation du Wifi comme mode de connexion au domicile.

A votre domicile, utilisez-vous une connexion Wifi (sans fil) pour vous connecter à Internet ?

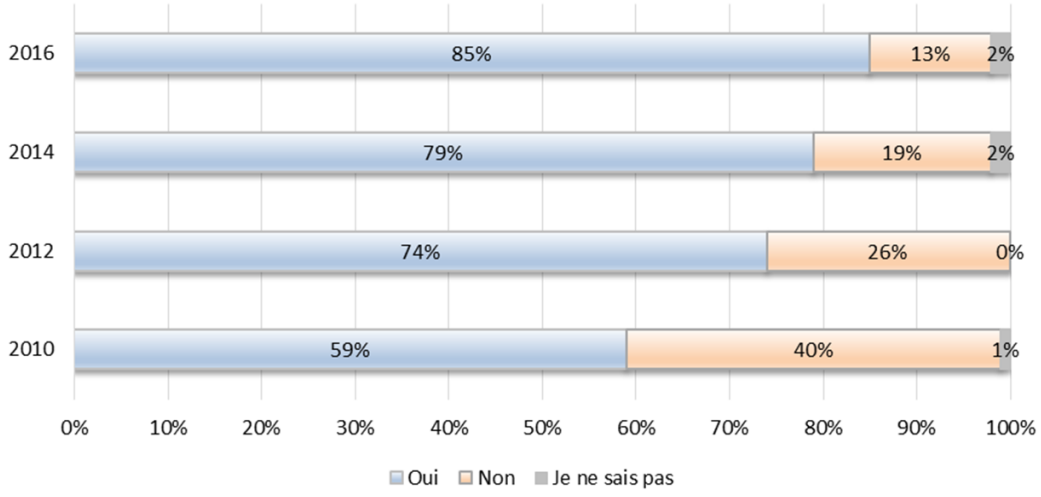


Figure 121 - Connexion Wifi (sans fil)

Le mélange des genres professionnel/personnel en cours de résorption ?

Bien que toujours élevé il est intéressant de noter que **le nombre de personnes interrogées faisant usage d'équipements professionnels dans leur sphère privée recule (- 4 points). Ceci, quelle que soit la catégorie socioprofessionnelle.**

Dans une moindre mesure, l'inverse est également en recul. En effet l'utilisation d'équipements personnels à des fins professionnelles baisse de 2 points.

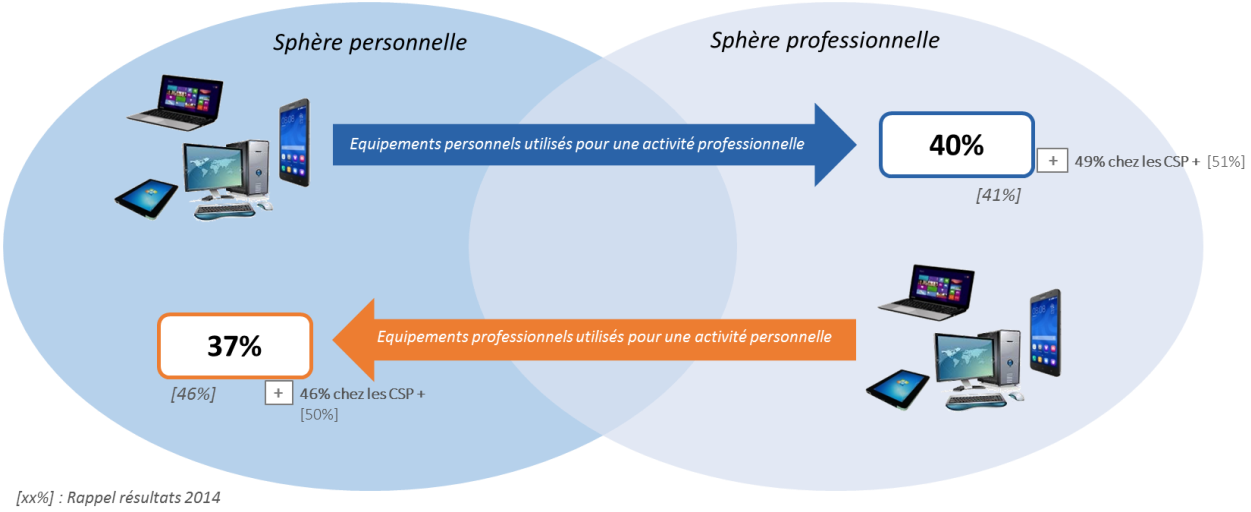


Figure 122 - Usage des équipements

Le BYOD reste tout de même utilisé par quasiment une personne sur deux pour les catégories socioprofessionnelles supérieures contre moins d'un sur trois pour les autres.

La raison de cette amorce de cloisonnement des matériels pour leur usage dédié est peut-être à chercher dans le durcissement des chartes informatiques et politiques des sociétés.

Ce comportement n'est en revanche pas signe d'un retour à une meilleure séparation de vie personnelle et professionnelle. Pour preuve la proportion, en constante augmentation (27% à 40%), de personnes se connectant à distance à leur réseau d'entreprise grâce à l'accès Internet de leur domicile.

L'économie collaborative mise à part, pas de révolution dans les usages de l'Internet.

Depuis 2014, on observe très peu de changement au niveau national en ce qui concerne les lieux de connexion à l'Internet : ils s'effectuent majoritairement depuis le domicile et seulement dans un cas sur 3 à l'extérieur.

Il est néanmoins à noter que, du fait du taux élevé de leur équipement en terminaux mobiles/nomades et de cet usage propre à leur génération, les plus jeunes sondés (15-29 ans) sont beaucoup plus nombreux que les autres à se connecter en mobilité totale (48% d'entre eux contre au mieux 36% pour leurs aînés de 30 à 44 ans et un peu moins de 2% pour les 75 ans et plus).

A titre personnel, sur Internet (sur smartphone ou ordinateur), quelles sont vos habitudes ?

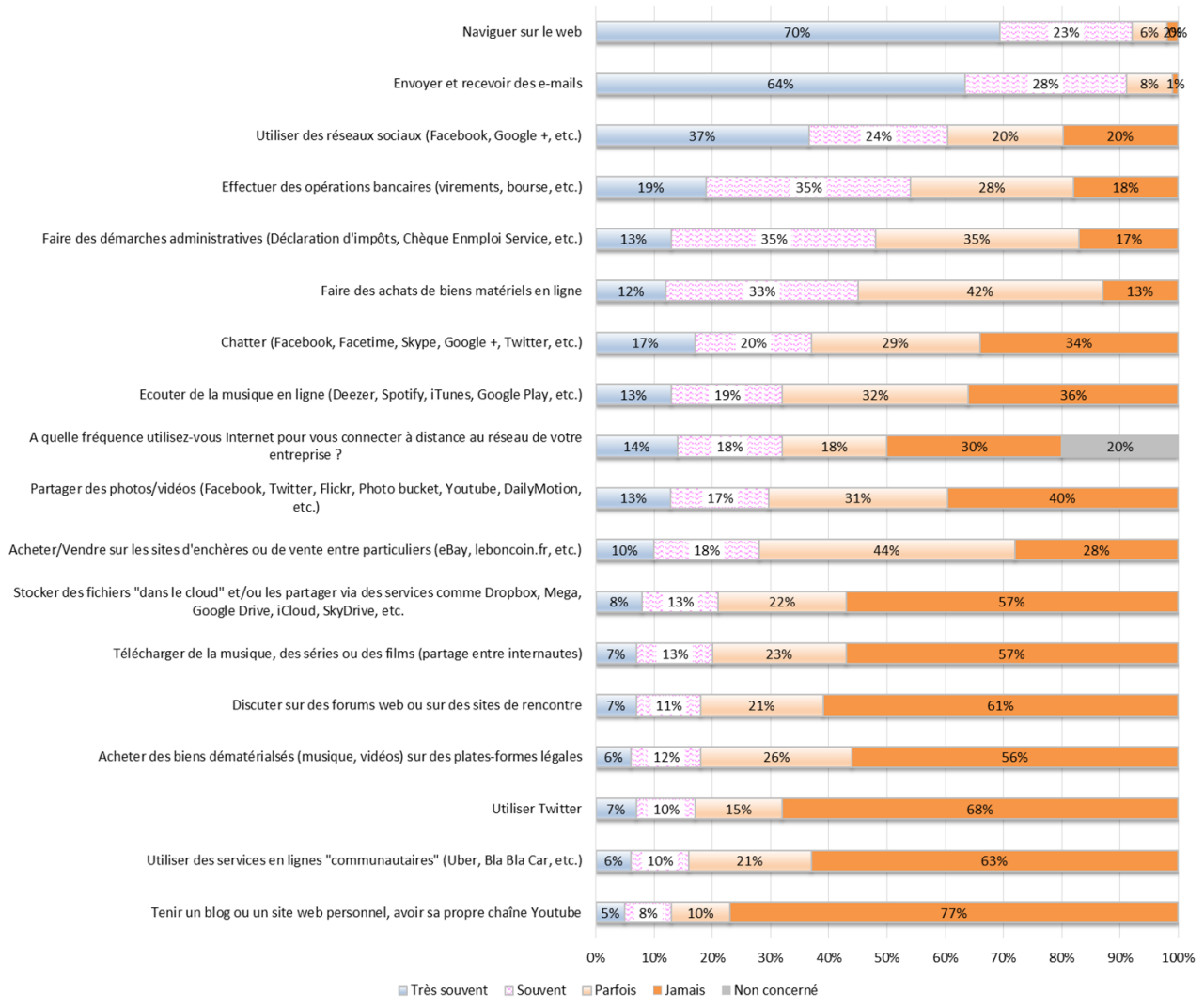


Figure 123 - Nature de l'usage de l'Internet

L'utilisation faite de l'Internet quant à elle se diversifie un peu plus.

Nous voyons par exemple que le phénomène de société récent dit d'économie collaborative, rendu possible principalement grâce aux nouvelles technologies, est bien présent : 16% des personnes interrogées en moyenne disent utiliser ce genre de service en ligne.

Encore une fois, le contexte générationnel oblige, les 15-29 ans sont même jusqu'à 1 sur 3 a souvent ou très souvent faire appel à ces nouveaux services.

Utilisez-vous des services en ligne communautaire (économie collaborative) ?

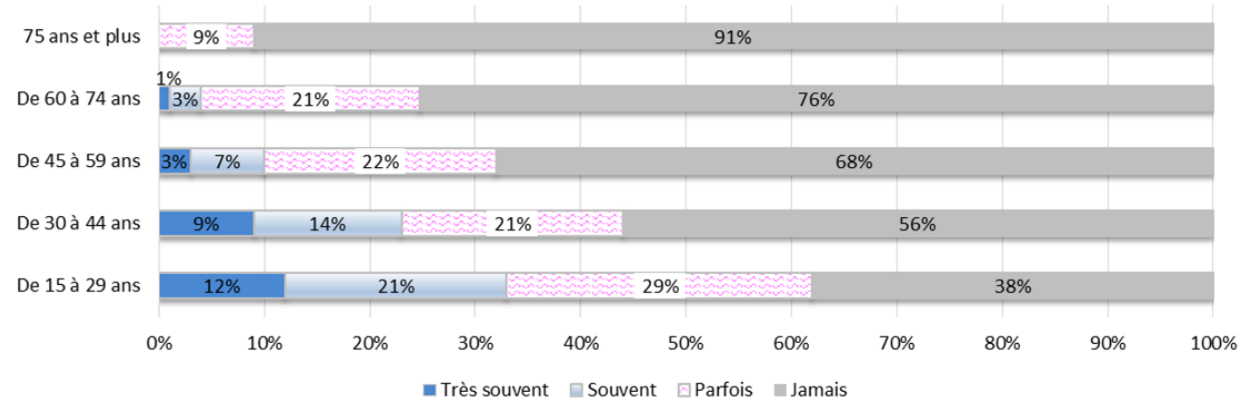


Figure 124 – Utilisation des services de l'économie collaborative selon les tranches d'âge

Les services de stockage dans le nuage, autre usage récent, ne progressent pas vraiment depuis 2014 pour les données personnelles pour lesquelles le stockage local est toujours privilégié. Ce point est détaillé par la suite (voir la section Utilisation du « cloud » : une grande incertitude page 96).

Néanmoins l'usage du « Cloud » pour le stockage des données professionnelles connait un meilleur succès (44% contre 30% pour les données personnelles).

Pour le reste, outre les classiques navigations sur la toile et gestion des e-mails qui représentent 9 cas sur 10 il est possible de voir deux autres grands scénarios d'utilisation se détacher :

- Avoir ou maintenir un lien social :

  60 % des sondés indiquent utiliser les réseaux sociaux souvent ou très souvent, 37% d'entre eux chatter et un peu moins de 30% partager leurs photos et vidéos,

- Se faciliter la vie courante :

  Avec la généralisation des services Internet dédiés à la personne, les Internautes effectuent de plus en plus de leurs démarches administratives en ligne (48% en 2016 contre 40% en 2014). Les opérations bancaires via Internet sont également largement utilisées (un tout petit peu plus d'une personne interrogée sur deux).

  L'acte d'achat en ligne est toujours aussi naturel qu'en 2014 même s'il connait une légère baisse pour les biens matériels neufs (- 5 points). Les achats/ventes d'occasion, les enchères ou entre particuliers reste constants. La vente de biens dématérialisée est en nette progression, 44% des internautes interrogés ayant au moins acheté une fois ce genre de produit, contre 35% d'entre eux seulement en 2014.

Le paiement en ligne oui, mais sous conditions.

Ce dernier aspect de la vie courante, l'achat en ligne est à mettre en relation avec le comportement du paiement en ligne.

En effet, s'il est devenu pour lui banal d'acheter en ligne, l'internaute sait rester vigilant lorsque vient le moment de payer. L'achat sans condition reste faible quel que soit le type de terminal (18% pour les ordinateurs, 9% pour les terminaux mobiles).

Il faut noter que le paiement sur Internet progresse nettement : ils sont 54% à ne jamais payer sur terminal mobile en 2016 contre 67% en 2014, idem sur les ordinateurs avec 8% en 2016 contre 11% en 2014.

L'achat (sous condition ou non) sur PC fixe ou portable reste nettement privilégié au détriment des smartphones et tablettes (74% vs 34%). On peut y avoir une question d'habitude mais également une question d'âge : on constate que les 15-29 ans paient ou sont prêts à payer depuis leur terminal mobile à 53%, alors que l'on passe à 30% pour les plus de 45 ans et 20% pour les plus de 75%. La stabilité de la connexion en mode mobile peut également être un frein à ces achats par crainte que la transaction ne reste dans un état incertain en cas de perte de réseau.

Les conditions requises majoritairement par les Internautes qui paient sur Internet sont essentiellement liées à la confiance (82% mettent comme condition que le site soit sécurisé, 61% que le paiement soit

sécurisé, 51% que le site ait une notoriété importante et 44% que le site dispose d'un intermédiaire de paiement). L'habitude est également un critère important.

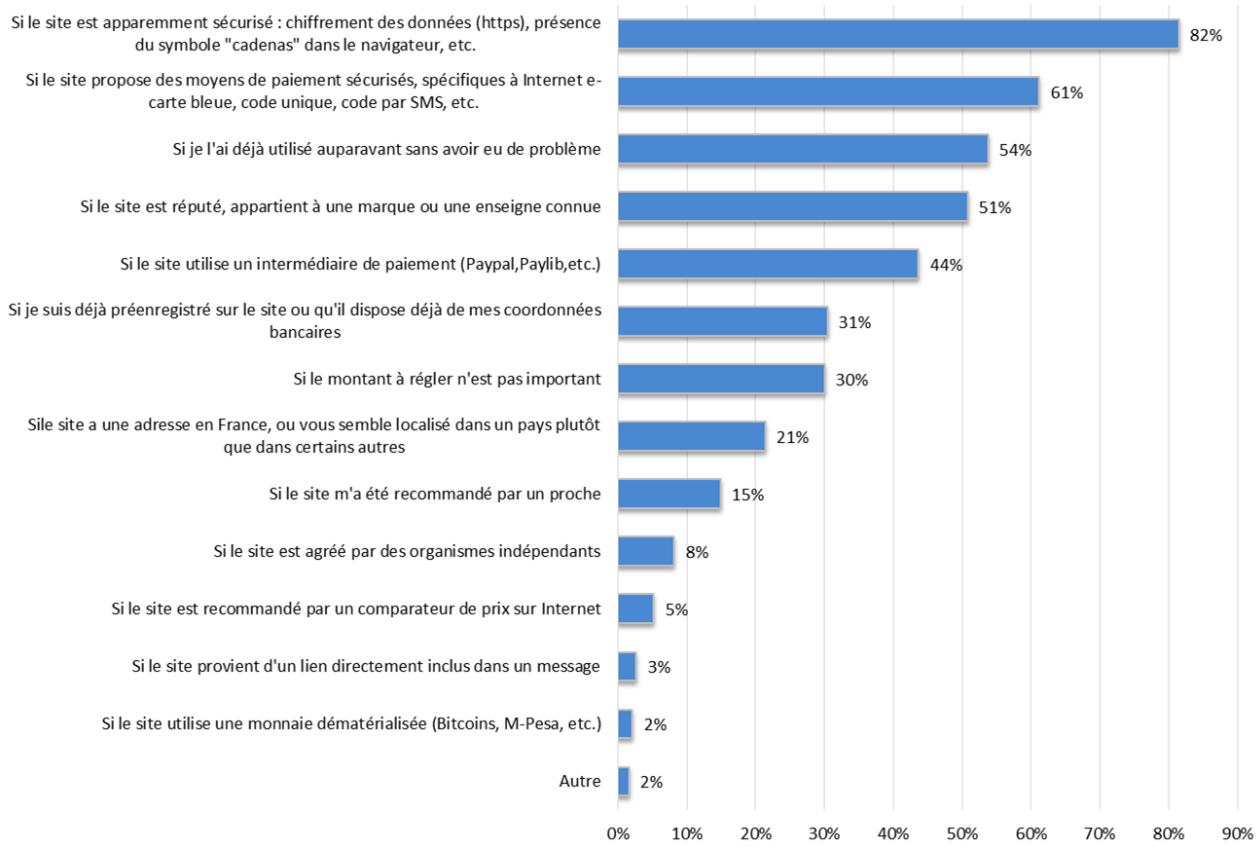


Figure 125 - Conditions requises par les internautes pour réaliser un paiement sur Internet

Concernant le recueil de données personnelles via la réponse à des questionnaires, la situation est assez stable par rapport à 2014 : 2/3 des sondés acceptent de le faire s'ils ont confiance dans le site qui les interroge, 12% le font sans conditions.

La situation diffère cependant en fonction de l'âge : les 15-29 ans acceptent de répondre sans conditions à 17% alors que les plus de 75 ans n'acceptent qu'à 5%. De même seuls 15% des 15-29 ans n'acceptent jamais de répondre alors qu'ils sont 28% chez les plus de 75 ans.

En synthèse, les usages ont peu évolué depuis 2014 et le besoin de confiance reste important. Ce qui a changé concerne les moyens d'accès à Internet : les smartphones et tablettes progressent fortement face aux ordinateurs fixes ou mobiles, même s'ils ne les ont pas encore rattrapés.

Partie III – Perception de la menace et sensibilité de l'utilisateur aux risques et à la sécurité de l'information

Les menaces d'Internet : une perception en hausse

Si la perception des risques sur les données personnelles (documents, photos, vidéos, etc.) avait fortement augmenté entre 2012 et 2014, elle est notablement stable cette année, en ce qui concerne les ordinateurs fixes ou portables.

Pour les smartphones et tablettes, la confiance continue de se dégrader : les internautes qui ne perçoivent aucun ou peu de risques pour leurs données sont aujourd'hui 27% contre 30% en 2014.

Quels risques pensez-vous qu'Internet fait courir à vos données (documents, photos, vidéos, etc.) ?

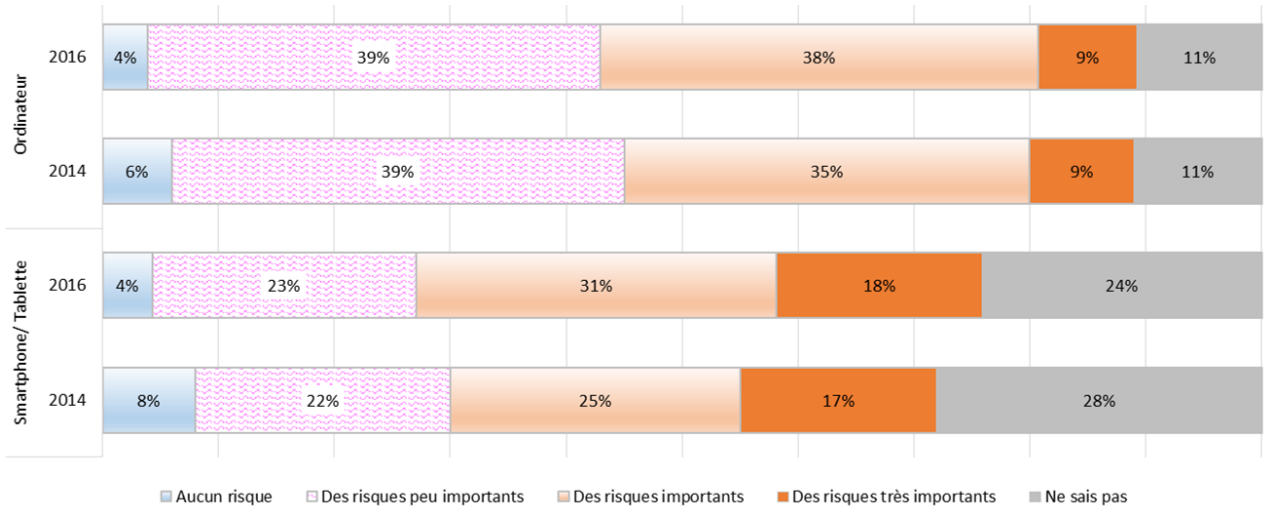


Figure 126 - Perception du risque concernant les données stockées sur les équipements connectés

Comme on le notait déjà en 2014, si la perception des risques a fait de gros progrès sur les ordinateurs, les internautes manquent sans doute encore de visibilité pour ce qui concerne les tablettes et les smartphones.

Des menaces sur la vie privée très largement perçues

Globalement, 89% des personnes interrogées estiment qu'il est important de protéger sa vie privée, voire très important pour 48% d'entre elles.

La perception des menaces d'Internet sur la vie privée reste extrêmement forte. 70% des personnes interrogées estiment qu'Internet met leur vie privée en danger (dont 17% fortement) et cette perception est inchangée depuis 2014.

On note par contre une différence sensible en fonction de l'âge des internautes. Les plus jeunes ont une plus grande perception du danger d'Internet que leurs ainés : 75% chez les moins de 30 ans, 68% chez les 30 à 44 ans et les plus de 60 ans.

Selon vous, Internet met-il en danger votre vie privée ?

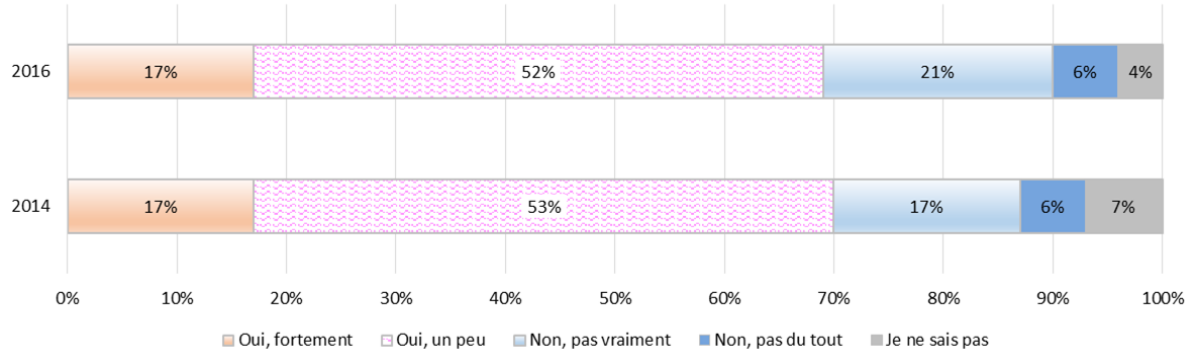


Figure 127 – Perception du danger d'Internet pour la vie privée

Les personnes interrogées sont encore plus inquiètes pour les mineurs : 93% d'entre elles pensent qu'Internet présente un danger pour les mineurs, que ce soit sur un ordinateur ou sur un équipement mobile (tablette ou smartphone). Sans surprise, seuls les plus jeunes minimisent quelque peu cette perception (10% chez les moins de 30 ans).

Une note rassurante : par rapport à 2014 on observe que les jeunes attachent plus d'importance à la protection de leur vie privée : ils sont 11% à penser qu'elle n'a pas d'importance, contre 19% lors de la précédente enquête.

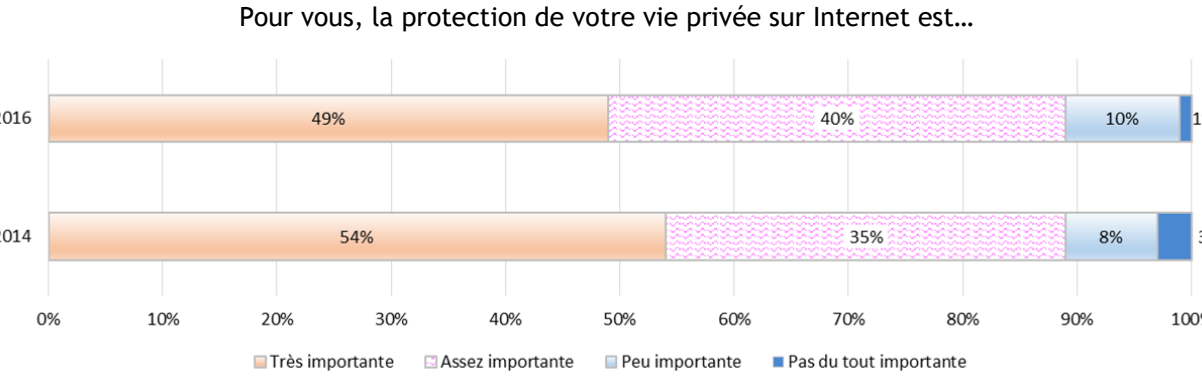


Figure 128 – Importance de la vie privée

Précautions de base : la moitié des internautes y pensent

Malgré cette perception du danger, les internautes ne semblent pas majoritairement savoir comment s'en protéger.

Ainsi, parmi ceux qui utilisent les réseaux sociaux, seuls les deux tiers (63%) disent vérifier et modifier régulièrement les réglages des paramètres de sécurité et de confidentialité de leur profil sur les réseaux sociaux.

Si l'on note, sans surprise, que le taux d'utilisation des réseaux sociaux diminue fortement avec l'âge (de 91% pour les moins de 30 ans à 69% pour les plus de 60 ans), on constate également que la prudence diminue, le taux de réglage des paramètres diminuant des plus jeunes (68%) aux plus âgés (58%).

Le constat est assez similaire pour ce qui concerne la protection dans le cadre de l'OS utilisé. En moyenne, seuls 51% des internautes disent modifier régulièrement les paramètres de sécurité et de confidentialité de leur profil sur le système d'exploitation (Windows, Linux ou Mac OS) de leur PC.

Vérifiez-vous et modifiez-vous régulièrement les paramètres de sécurité et de confidentialité de votre profil sur les réseaux sociaux/les OS ?

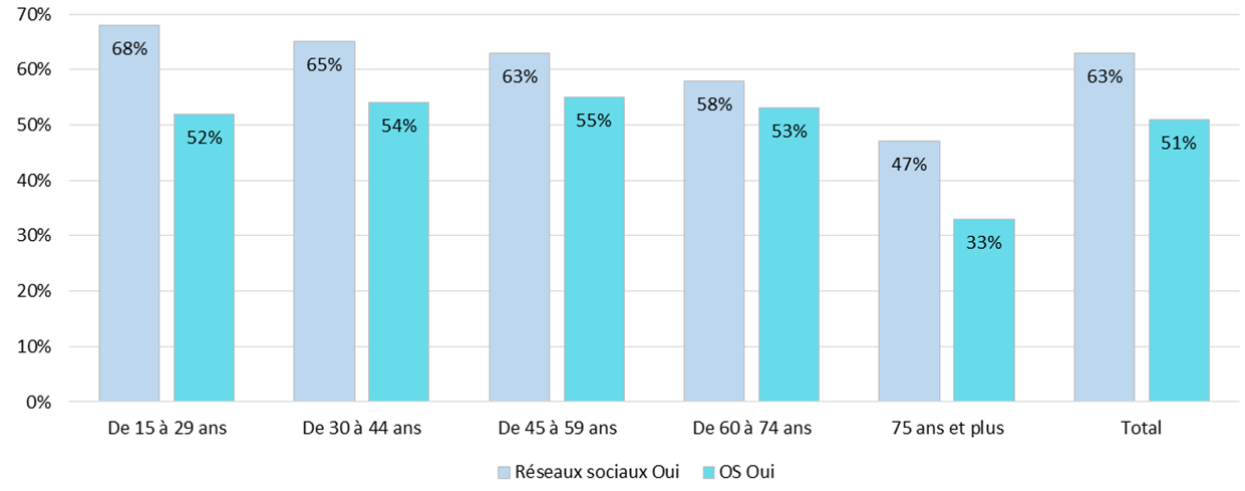


Figure 129 – Taux de surveillance des paramètres de profil selon l'âge

Utilisation du « cloud » : une grande incertitude

Interrogés sur la perception des risques du stockage dans le « cloud » vis-à-vis de la perte et de la destruction des données, ou sur leur confidentialité, plus d'un tiers des internautes avouent de pas savoir arbitrer le niveau de risque entre le « cloud » et le stockage local.

Pour ceux qui se prononcent, le stockage local parait légèrement plus sûr pour la confidentialité (33%) mais plus risqué (31%) pour la perte/destruction de données.

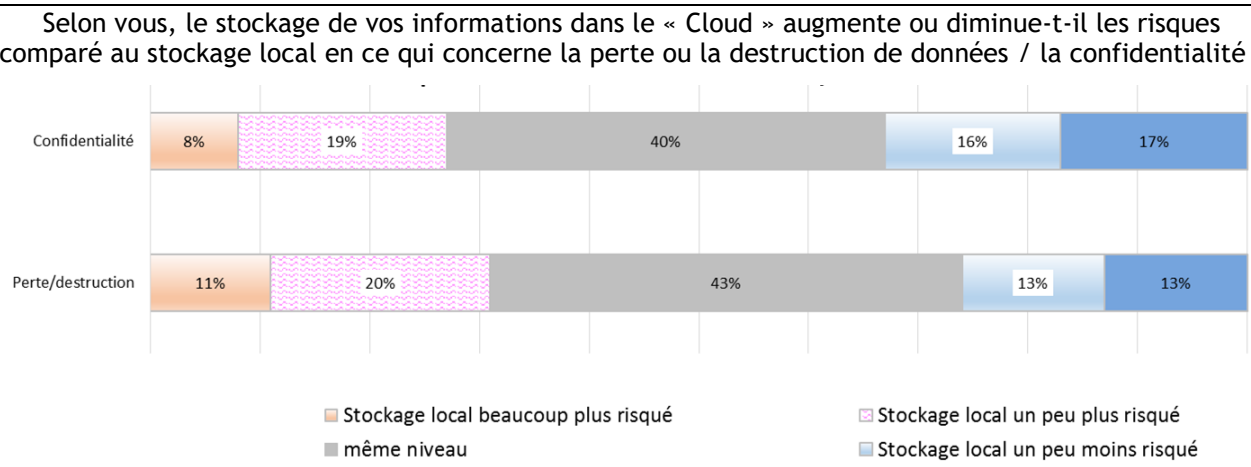


Figure 130 – Perception du risque du « Cloud » par rapport au stockage local

Perte ou vol de données : baisse sensible sur les PC

Si une personne sur 4 (24%) déclare avoir subi la perte ou le vol de données sur un ordinateur au cours des deux dernières années, la tendance qui se confirmait lors des deux précédentes enquêtes (35% en 2014) semble en voie de diminution.

Sur les équipements mobiles, la perte de données est en légère baisse (15%). Elle est bien moins fréquente que sur les postes de travail, ce qui s'explique sans doute par un usage plus encadré sur ce type de matériels où l'utilisateur ne dispose que de peu d'accès au système.

Interrogés pour la première fois cette année sur l'environnement « cloud », les internautes formulent un taux de perte de données sensiblement inférieur à celui des équipements personnels. Cela s'explique certainement par un accès plus difficile à l'environnement système, et par les moyens de protection intrinsèques de ce type d'environnement.

Dans les 24 derniers mois, avez-vous subi une perte ou un vol de données qui étaient stockées sur votre ordinateur, sur votre smartphone ou votre tablette, dans le Cloud ?

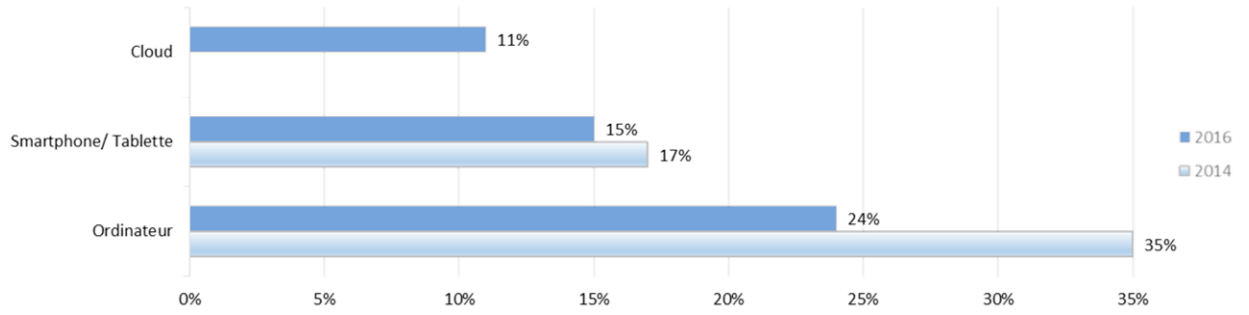


Figure 131 – Perte de données subie sur un ordinateur, un équipement mobile ou dans le Cloud

Sur PC, la panne et l'erreur de manipulation ne sont plus les causes majeures (5% et 4% contre 10% et 9% en 2014), ce qui pourrait s'expliquer par une maturité croissante des internautes.

Pour quelle(s) raison(s) avez-vous perdu ces données ? (plusieurs réponses possibles)

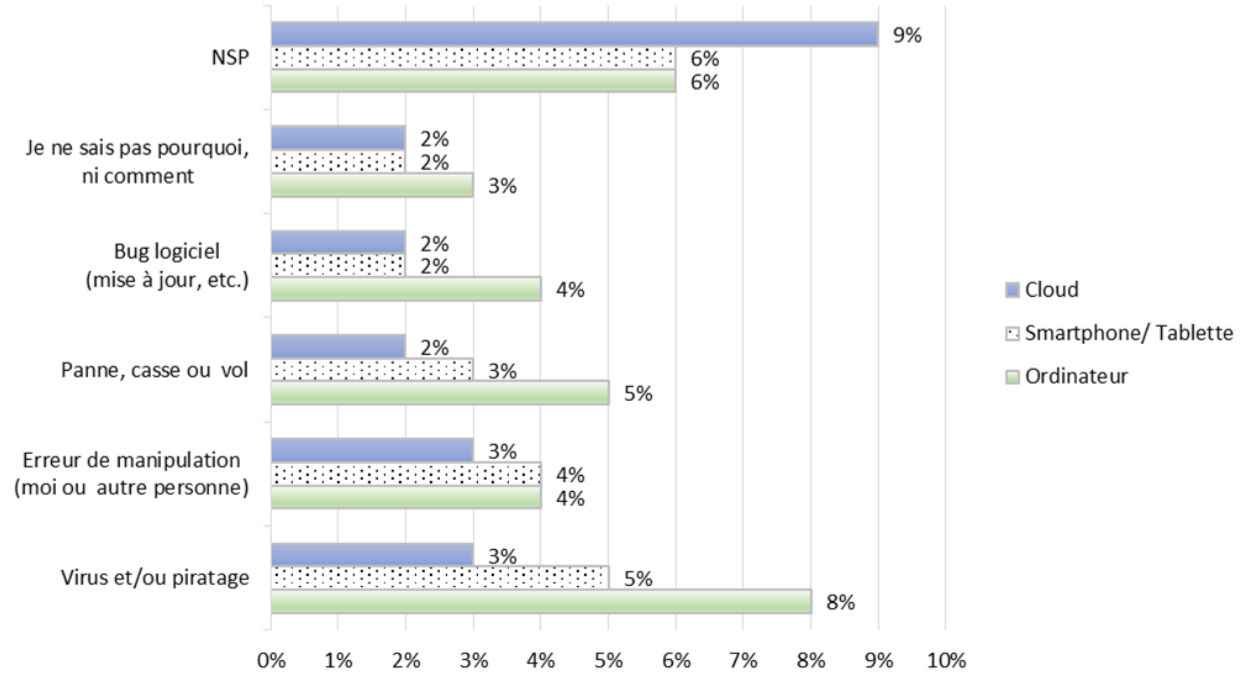


Figure 132 – Raisons des pertes de données sur un ordinateur, un équipement mobile ou dans le Cloud

Évolution de la menace sur les équipements informatiques

Les internautes estiment toujours très largement (45%) que les dangers pesant sur leurs ordinateurs et équipements mobiles demeurent importants et augmentent par rapport aux années précédentes.

Par rapport aux années précédentes, estimez-vous que les dangers et les risques auxquels votre ordinateur, vos smartphone ou tablettes, sont exposés sont…

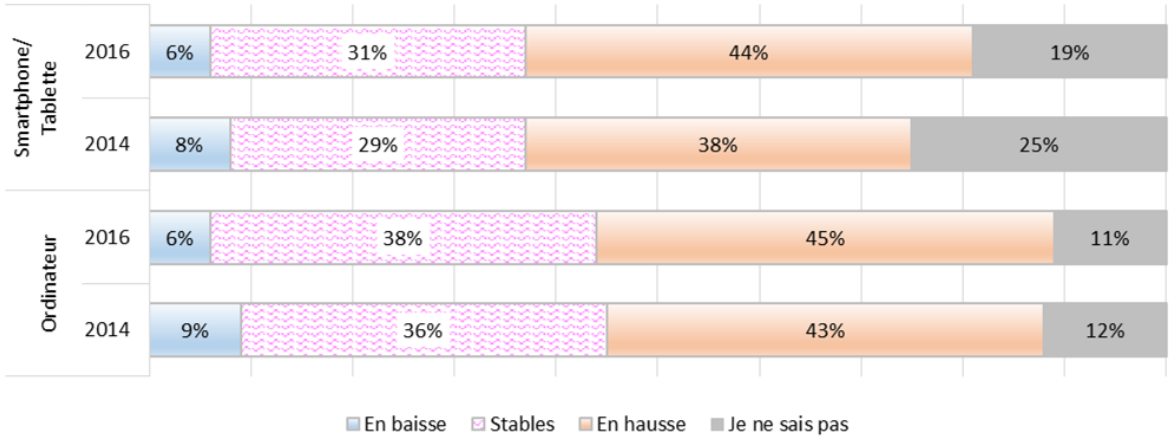


Figure 133 - Évolution de la perception du risque sur les équipements connectés

Si la perception de la tendance selon l'âge de personnes interrogées est relativement homogène pour les équipements mobiles, on note de fortes différences pour les utilisateurs d'ordinateurs : plus de la moitié des plus de 60 ans considèrent que le risque augmente, tandis que la moitié des moins de 30 ans pensent que le risque est stable ou en baisse.

Une perception des menaces en léger recul

L'enquête de cette année introduit une nouvelle façon de présenter la perception des menaces, qui permet une vue plus synthétique et un classement de menaces par ordre d'importance.

Un score moyen a été calculé en pondérant les réponses de la façon suivante : risque nul (1), peu important (2), important (4), très important (7), sans tenir compte des réponses « Je ne sais pas ».

Chaque menace est ainsi notée selon la répartition des réponses, un score de 4 ou plus dénotant un risque important, tandis qu'un score inférieur à 4 indique un risque modéré.

Sur les 20 menaces proposées aux internautes, 14 sont considérées comme représentant un risque important, mais pour la plupart, cette perception est en diminution sensible par rapport à 2014.

- L'infection par un virus : elle reste la menace la plus importante, mais cette perception varie sensiblement selon l'âge. Les plus de 45 ans sont plus de 80% à la considérer élevée ou très élevée, contre 70% pour les moins de 45 ans ;
- Les escroqueries à la carte bancaire ou l'hameçonnage viennent en deuxième place, sans doute en raison de la médiatisation de ce risque. La « professionnalisation » et l'habileté des pirates peuvent laisser penser que cette menace va continuer à progresser dans la perception des internautes.

En l'absence de protection adaptée, quel risque représentent les menaces suivantes ?

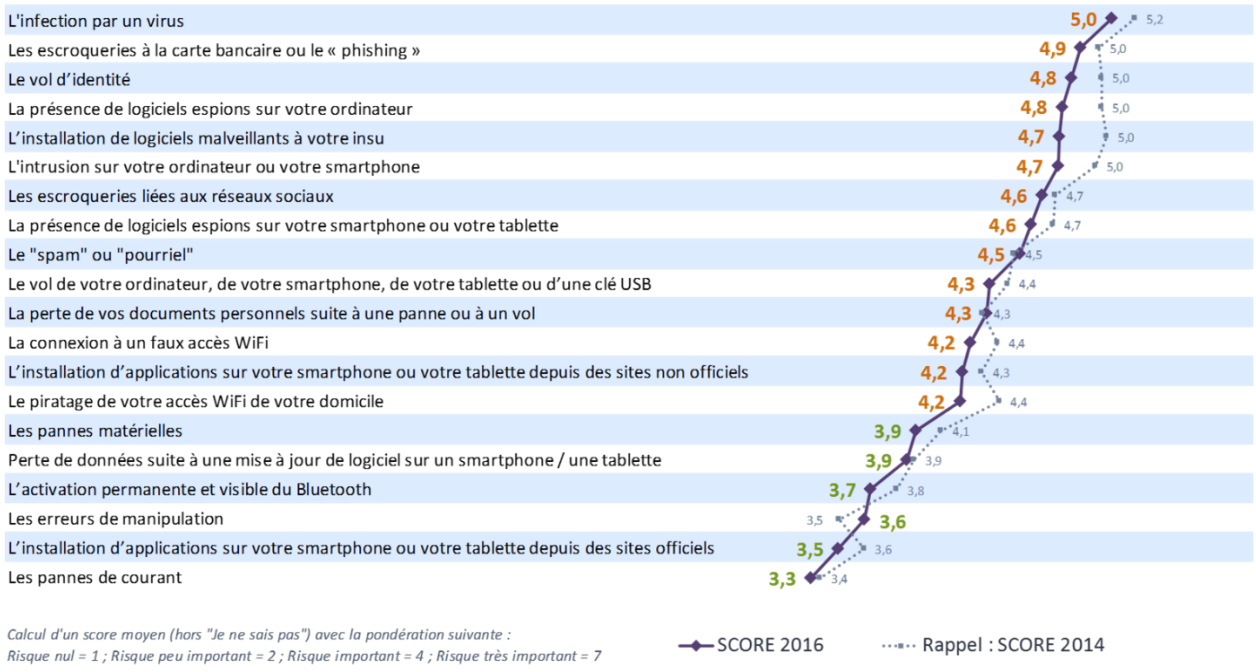


Figure 134 – Perception de la gravité de la menace en l'absence de protection adaptée

Globalement, Internet est donc perçu comme la principale source de menaces (virus, escroqueries, logiciels espions ou malveillants), contrairement aux menaces locales (piratage Wifi, vol de l'ordinateur, pannes de courant).

Paiement sécurisé à partir de quel dispositif ?

Comme en 2014, l'étude a montré que les internautes restent sur la même position en ce qui concerne la sécurité du paiement en ligne sur un ordinateur ou sur un smartphone et sur une tablette. Le paiement en ligne sur un ordinateur est perçu plus sécurisé (40%) que sur un smartphone ou une tablette (3%).

L'étude révèle également cette année que plus d'internautes (32% contre 28% en 2014) pensent que le paiement en ligne est aussi sécurisé sur un ordinateur que sur un smartphone ou tablette. Les personnes entre 15 ans et 44 ans sont davantage de cet avis que les autres tranches d'âge. Les personnes de plus de 60 ans hésitent à accorder la même confiance aux deux types de dispositifs. Probablement parce que cette tranche d'âge est beaucoup plus familière avec les ordinateurs que les smartphones et tablettes plus connus et utilisés par la nouvelle génération.

Pensez-vous que le paiement sur Internet est aussi sécurisé depuis un ordinateur et depuis un smartphone ou une tablette ?

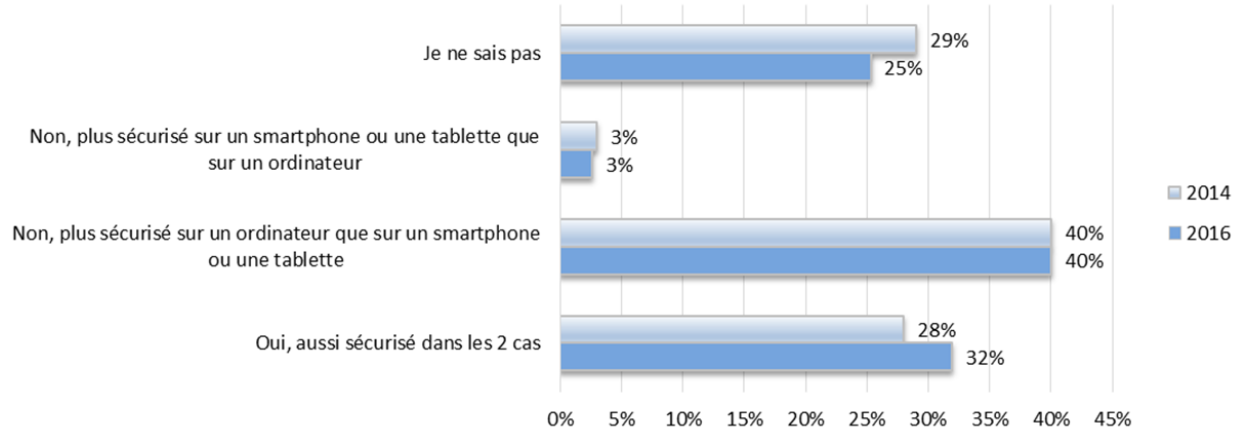


Figure 135 – Perception de la sécurité du paiement en ligne sur un ordinateur vs sur un smarphone

Cependant, la question laisse toujours de nombreux utilisateurs en difficulté puisque près de 25% ne savent pas en réalité se prononcer sur la question même si ce pourcentage est en diminution par rapport à 2014 (29%).

Les menaces actuelles d'Internet…

L'étude sur la question des éléments qui influencent positivement ou négativement le niveau de risque montre que l'antivirus tient toujours une place prépondérante sur la perception de la sécurité des internautes. Le score du niveau de risque reste sensiblement le même qu'il y a 2 ans.

Les internautes ont pleinement conscience que l'absence ou la mauvaise gestion des protections de leur ordinateur augmente considérablement la menace informatique. Ainsi, les utilisateurs de plus de 45 ans estiment que la navigation sans antivirus augmente fortement les risques même si l'estimation de ce risque est assez élevée également chez les moins jeunes. La nécessité de protéger les smartphones et tablettes est perçue comme moindre que pour un ordinateur. Il en est de même pour la sauvegarde des données qu'ils contiennent.

L'absence de certains dispositifs de sécurité tels que le pare-feu ou encore le manque de maturité des utilisateurs sur la connaissance de l'informatique augmente fortement le risque. Les internautes ont également conscience que la divulgation de leurs coordonnées est nuisible à la sécurité de l'information ainsi que l'utilisation du même mot de passe et de sa simplicité.

Quels sont les éléments influençant positivement ou négativement le risque ?

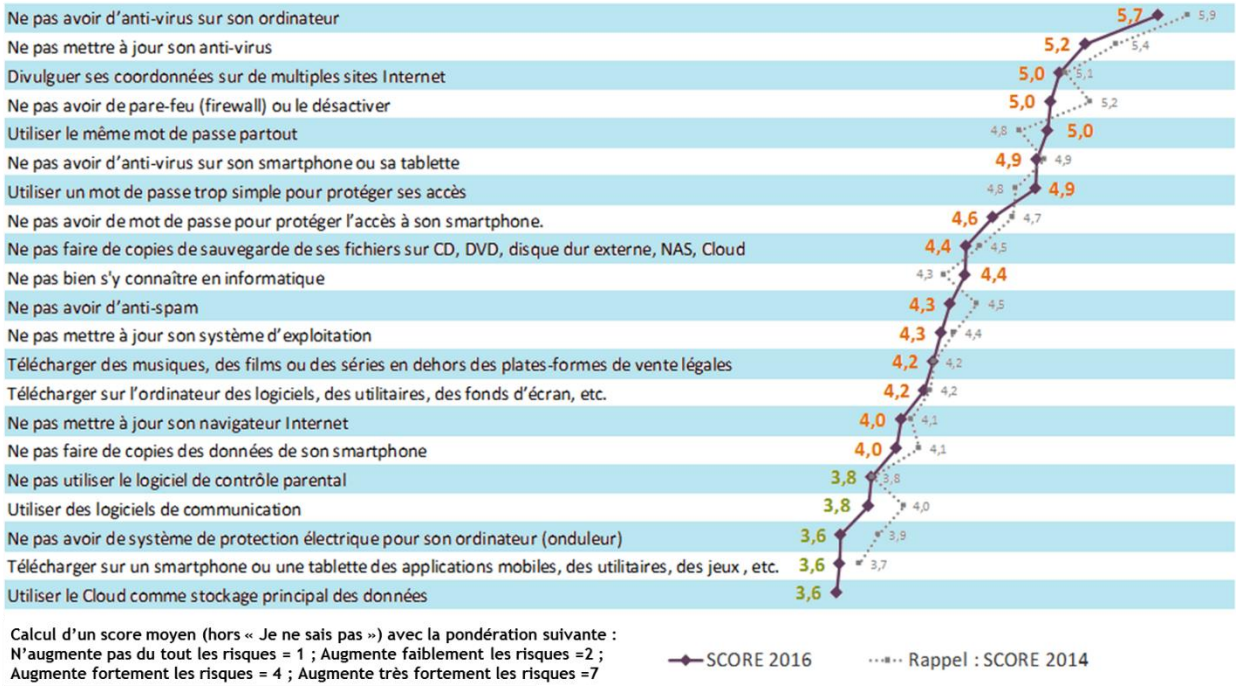


Figure 136 - Facteur d'influence du risque

Partie IV - Moyens et comportements de sécurité

Les outils de sécurité classiques sont toujours très utilisés

Les moyens classiques de protection des équipements informatiques semblent rester les plus privilégiés. Ainsi, les internautes optent pour les outils de sécurité les plus plébiscités tels que l'antivirus (88%), le pare-feu (80%), l'anti-spam (77%) et l'anti-spyware (74%).

Les internautes ont recours également à une protection de l'accès au Wifi (en lien avec la mise en place par les opérateurs Internet de "Clé Wifi" par défaut mais surtout grâce à la technique de chiffrement élaborée WPA2 et une utilisation de mot de passe complexe.

Quels moyens de protection utilisez-vous pour garantir la sécurité de votre ordinateur / de votre smarphone ou de votre tablette ?

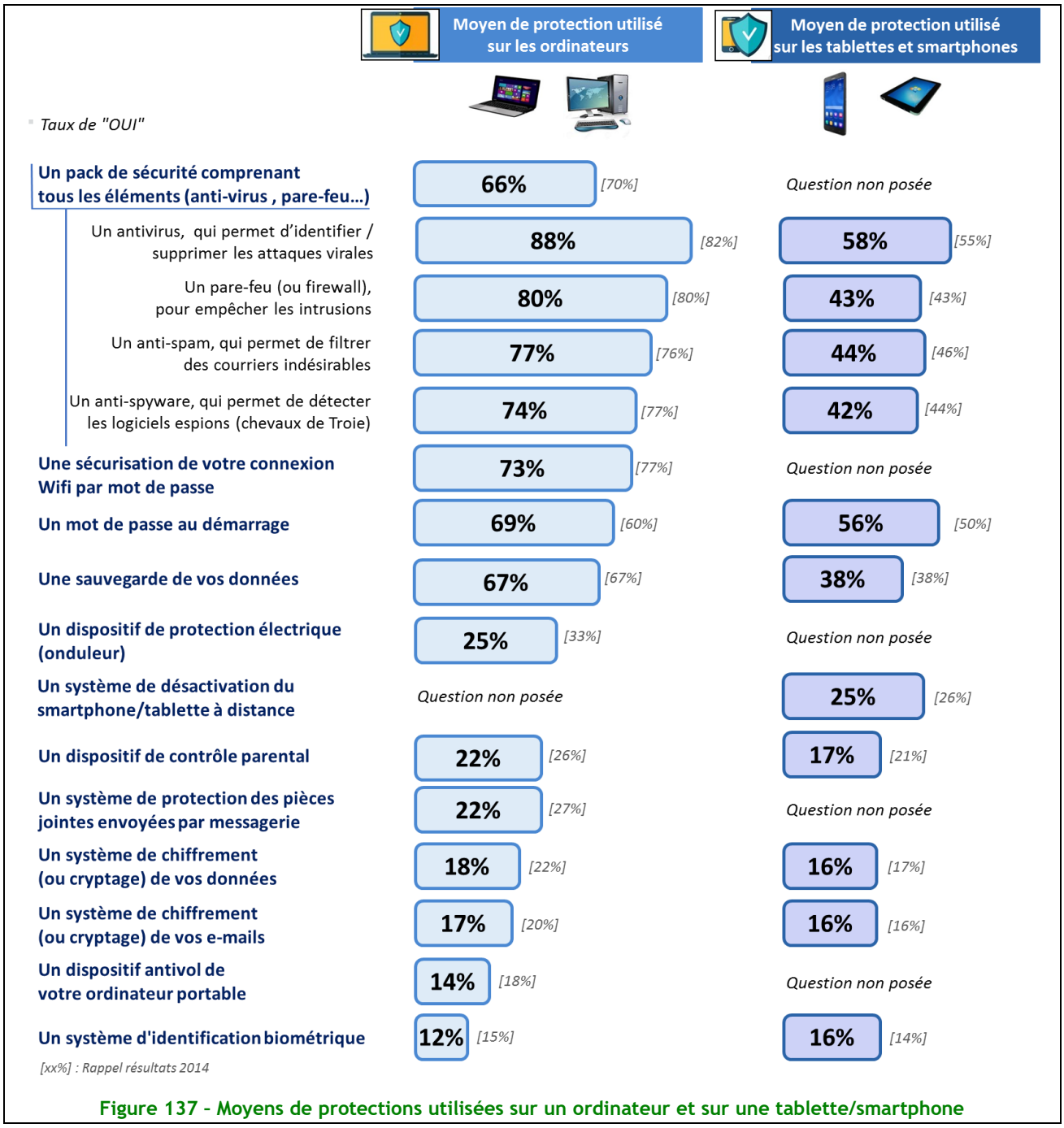


Figure 137 - Moyens de protections utilisées sur un ordinateur et sur une tablette/smartphone

Quels moyens de protection utilisez-vous pour garantir la sécurité de votre ordinateur personnel ?

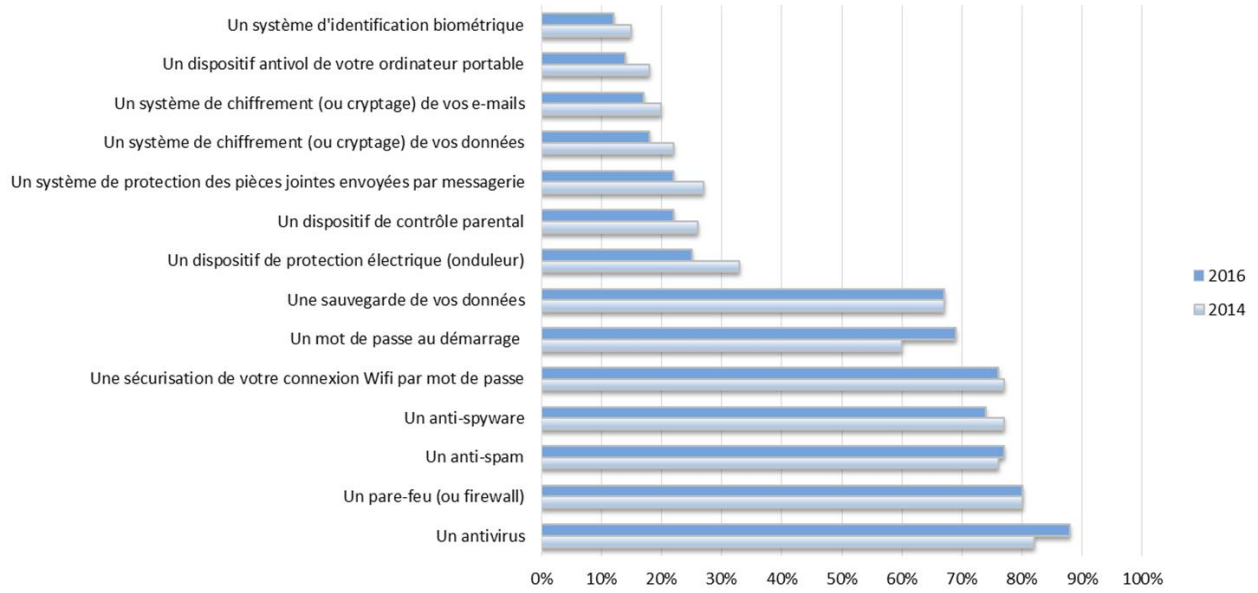


Figure 138 – Moyens de protection utilisés sur un ordinateur

Les moyens de protection utilisés sur un smartphone ou une tablette restent relativement faibles par rapport à l'ordinateur. Nous notons néanmoins que les recours utilisés sont les mêmes et l'usage de l'antivirus est au-dessus.

Des internautes globalement prudents, mais peu à l'aise avec les outils avancés de sécurité

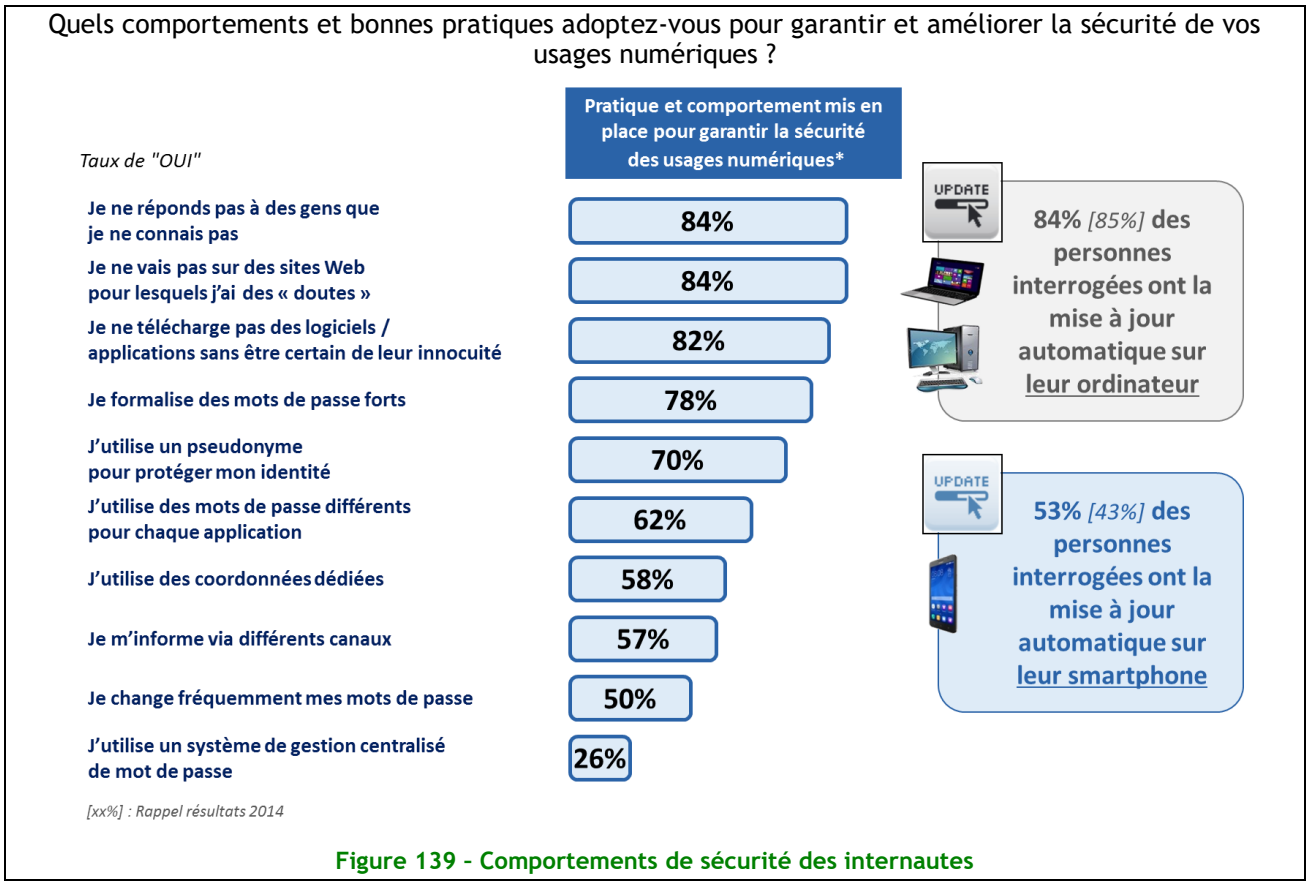


Figure 139 – Comportements de sécurité des internautes

Nous avons cherché cette année à affiner les comportements des internautes face aux enjeux de sécurité. Ainsi, au-delà des pratiques de mise à jour des systèmes qui sont maintenant bien intégrées (avec un progrès sur le téléphone mobile, certainement facilité par une simplification des interfaces des différents systèmes d'exploitation mobiles), les internautes sont globalement très attentifs – à plus de 70% - sur l'ensemble des postures de questionnement face aux risques potentiels (ne pas poursuivre lorsqu'il y a un risque face à un contenu d'origine inconnue).

Ils sont par ailleurs assez dynamiques dans la démarche d'information (57% se tiennent informés via différents canaux), mais en revanche encore peu à l'aise avec les outils de sécurité plus complexes tels que des systèmes de stockage sécurisé des mots de passe (26%), certainement parce que peu connus et parfois encore complexes à utiliser. Toutefois, la sécurité du mot de passe est une préoccupation forte, puisque 78% utilise des mots de passe forts et 62% des mots de passe différents pour chaque application.

Lorsqu'on analyse les réponses par sexe ou catégorie socio-professionnelle des internautes, on n'observe pas de grosses différences entre les groupes. En revanche, l'analyse des tranches d'âge permet d'observer des tendances intéressantes :

- S'agissant des mises à jour automatiques elles sont plus systématiques pour les ordinateurs des personnes les plus âgées (au-delà de 60 ans), et pour les smartphones des plus jeunes (en dessous de 30 ans),
- Pour ce qui est des précautions de base (confiance dans les sites douteux, utilisation de mots de passe forts…) ce sont les tranches d'âge les plus élevées (au-dessus de 50 ans) qui sont plus attentives,
- En revanche, s'agissant de la maîtrise de l'identité (utilisation de pseudonymes, courriels différents sur différents services), les classes d'âge plus jeunes sont beaucoup plus attentives,
- De même, des outils plus complexes comme ceux permettant la gestion centralisée de mots de passe sont mieux utilisés par les classes d'âge plus jeunes (en dessous de 60 ans).

L'ESPRIT DE L'ÉCHANGE

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

11, rue de Mogador
75009 Paris
✆ 01 53 25 08 80
clusif@clusif.fr

Téléchargez les productions du CLUSIF sur

www.clusif.fr