Insee Première

N° 1796

Avril 2020

Un tiers des grandes sociétés a vécu un incident de sécurité informatique en 2018

Indisponibilité des services informatiques, destruction ou altération de données, divulgation de données confidentielles : 16 % des sociétés de 10 personnes ou plus implantées en France déclarent avoir vécu un incident de sécurité informatique en 2018. Les sociétés de 250 personnes ou plus sont deux fois plus touchées. Quatre sociétés sur dix sont assurées contre ces incidents.

En 2019, presque toutes les sociétés de 10 personnes ou plus agissent pour leur sécurité informatique. Pour ce faire, deux tiers ont recours à des prestataires et plus de la moitié informe son personnel de ses obligations en la matière.

26 % des sociétés ont une documentation sur les mesures, pratiques ou procédures en matière de sécurité des systèmes d'information, autant qu'en 2015. C'est le cas de 71 % des sociétés de 250 personnes ou plus. Quelle que soit leur taille, sept sociétés sur dix ont défini ou révisé cette documentation au cours de l'année écoulée.

De plus, 86 % des sociétés mettent à jour régulièrement leurs logiciels et systèmes d'exploitation. C'est la mesure de sécurité la plus répandue. Les grandes sociétés sont beaucoup plus nombreuses à mettre en œuvre simultanément plusieurs mesures de sécurité informatique.

Enfin, la moitié des sociétés a une politique d'accès, de rectification et d'effacement des données personnelles : c'est deux fois plus qu'en 2015.

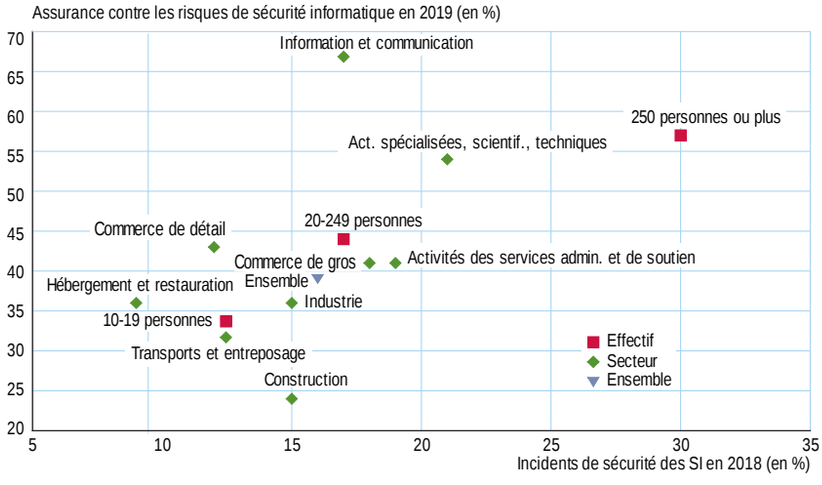
Nadège Pradines (division Enquêtes thématiques et études transversales, Insee)

16 % des sociétés de 10 personnes ou plus déclarent avoir vécu en 2018 un des incidents de sécurité informatique suivants : indisponibilité des services informatiques, destruction ou altération de données, divulgation de données confidentielles. C'est à peine plus qu'en 2014. C'est le cas de 13 % des **petites sociétés** (10-19 personnes) et de 30 % des **grandes sociétés** (250 personnes ou plus). Cette part va de 9 % dans l'hébergement-restauration à 21 % dans les activités spécialisées, scientifiques et techniques *(figure 1)*. Un incident, une défaillance ou une attaque peuvent avoir de lourdes conséquences, pour la société ou pour ses clients.

Quatre sociétés sur dix sont assurées contre ces incidents

Quatre sociétés de 10 personnes ou plus sur dix sont assurées contre les in-

1 Incidents de sécurité informatique et assurance contre ce risque



Lecture : en 2019, 67 % des sociétés de l'information et communication sont assurées contre les risques de sécurité informatique et 17 % déclarent avoir subi des incidents de sécurité informatique au cours de l'année précédente.
Champ : sociétés de 10 personnes ou plus, implantées en France, des secteurs principalement marchands hors secteurs agricole, financier et d'assurance.
Source : Insee, enquête TIC entreprises 2019.

Insee

cidents de sécurité informatique : une sur trois pour les petites sociétés, six sur dix pour les grandes. Dans l'ensemble, plus les sociétés sont exposées à ces incidents, plus elles sont dotées d'assurances contre ces risques. Il y a cependant quelques exceptions : les sociétés de l'information et de la communication sont fortement assurées et sont, en proportion, moins atteintes par des incidents. Elles sont davantage conscientes des risques et elles les prennent mieux en charge. À l'inverse, les sociétés de la construction sont les moins assurées contre ces risques alors qu'elles sont de plus en plus victimes d'incidents de sécurité informatique au cours des dix dernières années.
Les sociétés assurées déclarent un peu plus souvent avoir connu des incidents de sécurité informatique.

Principale conséquence : l'indisponibilité des services informatiques

En 2018, 12 % des sociétés de 10 personnes ou plus ont vécu une indisponibilité de leurs services informatiques due, par exemple, à une attaque extérieure par **déni de service** ou **rançongiciel** ou à une panne de logiciel ou de matériel informatique (à l'exclusion des pannes mécaniques et du vol). Les incidents aboutissant à la destruction ou à l'altération de données concernent moitié moins de sociétés (6 %). Ils peuvent être dus à l'attaque d'un programme malveillant (virus), à un accès non autorisé ou à une panne de logiciel ou de matériel informatique. Enfin, les incidents aboutissant à la divulgation de données confidentielles sont marginaux (2 %), mais leurs conséquences peuvent être très coûteuses pour les entreprises. Cette divulgation peut être engendrée par une intrusion, un dévoiement (*pharming*), une attaque par hameçonnage (*phishing*) ou des actions des propres employés de la société.
Ces résultats reflètent la déclaration des sociétés, parfois réticentes à communiquer sur ces événements, et excluent les incidents que la société ne connaît pas ou ne reconnaît pas comme étant des incidents de sécurité informatique. Ainsi, la plus grande part de grandes sociétés ou de sociétés des activités spécialisées, scientifiques et techniques concernées par un incident peut signifier qu'elles sont plus aptes à les repérer.

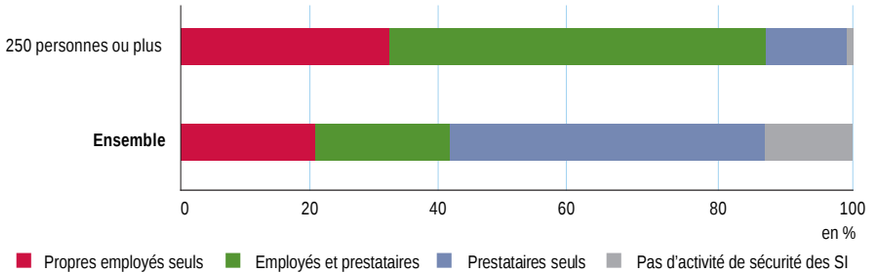
Neuf sociétés sur dix agissent pour leur sécurité informatique

En 2019, 87 % de sociétés de 10 personnes ou plus réalisent des activités en lien avec la sécurité de leur système d'information (SI) : tests de sécurité, formations à la sécurité des technologies de l'information et de la communication (TIC), résolution des incidents, etc. La sécurité des SI recouvre les mesures, les contrôles et les procédures appliquées aux SI afin de garantir l'intégrité, l'authenticité, la disponibilité et la confidentialité des données et des systèmes.
À l'inverse, 13 % des sociétés de 10 personnes ou plus ne réalisent pas d'activités en lien avec la sécurité de leur SI. Il s'agit essentiellement de petites sociétés : 20 % d'entre elles ne réalisent pas d'activités en lien avec la sécurité de leur SI contre 1 % parmi les grandes sociétés. Il s'agit aussi de sociétés dont le cœur de métier n'est pas numérique (24 % des sociétés de l'hébergement-restauration, 18 % des sociétés de la construction).
Par ailleurs, 67 % des sociétés ont recours à des prestataires pour réaliser des activités de sécurité informatique, parfois en plus des employés de l'entreprise, et 20 % les font réaliser uniquement par leurs propres employés *(figure 2)*. La présence au sein de l'entreprise d'employés conduisant certaines activités de sécurité informatique est très fréquente dans les grandes sociétés et dans le secteur de l'information et de la communication. Ce sont aussi ces deux catégories de sociétés qui réalisent le plus des activités en lien avec la sécurité de leur SI.
Dans plus de la moitié des sociétés, le personnel est informé de ses obligations en matière de sécurité des SI. Pour 35 % des sociétés, cette information se fait notamment *via* le contrat de l'employé. Elle peut faire aussi l'objet de formations volontaires (36 %) ou obligatoires (19 %).

La première mesure de sécurité est la mise à jour régulière des logiciels

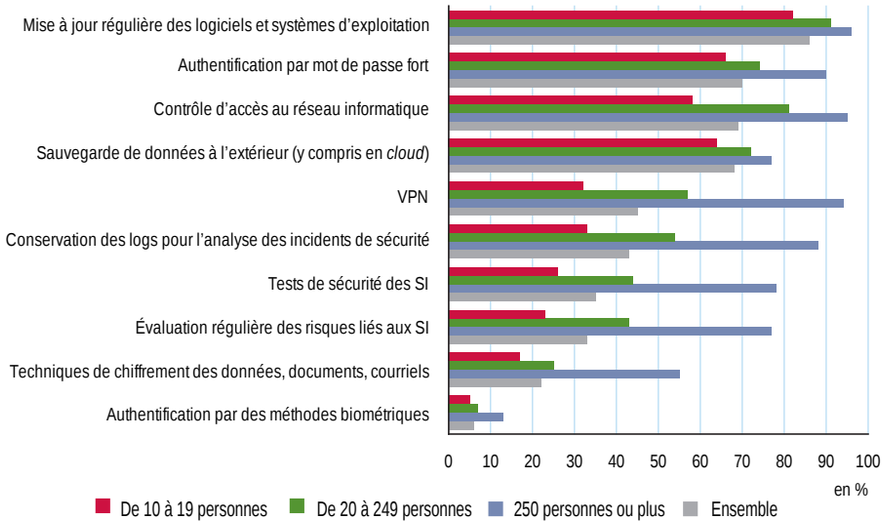
En 2019, 86 % des sociétés de 10 personnes ou plus mettent à jour régulièrement leurs logiciels et systèmes d'exploitation. C'est la mesure de sécurité la plus répandue *(figure 3)*. La mise à jour des logiciels permet notamment d'installer les derniers correctifs de sécurité émis par les éditeurs. Suivent l'authentification par mot de passe fort (70 %), le contrôle d'accès au réseau

2 Personnel réalisant les activités de sécurité des systèmes d'information en 2019



Lecture : en 2019, 20 % des sociétés de 10 personnes ou plus font réaliser les activités de sécurité des systèmes d'information par leurs seuls employés, contre 31 % des grandes sociétés.
Champ : sociétés de 10 personnes ou plus, implantées en France, des secteurs principalement marchands hors secteurs agricole, financier et d'assurance.
Source : Insee, enquête TIC entreprises 2019.

3 Mesures de sécurité des systèmes d'information (SI) en 2019



Lecture : 86 % des sociétés de 10 personnes ou plus mettent régulièrement à jour leurs logiciels et leurs systèmes d'exploitation.
Champ : sociétés de 10 personnes ou plus, implantées en France, des secteurs principalement marchands hors secteurs agricole, financier et d'assurance.
Source : Insee, enquête TIC entreprises 2019.

informatique (69 %) et la sauvegarde de données à l'extérieur, c'est-à-dire dans un bâtiment différent ou sur un serveur distant (68 %). Ces mesures, les plus courantes, sont utilisées dans une majorité de sociétés, quelle que soit leur taille, mais pas toujours simultanément.

D'autres mesures de sécurité, demandant une expertise plus forte, sont davantage utilisées dans les grandes sociétés : 94 % des sociétés de 250 personnes ou plus utilisent un **VPN** pour sécuriser leurs échanges de données, contre 45 % de l'ensemble des sociétés de 10 personnes ou plus. De même, 88 % des grandes sociétés conservent les *logs* (fichiers journaux) pour analyser les incidents de sécurité, soit deux fois plus que dans l'ensemble des sociétés.

Les grandes sociétés évaluent les risques et testent la sécurité de leur SI

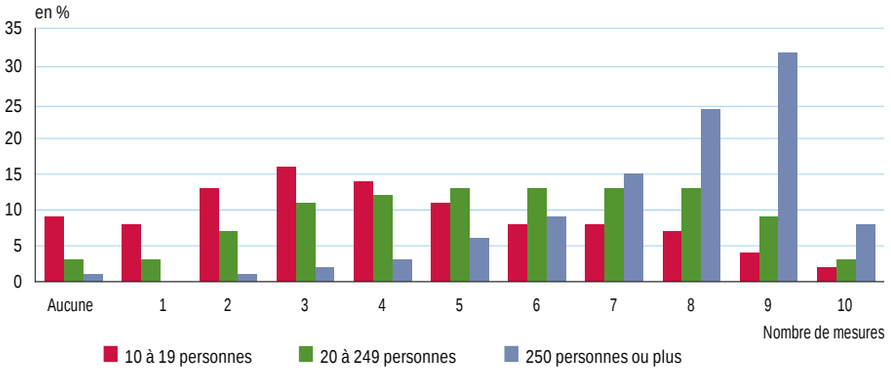
Parmi les sociétés de 250 personnes ou plus, trois quarts évaluent les risques liés aux SI, c'est-à-dire la probabilité et les conséquences des incidents de sécurité informatique. De même, trois quarts d'entre elles mènent des tests de sécurité : tests d'intrusion, tests du système d'alerte de sécurité ou des systèmes de sauvegarde, etc. À l'opposé, seul un quart des sociétés de 10 à 19 personnes mène de telles opérations. De plus, une grande société sur deux utilise des techniques de chiffrement des données, documents ou courriels, contre une petite société sur six. L'authentification par des mesures biométriques (empreintes digitales, reconnaissance faciale, vocale) est peu adoptée (6 % de l'ensemble des sociétés), avec de légères différences selon la taille.

De manière générale, les grandes sociétés sont beaucoup plus nombreuses à cumuler les mesures de sécurité informatique : 40 % d'entre elles cumulent au moins neuf mesures (sur les dix proposées dans l'enquête), contre seulement 6 % des petites sociétés *(figure 4)*. À l'opposé, 60 % des petites sociétés ont recours à moins de cinq mesures de sécurité différentes, contre seulement 7 % des grandes sociétés.

Un quart des sociétés documente ses procédures de sécurité informatique

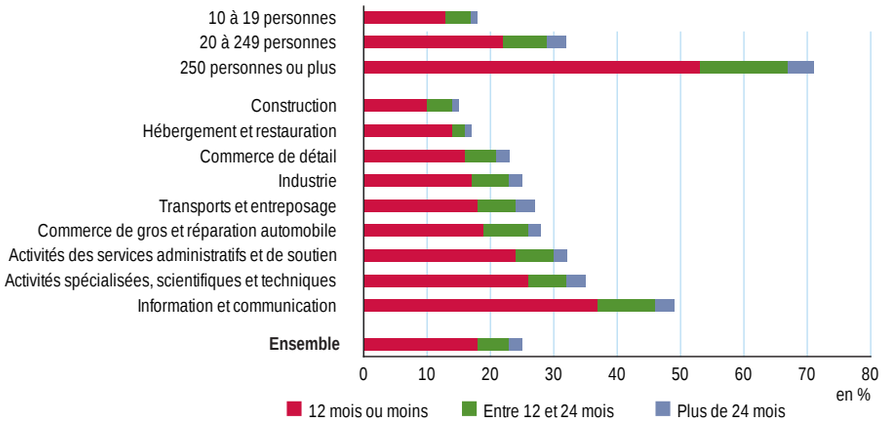
En 2019, comme en 2015, 26 % des sociétés de 10 personnes ou plus disposent d'une documentation sur les mesures, pratiques ou procédures en matière de sécurité des SI. C'est deux fois moins qu'au Danemark, en Irlande ou en Suède et en dessous de la moyenne de l'Union européenne à 28 (34 %). La France est au 23e rang, la Grèce détenant le niveau le moins élevé avec seulement 15 % des sociétés dotées d'une documentation de sécurité des SI.

4 Nombre de mesures de sécurité informatique selon la taille des sociétés en 2019



Note : 10 mesures de sécurité sont mentionnées dans le questionnaire de l'enquête. On ne présume pas de la qualité ou de l'étendue du recours à ces mesures.
Lecture : 9 % des sociétés de 10 à 19 personnes n'ont recours à aucune des mesures de sécurité informatique citées dans l'enquête TIC.
Champ : sociétés de 10 personnes ou plus, implantées en France, des secteurs principalement marchands hors secteurs agricole, financier et d'assurance.
Source : Insee, enquête TIC entreprises 2019.

5 Sociétés ayant une documentation en matière de sécurité des systèmes d'information (SI), selon la date de dernière mise à jour



Lecture : en 2019, 26 % des sociétés de 10 personnes ou plus ont une documentation en matière de sécurité des SI ; 18 % en ont une définie ou révisée au cours des 12 derniers mois.
Champ : sociétés de 10 personnes ou plus, implantées en France, des secteurs principalement marchands hors secteurs agricole, financier et d'assurance.
Source : Insee, enquête TIC entreprises 2019.

6 Part de sociétés ayant une politique d'accès, de rectification et d'effacement des données personnelles

en %

	2015	2019
De 10 à 19 personnes	20	42
De 20 à 249 personnes	32	59
250 personnes ou plus	62	86
Industrie	25	45
Construction	15	35
Commerce de gros	31	55
Commerce de détail	26	54
Transports et entreposage	24	44
Hébergement et restauration	21	45
Information et communication ; réparation d'ordinateur	48	78
Activités spécialisées, scientifiques et techniques	36	66
Activités des services administratifs et de soutien ; activités immobilières	30	56
Ayant vendu sur le *web* l'an précédent	38	69
Utilisant les médias sociaux	38	62
Utilisant une application de gestion de la relation client (CRM)	40	72
Ensemble	**26**	**51**

Lecture : en 2015, 20 % des sociétés de 10 à 19 personnes avaient une politique d'accès, de rectification et d'effacement des données personnelles.
Champ : sociétés de 10 personnes ou plus, implantées en France, des secteurs principalement marchands hors secteurs agricole, financier et d'assurance
Source : Insee, enquêtes TIC entreprises 2015 et 2019

Les grandes sociétés sont nettement plus concernées que les petites : c'est le cas de 71 % des sociétés de 250 personnes ou plus, contre 32 % des sociétés de 20 à 249 personnes et 18 % des sociétés de 10 à 19 personnes *(figure 5)*.

Par rapport à 2015, les sociétés qui ont une documentation sur la sécurité des SI en 2019 l'ont définie ou actualisée plus récemment : quelle que soit leur taille, sept sociétés sur dix l'ont fait pour la dernière fois au cours de l'année écoulée, contre cinq sur dix pour les sociétés dotées d'une telle documentation en 2015. À l'opposé, moins d'une société sur dix dotées d'une telle documentation en 2019 ne l'a pas mise à jour depuis plus de deux ans, contre un quart de celles qui avaient une telle documentation en 2015.

Comme en 2015, la moitié des sociétés de l'information et de la communication sont dotées d'une telle documentation, contre moins d'un cinquième dans la construction ou l'hébergement-restauration.

Politique d'accès aux données personnelles : deux fois plus qu'en 2015

En 2019, 51 % des sociétés de 10 personnes ou plus ont une politique d'accès, de rectification et d'effacement des données personnelles, contre 26 % en 2015. La mise en conformité des sociétés avec le règlement général sur la protection des données (RGPD), entré en vigueur en 2018, peut être une explication. Ainsi, 86 % des sociétés de 250 personnes ou plus ont une telle politique, contre 59 % des sociétés de 20 à 249 personnes et 42 % de celles de 10 à 19 personnes. Les secteurs les plus numérisés sont aussi ceux qui adoptent le plus souvent une telle politique *(figure 6)*.

Certains usages numériques impliquent le traitement de données personnelles permettant d'identifier une personne physique, directement ou indirectement. C'est le cas de la vente *web*, de l'utilisation des médias sociaux ou de la gestion des relations avec la clientèle. Quels que soient leur taille ou leur secteur, les sociétés concernées par l'un ou l'autre de ces usages déclarent plus souvent que les autres avoir une politique d'accès, de rectification ou d'effacement des données personnelles. ■

Sources

L'**enquête sur les technologies de l'information et de la communication et le commerce électronique** (TIC) de 2019 a été réalisée début 2019 auprès d'un échantillon de 12 500 sociétés implantées en France Cette étude s'appuie sur la définition juridique de l'entreprise (unité légale), et non sur la définition économique instaurée par la loi de modernisation de l'économie (LME) et son décret d'application n° 2008-1354 du 18 décembre 2008.

Les enquêtes TIC 2015 et TIC 2010 sont mobilisées pour des comparaisons temporelles. L'enquête 2010 porte sur un champ légèrement différent (sociétés de 10 salariés ou plus).

L'enquête porte sur les secteurs d'activité suivants : industrie, construction, commerce et réparation d'automobiles et de motocycles, transports et entreposage, hébergement et restauration, information et communication, activités immobilières, activités spécialisées, scientifiques et techniques, activités de services administratifs et de soutien (sections C à J, L, M hors 75, N et groupe 95.1 de la NAF rév. 2). L'échantillon est représentatif d'environ 181 000 sociétés.

Parmi les sociétés de l'échantillon, 73,4 % ont répondu à l'enquête. En matière de précision, l'intervalle de confiance à 95 % des résultats sur l'ensemble est de plus ou moins 1 point de pourcentage.

L'enquête vise à mieux connaître l'informatisation et la diffusion des TIC dans les entreprises. Les questions concernent la situation au moment de l'enquête, c'est-à-dire au cours du premier trimestre 2019 pour l'enquête TIC 2019. Des enquêtes analogues ont été menées dans tous les pays européens en application du règlement communautaire n° 1006/2009 sur la société de l'information. Leurs résultats et les rapports qualité sont disponibles sur le site d'Eurostat.

Définitions

Les **sociétés** sont ici des unités légales actives, sociétés ou entreprises individuelles, de 10 personnes ou plus (salariés ou non-salariés). Les **petites sociétés** occupent de 10 à 19 personnes. Les **grandes sociétés** occupent 250 personnes ou plus.

Le ***pharming*** (ou dévoiement) est une technique de piratage informatique. Elle consiste à dérouter la circulation d'un site *web* vers un faux site *web*, afin d'acquérir des informations.

Le ***phishing*** (hameçonnage ou filoutage) est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels concernant des internautes (noms d'utilisateur, mots de passe, informations sur une carte de crédit, etc.) dans le but de perpétrer une usurpation d'identité. Elle consiste à mettre l'internaute en confiance en se faisant passer pour un site ou un expéditeur connu (adresse, logo…). L'hameçonnage peut se faire par courrier électronique, par des sites *web* falsifiés ou d'autres moyens électroniques.

Une attaque par **déni de service** (*denial of service attack*, ou DoS) a pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser. Il s'agit la plupart du temps d'attaques à l'encontre des serveurs d'une entreprise.

Un **rançongiciel** (*ransomware*), ou logiciel de rançon, prend en otage des données personnelles en les chiffrant. Le logiciel propose ensuite de fournir la clef de chiffrement contre le paiement d'une rançon.

Un ***VPN*** (*virtual private network*, réseau privé virtuel) étend un réseau privé à travers un réseau public pour permettre un échange de données sécurisé.

Pour en savoir plus

- « Les technologies de l'information et de la communication et le commerce électronique 2019 », *Insee Résultats*, avril 2020.
- « ICT security in enterprises », *Statistics explained*, Eurostat, avril 2020.
- Pradines N., «*Cloud computing et big data* : la dématérialisation au service des sociétés européennes», in *L'économie et la société à l'ère du numérique*, coll. «Insee Références», édition 2019.
- Demoly E., Vacher T., « Sécurité numérique et médias sociaux dans les entreprises en 2015 », *Insee Première* n° 1594, mai 2016.

Direction Générale :
88 avenue Verdier
92541 Montrouge Cedex
Directeur de la publication :
Jean-Luc Tavernier
Rédacteur en chef :
A. Goin
Rédacteurs :
P. Glénat
C. Lesdos-Cauhapé
Maquette : B. Rols
Code Sage : IP201796
ISSN 0997 – 3192 (papier)
ISSN 0997 – 6252 (web)

- *Insee Première* figure dès sa parution sur le site internet de l'Insee : https://www.insee.fr/fr/statistiques?collection=116
- Pour recevoir par courriel les avis de parution (60 numéros par an) : https://www.insee.fr/fr/information/1405555

Insee
Mesurer pour comprendre