BOMGAR™

RAPPORT 2018 SUR LES MENACES LIÉES AUX ACCÈS PRIVILÉGIÉS

Ou l'urgence à protéger les identités et les accès privilégiés

I: PAYSAGE DES MENACES EN 2018

INTRODUCTION

L'attaque ransomware WannaCry de mai 2017 a mis à mal le NHS, le service de santé britannique, et a perturbé un grand nombre d'organisations dans plus de 150 pays. WannaCry n'était pourtant pas une attaque très sophistiquée : elle fut initiée à partir de failles prévisibles qui auraient pu être évitées si elles avaient été correctement prises en compte et traitées. Il y a eu bien d'autres attaques en 2017 à l'instar d'Uber et Equifax, dont les impacts et les conséquences auraient pu être bien plus limitées si les recommandations et les bonnes pratiques de cybersécurité avaient été respectées.

Les cyberattaques sont de plus en plus étendues et complexes, des escroqueries sous forme de phishing aux attaques crypto-monnaie, en passant par les attaques soutenues par les Etats et visant les systèmes de contrôle industriels.

Ces attaques représentent un défi croissant et rappellent aux organisations qu'elles ne doivent rien laisser au hasard face aux cybermenaces. Nous vivons dans une ère où la question n'est plus de savoir si nous allons subir des cyberattaques, mais quand. Les professionnels de la sécurité doivent tout faire pour mettre en place les moyens permettant de limiter les risques et de contenir l'ampleur des dégâts.

C'est ce que confirme l'édition 2018 de notre étude, puisque **50%** des sondés (contre 42% l'an dernier) confirment avoir déjà été victimes d'une compromission grave ou s'attendent à l'être dans les six prochains mois.

L'utilisation abusive ou les mauvaises pratiques liées aux identifiants privilégiés des salariés (**62%**) ou de tierces parties (**66%**) étant à l'origine d'un grand nombre de ces compromissions, il apparaît clairement que même si les entreprises comprennent les risques associés, elles ont des progrès à faire concernant la gestion de leurs identifiants privilégiés et la protection de leurs actifs et systèmes critiques.

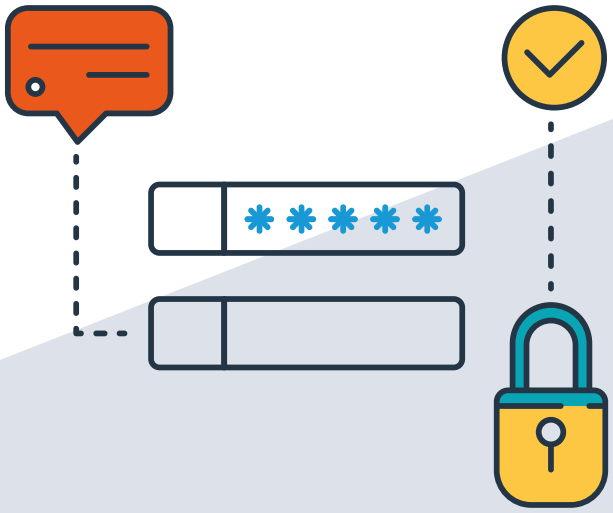
Les administrateurs IT et les fournisseurs tiers ont besoin d'un accès privilégié pour faire leur travail efficacement, mais le nombre de ces utilisateurs et des comptes privilégiés croît de façon exponentielle. L'accès aux systèmes et aux données est souvent autorisé sans réel contrôle.

Face à la recrudescence des menaces et à la mise en place de règlementations plus strictes telles que le RGPD de l'UE, jamais le besoin n'a été aussi impérieux de mettre en œuvre une stratégie de gestion et de contrôle des accès privilégiés au sein des organisations.

C'est bien cela qui déterminera le paysage des menaces en 2018 et ce à quoi les entreprises doivent s'atteler.

62% des sondés pensent qu'il est possible ou avéré qu'ils aient été victimes d'une compromission initiée par un *insider*

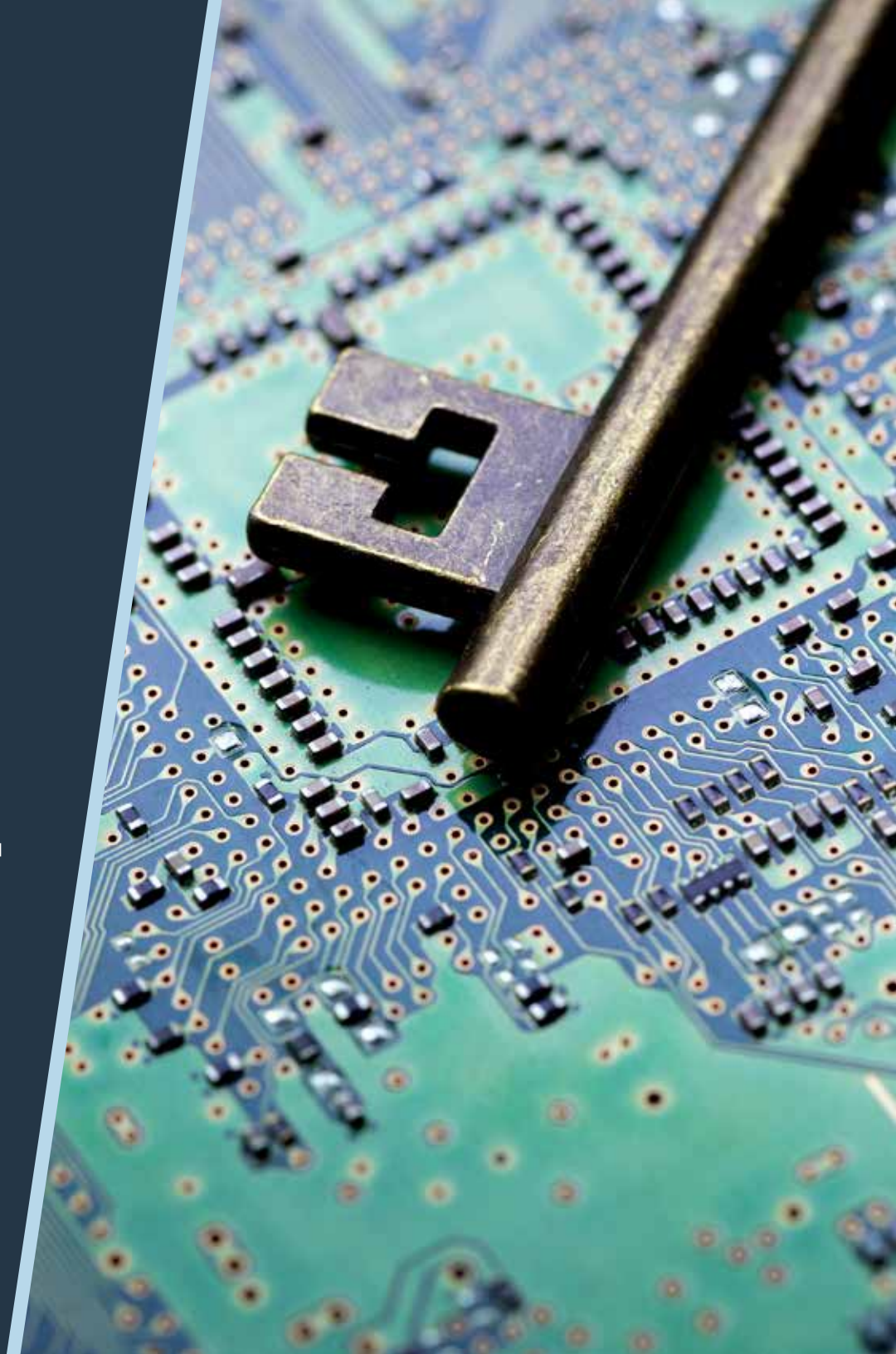
66% des sondés pensent qu'il est possible ou avéré qu'ils aient été victimes d'une compromission initiée par l'accès d'une tierce partie



MÉTHODOLOGIE DE RECHERCHE

1021 sondés, en charge des technologies d'accès des employés et prestataires aux systèmes informatiques, ont répondu à l'enquête en février 2018. Les sondés sont des professionnels IT au sein des équipes opérations, support/assistance IT, sécurité IT, conformité, gestion des risques, réseau etc. de leur entreprise. Différents secteurs d'activité sont représentés dont l'industrie, la finance, les services professionnels, la distribution, la santé, les télécoms et le secteur public. L'étude a été réalisée au Royaume-Uni, aux Etats-Unis, en Allemagne et en France.

II: UNE QUESTION DE CONFIANCE



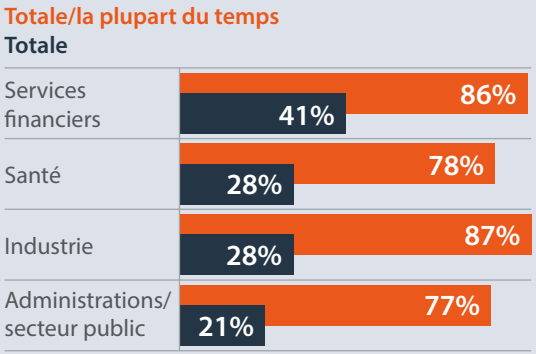
UNE QUESTION DE CONFIANCE

Les entreprises ont beau savoir que les cyberattaques sont de plus en plus probables - et que les accès privilégiés des salariés et des fournisseurs sont de plus en plus nombreux -, elles négligent souvent certains pans entiers de leur sécurité informatique et se contentent de « faire confiance ». Sans les moyens ou les ressources pour surveiller et gérer les accès privilégiés aux systèmes IT, ne reste qu'une culture fondée sur la confiance, même si elle est inefficace à détecter et éviter les compromissions de sécurité.

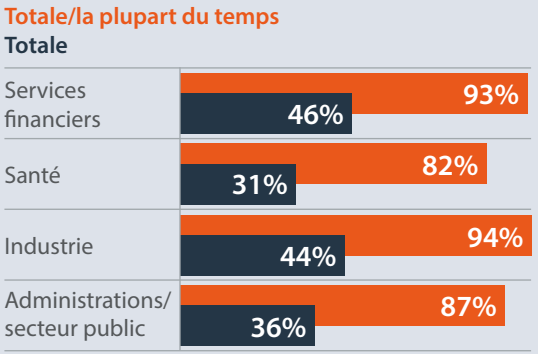
Le secteur le plus représentatif est celui des services financiers où **46%** des entreprises déclarent faire entièrement confiance aux salariés et **41%** faire entièrement confiance aux fournisseurs tiers. C'est plus que dans n'importe quel autre secteur (graph. n°1), alors même que les services financiers sont ceux qui ont eu le plus de risques de subir une compromission initiée par des *insiders* ou des tiers au cours de l'année précédente (graph. n°2). C'est aussi le secteur le plus préoccupé par l'intensification à venir des menaces liées aux salariés. Les entreprises du secteur financier se disent **très** ou **relativement** préoccupées par le risque que les identifiants de leurs salariés puissent être détournés à des fins malveillantes, de façon intentionnelle (**68%**) ou par le biais d'e-mails de phishing (**67%**), et ce de façon bien plus importante que dans tous les autres secteurs d'activité.

Graphique n°1

Confiance envers les fournisseurs tiers

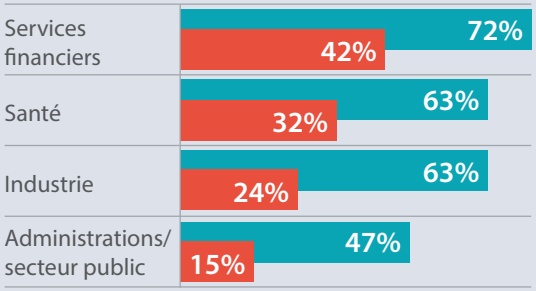


Confiance envers les *insiders*

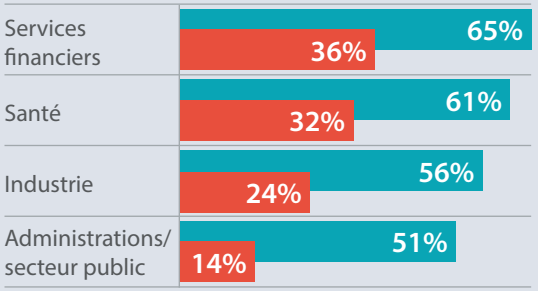


Graphique n°2

Failles initiées par l'accès de fournisseurs tiers



Failles initiées par l'accès d'*insiders*



UNE QUESTION DE CONFIANCE

Un grand nombre d'entreprises fait trop confiance aux salariés et aux tierces parties. Pourtant, la bonne foi n'est pas une stratégie de sécurité suffisamment robuste face aux nouveaux risques et menaces. Et même si les individus ne sont majoritairement pas mal intentionnés, beaucoup créent des brèches de sécurité par négligence ou pour contourner les règles de sécurité. Les entreprises doivent en prendre conscience et agir en conséquence.

Pour comprendre pourquoi la majorité des entreprises a encore du chemin à parcourir avant d'atteindre le niveau souhaité de visibilité et de contrôle sur leurs propres environnements IT, examinons de plus près la nature des risques auxquels elles s'exposent.

III: LE DÉFI DES PRIVILÈGES

LE DÉFI DES PRIVILÈGES

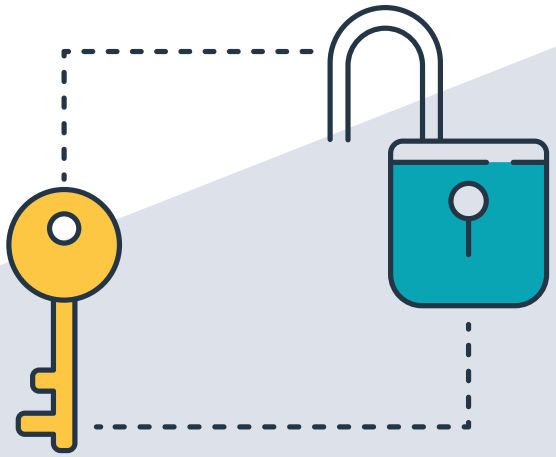
Une identité est « privilégiée » lorsqu'elle s'est vu attribuer un accès élargi à l'environnement IT d'une entreprise. De ce fait, elle a un droit d'accès admin aux systèmes IT les plus critiques de l'organisation, ainsi qu'à des données sensibles. Les utilisateurs bénéficiant d'accès privilégiés peuvent être des salariés de l'entreprise et des fournisseurs tiers, dont le nombre ne cesse de croitre. Qu'ils soient utilisés par les employés ou les prestataires, ces identifiants privilégiés sont des cibles de choix pour les fraudeurs et les cybercriminels.

Comme l'indique le graphique n°2, ce sont les entreprises du secteur financier qui sont les plus exposées au risque de compromissions via des salariés ou des tierces parties, puisque **65%** déclarent avoir été ou avoir possiblement été victimes d'une compromission initiée par un salarié au cours de l'année précédente, et **72%** à avoir été ou avoir possiblement été victimes d'une compromission liée à l'identité d'un tiers. Les chiffres pour les autres secteurs sont les suivants : santé (**61%** et **63%**), industrie (**56%** et **63%**) et secteur public (**51%** et **47%**).

Les identités des salariés et des tierces parties s'accompagnent de comportements distincts et de risques spécifiques. Il existe des solutions pour gérer et contrôler l'éventail des menaces que cela induit. Il ressort de notre étude que les entreprises choisissent l'une des trois options suivantes pour lutter contre les menaces :

- Utilisation d'une solution PIM/PAM (Privileged Identity Management et Privileged Access Management) de gestion des identités et des accès privilégiés (**46%**)
- Contrôle manuel de la création et de la gestion des identités privilégiées (**44%**)
- Aucun contrôle du tout (**10%**)

Ainsi, une entreprise sur dix n'a aucun contrôle sur les identités privilégiées et quasiment la moitié ne les contrôle que manuellement, sans système dédié. En plus d'être chronophage, cela les expose ouvertement à des cyberattaques.

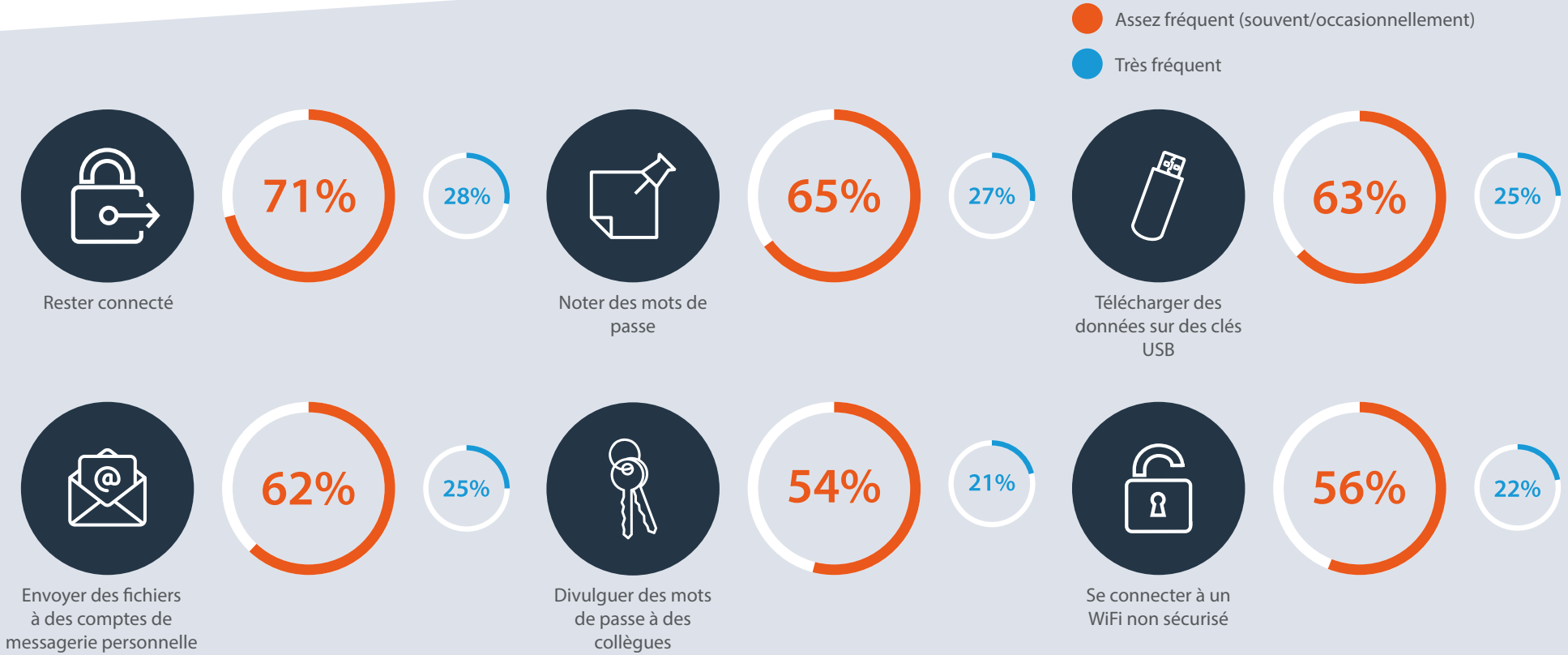


LE RISQUE DE L'*INSIDER*

Les *insiders* d'une entreprise ont besoin d'accès privilégiés aux systèmes et données sensibles pour être productifs et participer au développement de l'activité, mais accorder cette permission sans contrôle et sans traçabilité rend l'organisation vulnérable aux attaques.

D'un autre côté, quand les salariés se sentent contraints par des mesures de sécurité strictes qui les ralentissent ou entravent leurs opérations, ils cherchent souvent des raccourcis qui peuvent créer des comportements à risque, comme se connecter à des réseaux non sécurisés, télécharger des données sur des clés USB ou noter des mots de passe (graph. n°3).

Graphique n°3



LE RISQUE DE L'*INSIDER*

Ces comportements se généralisent : le nombre de sondés ayant répondu que ces pratiques se produisaient « assez fréquemment » a augmenté par rapport à l'année précédente. Le fait de noter des mots de passe est une pratique problématique citée par **55%** des entreprises en 2017 et **65%** en 2018. Divulguer des mots de passe à des collègues l'était pour **46%** des entreprises en 2017, contre **54%** en 2018. L'augmentation de ce nombre peut être révélatrice d'un problème croissant ou d'une prise de conscience des entreprises par rapport à l'an dernier. Alors que la protection des données et la lutte contre les failles de sécurité deviennent des enjeux majeurs, les entreprises s'intéressent et prennent davantage au sérieux ces comportements à risque. Dans tous les cas, ces chiffres témoignent d'un problème qu'il convient de résoudre.

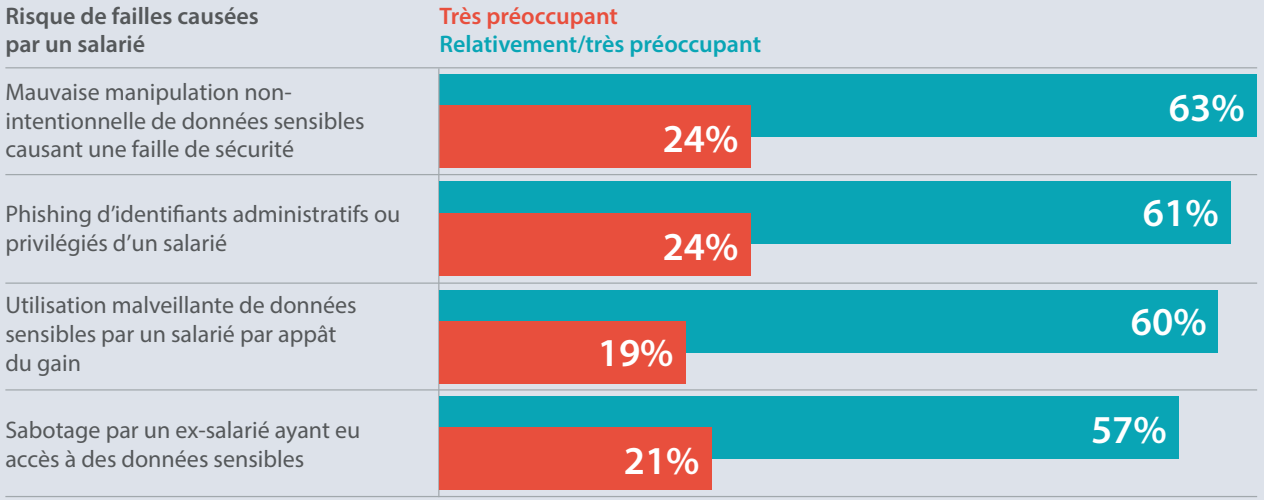
Intentionnels ou pas, ces comportements représentent une réelle menace de l'intérieur pour les entreprises (graph. n°4), d'autant plus que seulement 2 sondés sur 5 (**41%**) ont une confiance totale en leurs *insiders* ayant accès à des comptes privilégiés. L'étude révèle que les entreprises n'ont toujours pas, pour la plupart, le niveau de contrôle nécessaire pour faire face à ces préoccupations et gérer leurs comptes et utilisateurs privilégiés de façon à réduire nettement leur vulnérabilité.

35% seulement savent parfaitement quels salariés disposent d'accès privilégiés

37% seulement disposent de rapports sur les activités réalisées par les salariés privilégiés

34% seulement peuvent identifier les menaces spécifiques de la part de salariés disposant d'un accès privilégié

Graphique n°4
Risque de failles causées par un salarié



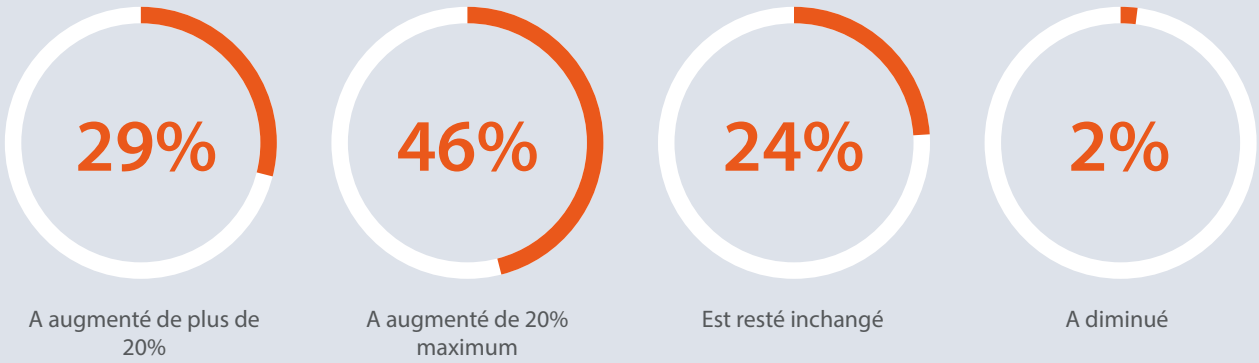
LE RISQUE DU TIERS

Les entreprises sont également exposées aux risques liés aux accès privilégiés de fournisseurs et tierces parties. Et la prolifération de ces utilisateurs tiers fait qu'il devient de plus en plus difficile pour les organisations de gérer ce risque grandissant.

Comme indiqué dans le graphique n°5, le nombre de fournisseurs tiers ayant accès aux systèmes IT des entreprises ne cesse de progresser, **75%** des entreprises déclarant en avoir au moins 20% de plus que l'année précédente. A ceci s'ajoute le fait que seulement **38%** se disent **très confiantes** dans leur capacité à encadrer le nombre des fournisseurs ayant des identités et des accès privilégiés, et seulement **35% très confiantes** quant au contrôle de leurs connexions. Les statistiques démontrent qu'il devient de plus en plus difficile de gérer le nombre des tierces parties ayant un accès quelconque aux réseaux IT, ce qui accroît le risque de compromission.

Le risque croissant provenant des fournisseurs tiers existe pour les organisations de toutes les tailles. Nos sondés travaillent dans des entreprises comptant entre 200 et 5000 employés, et toutes sont concernées par la multiplication des fournisseurs tiers. Dans les petites et moyennes entreprises (200-499 employés), **26%** constatent qu'autant de fournisseurs tiers que d'employés se connectent à leur réseau au cours d'une semaine. Quant aux grandes entreprises (plus de 5000 employés), **près d'une sur huit** ignore combien de fournisseurs se connectent réellement à leur réseau au cours d'une semaine.

Graphique n°5
Evolution du nombre de fournisseurs



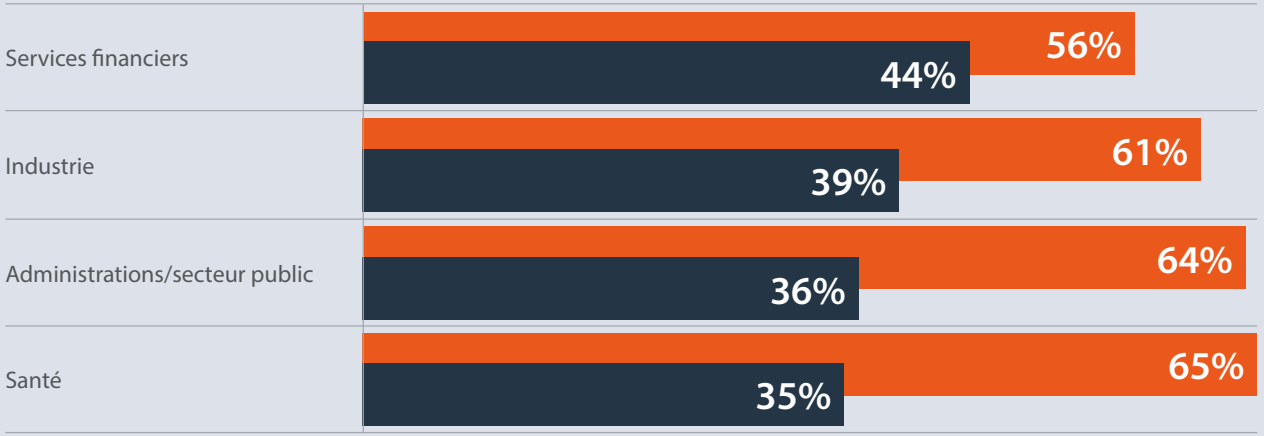
LE RISQUE DU TIERS

Comme le soulignait déjà le rapport 2017, les risques que représentent les tiers partis demeurent élevés. **76%** des entreprises indiquent que le fait qu'ils puissent partager les mots de passe réseau dans leurs propres entreprises représente un risque important ou fort. Parmi les risques les plus importants se trouvent également la gestion trop peu sécurisée des données à cause de partis tiers n'accordant pas assez d'importance à la sécurité des données (**76%**). Ou encore le risque que certains fournisseurs externalisent le travail auprès de sous-traitants, ce qui étend l'exposition et donc la surface d'attaque (**73%**). Une grande partie des risques émanent cependant des entreprises elles-mêmes, qui se reposent trop sur les fournisseurs tiers (**73%**) et accordent une trop grande confiance à leurs partenaires (**72%**).

Une façon de modérer et de gérer ce risque consiste à personnaliser et à adapter les accès accordés aux fournisseurs tiers. Pourtant, à peine plus de la moitié des entreprises (**56%**) met cela en place. Et alors que le niveau d'exposition des *insiders* est le plus élevé dans les entreprises du secteur bancaire, c'est bien là que l'on personnalise et adapte le moins les accès privilégiés des tierces parties (graph. n°6).

Graphique n°6
Type d'accès accordé à des fournisseurs tiers

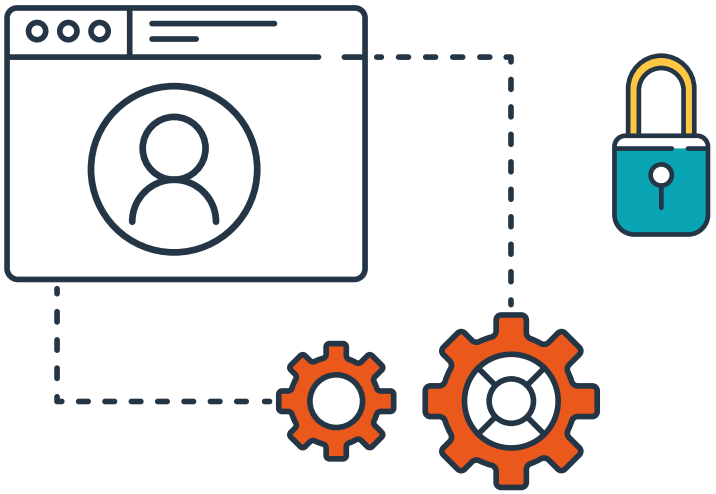
ON ou OFF/accès autorisé ou interdit
Différents niveaux d'accès selon les fournisseurs tiers



IV: CONTRÔLE, CONFIANCE, SÉCURITÉ

CONTRÔLE, CONFIANCE, SÉCURITÉ

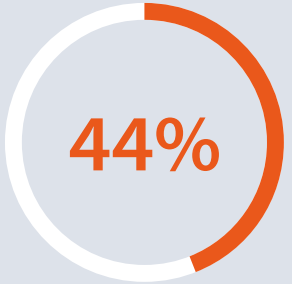
Comme le montre cette étude, certaines organisations utilisent une solution de gestion automatisée des identités et des accès privilégiés (PIM/PAM) afin de limiter les risques liés aux accès des salariés et tierces parties. Le graphique n°7 indique que moins de la moitié (**44%**) des entreprises utilisant une solution PIM/PAM ont subi une compromission sérieuse ou s'attendent à en subir une dans les 6 prochains mois, contre **69%** pour celles qui n'ont aucun contrôle sur leurs utilisateurs privilégiés. Nous pouvons donc en conclure que les entreprises dotées de solutions de ce type sont moins victimes de failles de sécurité et qu'elles ont une plus grande visibilité et un contrôle accru que celles qui utilisent des solutions manuelles ou pas de solution du tout.



Graphique n°7
% des entreprises ayant subi une faille sérieuse ou qui s'attendent à en subir une dans les 6 prochains mois

Aucun contrôle des identifiants privilégiés

Contrôle manuel des identifiants privilégiés



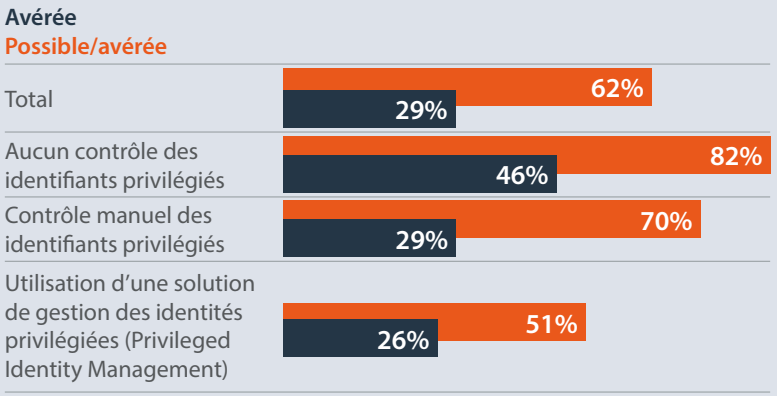
Utilisation d'une solution de gestion des identités privilégiées (Privileged Identity Management)

CONTRÔLE, CONFIANCE, SÉCURITÉ

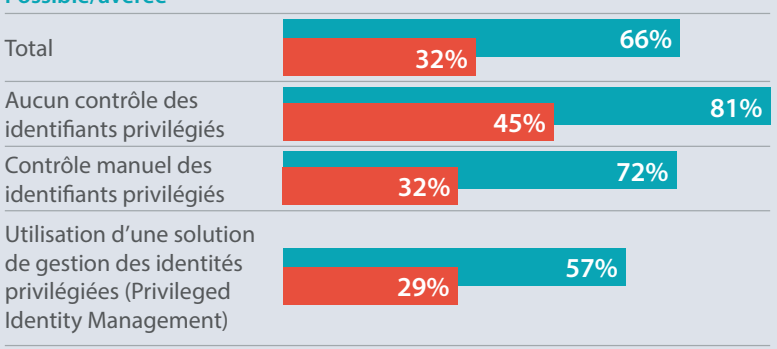
Plus précisément, les graphiques n°8 et 9 détaillent la répartition des failles entre celles initiées par un *insider* et par un parti tiers. Dans les deux cas, les entreprises qui utilisent une solution PIM/PAM pour gérer les utilisateurs et les comptes privilégiés expérimentent nettement moins de compromissions de sécurité.

Au cours de ce rapport, nous avons déjà mis en lumière le manque de visibilité des entreprises sur les employés ayant des accès privilégiés, ainsi que sur leur incapacité à rendre compte de l'activité de chaque utilisateur et à identifier les menaces provenant d'utilisateurs privilégiés.

Graphique n°8
Faille causée par un employé au cours de l'année précédente



Graphique n°9
Faille causée par un parti tiers au cours de l'année précédente

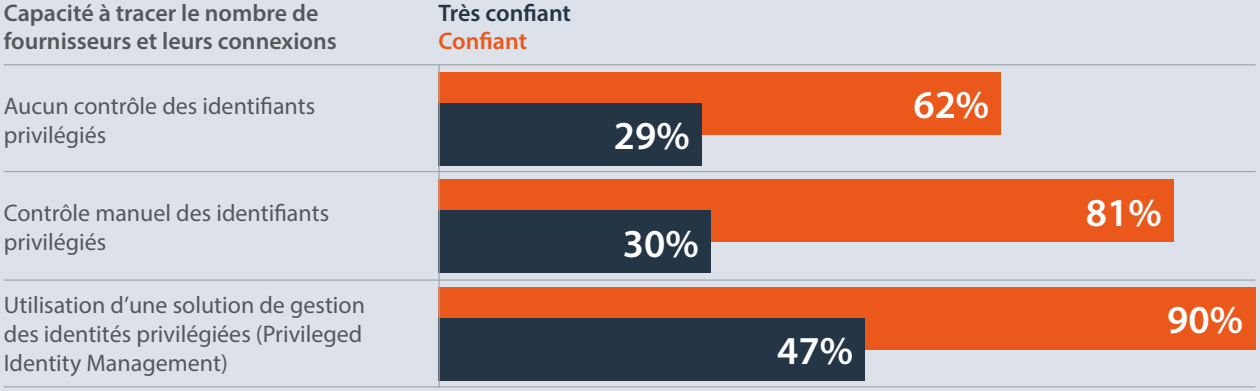


CONTRÔLE, CONFIANCE, SÉCURITÉ

La bonne nouvelle est que, en comparaison avec des entreprises n'effectuant aucun contrôle ou au mieux des contrôles manuels, celles qui utilisent une solution PIM/PAM sont bien plus confiantes en leur capacité à identifier et à détecter les menaces. Par exemple, **43%** des organisations utilisant des solutions PIM/PAM se disent confiantes dans leur capacité à identifier les menaces spécifiques de salariés ayant un accès privilégié contre **24%** pour celles n'ayant aucun contrôle des utilisateurs privilégiés et **26%** pour celles effectuant des contrôles manuels. Il est particulièrement intéressant de noter que les contrôles manuels n'offrent que très peu de visibilité en plus par rapport à l'absence totale de contrôles.

Il en est de même lorsque l'on s'intéresse à la visibilité des accès aux systèmes par les tierces parties. Comme indiqué dans le graphique n°10, les entreprises qui utilisent une solution PIM/PAM se disent être davantage en capacité de tracer le nombre de fournisseurs ayant des identités et des accès privilégiés, ainsi que la fréquence à laquelle ceux-ci se connectent à l'environnement informatique de l'entreprise.

Graphique n°10
Capacité à tracer le nombre de fournisseurs et leurs connexions



V: PROTÉGER LES IDENTITÉS ET LES ACCÈS PRIVILÉGIÉS DES MENACES

PROTÉGER LES IDENTITÉS ET LES ACCÈS PRIVILÉGIÉS DES MENACES

Cette étude démontre que de nombreuses interrogations cruciales subsistent quant à la façon dont les entreprises gèrent les accès des *insiders* et fournisseurs privilégiés à leurs systèmes informatiques. Avec l'évolution des cyberattaques, les risques encourus à cause d'identités et d'accès privilégiés compromis ou utilisés à mauvais escient ne cessent de croitre alors même que les règlementations se durcissent. Bien qu'il soit impossible d'éviter toutes les attaques, les professionnels de la sécurité informatique doivent mettre en place des contrôles et des politiques de moindre privilège afin d'en limiter les risques et les conséquences.

Les entreprises de toutes tailles et de tous secteurs d'activité peuvent désormais réduire leur surface d'attaque et mieux protéger leurs données critiques et systèmes IT grâce à des solutions permettant d'analyser et de gérer de façon continue et automatique les accès et identifiants de leurs *insiders* et prestataires privilégiés.

Les solutions PIM/PAM confèrent aux entreprises plus de visibilité et de contrôle sur leurs salariés et fournisseurs tiers disposant d'accès privilégiés. Des solutions conçues pour optimiser l'expérience utilisateur permettent par ailleurs d'accroître leur productivité et leur efficacité, d'automatiser la gestion des accès privilégiés et d'éliminer les risques associés à des comportements à risque. Couplée à la formation continue des salariés, l'adoption réussie d'une solution PIM/PAM permet l'analyse permanente, la protection et la gestion des identifiants privilégiés, renforçant ainsi la sécurité et éliminant un vecteur d'attaque majeur.

BOMGAR™

Les solutions Bomgar aident les organisations à contrôler et à gérer les accès privilégiés aux données et systèmes informatiques critiques, tout en optimisant la productivité des utilisateurs. Les solutions Bomgar leur permettent de se connecter rapidement et en toute sécurité aux systèmes tout en protégeant les identifiants et les terminaux des menaces. Les identifiants privilégiés sont analysés, stockés et renouvelés et les utilisateurs bénéficient de droits et de niveaux d'accès définis en fonction de leurs besoins.

Plus d'informations sur www.bomgar.com/fr