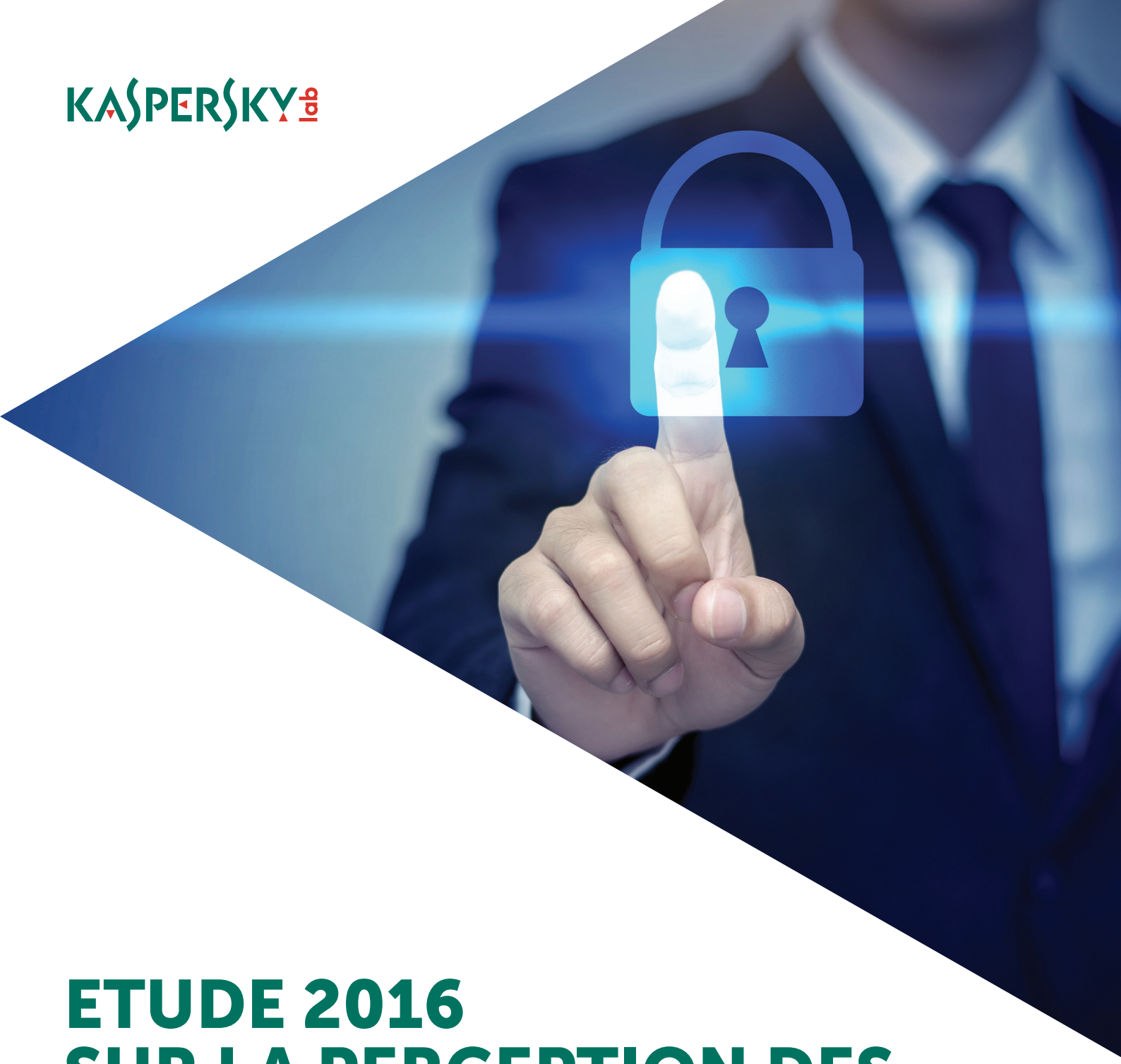


ETUDE 2016 SUR LA PERCEPTION DES MENACES INFORMATIQUES PAR LES ENTREPRISES EUROPÉENNES

Série de rapports spéciaux 2016 sur les risques liés à la sécurité informatique des entreprises

Kaspersky Lab

TABLE DES MATIÈRES

INTRODUCTION 3

PERCEPTION DES MENACES DE SÉCURITÉ INFORMATIQUE 4

DOMAINES D'EXPERTISE LES PLUS VULNÉRABLES 4

EXAMEN APPROFONDI DE LA PROTECTION
DES APPAREILS MOBILES 5

DOMAINES D'AMÉLIORATION : PERTES D'APPAREILS
PHYSIQUES, FUITES DE DONNÉES, PERTES DE DONNÉES 6

LA RÉALITÉ DE L'ENVIRONNEMENT DES MENACES 8

LA PRÉOCCUPATION PAR RAPPORT À L'EXPÉRIENCE 8

LES VECTEURS D'ATTAQUE COURANTS 9

MENACES SPÉCIFIQUES 10

- Attaques ciblées 10
- Cryptomalwares 11
- Attaques DDoS 12
- Attaques par phishing 13

LES CONSÉQUENCES 14

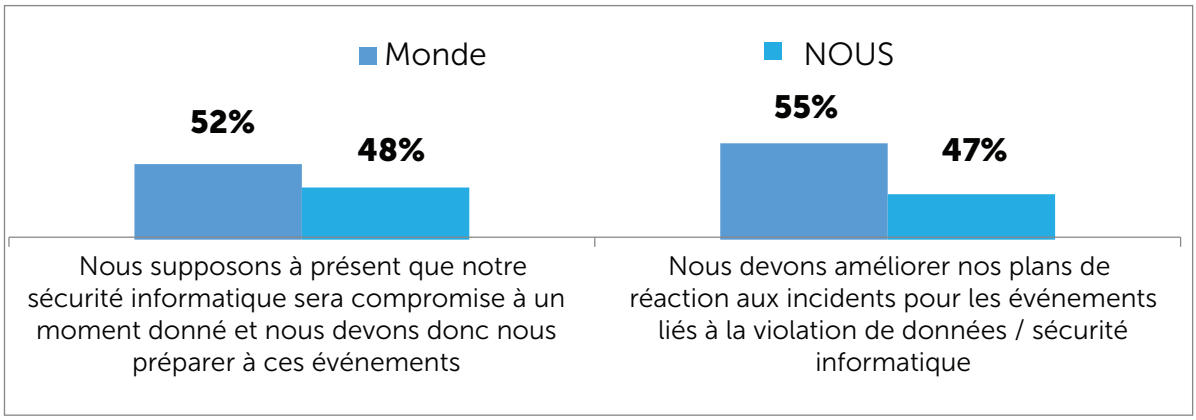
LES CAUSES PRINCIPALES DE LA FUITE DE DONNÉES :
EMPLOYÉS NON FORMÉS, PHISHING, PERTE D'APPAREILS 15

CONCLUSION : ÉTABLIR LE LIEN 16

INTRODUCTION

Pour enquêter sur la perception et la réalité du paysage des cybermenaces, en partenariat avec B2B International, Kaspersky Lab a réalisé une étude mondiale auprès de plus de 4 000 représentants d'entreprises de 25 pays. Nous avons interrogé les entreprises sur la manière dont elles perçoivent les principales menaces et les mesures prises pour les combattre. **Ce rapport fournit des informations tirées de sondages spécifiques à l'Europe occidentale.**

L'une des principales conclusions de l'enquête de cette année est basée sur la perception du paysage des menaces en général. Les entreprises déclarent unanimement que les cybermenaces sont très dommageables et que la cybersécurité est l'une des conditions majeures pour que les entreprises restent à flot. Cependant, les attitudes à l'égard des approches de protection générale sont en résumé assez mitigées, comme le montre le tableau ci-dessous.



Source : Rapport sur les risques liés à la sécurité informatique 2016, données concernant l'Europe occidentale

Le secteur de la cybersécurité reconnaît presque à l'unanimité qu'une stratégie de protection efficace doit prendre en compte le caractère inévitable d'une compromission. Bien sûr, les mesures de prévention comme la sécurité des terminaux, les pare-feux et les systèmes de protection contre les programmes malveillants restent une nécessité. Cependant, si malgré toutes les précautions, une violation se produit, les outils, les experts et les renseignements doivent être prêts pour réagir et réduire les dommages.

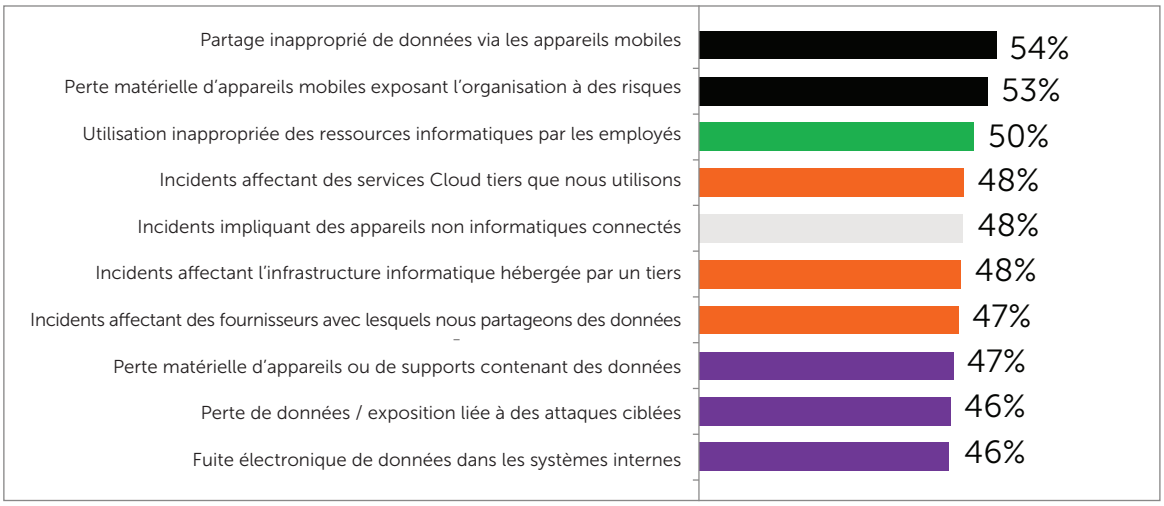
Tous les clients ne sont pas d'accord avec cela, comme le montrent nos conclusions. Seule la moitié (**52 %**) d'entre eux reconnaît la nécessité d'être mieux préparé à une compromission en matière de sécurité à l'échelle mondiale, **48 % sont d'accord avec cette affirmation en Europe occidentale**. remarquons également une part plus importante des entreprises qui établissent la nécessité d'améliorer la réponse aux incidents, grâce à leurs recherches généralement plus approfondies sur le paysage des menaces.

PERCEPTION DES MENACES DE SÉCURITÉ INFORMATIQUE

Cette année, nous avons adopté une nouvelle approche lorsque nous avons interrogé les entreprises sur les incidents liés à la cybersécurité. Bien que nous ayons couvert certaines menaces spécifiques, nous avons détourné notre attention des types d'attaques pour nous concentrer sur les dommages causés. Cela nous a permis de parler le même langage, tant avec les experts techniques que les dirigeants d'entreprise.

Alors comment les entreprises perçoivent-elles les menaces de sécurité informatique ?

DOMAINES D'EXPERTISE LES PLUS VULNÉRABLES



Source : Rapport sur les risques liés à la sécurité informatique 2016, données mondiales

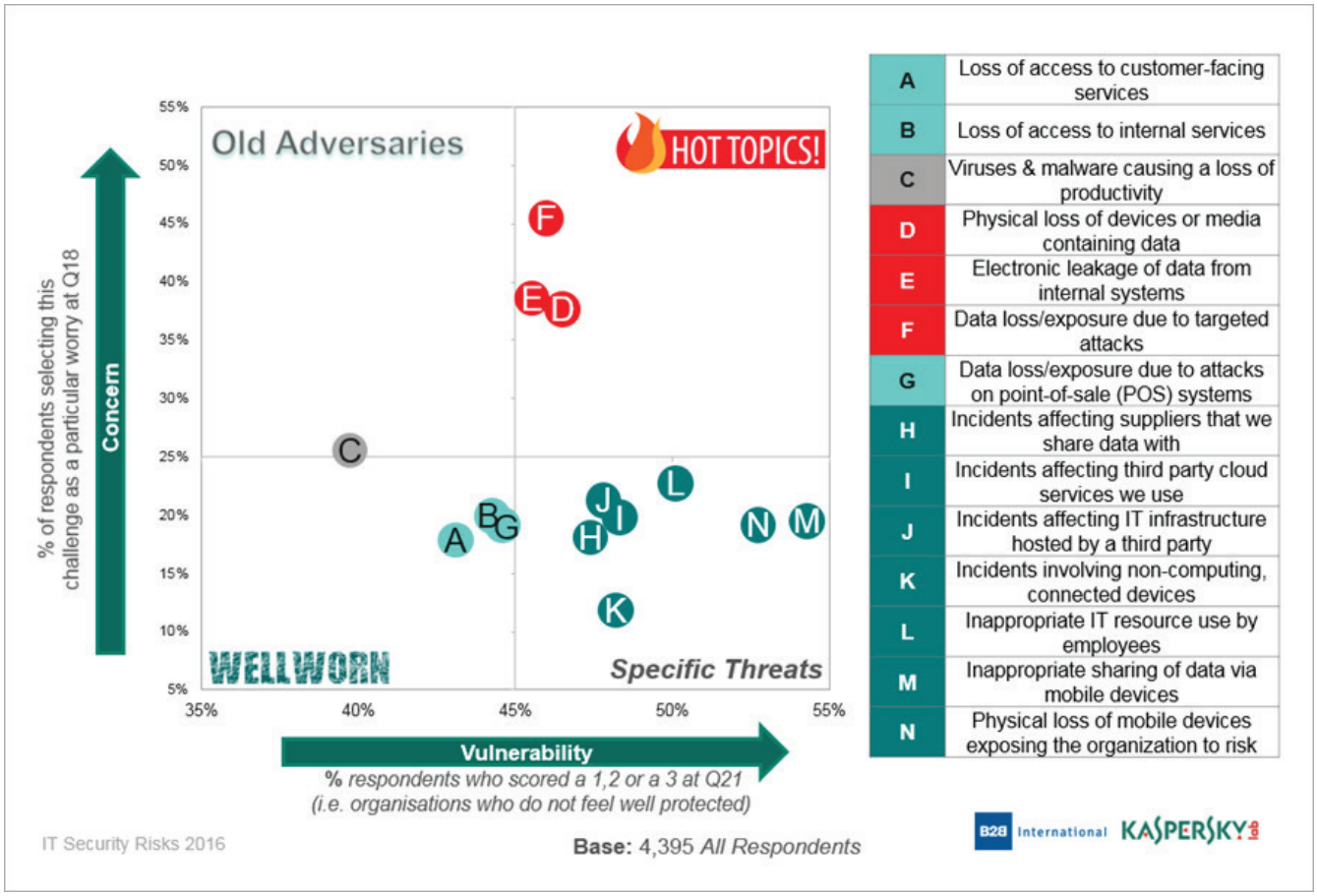
Six domaines vulnérables types sur dix sont directement liés à la crainte de perdre des données. Mais la vraie surprise est que le point de vulnérabilité le plus fréquent correspond à l'utilisation inappropriée ou le partage de données via les appareils mobiles, avec **54 %** des entreprises déclarant qu'elles ont des difficultés à comprendre comment faire face à cette menace à l'échelle mondiale, **55% en Europe occidentale.**

EXAMEN APPROFONDI DE LA PROTECTION DES APPAREILS MOBILES

Intéressons-nous de plus près à la menace d'attaques via les appareils mobiles. Les entreprises signalent que le nombre de smartphones et de tablettes au sein de leur organisation augmente rapidement. **37 %** des entreprises mondiales indiquent une augmentation importante des smartphones qui accèdent aux données d'entreprise et que cela doit être pris en compte selon différents points de vue, notamment celui de la sécurité. **L'infrastructure des entreprises d'Europe occidentale témoigne d'une plus grande maturité, mais 26 % des entreprises signalent tout de même une augmentation significative du nombre de smartphones**. La complexité croissante des infrastructures informatiques est une préoccupation générale qui fait augmenter les coûts d'entretien et de sécurité. **36 % des entreprises européennes admettent que la complexité de l'infrastructure informatique affecte directement leur capacité à maintenir le niveau de sécurité nécessaire, ce qui est nettement inférieur au résultat mondial (52 %). Il s'agit néanmoins du motif le plus fréquemment donné pour investir davantage dans la sécurité informatique en Europe occidentale**.

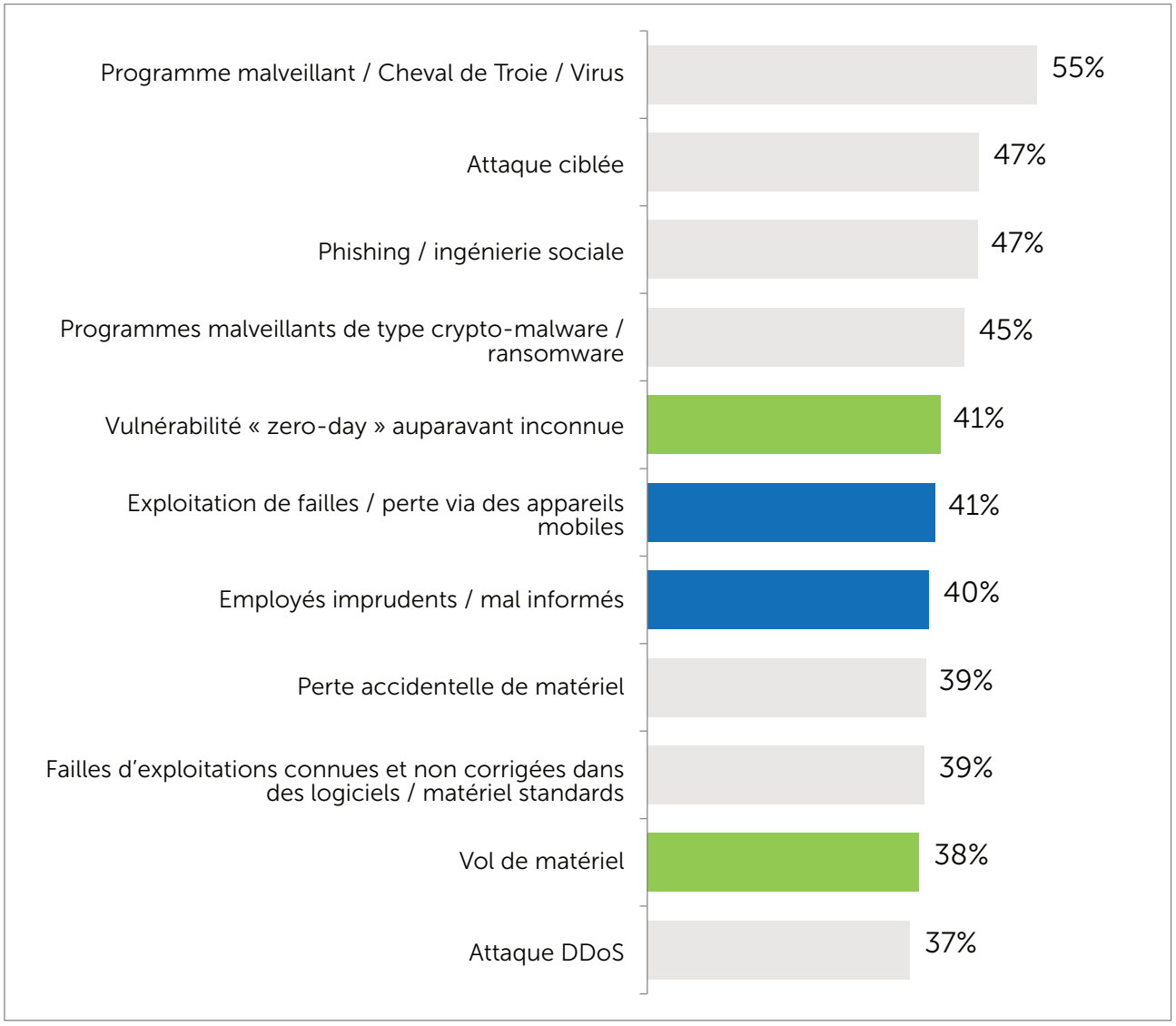
En outre, la complexité du problème dépasse largement l'utilisation d'appareils personnels dans un cadre professionnel (BYOD). Nous avons constaté qu'une part importante des entreprises signale une augmentation de tous les types d'appareils, incluant jusqu'aux serveurs virtuels et ordinateurs de bureau. En termes de sécurité, la source des appareils n'a pas vraiment d'importance. Ce qui importe, c'est d'avoir une stratégie de protection adéquate en place. Avec plus de la moitié des représentants d'entreprises interrogés déclarant qu'ils prévoient des difficultés dans la protection des données sur les appareils mobiles, cette question peut être identifiée comme le point le plus alarmant pour la sécurité des entreprises à l'heure actuelle. À l'avenir, il est vraisemblable que la protection s'étende aux instances virtuelles et aux appareils IoT, bien que de nombreuses entreprises signalent déjà que ces technologies sont problématiques pour la sécurité.

DOMAINES D'AMÉLIORATION : PERTES D'APPAREILS PHYSIQUES, FUITES DE DONNÉES, PERTES DE DONNÉES



Source : Rapport sur les risques liés à la sécurité informatique 2016, données mondiales

Comme nous pouvons le constater dans le graphique ci-dessus, presque tous les types de conséquences se situent dans la zone à haut risque : perte de données, incidents liés à des fournisseurs tiers, aux services Cloud ou aux appareils IoT et mobiles. Les attaques ciblées sont un domaine particulier qu'il convient de remarquer : face à cela, les entreprises sont très préoccupées et se sentent vulnérables. Il est également intéressant de noter que sur le plan de la perception, les entreprises se sentent bien protégées contre les attaques de programmes malveillants qui provoquent une perte de productivité. Mais il est assurément trop tôt pour oublier la menace que représentent les attaques de programmes malveillants.



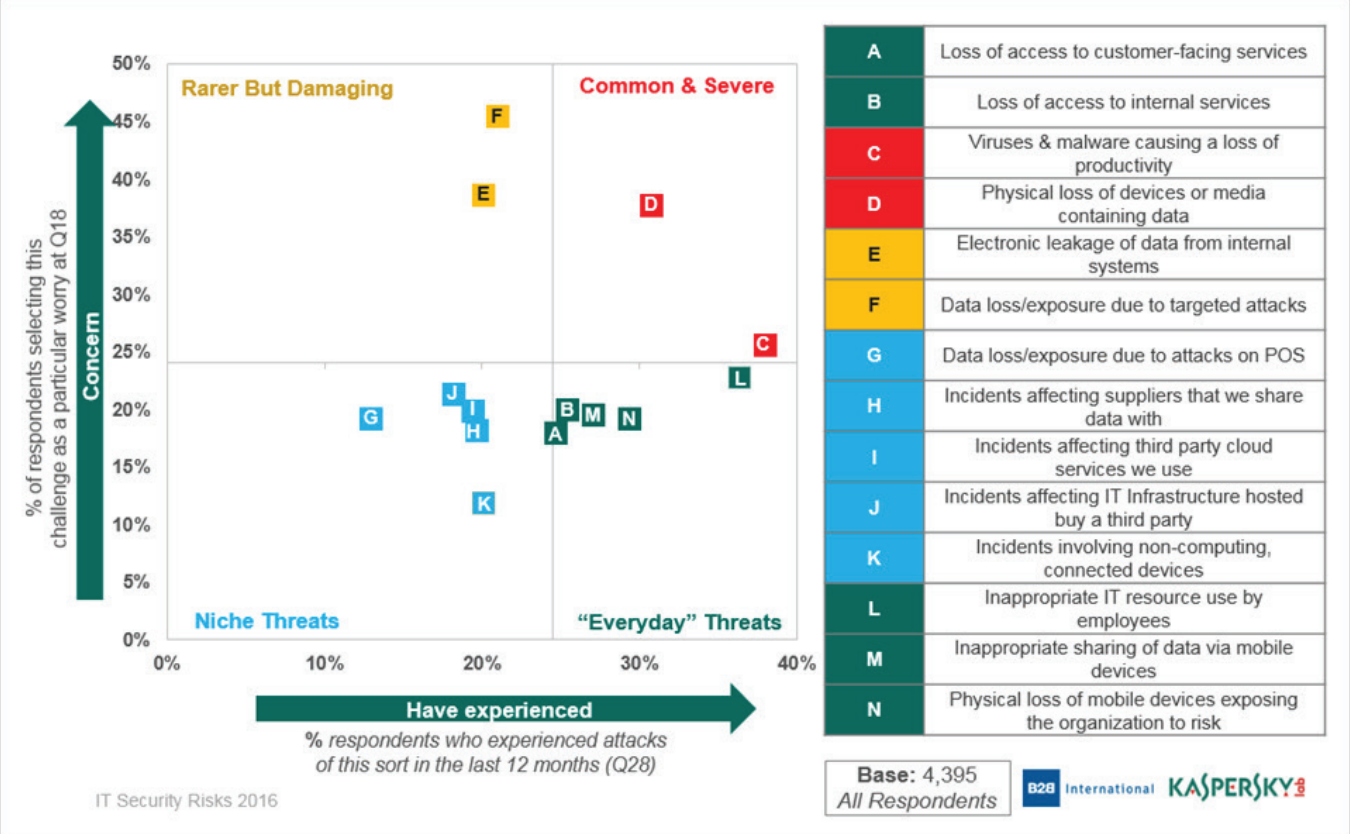
Source : Rapport sur les risques liés à la sécurité informatique 2016, données concernant la région Europe occidentale

Dans cette liste de menaces, nous remarquons les attaques DDoS et l'exploitation de failles non corrigées dans un logiciel standard, ainsi que les crypto-malwares. Le phishing est souvent la cause première de différents incidents de sécurité et **47 % des entreprises d'Europe occidentale** signalent qu'il s'agit d'une préoccupation majeure.

LA RÉALITÉ DE L'ENVIRONNEMENT DES MENACES

Comparer la perception à la réalité nous donne une répartition des cybermenaces différente et montre une fois de plus que la menace d'attaques par des programmes malveillants prévaut encore. Ceci est lié au fait que les entreprises ont fait l'expérience de cette menace plus que toute autre.

LA PRÉOCCUPATION PAR RAPPORT À L'EXPÉRIENCE

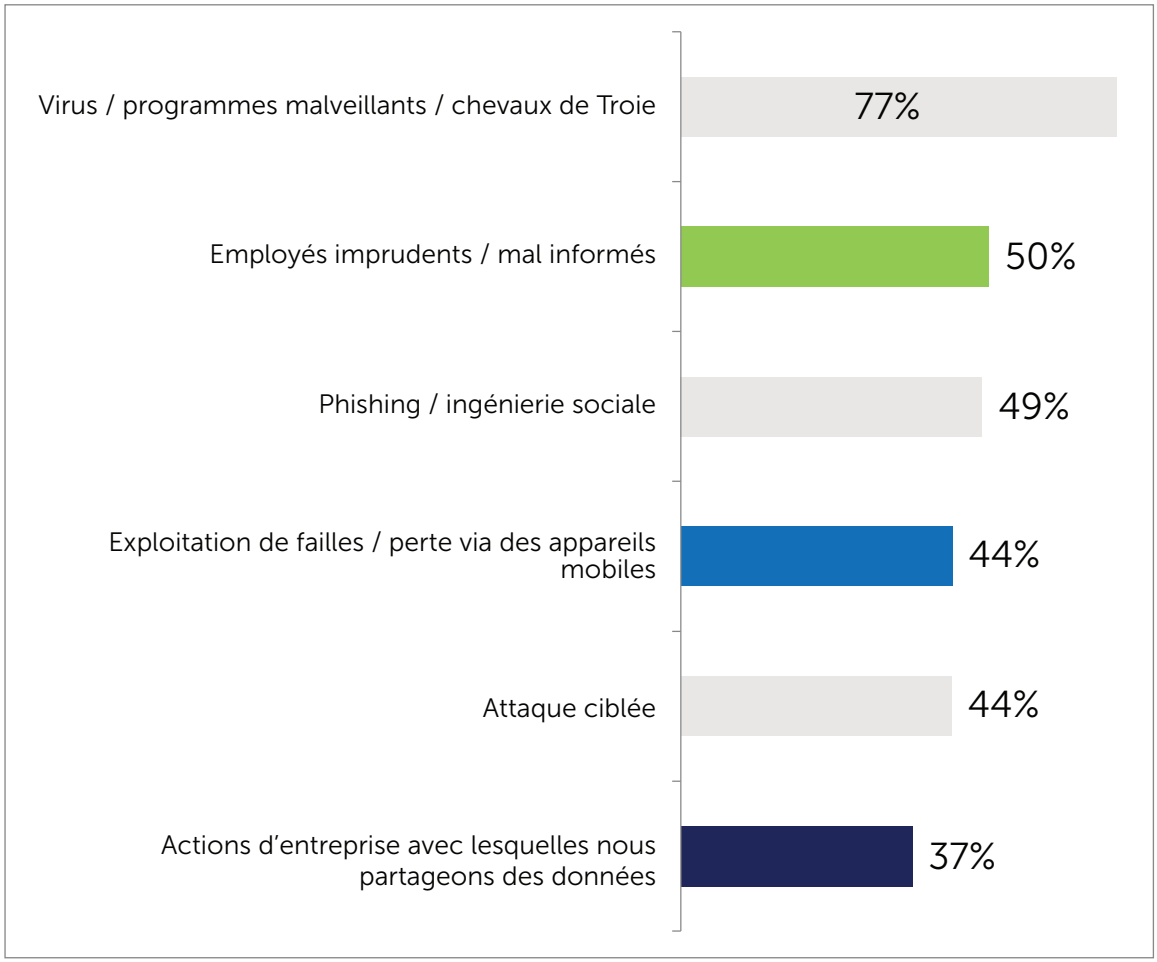


Source : Rapport sur les risques liés à la sécurité informatique 2016, données mondiales

Comme illustré ci-dessus, la menace la plus dangereuse en rapport avec la protection des données est la perte physique ou le vol de périphériques. D'autres menaces, comme la fuite de données depuis des systèmes internes, méritent réflexion. Les entreprises s'interrogent cependant quant à l'efficacité des efforts nécessaires sur le plan du retour sur investissement.

Heureusement, les nouvelles menaces liées à l'utilisation de services et d'infrastructures de tiers sont relativement rares et peuvent aujourd'hui être considérées comme des « menaces de niche ». Aussi, lorsqu'il s'agit de prédire les menaces futures, les défis liés au Cloud, à l'IaaS et à l'IoT sont assurément les meilleurs candidats du prochain casse-tête.

LES VECTEURS D'ATTAQUE COURANTS

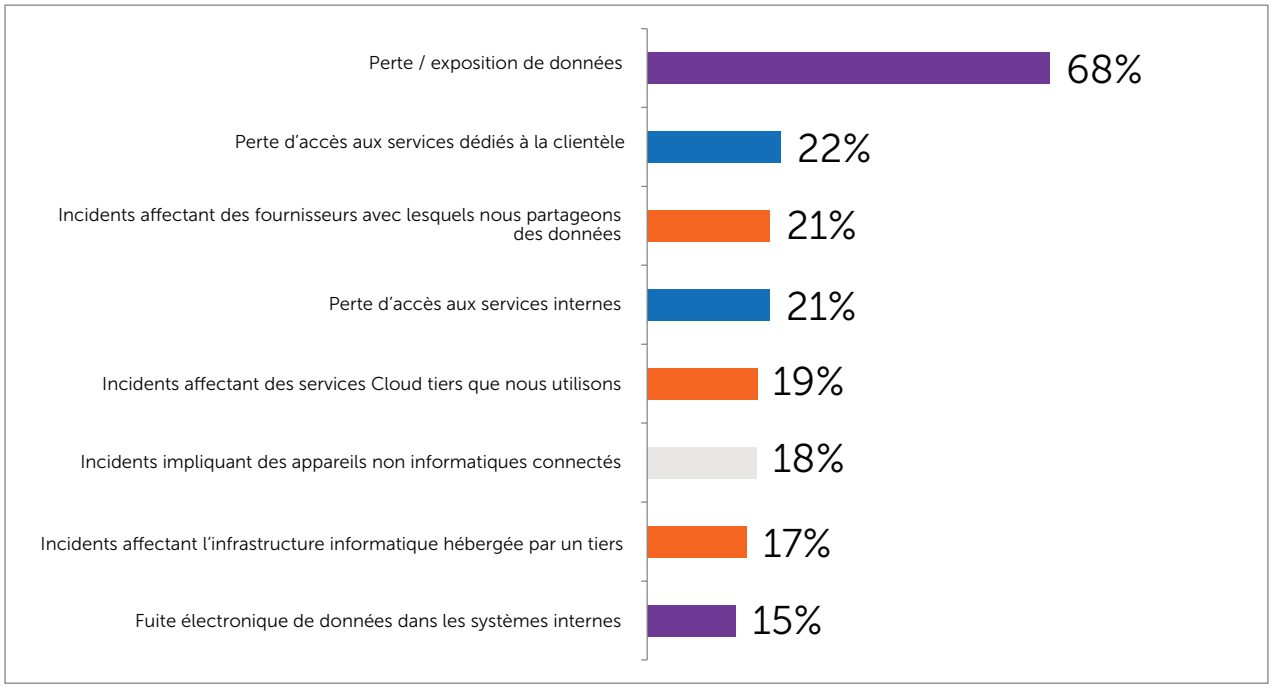


Source : Rapport sur les risques liés à la sécurité informatique 2016, données concernant la région Europe occidentale

La comparaison des « menaces les plus redoutées » et de l'expérience d'incidents réels met en lumière les domaines potentiels où les entreprises sont moins visibles. Nous observons encore une fois des difficultés à gérer la sécurité des appareils mobiles, mais les actes réalisés par des employés négligents constituent la plus grande révélation (**50 % des entreprises de la région Europe occidentale** indiquent que cela a contribué à une attaque réussie).

MENACES SPÉCIFIQUES

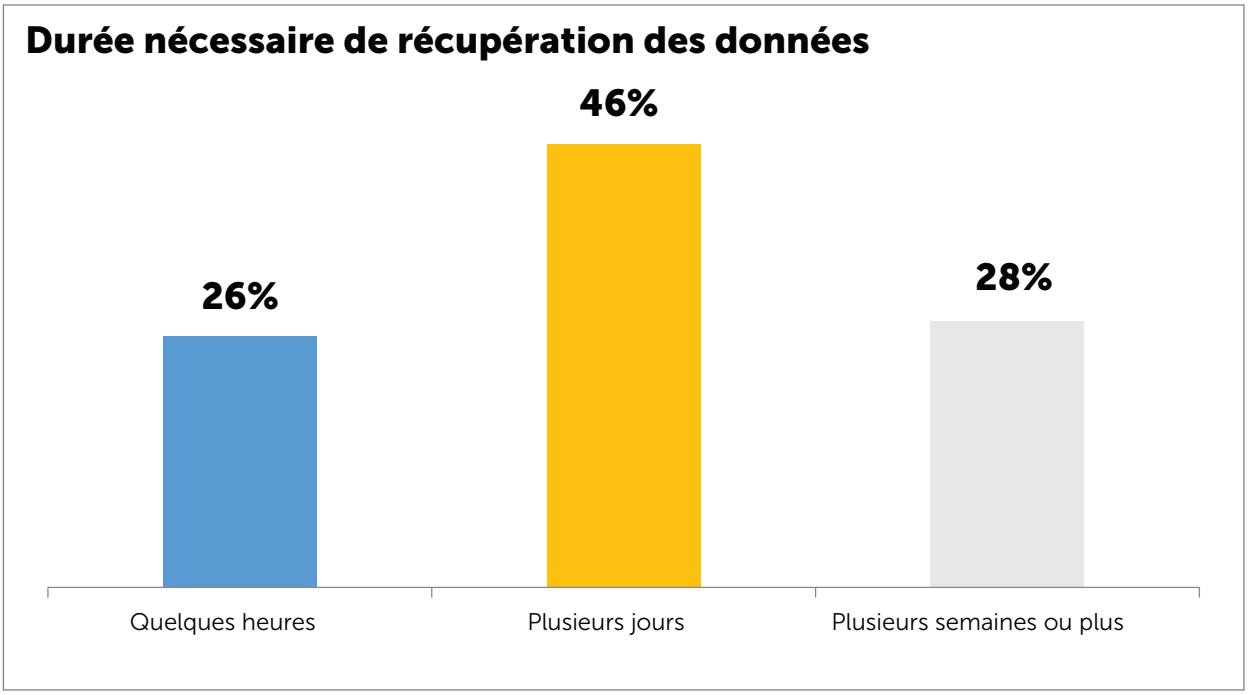
Attaques ciblées



Source : Rapport sur les risques liés à la sécurité informatique 2016, données mondiales

Ici, la perception et la réalité coïncident bien, car les conséquences les plus courantes d'une attaque ciblée sont la perte ou le vol de données. Les causes les plus courantes ayant contribué à une violation de sécurité ciblée réussie à l'échelle mondiale sont les compromissions de tiers (**46 %** ont signalé ce vecteur d'attaque), l'exploitation de failles sur les appareils mobiles (**48 %**), les actions d'hacktivistes (**37 %**) et les actions malveillantes du personnel interne (**38 %**).

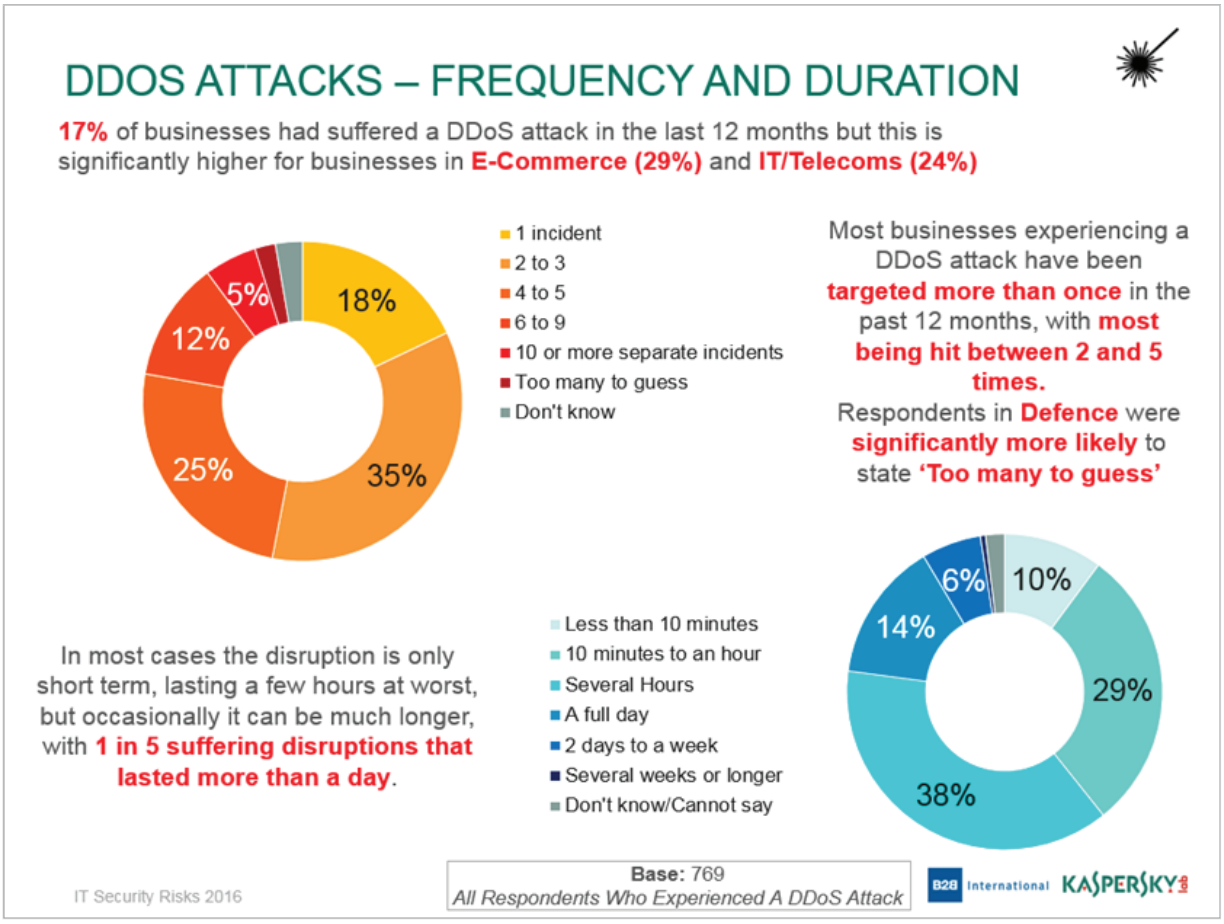
Cryptomalwares



Source : Rapport sur les risques liés à la sécurité informatique 2016, données concernant la région Europe occidentale

Les cryptomalwares ont été décrits de manière détaillée dans ce rapport sur les risques liés à la sécurité informatique. La constatation la plus importante est que pour trois incidents sur quatre, les entreprises subissent les conséquences pendant une longue période : des jours ou même des semaines sont nécessaires pour récupérer les données affectées. Globalement, **20 %** des entreprises du monde entier ont signalé un incident impliquant un ransomware, **18 % en Europe occidentale**.

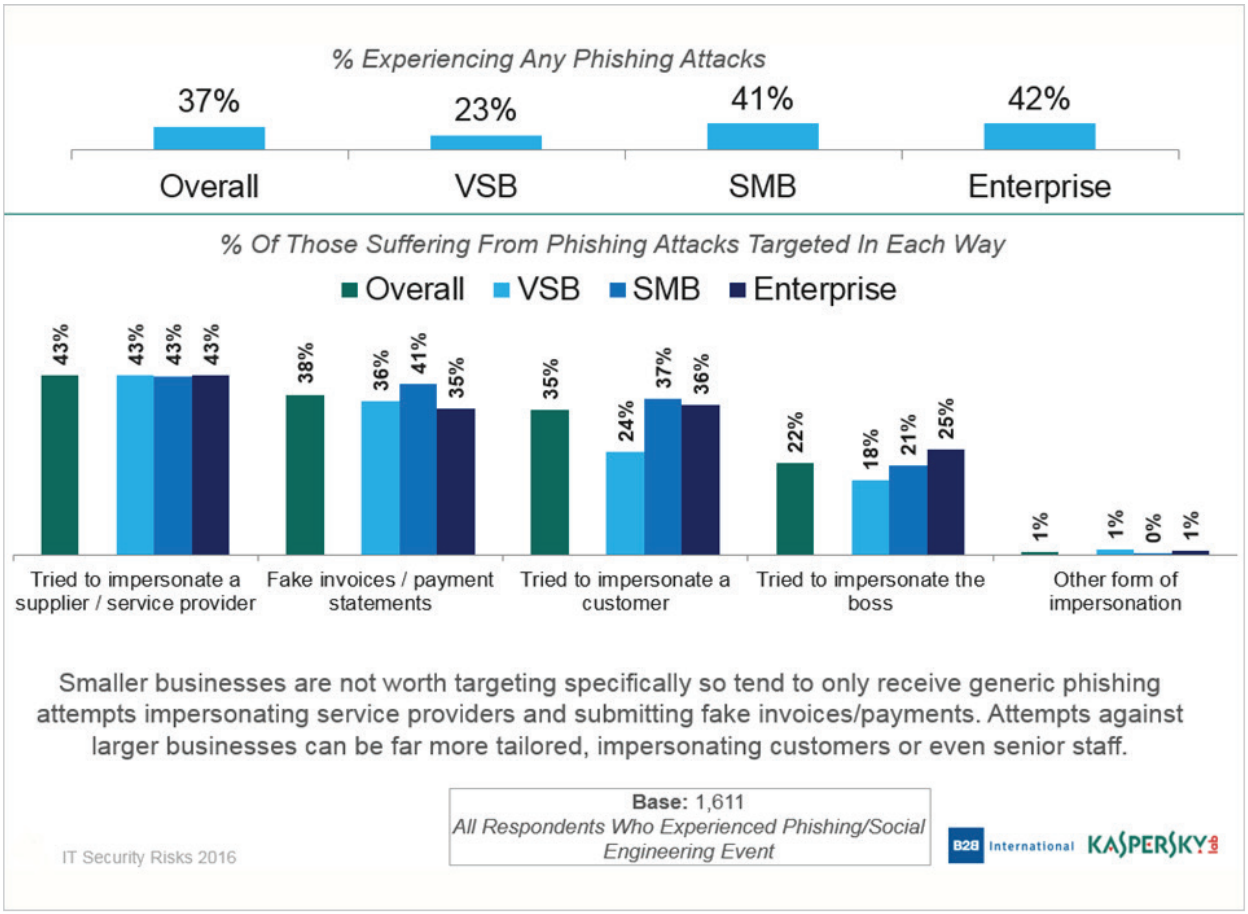
Attaques DDoS



Source : Rapport sur les risques liés à la sécurité informatique 2016, données mondiales

Nous avons découvert que **17 %** des entreprises ont subi une attaque DDoS au cours des 12 derniers mois, **14 % dans la région Europe occidentale**. Il est également important de noter que, pour la deuxième année consécutive, nous observons comment les attaques DDoS coïncident avec d'autres types de violation de sécurité (notamment les attaques ciblées). Un tiers (**32 %**) des personnes ayant signalé une attaque ciblée ont mentionné l'attaque par déni de service comme une contribution probable.

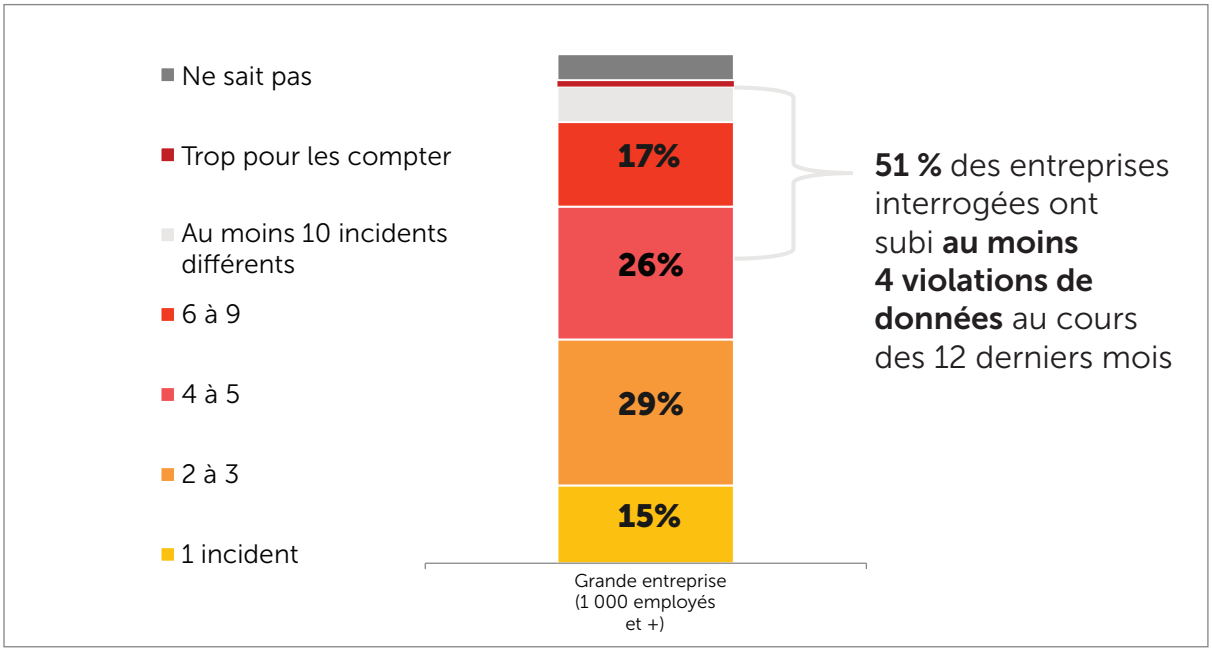
Attaques DDoS par phishing



Source : Rapport sur les risques liés à la sécurité informatique 2016, données mondiales

Étant donné l'importance perçue et réelle de la protection contre le phishing, nous avons demandé aux entreprises de fournir plus d'informations sur ce type d'attaque. Nous avons constaté que le type d'usurpation d'identité le plus fréquemment utilisé par les attaquants est de se faire passer pour un fournisseur ou un prestataire de services tiers. Globalement, **31 % des entreprises d'Europe occidentale ont connu au moins une attaque de phishing.**

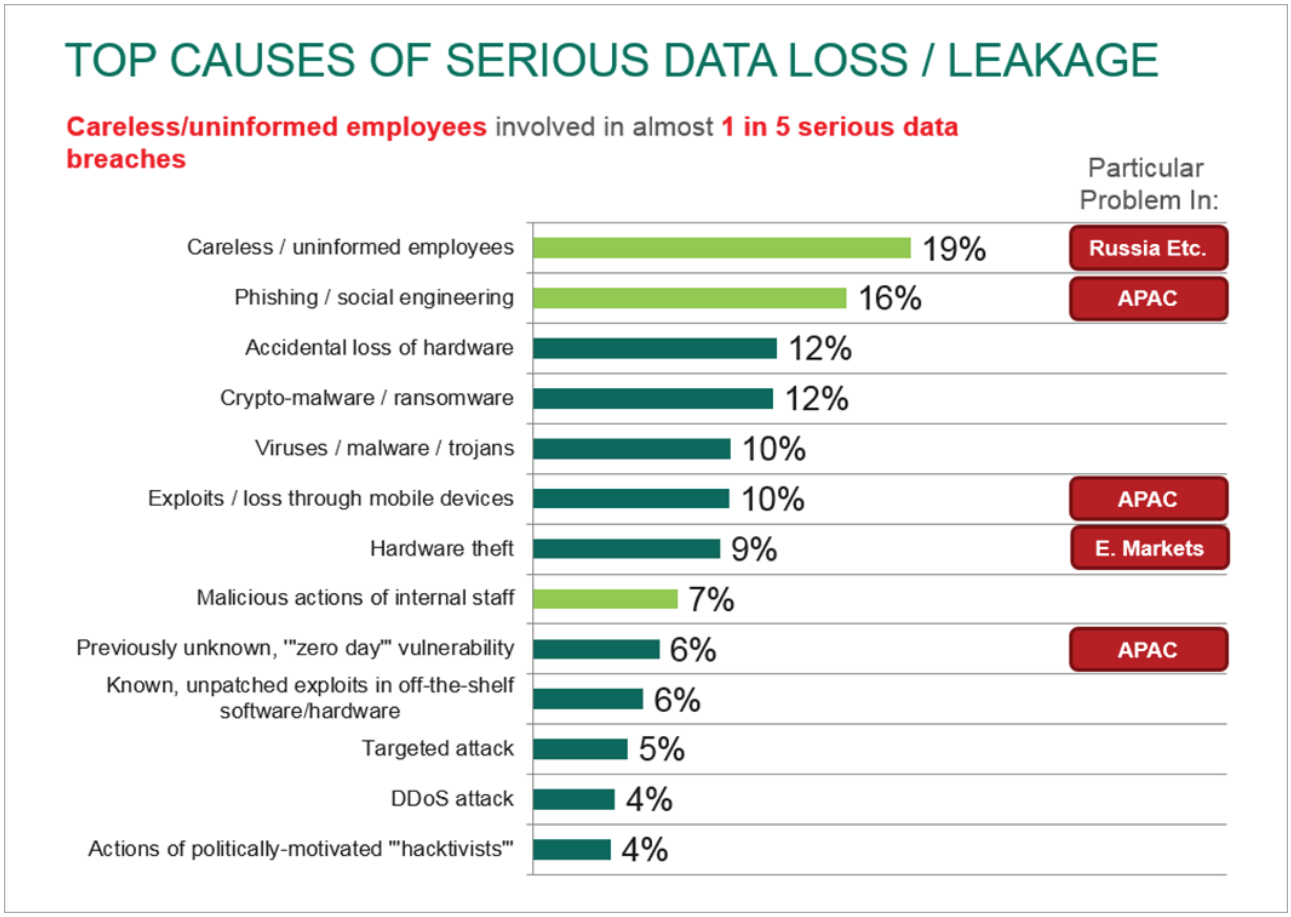
LES CONSÉQUENCES



Source : Rapport sur les risques liés à la sécurité informatique 2016, données mondiales

Notre enquête a révélé que 36 % des entreprises européennes ont subi des pertes de données en raison d'un incident de cybersécurité, ce qui est nettement inférieur à la proportion mondiale (43 %). Les petites entreprises employant jusqu'à 50 employés sont généralement moins touchées par les fuites de données et davantage par les temps d'arrêt, mais pour les PME et grandes entreprises, les pertes de données sont la conséquence inévitable d'attaques qui se produisent environ une fois par seconde dans le monde. **51 % des entreprises en Europe occidentale ont subi au moins quatre violations de données au cours des 12 derniers mois.**

LES CAUSES PRINCIPALES DE LA FUITE DE DONNÉES : EMPLOYÉS NON FORMÉS, PHISHING, PERTE D'APPAREILS



Source : Rapport sur les risques liés à la sécurité informatique 2016, données mondiales

Les employés négligents sont l'une des principales raisons de la perte ou du vol de données. Près d'une entreprise sur cinq (**19 %**) affirme que ce facteur a contribué à une violation grave des données. **En Europe occidentale, c'est aussi un facteur majeur, avec 13 % des entreprises qui mentionnent la négligence des employés comme étant une raison de violation de données majeure.**

La principale constatation de notre enquête sur la réalité des menaces est la multiplicité des menaces auxquelles sont confrontées les entreprises, des virus et du phishing à l'exploitation des vulnérabilités « zero-day » et aux attaques DDoS. Ce paysage des menaces montre l'importance des mesures classiques telles que la protection des terminaux contre les programmes malveillants, la lutte contre le phishing et l'évaluation de la vulnérabilité. Mais les menaces que constituent les attaques ciblées, l'exploitation des failles des appareils mobiles et les ransomwares appellent également à de nouvelles approches.

CONCLUSION : ÉTABLIR LE LIEN

Le secteur de la sécurité en est à un stade où les solutions classiques ne couvrent pas certaines des nouvelles menaces et les entreprises restent indécises par rapport aux méthodes qui vont au-delà de la prévention, comme la formation du personnel, les audits de sécurité et l'expertise-conseil. Ces nouvelles méthodes de protection sont tout à fait différentes des anciennes et dans un premier temps, il peut sembler relativement difficile de les déployer et d'en mesurer les résultats.

Alors quelle est la bonne approche ?

Nous sommes convaincus que 99 % des menaces de sécurité peuvent être repoussées par des technologies logicielles hautement efficaces, intelligentes et automatisées. Le 1 % restant ne requiert pas de technologie, simplement un regard nouveau.

La réussite du prochain fournisseur de sécurité majeur dépendra de sa capacité à rassembler de la façon la plus efficace possible des informations concernant le vaste éventail de cybermenaces et les méthodes de protection. Parler le même langage que les entreprises est en passe de devenir une nécessité d'importance capitale.

Chez Kaspersky Lab, nous pensons qu'être un conseiller de confiance est la priorité absolue. La technologie est importante, mais nous avons montré dans ce rapport que la façon dont les entreprises perçoivent la sécurité peut être différente de celle dont elles se protègent. Les stratégies de protection peuvent parfois exclure certains domaines de menace importants.

L'objectif de la véritable sécurité de nouvelle génération est donc d'établir le lien entre le domaine de la perception des menaces, celui de la réalité et l'approche en matière de protection, afin de les équilibrer parfaitement. Dans un monde idéal, les entreprises constatent que des menaces réelles les attaquent, interprètent ces données avec précision et construisent des défenses pour prévenir et prédire les attaques futures selon ce modèle de menace précis.

Securelist, la ressource destinée à la recherche technique, l'analyse et la réflexion des experts de Kaspersky Lab.

Suivez-nous

Site Entreprises Kaspersky Lab

Blog d'Eugene Kaspersky

Blog B2C de Kaspersky Lab

Blog B2B de Kaspersky Lab

Service d'informations de sécurité de Kaspersky Lab

Académie Kaspersky Lab