vmware®

France

Édition 2021 du rapport VMware sur l'état des menaces en France

2021

Introduction

Cette étude a pour objectif de comprendre les difficultés et les défis auxquels les entreprises françaises sont confrontées face à la montée des cyberattaques. Elle identifie les tendances de piratage et d'actes de malveillance, ainsi que l'impact des violations sur le plan financier et de la réputation des entreprises visées au cours d'une année hors norme. Elle examine l'approche adoptée par les entreprises françaises concernant l'adoption de nouvelles technologies, la mise en œuvre d'une stratégie de sécurité Cloud-first ainsi que la complexité de l'environnement de gestion de la cybersécurité.

Ce rapport dévoile les stratégies adoptées par les responsables de la sécurité (ou RSSI) pour répondre aux défis des espaces de travail distribués et adapter les défenses afin que la sécurité soit intrinsèque à l'infrastructure et aux opérations.

Synthèse de la direction :

Avant-propos

CONTEXTE DE LA CYBERSÉCURITÉ EN FRANCE

Rick McElroy, stratégiste en cybersécurité chez VMware

Tout est différent, et pourtant pareil.

Les professionnels de la cybersécurité qui ont contribué à la quatrième édition de notre rapport sur l'état des menaces en France sont dans une position très différente par rapport à ce qu'ils exprimaient lors de notre questionnaire en 2020. En un an, nous avons assisté à la plus grande transformation des habitudes de travail de l'histoire, et les équipes de sécurité président désormais sur un écosystème qui est plus distribué et hétérogène que jamais.

Les programmes de transformation numérique ont progressé rapidement, car la surface de cyberattaque s'est soudain trouvée étendue aux salons, cuisines, réseaux domestiques et appareils personnels. Les télétravailleurs se comportent de façon très différente des collaborateurs qui vont au bureau, notamment en accédant au réseau à des heures imprévisibles, car ils tentent de rester productifs tout en s'occupant de leur famille et en appliquant les recommandations des autorités. Par conséquent, le trafic réseau a changé au point d'en être méconnaissable. Les défenseurs doivent adapter leurs systèmes de veille et les points de déclenchement d'alertes, ou risquer de laisser les agresseurs exploiter des schémas atypiques pour masquer leurs tentatives d'infiltration.

Dans ce contexte évoluant rapidement, certaines choses ne changent pas, car s'il est une industrie qui n'est pas perturbée par la COVID-19, c'est bien la cybercriminalité.

La fréquence des attaques est élevée et elles sont toujours plus élaborées, ce qui rend les violations inévitables.

Plus des quatre cinquièmes (81 %) des 279 répondants disent que le nombre d'attaques a augmenté au cours de l'année passée et, parmi ces derniers, 96 % pointent du doigt l'augmentation soudaine du nombre de télétravailleurs. 89 % pensent que les attaques sont de plus en plus sophistiquées.

Le résultat ? Le nombre de violations est significatif, car les répondants qui ont subi une cyberattaque font état de **2,18 violations en moyenne par an**. Et il ne s'agit pas d'incidents mineurs, car dans huit cas sur dix, la violation est un incident grave

Les RSSI ne peuvent pas voir dans les coins

Les volumes de cyberattaques ont augmenté, mais l'application à marche forcée du télétravail fait que certaines entreprises n'ont pas assez de recul. Le comportement erratique des collaborateurs, les appareils personnels et les réseaux domestiques réduisent la visibilité, ce qui crée des angles morts et des zones d'ombre où les attaques peuvent passer inaperçues. Par conséquent :

96 %

estiment que l'augmentation des attaques résulte du télétravail

2,18

violations en moyenne par organisation et par an

82 %

disent avoir constaté une violation substantielle

nécessitant un signalement aux régulateurs ou l'intervention d'une équipe spécialisée dans les contre-mesures.

De toute évidence, les équipes de sécurité sont sous pression et il n'y a pas de place pour la complaisance :

74 % des RSSI français interrogés craignent que leur organisation subisse une violation significative au cours de l'année à venir.

Les Rançongiciels, les Technologies de Sécurité Périmées, et les Applications Tierces Constituent les Principales Sources de Violations

Lorsque nous avons demandé quelle était la cause de ces violations, les trois vecteurs les plus cités mettent en avant les menaces externes et les vulnérabilités internes. Les rançongiciels sont les plus répandus et à l'origine de 21 % des violations, suivis de près par les applications tierces, puis par les technologies de sécurité obsolètes.

Résurgence des rançongiciels

Les rançongiciels redeviennent l'une des principales causes de violations, car les attaquants lancent des campagnes sophistiquées et lucratives à plusieurs niveaux.

21 %

de toutes les violations sont imputables aux rançongiciels

Le basculement rapide vers le télétravail en tout lieu a mis en danger les organisations qui avaient négligé leur hygiène de sécurité et n'avaient pas mis en œuvre des mesures d'authentification multifacteur, à un moment où l'entreprise étendue est mise sous pression par des tiers créant des risques significatifs de violation.

En plus de ces menaces, la montée en puissance rapide des rançongiciels génère une tension difficile à gérer. Les campagnes se déroulent en plusieurs phases (pénétration, implantation, vol de données et extorsion) qui font monter la pression et exploitent les perturbations générées par le télétravail. Dans la plupart des attaques par rançongiciels, les e-mails restent le principal vecteur d'entrée.

Appréhension autour du développement et de la consommation des applications

Les applications tierces constituent une cause répandue de violations selon les RSSI que nous avons contactés. 77,5 % d'entre eux soulignent en effet qu'elles constituent un facteur d'innovation. Par conséquent, il n'est pas surprenant que les équipes de sécurité tentent d'affiner leur approche de la consommation et du développement de ces applications.

Près de 84 % des répondants concèdent[1] qu'ils ont besoin d'une meilleure visibilité des données et des applications pour prévenir les attaques, et un nombre équivalent estime que le renforcement de la sécurité contextuelle est nécessaire pour mesurer le niveau de sécurité tout au long du cycle de vie de l'application. Près de quatre répondants sur cinq reconnaissent l'impact de la pandémie de COVID-19 et pensent qu'ils doivent aborder la sécurité sous un autre angle, en raison de l'augmentation de la surface d'attaque.

Les applications sont également en tête de liste des points les plus vulnérables sur le parcours des données, mais cette liste ne s'arrête pas là.

Les charges de travail sont en forte progression en tant que source de vulnérabilité perçue.

[1] Regroupe les options Tout à fait d'accord et Plutôt d'accord.

14 % des répondants indiquent que les charges de travail constituent le point le plus exposé aux violations dans le parcours des données de leur organisation tout en relevant que cela n'était pas le cas il y a 12 mois.

En outre, 5 % précisent qu'il s'agit du point le plus vulnérable depuis plus de 12 mois. Les équipes reconnaissent que les anti-virus traditionnels ne permettent pas de sécuriser les charges de travail du serveur et que les erreurs de configurations présentent un risque significatif de violations. Cela résulte souvent du profil différent des équipes chargées de la sécurité et de l'infrastructure : les équipes responsables de la sécurité ne savent pas comment les charges de travail doivent se comporter, tandis que les équipes responsables de l'infrastructure ne disposent pas de l'expérience nécessaire pour repérer les comportements liés aux attaques. Cette année nous pensons que les organisations tenteront de remédier à cela et de renforcer les défenses des charges de travail dans le Cloud.

Concernant le Cloud, notre étude a constaté qu'un mouvement inexorable est en cours. Presque tous les RSSI que nous avons interrogés appliquent une stratégie de sécurité Cloud-first ou prévoient de l'appliquer très rapidement. Il s'agit d'un changement considérable qui démontre que les organisations accélèrent le développement de leur feuille de route de sécurité cloud en réponse aux défis de la pandémie. Dans certains cas, ce mouvement est déjà en cours, mais les entreprises lui donnent un sérieux coup d'accélérateur, car un univers Cloud-first appelle une sécurité Cloud-first à toute épreuve.

Nous espérons que vous trouverez notre quatrième rapport sur l'état des menaces en France révélateur et instructif.

Principaux Constats

La fréquence des attaques et les risques de violation restent élevés.

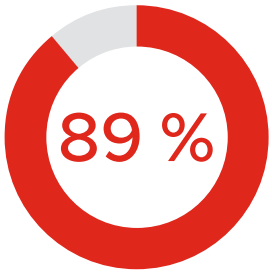
La fréquence des attaques est élevée et celles-ci sont toujours plus sophistiquées, ce qui rend les violations inévitables.

81 %

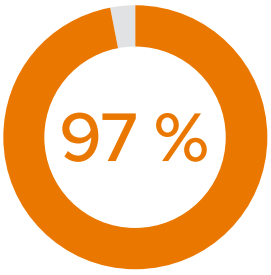
des répondants indiquent que les volumes d'attaque ont augmenté au cours des douze derniers mois, avec une moyenne de 43 % pour toutes les organisations concernées.

96 %

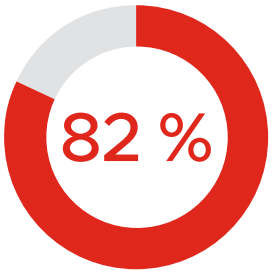
de ceux ayant subi une cyberattaque pensent que leur fréquence a augmenté à cause de l'extension du télétravail.



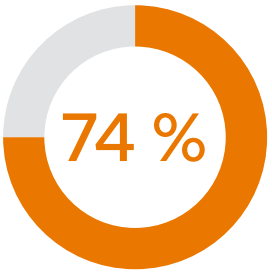
de ceux ayant subi une cyberattaque disent que ces attaques sont plus sophistiquées.



ont subi au moins une violation au cours des douze derniers mois et dans les organisations touchées, il y a eu en moyenne 2,18 violations pendant cette période.



indiquent que les violations subies étaient significatives.



craignent une violation significative au cours des douze mois à venir.

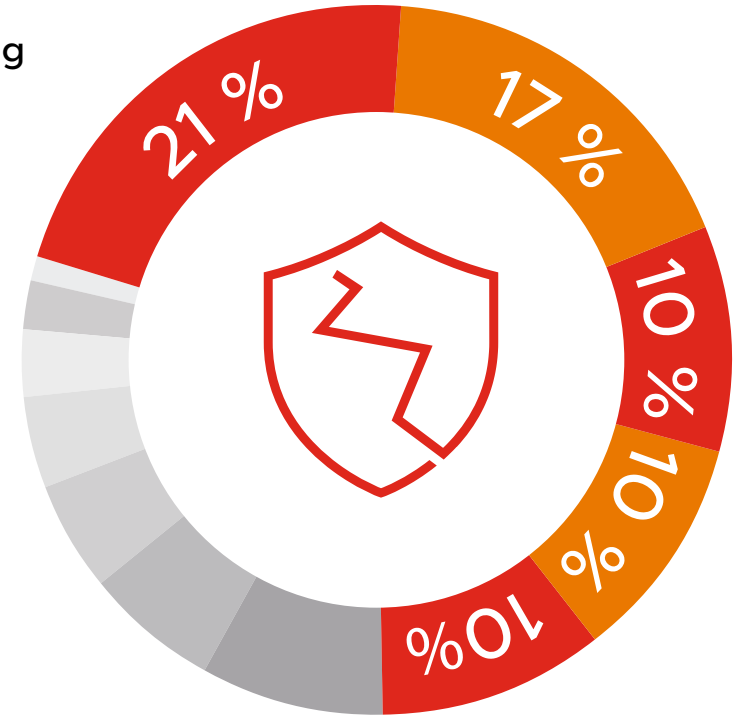
Les rançongiciels, les applications tierces, une sécurité obsolète et les charges de travail constituent les principales préoccupations des RSSI

Les principaux vecteurs de violations mettent en avant les menaces externes et les faiblesses internes.

Principaux vecteurs de cyberattaque :

Les applications tierces se classent deuxième avec 17 %

Les rançongiciels viennent au premier rang avec 21 %



Une technologie obsolète vient en troisième avec 10 %

Les attaques d'applications Web (10 %) et l'hameçonnage (10 %) complètent le lot des cinq principales causes.

Les applications et les charges de travail sont également en tête de liste des points les plus vulnérables sur le parcours des données, mais cette liste ne s'arrête pas là.

L'extension des surfaces d'attaques pousse les RSSI à repenser leur approche traditionnelle de la sécurité

La bonne nouvelle est que les changements fondamentaux de sécurité sont bien compris à une époque numérique ultra-connectée et propice au télétravail :

79 % des répondants conviennent qu'ils doivent renouveler leur approche de la sécurité, car la surface d'attaque est plus étendue.

83 % conviennent qu'ils doivent renforcer la sécurité contextuelle pour pouvoir suivre les données tout au long de leur cycle de vie.

84 % conviennent qu'ils ont besoin d'une meilleure visibilité des données et des applications pour prévenir les attaques.

La simplification, la consolidation et l'adoption de la stratégie Cloud-first font partie des plans pour 2021.

Les RSSI interrogés semblent s'être lancés sur la voie de la consolidation technologique et de l'adoption d'une approche de sécurité plus intrinsèque, tandis que 42 % disent élargir leur budget de sécurité pour atteindre cet objectif.

43 % ont mis à jour leur technologie de sécurité pour limiter les risques.

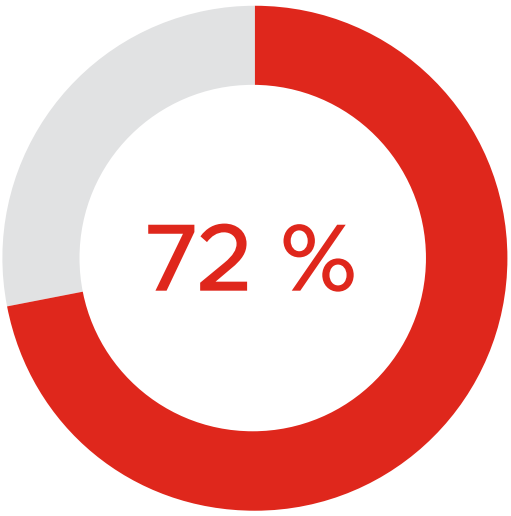
38 % renforcent la sécurité de leur infrastructure et des applications, et réduisent le nombre de solutions spécialisées.

38 % ont réactualisé leur politique de sécurité et leur approche pour réduire les risques.

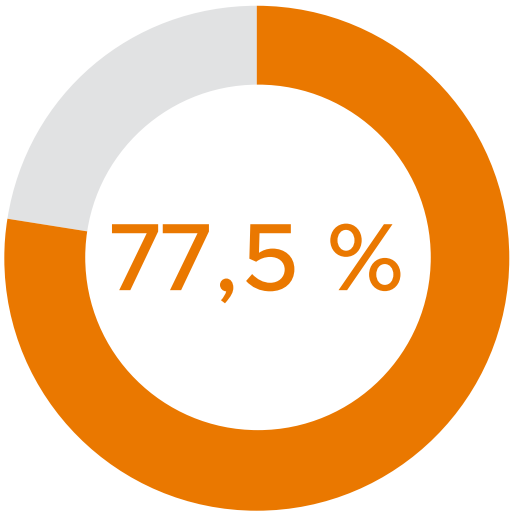
99 % ont adopté une stratégie de sécurité Cloud-first ou prévoient de le faire.

L'IA est le nouvel horizon de l'innovation, mais les doutes sur sa sécurité freinent-ils la progression ?

Le nouvel horizon de l'innovation au service des entreprises est l'intelligence artificielle, car les entreprises recherchent une nouvelle approche pour mettre en place des services clients et des expériences numériques plus compétitifs.

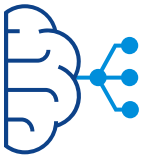


Et pourtant, 72 % des répondants conviennent que les problèmes de sécurité ralentissent l'adoption d'applications basées sur l'IA/l'apprentissage machine pour améliorer ces services.



Et 77,5 % des répondants conviennent que leur capacité à innover dépend du développement et de la mise à disposition d'applications de façon plus sécurisée.

L'IA est le nouvel horizon de l'innovation, mais les doutes sur sa sécurité freinent-ils la progression ?



La plupart des répondants s'inquiètent du risque de ne pas pouvoir saisir l'opportunité numérique.

71 % conviennent que le marché des solutions de sécurité est trop complexe pour les pousser à changer leur politique de sécurité, même s'ils savent que la sécurité informatique en place ne fonctionne pas.

80 % conviennent que leur équipe de direction/d'administration est de plus en plus inquiète lorsqu'ils déploient de nouvelles applications, en raison du risque croissant de menaces et de dommages résultant des violations de données/attaques.

76 % conviennent qu'ils aimeraient utiliser davantage l'IA et l'autoapprentissage dans leurs applications pour améliorer la sécurité et les services.

84 % conviennent qu'ils ont besoin d'une meilleure visibilité des données et des applications pour prévenir les attaques.

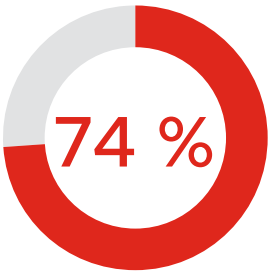
Sécurisation de la marque et de la réputation – Un changement est-il urgent ?

La marque et la réputation restent le Saint-Graal des entreprises, et cette quête n'a rien de facile. Cependant, l'impact des violations de la sécurité sur la réputation est bien plus violent que l'impact financier.

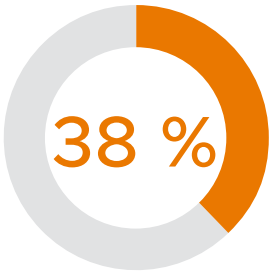
82,5 % des répondants ont dû faire un signalement aux régulateurs, ou recruter un cabinet spécialisé dans la réponse aux incidents, pour remédier à l'atteinte à la réputation résultant de violations significatives.

82 % des répondants ont dû faire un signalement aux régulateurs, ou recruter un cabinet spécialisé dans la réponse aux incidents, pour remédier à l'atteinte à la réputation résultant de violations significatives.

La prise de conscience de ces violations de sécurité est mitigée et le changement n'est pas encore perçu comme urgent malgré la dégradation du contexte des menaces.



craignent une nouvelle violation significative au cours de l'année à venir.



ont réactualisé leur politique de sécurité et leur approche pour atténuer les risques.

Résultats Complets de L'étude

Avez-vous constaté une augmentation des cyberattaques visant votre entreprise au cours des 12 derniers mois ? Le cas échéant, dans quelle proportion ?

81 % des RSSI interrogés disent avoir subi une augmentation des cyberattaques visant leur organisation au cours des 12 derniers mois, et l'augmentation moyenne était à hauteur de 43 %. 85,5 % des répondants du secteur des services financiers ont pour leur part constaté une augmentation moyenne des attaques de 55 %.

Le secteur de la santé est en meilleure posture avec une augmentation moyenne du volume de 32 %.

La taille est importante concernant le volume d'attaques. Les organisations de plus petite taille subissent un nombre moyen d'attaques inférieur à celui des plus grandes.

Celles qui ont entre 31 et 40 personnes dans leur équipe informatique signalent une augmentation moyenne du volume d'attaque de 52 %, à rapprocher de l'augmentation moyenne qui est de 43 %.

Le nombre de cyberattaques type sur votre système a-t-il globalement changé du fait d'un nombre accru de collaborateurs travaillant à domicile du fait de la pandémie de COVID-19 ?

96 % des répondants qui ont subi des cyberattaques disent qu'ils ont constaté une hausse de leur fréquence en raison de l'extension du télétravail.

Pratiquement tous les répondants (97,5 %) qui travaillent pour une administration ont constaté une augmentation des attaques en relation avec le télétravail, avec une croissance moyenne de 49 % et, plus surprenant, si 94 % des personnes travaillant dans les services financiers ont bien constaté une augmentation, celle-ci est beaucoup plus basse à 29 %.

Les organisations ayant une équipe de 31 à 40 personnes ont constaté la plus forte augmentation moyenne des attaques, avec 42 %.

Les cyberattaques visant votre entreprise sont-elles devenues plus sophistiquées ou plus simples au cours des 12 derniers mois ?

En termes de degré d'élaboration des attaques, 89 % des RSSI interrogés qui ont subi une cyberattaque jugent les attaques plus sophistiquées. Cette augmentation est significative, car seulement un tiers d'entre eux portait un jugement similaire dans le rapport de juin 2020.

> 89 % des RSSI interrogés qui ont subi une cyberattaque jugent les attaques plus sophistiquées.

Plus de la moitié (58 %) des personnes qui ont subi une cyberattaque disent que les attaques auxquelles elles doivent faire face sont significativement ou modérément plus sophistiquées, ce qui laisse entendre qu'il y a un noyau dur d'acteurs malveillants qui continue de développer et d'affûter les techniques d'attaque.

Les preuves disponibles semblent indiquer que les services financiers sont particulièrement visés. 91 % des répondants de ce secteur signalent des attaques plus sophistiquées et 64 % estiment que les attaques sont devenues modérément ou significativement plus complexes. En revanche, les administrations sont moins affectées par les attaques de type évolutif. Seulement 27,5 % des personnes interrogées dans ce secteur relèvent des attaques modérément ou significativement plus sophistiquées.

Les attaquants réservent leurs attaques les plus sophistiquées aux organisations de plus grande taille, car celles-ci relèvent un pourcentage plus important d'attaques significativement plus sophistiquées. Cela reflète le fait que plus l'entreprise est grande, plus ses données sont volumineuses et précieuses, ce qui offre plus d'opportunités aux cybercriminels de monétiser leur travail.

Quel est le type d'attaque le plus virulent (plus fréquent) subi par votre entreprise au cours des 12 derniers mois ?

Le contexte français des attaques est divers, avec peu de personnes faisant l'expérience de la même combinaison de types d'attaque et relevant un type d'attaque dominant. Cela souligne les défis auxquels les RSSI français sont confrontés, car ils doivent mettre en place des mesures stratégiques et tactiques face à un mélange incroyablement divers de vecteurs et de techniques d'attaque.

Les rançongiciels sont en tête de liste, avec 13 % des répondants ayant subi une cyberattaque les constatant le plus souvent. Cependant, les applications tierces et les logiciels malveillants génériques (commodity malware) sont juste derrière comme principal type d'attaque pour 12 % et 11 % des répondants respectivement.

Les attaques ciblées (custom malware) et exploitant les vulnérabilités de la technologie 5G représentent respectivement 9 % pour tous ceux qui ont subi une cyberattaque. Dans le rapport de juin 2020, pas moins de 71 % des répondants indiquent que Google Drive™ (pour les attaques basées sur le Cloud) était le type d'attaque le plus prolifique.

Les rançongiciels visent de façon disproportionnée les administrations, où 37,5 % des personnes interrogées les jugent les plus fréquentes. En revanche, les applications tierces posent plus de problèmes dans le secteur de la santé, où elles affectent 30 % des organisations.

Combien de fois votre entreprise a-t-elle été touchée par une cyberattaque au cours des 12 derniers mois ?

96 % des organisations consultées ont subi une violation au cours de l'année passée.

La quasi-totalité des RSSI interrogés disent que leur organisation a été victime d'une cyberattaque au cours de l'année passée (96 %). Ce chiffre est en baisse par rapport aux 99 % qui ont signalé une violation en 2020.

De même, le nombre moyen de violations subies par chaque organisation est passé de 3,7, en juin 2020, à 2,18 dans le présent rapport. Plus d'un quart (28 %) des répondants indiquent que leur organisation a subi entre deux et cinq attaques.

Le secteur de l'agro-alimentaire a subi le plus grand nombre d'attaques, soit 2,86, tandis que les administrations n'en relèvent que 1,55. Les autres secteurs signalant une fréquence supérieure à la moyenne sont le commerce de détail (2,53), la fabrication et l'ingénierie (2,45), et la distribution d'énergie et d'eau (2,50).

La fréquence des attaques est plus importante dans les organisations de taille intermédiaire comptant entre 2 001 et 5 000 salariés, avec une moyenne de 3,86.

Quelle a été la principale cause de ces violations ?

Pour 21 % des RSSI ayant subi une cyberattaque, les rançongiciels sont les principaux coupables. Pour 17 % d'entre eux, la violation est due à une application tierce, tandis que la découverte désagréable que leur technologie de sécurité est obsolète représente 10 % des violations. Cette situation est aggravée par les attaques d'applications Web (10 %), le hameçonnage (10 %) et les processus qui se révèlent moins solides qu'ils le devraient (10 %). Les contraintes exercées par le basculement brutal vers le télétravail fragilisent clairement les zones où les politiques et la technologie n'ont pas pu suivre l'évolution de l'environnement.

Plus loin dans la liste, mais toujours significatif, 8 % des attaques sont attribuables aux vulnérabilités du système d'exploitation. Toutefois, l'organisation n'est qu'en partie responsable, avec 7,5 % des violations résultant d'attaques par island hopping (piratage d'une entité tierce avant de remonter vers la cible finale), et 3 % de plus provenant de la chaîne logistique. Ces résultats illustrent de façon éloquente la diversité des sources de violations et le fait que les RSSI français doivent intervenir sur plusieurs fronts.

Les rançongiciels sont particulièrement virulents dans les administrations, où la fréquence de ce type d'attaque est au plus haut et responsable de plus de la moitié (52,5 %) des violations. C'est également un problème dans le secteur de la santé, où il a été identifié par près d'un tiers (30 %) des répondants comme une cause première. Les services financiers sont particulièrement vulnérables aux attaques par les applications Web et les processus ne sont pas aussi robustes qu'ils le devraient, car ceux-ci sont à l'origine de 15 % des violations dans chaque cas.

Les organisations employant de 1 001 à 2 000 personnes sont particulièrement vulnérables aux violations liées aux rançongiciels, avec 32,5 % des violations se produisant de cette manière. Et celles dont l'équipe IT compte de 31 à 40 personnes ont subi un fort pourcentage de violations liées à des rançongiciels (29 %).

Quel pourcentage des violations par une cyberattaque au cours des 12 derniers mois pensez-vous être une violation significative (à savoir une violation entraînant un signalement aux régulateurs ou un appel à une équipe spécialisée dans les contre-mesures pour la restauration, etc.) ?

Les violations ont des conséquences sérieuses. La plupart des répondants (82 %) ont dû faire un signalement aux régulateurs ou recruter un cabinet spécialisé dans la réponse aux incidents pour remédier aux violations.

82 % des organisations ont constaté une violation substantielle.

Plus de la moitié (53 %) des répondants qui ont subi une cyberattaque indiquent que 21 à 30 % d'entre elles constituent des violations significatives, tandis que 16 % pensent que 31 à 40 % des violations sont significatives.

Dans le secteur des services financiers, les répondants ont la moyenne la plus élevée, 27,69 %, dont 24 % affirmant que 31 à 40 % des failles étaient significatives, et 12 % admettent que 41 à 50 % des violations ont dû être signalées au régulateur.

Quelles ont été les conséquences de ces violations pour votre entreprise sur le plan financier et de sa réputation ?

Un peu moins du tiers (32 %) des répondants qui ont subi une cyberattaque indiquent que les violations de données affectant leur organisation ont eu un impact financier négatif. Cela est supérieur à la moyenne générale de 24 % et bien supérieur aux 21,5 % qui reconnaissaient avoir subi un impact financier dans l'étude de juin 2020.

Le pourcentage d'organisations déclarant n'avoir déploré aucun impact financier suite à une violation s'est également réduit, de 78,5 % en juin 2020 à 57 % dans ce rapport.

Fait intéressant, 24 % des entreprises de services financiers déclarent avoir subi un impact financier considérable, ce qui est supérieur à tout autre secteur. Les administrations sont les moins concernées par les impacts financiers, car 85 % d'entre elles disent ne pas avoir été touchées.

De manière globale, les répercussions sur la réputation de la marque sont plus graves. 82,5 % des répondants ayant subi une cyberattaque affirment que leur marque a subi un impact négatif suite à une violation de données, contre 75 % dans le rapport de juin 2020. 17 % estiment que les dommages sont sérieux.

Seuls 16 % déclarent qu'il n'y a pas eu de perte de réputation suite à une violation.

Un quart (25 %) des administrations indiquent ne pas avoir subi un impact négatif.

Dans quelle mesure craignez-vous les violations significatives qui risquent de toucher votre organisation au cours des 12 prochains mois ?

Le risque de violations significatives au cours de l'année à venir est particulièrement anxiogène. Près des trois-quarts (74 %) des répondants ont peur ou très peur d'une violation dans leur entreprise.

Le secteur des services financiers est particulièrement sur ses gardes, avec 88 % des répondants déclarant qu'ils craignent une violation. Moins de la moitié (38 %) des répondants dans les administrations publiques craint une violation.

Quelles mesures avez-vous prises (contre le risque de violations), le cas échéant ?

Concernant les plans de réduction du risque de violation, les répondants privilégient la simplification et la consolidation des solutions de sécurité, ainsi que la mise en place d'une sécurité intrinsèque. Les autres facteurs importants sont l'actualisation des technologies et des politiques, ainsi que la mobilisation d'un budget pour ce problème.

38 % des répondants prévoient **d'intégrer davantage la sécurité dans leur infrastructure et les applications, et de réduire le nombre de solutions spécialisées.** Ce chiffre monte à 54,5 % dans le secteur de la fabrication.

43 % déclarent avoir **adapté la sécurité pour atténuer les risques**, en utilisant les ressources existantes. En particulier, les organisations de santé sont plus enclines à adapter la technologie (59 %). 43 % ont **mis à jour leur technologie de sécurité pour réduire les risques.**

38 % déclarent avoir **réactualisé leur politique de sécurité et leur approche pour réduire les risques** – une tactique importante étant donné les changements significatifs du paysage de sécurité au cours de l'année écoulée. 53 % des entreprises de l'agro-alimentaire, 54,5 % des entreprises de fabrication et d'ingénierie ont adopté cette approche.

38 % des répondants prévoient d'intégrer davantage la sécurité dans leur infrastructure et les applications, et de réduire le nombre de solutions spécialisées.

42 % ont **augmenté le budget de sécurité**. Les secteurs de l'administration publique (46 %), de la santé (41 %) et de la vente au détail (53 %) prévoient tous d'augmenter leur budget de sécurité.

Il est intéressant de noter que les organisations pensent que la stratégie est plus efficace que de simplement mettre plus d'argent ; l'augmentation du budget venant en troisième position sur la liste des priorités, derrière l'actualisation et l'adaptation de la technologie de sécurité.

Dans quelle mesure êtes-vous d'accord ou non avec les déclarations suivantes concernant le développement et la consommation des applications dans votre organisation ?

Concernant les nouvelles approches des défis de sécurité relatifs au développement et à la consommation d'applications dans leur organisation, les répondants nous ont beaucoup appris sur les problèmes auxquels ils étaient confrontés.

> 84 % ont besoin d'une meilleure visibilité des données et des applications

La visibilité est une préoccupation majeure. 84 % conviennent qu'ils ont **besoin d'une meilleure visibilité sur les données et les applications pour prévenir les attaques**. Ce chiffre atteint 86 % dans le secteur de la santé avec 47 % des personnes qui sont tout à fait d'accord.

> 83 % conviennent qu'ils doivent renforcer la sécurité contextuelle pour suivre les données tout au long de leur cycle de vie.

79 % des répondants en France conviennent que les changements du paysage d'attaque dus à la pandémie de COVID-19 les poussent à repenser la sécurité et reconnaissent qu'ils **doivent envisager la sécurité sous un autre angle, car la surface d'attaque est plus étendue**.

83 % conviennent qu'ils doivent r**enforcer la sécurité contextuelle pour pouvoir suivre les données tout au long de leur cycle de vie**. Cela est caractéristique de la majorité des environnements qui sont axés sur les menaces et réactifs par nature.

Les responsables informatiques savent que les environnements dynamiques impliquent une approche orientée sur le contexte.

Les RSSI interrogés en France n'ont aucune illusion sur le caractère essentiel de la sécurité des applications pour leur activité. 77,5 % conviennent que la capacité d'innovation de l'entreprise dépend de la **capacité des éditeurs à construire, gérer et distribuer des applications de façon plus sécurisée**.

77,5 % des répondants **se sentent prêts à déployer de nouvelles applications, parce qu'ils savent qu'elles seront sécurisées**.

L'introduction de l'IA dans le développement d'applications sécurisées produit des réactions très contrastées. 72 % conviennent que les **problèmes de sécurité ralentissent l'adoption d'applications basées sur l'IA etl'autoapprentissage pour améliorer ces services**, mais 76 % affirment aussi qu'ils **aimeraient pouvoir recourir davantage à l'IA et l'autoapprentissage dans les applications pour améliorer la sécurité et les services**.

Près des trois quarts des répondants (71 %) estiment que le **marché des solutions de sécurité est trop complexe pour les pousser à changer leur politique de sécurité, même s'ils savent que la sécurité informatique en place ne fonctionne pas**, ce qui laisse entendre que les éditeurs ont du travail devant eux pour simplifier et unifier leur proposition.

Enfin, 80 % reconnaissent que la sécurité des applications avait un écho dans les conseils d'administration, et que leur **équipe de direction/d'administration est de plus en plus inquiète lorsque de nouvelles applications sont commercialisées, en raison du risque croissant de menaces et de dommages résultant des violations de données/attaques**.

Selon vous, quel est le point le plus vulnérable du parcours des données dans votre infrastructure de sécurité, et cela a-t-il changé au cours des 12 derniers mois ?

Les applications sont désignées comme le maillon faible du parcours de données et il est clair que ce problème n'est pas nouveau. Mais plus intéressant encore, les charges de travail sont de plus en plus perçues comme une source de vulnérabilité. Nous devrions voir les organisations porter davantage d'attention à la résolution de ce risque au cours de l'année à venir.

48 % Application

Pour 28 % le sont maintenant et l'étaient déjà il y a 12 mois, 19,7 % le sont maintenant, mais ne l'étaient pas il y a 12 mois

19 % Charges de travail

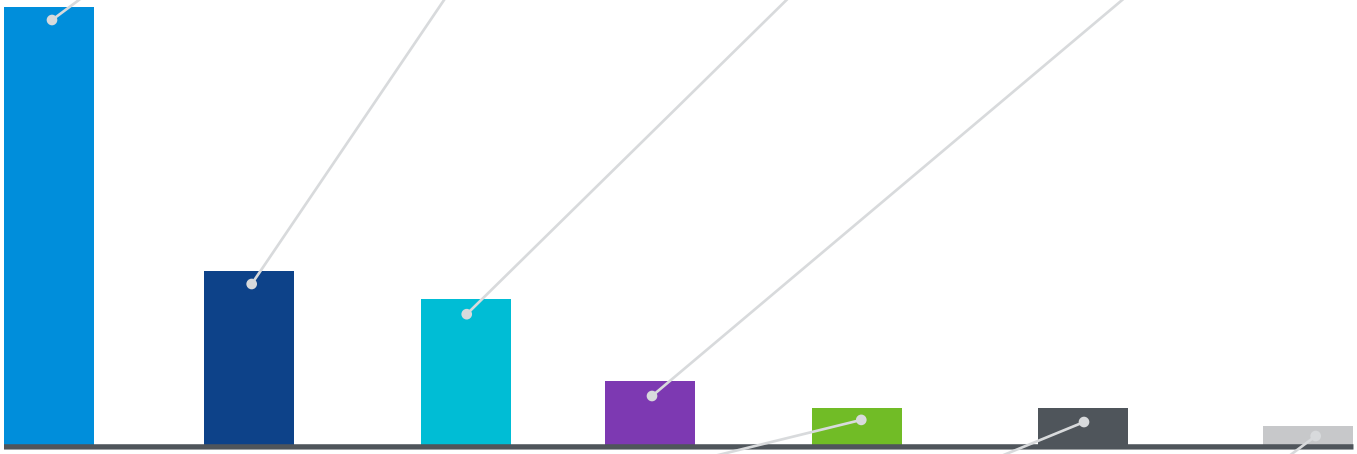
Pour 4,7 % le sont maintenant et l'étaient déjà il y a 12 mois, 14,3 % le sont maintenant, mais ne l'étaient pas il y a 12 mois

16 % Réseau

Pour 10,8 % le sont maintenant et l'étaient déjà il y a 12 mois, pour 5 % le sont maintenant, mais ne l'étaient pas il y a 12 mois

7 % Terminaux

Pour 5 % le sont maintenant et l'étaient déjà il y a 12 mois, pour 1,8 % l'étaient maintenant, mais ne l'étaient pas il y a 12 mois



4 % Périphérie

Pour 3,2 % l'est maintenant et l'était déjà il y a 12 mois, pour 0,7 % l'est maintenant, mais ne l'était pas il y a 12 mois

4 % Cloud

Pour 3,2 % l'est maintenant et l'était déjà il y a 12 mois, pour 0,7 % l'est maintenant, mais ne l'était pas il y a 12 mois

2 % Conteneurs

Pour 1,4 % le sont maintenant et l'étaient déjà il y a 12 mois, pour 0,4 % l'étaient maintenant, mais ne l'étaient pas il y a 12 mois

Comment les organisations ont-elles fait face aux défis du passage au télétravail ?

Nous avons demandé aux RSSI interrogés d'évaluer leur succès lors du passage au télétravail et si une approche axée sur la sécurité aurait pu les aider à effectuer une meilleure transition.

76 % confirment qu'ils sont parvenus à rendre leur personnel opérationnel à distance et que la sécurité n'a pas été un obstacle. Cela témoigne du travail des équipes de sécurité qui sont plus que jamais au cœur des opérations. Les répondants travaillant dans la santé et l'administration publique ont eu de bons résultats, avec 65 % et 64 % respectivement déclarant que la sécurité n'a pas été un obstacle lors du passage au télétravail. En revanche, les RSSI des services financiers ont fait l'expérience de difficultés, avec seulement 34 % tout à fait d'accord et 14,5 % pas d'accord avec le fait qu'ils sont parvenus à rendre le personnel opérationnel sans problème.

Les répondants savent qu'il reste toujours des possibilités d'amélioration, avec 78 % convenant qu'une approche axée sur la sécurité aurait augmenté leur capacité à permettre au personnel de travailler depuis un autre endroit sans perte de productivité. L'enquête précédente portant sur VMware faisait un constat similaire et avait identifié l'incapacité à mettre en place l'authentification multifacteur comme le principal problème auquel les équipes IT sont confrontés lors du passage au télétravail. Depuis, il y a eu une prise de conscience au plus haut niveau et il devrait être plus facile pour les RSSI de s'assurer du soutien du conseil d'administration pour une approche axée sur la sécurité.

Avez-vous adopté une stratégie de sécurité Cloud-first ou prévoyez-vous de le faire ?

Les répondants ont quasi unanimement (99 %) déclaré qu'ils prévoyaient d'adopter une stratégie de sécurité Cloud-first immédiatement ou dans un futur proche.

> 99 % utilisent déjà ou prévoient d'utiliser une approche cloud-first pour protéger l'organisation.

54 % du total disent qu'ils adoptent une approche Cloud-first depuis plus d'un an contre 37 % depuis moins de 12 mois. D'autre part, 7 % prévoient d'adopter la stratégie Cloud-first au cours de l'année à venir ou par la suite.

Le niveau de maturité de la stratégie Cloud-first est élevé dans les services financiers, où 57% des entreprises interrogées ont une stratégie Cloud-first depuis plus de 12 mois et 35,5 % depuis moins de 12 mois. 66 % des personnes travaillant dans l'administration publique ont une stratégie de sécurité Cloud-first depuis plus d'un an.

Enseignements Clés et Actions

Notre quatrième rapport sur l'état des menaces en France révèle que les professionnels senior de la cybersécurité et les organisations qu'ils servent continuent de faire face à de gros volumes de menaces sophistiquées. Cela est exacerbé par la forte dispersion du personnel imposée par le télétravail et même si la plupart des organisations ont bien négocié ce virage, les RSSI reconnaissent qu'une approche axée sur la sécurité aurait simplifié la transition.

Il ne fait aucun doute que la pandémie de COVID-19 a transformé l'environnement de la cybersécurité et continuera d'influer sur sa stratégie de sécurité. Pour sa part, l'industrie de la cybersécurité doit se concentrer sur des solutions réduisant la complexité opérationnelle tout en assurant une protection robuste des environnements de travail distribués qui finira par s'imposer comme le nouvel état par défaut dans la plupart des organisations.

L'analyse des réponses révèle des points importants à prendre en compte en matière de cybersécurité au cours de l'année à venir.

Priorité à l'amélioration de la visibilité

Les organisations ont un problème de visibilité résultant du passage rapide au télétravail. La véritable échelle des attaques est difficile à discerner, car les défenseurs ne peuvent pas voir dans les coins où les appareils mobiles personnels et les réseaux domestiques ont été greffés dans l'écosystème de l'entreprise. Ajoutez à cela le défi de la surveillance des applications tierces et des éditeurs, et le nombre d'angles morts prolifère.

Dit plus simplement, les défenseurs ne connaissent pas l'étendue de ce qu'ils ignorent, ce qui expose les entreprises aux risques. Cette connaissance limitée du contexte de risque place les défenseurs dans une situation désavantageuse pour réduire la surface d'attaque. Les organisations doivent prioriser la visibilité de tous les terminaux et de toutes les charges de travail pour sécuriser l'environnement de télétravail. Des renseignements situationnels fiables précisant le contexte des menaces aideront les défenseurs à établir des priorités et gérer le risque avec assurance.

Gestion de la résurgence des rançongiciels

Les cyberattaques sont toujours plus sophistiquées et les rançongiciels ne font pas exception. Les attaquants parviennent à s'introduire sur les réseaux sans être détectés, exfiltrent les données et créent des accès dérobés avant de lancer des

demandes de rançon et/ou de monétiser directement les données volées. Afin de ne pas subir des attaques répétées, les organisations doivent mettre en place une protection avancée contre les rançongiciels avec des contre-mesures efficaces, capables de détecter les présences hostiles dans leur environnement.

Poursuivre l'effort d'actualisation des techniques de sécurité et de renforcement des processus

Les mesures de sécurité obsolètes et les maillons faibles des processus demeurent un risque significatif pour les organisations, et le passage au télétravail l'aggrave. Alors que nous émergeons de la phase de réponse immédiate et que les conditions futures deviennent discernables, il est impératif que les organisations identifient les changements essentiels à apporter aux processus et les technologies nécessaires pour accompagner le télétravail et le travail hybride en toute sécurité et atténuer les risques.

Assimiler la sécurité à un service distribué

Il fut un temps où les équipes de sécurité sécurisaient les ordinateurs de bureau de salariés travaillant en campus et qui se connectaient à des applications métier s'exécutant sur des serveurs dans un Data Center appartenant à l'entreprise. Le monde est beaucoup plus compliqué aujourd'hui avec des télétravailleurs qui se connectent à des applications s'exécutant sur une infrastructure qui peut être ou ne pas être gérée, possédée ou contrôlée par l'entreprise. Avec autant de nouvelles surfaces et de types différents d'environnement à défendre, la sécurité ne peut plus être assurée sous forme d'une litanie de produits spécialisés et de goulots d'étranglement du réseau. Au contraire, les contrôles des terminaux et des réseaux doivent être assurés en tant que service distribué. Cela signifie que la sécurité doit suivre les ressources à protéger, quel que soit le type de votre environnement.

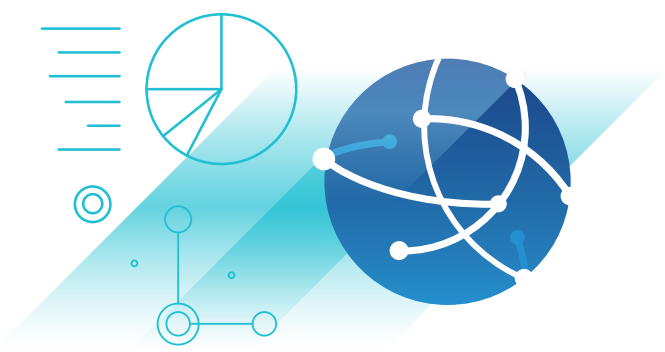
Adopter une approche intrinsèque de la sécurité Cloud-first

Le principal défi identifié par notre enquête est l'adoption d'une stratégie de sécurité Cloud-first. La magnitude du basculement qui s'est produit en un laps de temps si court est sans précédent ; très peu de RSSI décrivaient leur stratégie de sécurité comme Cloud-first avant 2020. C'est le résultat logique des organisations qui ont dû faire face aux pratiques de travail soudainement distribuées sous la pression de la pandémie.

Mais l'adoption du Cloud n'est pas une panacée de la sécurité, car tous les Clouds ne sont pas équivalents, et des contrôles doivent être validés par les organisations qui les consomment, car si des agresseurs veulent mener une attaque à grande échelle, le Cloud est le meilleur endroit pour le faire. Alors que la dynamique de ce changement s'accélère, les investissements dans la sécurisation du Cloud public vont devenir essentiels. Lorsque vous opérez une transition vers un Cloud public, vous pénétrez dans une zone très dangereuse où la sécurité ne dépend plus de vos seules actions, mais aussi de celles de vos voisins. Vous avez toujours la possibilité de sécuriser vos propres ressources, mais vous n'avez aucun contrôle sur ceux qui partagent cet environnement avec vous. Les organisations doivent donner la priorité à la sécurisation des charges de travail en tout point du cycle de vie de sécurité, car le grand mouvement de passage au le Cloud continue.

Enfin, l'édition 2021 du rapport sur l'état des menaces en France donne l'image d'une industrie déterminée à s'appuyer sur les succès de l'année passée et à répondre à l'évolution de l'environnement des menaces. Les RSSI ont une idée précise de la direction qu'ils souhaitent suivre et des outils qui leur permettront de garder une longueur d'avance sur les attaquants.

Méthodologie



VMware a commandité une étude, réalisée par un cabinet de recherche indépendant, Opinion Matters, en décembre 2020. 279 DSI, directeurs techniques et directeurs de la sécurité travaillant en France dans les secteurs suivants ont été interrogés : finance, santé, administration centrale et locale, commerce de détail, fabrication et ingénierie, agroalimentaire, distribution d'énergie et d'eau, services professionnels, et médias et divertissements. Il s'agit du quatrième rapport sur l'état des menaces en France, qui fait suite à l'étude précédente, réalisée en juin 2020. Ce rapport s'inscrit dans un projet plus vaste couvrant 14 pays : Allemagne, Australie, Arabie saoudite, Canada, Espagne, États-Unis, France, Italie, Japon, Moyen-Orient, Pays-Bas, Pays scandinaves, Royaume-Uni et Singapour.

À propos de VMware

Partout dans le monde, la technologie VMware fait fonctionner les infrastructures numériques les plus complexes. Les solutions propriétaires de Cloud, de modernisation des apps, de réseau, de sécurité et d'espaces de travail numériques aident les clients à déployer n'importe quelle application sur tout type de Cloud, quel que soit le terminal. Basée à Palo Alto, en Californie, l'entreprise VMware s'engage à œuvrer pour le bien, grâce à des innovations technologiques révolutionnaires ou son impact à l'échelle mondiale. Pour plus d'informations, rendez-vous sur vmware.com/fr/company.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com