PAPIER NOIR ET BLANC

451 Research | Advisory

Rapport d'étude du projet MANRS

AOUT 2017

MANDATÉ PAR

Internet Society

A propos de ce document

Un document Black & White est une étude basée sur des données d'enquête de recherche primaire qui évalue la dynamique du marché d'un segment clé de la technologie d'entreprise à travers le prisme de l'expérience "sur le terrain" et des opinions de vrais praticiens - ce qu'ils font et pourquoi ils le font.

À propos de 451 Research

451 Research est une société de recherche et de conseil en technologies de l'information de premier plan. En mettant l'accent sur l'innovation technologique et les perturbations du marché, nous fournissons des informations essentielles aux leaders de l'économie numérique. Plus de 100 analystes et consultants fournissent ces informations par le biais de recherches syndiquées, de services de conseil et d'événements en direct à plus de 1 000 organisations clientes en Amérique du Nord, en Europe et dans le monde entier. Fondée en 2000 et basée à New York, 451 Research est une division de The 451 Group.

NEW YORK
1411 Broadway New York, NY 10018
+1 212 505 3030

SAN FRANCISCO
140, rue Geary
San Francisco, CA 94108
+1 415 989 1555

LONDRES
Paxton House 30, Artillery Lane
Londres, E1 7LS, Royaume-Uni
+44 (0) 207 426 1050

BOSTON
75-101, rue fédérale
Boston, MA 02110
+1 617 598 7200

RÉSUMÉ EXÉCUTIF

Le projet Mutually Agreed Norms for Routing Security (MANRS) a été fondé avec l'objectif ambitieux d'améliorer la sécurité et la fiabilité de l'Internet mondial. À l'approche du troisième anniversaire de sa création, une étude a été entreprise pour mieux comprendre les attitudes et les perceptions des fournisseurs de services Internet et de la communauté des entreprises au sens large à l'égard du projet MANRS. Ce rapport documente les résultats de cette étude et fournit des conseils et des perspectives sur l'état et l'avenir du projet MANRS. Il comprend des cas d'utilisation pour les fournisseurs de services et les entreprises qui soulignent les avantages de la participation au projet MANRS.

L'interprétation de l'étude a donné lieu à des résultats intéressants qui sont pertinents pour les participants et le conseil du projet. Les points clés de l'étude sont les suivants :

- Si MANRS lui-même n'est pas bien connu des entreprises, ses attributs sont très appréciés.
- Les entreprises attendent beaucoup des efforts de MANRS.
- La perception de MANRS par les entreprises peut se traduire par une augmentation des revenus pour les fournisseurs de services.
- Les actions existantes du MANRS couvrent un ensemble raisonnable de contrôles.
- Il existe des options permettant d'étendre les actions du MANRS pour certains fournisseurs.

L'étude montre que le projet MANRS présente un potentiel considérable non réalisé et que l'intérêt des entreprises devrait inciter davantage de prestataires de services à y participer. L'éducation du marché pourrait être particulièrement efficace pour surmonter l'inertie opérationnelle à laquelle de nombreux fournisseurs sont confrontés.

Description du projet

Ce projet de recherche a été entrepris pour mieux comprendre les progrès réalisés par le MANRS, y compris sa visibilité et sa perception au sein des communautés d'entreprises et de fournisseurs de services, et pour explorer les mesures qui pourraient être prises pour accroître la participation et la sensibilisation. Des études discrètes ont été menées auprès de populations distinctes de fournisseurs de services et de personnel informatique d'entreprise impliqués dans des contrats de services Internet. Les études ont permis d'identifier leur connaissance du MANRS et d'approfondir leurs opinions sur les différents aspects de la mise en œuvre et la valeur perçue des actions du MANRS. Les réponses à l'étude ont été analysées, et les corrélations et divergences entre les deux groupes ont été évaluées. Ce rapport détaille les résultats et les conclusions qui ont été faites.

Deux cas d'utilisation ont été créés en plus de ce rapport, l'un concernant les entreprises et l'autre les fournisseurs de services. Chacun d'eux examine les avantages d'une plus grande implication dans MANRS pour le groupe spécifique et s'appuie sur les données recueillies dans le cadre des études

Méthodologie de l'étude

Il peut être complexe de parvenir à une compréhension plus approfondie des perceptions dans des domaines aussi vastes que la sécurité de l'information et du routage. L'étude entreprise dans le cadre de ce projet visait à comparer les résultats de deux communautés distinctes mais interconnectées. On s'attendait à ce que les fournisseurs de services aient une certaine exposition au MANRS, et que le niveau de compréhension soit important. Pour les entreprises, on s'attendait à ce que l'exposition soit plus limitée et que les aspects les plus importants soient l'alignement des valeurs sur les caractéristiques des MANRS. Pour cette raison, bien que les études aient travaillé à partir d'une base commune, les ensembles de questions utilisées avaient une orientation différente pour chacun des groupes cibles. Une organisation indépendante a été utilisée pour mener les études finales.

L'étude sur les fournisseurs de services avait une portée plus étroite et était plus approfondie que l'étude sur les entreprises. L'ensemble des questions a été testé sur un groupe initial de 10 fournisseurs dont on savait qu'ils comprenaient le projet MANRS. Elle a été menée par le biais d'entretiens téléphoniques ouverts. Les résultats des entretiens du groupe initial n'ont pas été inclus dans l'étude, mais ont été utilisés pour façonner les ensembles de questions finales pour chaque groupe suivant. Le groupe initial était géographiquement diversifié, avec des représentants d'Asie, d'Europe et d'Amérique du Nord. L'étude formelle a consisté en des entretiens téléphoniques avec 25 employés de fournisseurs de services sélectionnés au hasard pour s'assurer qu'ils participaient aux décisions relatives aux opérations d'infrastructure de routage et qu'ils occupaient des postes de direction au sein de leur organisation. Ce groupe provenait presque exclusivement d'Amérique du Nord et présentait une répartition égale de la taille des organisations, avec une taille médiane de 2 500 à 4 999 employés.

L'étude sur les utilisateurs en entreprise a été menée par formulaire Web auprès d'un groupe de 250 répondants sélectionnés de manière aléatoire pour s'assurer qu'ils faisaient partie du personnel de gestion informatique impliqué dans l'achat et la passation de marchés de services Internet. La taille des entreprises a été limitée à un minimum de 1 000 employés afin de cibler celles dont les besoins en services Internet sont les plus importants. Les personnes interrogées provenaient principalement d'Amérique du Nord et étaient largement réparties entre les différents secteurs d'activité. Les entreprises de fabrication et de services professionnels étaient les plus représentées, chacune de ces verticales représentant 14 % du panel total. Les secteurs de la santé, des télécommunications et de la vente au détail les suivaient de près, avec des pourcentages à un chiffre pour les autres secteurs verticaux. La taille médiane des organisations était également de 2 500 à 4 999.

Aperçu des résultats

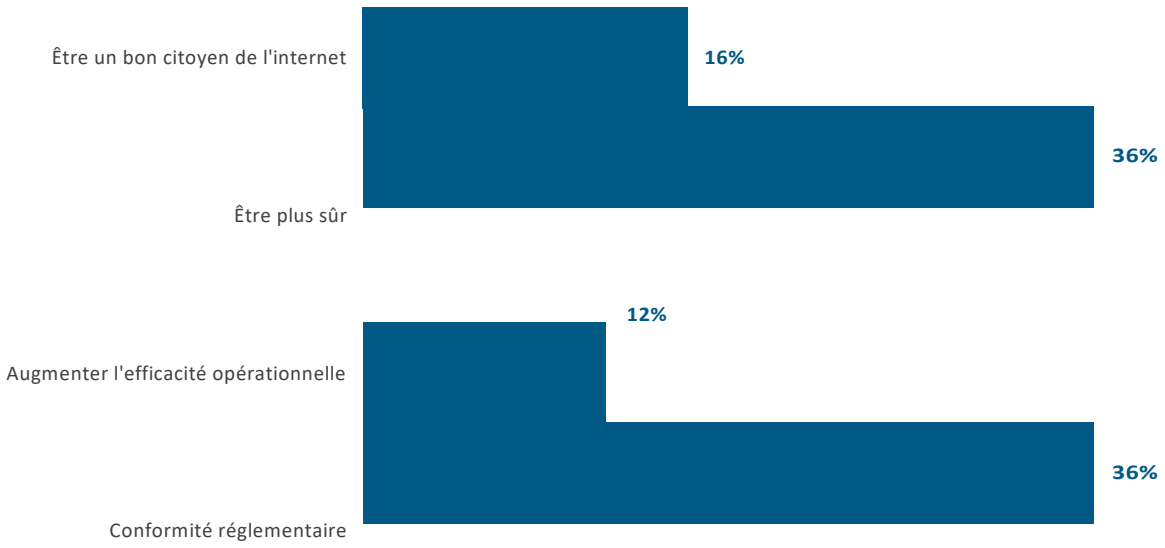
Les études ont confirmé nos attentes, à savoir que la visibilité de MANRS pouvait être améliorée tant auprès des entreprises que des fournisseurs de services. Elles ont également révélé que les fournisseurs de services sous-estimaient la valeur que leurs clients accordent à leur positionnement général en matière de sécurité. Un résultat inattendu est la mesure dans laquelle les entreprises considèrent la sécurité comme une valeur essentielle pour elles-mêmes. Cela peut être le résultat d'une sensibilisation accrue due à une couverture médiatique plus importante des incidents de sécurité, mais pourrait également refléter une maturité croissante du positionnement informatique dans les entreprises.

Détails de l'étude sur les prestataires de services

L'étude des prestataires de services a confirmé bon nombre des préoccupations qui avaient été exprimées lors de l'évaluation initiale. Toutefois, ces préoccupations ne sont peut-être pas entièrement fondées, car un seul répondant a déclaré avoir mis en œuvre la plupart des actions du projet MANRS et, par conséquent, les fournisseurs de services interrogés n'ont pas d'expérience directe de la mise en œuvre du projet MANRS. Cela signifie que les perceptions de la base de l'enquête sont une représentation raisonnable de la communauté des fournisseurs de services que le projet MANRS espère atteindre - à savoir, ceux qui n'ont pas encore participé. Près d'un tiers des répondants n'avaient pas entendu parler du MANRS, tandis qu'un peu plus étaient bien au courant du projet. Cela signifie que les estimations des efforts de mise en œuvre sont spéculatives. Il est intéressant de noter qu'aucun des répondants ne craignait que le MANRS augmente l'effort ou la complexité opérationnelle, alors que plus des deux tiers (68 %) pensaient qu'il pourrait les diminuer. Très souvent, les technologies nouvelles et non éprouvées sont perçues comme nécessitant plus d'efforts, ce qui est un signe positif quant aux attentes des fournisseurs de services. Cela dit, un peu plus de la moitié (52 %) des répondants étaient modérément préoccupés par le fait que la mise en œuvre de MANRS puisse entraîner une interruption de service - 24 % n'étaient pas préoccupés, tandis qu'un nombre égal était très préoccupé, ce qui indique qu'une certaine perturbation opérationnelle était à prévoir.

Les implications de la culpabilité après l'adoption du MANRS étaient modérées pour 60% des répondants, mais 28% n'ont exprimé aucune inquiétude. Cela est très probablement dû aux différents styles d'engagement avec les clients chez les divers fournisseurs de services. Ceux qui s'identifient déjà à un intérêt pour la sécurité avaient des niveaux de préoccupation plus faibles.

Figure 1 : Raisons de la mise en œuvre



Source : Étude de 451 Research : MANRS Perception et Action, juillet, 2017

Il y a eu une déconnexion peu surprenante concernant le processus de décision autour de MANRS. Alors que 64% des personnes interrogées ont déclaré que la direction technique serait le moteur de l'adoption, seulement 4% de ces équipes avaient l'autorité pour le mettre en œuvre - au lieu de cela, 80% des fournisseurs de services auraient besoin de l'approbation de la direction de niveau intermédiaire ou supérieur (40% pour chacun). Cela posera des problèmes dans les organisations où les impératifs de mise en œuvre ne sont pas clairement communiqués dans l'ensemble de l'organisation.

Les motivations pour la mise en œuvre étaient également en décalage avec les résultats des entreprises. Alors que 97% des entreprises envisageaient d'inclure la conformité au MANRS dans un appel d'offres et que 13% l'envisageraient pour une exigence de verrouillage, les résultats de l'enquête auprès des fournisseurs de services reflétaient un manque de compréhension de cette importance. Seulement 12 % des fournisseurs de services planifieraient la mise en œuvre si une exigence de MANRS était incluse dans une demande de propositions. Pour 72 % d'entre eux, cela inciterait à la réflexion, et pour 16 %, cela n'aurait aucun impact. Ces réponses peuvent être considérées comme spéculatives, étant donné que la conformité au MANRS a été peu ou pas utilisée dans la sélection des fournisseurs. Nous estimons que les réponses pencheraient davantage en faveur de la mise en œuvre s'il y avait une expérience de la conformité aux SRM dans les processus de DP et d'appel d'offres.

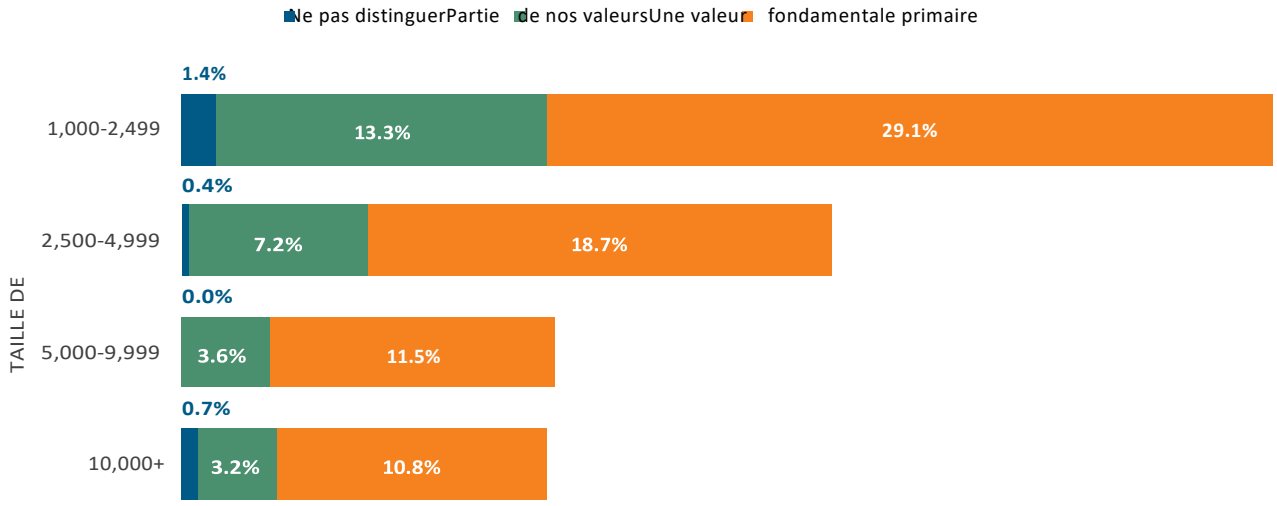
IMPACTS DES ÉTUDES SUR LES PRESTATAIRES DE SERVICES

La communauté des fournisseurs de services fait preuve d'un enthousiasme prudent à l'égard de MANRS. C'est encourageant dans la mesure où l'on s'attend à ce que les clients n'apprécient pas les MANRS. Cependant, pour accroître les motivations de mise en œuvre, il existe un manque de connaissances qui doit être comblé par l'éducation, et il faut des histoires solides des deux côtés. MANRS pourrait inciter les entreprises à dépenser davantage auprès des fournisseurs de services, ce qui est un message que la direction souhaite entendre, et les entreprises apprécient les détails de sécurité que les équipes techniques sont désireuses de promouvoir. L'intérêt des entreprises pour l'inclusion de MANRS dans les processus de demande de propositions et d'appel d'offres ne peut qu'accroître ce potentiel.

Détails de l'étude sur les entreprises

La partie de l'étude consacrée aux entreprises a examiné les préoccupations en matière de sécurité et a exploré leur alignement avec les valeurs de MANRS. Un nombre surprenant d'entreprises interrogées (71%) ont déclaré que la sécurité était une valeur fondamentale pour leur organisation. L'évaluation de la répartition par taille d'entreprise a montré que les petites entreprises se préoccupaient davantage de la sécurité dans le cadre de leurs valeurs fondamentales. Ce niveau de préoccupation a persisté dans de nombreuses réponses de l'étude sur les entreprises.

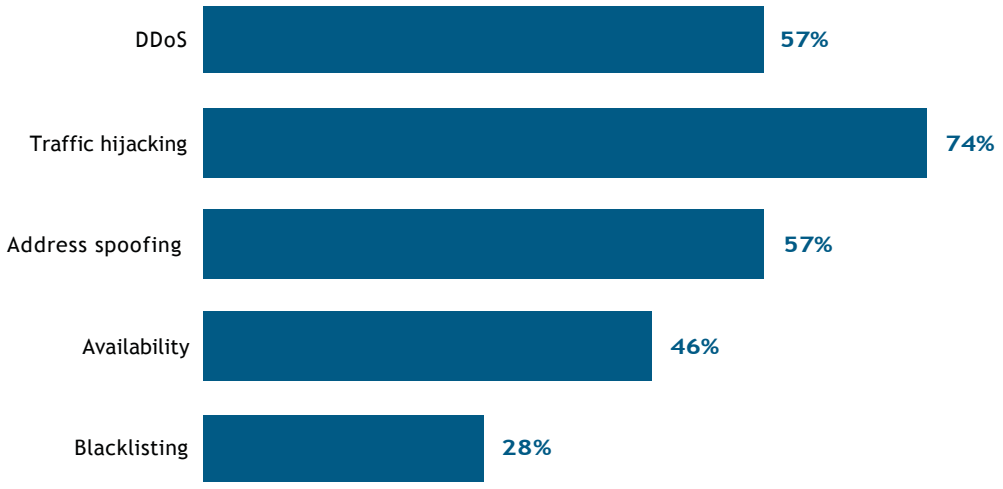
Figure 2 : Importance de la posture de sécurité globale



Source : Étude de 451 Research : MANRS Perception et Action, juillet, 2017

Lorsque l'on examine les types de problèmes de sécurité, le détournement de trafic arrive en tête de liste. Cela peut être considéré comme une autre confirmation que l'accent mis par les répondants sur les services Internet peut les sensibiliser davantage aux types de problèmes que MANRS cherche à résoudre. C'est de bon augure pour leurs attentes.

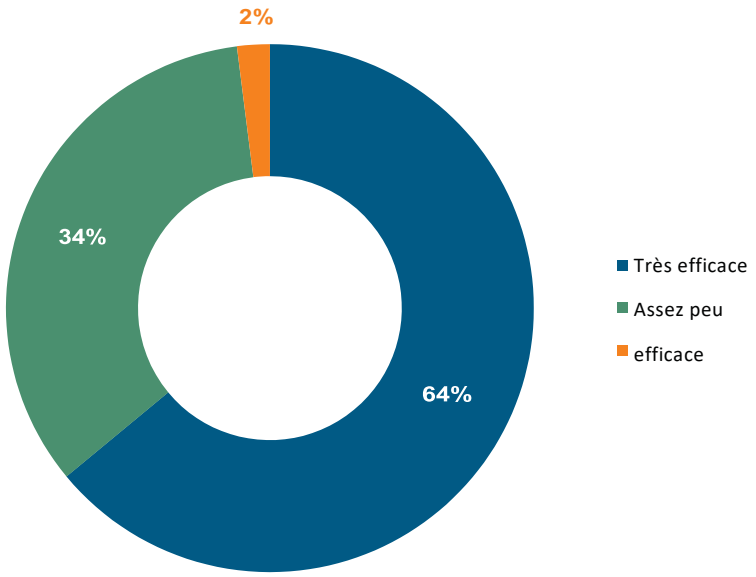
Figure 3 : Préoccupations en matière de sécurité sur Internet



Source : Étude de 451 Research : MANRS Perception et Action, juillet, 2017

Parallèlement à ces préoccupations, il y avait une confiance dans le fait que les actions du MANRS pourraient être efficaces pour y faire face. Cela a paral- lement entraîné un ensemble de réponses positives aux valeurs du MANRS et aux attentes exprimées dans les entrées narratives

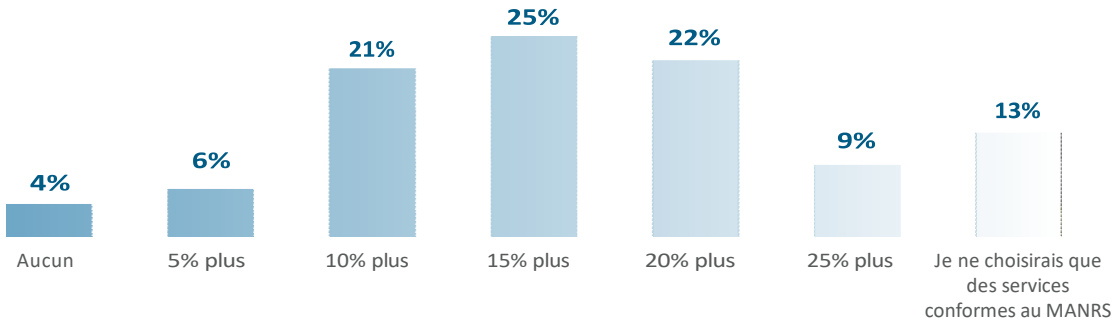
Figure 4 : Efficacité du MANRS



Source : Étude de 451 Research : MANRS Perception et Action, juillet, 2017

Plus important encore, les entreprises ont montré qu'elles étaient prêtes à payer pour ce qu'elles considéraient comme précieux. En identifiant l'augmentation de prix qu'elles supporteraient pour la conformité au MANRS, la valeur médiane était de 15% - une prime impressionnante pour ce qui est souvent considéré comme un service de base.

Figure 5 : Prime de tarification d'entreprise pour MANRS



Source : Étude de 451 Research : MANRS Perception et Action, juillet, 2017

En outre, 13 % ont indiqué que, s'ils étaient disponibles, ils ne choisiraient qu'un fournisseur conforme au MANRS dans une situation de concurrence.

IMPACTS DES ÉTUDES D'ENTREPRISE

Les résultats des entreprises indiquent qu'il existe de grandes opportunités pour les fournisseurs de services qui participent à MANRS. Les décideurs d'entreprise recherchent les types de valeurs que MANRS confère aux participants. Les possibilités d'augmentation des revenus et d'amélioration de la compétitivité sont réelles et importantes. La sécurité est un domaine d'intérêt majeur pour les entreprises, et MANRS peut être une marque de confiance dans une partie essentielle de leur infrastructure informatique à un moment où il est de plus en plus difficile de différencier les fournisseurs.

Cas d'utilisation

Les deux cas d'utilisation de ce projet de recherche traitent des avantages de la participation au MANRS pour les fournisseurs de services et les entreprises. Ils sont livrés sous forme de documents séparés et sont inclus ici à titre de référence.

Recommandations

Les études ont montré qu'il existe un potentiel important pour l'adoption supplémentaire du projet MANRS tel qu'il existe aujourd'hui, ainsi que des options pour étendre le programme à certains segments de la communauté des fournisseurs de services. Les principales conclusions de l'étude peuvent être résumées comme suit :

- La sensibilisation au MANRS dans l'entreprise pourrait inciter les fournisseurs de services à participer.
- La formation des prestataires de services aux valeurs de l'entreprise pourrait stimuler la participation.
- Un certain niveau d'implication réglementaire peut être nécessaire.

La sensibilisation au MANRS dans l'entreprise peut se faire par le biais de partenariats avec les fournisseurs de services participants. Les entreprises indiquent qu'elles considèrent les fournisseurs de services comme des sources d'autorité technique, et les fournisseurs tirent des avantages directs en termes de position concurrentielle dans le cadre de cette promotion. Il existe d'autres voies par le biais des organisations de pairs pour les entreprises, telles que les groupes d'utilisateurs et les communautés en ligne. Il s'agit également d'avenues qui pourraient être poursuivies en partenariat avec les fournisseurs de services. Les forums axés sur la sécurité présentent le plus grand potentiel, tels que :

- ISACA - Un organisme sans but lucratif qui offre une certification et une communauté en matière de sécurité et de gouvernance.
- RSA Conference - Conférence axée sur la sécurité où des sessions MANRS pourraient être proposées.
- (ISC)2 - Un organisme de certification de sécurité à but non lucratif qui organise également des conférences sur la sécurité.
- InfraGard - Organisme de coordination américain parrainé par le Federal Bureau of Investigation et chargé de la protection des infrastructures.

Il sera important d'éduquer davantage les fournisseurs de services sur le niveau de valeur que les entreprises voient dans MANRS. Il existe un déséquilibre évident à ce niveau, et la différenciation qu'offre le MANRS aux yeux des décideurs d'entreprise joue en faveur des fournisseurs. Étant donné la taille réduite de la communauté, la promotion directe peut être efficace, de même que les événements ciblés. Les groupes d'opérateurs et les conférences spécifiques aux fournisseurs pourraient inclure :

- NANOG, RIPE, AfNOG, APRICOT et autres groupes d'opérateurs.
- HostingCon - Conférence annuelle axée sur les fournisseurs de services

Tant les fournisseurs de services que les entreprises ont indiqué qu'un certain niveau d'implication réglementaire serait un moteur important pour l'adoption des MANRS. Il s'agit d'un domaine où nous recommandons la prudence, car la nature et la direction de la réponse dans les interactions gouvernementales peuvent être difficiles à gérer. Une voie efficace consisterait à travailler avec les auditeurs et les organisations de l'industrie pour promouvoir des activités qui s'alignent sur les impératifs gouvernementaux. Les efforts déployés par le National Institute of Standards (NIST) des États-Unis et l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) ont abouti à des recommandations visant à améliorer la sécurité des entreprises. La tâche d'interpréter et de mettre en œuvre ces recommandations incombe souvent aux auditeurs et aux sociétés de services de sécurité. Travailler à l'intégration du MANRS dans leurs pratiques pourrait être un moyen pratique de tirer parti des priorités des mandats réglementaires sans risquer une action gouvernementale directe. Le cadre COBIT de l'ISACA est une autre possibilité. Il peut également y avoir des pistes avec des organisations telles que le Payment Card Industry Security Standards Council, mais celles-ci sont moins directement pertinentes pour le public cible de MANRS. L'avenir du MANRS peut inclure un certain nombre d'options pour l'élargissement de son mandat. Les activités actuelles du MANRS correspondent bien à l'étendue des responsabilités des fournisseurs de services Internet. Alors que de plus en plus de fournisseurs commencent à offrir des services de sécurité améliorés, le MANRS pourrait offrir des conseils dans ces domaines.

seulement légèrement derrière les initiatives de sensibilisation à la sécurité. C'est une indication forte de la priorité que les entreprises accordent à la gestion de la sécurité opérationnelle. Les fournisseurs de services peuvent proposer des conseils et des services gérés pour répondre à ces demandes.

Dans cette étude, les entreprises ont identifié les préoccupations relatives à l'intégrité du trafic comme une priorité élevée. L'acheminement, l'interception et le détournement du trafic ont été signalés comme la principale préoccupation en matière de sécurité (74 %, le DDoS et l'usurpation d'adresse arrivant en deuxième position avec 57 % chacun), tandis que la validation de l'itinéraire a été la principale valeur MANRS (32 %) dans une question distincte. Cette préoccupation pourrait s'étendre à d'autres domaines de l'intégrité des infrastructures. MANRS pourrait identifier des technologies telles que la sécurité de l'espace de noms, qui est abordée avec DNSSEC. Alors que les fournisseurs de services s'appuient sur les bureaux d'enregistrement pour la mise en œuvre des DNSSEC, ils ont souvent des relations de travail étroites et pourraient fournir des services de mise en œuvre aux entreprises qui cherchent à mettre en œuvre les DNSSEC. Cela pourrait renforcer le rôle de conseiller de sécurité de confiance que les fournisseurs de services ont déjà commencé à assumer.

MANRS pourrait également aider à définir le cadre d'une autre opportunité de revenus pour les fournisseurs de services. De nombreuses entreprises intègrent des flux de renseignements dans leurs opérations. Elles cherchent à améliorer leur connaissance de la situation et sont intéressées par les informations opérationnelles qui peuvent être transmises aux systèmes SIEM. Les flux d'informations et d'événements que les actions de MANRS pourraient générer ont de la valeur pour les entreprises. Les contrôles d'anti-spoofing et de validation de route génèrent souvent des messages de journal qui pourraient être fournis comme flux de renseignements. Le projet MANRS pourrait définir un format standard pour ces flux d'informations afin d'aider les fournisseurs de services à les intégrer à leurs entreprises clientes. Cet effort pourrait être réalisé en collaboration avec d'autres organisations qui créent des formats pour l'échange d'informations de sécurité. STIX, Cybox et TAXII trouvent aujourd'hui des applications dans un certain nombre d'entreprises et constitueraient des points de départ utiles. La création de services monétisables dans le cadre de MANRS pourrait être une raison supplémentaire de participer.

Bien qu'il ait été difficile de créer une augmentation spectaculaire de l'adoption du MANRS, les études ont montré qu'il existe une solide concordance entre les motivations des fournisseurs de services et les aspirations des entreprises. Avec des efforts supplémentaires, le rapprochement de ces deux éléments pourrait créer un avenir radieux pour les systèmes MANRS.

A propos de l'auteur

Eric Hanselman est l'analyste en chef de 451 Research. Il possède une connaissance approfondie et pratique d'un large éventail de domaines informatiques, avec une expérience directe dans les domaines des réseaux, de la virtualisation, de la sécurité et des semi-conducteurs. Il coordonne l'analyse du secteur à travers le vaste portefeuille de disciplines de 451 Research. La convergence des forces à travers le paysage technologique crée des changements tectoniques dans l'industrie, notamment SDN/NFV, l'hyperconvergence et l'Internet des objets (IoT). Eric aide les clients de 451 Research à naviguer dans ces eaux turbulentes et à déterminer leurs impacts et la manière dont ils peuvent les capter au mieux.

Pendant plus de 20 ans, Eric a travaillé avec les leaders du secteur dans un large éventail de technologies, et plus récemment en tant que directeur technique de Leost- ream Corporation, un fournisseur de gestion de la virtualisation. Avant cela, Eric a fourni des solutions de sécurité pour IBM et Internet Security Systems. Chez Wellfleet/Bay Networks, Sitara Networks et NEC, il a participé à l'introduction de nombreuses nouvelles technologies allant de l'analyse d'images à haute performance aux déploiements pour IPv6. Eric est titulaire d'un brevet sur les systèmes de compression d'images. Il est également membre de l'Institute of Electrical and Electronics Engineers (IEEE), professionnel certifié en sécurité des systèmes d'information (CISSP) et professionnel certifié VMware (VCP), et il intervient fréquemment dans les principales conférences du secteur. Il a étudié la chimie au Reed College.

Annexe I : Fournisseurs de services - La sécurité permet de faire de meilleures affaires

APERÇU

Il peut être difficile pour les fournisseurs de services Internet de se différencier sur le marché actuel. Les clients sont souvent perplexes quant à la différenciation des capacités et des performances entre les fournisseurs, et il peut être difficile d'exprimer clairement la valeur qu'offre un fournisseur. Des distinctions concrètes sont possibles dans le domaine de la sécurité, dont la valeur est bien établie auprès des entreprises et qui peut avoir un impact significatif sur les processus d'achat et de décision des clients. Le projet Mutually Agreed Norms for Routing Security (MANRS) peut fournir une marque de compétence en matière de sécurité et d'engagement communautaire pour les fournisseurs qui sont en mesure de participer. Cette distinction peut ajouter une valeur concurrentielle à un fournisseur et peut également améliorer l'efficacité opérationnelle. Une nouvelle étude de 451 Research a détaillé cette valeur et la manière dont les fournisseurs de services peuvent la mettre à profit.

VALEUR D'ENTREPRISE

Lorsque les entreprises cherchent à sélectionner des partenaires d'infrastructure, elles jonglent avec un ensemble d'exigences qui peuvent être difficiles à gérer. Lorsqu'elles ont du mal à déterminer la valeur des aspects concurrents des offres des différents fournisseurs, leur attention se porte souvent sur le prix. Pour déplacer le point de décision au-delà du seul prix, les fournisseurs doivent présenter des qualités facilement identifiables et capables de les différencier. L'étude de 451 Research a montré que la posture de sécurité d'un fournisseur de services est importante pour les entreprises et que la participation à MANRS a de la valeur. Bien que MANRS ne soit pas très connu des entreprises, les idées que le projet représente sont tenues en haute estime et ont une réelle valeur pour les acheteurs des entreprises.

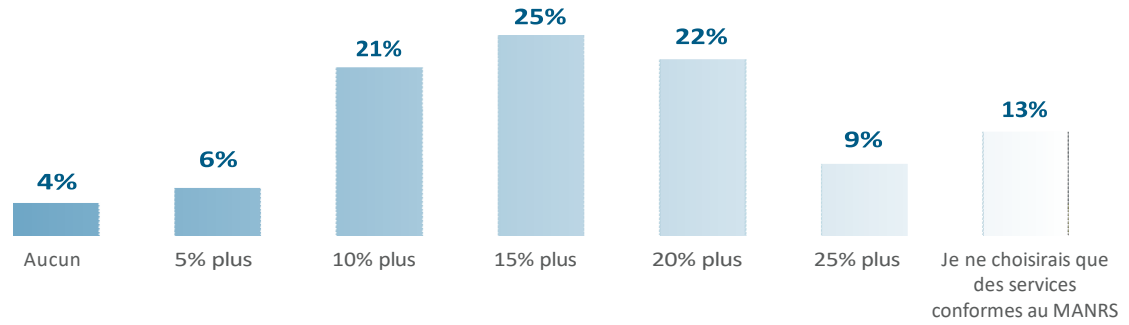
L'étude comprenait une brève introduction au projet, puis demandait aux répondants comment ils appréciaient ce que la participation au projet MANRS leur offrait et quels étaient les directives et les résultats du projet qui leur étaient les plus utiles. La première de ces évaluations consistait à déterminer combien ils seraient prêts à dépenser davantage, le cas échéant, pour obtenir des services d'un fournisseur participant au projet MANRS. La valeur médiane de la prime de prix était de 15 % - une évaluation considérable pour ce qui est considéré comme un service de base par de nombreux acheteurs. De plus, 33% des répondants ont déclaré qu'ils utiliseraient la participation au MANRS comme un critère exclusif de sélection des fournisseurs, s'il était disponible. Un total de 97% étaient intéressés à mettre la participation au MANRS dans les exigences des DP et des appels d'offres.

Cette évaluation signifie que la participation au MANRS peut apporter une série d'avantages aux prestataires de services :

- ③ Amélioration du positionnement concurrentiel dans le processus de demande de propositions et d'appel d'offres.
- ③ Augmentation de la fidélisation des clients et diminution du taux de désabonnement
- ③ Possibilités de services à valeur ajoutée

Tout cela s'ajoute aux avantages internes que les fournisseurs de services peuvent obtenir avec MANRS. Les fournisseurs de services peuvent améliorer leur efficacité opérationnelle en établissant de meilleures voies de communication avec leurs pairs. Ils ont également la possibilité d'améliorer les opérations de sécurité en identifiant plus tôt les problèmes avec les clients et les pairs, sans oublier la valeur ajoutée de la contribution à la sécurité globale de la communauté Internet.

Figure 1 : Prime de tarification d'entreprise pour MANRS



Source : Étude de 451 Research : MANRS Perception et Action, juillet, 2017

MONÉTISATION DE MANRS

Il existe plusieurs façons pour les prestataires de services de mettre à profit la valeur de la participation au MANRS :

- ③ Inclure le MANRS dans les propositions
- ③ Faire connaître les valeurs du MANRS aux clients
- ③ Offrir des services à valeur ajoutée

Capitaliser directement sur la valeur du MANRS en augmentant les prix est problématique. La réalité de la plupart des marchés est que les comparaisons de prix se feront indépendamment des autres aspects d'une décision d'achat. Là où la participation au MANRS peut être utile, c'est dans la réduction des niveaux d'escompte requis pour obtenir des contrats. La participation au MANRS peut être utilisée pour augmenter la probabilité de sélection dans un processus concurrentiel. Elle peut être utilisée comme un moyen d'éliminer les concurrents qui ne sont pas qualifiés. Les résultats de l'étude ont montré que les entreprises sont enthousiastes à l'idée d'inclure le MANRS comme critère de sélection. Une analyse supplémentaire a montré que les améliorations de la position concurrentielle et les réductions des rabais nécessaires pourraient ajouter jusqu'à 7% aux revenus à long terme.

Les clients apprécient la participation au MANRS, et les prestataires de services peuvent en tirer parti en faisant connaître leur participation. En incluant des informations et une image de marque dans le marketing et les communications destinées aux clients et au marché en général, les fournisseurs de services peuvent faire une forte impression dans un domaine que les clients considèrent comme précieux. Faire connaître le MANRS peut rafraîchir la compréhension qu'ont les clients des capacités précieuses de leurs fournisseurs et peut réduire la probabilité qu'ils envisagent de changer de fournisseur. Ce lien avec le client peut être renforcé par des communications axées sur la sécurité et la création d'une communauté. L'étude de 451 Research a également montré que le fait de faire partie d'une communauté plus large qui travaille à l'amélioration de la sécurité de l'Internet est un autre aspect du MANRS qui est important pour les clients.

Les fournisseurs de services peuvent gagner des revenus supplémentaires en ajoutant des services dérivés de MANRS à leur portefeuille. Les contrôles anti-spoofing qui enregistrent l'activité peuvent être utilisés pour générer des rapports périodiques pour les clients. Ces rapports peuvent faire partie d'un flux de renseignements qui alerte les clients sur les mauvaises configurations ou les attaques potentielles. Ce type de service peut être peu coûteux à exploiter, s'il est correctement automatisé, et peut offrir une liaison supplémentaire aux clients, en plus de générer des revenus.

CONCLUSIONS

Pour les fournisseurs de services, la participation au projet MANRS présente des avantages considérables. Elle peut accroître leur valeur pour les clients et potentiellement augmenter leurs revenus. Les directives MANRS constituent un guide utile pour accroître l'efficacité opérationnelle tout en contribuant à l'amélioration de la sécurité de la communauté Internet. La combinaison de l'impact sur les clients et des avantages internes devrait être une motivation suffisante pour que les fournisseurs fassent partie de cette communauté en pleine expansion.

Annexe II : Entreprises - Rejoindre une communauté pour une plus grande sécurité

APERÇU

Les entreprises doivent relever de nombreux défis dans l'exploitation de leur infrastructure informatique, et l'un des plus importants est la sélection des fournisseurs de services. L'évaluation des capacités et des performances des fournisseurs peut être un processus complexe. Un facteur qui peut aider à prendre cette décision est la participation d'un fournisseur au projet Mutually Agreed Norms for Routing Security (MANRS). MANRS est un projet de collaboration qui se concentre sur des mesures concrètes pour améliorer la position de sécurité des participants et contribuer ainsi à la sécurité globale de la communauté Internet. En travaillant avec un fournisseur de services qui fait partie du projet MANRS, les entreprises peuvent se placer à l'avant-garde de ceux qui ont une position favorable à la sécurité et rejoindre la grande communauté Internet qui s'efforce d'améliorer la sécurité et la fiabilité.

LES OBJECTIFS DU PROJET MANRS

Le projet MANRS vise à améliorer la sécurité et la fiabilité de l'Internet mondial en normalisant les contrôles et les principes d'exploitation utilisés par les opérateurs de réseaux. Il définit un ensemble de quatre actions que les participants mettent en œuvre dans le cadre de leurs opérations et de leurs interactions avec les autres. Collectivement, ces efforts visent à freiner les activités accidentelles ou intentionnelles qui peuvent nuire à la fiabilité de l'internet. Les quatre actions sont les suivantes :

- Filtrage des routes - Prévention de la propagation d'informations de routage incorrectes.
- Anti-spoofing - Prévention du trafic avec des adresses IP sources usurpées.
- Coordination - Faciliter la communication opérationnelle mondiale et la coordination entre les opérateurs de réseau.
- Validation globale - Faciliter la validation des informations de routage à l'échelle mondiale.

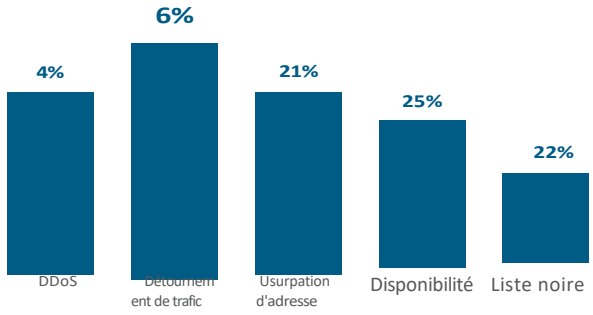
Ensemble, ces actions peuvent contribuer à prévenir les problèmes et à accélérer leur résolution lorsqu'ils surviennent. Les fournisseurs de services qui participent au MANRS se sont engagés à prendre part à cet effort. L'un des défis de la structure de l'Internet est qu'elle nécessite des efforts communautaires plus importants comme celui-ci pour être efficace. Cet effort peut contribuer à réduire les problèmes récurrents, tels que le détournement de trafic, les attaques par déni de service (DDoS) et le détournement de trafic.

L'ÉTUDE MANRS

Dans le but d'évaluer le projet MANRS et son impact sur les entreprises et les fournisseurs de services, 451 Research a réalisé une étude approfondie dont les résultats fournissent des données comparatives utiles sur l'importance et l'impact du projet pour les entreprises. Plus de 70 % des personnes interrogées dans le cadre de l'étude ont indiqué que la posture de sécurité de l'information était une valeur essentielle pour leur organisation.

L'étude s'est également penchée sur les préoccupations des entreprises en matière de sécurité sur Internet et a cherché à quantifier la manière dont elles comptent y répondre. La plus grande préoccupation était le détournement de trafic, un problème qui a souvent fait la une des journaux et qui, au-delà de ses implications en matière de sécurité, a des répercussions sur la satisfaction des clients.

Figure 1 : Préoccupations en matière de sécurité sur Internet

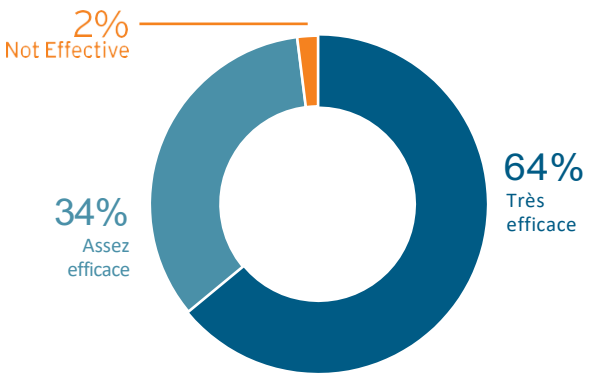


Source : Étude de 451 Research : MANRS Perception et Action, juillet, 2017

Les deux préoccupations les plus importantes suivantes ont un lien intrinsèque. Si les attaques par déni de service sont une source de préoccupation, l'usurpation d'adresse - la technique qui peut être utilisée pour masquer l'origine des attaques DDoS - a suscité autant d'inquiétude parmi les répondants à l'étude. Le projet MANRS cherche à traiter les causes de ces préoccupations par le biais de ses quatre actions.

L'étude a également évalué l'opinion des organisations répondantes sur l'efficacité du projet MANRS à résoudre les problèmes qui les préoccupent. La quasi-totalité des répondants ont déclaré qu'ils pensaient qu'avec le temps, le projet aiderait à résoudre les problèmes de sécurité sur Internet. Près des deux tiers ont estimé qu'il serait très efficace.

Figure 2 : Efficacité du MANRS



Source : Étude de 451 Research : MANRS Perception et Action, juillet, 2017

SUR LEVIER MAN POUR L'ENTREPRISE

L'un des principaux avantages du projet MANRS pour les entreprises est l'indication qu'il donne de l'attitude et de l'initiative des fournisseurs de services en matière de sécurité opérationnelle. L'entreprise typique déploie des efforts considérables pour sélectionner ses partenaires d'infrastructure informatique, mais il peut être difficile de trouver des critères de sélection efficaces. Les fournisseurs de services qui participent à MANRS ont fait un effort pour améliorer leur position de sécurité et travaillent avec une communauté plus large pour réduire les menaces à la sécurité et à la stabilité d'Internet. La participation à MANRS peut être une mesure de sélection raisonnable et peut être incluse dans les processus de demande de propositions, d'appel d'offres et d'achat pour améliorer la compréhension des capacités d'un fournisseur. Dans l'étude de 451 Research, 97% des répondants ont indiqué qu'ils envisageraient d'inclure la participation au MANRS dans leur processus de sélection.

Le projet MANRS permet également aux organisations de rejoindre une communauté plus large qui se préoccupe de la sécurité. Cela peut aider les organisations qui cherchent à collaborer pour répondre aux préoccupations. Cela peut être un moyen d'identifier les partenaires de l'écosystème avec lesquels les entreprises peuvent unir leurs forces pour créer une base plus solide pour la sécurité. Dans les secteurs réglementés, les liens MANRS peuvent être un facteur supplémentaire à prendre en compte par les auditeurs lorsqu'ils évaluent la posture de sécurité globale d'une organisation.

MANRS peut également renforcer les résultats d'une entreprise. Comme l'a montré l'étude de 451 Research, la plupart des organisations sont préoccupées par la sécurité, et le fait de faire partie de la communauté MANRS peut renforcer les références de l'entreprise en matière de sécurité. Cela permet de communiquer l'investissement d'une entreprise en matière de sécurité à ses clients. L'implication de MANRS peut être incluse dans les documents marketing et faire partie d'une déclaration de marque plus large. Bien que le projet MANRS vise les fournisseurs de services, toute organisation ayant conclu des accords d'échange de trafic (peering) impliquant BGP peut également faire partie de la communauté. L'intégration des actions MANRS dans les opérations informatiques peut ajouter de la maturité et augmenter l'efficacité opérationnelle.

CONCLUSIONS

Le projet MANRS offre un certain nombre d'avantages pour les entreprises qui sont directement réalisables. La participation au projet MANRS doit être soigneusement étudiée, non seulement par les fournisseurs de services d'une entreprise, mais aussi potentiellement par l'organisation elle-même. La communauté Internet au sens large peut bénéficier de la sensibilisation accrue à la sécurité qu'offre le projet, et les entreprises jouent un rôle important à cet égard. Les entreprises qui rejoignent la communauté MANRS peuvent améliorer leur position en matière de sécurité, ainsi que leurs activités.

Annexe III

LANGUE DE L'APPEL D'OFFRES POUR LA SÉLECTION DE MANRS

Voici un exemple de langage qui pourrait être utilisé par les entreprises désireuses d'intégrer la conformité au MANRS dans un processus de demande de proposition pour la sélection de fournisseurs de services Internet. Il s'agit uniquement d'un exemple et non d'un avis juridique. Un conseiller juridique approprié devrait toujours être consulté lors de la préparation de tout document de demande de proposition.

Exigences en matière d'éligibilité pour les organisations proponibles

1. Conformité de l'organisation proposante au MANRS

XXXX soutient les efforts de la communauté Internet au sens large pour améliorer la résilience et la sécurité. Toutes les organisations proposantes doivent avoir participé et s'être conformées au projet Mutually Agreed Norms for Routing Security *(https://* www.manrs.org) pendant au moins les 30 jours précédant la soumission de la proposition. Les organisations proposantes maintiendront leur conformité pendant toute la durée du contrat et informeront XXXX si, à tout moment, la conformité n'est plus assurée. La notification doit se faire par l'intermédiaire des contacts spécifiés dans le contrat et doit prendre la forme d'une communication écrite. La conformité sera déterminée par la mise en œuvre d'au moins l'ensemble minimum d'actions attendues définies par le projet MANRS. Les manquements à la conformité seront considérés comme une violation matérielle de tout contrat en vigueur.