REVUE DE PRESSE
MAI 2018

Retrouvez tous les articles parus dans la presse au sujet de NetXP

Mercredi 9 mai – *Distributique.com*

NetXP fait sa première incursion en région en s'installant à Nantes

[Michaël Briquet, directeur associé de

NetXP : « En 2017, nous avons dégagé 10% de chiffre d'affaires supplémentaires et un REX d'environ 10%. Nous aurions pu faire beaucoup mieux avec davantage de collaborateurs. »…]

https://www.distributique.com/actualites/lire-netxp-fait-sa-premiere-incursion-en-region-en-s-installant-a-nantes-27698.html

Vendredi 11 mai – *FranceActu.net*

NetXP choisit Nantes pour sa première incursion régionale !

[Fondé en 2001, le prestataire francilien NetXP n'avait pas, jusqu'ici, éprouvé le besoin de s'implanter hors de son fief pour se développer. Début avril, cette société de conseil (sécurité, cloud, réseaux et télécoms) et fournisseur de services managés (infogérance, hébergement sur mesure, SOC labellisé CERT) a changé son fusil d'épaule…]

https://www.franceactu.net/technologie/netxp-choisit-nantes-pour-sa-premiere-incursion-regionale/

Vendredi 11 mai – *Le Monde Informatique*

NetXP choisit Nantes pour sa première incursion régionale

[La société de services et de conseils informatiques NetXP a ouvert une agence à Nantes début avril. Elle compte recruter une dizaine de collaborateurs d'ici deux ans…]

https://www.lemondeinformatique.fr/actualites/lire-netxp-choisit-nantes-pour-sa-premiere-incursion-regionale-71700.html

Mardi 15 mai – *Flash Infos Edition Paris IDF Centre Val de Loire*

NetXP s'implante à Nantes !

[Le Prestataire de conseils et services informatiques NetXP / T : 01.46.48.26.00 (siège à Boulogne Billancourt) a procédé au début du mois d'avril 2018 à l'ouverture à Nantes de son premier bureau en dehors d'Ile de France…]

Journal impression

Jeudi 24 mai – *Undernews.fr*

Cybersécurité – Qu'est-ce qu'un Wireless Intrusion Prevention System ?

[La demande de mobilité des utilisateurs ayant augmenté, les réseaux Wifi se sont fortement développés ces dernières années. De ce fait, et au vu de l'accès au réseau que ce service propose, de multiples attaques existent, engendrant une nécessité d'utiliser des systèmes de défense plus ou moins perfectionnés…]

https://www.undernews.fr/reseau-securite/cybersecurite-quest-ce-quun-wireless-intrusion-prevention-system.html

Jeudi 24 mai – *CBP Channel Business Partners*

Qu'est-ce qu'un Wireless Intrusion Prevention System ?

[La demande de mobilité des utilisateurs ayant augmenté, les réseaux Wifi se sont fortement développés ces dernières années. De ce fait, et au vu de l'accès au réseau que ce service propose, de multiples attaques existent, engendrant une nécessité d'utiliser des systèmes de défense plus ou moins perfectionnés…]

https://www.channelbp.com/content/quest-ce-quun-wireless-intrusion-prevention-system

Jeudi 24 mai – *Solutions numériques*

Qu'est-ce qu'un Wireless Intrusion Prevention System ?

[La demande de mobilité des utilisateurs ayant augmenté, les réseaux Wifi se sont fortement développés ces dernières années. De ce fait, et au vu de l'accès au réseau que ce service propose, de multiples attaques existent, engendrant une nécessité d'utiliser des systèmes de défense plus ou moins perfectionnés…]

https://solutions.digiplace.fr/communiques/quest-ce-quun-wireless-intrusion-prevention-system-2/

Jeudi 24 mai – *IT Numeric*

Qu'est-ce qu'un Wireless Intrusion Prevention System ?

[La demande de mobilité des utilisateurs ayant augmenté, les réseaux Wifi se sont fortement développés ces dernières années. De ce fait, et au vu de l'accès au réseau que ce service propose, de multiples attaques existent, engendrant une nécessité d'utiliser des systèmes de défense plus ou moins perfectionnés…]

http://www.itnumeric.com/quest-ce-quun-wireless-intrusion-prevention-system-communique/

Jeudi 24 mai – *IT for Business*

Qu'est-ce qu'un Wireless Intrusion Prevention System ?

[La demande de mobilité des utilisateurs ayant augmenté, les réseaux Wifi se sont fortement développés ces dernières années. De ce fait, et au vu de l'accès au réseau que ce service propose, de multiples attaques existent, engendrant une nécessité d'utiliser des systèmes de défense plus ou moins perfectionnés…]

http://www.itforbusiness.fr/leaders/item/10366-qu-est-ce-qu-un-wireless-intrusion-prevention-system

Jeudi 24 mai – *Global Security Mag*

Qu'est-ce qu'un Wireless Intrusion Prevention System ?

[La demande de mobilité des utilisateurs ayant augmenté, les réseaux Wifi se sont fortement développés ces dernières années. De ce fait, et au vu de l'accès au réseau que ce service propose, de multiples attaques existent, engendrant une nécessité d'utiliser des systèmes de défense plus ou moins perfectionnés…]

https://www.globalsecuritymag.com/Qu-est-ce-qu-un-Wireless-Intrusion,20180524,78804.html

Vendredi 25 mai – *M to M mag.com*

Qu'est-ce qu'un Wireless Intrusion Prevention System ?

[La demande de mobilité des utilisateurs ayant augmenté, les réseaux Wifi se sont fortement développés ces dernières années. De ce fait, et au vu de l'accès au réseau que ce service propose, de multiples attaques existent, engendrant une nécessité d'utiliser des systèmes de défense plus ou moins perfectionnés…]

http://www.mtom-mag.com/article6124.html

Vendredi 25 mai – *Sécurité DSIsionnel*

Qu'est-ce qu'un Wireless Intrusion Prevention System ?

[La demande de mobilité des utilisateurs ayant augmenté, les réseaux Wifi se sont fortement développés ces dernières années. De ce fait, et au vu de l'accès au réseau que ce service propose, de multiples attaques existent, engendrant une nécessité d'utiliser des systèmes de défense plus ou moins perfectionnés…]

http://securite.dsisionnel.com/2018/05/quest-ce-quun-wireless-intrusion-prevention-system/

Mardi 29 mai – *Informatiquenews.fr*

Se prémunir des attaques contre les mobiles

[La demande de mobilité des utilisateurs ayant augmenté, les réseaux Wifi se sont fortement développés ces dernières années. De ce fait, et au vu de l'accès au réseau que ce service propose, de multiples attaques existent, engendrant une nécessité d'utiliser des systèmes de défense plus ou moins perfectionnés…]

http://www.informatiquenews.fr/se-premunir-des-attaques-contre-les-mobiles-madeleine-wouters-netxp-57075

Mercredi 30 mai – *Infoprotection.fr*

Wireless Intrusion Prevention System (WIPS) : le point sur leur degré d'efficacité

[Selon le cabinet d'expertise parisien NetXP, mieux vaudrait se méfier de ces solutions destinées à protéger les réseaux WiFi. Leurs performances variant selon l'utilisation que l'on en fait, mais aussi selon le degré de sophistication de leurs fonctionnalités…]

http://www.infoprotection.fr/?IdNode=2511&Zoom=b472a50d92b1f018025e930ac7488256&xtor

NetXP fait sa première incursion en région en s'installant à Nantes

CRÉATION D'AGENCE,

Michaël Briquet, directeur associé de NetXP : « En 2017, nous avons dégagé 10% de chiffre d'affaires supplémentaires et un REX d'environ 10%. Nous aurions pu faire beaucoup mieux avec davantage de collaborateurs. »

La société de conseil et fournisseur de services managés francilien NetXP a ouvert une agence à Nantes début avril. Elle espère y compter une dizaine de collaborateurs au plus tard dans deux ans.

Fondé en 2001, le prestataire francilien NetXP n'avait pas, jusqu'ici, éprouvé le besoin de s'implanter hors de son fief pour se développer. Début avril, cette société de conseil (sécurité, cloud, réseaux et télécoms) et fournisseur de services managés (infogérance, hébergement sur mesure, SOC labellisé CERT) a changé son fusil d'épaule. Elle a ouvert une agence à Nantes située au 12 avenue Carnot. Chargé de couvrir le grand-ouest, le point de présence est piloté par Pierre-Emmanuel Masson, un ancien de chez Wavestone et de Gigalis qui baigne dans le tissu économique local. Pour l'heure, l'homme est le seul représentant de NetXP à Nantes. Il devrait être rejoint par trois consultants avant la fin de l'année et être entouré d'une dizaine de collaborateurs d'ici un an et demi à deux ans.

Ouvrir en région pour accéder à un nouveau vivier d'embauches

« Nous avons aussi étudié la possibilité de nous installer à Toulouse, Lille, Lyon et Bordeaux. Notre choix s'est porté sur Nantes notamment parce que la concurrence y est moins forte sur nos activités, que de beaux prospects y sont présents, et que le vivier de compétences local renferme les types de profils que nous recherchons », explique Michaël Briquet, le directeur associé de NetXP. Elargir ses capacités à recruter est une vraie nécessité pour que l'entreprise aux 100 salariés maximise son potentiel de croissance. *« En 2017, nous avons dégagé 10% de chiffre d'affaires supplémentaires et un REX d'environ 10%. Nous aurions pu faire beaucoup mieux avec davantage de collaborateurs »*, indique le dirigeant.

A l'issue de son exercice fiscal en cours, NetXP pense cette fois-ci dépasser les 10% de croissance. Si les prestations de conseil qu'elle propose aux grandes entreprises sont sa principale source de revenus, elle compte aussi beaucoup sur ses services managés ciblant le mid-market pour stimuler ses facturations. Ils permettent en effet à l'entreprise de bénéficier d'un effet de levier induit par le fait qu'elle délivre ces prestations via un effectif mutualisé.

Par Fabrice Alessi

NetXP choisit Nantes pour sa première incursion régionale

11/05/2018 29 0

Partager sur Facebook Tweeter sur twitter

Fondé en 2001, le prestataire francilien NetXP n'avait pas, jusqu'ici, éprouvé le besoin de s'implanter hors de son fief pour se développer. Début avril, cette société de conseil (sécurité, cloud, réseaux et télécoms) et fournisseur de services managés (infogérance, hébergement sur mesure, SOC labellisé CERT) a changé son fusil d'épaule. Elle a ouvert une agence à Nantes située au 12 avenue Carnot.

Chargé de couvrir le grand-ouest, le point de présence est piloté par Pierre-Emmanuel Masson, un ancien de chez Wavestone et de Gigalis qui baigne dans le tissu économique local. Pour l'heure, l'homme est le seul représentant de NetXP à Nantes. Il devrait être rejoint par trois consultants avant la fin de l'année et être entouré d'une dizaine de collaborateurs d'ici un an et demi à deux ans.

Ouvrir en région pour accéder à un nouveau vivier d'embauches

« Nous avons aussi étudié la possibilité de nous installer à Toulouse, Lille, Lyon et Bordeaux. Notre choix s'est porté sur Nantes notamment parce que la concurrence y est moins forte sur nos activités, que de beaux prospects y sont présents, et que le vivier de compétences local renferme les types de profils que nous recherchons », explique Michaël Briquet, le directeur associé de NetXP. Elargir ses capacités à recruter est une vraie nécessité pour que l'entreprise aux 100 salariés maximise son potentiel de croissance. « En 2017, nous avons dégagé 10% de chiffre d'affaires supplémentaires et un REX d'environ 10%. Nous aurions pu faire beaucoup mieux avec davantage de collaborateurs », indique le dirigeant.

A l'issue de son exercice fiscal en cours, NetXP pense cette fois-ci dépasser les 10% de croissance. Si les prestations de conseil qu'elle propose aux grandes entreprises sont sa principale source de revenus, elle compte aussi beaucoup sur ses services managés ciblant le mid-market pour stimuler ses facturations. Ils permettent en effet à l'entreprise de bénéficier d'un effet de levier induit par le fait qu'elle délivre ces prestations via un effectif mutualisé.

FLASH INFOS
L'actualité économique de votre région

PAYS :France
PAGE(S) :1
SURFACE :5 %
PERIODICITE :Quotidien

► 15 mai 2018 - N°2664 - Edition Paris Ile-de-France Centre Val-deLoire

92 / INFORMATIQUE : NetXP s'implante à Nantes

Le prestataire de conseils et services informatiques **NETXP** / **T** : 01.46.48.26.00 (*siège à Boulogne Billancourt*) **a procédé au début du mois d'avril 2018 à l'ouverture à Nantes de son premier bureau en dehors d'Ile de France**. Le nouveau site doit permettre à la société de couvrir le Grand-Ouest et compter trois collaborateurs rapidement, pour un objectif d'une dizaine de personnes dans deux ans. **www.netxp.fr**

Cybersécurité – Qu'est-ce qu'un Wireless Intrusion Prevention System?

La demande de mobilité des utilisateurs ayant augmenté, les réseaux Wifi se sont fortement développés ces dernières années. De ce fait, et au vu de l'accès au réseau que ce service propose, de multiples attaques existent, engendrant une nécessité d'utiliser des systèmes de défense plus ou moins perfectionnés. Les Wireless Intrusion Prevention System font partie de ces systèmes de défense.

Avis d'expert par Madeleine WOUTERS, Consultante Sécurité chez **NetXP**

Définition des Wireless Intrusion Prevention System : les WIPS

Étant données les caractéristiques physiques des systèmes, ces réseaux sont particulièrement sensibles à des attaques bien spécifiques (un VPN vous protège par exemple des attaques man-in-the-middle en chiffrant vos données et en les isolant dans un tunnel privé). Celles-ci vont utiliser le fait que l'on puisse facilement intercepter ou encore envoyer des trames sur le trafic radio. Ces attaques radio peuvent aller de l'écoute simple des machines présentes à l'installation de points d'accès illégitimes (Rogue AP) en passant par l'imitation d'un point d'accès ou encore un brouillage radio.

Afin de prévenir ces attaques au mieux, les Wireless Intrusion Prevention System (WIPS) sont utilisés. Ce sont des systèmes permettant l'écoute radio et la reconnaissance de modèles d'attaques afin d'alerter l'administrateur du système de la menace.

Un WIPS est composé de trois parties : un système radio permettant d'écouter le trafic, un serveur de management, permettant de stocker l'ensemble des données et enfin une console de management, permettant à l'utilisateur d'avoir une interface facile d'utilisation.

Différents types de solutions sont possibles, selon l'utilisation qui sera faite du WIPS :

- Integrated WIPS : le point d'accès Wifi scanne le réseau lorsqu'elle ne reçoit ni n'envoie rien. Il s'agit de la solution la moins chère ;
- Hybrid WIPS : le point d'accès Wifi peut scanner le réseau, même durant l'envoi ou la réception de données de clients ;
- Overlay WIPS : il s'agit d'une solution WIPS indépendante, comprenant des boîtiers spécifiques.

Selon les solutions utilisées, le WIPS peut reconnaître différentes attaques, dont au minimum la détection d'un point d'accès illégitime (Rogue AP) sur le réseau et la détection de points d'accès de réseaux voisins (exemple : entreprise voisine, réseaux particuliers). Certaines plateformes donnent également la possibilité de réagir face à une attaque de déni de service ou DoS, c'est-à-dire de pouvoir éventuellement configurer un seuil de tolérance et moduler la réaction à avoir une fois ce seuil dépassé. La plupart des dispositifs permettent aussi de lancer des contre-attaques à ces attaques radio. Elles se concrétisent souvent par l'envoi de trames de dés-association.

Limites à l'utilisation des WIPS

Afin de se protéger, il est pertinent d'acquérir des solutions WIPS et de les configurer suivant son besoin. L'intérêt est ici d'avoir une réaction rapide à l'attaque, voire immédiate dans le meilleur des cas. La personnalisation peut passer par la mise en place de filtres, permettant alors de mettre

en évidence le point d'accès illégitime pour déclencher ensuite une réponse. Un bon moyen de se protéger serait également d'envoyer un rapport aux équipes d'administration du réseau, dès qu'une attaque de ce type est repérée. De cette manière, elles peuvent réagir manuellement et rapidement. Enfin, automatiser la réponse à incident en fonction de l'attaque repérée semble être le moyen le plus simple de procéder, mais peut amener des risques de faux positifs.

Cependant, peu de solutions de WIPS intégrés proposent de telles possibilités de personnalisation aussi poussées. La plupart proposent un classement manuel des points d'accès détectés, c'est-à-dire déclarer ces points d'accès voisins comme connus et donc non dangereux. Elles proposent également la possibilité de créer des rapports ponctuels ou selon une fréquence donnée, sur des sujets divers, sans entrer dans le détail des attaques détectées. De plus, la contre-mesure permettant de se protéger contre ces attaques radio utilise une action qui s'apparente à du déni de service ou DoS, par l'envoi de trames de dés-association. Outre l'illégalité de cette réaction (tout du moins en France), elle peut s'avérer inefficace. En effet, certains appareils utilisent l'amendement 802.11w sorti en 2009 qui protège les appareils de certaines attaques DoS par l'envoi de trames de management et notamment les attaques DoS par trames de dés-association ou de dés-authentification.

Conclusion

Les WIPS peuvent être des outils très utiles pour la sécurisation d'un service Wifi. Ils permettent entre autres de détecter des points d'accès voisins ou encore illégitimes et d'avoir une analyse des trames circulant dans le périmètre physique du réseau Wifi. Ils offrent une possibilité de contre-attaque sous forme d'envoi de trames de dés-association. Cependant, la performance de ces outils dépend en grande partie de l'utilisation qui en est faite et de sa configuration, malheureusement limitée dans le cas de WIPS intégrés, ainsi que par les protections mises en place sur les points d'accès illégitimes.

Vous avez aimé cet article ? Alors partagez-le en cliquant sur les boutons ci-dessous :


(Pas encore noté)
Loading...

Vous aimerez aussi :

Cybersécurité – 6 astuces pour protéger votre réseau Wifi

Cybersécurité : Les trois mesures à prendre pour protéger la communication unifiée

Piratage – LastPass victime d'une intrusion

Cybersécurité : Les vecteurs de menaces les plus couramment négligés

Mots clés : cyberattaques, Cybersécurité, Hybrid WIPS, Integrated WIPS, Overlay WIPS, point d'accès, protection, Wifi, WIPS, Wireless Intrusion Prevention System

ARTICLE PRECEDENT

Cliquez ici pour annuler la réponse.

Connexion via :

Nom (required)

Mail (required)

Site Web (optionnel)

Notifiez-moi des commentaires à venir via e-mail. Vous pouvez aussi vous abonner sans commenter.

Wireless Intrusion Prevention System (WIPS) : le point sur leur degré d'efficacité

29-05-2018

Réagir | Imprimer | Envoyer | S'abonner

Selon le cabinet d'expertise parisien NetXP, mieux vaudrait se méfier de ces solutions destinées à protéger les réseaux WiFi. Leurs performances variant selon l'utilisation que l'on en fait, mais aussi selon le degré de sophistication de leurs fonctionnalités.

"Integrated", "hybrid" ou bien "overlay", les WIPS se déclinent en trois types de solutions de qualité variable.
Image Pixabay

Attention aux réseaux WiFi ! Nombreux sont les internautes qui font confiance aux connexions WiFi supposées être sécurisées, par exemple dans les banques, les hôtels ou les aéroports. Mais il n'en est rien ! Au contraire, les réseaux WiFi, et particulièrement publics, sont devenus une cible de choix pour les hackers. Pour lutter contre ce danger, des systèmes de défense ont été développés par les éditeurs de solutions de cybersécurité, à l'instar des Wireless Intrusion Prevention System (WIPS). Capables de détecter une attaque sur le réseau, ces systèmes d'écoute radio ont fait leurs preuves. Or, pour le cabinet d'expertise spécialisé en infrastructures techniques du système d'information NetXP, leur efficacité dépend avant tout de l'utilisation que l'on en fait. NetXP nous livre son point de vue sur les avantages et les inconvénients des WIPS.

Des attaques visant le trafic radio

Aujourd'hui, les cyberpirates ont considérablement affûté leurs armes en matière d'attaque des réseaux WiFi. Ils s'attaquent désormais au trafic radio du réseau, afin d'intercepter les caractéristiques physiques des systèmes ou encore d'y envoyer des trames. « Ces attaques radio peuvent aller de l'écoute simple des machines présentes à l'installation de points d'accès illégitimes (Rogue AP) en passant par l'imitation d'un point d'accès ou encore un brouillage radio », précise Madeleine Wouters, consultante sécurité chez NetXP.

Surveiller le trafic radio

D'où l'idée de créer des solutions de défense, basées sur un système radio capable d'écouter le trafic, telles que les WIPS. Ces solutions se composent de trois éléments, à savoir un système radio, un serveur de management chargé de stocker les données ainsi qu'une console de management, qui sert d'interface à l'utilisateur. Parmi les fonctionnalités de ces solutions, et selon leur degré de sophistication, figure la possibilité de reconnaître différentes attaques telles que la détection d'un point d'accès illégitime, que l'on appelle Rogue AP, sur le réseau. Ou la détection de points d'accès de réseaux environnants, tels que ceux d'une entreprise voisine ou d'un réseau de particuliers. « Certaines plateformes donnent également la possibilité de réagir face à une attaque de déni de service ou DoS, c'est-à-dire de pouvoir éventuellement configurer un seuil de tolérance et moduler la réaction à avoir une fois ce seuil dépassé. La plupart des dispositifs permettent aussi de lancer des contre-attaques à ces attaques radio. Elles se concrétisent souvent par l'envoi de trames de désassociation », ajoute Madeleine Wouters.

L'importance de la personnalisation de la configuration

Solution miracle ? Selon le cabinet d'expertise, pas tant que ça ! Tout dépend de l'utilisation que l'on en fait. L'intérêt étant de configurer ces WIPS selon des besoins spécifiques. « Il s'agit d'avoir une réaction rapide à l'attaque, voire immédiate dans le meilleur des cas. La personnalisation peut passer par la mise en place de filtres, permettant alors de mettre en évidence le point d'accès illégitime pour déclencher ensuite une réponse », estime la consultante. Autre solution : automatiser les réactions à un incident en fonction du type d'attaque, au risque de déclencher des fausses alertes.

Les limites de ces solutions

Le cabinet estime qu'il n'existe en fait que peu de solutions WIPS dotées de telles capacités. La plupart (WIPS intégrés ou hybrides) se restreignant à des fonctionnalités plus basiques, telles que le classement manuel des points d'accès détectés comme les points d'accès voisins, ou encore la création de rapports peu exhaustifs. « De plus, la contre-mesure permettant de se protéger contre ces attaques radio utilise une action qui s'apparente à du déni de service ou DoS, par l'envoi de trames de désassociation. Outre l'illégalité de cette réaction (du moins en France), elle peut se révéler inefficace. En effet, certains appareils utilisent l'amendement 802.11w, sorti en 2009, qui protège les appareils de certaines attaques DoS par l'envoi de trames de management et notamment les attaques DoS par trames de désassociation ou de désauthentification ».

Ségolène Kahn