IOSR Journal Of Humanities And Social Science (IOSR-JHSS)
Volume 29, Issue 11, Series 2 (November, 2024) 48-58
e-ISSN: 2279-0837, p-ISSN: 2279-0845.
www.iosrjournals.org

Etude Comparative Des Systèmes De Prévention D'intrusion Pour La Protection D'un Réseau D'entreprise

Par Ass. Alexandre Nteziyaremye Ruhozaho

Résumé
Actuellement, suite à l'évolution technologique, la plupart des petites et moyennes entreprises (PME) se heurtent au défis de cyberattaques suite à l'usage de la connexion Internet non sécurisée ou sécurisé via l'anti-virus avec les mécanismes passifs qui ne nous garantissent pas leur mode de fonctionnement technique informatique sûr.
Pour ce faire, plusieurs études ont été menées sur les attaques réseaux et la façon de protéger le réseau d'une entreprise adoptant ainsi des solutions passives telles que les HIDS, NIDS et NIPS qui présentent toujours des insuffisances même quand elles fonctionnent correctement à cause d'une mauvaise utilisation (DAGON, 2006). Et comme les systèmes de sécurité actuels ont tendance à intégrer les IDS et IPS directement dans les firewalls, et dans l'antivirus de façon à renforcer la coopération entre ces équipements de sécurité complémentaires, dans ce cas l'usage de la technologie antivirus et/ou les firewalls pour faire les tests dans notre étude.
Ainsi donc, il est impérieux d'intégrer la sécurité appropriée pouvant leur faciliter la tâche pour bien améliorer leur système et leur mode de gestion au quotidien avec une garantie satisfaisante répondant valablement à leurs besoins.
C'est pourquoi, nous allons faire une étude comparative des IPS logiciel (HIPS), pour voir de quelle manière les entreprises peuvent faire un bon choix et arriver à bien sécuriser leurs réseaux, parce que les entreprises sont toujours victimes d'attaques malgré le déploiement d'IPS sur le réseau.
Mots clés : *Etude comparative-Systèmes de prévention d'intrusion et protection d'un réseau d'entreprise*

Date of Submission: 24-10-2024 Date of Acceptance: 04-11-2024

I. Introduction

À l'ère numérique actuelle, il est plus essentiel que jamais de protéger votre réseau contre les cybermenaces. Un Système de prévention des intrusions (IPS) est un outil essentiel de sécurité réseau. Aucun système d'information n'est sûr à 100%, parmi les préceptes connus sur la sécurité informatique se trouve celui énonçant que, pour une entreprise connectée à l'Internet, le problème aujourd'hui n'est plus de savoir si elle va se faire attaquer, mais quand cela va arriver; une solution possible est alors d'essayer de repousser les risques dans le temps par la mise en œuvre de divers moyens destinés à augmenter le niveau de sécurité.

Pour contrer les menaces d'intrusion, les entreprises se tournent de plus en plus vers les solutions de détection d'intrusion, dont les possibilités faramineuses sont vantées par les sociétés éditrices de ces logiciels. Mais le décalage entre le discours commercial et les possibilités techniques réelles de ces produits peut être important, et les conséquences fâcheuses lorsqu'il s'agit de sécurité de l'information

En matière de cyber-sécurité, les attaquants disposent d'un avantage déloyal parce qu'ils peuvent parvenir à leurs fins à cause d'une faiblesse dans les défenses, tandis que les entreprises doivent surveiller et sécuriser la surface d'attaque de l'entreprise dans son ensemble. Les défenseurs sont également entravés par des volumes de données de sécurité considérables et en croissance constante, par les silos de données de sécurité et par un incapacité à corréler les données de manière à leur permettre de gérer les mesures correctives et les autres activités de sécurité de manière cohérente au sein de l'entreprise.

La sécurisation et la protection totale d'un réseau impliquent un certain nombre de défis à relever pour les organisations. Même si nous pouvons mentionner ces défis, les informations concernant l'inefficacité de la protection réseaux, ne sont pas exhaustives.

L'entreprise peut faire face à d'autres circonstances dont nous ne faisons pas mention dans notre travail. La solution à ces défis, qu'ils soient abordés ici ou non, est la même : les entreprises devez surveiller en temps réel et archiver toutes données qui circulent sur les réseaux, par les outils spécialisés dont fait partis les IDS/IPS. Mais les attaques font toujours face dans les réseaux des entreprises et qui continuent à causer des dégâts. Ceux IPS ne sont-ils pas capables de mettre en termes aux attaques réseaux, pour qu'on puisse cette fois-ci avoir un réseau dont la sécurisé tend cent pourcents. Si nous prenons comme exemples les attaques les plus connues dans les mondes de affaire ces cinq dernières années et qui ont marqué les esprits des ingénier en sécurité réseau.

Ces attaques sont dites de l'inefficacité de systèmes de protections du réseau et qui ont effets sur la vie quotidienne

de l'entreprise. Le moi janvier 2017 a été marqué par le piratage du réseau social Instagram.

Les numéros de téléphone et les adresses e-mail de 6 millions d'utilisateurs ont été rendus publics et ils étaient mis en vente sur le darknet. Même si aucun mot de passe n'a été récupéré, certaines informations ont de la valeur puisqu'elles appartiennent aux grand célébrités.

Les dirigeants d'Instagram pensent que le pirate "Doxagram" a exploité la faille d'une API qu'ils assurent avoir corrigée aujourd'hui. (https://www.lemonde.fr/: 11h30 10 février 2024) Equifax, société de crédit américaine, a révélé avoir subi une attaque en juillet 2017 (https://blog.avast.com/: 11h 10 février 2024) .

Les données personnelles (noms, dates de naissance, numéros de sécurité sociale, permis de conduire) de quelques 143 millions de clients américains, canadiens et britanniques seraient concernés ainsi que 200 000 numéros de carte bancaires. Les plaintes contre l'entreprise s'accumulent ainsi que les soupçons de délit d'initié.

En effet, d'une part, la vulnérabilité d'Apache Struts utilisée par les hackers était connue depuis mars et d'autre part, plusieurs cadres de l'entreprise ont fortement vendu des actions quelques jours avant que la faille de sécurité ne soit rendue publique (https://secludit.com/ : 10h15 15 février 2024). Les problèmes du manque un bon système de protection contre les attaques réseaux rendent l'entreprise faible sur poussières plans.

La présence d'un intrus dans un réseau et s'il n'est pas détecté à temps, il peut causer des dégâts et qui auront les effets néfastes sur la vie de l'entreprise et de ses employés, à titre d'exemple nous pouvons citer : Perte de productivité : le fait que les pirates accèdent au réseau, peut faire perdre du temps à vos employés en les envoyant des mails tout en se passant comme un des leurs, et entraînant ainsi une perte de productivité, car les employés vont toujours vouloir répondre à ces mails.

Fuites d'informations sensibles ou confidentielles : des données, telles que des informations relatives aux produits, des informations propriétaires, des secrets industriels, des informations sur l'entreprise ou d'autres données sensibles, peuvent être divulguées, par inadvertance ou non, via le faux chate que peut créer un pirate dans le réseau de l'entreprise.

Une enquête (https://www.microfocus.com/ : 9h30 19 février 2024) Osterman Research a révélé que 14 % des organisations avaient connu des fuites d'informations sensibles ou confidentielles via les faux chates, 11 % via Facebook, 9 % via Twitter et 10 % via LinkedIn. Cette perte de données peut entraîner des pertes d'argent astronomiques en raison d'une réputation compromise, de litiges éventuels et de la perte d'avantage concurrentiel. Harcèlement et cyber intimidation : grâce à l'accès au réseau interne, les pirates peuvent en toute facilité harceler ou intimider des collègues, des sous-traitants, des clients, etc. Cela peut créer un environnement de travail hostile et mener à des plaintes, à des poursuites et à une rotation plus importante du personnel.

Communication inappropriée : les pirates s'ils demeurent invisibles, peuvent facilement partager des textes ou des images obscènes, vulgaires ou inappropriés à la fois en interne et en externe via votre réseau. Perte de contrôle du message de la marque : grâce à l'accès à votre, les pirates peuvent accéder à vos comptes des réseaux sociaux et publier des informations en ligne à propos de votre entreprise avec votre identité.

Celles-ci peuvent être liées à votre entreprise et pourraient influencer la façon dont votre marque est perçue. Et pourraient publier des messages et des images inappropriés sur la page de l'entreprise (que ce soit par inadvertance ou par malveillance), nuisant ainsi à votre marque (https://www.imt.fr/ : 3h 22 février 2024).

Violations de la confidentialité : de nombreuses entreprises traitent des informations protégées, notamment des données financières (informations de compte, numéros de sécurité sociale, informations boursières, accords commerciaux), de santé (données médicales protégées) et gouvernementales (documents confidentiels ou classés).

Ces types d'informations pourraient être volés et partagés sur internet ou vendus aux ennemies et entraînant des violations de la confidentialité, ainsi que des problèmes d'espionnage ou de trahison.(https://www.lemonde.fr/ : 10h 22 février 2024)

Perte d'avantage concurrentiel : votre entreprise peut disposer de nombreuses idées, secrets ou données propriétaires qui vous procurent un avantage sur la concurrence. Une fois ce type d'informations volé, entraînant ainsi la perte de cet avantage concurrentiel.

Etant donné que, les attaques réseau sont toujours multiples pas parce que il y a pas un système de sécurité, mais parce que dans certaines sociétés on utilise plusieurs système sans en maîtriser le fonctionnement, ce qui les amènent vers un système non efficace.

Tenant compte de tous ces problèmes que nous venons d'énumérer ci-dessus, nous y avons dégagé une seule et unique question spécifique qui est formulée de manière suivante et qui est la problématique de cette étude :

Comment peut-on aider les entreprises à faire un bon choix d'un système de prévention d'intrusion ?

L'hypothèse étant considérée comme une réponse que tout chercheur se propose de façon provisoire aux questions de son étude, notre réponse s'ouvre provisoirement à la question posée dans la problématique :

Pour aider les entreprises à faire un choix d'un système de prévention d'intrusion, une étude comparative de ces systèmes serait une solution pour trouver les critères de choix et permettrait une bonne protection contre les attaques réseau.

II. Méthodologie Appliquée

Cette partie reprend respectivement l'instrument utilisé pour la récolte des données, la population et l'échantillon de

l'étude ainsi que les techniques d'analyse et de traitement des données

Instrument de recherche

Notre étude étant purement descriptive et comparative, la réalisation de cette recherche a fait recours à la méthode de l'enquête par questionnaire et qui vise à recueillir les réponses de la part des entreprises œuvrant dans la Ville de Goma.

Via le logiciel SPHINX Plus [2] qui est un logiciel d'enquête et d'analyse des données. Selon Florence (2006), Avec ce logiciel nous partirons du traitement de l'enquête comportant l'étape de la rédaction du questionnaire et l'analyse des résultats enfin l'analyse statistique de données de toute nature.

- Le traitement statistique des données récoltées , en les organisant et de traiter les d'une manière quantitative sous forme des tableaux des effectifs et des graphiques ;
- L'analyser les opinions émises par les enquêtés en vue d'en ressortir les éléments similaires pendant l'étape de catégorisation pour bien faire d'étude et analyse de l'existant;
- La comparaison des solutions logiciels IPS par des simulations avec les outils dédiées à la sécurité informatique dans un laboratoire de simulation de teste d'intrusion physique avec des machines physiques.

Dans cet article nous allons faire la comparaison en passant en paramètre critères suivants :

- Les capacités de détection
- La compréhension du contexte
- L'utilisation du renseignement sur les menaces
- La nature de la licence du système d'exploitation
- Le coût d'implantation

La population et l'échantillon de l'étude

La population concernée pour cette étude est composée des entreprises de la ville de Goma basée sur la description des IPS et la situation actuelle de sécurité réseau.

Pour faire, nous avions mené une enquête dans certaines entreprises de la ville de Goma et avec comme critère de sélection, avoir un réseau en son sein. Lors du calcul de notre panel représentatif formant l'échantillon d'enquête nous avions ciblé 100 entreprises comme la taille de notre échantillon,

Ainsi, nous avions lancé et soumis 100 questionnaires à nos enquêtés et qui ont été bel et bien recueillis comme tels avec les mêmes effectifs.

Tableau n°1 : Présentation de nos enquêtés selon leurs secteurs d'activité

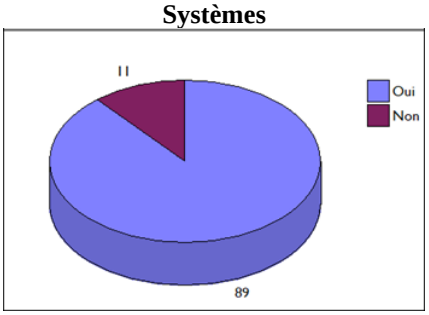
Secteur d'activité	Nombre de citations	Fréquence
Administration (public)	15	15,0%
Education	30	30,0%
Transport	21	21,0%
Commerce et vente	18	18,0%
Banque	8	8,0%
Industrie	8	8,0%
Autres	0	0,0%
TOTAL OBS.	**100**	**100%**

Source : Résultats de nos analyses avec SPHINX Plus [2]

Le panel représentatif ayant participé à notre enquête comme le montre ce tableau ci- dessus, est équilibré avec 15,0% de réponses émanant du secteur public, 8,0% de l'industrie, 21,0% Transport, 8,0% du secteur Banque, 30,0% du secteur de l'éducation, 0,0% dans autres secteurs d'activités que nous n'avions pas mentionné sur les questionnaires et de celui de commerce et vente qui vienne en tête avec 18,0%.

Comme l'indique le graphique ci-dessous que, 89,0 % d'entreprises interrogées affirment qu'elles ont déjà été touchées par au moins une cyber-attaque et 11,0 % ont répondu qu'ils n'ont jamais été victimes d'une attaque sur leurs réseaux. Nous nous pensons, qu'ils ne reconnaissent pas peut qu'ils sont victime même, jusqu'à cette date, manque de système de sécurité.

Graphique N°1 : Présentation Graphique De Nos Enquêtés Selon Leurs Cyber-Attaques Dans Leurs Systèmes



Source : Résultats De Nos Analyses Avec SPHINX Plus [2]

III. Concepts Usuels

La sécurité informatique : c'est un terme large qui réunit les moyens humains, technologiques, organisationnels qui tentent de garantir certaines propriétés d'un système d'information. (L. BLOCH, 2018).

La sécurité IT (ou ***sécurité informatique***) est un dispositif vaste et multiforme visant à protéger un réseau informatique et ses données contre toute violation, fuite, publication d'informations privées ou attaque.(Hewlett Packard, 2024)

Virus : C'est un petit programme qui a la faculté de se reproduire automatiquement. Il va recopier son propre code tel quel, ou en le modifiant, dans des éléments qui sont déjà dans l'ordinateur. Le plus souvent son but est de nuire.

Denis de service : c'est une attaque qui consiste à paralyser un service ou un réseau complet, et l'utilisateur ne peut plus accéder au ressources, Les deux exemples principaux, sont le " ping flood " ou l'envoi massif de courrier électroniques pour saturer une boîte aux lettre (mailbombing).

Vulnérabilité : est une faiblesse d'un système de sécurité se traduisant par une incapacité partielle de celui-ci à faire face aux menaces informatiques qui le guettent. Par exemple, une erreur d'implémentation dans le développement d'une application, est exploitée pour nuire à l'application (pénétration, refus de service, ...etc.). Elle peut être également provenir d'une mauvaise configuration. (https://nvd.nist.gov/cwe.cfm#cwes: 10h 25 février 2024).

Menace : elle désigne l'exploitation d'une faiblesse de sécurité par un attaquant, que ce soit interne ou externe a l'entreprise. La probabilité qu'elle soit une faille de sécurité, est évaluée par des études statistiques même si elle est difficile à réaliser.

Risque : les menaces engendrent des risques et des couts humains et financiers : perte de confidentialité des données sensibles, indisponibilité des infrastructures et des données, dommages pour le patrimoine intellectuel et la notoriété. Les risques peuvent survenir si les systèmes menacés présentent des vulnérabilités. (Sofiane MAZA, 2010)

Une attaque : est le résultat de l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel, erreur de configuration,...etc.) à des fins non connues par l'exploitant du système et il est généralement préjudiciables.

Intrusion : c'est réaliser une attaque ou une menace pour un système d'informatique, pour que ce dernier ne soit plus en sécurité.

Un pare-feu : Un pare-feu est logiciel et/ou matériel qui filtre et protège un système en bloquant les connexions venant de l'extérieur (entrées) ou de l'intérieur (sorties) pour empêcher ou autoriser l'accès à des services Web. Il permet aussi de faire de la translation d'adresse pour servir de routeur. Si le système est plus sophistiqué (et surtout plus récent), il peut prendre automatiquement des mesures pour empêcher ou stopper l'attaque en cours. Par exemple, il coupera les connexions suspectes ou même (pour une attaque distante) reconfigurera le pare-feu pour qu'il refuse tout ce qui vient du site incriminé. Il pourra également prévenir l'administrateur. (Farah Jemili, 2013: p50)

Serveur proxy : Un serveur proxy appelé aussi serveur mandataire, est un composant logiciel informatique qui joue le rôle de l'intermédiaire entre deux machines pour surveiller leurs échanges. La plupart du temps le serveur proxy est utilisé pour le web, il s'agit alors d'un proxy HTTP. Toutefois il peut exister des serveurs proxy pour chaque protocole applicatif.

Systèmes de prévention d'intrusion ou **Intrusion Prevention System (IPS):** Un système de prévention d'intrusion est un ensemble de composants logiciels et/ou matériels dont la fonction principale est d'empêcher toute activité suspecte détectée au sein d'un système.

Système détection d'intrusion ou **Intrusion Detection System (IDS):** la détection d'intrusions consiste à analyser les informations collectées par les mécanismes d'audit de sécurité, à la recherche d'éventuelles attaques. Bien qu'il soit possible d'étendre le principe, nous concentrerons sur les systèmes informatiques. Les méthodes de détection d'intrusion diffèrent sur la manière d'analyser le journal d'audits. Un **système de prévention et de détection des intrusions,** ou **IDPS** (Intrusion Detection and Prevention System), est une solution qui permet de surveiller un réseau à la recherche de menaces et d'agir de manière à contrer celles qui ont été détectées. (https://www.redhat.com/: 10h05 25 février 2024)

IV. Présentation Des Résultats

Résultats du logiciel SPHINX Plus [2]

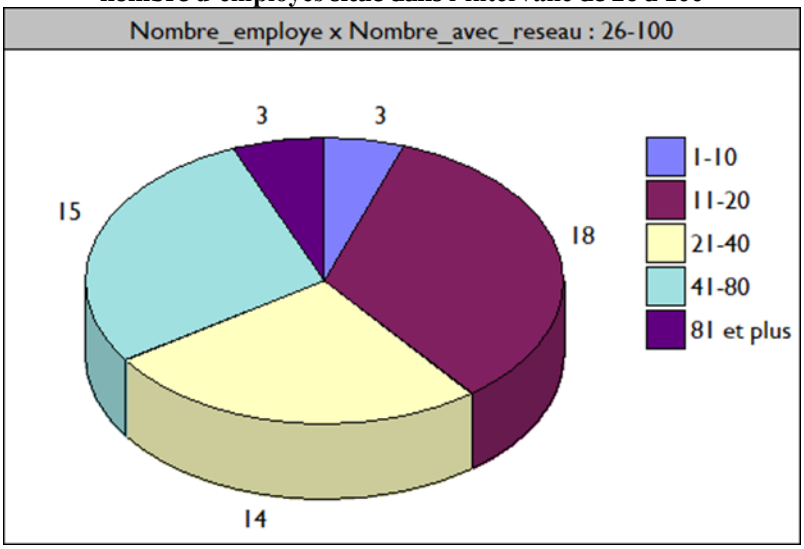
Comme nous l'avons énoncé ci-haut nos résultats ont été réalisés dans le logiciel SPHINX Plus 2 et se présentent de la manière suivante :

Tableau n°2 : Présentation de nos enquêtés faisant usage un réseau dans leur système

Nombre d'employés	Nombre d'employés travaillant au quotidien sur le réseau					TOTAL
	1-10	11-20	21-40	41-80	81 et plus	
0-25	9,0	14,0	1,0	0,0	0,0	24,0
26-100	3,0	18,0	14,0	15,0	3,0	53,0
101-250	0,0	1,0	7,0	5,0	6,0	19,0
251-1000	0,0	0,0	0,0	0,0	4,0	4,0
Plus de 1000	0,0	0,0	0,0	0,0	0,0	0,0
TOTAL	**12,0**	**33,0**	**22,0**	**20,0**	**13,0**	**100,0%**

Source : Résultats de nos analyses avec SPHINX Plus [2]

Graphique n°2 : Présentation graphique de nos enquêtés faisant usage un réseau dans leur système avec nombre d'employés situé dans l'intervalle de 26 à 100



Source : Résultats de nos analyses avec SPHINX Plus [2]

Ce tableau croisé de deux variables associé à ce graphique, présentent les résultats issus de la comparaison des effectifs entre le nombre d'employés que compte les entreprises et le nombre d'employés qui travaillent sur l'outil informatique connecté au réseau dans chaque secteur d'activité que nous avions ciblé.

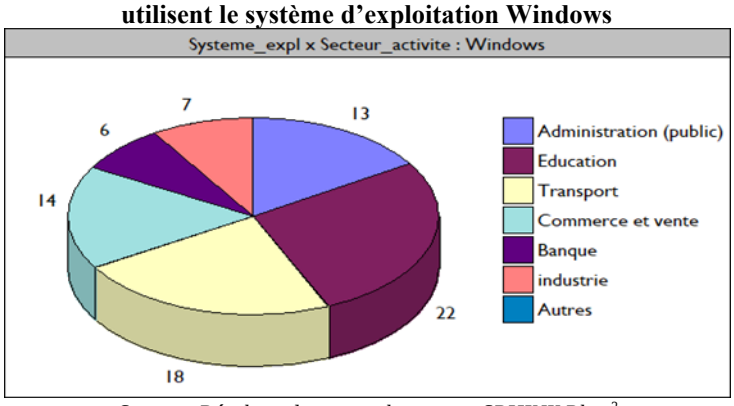
Un effectif de 9 de nos enquêtés soit 9,0% situé dans l'intervalle de 0-25 et de 1-10 indiquant respectivement le nombre d'employés et ceux travaillant au quotidien sur le réseau, 14 de nos enquêtés soit 14,0% situé dans l'intervalle de 0-25 et de 11-20, 1 de nos enquêtés soit 1,0% situé dans l'intervalle de 0-25 et de 21-40 et 0 soit 0,0% pour le reste de cette ligne de l'intervalle de 0-25 donc de l4intervavalle de 40-80 et 81 et plus.

Tableau n°3 : Présentation de nos enquêtés par rapport secteur d'activité et les systèmes d'exploitation utilisés

Système d'exploitation installé sur ordinateur	Secteur d'activité							TOTAL
	Administration (public)	Education	Transport	Commerce et vente	Banque	industrie	Autres	
Windows	13,0	22,0	18,0	14,0	6,0	7,0	0,0	**80,0**
Linux	2,0	8,0	3,0	4,0	2,0	1,0	0,0	**20,0**
Autre	0,0	0,0	0,0	0,0	0,0	0,0	0,0	**0,0**
TOTAL	**15,0**	**30,0**	**21,0**	**18,0**	**8,0**	**8,0**	**0,0**	**100,0%**

Source : Résultats de nos analyses avec SPHINX Plus [2]

Graphique n°3 : Présentation graphique de nos enquêtés par rapport secteur d'activité et qui utilisent le système d'exploitation Windows



Source : Résultats de nos analyses avec SPHINX Plus [2]

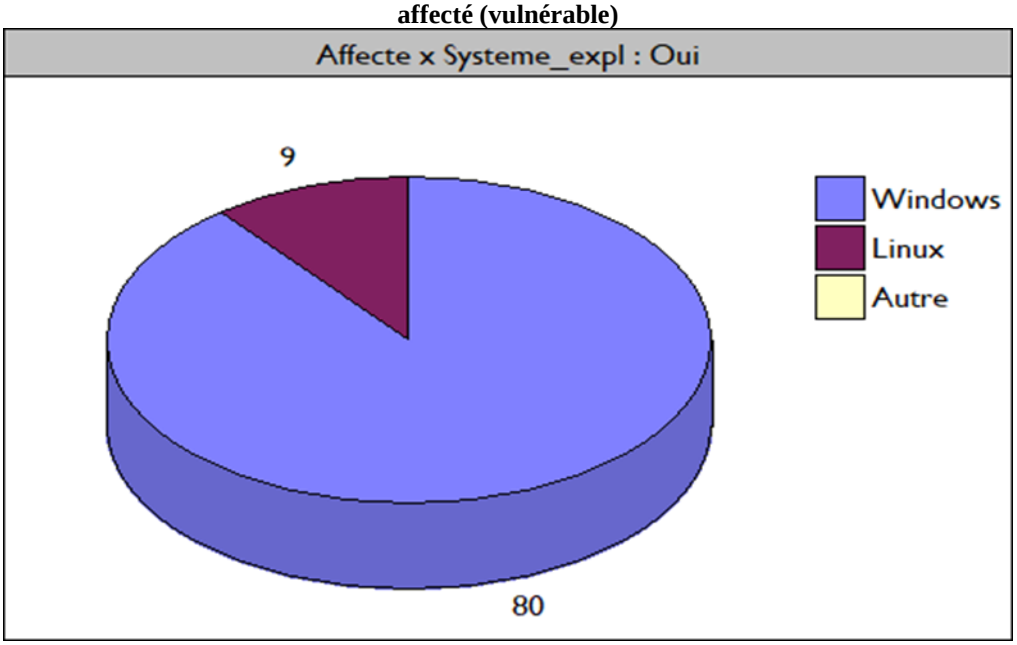
Selon l'usage de système d'exploitation, il sied de préciser que le système d'exploitation le plus utilisé c'est le Windows et représente 80,0% contre 20,0% pour Linux dans l'ensemble des secteurs d'activités ayant été ciblé dans notre panel représentatif.

Tableau n°4 : Présentation de nos enquêtés par rapport au système d'exploitation le plus affecté (vulnérable)

Déjà été affecté	Système d'exploitation utilisé			TOTAL
	Windows	Linux	Autre	
Oui	80,0	9,0	0,0	**89,0**
Non	0,0	11,0	0,0	**11,0**
TOTAL	**80,0**	**20,0**	**0,0**	**100,0%**

Source : Résultats de nos analyses avec SPHINX Plus [2]

Graphique n°4 : Présentation graphique de nos enquêtés par rapport au système d'exploitation le plus affecté (vulnérable)



Source : Résultats de nos analyses avec SPHINX Plus [2]

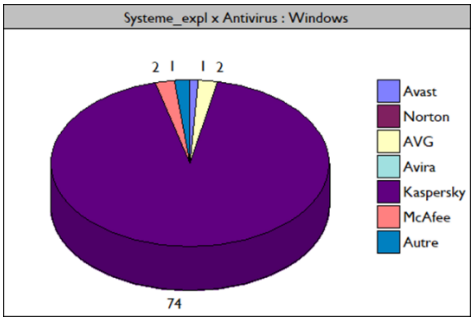
Partant des données présentés dans le tableau n°4, nous constatons que bon nombre d'entreprises qui utilisent le système d'exploitation Windows ont déjà connus beaucoup d'attaques et qui représentent 80,0% contre 9,0% par rapport à celles qui utilisent le système d'exploitation Linux. Par contre le reste qui n'a jamais été attaqué utilise le système d'exploitation seulement Linux et qui représente 11,0%

Tableau n°5 : Présentation de nos enquêtés par rapport au système d'exploitation et l'antivirus utilisé

Système d'exploitation	Antivirus utilisé							TOTAL
	Avast	Norton	AVG	Avira	Kaspersky	McAfee	Autre	
Windows	1,0	0,0	2,0	0,0	74,0	2,0	1,0	**80,0**
Linux	0,0	0,0	0,0	2,0	3,0	0,0	15,0	**20,0**
Autre	0,0	0,0	0,0	0,0	0,0	0,0	0,0	**0,0**
TOTAL	**1,0**	**0,0**	**2,0**	**2,0**	**77,0**	**2,0**	**16,0**	**100,0%**

Source : Résultats de nos analyses avec SPHINX Plus [2]

Graphique n°5 : Présentation graphique de nos enquêtés par rapport au système d'exploitation et l'antivirus utilisé



Source : Résultats de nos analyses avec SPHINX Plus [2]

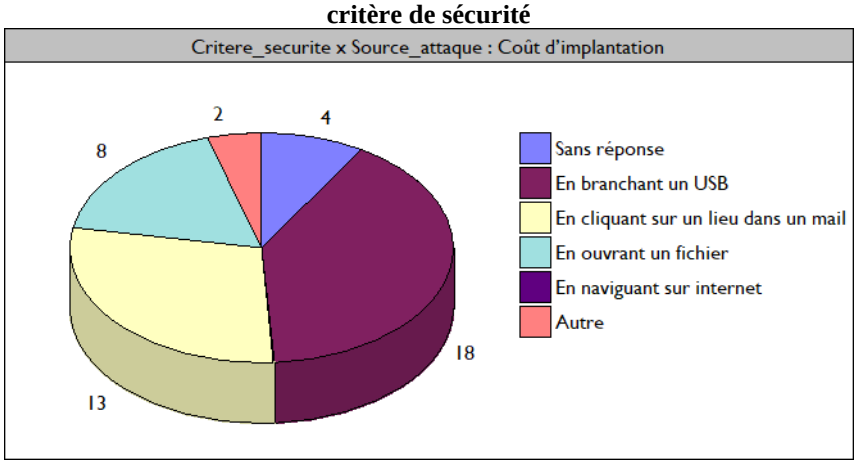
Parmi les solutions antivirus les plus utilisé par nos enquêtés sous Windows, nous voyons que Kaspersky vient en tête avec une fréquence de 74 soit 74,0% de nos enquêtés, suivi de AVG et McAfee avec une fréquence pour chacune de 2 soit 2,0% par après viennent Avast et les autres avec une fréquence de 1 soit 1,0% de nos enquêtés et les autres viennent Norton, Avira avec une fréquence de 0 soit 0,0% chacun.

Tableau n°6 : Présentation de nos enquêtés par rapport à la source d'attaque et le choix du critère de sécurité

Critère sécurité	Source d'attaque						TOTAL
	Sans réponse	En branchant un USB	En cliquant sur un lieu dans un mail	En ouvrant un fichier	En naviguant sur internet	Autre	
Coût d'implantation	4,0	18,0	13,0	8,0	0,0	2,0	**45,0**
Performance du système	1,0	14,0	3,0	6,0	0,0	3,0	**27,0**
Autre	6,0	7,0	2,0	1,0	1,0	11,0	**28,0**
TOTAL	**11,0**	**39,0**	**18,0**	**15,0**	**1,0**	**16,0**	

Source : Résultats de nos analyses avec SPHINX Plus [2]

Graphique n°6 : Présentation graphique de nos enquêtés par rapport à la source d'attaque et le choix du critère de sécurité



Source : Résultats de nos analyses avec SPHINX Plus [2]

45,0% des entreprises enquêtées choisissent leurs coûts d'implantation du système de sécurité, 27,0% font leurs choix en tenant en compte sur le système de sécurités par rapport à la performance et 28,0% font le choix n'est pas sur

base de la performance et ni du coût d'implantation. Pour les entreprises qui ont déjà été victimes d'une au plusieurs attaques, disent que les sources de ce menaces sont multiples selon le tableau n°6, avec 39,0% qui viennent sur les périphérique USB, 18,0% en cliquant sur les liens de mails, 16,0% leurs menaces viennent d'ailleurs, 15,0% en ouvrant des fichiers, 11,0% se sont abstenus et 1,0% dans en navigant sur internet.

V. Résultats De L'étude Comparative De IPS Et IDS

La Comparaison Des Ips

Dans cette partie nous voulons compares les IPS/IDS logiciels que nous avions vu qu'ils sont plus utilisés par nos enquêtés comme le montrent les résultats de l'enquête dans le premier chapitre.

AVG Internet Security

AVG Internet Security est un logiciel antivirus très populaire pour les systèmes d'exploitation Windows et Linux. À ses débuts en 1991, il a été développé par la société tchèque Grisoft basée à Brno, avant que les investisseurs de Benson Oak puis, plus récemment, Intel Capital et Enterprise Investors, n'entrent dans son capital en 1995, puis en 2005. Grisoft est devenue AVG Technologies le 21 janvier 2008. AVG était le sigle des mots anglais Anti-Virus Guard, A.V.G. signifie Anti-Virus of Grisoft.

L'antivirus AVG est une composante de la gamme de sécurité AVG qui contient un antivirus, un anti-espions, un anti-pourriels, un IDS/IPS et un pare-feu. Le logiciel est disponible en version gratuite (graticiel) ou par abonnement. AVG appartient au groupe Avast Software depuis l'année 2016.

Kaspersky Internet Security

Kaspersky Internet Security ou KIS est une suite de sécurité développée par la société russe Kaspersky Lab compatible avec Windows, Mac, Androïde et IPad. KIS propose la détection et la suppression des logiciels malveillants, du spam, et bloque les tentatives hameçonnage, les détournements de données et l'accès non autorisées au réseau et à la webcam.

Tableau n°7 : Présentation comparative d'AVG et Kaspesrsky

	AVG	**Kaspersky**
Prix	**63,99 $**	**29,99 $**
Garantie de remboursement	oui	oui
Pour la partie coût pour se procurer ce système, de de nous constatons qu'AVG est deux fois plus chères que Kaspersky avec une différence de 34$.		
BALAYAGE		
Antivirus en temps réel	oui	oui
Analyse manuelle des virus	oui	oui
Analyse de virus USB	oui	oui
Analyse de démarrage du registre	oui	oui
Analyse automatique des virus	oui	oui
Analyse planifiée	oui	oui
TYPE DE MENACE		
Anti-Spyware	oui	oui
Anti-vers	oui	oui
Anti-Trojan	oui	oui
Anti-rootkit	oui	oui
Anti hameçonnage	oui	oui
Anti-spam	oui	oui
Protection de la messagerie	oui	oui
Protection Chat / Messagerie instantanée	non	oui
Prévention des logiciels publicitaires	oui	oui
COMPATIBILITÉ		
les fenêtres	oui	oui
Mac	oui	oui
Android	oui	oui

IOS	non	oui
USAGE		
Facile d'utilisation	oui	oui
FONCTIONNALITÉS SUPPLÉMENTAIRES		
Pare-feu	oui	oui
Contrôle parental	oui	oui
Mode joueur	non	oui
Service VPN	oui	oui
Optimiseur de smartphone	non	non
Mise au point de l'appareil	oui	non
Navigateur sécurisé	oui	oui
SOUTIEN		
Aide en direct	non	oui
Assistance téléphonique	non	oui
Support par email	non	non
Support de ticket	oui	oui

Source : https://africa.kaspersky.com/ 2024 et https://www.avg.com/fr-fr/all-products 2024

En analysant ce tableau de fonctionnalités, nous pouvons remarquer que ces deux produits sont loin d'être des projets amateur car ils possèdent des options très intéressantes. Mais pour devenir des grand HIPS respectés par les entreprises, ils devront favoriser le développement de ses méthodes de détection et de prévention ainsi que simplifier l'accès à l'application par une documentation complétée et des interfaces facilitant la gestion et l'analyse des logs.

Test comparatif virale avec l'extension .com :

Les deux systèmes de sécurité, ont tous détectent la menace et ils notifient l'utilisateur

Test comparatif des menaces venant de l'internet avec le lien :

Nous avons utilisé ce lien ci-dessous pour tester les accès dangereux et qui a l'apparence d'une signature virale à cause des caractères qui viennent le point d'interrogation :
https://fr.safetydetective.com/recommended/antivirussoftware/eu/?gclid=EAIaIQobCMIxrvR-5-C4wIVluFRCh28cwQjEAAYASAAEgKJgfD_BwE

Pour AVG : IPS a détecté la menace avec interruption en temps réel et il a notifié « menace écartée. Nous avons annulé la connexion à fr.safetydetective.com car cet élément était infecté par ***URL*** :*Blacklist.* »
Détecté par : Agent Web,
Statut : connexion annulée

Quant à KIS lorsque nous avions lancé le même lien dans le navigateur l'IPS a laissé passer la connexion et nous avions accédé aux meilleurs antivirus.

Pour ce cas nous pouvons dire que c'est un faux positif de la part d'AVG et KIS lui n'a rien détecté et nous a donner l'accès à la page demandée car ce n'est pas un lien dangereux en soit. Pour tester le téléchargement dangereux, nous avons utilisé test aligne avec ce lien :

https://media.kaspersky.com/utilities/avtest/level2.zip?_ga=2.213146132.1838765424.156681 28131166477688.1566812813

Les deux technologies ont tous bloquer le téléchargement de ce fichier, comme le montre l'image ci-dessous avec KIS qui l'a détecté comme un lien infecté par EICAR-Test-File.

Fig. 1: Détection et interruption de la connexion IPS/KIS

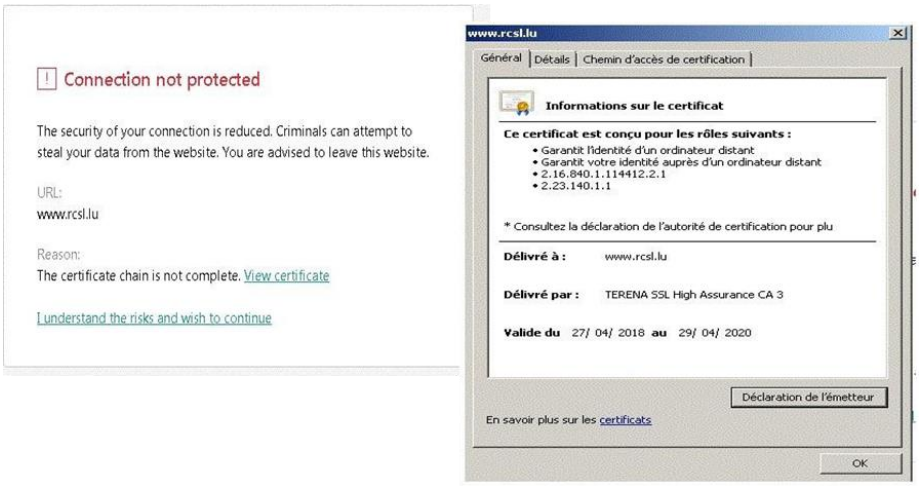


Fig. 2. Détection et interruption de la connexion faute de Certificat

Pour créer ces fichier sans que ils soient supprimés par l'antivirus, comme nous avons constaté avec les tests virale, nous allons désactivez notre anti-virus (anti-spywares, antitrojans) que nous allons activer après l'envoi des mails pour voir sa réaction lors de téléchargement.

Fig. 3: Détection de menaces par Gmail

VI. Discussion Des Résultats

La visée principale de cette étude comparative était de cerner les des systèmes de prévention d'intrusion pour la protection d'un réseau d'entreprise en rapport aux menaces liées aux cyberattaques.

D'où, c'était question de pouvoir songer au renforcement de la sécurité de système de prévention des intrusions (IPS) protège votre réseau contre les cybermenaces en surveillant et en analysant activement le trafic réseau.(https://www.cybersecurityconsultingops.com : 13h 10 avril 2024)

Comme nous venons de le voir, l'état actuelle, de la sécurité sur les réseaux et leur manière d'utiliser les systèmes de sécurité, bon nombre d'entreprises qui utilisent le système d'exploitation Windows ont déjà connus beaucoup d'attaques et qui représentent 80,0% contre 9,0% par rapport à celles qui utilisent le système d'exploitation Linux. Par contre le reste qui n'a jamais été attaqué utilise le système d'exploitation seulement Linux et qui représente 11,0%.

Selon l'usage de système d'exploitation, il sied de préciser que le système d'exploitation le plus utilisé c'est le Windows et représente 80,0% contre 20,0% pour Linux dans l'ensemble des secteurs d'activités ayant été ciblé dans notre panel représentatif. Toutefois, il est à préciser que le système d'exploitation Linux est beaucoup plus utilisé dans le secteur de l'Education avec une fréquence de 8 soit 8,0% suivi respectivement du secteur de commerce et vente avec une fréquence de 4 soit 4,0%, de Transport avec une fréquence de 3 soit 3,0%, de l'Administration (public) et les Sociétés bancaires avec chacune une fréquence de 2 soit 2,0%. Pour le domaine industriel avec une fréquence de 1 soit 1,0% enfin pour les autres domaines c'est avec une fréquence de 0 soit 0,0%.

Partant de la sécurité et de la source d'attaque, 45,0% des entreprises enquêtées choisissent leurs coûts d'implantation du système de sécurité, 27,0% font leurs choix en tenant en compte sur le système de sécurités par rapport à la performance et 28,0% font le choix n'est pas sur base de la performance et ni du coût d'implantation.

Quant aux entreprises qui ont déjà été victimes d'une au plusieurs attaques, disent que les sources de ce menaces

sont multiples selon le tableau n°6, avec 39,0% qui viennent sur les périphérique USB, 18,0% en cliquant sur les liens de mails, 16,0% leurs menaces viennent d'ailleurs, 15,0% en ouvrant des fichiers, 11,0% se sont abstenus et 1,0% dans en navigant sur internet.

Pour les deux solutions antivirus les plus utilisé par nos enquêtés sous Windows, nous voyons que Kaspersky vient en tête avec une fréquence de 74 soit 74,0% et (AVG ouMcAfee) avec une fréquence pour chacune de 2 soit 2,0% et qui ont fait l'objet de notre test d'essai pour l'expérimentation système.

VII. Conclusion

Les systèmes implémentés au sein des entreprises de la Ville de Goma connaissent des menaces dues à plusieurs facteurs pour le systèmes fonctionnant en réseau. Ces menaces issues des cyberattaques suite à un dysfonctionnement lié à la non intégration des mécanismes de cybersécutés causent préjudices aux système ainsi implanté. D'où, cette étude comparative portant *les systèmes de prévention d'intrusion pour la protection d'un réseau d'entreprise* mérite une attention particulière pour des solution palliatives aux défis précités.

Vue la complexité du ce domaine de notre étude, vue l'avancement technologique et de menaces, le système de sécurité doit être primordial pour garder l'équilibre et la qualité de service dans l'entreprise et sur son réseau entier. Mais faire un bon choix n'est pas chose facile pour les entreprises. C'est pourquoi nous avions proposé en annexe de cette étude certaines solutions des tests d'expérimentation système qui pourront aider et orienter les entreprises dans leur choix d'un système de prévention d'intrusion et selon leurs besoins via cette étude comparative afin de permettre une bonne protection contre les attaques connues en réseau.

Après avoir étudié, analyser et comparer les IPS pour la protection des réseaux d'entreprise. Etant donné que les données sont tellement sensibles, il faudra songer à bien les protégées par un système de sécurité efficace.

Cependant, notre hypothèse a été bel et bien confirmée conformément aux résultats repris dans les tableaux n°2, n°3, n°5, n°6, n°7, par rapport aux résultats excessifs et interprétation et à bien fouiller les critères et étapes à suivre pour four un bon choix d'un IPS, pour lutte contre les attaques dans réseaux de l'entreprises.

Partant de ces résultats, nous croyons avoir apporté un petit plus aux entreprises en matière de sécurité réseau ceux-là pourront leur servir comme solutions en guise de prévention d'intrusion.

Références Bibliographiques

[1] Dagon, N. (2006). Détection Et Prévention D'intrusion, In Loria, Juin, Tome I, Nancy
[2] L. Bloch Et Al, (2018). Sécurité Informatique (Principes Et Méthode), Eyrolles, Paris,
[3] Florence Nicolau (2006). Logiciel Le Sphinx Plus 2 Version 5, Chavanod
[4] Hewlett P, (2024). Qu'est-Ce Que La Sécurité Informatique ?, Qu'est-Ce Que La Sécurité Informatique ? | Glossaire | Hpe Africa, Enterprise Development Lp, Consulté Le 06 Février 2024 A 10h11
[5] Farah, J. (2013). Système De Détection Et De Prévision D'instrusions, Ensi
[6] Sofiane Maza (2010), Une Méthodologie De Développement Sécurisé Des Systèmes D'information Avancés, Mémoire De Master En Informatique, Université Mohamed Khider – Biskra.
[7] Https://Blog.Avast.Com/Fr/Piratage-Equifax-Quelles-Consequences , Consulté Le 10 Février 2024 A 11h25
[8] Https://Nvd.Nist.Gov/Cwe.Cfm#Cwes, Consulté Le 25 Février 2024 A 10h05
[9] Https://Secludit.Com/Blog/Cyber-Attaque-Dequifax-Pme-Etes-Autant-Vulnerables/ , Consulté Le 15 Février 2024 A 10h15
[10] Https://Www.Cybersecurityconsultingops.Com : Consulté 20 Avril 2024 A 13h
[11] Https://Www.Imt.Fr/Cybersecurite-Nouvelles-Problematiques-A-Maitriser/ , Consulté Le 22 Février 2024 A 13h10
[12] Https://Www.Lemonde.Fr/Pixels/Article/2018/08/15/Piratage-Des-Centaines-D-Utilisateurs-Instagram-Perdent-L-Acces-A-Leur-Compte_5342781_4408996.Html, Consulté Le 10 Février 2024 11h30
[13] Https://Www.Lemonde.Fr/Technologies/Article/2009/01/12/Internet-L-Impossible-Securite-Du- Reseaumondial_1136896_651865.Html, Consulté En Ligne 22 Février 2024 A 10h
[14] Https://Www.Microfocus.Com/Media/Flyer/Top_Network_Risks_And_Concerns_For_Corpor Ations_Flyer_Fr.Pdf , Consulté Le 19 Février 2024 A 9h30
[15] Https://Www.Redhat.Com/Fr/Topics/Security/What-Is-An-Idps, Consulté Le 25 Février 2024 A 10h22
[16] Https://Africa.Kaspersky.Com/ , Consulté Le 25 Février 2024 A 15h
[17] Https://Www.Avg.Com/Fr-Fr/All-Products, Consulté Le 25 Février 2024 A 15h