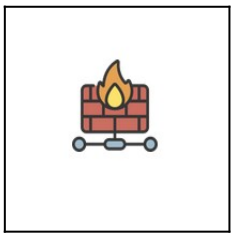
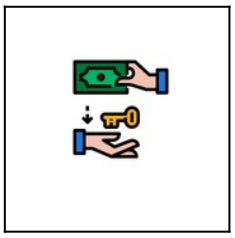
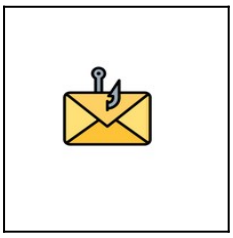
SAUTIE Thomas
IRIS (Mediaschool)
15/01/2025

VEILLE CYBERSECURITE

ANTICIPATION ET PRÉVENTION DES CYBERATTAQUES

Analyses, solutions technologiques et recommandations stratégiques

Introduction

Contexte :

Le monde des technologies numériques est en constante expansion. La cybersécurité est devenue quant à elle de plus en plus complexe du fait des cybermenaces qui chaque jours évoluent sans cesse, accompagné de nouvelles techniques et tactiques de plus en plus sophistiquées. L'impact de celles-ci sur les entreprises, les hôpitaux, les gouvernements et les infrastructures critiques est devenu considérable.

Problématique :

Comment anticiper et prévenir les nouvelles formes de cyberattaques dans un environnement numérique en constante évolution ?

Les pirates informatiques, ou hackers, motivés par des gains idéologiques ou financiers, exploitent constamment le monde à la recherche de systèmes d'informations vulnérables. La réelle question à se poser est, comment les entreprises et organisations peuvent se préparer et anticiper ce type d'attaques et menaces au quotidien.

Objectifs :

- Analyser les cyberattaques émergentes
- Comprendre leurs portées
- Proposer une solution pour les anticiper

A l'avenir cette veille permettra aux entreprises d'être guidées dans la mise en page de stratégies efficaces afin de protéger leurs données qu'elles soient sensibles ou non, ainsi que leurs systèmes d'informations.

Table des matières

1. Introduction……(2)

2. Démarche de cette veille informatique
   a) Outils de surveillance……...(4)
   b) Méthodologie……(5)

3. Analyse
   a) Différents types de cyberattaques émergentes……...(6)
   b) Conséquences……...(7/8)
   c) Approche proactive……...(8)

4. Solutions technologiques
   a) SIEM……...(9)
   b) Anti-ransomwares……..(10)
   c) Pare-feu……(11)

5. Mise en œuvre
   a) Phase 1……(12)
   b) Phase 2……....(13)
   c) Phase 3……(14)

6. Résultats……..(15)

7. Limites et Défis……(16)

8. Glossaire……(17/18)

9. Sources……(19)

Démarche pour cette veille informatique

Outils de Surveillance :

Pour que cette veille informatique soit le plus efficace possible, plusieurs outils de surveillances doivent être nécessairement utilisés, notamment :

- ✗ SIEM (Security Information ans Event Management) :

Cet outil sera utilisé pour collecter, analyser puis corréler le événements de sécurité pour aboutir sur une détection des menaces en temps réel.

Actuellement sur le marché, le produit « Splunk » est l'un des logiciel les plus complet en termes de fonctionnalités. Il permet de fournir une vue d'ensemble complète de la sécurité. De plus, il est facile d'utilisation et facile à parcourir malgré sa complexité. Les deux options les plus utiles sont, la fonction « visualisation » et « analyse des ressources ».

- ✗ Outils de détection de ransomwares :

Afin de répondre à notre besoin, le pack « NinjaOne Portect » est un logiciel qui nous permettra de détecter et de neutraliser les ransomwares avant qu'ils ne cryptent les fichiers dits « critiques ».

En effet, ce logiciel aide à prévenir, détecter et répondre à ces cybermenaces pouvant atténuer potentiellement la fonctionnalité des organisations et entreprises. Il permet donc de réduire l'impact des ransomwares sur votre entreprises.

- ✗ Agences CERT (Computer Emergency Response Team) :

L'outil CERT permet de fournir des alertes et des informations sur les menaces en cours. En effet, celui-ci fournit une assistance technique 24h/24h sur les incidents en terme de sécurité d'ordinateurs et/ou de réseaux.

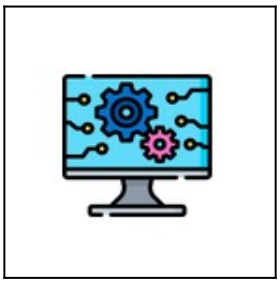
Cet outil propose deux services principaux :

- Répondre aux demandes d'assistance de sécurité (réseaux, systèmes d'informations…)

- Traiter les alertes et réagir aux attaques informatiques

Méthodologie :

La méthodologie que nous allons utiliser pour cette veille repose sur une combinaison d'approche. Elle se divise en trois points importants et différents, le point technologique, stratégique et législatif.



Veille technologique :

→ Surveiller les nouvelles technologies et innovations

→ Détection des vulnérabilités et failles exploitables

→ Analytique structuré des incidents

→ Utilisation d'outils de cybersurveillance

Veille stratégique :

→ Analyser les mouvements des pirates informatiques

→ Études des nouvelles techniques d'attaques et tendance du dark web

→ Suivi de l'ensemble des motivations des attaquants

→ Développer une stratégie adaptée pour faire face aux menaces émergentes

Veille législative :

→ Suivi des nouvelles lois en terme de cybersécurité

→ Étude approfondie des politiques gouvernementales

→ Veille sur les certifications de sécurité

→ Impacts des régulations sur les pratiques des entreprises

Analyse

Types de cyberattaques émergentes :

- ✗ Le Ransomware :

Les rançongiciels ou ransomwares sont des types de logiciels malveillants, utilisés pour bloquer l'accès à l'ordinateur ou même à des fichiers. Ce blocage est dû à un chiffrement de la cible visée (ordinateurs, fichiers,…). Les pirates informatiques, réclament le plus souvent à la victime de l'argent d'un montant demandé afin que celle-ci puisse accéder à nouveau à ses fichiers, son ordinateur etc..

- ✗ Le Zéro-day :

Le terme Zéro-day ou faille Zéro-day, désigne le fait que le développeur, par exemple, prend connaissance d'une faille. Cet aboutissement signifie qu'il possède « zéro jours » pour la corriger. De ce fait, les attaques Zéro-day surviennent quand les cybercriminels exploitent cette faille avant que le développeur n'ait la possibilité de la rectifier. Il a donc accès à plusieurs informations selon la faille trouvée, le plus souvent des données sensibles, et la aussi une demande de rançon est demandée.

- ✗ Le Phishing :

L'hameçonnage ou Phishing, est une technique frauduleuse destinée à appâter une personne pour l'inciter à communiquer des données personnelles (carte bancaire, compte d'accès,..), se faisant passer pour une tiers de confiance. Une fois les informations volées, celles-ci peuvent être revendues ou du chantage peut être réalisé.

- ✗ Le DdoS :

Une attaque DdoS (Distrbuted Denial of Service), vise à rendre un serveur dysfonctionnel ou inaccessible afin de provoquer une panne ou un fonctionnement dégradé du service en ligne. Il permet donc de perturber une organisation ou entreprise par exemple, cette attaque peut elle aussi faire l'objet d'une demande de rançon.

Conséquences des cyberattaques :

Une cyberattaque peut être réalisée pour différentes raisons, il y a deux raisons principales, qui sont le plus souvent le fruit de la demande du pirate informatique sur des organisations et entreprises ou autres.

➔ <u>Conséquences financières :</u>

En effet ces cyberattaques peuvent avoir un impact financier conséquent, en 2022 une étude a montré que ces attaques avait entraîné une perte élevée a 6 000 milliards USD par an dans le monde. Il a 3 principales pertes de revenus pour les entreprises et organisations.

→ Les frais de réparation

Les entreprises doivent investir dans la réparation des systèmes informatiques endommagés par ces attaques (remplacement de matériel, correction des vulnérabilité, mesure de sécurité)

→ Les pertes de revenus

Si ces attaques entraînent une interruption de la production ou des services des entreprises, celles-ci peuvent perdre des revenus importants vis a vis de leurs clients qui pourraient choisir de se rediriger vers un concurrent.

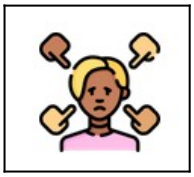
→ Les sanctions et amendes

En réalité, si l'entreprise est reconnue responsable de ne pas avoir suffisamment protégé les données sensibles des clients ou des employés, celle-ci peut recevoir une amende.

X	Réparations (€)	Pertes (€)	Sanctions (€)
2022	55 000 € (coût moyen par cyberattaque)	14 000 € par incident (jusqu'à 220 000 € pour certaines)	Plusieurs millions d'euros
2023	59 000 € (coût moyen par cyberattaque)	14 720 € par incident (jusqu'à 230 000 € pour certaines)	Plusieurs millions d'euros

<u>Coûts des cyberattaques en France : 2022 et 2023</u>

➔ Conséquences réputationnelles :



Les cybermenaces sont constamment présentes et ce de plus en plus, elles sont en constante croissance mettant en péril non seulement la sécurité des données pour les entreprises mais également leurs réputations.

En effet, lorsque celles-ci sont victimes d'une attaque par un pirate informatique, la perte de confiance de ses clients et partenaires ne peut qu'être inévitable. Les causes de ces attaques ne sont rien d'autre que de la dégradation de leurs images, les classants comme peu fiable aux yeux non seulement des autres entreprises avec qui elles travaillent, mais aussi de leurs propres employés. Ces réputations peuvent avoir des répercutions lourdes.

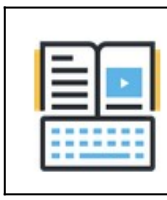
→ Les organisations victimes de cyberattaques perdent la confiance de leurs clients et partenaires, qui iront à l'avenir chez des concurrents de l'entreprise ciblée.

→ Perte de la réputation de l'entreprise, c'est à dire que celle-ci serait catégorisée comme une entreprise avec peu de confiance, que ce soit pour ses employés comme clients, cela peut aboutir sur crise de celle-ci, et dans le pire un fermeture de l'entreprise

➔ Approche proactive :

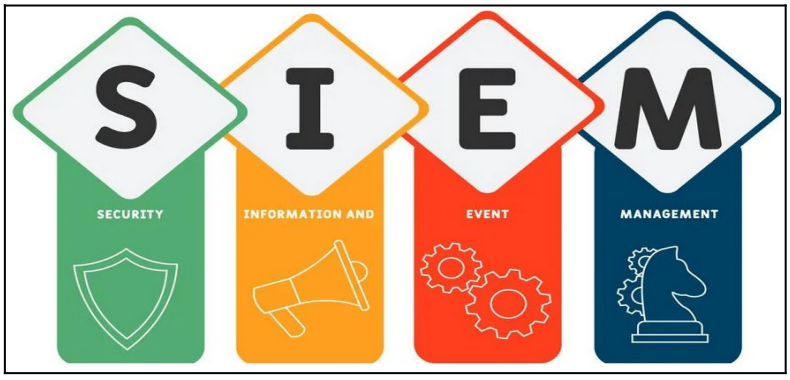
Pour lutter contre ces conséquences, les entreprises se doivent d'anticiper les cyberattaques en utilisant des solutions de surveillance et en appliquant des stratégies de défense en profondeur. Par ailleurs il est possible de minimiser l'approche de ces attaques en formant son personnel, ou même en misant sur l'innovation pour être en avance sur le marché. Cela permets de limiter les risques mais toute fois requière parfois énormément d'argent et donc un gros budget.

→ Matériels récents
→ Groupe IS
→ Stratégies de défense



→ Formations CNIL
→ Formations ANSSI
→ E-learning

Solutions technologiques



Solution SIEM :

La solution SIEM est une réelle solution avancée de surveillance qui permet de collecter, centraliser puis analyser les événements de sécurité. Elle permettra aux organisations d'être informées en temps réel sur les menaces et donc pouvoir permettre de prendre les mesures de cyberdéfense nécessaires pour faire face aux attaquants (pirates informatiques).

Cet outil est donc très efficace en particulier pour enregistrer les journaux d'événements des différents systèmes informatiques tels que :

- Pare-feu
- Serveurs
- Etc...
- Antivirus
- Réseaux

A partir de cette centralisation très efficace, il est capable d'identifier les comportements suspects et douteux et générer des alertes si l'une des activités sur le système informatique semble anormale, ainsi qu'une réaction rapide aux menaces.

Avantages :

→ Surveillance en continu + en temps réel (des activités suspectes)
→ Interdépendance des événements (si l'ensemble des réponses sont normales et non douteuses)
→ Automatisation des alertes (réaction rapide aux incidents en temps réel)

Inconvénients :

→ Son coût (autant pour la mise en place que pour la maintenance de l'outil)
→ Expertise avancée pour l'utilisation de ce logiciel (formation à passer pour se perfectionner sur l'outil afin d'assurer le potentiel de son utilisation)

Solution de l’outil de détection de ransomwares :

Comme nous avons pu le voir, les attaques rançongiciel sont parmi les plus destructrices pour les entreprises. Pour réussir à les anticiper les solutions modernes utilisent les technologies d’intelligence artificielle (IA) et de machine learning (ou apprentissage). Ces deux révolutions permettent d’analyser constamment le trafic du réseau, les comportements anormaux des fichiers et même les activités des utilisateurs pouvant attaquer avant qu’elles ne soient données. Cette anticipation peut vraiment faire la différence pour les entreprises qui souhaitent s’en équiper.

Avantages :

→ Détection proactive des menaces a l’aide de l’IA

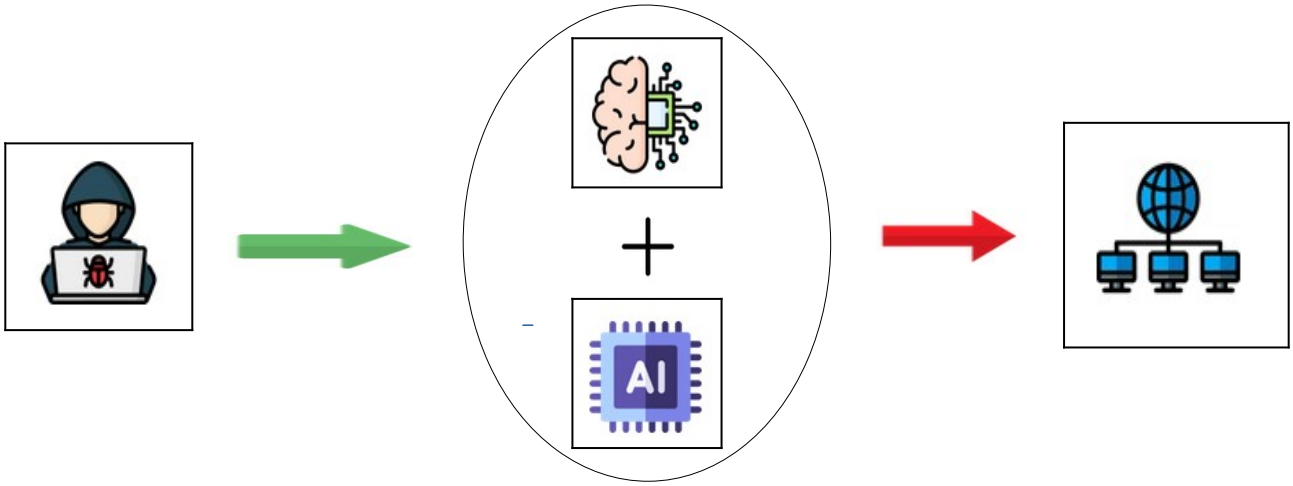
→ Neutralisation des ransomwares en amont de leurs impacts sur le système

→ Réduction conséquente de temps de réponse en cas d’attaques

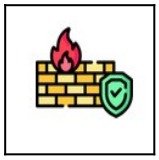
Inconvénients :

→ L’apparition de nouveaux ransomwares capables de contourner le système de détection de cet outil

→ Maintenance de l’outil (mise à jour régulières afin d’être à jour sur l’évolution des menaces)



Solution d’un Pare-feu de nouvelle génération :



En effet, un pare-feu de nouvelle génération ne se contente pas seulement de filtrer les adresse IP et les ports mais il analyse le contenu du paquet réseau, les applications ainsi que le comportements des utilisateurs. Donc l’impact des études de recherches et des tentatives d’intrusion en temps réel. L’un des plus fiable est le NGFW, il possède des fonctionnalités d’IDS et IPS (Intrusion Detection and Prevention System) et de Sanboxing pour but d’isoler les suspects avant qu’ils ne puissent réellement agir sur le système informatique.

Avantages :

→ Analyse des paquets afin d’assurer une meilleure détection des menaces

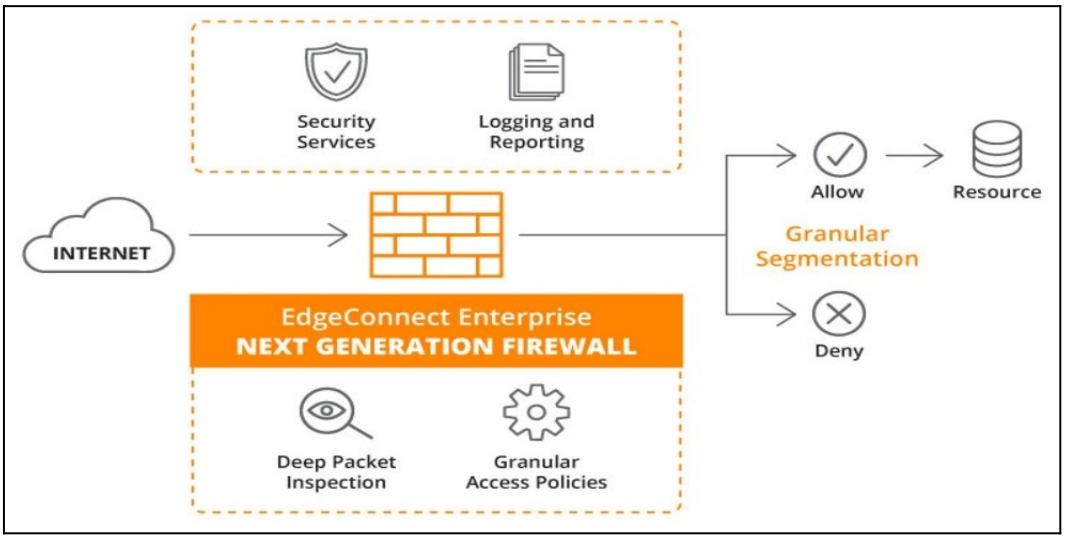
→ Protection avancée contre les menaces telles que les exploitations de faille Zéro-day

→ Intégration avec d’autres solutions de cybersécurité comme les SIEM

Inconvénients :

→ Les configurations avancées de cet outil ralentissent le réseau si celui-ci n’est pas optimisé

→ Beaucoup de suivi contant des adaptateurs afin de pourvoir contrer les nouveaux types de menaces émergentes



Schématisation du Pare-feu NGFW

Mise en place des solutions données

La mise en œuvre de ces solutions demande une approche du problème en trois phases respectant un objectif bien précis.

Phase 1) Préparation et Déploiement

→ Évaluation des risques

Tout d'abord on identifie les différentes vulnérabilités existantes au sein de notre système informatique, en l'analysant de A à Z.

→ Installation et Configuration des outils

Installation et mise en place des trois différentes solutions proposées (SIEM, Anti-ransomwares et pare-feu NGFW), tout en apportant les configurations nécessaires à ce que l'on souhaite protéger et comment l'on souhaite qu'ils agissent.

→ Sensibilisation et formations des IS (Ingenieur Systeme) et des employés au sein des équipes d'IT (Information Technology) et de l'entreprise.

Grace au E-learning, et à diverses formations au sein des organisations, il est préférable de former les ingénieurs sur les risques du monde informatique en émergence de jour en jour. Grace à cette sensibilisation, et à la formation des outils utilisés, les menaces ne peuvent qu'être réduites même si l'être humain est faillible.

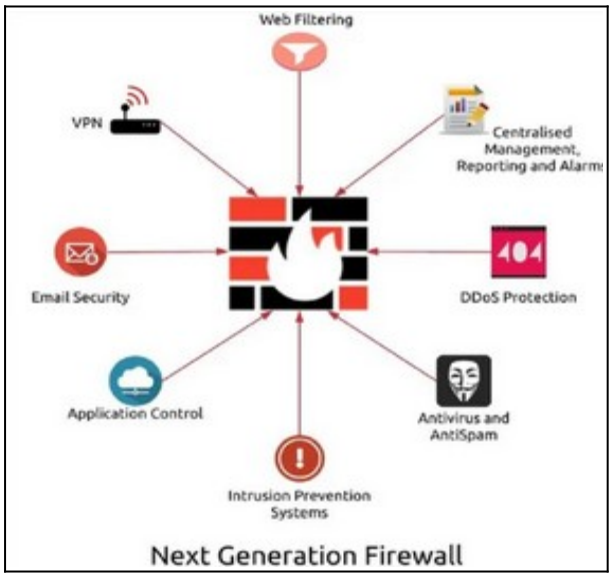
SecNum académie
ANSSI

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Phase 2) Surveillance active et améliorations

→ Suivi en temps réellement (SIEM + Pare-feu)

Le SIEM (Security Information ans Event Management) et les pares-feux dits de « Next Gene » réalise une surveillance en continue sur le système informatique. Lorsque les activités semblent suspectes ils alertent les équipes de cybersécurité pour une intervention le plus rapidement possible.



Schématisation d'un Pare-feu « New Gene »

→ Analyse des alertes

L'ensemble des alertes générées ne correspond pas forcement à une attaque réelle. C'est pour cela qu'il est aussi nécessaire de pratiquer une analyse régulière accompagnée de rendu complet.

→ Mise à jour des systèmes

Les hackers sont constamment à la recherche de nouvelles cybermenaces possibles, en conséquence les logiciels de protection doivent être mis à jours régulièrement pour rester à jour sur les menaces en essors. L'application de patch de sécurité et la mise à jour des antivirus permettent donc potentiellement de contrer les différentes variantes de cyberattaques.

+

+

=

Diminution des risques d'attaques et des opportunités pour les pirates informatiques

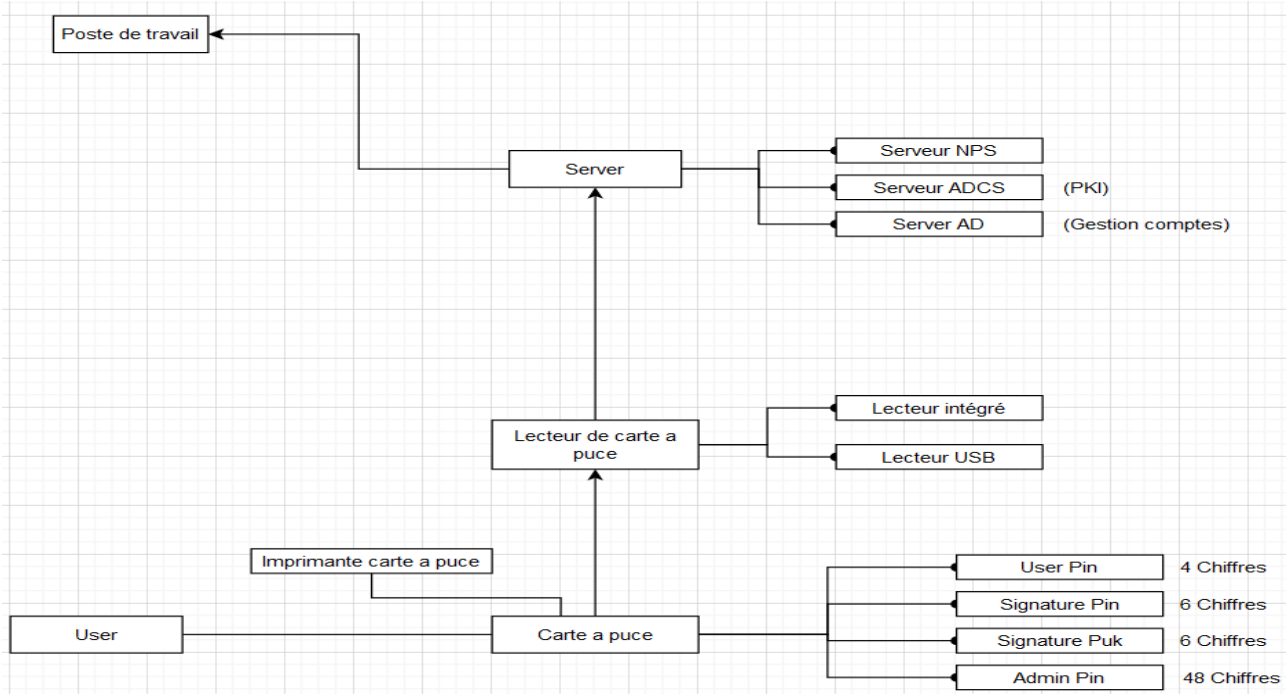
Phase 3) Réponse aux incidents et améliorations de la cybersécurité

→ Protocole de sécurité en autonomie

Le fait que ces logiciels soient en constante utilisation, entraîne une sûreté et sécurité optimale au quotidien. Ces actions ralentissent considérablement la propagation de piratage de données sensibles.

→ Plan et remédiation

Après une cyberattaque, il est crucial de restaurer les parties de la sauvegarde sécurisée et les identifiants des accès compromis. Afin d'éviter une nouvelle intrusion, il est nécessaire de renforcer les politiques d'authentification, comme par exemple la mise en place d'une authentification multifacteurs (MFA), à l'exemple des cartes à puce pour une connexion accompagnée d'un AD.



Exemple d'authentification multi-acteurs possible

→ Audit et analyse post-attaque

Une fois les cyberattaques neutralisées par un audit de sécurité, celui-ci peut mener sur la piste des volontés de l'attaquant et comprendre la cible visée. Grace à ceci, il est préférable de renforcer la partie de système informatique visée par les attaquants, donc ajuster les mesures de protection et l'amélioration de la stratégie de cybersécurité.

Résultats attendus

→ Réduction des incidents de sécurité de 30 % (sensibilisation et amélioration de capacité de détection des cyberattaques)

Ces cyberattaques sont le plus souvent du à des erreurs humaines, à l'exemple de l'ouverture des mail (phishing..) ou même l'utilisation du même mot de passe pour toutes ses connexions à un service quelconque. Pour diminuer cet impact conséquent, il est attendu que les entreprises forment leurs employés mais aussi qu'elles simulent ce type d'attaques à leurs employés afin de les mettre en conditions pour essayer de les préparer au maximum pour le jour ou celles-ci se présenteraient. De plus la mise en place des outils proposés comme le SIEM permet déjà d'empêcher cela, une fois ces deux choses impliquées dans l'organisation, la diminution d'attaque se révèle efficace.

→ Renforcement de l'infrastructure / réseaux (augmenter les chances de protection des données sensibles)

La protection de nos données est essentielle pour éviter des pertes financières pour une entreprise ainsi que les atteintes à sa réputation. Il est donc important pour celles-ci d'inclure un chiffrement des données, l'authentification multi-facteurs ainsi que le contrôle strict des accès (rôles particuliers). De plus, une sauvegarde automatique est nécessaire en cas d'attaques pour récupérer les données perdues malgré la capture de celles-ci par le pirate. En conséquence il est impérial que la totalité de la démarche soit respectée.

→ Optimisation des processus de cybersécurité pour une meilleure visibilité et anticipation des menaces

L'amélioration continue des processus de cybersécurité repose sur l'analyse des données et l'intelligence artificielle. Des solutions avancées de Threat Intelligence permettent l'identification des nouvelles tendances en terme d'attaques. En approche proactive, les entreprises ne se contentent pas de réagir aux incidents, mais elles mettent en place des stratégies de prévention sur des simulations d'attaques et des audits réguliers en formant leur personnel à ces éventualités.

Limites et Défis

✗ Coût élevé :

→ Implémentation de solutions avancées comme les SIEM et les Pare-feu « New Gene » représentent un investissement financier important.

→ les PME peuvent avoir du mal à atteindre le budget nécessaire et donc de trouver une réelle nécessité dans l'installation et la mise en place de ses outils.

✗ Besoin d'une expertise avancée :

→ L'intervention d'une équipe qualifiée est indispensable pour interpréter les alertes et configurer ces outils, ou alors elle doit déjà faire partie de l'entreprise.

→ Une formation continue des employés par les administrateurs réseaux ou des formations internet (MOOC, E-learning,..), est essentielle mais dure à maintenir au sein d'une entreprise sur le long terme.

✗ L'évolution des menaces :

→ Développement de nouvelles techniques d'attaque pouvant contourner les techniques de protection mises en place.

→ La diffusion sur les réseaux d'une communication sur ces cybermenaces est nécessaire afin de rester efficace face aux attaques, d'où les erreurs humaines sur ces sujets sensibles.

Malgré les défis liés au coûts (budget), à l'expertise nécessaire ou requise et à l'évolution des nombreuses menaces de jour en jour, renforcer sa cybersécurité doit devenir la priorité numéro une pour les entreprises. L'adoption de solutions avancées telles que proposées (SIEM, Pare-feu, …), améliore la surveillance ainsi que la détection d'attaques avec des alternatives plus accessibles mais plus risquées pour les PME.

L'expertise peut-elle, être acquise via des formations et de la prévention interne ou même en ligne, bien que celle_ci ne dépend que de l'assiduité du personnel au sein de celles-ci. Face aux cybermenaces en constante évolution, une communication efficace et des protocoles de surveillance permettent de limiter les erreurs humaines. En renforçant leurs infrastructures, les entreprises peuvent anticiper les attaques, garantissant ainsi un avenir solide et sécurisé au maximum.

Glossaire

SIEM	Solution de sécurité permettant aux entreprises ou organisations de détecter les cybermenaces avant que celles-ci perturbent leurs activités.
Ransomware	Logiciel ou virus malveillant qui bloque l'accès à l'ordinateur ou aux fichiers de la cible visée.
Ddos	Cybercrime visant à rendre inaccessible un serveur par l'envoie de multiples requêtes afin de le saturer.
Phishing	Technique frauduleuse visant à leurrer la cible pour l'inciter à communiquer des données personnelles.
Splunk	Plateforme de surveillance de big data qui simplifie la collecte et la gestion de gros volumes de données.
CERT	Agence dont l'équipe est spécialisée en cybersécurité dédié à la gestion des incidents de sécurité informatique.
Dark web	Ensemble caché de sites internet accessibles uniquement par un navigateur spécialement conçu à cet effet.
Zéro-day	Risque de sécurité dans un logiciel qui n'est pas connu publiquement et dont le fournisseur n'a pas connaissance.
USD	Dollar des Etat-Unis.
Pare-feu	Système de sécurité de réseau informatique qui limite le trafic internet entrant, sortant ou à l'intérieur d'un réseau privé.
Antivirus	Programme informatique qui a pour principale vocation d'identifier, de neutraliser, voir éliminer les virus informatique.
Serveur	Système qui met des ressources, des données, des services ou des logiciels a la disposition d'autres ordinateurs, qualifiés de « client » sur un réseau.
Machine learning	Sous ensemble de l'IA visant a apprendre aux machines à tirer des enseignements des données et s'améliorer.
Adresse IP	Endroit où réside un ordinateur au sens virtuel, elle ne donne pas de coordonnées GPS.

Un port	Point virtuel où la connexions réseau commencent et se terminent.
Paquet réseau	Petit segment d'un message plus important, les données informatiques sont divisées en paquets.
IPS	Technologie de sécurité conçue pour détecter et bloquer activement les accès non autorisés, les activités malveillantes et les menaces potentielles au sein d'un système informatique.
Sandboxing	Une pratique de sécurité dans laquelle vous utilisez un environnement isolé, ou une « Sand box », pour les tests.
NGFW (pare feu « New Gene »)	Un pare-feu conçu pour protéger les entreprises contre les cybermenaces modernes .
IS	Acronyme d'Ingénieur système.
IT	Terme qui englobe le monde des technologies.
E-learning	C'est un dispositif d'apprentissage qui est organisé à distance et en ligne, à partir de l'outil informatique.
CNIL	Commission Nationale de l'Informatique et des Libertés, est chargée de veiller à la protection des données personnelles.
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information est l'autorité nationale en matière de cybersécurité. Sa mission est de comprendre, prévenir et répondre aux risques (cybersécurité).
MFA	Authentification possédant plusieurs couches de protection.
AD	Base de données et ensemble de services qui permettent de mettre en lien les utilisateurs avec les ressources réseau dont ils ont besoin pour mener à bien leurs missions.
PME	Une entreprise qui compte généralement moins de 250 employés et un chiffre d'affaires annuel est inférieur à 1 milliard d'euros.
MOOC	Cours en ligne ouverts et massifs.
Chiffrement	Procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible.
Threat inteligence	Processus d'identification et d'analyse des cybermenaces.

Sources

https://cyber.gouv.fr/publications/recommandations-pour-la-protection-des-systemes-dinformation-essentiels

https://www.interieur.gouv.fr/actualites/actualites-du-ministere/rapport-annuel-sur-cybercriminalite-2024

https://www.economie.gouv.fr/entreprises/rancongiciels-ransomware-protection

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/rancongiciels-ransomwares#victime-ransomware

https://fr.wikipedia.org/wiki/Spear_phishing

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/hameconnage-phishing

https://www.economie.gouv.fr/entreprises/attaque-par-deni-service-ddos

https://korben.info/hackropole-plateforme-apprentissage-cybersecurite-france.html

https://thehackernews.com/

https://www.offsec.com/

https://www.reddit.com/

https://thecyberwire.com/

https://x.com/?mx=2

https://www.youtube.com/

https://cyber.gouv.fr/

https://www.cybersecura.com/

https://www.linkedin.com

https://www.flaticon.com/

https://app.diagrams.net/

https://www.fedlex.admin.ch/eli/oc/2024/257/fr

https://france.scc.com/

https://www.data.gouv.fr/fr/

https://www.microsoft.com/fr-fr/security/business/security-101/what-is-siem

https://fr.wikipedia.org/wiki/Wikip%C3%A9dia:Accueil_principal