Institution des Chartreux

Veille informationnelle

Documentation

FAUBLADIER--ANETTE Alexandre
01/10/2024

Table des matières

Veille informationnelle : Quelles sont les méthodes de sécurisation d'un serveur de virtualisation avec une approche multi-outils ?

Introduction

La sécurisation des systèmes d'information est devenue un enjeu central pour les entreprises, au même titre que leurs activités de production et de développement. Dans un monde où l'économie numérique repose en grande partie sur la mise à disposition de services digitaux — comme l'hébergement de sites, le streaming ou le stockage en ligne — les machines virtuelles (VM) jouent un rôle crucial. Elles permettent aux entreprises d'optimiser leurs ressources et de déployer rapidement des services pour leurs clients. Cette virtualisation repose sur des hyperviseurs, logiciels essentiels permettant de créer, gérer et surveiller plusieurs machines virtuelles sur un seul serveur physique.

1. Les hyperviseurs

Les hyperviseurs constituent aujourd'hui la pierre angulaire de l'infrastructure informatique d'une organisation. Ils orchestrent la virtualisation de multiples applications, bases de données et outils nécessaires à l'activité de l'entreprise, garantissant ainsi la fluidité et la cohérence des opérations. Cependant, ce rôle central en fait également une cible privilégiée pour les attaques informatiques. Une faille au niveau d'un hyperviseur pourrait compromettre l'intégrité de tous les systèmes virtualisés qu'il contrôle, exposant l'entreprise à des risques considérables.

Les technologies de virtualisation occupent une place de plus en plus significative depuis les années 2000. Ce phénomène est dû en grande partie à l'évolution de nouvelles pratiques telles que la virtualisation des postes de travails (serveur Windows et linux par exemple), la virtualisation des applications d'entreprises, du stockage ou encore même à l'émergence du cloud computing.

2. Contexte

C'est dans ce contexte que la sécurisation des serveurs de virtualisation prend tout son sens. Nous explorerons dans ce document les enjeux et les méthodes de sécurisation des serveurs de virtualisation, en particulier à travers une approche multi-outils, qui combine différentes technologies et solutions pour renforcer les protections. Cette veille informationnelle s'appuie sur des sources fiables et reconnues, avec pour objectif de souligner l'importance d'une stratégie de sécurité robuste et adaptée à l'évolution constante des menaces informatiques.

Cycle de veille informationnelle

1. Définition des objectifs et délimitation du périmètre de la veille

Le cycle de veille informationnelle est une méthode structurée et continue permettant aux entreprises de suivre, analyser et exploiter des informations essentielles à leur domaine d'activité. Pour garantir une veille efficace, chaque étape du cycle repose sur une démarche rigoureuse et l'utilisation d'outils spécialisés facilitant la gestion des

informations recueillies. Cette première partie de la veille nous permet de pouvoirs définir des objectifs clairs et précis.

L'objectif de cette veille servira de documentation sur des interrogation future lors de mon parcours professionnelle ainsi de développer nos connaissances sur ce sujet.

2. Collecte des informations

Cette phase repose sur l'identification et l'utilisation d'outils de collecte adaptés, permettant d'obtenir des informations provenant de sources crédibles.

Les principales sources d'informations utilisée ont été les suivantes :

- Google Dorking : recherches précises et filtrages des requêtes en fonctions de mots clé précis.
- Wikipédia : grande source de connaissances
- Crowdstrike : Grande entreprise de cybersécurité

L'objectif est donc de garantir une collecte d'informations pertinentes et de qualité permettant ainsi d' éviter les biais et les informations obsolètes.

3. Analyse des informations

L'analyse et la qualification consiste à évaluer la pertinence et la fiabilité des données obtenues, puis à les catégoriser selon leur utilité pour le sujet étudié. Cette phase de tri est essentielle, car elle permet de hiérarchiser les informations et d'éliminer celles qui sont peu fiables ou non pertinentes pour la sécurisation des serveurs de virtualisation.

Il est également recommandé de classer les informations par thèmes, par exemple en utilisant des tags ou des mots-clés qui facilitera donc leur utilisation. De plus, l'évaluation qualitative des informations, comme la validité des sources et la mise en contexte de chaque donnée, est cruciale pour renforcer l'analyse finale de la veille.

L'information sera donc traitées en fonction des nécessités et du sujet définis au préalable. Le but final est donc d'éviter le surplus d'informations.

4. Organisation des données

Pour assurer une veille efficace, l'organisation des données recueillies est essentielle. Utiliser des outils de Mind Mapping ou des applications de gestion de contenu comme Notion ou Obsidian qui permettent de structurer l'information de manière logique et accessible.

Ces outils facilitent la création de hiérarchies et de relations entre les données, ce qui permet d'identifier rapidement les informations pertinentes lors des analyses ou des consultations futures.

Une bonne pratique consiste à établir un système de classement qui regroupe les informations par thématiques, comme les types de vulnérabilités ou les tendances émergentes en matière de cybersécurité. De plus, conserver un

historique des informations permet d'analyser les évolutions des menaces au fil du temps, et ainsi d'ajuster les stratégies de sécurité en conséquence.

5. Diffusion des informations

La diffusion des informations collectées et analysées doit être réalisée de manière efficace et ciblée. Il est crucial de déterminer le public cible pour chaque type d'information, qu'il s'agisse des équipes techniques, de la direction ou d'autres parties prenantes. Les canaux de diffusion peuvent inclure des newsletters internes, des rapports de synthèse, ou des présentations visuelles, comme des infographies, qui rendent les données plus accessibles et compréhensibles.

L'objectif de cette diffusion est de garantir que les connaissances acquises à travers la veille sont mises à la disposition des personnes concernées, leur permettant ainsi de prendre des décisions éclairées. De plus, il est important de recueillir des retours sur la pertinence et l'utilité des informations diffusées, afin d'ajuster les pratiques de veille et d'améliorer en continu le processus.

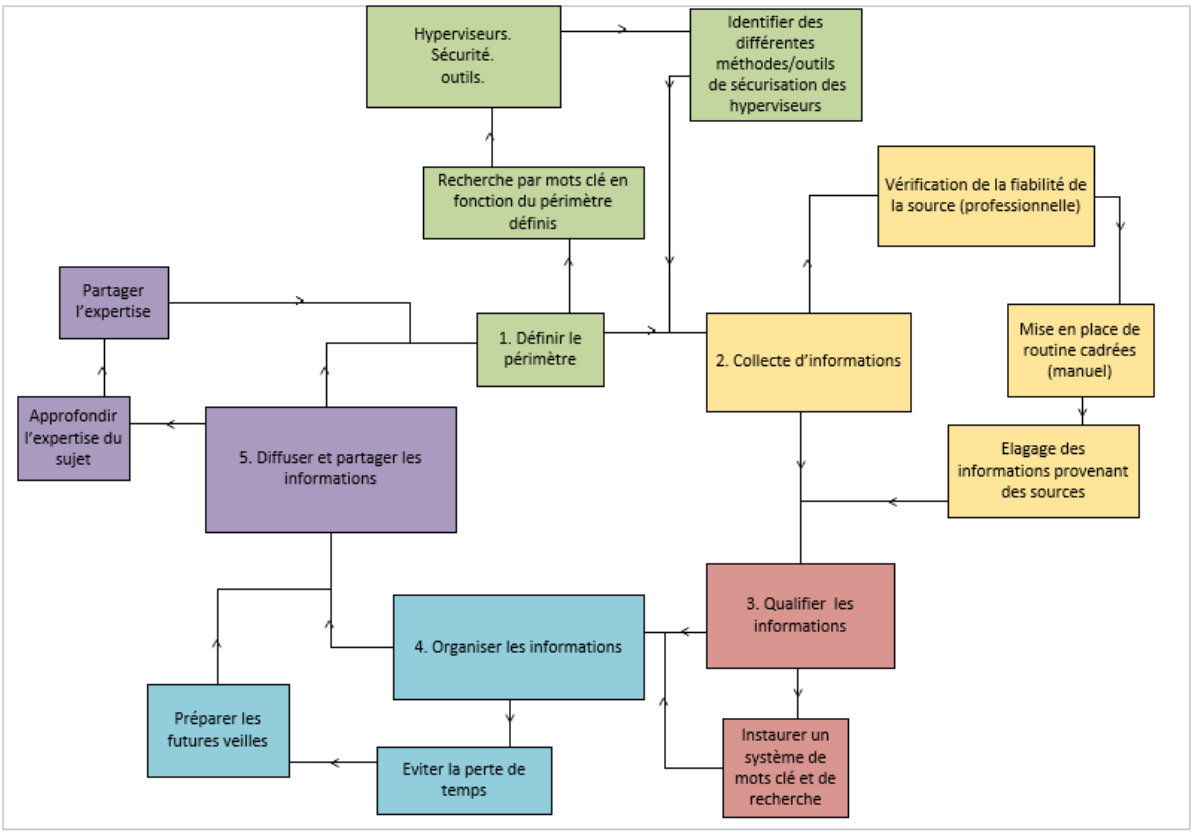

Figure 1 – Schéma de processus de veille.

Mise en œuvre de la veille

1. Définition des objectifs et délimitation du périmètre de la veille

La première étape de la mise en œuvre d'une veille informationnelle est la définition claire des objectifs et la délimitation du périmètre. Cette phase est cruciale, car elle permet de concentrer les efforts de veille sur des sujets précis et pertinents. Par exemple, dans le cadre de la sécurisation des hyperviseurs, les objectifs pourraient inclure la surveillance des vulnérabilités des hyperviseurs, la détection des nouvelles menaces et l'identification des meilleures pratiques en matière de sécurité.

Pour définir ces objectifs, il est important d'impliquer les parties prenantes, notamment les équipes de sécurité informatique, les administrateurs systèmes, et éventuellement les utilisateurs finaux. En collaboration avec ces acteurs, il est possible de dresser une liste des sujets prioritaires à surveiller, tels que :

- Les vulnérabilités récentes des hyperviseurs.
- Les techniques d'attaque émergentes.
- Les recommandations et mises à jour de sécurité fournies par les fabricants de logiciels.

La délimitation du périmètre permet de réduire le risque de dispersion des informations en se concentrant sur les menaces les plus probables et actuelles. Cela inclut également la sélection de sources d'information fiables et pertinentes, comme les rapports de CERT-FR ou encore ceux de l'ANSSI, qui fournissent des informations à jour sur les menaces spécifiques à la virtualisation.

2. Collecte des informations

Une fois les objectifs et le périmètre définis, la prochaine étape consiste à procéder à la collecte d'informations. Cette phase implique l'identification et l'utilisation d'outils et de méthodes adaptés pour recueillir des données pertinentes. La collecte peut être réalisée à travers plusieurs canaux :

- Outils de veille automatisés : Utiliser des agrégateurs de contenu comme Feedly ou des systèmes d'alerte (par exemple, Google Alerts) permet de recevoir des mises à jour en temps réel sur des sujets spécifiques. Par exemple, en configurant des alertes pour les nouvelles vulnérabilités des hyperviseurs, il est possible de rester informé sans nécessiter de recherche manuelle constante.
- Sources d'informations variées : La collecte doit s'étendre à une variété de sources, y compris les publications académiques, les blogs spécialisés en cybersécurité, les bulletins d'information et les forums de discussion. Les bases de données telles que le Common Vulnerabilities and Exposures (CVE) fournissent des informations essentielles sur les failles connues.
- Sondages et enquêtes : Dans certains cas, il peut être pertinent de recueillir des informations directement auprès des utilisateurs ou des experts en sécurité. Des enquêtes peuvent être menées pour évaluer la perception des menaces ou recueillir des expériences sur des incidents de sécurité passés.

L'objectif de cette collecte d'informations est de garantir la qualité et la pertinence des données. Il est essentiel de filtrer les informations afin d'éviter les biais et de se

concentrer uniquement sur les données qui contribueront à une compréhension approfondie des menaces et des solutions de sécurité.

3. Analyse des informations

L'analyse des informations collectées est une étape cruciale qui permet d'évaluer la pertinence et la fiabilité des données. Cette phase implique plusieurs sous-étapes :

- Évaluation de la fiabilité des sources : Chaque source d'information doit être scrutée pour déterminer sa crédibilité. Par exemple, les publications émanant d'instituts de recherche ou de gouvernements sont généralement considérées comme plus fiables que les informations provenant de forums ou de blogs non vérifiés.
- Catégorisation des données : Les informations doivent être triées et organisées par thèmes, comme les types de vulnérabilités, les techniques d'attaque, ou les mesures de mitigation. Utiliser des tags ou des mots-clés peut faciliter cette tâche, en rendant les informations plus accessibles et exploitables lors des analyses futures.
- Évaluation qualitative : Il est également important de mettre en contexte les données en les reliant aux objectifs de la veille. Par exemple, des informations sur une nouvelle vulnérabilité doivent être confrontées à l'environnement spécifique de l'organisation et à son infrastructure pour évaluer leur impact potentiel.

Cette analyse permet d'éliminer les informations peu fiables ou non pertinentes, renforçant ainsi la qualité des conclusions tirées de la veille. Le but final est de fournir une base solide pour les décisions futures et les actions à entreprendre en matière de sécurité.

4. Organisation des données

Pour tirer le meilleur parti des informations collectées et analysées, une organisation claire et structurée est nécessaire. Plusieurs outils et techniques peuvent être mis en place :

- Systèmes de gestion de contenu : Utiliser des outils comme Notion, Obsidian ou des logiciels de mind mapping permet de centraliser les informations et de les organiser de manière logique. Ces outils facilitent la création de bases de données accessibles et navigables, où chaque entrée peut être liée à d'autres informations pertinentes.
- Classification par thèmes et sous-thèmes : Les données doivent être triées par catégories définies lors de la phase de définition des objectifs. Par exemple, un dossier dédié aux vulnérabilités des hyperviseurs pourrait contenir des sous-dossiers pour chaque type de vulnérabilité (VM Escape, élévation de privilèges, etc.).
- Archivage et accès : Maintenir un historique des informations recueillies est crucial pour des analyses futures. Les données doivent être archivées de manière à pouvoir être consultées facilement, notamment pour réaliser des comparaisons avec des situations antérieures ou pour anticiper des menaces émergentes.

Une organisation soignée des données contribue à une gestion efficace de la veille, garantissant que les informations sont non seulement accessibles, mais également exploitables lors de la prise de décisions stratégiques en matière de sécurité.

Synthèse des résultats de la veille

1. Quels sont les risques et conséquence potentiels pour un hyperviseur ?

Les Hyperviseurs sont au cœurs de l'infrastructure d'une organisation et sont donc exposer à plusieurs type de menace qui peuvent gravement compromettre la sécurité d'une organisation :

1.1 Évasion de VM :

Cette attaque permet à un utilisateur d'une machine virtuelle de contourner l'hyperviseur et d'accéder directement au système hôte ou aux autres VM hébergées. Un tel accès non autorisé peut conduire à la compromission de données sensibles dans toutes les VM de l'hôte (source : Wikipedia, Sécurité des hyperviseurs).

1.2 Élévation de privilèges

Parfois, des failles dans l'hyperviseur permettent à des attaquants d'obtenir des privilèges d'administration, ce qui leur offre un contrôle complet sur l'hyperviseur et ses machines virtuelles. Cela représente un risque majeur, car cela peut faciliter des actions malveillantes, comme la destruction de données ou la propagation de logiciels malveillants.

1.3 Attaques par déni de service (DoS)

Ces attaques visent à submerger l'hyperviseur en sollicitant massivement ses ressources, ce qui peut entraîner une indisponibilité des services et une interruption des opérations de l'entreprise. Les attaques DoS peuvent également compromettre la fiabilité des VM hébergées en perturbant leurs ressources disponibles (CPU, RAM).

2. Quels sont les solutions et les recommandation pour protéger un hyperviseur ?

La majorité des informations que l'on retrouve sur les source d'informations tels que it-connect ou encore Crowdstrike nous donne des astuces et des recommandations tel que les mises à jour permettre au système d'informations d'avoir les dernières technologies pour sécuriser les système et corriger les potentiels failles qui aurait pu permettre à de potentiels attaquant de s'infiltrer illégalement dans les SI des organisations.

A. Prévenir contre les inondations

Installer les serveurs dans des salles surélevées ou dans des zones sans risque d'inondation est une première étape de précaution. Dans les environnements sensibles, les centres de données incluent souvent des capteurs d'humidité et des systèmes de drainage automatique. Ces dispositifs permettent de détecter les fuites d'eau, d'alerter les équipes en temps réel et de rediriger l'eau pour éviter des dommages. Par exemple, des entreprises comme AWS et Google Cloud adoptent des systèmes de gestion de l'eau qui assurent une surveillance continue et une prévention des inondations, un standard pour les data centers modernes afin de garantir la disponibilité continue des services en cas de fuites imprévues.

B. Prévenir contre les incendies

La mise en place de dispositifs de sécurité contre les incendies est essentielle dans les environnements abritant des serveurs. Les salles doivent être équipées de détecteurs de fumée et de systèmes d'extinction d'incendie adaptés aux équipements électroniques, comme les systèmes à gaz inerte (FM200). Contrairement aux extincteurs à eau, les systèmes à gaz permettent d'éteindre les incendies sans endommager le matériel informatique sensible. Les centres de données de Microsoft Azure, par exemple, utilisent de tels systèmes combinés à des extincteurs portables spécifiques pour des interventions rapides, permettant de réduire les risques de destruction des données.

C. Installation d'une ventilation stable

Une ventilation stable et contrôlée est indispensable pour prévenir les surchauffes des équipements et maintenir un environnement optimal. Les data centers de grande taille utilisent souvent des systèmes de climatisation de précision capables de réguler la température et l'humidité. En plus des systèmes de ventilation redondants (N+1 ou 2N) qui prennent le relais en cas de panne, des configurations d'allées chaudes et froides organisent les flux d'air pour éviter la circulation d'air chaud. Les centres de données comme ceux d'Equinix ou Google Cloud utilisent cette technique pour garantir des températures stables et prolonger la durée de vie des équipements.

D. Mise en place d'une sécurité physique

Restreindre l'accès aux salles serveurs est une priorité pour empêcher les intrusions et les sabotages potentiels. Des dispositifs comme des badges, des lecteurs biométriques et des caméras de surveillance sont souvent intégrés aux infrastructures de sécurité. Les centres de données de Microsoft Azure, par exemple, utilisent un contrôle d'accès biométrique pour les zones sensibles. Cette technologie permet de limiter les accès aux personnels autorisés et d'assurer une traçabilité des mouvements dans les zones critiques.

E. Lutter contre les pannes de courant

Pour assurer la continuité des services, les data centers doivent être équipés de systèmes de secours comme des onduleurs (UPS) et des générateurs de secours. Les UPS fournissent une alimentation temporaire en cas de coupure pour éviter l'arrêt brutal des serveurs, tandis que les générateurs assurent une alimentation de longue durée jusqu'à la restauration de l'électricité. Par exemple, le centre de données Equinix utilise un système de redondance électrique, combinant UPS et générateurs, pour garantir une disponibilité permanente des services, même en cas de pannes prolongées.

3. Protection et sécurisation d'un hyperviseur logiquement

A. Zero trust

En appliquant le principe de Zero Trust, chaque accès est validé sans présupposer de la sécurité de l'utilisateur. Cela inclut une vérification constante des accès, même pour les utilisateurs internes. Google a mis en place une approche Zero Trust appelée BeyondCorp pour ses propres environnements, qui repose sur une gestion fine des accès en fonction des risques.

B. Logiciels type IPS

Les systèmes de prévention d'intrusion détectent et bloquent les tentatives d'attaque en temps réel. Par exemple, Cisco propose des solutions IPS qui analysent les flux réseau pour repérer les tentatives de connexion suspectes, offrant ainsi une couche de protection supplémentaire.

C. Limiter les accès aux VM

Restreindre les accès aux seules VM nécessaires par rôle et fonction. Par exemple, un développeur pourrait avoir un accès limité à une VM de test sans droits d'administration, tandis que les administrateurs disposent d'un accès global sous surveillance. Cette restriction réduit le risque d'attaque si un compte est compromis.

D. Incorporer des solutions de segmentation des machines

Segmenter les VM par groupe ou fonction isole les environnements et empêche une attaque de se propager entre les VM. Les environnements multi-tenant, comme ceux des entreprises SaaS, utilisent cette méthode pour garantir que les données des différents clients restent protégées même en cas de faille dans une VM.

E. Gestions des logs

La centralisation et l'analyse régulière des journaux permettent de détecter les anomalies et de prévenir les incidents. Des solutions de gestion des logs, comme Splunk ou Elastic Stack, permettent de collecter et analyser les journaux de sécurité pour identifier les comportements suspects. Les entreprises peuvent ainsi réagir rapidement à une tentative d'intrusion détectée dans les logs.

Synthèse de la mise en œuvre de la veille

La mise en œuvre de la veille informationnelle pour sécuriser un hyperviseur nécessite une approche organisée et optimisée, suivant plusieurs principes pour assurer l'efficacité du processus tout en limitant la surcharge d'informations. Voici les principaux aspects de cette mise en œuvre, en intégrant des idées de rationalisation, d'organisation et de partage d'informations.

Délimitation du périmètre

Pour une veille efficace, il est crucial de limiter les sujets à surveiller aux menaces spécifiques, comme les vulnérabilités des hyperviseurs et les méthodes d'attaque ciblées, par exemple les VM Escape et l'élévation de privilèges. Cela réduit le risque de dispersion des informations et améliore la qualité des données traitées.

Délimiter le périmètre nous permet de centraliser nos informations et nous permet par la même occasion d'éviter de faire un hors sujet. La restriction du flux d'information permet à la veille d'être précise sur l'étude du sujet comme par exemple établir une source d'information claire. En se concentrant sur des sources fiables comme les rapports de sécurité de CERT-FR et des bases de vulnérabilités (CVE), la veille peut cibler des informations à jour et pertinentes, facilitant une réaction rapide face aux nouvelles menaces.

Collecte d'information

Une bonne collecte d'information nous permet de vérifier les sources ainsi que les informations que l'on obtient, une des bonne pratique est de collecter depuis des sources qui sont professionnelle et reconnu pour l'être. Le but est d'éviter les erreurs de compréhension ainsi que de source qui ne serait pas fiable.

Optimisation des Ressources

L'optimisation des ressources disponibles est essentielle pour maintenir une veille active sans surcharger les équipes.

La collecte ciblée avec des outils spécialisés est l'utilisation d'agrégateurs de contenu (ex. Feedly) et de systèmes d'alertes automatiques qui permet de centraliser les informations. Les sources prioritaires, comme les bases de données de vulnérabilités, doivent être configurées pour envoyer des notifications régulières, garantissant ainsi une mise à jour en temps réel sans intervention constante (UQAM, E-Works).

La gestion efficace du temps permet d'alléger la charge de travail, des routines automatisées, comme les alertes Google, permettent de recevoir des informations spécifiques sur les nouvelles failles de sécurité. Des outils de gestion de tâches (comme Trello ou Asana) peuvent aussi aider à organiser et prioriser les activités de veille, en planifiant des moments dédiés à l'analyse et à la diffusion des informations.

Organisation et Structuration des Données

Une organisation claire et une structuration adéquate des informations sont essentielles pour faciliter leur consultation et leur exploitation.

La classification des informations doit inclure des tags spécifiques, par exemple "VM Escape", "DoS", ou "élévation de privilèges". Ces tags facilitent l'accès rapide aux données et leur traitement en fonction des besoins de l'équipe. De plus, trier les informations par dates ou degré de menace est utile pour visualiser l'évolution des risques et prioriser les réponses.

L'archivage structuré utilise des outils comme Notion, Obsidian ou encore SharePoint pour centraliser les informations et créer des dossiers thématiques est essentiel. Cela permet de retrouver facilement les informations historiques pour effectuer des analyses comparatives ou anticiper de nouvelles menaces sur la base de tendances observées.

Conclusion

La veille informationnelle sur la sécurité des hyperviseurs dans les environnements virtualisés a révélé l'importance cruciale d'une vigilance continue et d'une approche multi-outils pour faire face aux menaces croissantes. Avec l'essor de la virtualisation dans les entreprises, les hyperviseurs se positionnent au cœur de l'infrastructure IT, et leur sécurité devient une priorité stratégique.

Les analyses ont permis d'identifier des risques majeurs, tels que l'évasion de VM, l'élévation de privilèges et les attaques par déni de service, qui démontrent le niveau de vulnérabilité auquel les entreprises sont confrontées. Ces menaces, sophistiquées et ciblées, ne cessent d'évoluer et nécessitent des stratégies de protection adaptées, tant sur le plan physique que logique.

La mise en œuvre de la veille a permis de rationaliser les informations pour éviter l'infobésité et de concentrer les efforts sur les vulnérabilités et tendances les plus pertinentes. En intégrant des outils de collecte automatisée et en priorisant les sources de haute qualité, la veille informationnelle est devenue un levier essentiel pour identifier les menaces émergentes et anticiper les failles avant qu'elles ne soient exploitées par des cybercriminels. Cette approche proactive, combinée à des pratiques de segmentation réseau, de contrôle d'accès strict, et de gestion des logs, contribue à minimiser les risques liés aux failles de l'hyperviseur.

À l'instar des conclusions tirées des études sur la veille dans le secteur bancaire, notre analyse met en avant la nécessité de mesures préventives robustes. Dans un contexte où les cyberattaques deviennent de plus en plus sophistiquées, il est essentiel d'instaurer une culture de sécurité au sein des organisations, en sensibilisant les équipes à l'importance de la sécurité des hyperviseurs et en renforçant les contrôles d'accès. L'implémentation de solutions comme l'authentification multifactorielle et l'approche Zero Trust permet de renforcer la sécurité et de réduire les risques d'intrusion.

En somme, la veille informationnelle sur la sécurité des hyperviseurs a non seulement mis en lumière les risques spécifiques aux environnements virtualisés, mais a également permis de déployer des solutions adaptées pour renforcer la résilience de l'organisation face aux menaces. Cette démarche de surveillance et d'anticipation continue est devenue un pilier fondamental pour les entreprises, qui doivent être en mesure de répondre rapidement aux nouvelles vulnérabilités.

À mesure que les technologies évoluent, la veille doit rester un processus dynamique, assurant une adaptation constante aux défis et une capacité accrue à protéger l'infrastructure critique, soutenant ainsi la confiance des utilisateurs et la fiabilité des services numériques.

Bibliographie

https://fr.wikipedia.org/wiki/S%C3%A9curit%C3%A9_des_hyperviseurs

https://www.it-connect.fr/

https://www.crowdstrike.com/fr-fr/cybersecurity-101/cloud-security/hypervisors/

https://cyber.gouv.fr/publications/securite-des-systemes-de-virtualisation (pdf)

https://blogs.vmware.com/security/2020/06/virtualization-security.html