6 FEVRIER 2024

RENDEZ-VOUS AUTOUR DE VMS

Rendez-vous autour de VMS du 06 février 2024.

Mardi 6 février nous tenions un nouveau "*Rendez-vous autour de VMS*" en conférence zoom, ciblé sur la sécurité. Nous avons accueilli trois partenaires : **Imperva**, éditeur et fournisseur de services cybersécurité et filiale de Thales, **Commvault**, éditeur de solutions de protection des données, et **VSI** qui nous a présenté les mises à jour de sécurité et sa prochaine CEO. Les orateurs ont fait l'effort de s'exprimer en français afin de permettre la meilleure compréhension par nos membres et nous les en remercions particulièrement.

RAPIDE COUP D'ŒIL SUR LES INTERVENTIONS :

Imperva :

- Directive européenne *NIS2* et ses conséquences, son calendrier d'application, les obligations, reporting et pénalités.
- Services pour accompagner les entreprises.
- Sécurité des données et l'analyse des requêtes *SQL/NoSQL*.

Commvault :

- Offre VMS de l'éditeur.
- Traitements avancés sur le backup sans perturber la production: Analyse comportementale/AI, stockage local *onPrem* ou *cloud*, et déclencheur de sécurité avec notion de "*honey pot*".

Actualité **Heptapod** :

- Forge logicielle basée sur *Git/Mercurial* supportée en natif sur VMS.

VSI :

- Point sur les mises à jour de sécurité.
- Présentation par la nouvelle CEO des recommandations et ressources pour migrer vers x86.
- Echange sur les licences *hobbyist* et contributions Open source.

IMPERVA

EU Network & Information Systems Directive (NIS2)

Mohamed Lallouch, Data Security Specialist

Mohamed Lallouch nous a présenté la directive européenne *NIS2* (Network & Information Systems). Elle vient réviser la version précédente adoptée en 2016. L'objectif est d'améliorer les capacités de cybersécurité des réseaux et systèmes d'information en regard de l'augmentation des attaques. Cette nouvelle directive vient étendre la précédente, couvre plus de secteurs d'industrie et introduit de nouvelles obligations de gestion des risques et de déclaration d'incidents. Directive adoptée en janvier 2023, les 27 états de l'Union doivent la retranscrire dans leurs lois nationales avent octobre 2024. La précédente directive *NIS* avait été traduite par plusieurs textes en droit français dont le volet cyber de la Loi de Programmation Militaire de 2018.

La directive classe les organisations entre essentielles et critiques. On observe un durcissement des obligations de cybersécurité et de reporting d'incidents. Les pénalités en cas de non-conformité augmentent fortement, pouvant atteindre 10 millions d'euros ou 2% du chiffre d'affaires annuel.

La directive *NIS* considérait déjà comme essentiels les secteurs suivants : santé, transports, infrastructure numérique, eaux, banque, marchés financiers et énergie. *NIS2* vient y ajouter les fournisseurs de services numériques, la gestion des déchets, les pharmaciens/médicaments et labos, l'espace et les administrations publiques. La nouvelle catégorie des secteurs importants regroupe les fournisseurs de communications, la chimie, la production et la distribution alimentaire, les industries manufacturières, les réseaux sociaux et places de marché en ligne, et les services postaux.

Les mesures techniques, opérationnelles ou d'organisation pour gérer les risques cyber incluent notamment l'analyse des risques, la gestion des incidents, la continuité d'activité, les approvisionnements, la sécurité des systèmes et réseaux, la formation et les RH, la cryptographie et l'authentification à facteurs multiples (*MFA*) afin de prévenir ou minimiser l'impact des incidents sur les utilisateurs.

La déclaration d'incidents doit venir dans les 24h, une analyse plus poussée doit être fournie dans les 72h, suivie d'un rapport final avec l'incident, sa cause et les mesures de contrôle dans les 72h suivantes. Les pénalités pour non-conformité peuvent atteindre des niveaux très élevés, et dans le cas des entités essentielles l'autorité de contrôle peut obliger à certaines mesures ou même suspendre les responsables en cas de non respect de ces obligations...

En regard de ces obligations nouvelles ou renforcées, Imperva propose une offre de services pour accompagner les entreprises et les aider à mettre en place les outils et méthodes adaptés. Le domaine de la sécurité des données est particulièrement ciblé et la compréhension des langages de requêtes *SQL* et *NoSQL* permet une analyse fine des menaces et incidents. Des offres technologiques dans le domaine crypto et *MFA* sont proposées avec d'autres entités du groupe *Thales* pour la gestion des identités, des données et des applications.

L'éditeur *Imperva* est né en 2002 en Californie. Ses offres de cybersécurité couvrent la protection des applications (*Web Application Firewall*), des APIs et des données. L'entreprise a été intégrée au groupe *Thales* après rachat en 2023 dans la branche

cybersécurité, en complément des offres de gestion d'identité. C'est la seconde plus grosse acquisition de *Thales* après *Gemalto*.

COMMVAULT

Commvault : Solutions de protection des données sur VMS

Sébastien Weber, Senior System Engineer

Regroupement d'offres *SaaS* et *OnPremises.*
Depuis 27 ans.
Backup = dernier rempart aux attaques cyber.
Détecter en amont les menaces.
Approche *cloud* depuis longtemps, données des clients exportées vers les grands fournisseurs de *cloud*.
Certifié *FedRamp* high. *FedRamp* est un ensemble de règles de sécurité *cloud* pour les fournisseurs des agences gouvernementales US.
Revendique une activité R&D forte (brevets actifs et nouveaux dépôts, 30% du CA, 1/3 des effectifs)
Une même interface qui couvre tous les usages, historiques, *OnPremise* et *cloud*
Inclut une protection contre les rançongiciels
Agnosticité et portabilité : restaurer sur une plateforme un backup d'une autre plateforme (BD, virtualisation, o*nprem/cloud*)
Test de restauration *Cleanroom Recovery* dans le *cloud* pour analyse de malware, portes dérobées...
Une seule interface pour tout le SI, tout le backup est centralisé.
Consommé en mode *OnPrem*, *SaaS* et aussi en mode *appliance*.
Nouveauté : *ThreatWise/cyberdeception* : émulation de leurres ou d'objets attirants pour un attaquant, anciens OS, objets connectés… pour tracer les attaques.
Analyse des risques : identification des données de nature redondantes, obsolète, triviales.
Réduction des doublons, archivage des anciennes données, suppression des données qui n'ont pas à être sauvegardées. Le but est de réduire la durée/fenêtre de backup.
Scan/indexation pour données sensibles (ex soumises à RGPD) pour mieux les protéger.
Qui accède à quoi ? contrôle des droits d'accès.
Ces traitements et analyses sont réalisées sur le backup, sans perturber la production.
SecurityIQ dashboard : *scoring* de sécurité à chaque mise à jour
Ransomeware protection : suppression des accès utilisateurs, seul Commvault peut accéder aux données. Analyse comportementale (AI/ML) de l'activité.
Auto Recovery : pilotage de *PRA*, réplication sur site distant, changement de cible (*HW*, *VM*, *cloud provider*), test de *PRA* dans bulle isolée.
Threat scan : relecture des backups avec antivirus à jour, analyse IA
Backup & Recovery classique. Isolation *Air gapping*, gestion clés de chiffrement & mots de passe.

Intégration avec OpenVMS

Architecture 2 tiers ou 3 tiers : *control plane/command center, data plane* (qui fait transiter les données), stockage. *Hyperscale X Appliance*. Système proxy (Linux) avec *filesystem* Commvault qui fait l'interface avec VMS. Petit agent sur VMS. Le proxy fait la déduplication. Une fois que les données sont au format Commvault elles peuvent être

copiées/dupliquées sur tous supports.
Licence sur VMS à la volumétrie des données sauvegardées.
Versions VMS supportées/prérequis : HP Itanium 8.3, 8.4. VSI Itanium 8.4-2 & L1 avec pile *HP TCP/IP*.
Restauration complète : besoin d'une installation de base de l'OS avant de restaurer les données sauvegardées par Commvault. Pour Linux, Windows et VMs, Commvault fournit les images de boot minimales.
Nouvelle interface console HTML5, remplace Java.
Définition interactive d'accès système sur le serveur VMS, déclaration de *l'access node* (système proxy) et d'un plan de sauvegarde. Restaurations complètes ou fichier, éventuellement croisé.

Architecture

Stockage local/onPrem, *multicloud* ou *cloud* hybride. Le *Control Plane* (Commserve) peut être multiple. Interface user, en physique ou VM, sur Windows ou Linux. *Data Plane* : serveurs de média/media agent, déduplication niveau bloc global multimachine, cible NAS, SAN, Objet et bande.
Illustration d'exemples multisite + externalisation vers fournisseurs de *cloud* qui "parlent" *S3* ou Commvault *AirgapProtect* sur Azure.
Sécurité : production + leurres "*honey pot*"
Détection d'anomalies proactive. *Scan* des changements live + contrôle antivirus post backup.
En cas d'anomalie remontée du dernier backup clean.
Intégration avec gestionnaires de sécurité *SIEM* / *SOAR*.
Stockage immuable / *Air gap* (firewall) avec *CyberVault* distant. *TreatScan* : nettoyage des menaces dans les backups.

Né en 1997 au New Jersey Commvault a depuis l'origine proposé des solutions incluant VMS dans son offre de sauvegarde, restauration après sinistre et archivage multiplateforme.

Q/R : les backups sont devenus une cible prioritaire pour les attaques cyber/rançon.
Support de VMS/x86 : sera traité comme toute autre VM directement au niveau hyperviseur.

ACTUALITE HEPTAPOD

Georges Racinet

La version 1.0 d'Heptapod basée sur GitLab et qui ajoute le support de Mercurial sort aujourd'hui.
Une forge logicielle basée Git ou Mercurial, avec support de Mercurial en natif sur VMS.
Plus de détails sur *https://heptapod.net*

VSI

Adam Hoff Nielsen (Sales Director Emea)

Adam Hoff Nielsen a surtout évoqué les questions de sécurité et les mises à jour récentes.

Les points principaux sont :

- Rappel des qualités de sécurité historiques de OpenVMS
- Une initiative générale sur la sécurité est en cours chez VSI :

- pour certification *HITRUST* au printemps
- programme de reporting CVE
- conformité partielle *NIST-2*
- étude pour une certification ISO 27001

En termes de produits :

- enquête sur le rôle de backup
- l'agent *ACME* intégrera les solutions *MFA* en v9.2-3
- en v9-2 *OpenSSH* 8.9 configurable pendant l'installation de OpenVMS ; *OpenSSL 3.1* avec le module *FIPS*

Il a ensuite indiqué que les applications qui dépendent de *SSL111* doivent basculer vers *SSL3* car il n'y aura plus de mises à jour pour *SSL111*.

Concernant VMS, Adam a indiqué que "les éventuelles mises à jour de sécurité de VMS à venir seront disponibles sur les versions historiques (*Alpha*, *Integrity*) durant leur période de support selon notre feuille de route (voir https://vmssoftware.com/about/roadmap/), ainsi que sur la version x86". Pour toutes ces questions VSI recommande le passage vers x86 au plus tôt.

Darya Zelenina

Adam a ensuite passé le relais à Darya Zelenina, appelée à diriger VMSsoftware très prochainement, basée en Europe, et qui parle français.

Darya Zelenina entrera en fonction en juin prochain en tant que nouvelle directrice générale de VMS software. Elle est déjà connue des utilisateurs français depuis une présentation sur les formations lors de l'anniversaire de VMS et des contacts lors des premiers *bootcamps* avec VSI.

Fragments significatifs de sa communication :

"*C'est un réel bonheur d'être parmi vous. Je tiens à souligner la valeur exceptionnelle que VMSgenerations apporte à notre communauté globale d'utilisateurs*"

Elle est arrivée en 2017, a mené de nombreux projets sur la formation, la documentation et le marketing.

Elle a été responsable pays pendant 3 ans en Russie.

Darya a été à l'avant-garde des changements internes visant à moderniser l'entreprise, faciliter les interactions commerciales, favoriser le transfert de connaissance et la continuité opérationnelle.

Sa priorité : aider les clients à migrer vers x86 en leur fournissant les outils, l'infrastructure nécessaire et en veillant à ce qu'OpenVMS fonctionne parfaitement dans cet environnement.

On ne peut plus compter sur les serveurs *Alpha* ou *Integrity*, il est impératif de migrer vers x86 dès que possible.

Darya est ensuite passé à un exposé de méthodes, ressources et recommandations pour le portage vers ***x86***.

Il faut commencer au plus tôt l'inventaire.

Ressources de préparation chez VSI:

- Script *VSI$SUPPORT*,
- *Application Evaluation checklist*.
- Formulaire à retourner / estimation de la complexité et du coût.

Documentations fournies par VSI, instructions de configuration sur différents hyperviseurs.

Article Wiki / "considérations pour le portage x86" : points à vérifier dans le code, article ouvert aux contributions de la communauté.

Recommandation : Utiliser le plugin *IDE* (surbrillance, débogueur, gestion des sources).

Recommandation : Nécessité d'avoir des jeux de tests.

Post migration : établir un environnement de production, migrer les données. Maintenir un environnement original de secours/retour arrière durant la période d'observation de la nouvelle production.

Eléments clés d'une migration réussie, d'après les témoignages :

- Application à jour
- l'équipe connait bien l'application et ses dépendances
- la direction supporte la migration et comprend les difficultés
- S'il y a besoin d'aide : contactez VSI pour un service de découverte gratuit.

"*X86 représente l'avenir de VMS, plus tôt vous commencerez à réfléchir à la migration mieux ce sera.Nous partageons les liens vers toutes les ressources pour vous aider. Nous sommes impatients de vous aider dans vos migrations*".

ECHANGES ET QUESTIONS EN FIN DE SESSION

Q : exemples de migration vers x86 ?

R VSI: Oui, quelques clients en phase de découverte, ont commencé mais pas fini les migrations. Quelques partenaires qui ont fini la migration. Exemple Mimer éditeur de BD suédois a fini sa migration.

R HF : Oui, environ 80 à 100 clients en évaluation, test ou ayant entamé la migration. Accèdent via le service portal au support VSI avec lien engineering rapide.

Environ 1500 appels ouverts à ce jour sur les problématiques de migration.

Q : quelle répartition géographique ?

R HF: Un peu partout, alignée sur les clients de la base installée.

Q : types particuliers/profil ?

R HF: également réparti.
R : beaucoup de partenaires. Pas mal d'appels d'Oracle…

Outils : Script VSI$SUPPORT + Questionnaire à retourner à VSI.

Ensuite réunion avec VSI pour faire le point du portage et des problèmes à étudier.

Q : forum d'expérience clients qui acceptent d'en parler ?

R VSI : Le forum VSI est ouvert à cela si des clients veulent en parler.

(https://forum.vmssoftware.com/)

R VMSgenerations : question évoquée avec Adam, la première étape est d'avoir des clients qui ont migré, ensuite on pourra présenter leur expérience. Sans doute au 2è semestre.

Q : nombre de licences hobbyist ?

R VSI: Les licences d'évaluation [pour le portage x86, ndlr] sont complètes, test de x86 et possibilité d'ouvrir des appels. Les licences *hobbyist* ne permettent pas d'ouvrir directement des appels au support, mais les utilisateurs ont accès au forum VSI. Si le problème signalé est un bug, il sera remonté par un modérateur VSI. Le forum fournit aussi de l'aide à l'installation. Beaucoup d'employés VSI (jusqu'aux plus hauts responsables) répondent dans le forum.

Pour demander une licence d'évaluation : *https://share.hsforms.com/1-7usw4WOQtu6JGk9z8gPKAdi37l*

Q GC : support des ISV/éditeurs : avant il y avait deux options : option gratuite/payante avec accès au support ?

R DZ : on a un responsable ISV qui donne les licences. On va mettre l'adresse dans le chat. (*isv@vmssoftware.com*)

R HF : A priori pas de changement, partie gratuite et l'autre payante avec support. Pour x86 si la demande de licence d'évaluation est acceptée cela donne l'accès au support via le service portal. Pour présenter la demande, voir à la page d'accueil de VSI "*Apply for a license*".

Q MS : prise en compte des partenaires commerciaux ou prestataires VMS : y a-t-il un programme pour les intégrer pour accompagner les clients dans la transition vers x86 ? Ou est-ce exclusivement VSI qui fait ?

R DZ : ce n'est pas seulement VSI qui accompagne. Tout le monde peut aider ou accompagner les clients en migration vers x86. VSI a de l'expérience sur ce sujet, mais pas l'exclusivité.

R HF : Si un client a une licence d'évaluation ou un contrat de support, un partenaire peut ouvrir un appel pour le compte de ce client si besoin.

Q GC : Open source, sujet qui revient souvent dans les questions à VMSgenerations : dans le cadre des travaux de portage est il envisagé une collaboration de VSI avec des spécialistes de certains logiciels Open source ?

Pour le moment cela semble difficile, par exemple sur la question du standard de mise à disposition des sources de ces produits. Y a-t-il sur le long terme l'idée de favoriser des collaborations entre VSI et des développeurs d'Open source externes ? VSI devrait ouvrir un peu plus la porte à la collaboration.

R DZ : pouvez-vous expliquer le type de collaboration que vous envisagez ?

R GC : exemple Python : aucune collaboration avec un des spécialistes français (JFP). On est arrivé à deux filières qui avançaient sans collaborer. On avait des problèmes de réception des sources dans un format standard. Il y a maintenant des produits Open source au catalogue VSI, ce serait bien de pouvoir participer au développement comme cela se fait pour n'importe quel autre Open source. Actuellement la participation au développement d'Open source lié à VMS est quasiment fermée. Elle est absolument différente des standard Open source. On nous dit chez VSI "on n'a pas les ressources pour le faire". Cela fait 10 ans que VSI existe… il est temps d'y remédier.

R DZ : Je ne connais pas toute l'histoire ici. Nos offres Open source correspondent à des demandes de clients. Nous n'avons pas vraiment de programme Open source comme vous l'avez dit.

R HF : pas de changement à ce jour. Toujours problème de ressource pour mettre directement un environnement Open source standard sur le net. D'autre part VSI supporte ces Open source et le prix est inclus dans la licence VMS. Ca donne moins de liberté pour permettre à tout le monde de modifier les sources.

Remarque GC : Ce genre de problématique est commun à tous les logiciels Open source et ailleurs cela n'a jamais empêché le développement collaboratif classique. Une partie du code est en expérimentation et à un moment il est validé. La position de VSI est que comme VSI supporte le code il n'est pas possible de l'ouvrir. Ce n'est pas une position Open source claire. Nous avons des problèmes pour convaincre des jeunes générations à venir sur VMS, mais quand ils découvrent que c'est de l'Open source figé cela n'aide pas à convaincre de l'intérêt de VMS.

R MS : suggestion : VMSgenerations pourrait décrire les directions sur lesquelles les membres pourraient proposer de l'aide à VSI.

HF : Homi Faris

DZ : Darya Zelenina

MS : Miroslaw Szczeblewski

GC : Gérard Calliet

Nous encourageons les membres qui veulent s'impliquer et agir sur les actions de l'association à nous rejoindre pour porter plus loin les projets qui les motivent.

Un prochain message sera diffusé à ce sujet.

Le bureau de l'association est à l'écoute des utilisateurs sur les thèmes qu'ils souhaitent que nous adressions, et plus largement sur toute contribution, réaction ou suggestion pour que l'activité de l'association soit le reflet des attentes de tous.

N'hésitez donc pas à nous écrire à l'adresse mail : contact@vmsgenerations.fr