Rechercher

valables jusqu'au 30 avril aux prix partenaires indiqués.
PROMOTIONS
En savoir plus !

Crayon France finit 2020 sur une croissance de 20% et vise 25% pour 2021
26 mars - 17h00

Les jeunes professionnels de l'IT rêvent de devenir freelance
26 mars - 13h17

IBM annonce de nouveaux services de conseil et de services infogérés pour le cloud et les environnements hybrides
26 mars - 12h35

AWS recrute le patron de Tableau comme nouveau CEO
26 mars - 11h53

Computacenter France : les revenus ont progressé en 2020 mais les services et le résultat ont reculé
25 mars - 17h40

Les dépenses d'infrastructures cloud dépassent les dépenses de matériels et logiciels de centres de données
25 mars - 14h36

Deux dirigeants français sur trois prévoient

EXPERTISES

TÉMOIGNAGES PARTENAIRES

Hafnium et ses conséquences vu par cinq prestataires IT

le 15-03-2021
Par Johann Armand

Email
Print
Facebook
Twitter
Linkedin

Nous avons demandé à quelques prestataires IT de nous décrire de quelle manière Hafnium les avait affectés eux et leurs clients. Nous publions ici les témoignages de Hervé Thibault, directeur technique Metsys ; Nicolas Leroy-Fleuriot, Pdg de Cheops Technology ; Audrey Girmens, directrice générale d'Inforsud ; Damien Ecrohart, responsable des projets innovants de Soluceo ; et Benoît Thomas, technical manager Agility Center chez Exakis Nelite, en charge des outils de communications unifiées et de messagerie.

Les vulnérabilités Hafnium qui affectent les serveurs Microsoft Exchange se révèlent exceptionnelles de par la criticité des serveurs potentiellement concernés, le nombre de clients affectés, la rapidité avec laquelle elles commencé à être exploitées.

Qui est concerné ?


Hervé Thibault, directeur technique de Metsys

Les clients potentiellement affectés par Hafnium sont minoritaires mais non négligeables. « *Tout serveur Exchange publié sur Internet sur le port TCP443 [HTTPS] est impacté* », rappelle Nicolas Leroy-Fleuriot. En l'occurrence, « *les clients les plus exposés sont les clients ayant conservé une infrastructure entièrement sur site (« full on-prem ») »*, expose Hervé Thibault, directeur technique de Metsys.

Une catégorie de clientèle devenue minoritaire ces dernières années, environ 80% des clients ayant basculé sur une version online, aux dires des prestataires interrogés. Autre catégorie potentiellement affectée : les clients en architectures hybrides. « *20% de nos clients infogérés ont dans leur architecture un serveur Exchange dont une version est concernée par la faille* », estime ainsi Audrey Girmens chez Inforsud.

Que faut-il faire ?


Benoît Thomas, technical manager Agility Center chez Exakis-Nelite

Tous s'accordent pour dire qu'il a fallu réagir très vite. La particularité de ces 4 CVE [Common Vulnerabilities and Exposures] c'est qu'elles ont commencé à être exploitée par plusieurs groupes d'attaquants dès leur révélation le 18 février et avant même la disponibilité des patchs Microsoft (prévus le 3 mars), comme le rappelle Benoît Thomas d'Exakis Nelite.

Dans ce contexte, la première chose à faire était d'exécuter les scripts fournis par Microsoft pour s'assurer que les infrastructures des clients étaient protégées et, dans le cas contraire, de déployer les patchs. « *Notre urgence [a été] de déployer les patchs au plus vite afin de limiter la durée d'exposition de ces serveurs Exchange*, souligne Audrey Girmens. *Nos équipes sont mobilisées pour prendre contact avec nos clients, leur expliquer le contexte, la faille et les enjeux. Puis nous planifions l'intervention avec nos clients, ce sont nos consultants Réseaux & Systèmes et nos experts cybersécurité qui réalisent l'opération selon la méthodologie définie en interne.* »

Chez Cheops, « *ceux ayant souscrit à nos services de maintien en conditions opérationnelles (MCO) de leur architecture Exchange ont été patchés dans les 48h* », indique Nicolas Leroy-Fleuriot. « *[Compte-tenu] de la criticité alarmante des attaques chez les clients impactés, nous avons aussi appliqué notre devoir de conseil et assistance à tous nos clients pour leur expliquer l'urgence de la mise en sécurité de leur service de messagerie* […] », poursuit ce dernier.

Patch et Cumulative Update

Une fois les patchs déployés, la deuxième étape consiste à installer la dernière Cumulative Update (CU) d'Exchange, qui corrige les vulnérabilités. « *Une installation longue car la dernière CU remplace une grosse partie du code source Exchange et nécessite une extension du schéma Active Directory* », souligne Benoît Thomas, d'Exakis Nelite.


Damien Ecrohart, responsable des projets innovants chez Soluceo

Et une fois la CU installée, il faut encore s'assurer que les clients n'ont pas été compromis. « *Nous restons vigilants pour la suite, même après la correction, en utilisant les éléments fournit Microsoft pour rechercher les indicateurs de compromission (IOC) associés aux vulnérabilités de type « zero-day »*, relate Damien Ecrohart, de Soluceo, chez qui c'est essentiellement l'équipe support, avec l'aide de l'équipe sécurité, qui a traité la remédiation en proposant un accompagnement à l'intégralité des clients.

Chez Metsys, Hervé Thibault relate : « *lorsque nous avons eu connaissance du problème, le 2 mars 2021, notre stratégie a été de nous appuyer sur notre SOC (Security Operations Center) pour proposer une réponse centralisée, claire et structurée à nos clients. Les forces commerciales et techniques ont été mobilisées sur le premier « geste barrière » à indiquer à nos clients : limiter la « contamination » en appliquant les correctifs de sécurité sur tous les Exchange Server (2023, 2016, 2019) concernés. En parallèle, le SOC, accompagné d'experts Exchange de différentes agences, prépare un plan d'action pour traiter le « mal » en profondeur, sur la base des recommandations proposées par Microsoft et via différents angles de détection : Analyse des logs Exchange, identification de process connus dans l'attaque (procdump, powercat), détection d'activités « suspicieuses », notamment au travers de Microsoft Defender for EndPoints (ex-Defender ATP) et Azure Sentinel, l'outil de SIEM de notre SOC. Nous en sommes maintenant dans la phase d'analyse des dégâts et de corrections plus en profondeur avec nos clients.* »

Qui est à la manœuvre ?

Bien-entendu, devant l'urgence de la situation, les partenaires ont pu mobiliser des ressources au détriment d'autres projets moins urgents.


Audrey Girmens, directrice générale d'Inforsud

« *Ces opérations peuvent impacter nos plannings de projets d'infrastructure mais nous préférons assurer le déploiement de ces patchs au plus tôt pour une meilleure sécurisation de nos clients*, admet Audrey Girmens. *Nous partageons ces impacts avec nos clients en toute transparence* ».

« *Nous sommes effectivement en tension sur des ressources d'expertise, notamment parce que nous avons un certain nombre de collaborateurs qui disposent d'une double expertise Active Directory & Exchange Server, et qui sont donc déjà fortement mobilisés chez des clients qui subissent des attaques autour d'Active Directory (notamment faille Zerologon), avec souvent des opérations de récupération très lourdes à mettre en œuvre* », explique pour sa part Hervé Thibault. Avant de nuancer : « *Mais notre offre « Services Managés » SOC, avec son organisation et son mode de delivery, nous a permis quand même d'être très réactif sur le sujet et de répondre présent, en complément de la proximité des clients via nos agences régionales.* »

Ce qu'Hafnium enseigne au marché


Nicolas Leroy-Fleuriot, Pdg de Cheops Technology

Pour autant, l'affaire Hafnium présente quelques vertus aux yeux des partenaires. Cela peut être l'opportunité de vendre de nouveaux services. C'est le cas chez Cheops Technology où « *lors de l'application du plan de remédiation chez nos clients nous pouvons relever aussi des axes d'amélioration*, relate Nicolas Leroy-Fleuriot. *Nous sommes dans certains cas sur des basiques, avoir un inventaire à jour, une solution de patchmanagement, une surveillance du périmètre de sécurité, une revue des accès, appliquer les bonnes pratiques de sécurité, intégrer la sécurité dans les projets…* ».

Chez Metsys, on y voit l'occasion de rappeler les règles de prudence aux clients. « *Ce nouvel exploit vient nous rappeler que tous les composants du SI sont potentiellement impactés et ciblés, comme le fut en son temps Slammer (2003) qui ciblait les environnements SQL, et comme l'est aujourd'hui cette nouvelle attaque qui vise un élément hautement stratégique des entreprises* », souligne Hervé Thibault. À l'intention des clients, il ne peut que répéter : « *patchez, patchez, patchez !* » Et s'il devait garder un enseignement, c'est « *la supériorité de l'approche SOC, qui permet d'être en capacité de répondre* [aux] *clients de manière très réactive, sans désorganiser* [les] *organisations/prestations techniques existantes. Et pour* [les] *clients du SOC, c'est la garantie d'un canal prioritaire pour le traitement de leurs incidents.* »