Bitdefender permet à TUI Benelux de détecter les failles de sécurité en temps réel et de réaliser des enquêtes forensics poussées

LE DÉFI

TUI Benelux exploite trois datacenters équipés d'outils assurant une redondance et sont gérés par une équipe IT de 160 personnes. "Comme toute autre entreprise gérant un grand nombre de transactions clients et traitant de données sensibles, la sécurité de l'information est primordiale chez TUI", déclare Theo Kip, IT Risk and Compliance Officer chez TUI Benelux. "Naturellement, tous nos terminaux, tels que les PC et les ordinateurs portables, sont équipés d'une solution antimalware, et nos réseaux et serveurs sont protégés par des pare-feux et autres outils de cybersécurité. Néanmoins, nous avons constaté que nous pouvions faire encore mieux".

Une révision de la loi néerlandaise sur la protection des données personnelles et, dans son sillage, l'obligation de signaler les fuites de données, ont poussé l'entreprise à chercher urgemment des moyens d'améliorer ses outils actuels d'enregistrement des événements de sécurité. Theo Kip explique : "Lors d'une visite sur un salon professionnel, nous avons rencontré les équipes de Bitdefender. Leur solution d'analyse de sécurité du trafic réseau (NTSA) m'a semblé une option intéressante : non seulement elle offrait une détection 'inside out' des malwares, mais elle fournissait également les capacités les plus complètes du marché en matière d'enquêtes forensics".

LA SOLUTION

TUI Benelux a demandé à Bitdefender de mettre en place un PoC (Preuve de Concept). Theo Kip précise : "Pendant le PoC, nous avons travaillé en étroite collaboration avec les experts de Bitdefender. Nous avons évalué en détail la solution. Et nous avons même demandé à Bitdefender d'ajouter des fonctionnalités. Par exemple, nous avons eu des demandes concernant le traitement des alertes, l'assignation des tickets et la documentation des incidents. Bitdefender a pris nos demandes en compte".

Suite au PoC, TUI Benelux a décidé de déployer la technologie Bitdefender NSTA. "Le PoC a été très convaincant", ajoute Theo Kip. "Nous avons fait le choix d'acquérir un total de trois appliances NTSA pour nos datacenters aux Pays-Bas et en Belgique".

TUI AG, l'un des leaders mondiaux du tourisme, prend en charge 20 millions de voyageurs par an. TUI est bien plus qu'un simple tour opérateur : il possède plus de 300 hôtels dans 30 pays, ainsi qu'une flotte d'une quinzaine de bateaux de croisière et plus de 150 bus et avions. TUI Benelux regroupe les activités belges et néerlandaises, et gère plus de 1,6 million de voyageurs par an rien qu'aux Pays-Bas.

Industrie
Tourisme

Siège
TUI AG - Hanovre, Allemagne

TUI Benelux - Enschede, Pays-Bas ; Ostende, Belgique

Employés
TUI AG – 67 000 à travers le monde

TUI Benelux – 2 500 (équipe informatique : 160)

Ronny Tyink, Team Leader System Engineering Network TUI Benelux, explique pourquoi il a choisi l'appliance physique plutôt que la version sous forme de machine virtuelle : "Nous n'avions pas VMware installé et configuré sur tous nos sites. La version physique a l'avantage de pouvoir fonctionner indépendamment de la disponibilité de VMware".

Étant donné que la phase de PoC s'est parfaitement bien déroulée, le déploiement des appliances Bitdefender s'est avéré très simple et rapide, explique Theo Kip. "En fin de compte, Bitdefender a laissé les appliances que nous avions utilisés lors du PoC. Cela nous a permis d'économiser beaucoup de temps et d'efforts. Le partie hardware n'est pas le plus important dans la technologie Bitdefender. La Threat Intelligence en cybermenaces est, à mon avis, la partie cruciale".

LES RÉSULTATS

La solution Bitdefender NTSA a fait ses preuves depuis son déploiement chez TUI Benelux en septembre 2016. Theo Kip le confirme : "Par exemple, nous avons reçu des alertes concernant des malwares lorsque les ordinateurs portables infectés de collègues du Maroc et de Suisse se sont connectés à notre réseau interne. Grâce à la technologie Bitdefender NTSA et à la fonctionnalité de journalisation, nous avons pu avoir des détails précis sur les cyberattaques, notamment quels ont été les appareils touchés et à quels emplacements. La solution nous permet de transformer la suspicion en certitude".

Suite aux excellents retours d'expérience autour de la technologie Bitdefender NTSA, Theo Kip et Ronny Tyink n'excluent pas la possibilité que la solution soit déployée au sein d'autres filiales de TUI. Theo Kip précise : "J'ai des discussions régulières avec mes collègues européens pendant les réunions du TUI Information Security Board. Nous y discutons de l'actualité et définissons les politiques de sécurité de l'information pour l'ensemble du groupe TUI. C'est une bonne occasion pour discuter de Bitdefender NTSA avec mes collègues".

"Grâce à la technologie Bitdefender NTSA et à la fonctionnalité de journalisation, nous avons pu voir exactement qui avait été infecté, sur quel périphérique et à quel endroit. La solution nous permet de transformer la suspicion en certitude".

Theo Kip, IT Risk and Compliance Officer, TUI Benelux

Solution Bitdefender
- Bitdefender Network Traffic Security Analytics

Environnement
- VMware vSphere

Systèmes d'exploitation
- Microsoft Windows

19052020-Bitdefender-CaseStudy-TUI-crea3687-a4-fr_FR