TÉMOIGNAGE CLIENT AKAMAI

Kaneka Corporation

Kaneka Corporation renforce sa stratégie de sécurité et protège le trafic direct vers Internet avec Secure Internet Access Enterprise

Améliorer la sécurité à travers l'ensemble du groupe

Kaneka est un fabricant complet de produits chimiques qui produit et vend une large gamme de matériaux et de produits, dont des produits chimiques, des produits pharmaceutiques, des produits alimentaires, des équipements médicaux et des matériaux électroniques.

L'entreprise, dont les sièges sociaux sont situés à Tokyo et à Osaka, compte 3 500 employés directs et plus de 10 000 employés sur l'ensemble des effectifs consolidés du groupe.

Le Centre de solutions IoT de l'entreprise supervise à lui seul les systèmes d'information et la sécurité de l'ensemble de l'entreprise. Sous la direction de Tetsuro Yabuki, directeur du Groupe de solutions d'entreprise, le Centre a activement encouragé l'utilisation de SaaS/PaaS et la centralisation des serveurs virtualisés dans le cadre de sa politique de promotion du cloud, qui a débuté par l'adoption de Microsoft 365 dans l'ensemble de l'entreprise en 2011. Actuellement, outre le fait qu'environ 90 % des serveurs basés sur Windows sont déployés sur Microsoft Azure ou dans des environnements de cloud privés, une configuration de cloud hybride est également utilisée pour l'infrastructure des systèmes stratégiques de l'entreprise.

Le Centre de solutions IoT s'efforce depuis quelque temps de résoudre des problèmes spécifiques tout en poursuivant sa transformation informatique vers un environnement tourné vers le cloud, le principal enjeu étant l'amélioration de la sécurité sur l'ensemble du groupe Kaneka.

Facilité et rapidité de déploiement à l'échelle mondiale

M. Yabuki explique qu'en raison de l'absence de tout incident de cybersécurité grave chez Kaneka depuis un certain temps, les employés n'étaient guère préoccupés par les cyberattaques et étaient généralement peu sensibilisés à la sécurité.

« Toutefois, une série d'incidents de sécurité inquiétants survenus en 2017 ont complètement changé la donne », a-t-il ajouté.

« Bien que chaque incident de sécurité individuel n'ait pas été grave, le cyber-risque encouru par l'entreprise est devenu manifeste, et le Centre de solutions IoT a dû, à lui seul, résoudre ces problèmes le plus rapidement possible. Nous avons élaboré un plan visant à améliorer en profondeur le dispositif de sécurité de Kaneka et avons établi une politique visant à renforcer la gouvernance de la sécurité sur l'ensemble du Groupe, y compris dans nos bureaux à l'étranger », déclare M. Yabuki.

Kaneka Corporation
Tokyo, Japon
www.kaneka.co.jp/

Secteur
Distribution et grande distribution

Solution
Secure Internet Access Enterprise

Impacts majeurs

- Amélioration générale de la sécurité du trafic Web sortant en deux mois grâce à un simple changement de DNS
- Protection rapide des filiales dotées d'une connectivité directe vers Internet
- Blocage et identification proactifs des points de terminaison compromis

Le plan exhaustif de cybersécurité de Tetsuro Yabuki comprenait l'amélioration de son dispositif de sécurité contre les menaces pesant sur le trafic réseau sortant et entrant et contre les menaces susceptibles de compromettre les terminaux des points de terminaison. Ayant déjà sélectionné une plateforme de protection des points de terminaison et des solutions de détection et de réponse des points de terminaison, Kaneka entendait les compléter en ajoutant un niveau de protection supplémentaire pour son trafic sortant. Pour cela, l'entreprise a décidé de mettre en œuvre Secure Internet Access Enterprise, la solution de sécurité basée dans le cloud d'Akamai.

Le service Secure Internet Access Enterprise bloque le trafic malveillant à l'aide des renseignements exhaustifs d'Akamai sur les menaces en temps réel, bloquant de manière proactive les requêtes DNS malveillantes en les redirigeant simplement vers l'Intelligent Edge Platform d'Akamai. Ce service empêche de manière préventive les terminaux de l'entreprise de se connecter à des sites Web malveillants et à des serveurs commande et contrôle (C2), ce qui réduit considérablement le risque que les terminaux soient compromis par hameçonnage ou par des logiciels malveillants, ce qui pourrait entraîner le vol d'informations de l'entreprise. Les mises à jour automatiques et continues des informations sur les menaces éliminent le besoin de toute intervention manuelle des administrateurs.

Keiji Fujimoto, responsable du Groupe de solutions d'entreprise, en charge des mesures de sécurité globales, nous explique les raisons de l'adoption de Secure Internet Access Enterprise.

« L'un des critères qui nous ont poussés à choisir Secure Internet Access Enterprise était le caractère innovant et la simplicité d'utilisation du DNS en tant que solution pour assurer la sécurité, qui est véritablement unique. Nous estimions qu'il s'agissait d'une solution que seul Akamai, le plus grand fournisseur DNS au monde, pouvait proposer. Nous pensons qu'il s'agit d'un service de sécurité dans le cloud révolutionnaire qui tire parti de manière experte des points forts d'Akamai. »

En outre, M. Fujimoto estime que Secure Internet Access Enterprise répondait parfaitement aux exigences de protection du trafic sortant de Kaneka.

« Ce plan de cybersécurité avait également pour objectif d'unifier les mesures de sécurité au sein de l'ensemble du Groupe Kaneka et de renforcer notre gouvernance de la sécurité. La facilité et la simplicité de la mise en œuvre de Secure Internet Access Enterprise ont permis d'accélérer le déploiement de ces mesures. Nous avons également été bluffés par la capacité de Secure Internet Access Enterprise à bloquer les communications malveillantes, quelle que soit la structure du réseau de notre entreprise. »

Un déploiement dans les bureaux à l'étranger de l'entreprise en l'espace de deux mois

Kaneka protège déjà l'ensemble des points de sortie de son réseau d'entreprise à l'aide de Secure Internet Access Enterprise et a pratiquement terminé le déploiement de la solution auprès des entreprises du groupe situées au Japon et à l'étranger.

Les systèmes d'information des bureaux et des sièges sociaux de Kaneka à l'étranger sont répartis sur quatre régions : Amérique du Nord et du Sud, Europe/Afrique, Malaisie et Japon/Asie. Le Japon ayant pris la tête du système de renforcement de la gouvernance de la sécurité, les équipes de sécurité de l'information représentant les trois autres régions se sont alignées sur le Japon pour déployer Secure Internet Access Enterprise à l'échelle mondiale.

« La coopération autour de la mise en œuvre de Secure Internet Access Enterprise dans les différentes régions a été très simple. Je parle de mise en œuvre, mais tout ce que nous avions à faire était de changer la destination de la requête DNS récursive. Le déploiement à l'étranger s'est donc déroulé sans problème et nous avons pu le réaliser en deux mois », rapporte M. Fujimoto.

Protection des connexions directes vers Internet

Pour les entreprises du groupe implantées au Japon, M. Yabuki et son équipe ont visité et convaincu les entreprises qui n'utilisaient pas le centre de données de Kaneka, c'est-à-dire qui exécutaient leurs systèmes dans des environnements séparés et disposaient de points de sortie directs vers Internet distincts.

Outre le déploiement de Secure Internet Access Enterprise au sein même de Kaneka, l'entreprise utilise

> Le principe visant à utiliser le DNS comme mesure de sécurité est à la fois révolutionnaire et tout à fait logique. C'est une solution que seule une entreprise comme Akamai peut proposer.
>
> **Keiji Fujimoto**
> Responsable du Groupe de solutions d'entreprise, Centre de solutions IoT de Kaneka Corporation

désormais Secure Internet Access Enterprise pour protéger le trafic sortant des bureaux disposant d'une connexion directe vers Internet.

« Chez Kaneka, bien que nous n'autorisions actuellement que les connexions directes vers Internet dans certains bureaux, nous avions besoin d'un dispositif capable de protéger le trafic sortant de ces bureaux. Je suis particulièrement satisfait de la facilité avec laquelle Secure Internet Access Enterprise nous a permis d'y parvenir », déclare M. Fujimoto.

Identification rapide des terminaux compromis

Secure Internet Access Enterprise ayant été adopté à travers l'ensemble du Groupe Kaneka, et Kaneka et l'ensemble de ses entreprises composant le Groupe bloquant désormais de manière proactive les communications vers les sites Web malveillants et les serveurs C2 depuis tous les terminaux, le Centre de solutions IoT est désormais en mesure de détecter et de vérifier rapidement tout terminal effectuant des communications malveillantes. M. Yabuki affirme que, de ce fait, l'entreprise est en mesure de prendre des mesures immédiates pour traiter les terminaux à risque dans l'ensemble des entreprises du Groupe Kaneka.

« Il suffit d'un seul "terminal à risque" au sein du Groupe pour que le problème se transforme potentiellement par la suite en un problème majeur. Le fait de pouvoir identifier ce type de terminaux à travers l'ensemble du Groupe grâce à Secure Internet Access Enterprise s'est avéré extrêmement efficace », déclare M. Yabuki.

M. Fujimoto ajoute qu'il arrivait parfois qu'une personne au sein de l'organisation démarre un terminal qui n'avait pas été utilisé depuis longtemps, et que ce terminal soit alors identifié comme étant à risque.

« Il s'agit là de situations dans lesquelles on peut se retrouver sans s'en rendre compte à utiliser un ancien terminal infecté par un logiciel malveillant, ayant échappé au contrôle du département des systèmes d'information. Lorsque de tels risques de sécurité se matérialisent, un autre avantage offert par l'utilisation de Secure Internet Access Enterprise est la possibilité de détecter rapidement le terminal, de bloquer ses communications et de mettre un terme à cette menace », ajoute M. Yabuki.

« Les mesures de sécurité sont une composante essentielle du monde des affaires », poursuit M. Yabuki. « C'est exactement la raison pour laquelle nous pensons que nous devons investir dans la sécurité de manière en accord avec le volume de nos ventes et notre réputation. Cette soudaine apparition d'incidents de cybersécurité chez Kaneka est probablement liée à une augmentation significative du degré de notoriété de l'entreprise suite à de récentes activités promotionnelles. Plus la valeur d'une entreprise augmente, plus les cyber-risques se multiplient. C'est pourquoi il est important de se concentrer sur l'exploitation de technologies innovantes telles que Secure Internet Access Enterprise, tout en continuant à améliorer nos mesures pour protéger la valeur de notre entreprise. »

kaneka

L'entreprise a été créée en septembre 1949 suite à sa séparation de la Kanegafuchi Spinning Company, Ltd. Lors de sa création, l'entreprise était connue sous le nom de Kanegafuchi Kagaku Kogyo Co, Ltd. (remplacé par son nom actuel en 2004). L'entreprise a débuté en tant que fabricant de produits chimiques en développant le polychlorure de vinyle, baptisé Kanevinyl par l'entreprise. Aujourd'hui, l'entreprise propose une large gamme de produits chimiques, de résines fonctionnelles, de résines moussantes, de produits alimentaires, de produits pharmaceutiques, d'équipements médicaux, de matériaux électroniques, de cellules solaires et de fibres synthétiques. Ces dernières années, l'entreprise a étendu sa philosophie visant à rendre le monde plus sain en contribuant à la protection de l'environnement mondial, notamment en développant le polymère biodégradable PHBH, qui est 100 % biodégradable dans l'eau de mer, ainsi qu'en fournissant des compléments alimentaires tels que la forme réduite de la coenzyme Q10 (Ubiquinol) et en fabriquant et en vendant des produits laitiers tels que le produit « Milk for Bread » : https://www.kaneka.co.jp/.