Étude de cas

Conseil municipal de Coventry

RansomCare

La municipalité de Coventry protège ses citoyens, son personnel et ses services grâce à la meilleure défense contre les ransomwares proposée par Ricoh

Le conseil municipal de Coventry se sentait de plus en plus concerné par la recrudescence d'attaques par ransomware. Les périodes de confinement liées au COVID-19 ont accentué l'inquiétude sur les risques de cybersécurité car il devenait complexe de s'assurer des bonnes pratiques du personnel alors en télétravail. Pour sécuriser son réseau, Coventry a donc décidé de déployer RICOH RansomCare, une décision qualifiée d'« évidence ».

Résumé

Nom : Conseil municipal de Coventry
Lieu : Coventry, West Midlands
Taille : 5 500 employés
Activité : Administration locale

Défis

- Risque pour la continuité du service et coût élevé lié à la récupération des données
- La pandémie de COVID-19 et le télétravail ont accentué le problème
- Menace croissante des attaques de ransomware

Solution

- Ricoh RansomCare
- Conseils d'experts Ricoh

Avantages

- Offre une des meilleures défenses contre les ransomwares
- Protège contre la menace accentuée par davantage d'employés travaillant en distanciel
- Offre un bon rapport protection/prix au regard des potentiels dommages et au coût de l'attaque
- Installation simple et rapide en une demi-journée seulement
- Impact minimal et peu d'intrusion sur l'infrastructure informatique

Étude de cas: Conseil municipal de Coventry

Défis

Le conseil municipal de Coventry est une instance décisionnelle chargée de fournir des services administratifs locaux aux 360 000 habitants de la ville. Coventry a été désignée comme la ville britannique de la culture en 2021. Le conseil a mis en œuvre un programme de transformation numérique pour améliorer le fonctionnement et la prestation des services proposés à la communauté. Il vise à développer une main-d'œuvre plus agile grâce à des technologies innovantes telles que Microsoft Office 365, des outils de communication et de collaboration, et à doter l'ensemble du personnel d'une technologie mobile.

Cette stratégie numérique s'accompagne d'un solide régime de cybersécurité, avec plusieurs technologies en place pour assurer la protection des citoyens, du personnel du conseil et des services qu'il fournit. Grâce à cette approche stratifiée de la sécurité informatique, les systèmes du conseil sont très bien protégés contre les menaces connues ou inconnues.

Mais comme beaucoup d'autres organisations et entreprises, la municipalité de Coventry est de plus en plus préoccupée par les ransomwares. Il s'agit d'un logiciel malveillant que des criminels motivés par l'argent utilisent pour attaquer les données.

Une fois dans le système d'une entreprise, le ransomware crypte les fichiers pour les rendre inaccessibles. Il modifie les extensions des fichiers plutôt que leur nom, de sorte qu'il est difficile de retrouver les fichiers corrompus. Les ransomwares peuvent infecter jusqu'à 7 000 fichiers par minute. Les criminels exigent ensuite un paiement et prennent donc en otage les données et informations essentielles de l'entreprise.

L'impact des ransomwares a été mis en évidence lorsqu'une autre autorité locale britannique a été attaquée fin février. Il lui a fallu deux mois pour récupérer ses données et rétablir ses services. Une entreprise internationale touchée par un ransoware a vu le cours de ses actions s'effondrer et la restauration lui coûter des millions d'euros. L'autre facteur qui a poussé le Conseil municipal de Coventry à agir est la pandémie de COVID-19 et la vulnérabilité accrue due au nombre élevé d'employés travaillant à domicile.

« La défense traditionnelle contre les cyberattaques repose sur la technologie des points d'extrémité (endpoints), comme les pares-feux ou les logiciels antivirus, et l'intrusion dans le réseau ; elle se concentre davantage sur la prévention plutôt que sur le cryptage. Son but est d'empêcher toute intrusion dans votre réseau. Mais que se passe-t-il si quelque chose s'introduit dans votre réseau ? C'est le véritable danger des ransomwares. Le seul moyen de l'arrêter est un verrouillage physique. Mais le temps que vous le fassiez, beaucoup de dégâts ont déjà été faits », explique Gary Griffiths, ICT Engagement Lead, Conseil municipal de Coventry. « Le problème principal concerne le temps et le coût de la restauration des services et c'est un problème croissant. »

Le Conseil municipal de Coventry a discuté du problème avec Ricoh, qui est désormais l'un de ses principaux partenaires stratégiques. En réponse à cette menace, Ricoh a développé une solution pour aider les organisations à se défendre contre les ransomwares. M. Griffiths explique : « Lors de nos recherches et de notre évaluation de la solution de Ricoh, nous avons constaté qu'il n'existait rien de tel sur le marché pour offrir une dernière ligne de défense aussi efficace. La décision de choisir la solution Ricoh n'a donc pas été difficile à prendre. »

Solution

Le Conseil municipal a installé la solution RansomCare de Ricoh créée par BullWall et y a associé les services d'assistance de cybersécurité de Ricoh. RansomCare est une application sans agent qui est installée sur un serveur virtuel dans le système informatique central du conseil et non à chaque endpoint. Elle surveille, en temps réel, les données de l'ensemble de l'entreprise. Elle peut repérer une attaque de ransomware, généralement via un ordinateur portable ou un ordinateur de bureau, n'importe où sur le réseau, même si celle-ci a réussi à contourner les systèmes de sécurité existants. Instantanément, RansomCare verrouille l'emplacement et empêche la propagation du ransomware.

Un tableau de bord présente au service informatique une image en temps réel de l'activité et déclenche une alerte instantanée en cas d'attaque. Le système fournit automatiquement un audit et un rapport d'attaque détaillés à des fins d'analyse et de conformité avec le RGPD.

La solution a commencé par protéger les principales données du conseil municipal, mais elle est maintenant appliquée à d'autres données telles que les applications SharePoint et Office 365 hébergées sur site. Bien que le Conseil municipal de Coventry n'en ait pas aujourd'hui l'usage, RansomCare peut également protéger les données dans le Cloud.

Afin d'aider la municipalité, le service de Ricoh comprenait cinq jours de conseil portant sur l'installation, la surveillance et la formation, le tout à distance. La solution a été évaluée, planifiée, testée et déployée en deux mois. L'installation du logiciel a été encore plus rapide : une demi-journée seulement. Le logiciel BullWall a été loué à Ricoh dans le cadre d'un plan d'assistance de 5 ans.

Avantages

La solution Ricoh RansomCare offre au Conseil municipal de Coventry l'une des meilleures défenses contre les ransomwares actuellement disponibles sur le marché. Elle est rapide et facile à installer et a un impact minimal sur l'infrastructure et les performances informatiques. Par rapport à l'impact sur les services, la continuité des activités et le coût de la gestion d'une attaque de ransomware, elle offre un très bon rapport qualité-prix. Même en cas d'attaque, RansomCare la stoppe instantanément avant qu'elle ne cause des dommages considérables. La solution protège les données que le conseil municipal utilise pour fournir ses services, qu'il s'agisse des routes, de l'éducation, des services sociaux ou des finances.

M. Griffiths déclare : « Avec un peu de chance, la municipalité de Coventry ne subira jamais d'attaque de ransomwares, mais la solution RansomCare de Ricoh est comme une police d'assurance. Si nous n'avions pas fait cela et que nous avions subi une attaque, nous aurions dû expliquer pourquoi, pour le prix de la solution, nous aurions pu éviter le blocage du système pendant des mois et les millions dépensés pour réparer les données. Désormais, si une attaque de ransomware venait à contourner nos défenses de façade, nous aurions une assurance. »

L'un des principaux avantages a été de contrer l'impact du confinement imposé pendant la pandémie de COVID-19. La municipalité a reconnu que les risques étaient accrus en raison de l'augmentation du nombre d'employés travaillant à distance. Malgré des systèmes de sécurité robustes, le plus grand risque pour une organisation est qu'un utilisateur commette une erreur, clique sur un lien dans un courriel et accède à des sites Web dangereux ou qu'il insère qu'il utilise un support de stockage USB infecté. Ce risque augmente lorsque les personnes sont éloignées du bureau et moins attentives aux pratiques de sécurité.

M. Griffiths ajoute : « RansomCare est là pour protéger le réseau au cas où quelque chose s'y introduirait. Il se peut qu'il ne soit jamais utilisé. Mais avec les inquiétudes au niveau mondial concernant la croissance des attaques de ransomwares et les cybercriminels qui deviennent de plus en plus créatifs, nous faisons plus que la plupart des gens pour protéger la municipalité, ses données et les services qu'elle offre. »

Solution/Produits de Ricoh RansomCare

- RansomCare
- Logiciel Bullwall
- Services de formation et conseils Ricoh

« Avec un peu de chance, le Conseil municipal de Coventry ne subira jamais d'attaque de ransomware, mais la solution RansomCare de Ricoh est comme une police d'assurance. Si nous n'avions pas fait cela et que nous avions subi une attaque, nous aurions dû expliquer pourquoi, pour le prix de la solution, nous aurions pu éviter le blocage du système pendant des mois et les millions dépensés pour réparer les données. Désormais, si une attaque de ransomware venait à contourner nos défenses de façade, nous aurions une assurance supplémentaire concernant la façon dont nous pouvons gérer l'impact. »

Gary Griffiths, ICT Engagement Lead, Conseil municipal de Coventry

RICOH
imagine. change.