

Casus

Gemeente Coventry
Ricoh RansomCare -
powered by BullWall

RICOH
imagine. change.

De gemeente Coventry stopt ransomware met Ricoh RansomCare - powered by BullWall



Thuiswerken en hybride werken wordt meer en meer de norm. Ook in de gemeente Coventry in Engeland. Mede daardoor maakten ze zich daar steeds meer zorgen over het toenemende aantal ransomware-aanvallen.

De gemeente zocht een oplossing die snel en simpel te installeren is én die een extra verdedigingslinie vormt tegen een mogelijke aanval. Dat werd Ricoh RansomCare - powered by BullWall.

Samenvatting

Opdrachtgever: Gemeente Coventry
Locatie: West Midlands, Engeland
Personeel: 5500 medewerkers
Activiteiten: Lokale overheid

Vraagstuk

- Groeiend aantal ransomware-aanvallen
- Bedreigt de continuïteit van de dienstverlening
- Risico op hoge herstelkosten

Oplossing

- Ricoh RansomCare - powered by BullWall
- Deskundig advies van Ricoh

Voordelen

- Beschermt tegen ransomware
- Vermindert risico's van collega's die op afstand werken
- Voorkomt schade en hoge kosten door een aanval
- Makkelijk en snel te installeren, in een halve dag
- Heeft minimale impact op de IT-infrastructuur

Uitdaging

De gemeente Coventry ligt in de regio West Midlands in Engeland en telt zo'n 360.000 inwoners. Een aantal jaar geleden rolde de gemeente een digitaal transformatieprogramma uit, om de dienstverlening aan burgers en ondernemers te verbeteren.

De gemeente wil voor alle medewerkers flexibele manieren van (samen)werken mogelijk maken. Ze ontsluiten innovatieve communicatie- en samenwerkingstools en mobiele toepassingen. Onderdeel van dit streven is een cybersecurity-aanpak met verschillende technologieën die inwoners, medewerkers en de gemeentelijke dienstverlening beschermen. Zodat de systemen een betrouwbare barrière vormen tegen bekende en onbekende dreigingen.

Toch ging de gemeente Coventry zich gaandeweg zorgen maken over het toenemende aantal ransomware-aanvallen wereldwijd. Met dit soort aanvallen kapen criminelen data om hier financieel voordeel mee te behalen. Ransomware versleutelt documenten in het systeem van een organisatie, zodat de toegang geblokkeerd wordt. Het kan tot wel 7000 bestanden per minuut infecteren. Ransomware verandert bestandextensies en niet de namen, zodat het moeilijk is om beschadigde bestanden te detecteren.

De impact van ransomware werd pijnlijk duidelijk toen eind februari een andere lokale overheidsinstantie in het VK werd aangevallen. Het kostte ze twee maanden om alle gegevens en diensten te herstellen. En een internationaal bedrijf dat werd getroffen door ransomware, zag zijn aandelenkoers kelderen. Het kostte miljoenen om dit te herstellen. De druppel voor de gemeente Coventry was dat ze zich bewust werden van de risico's die thuiswerken met zich meebrengt.



Garry Griffiths is ICT Engagement Lead bij de gemeente Coventry. Hij vertelt: *“Een traditionele bescherming tegen cyberaanvallen bestaat uit preventieve endpoint-technologie. Denk aan firewalls, antivirussoftware en netwerkpenetratie. Deze zijn niet gericht op een uitbraak en encryptie, ze stoppen simpelweg alles wat je netwerk in wil komen. Maar wat als daar tóch iets doorheen komt? Dat is het echte gevaar van ransomware. Een lockdown is dan vaak de enige manier om dit te stoppen. Maar als dat lukt, is er meestal al grote schade aangericht. Het kost dan veel tijd en geld om de dienstverlening weer up and running te krijgen.”*

De gemeente Coventry besprak de uitdaging met Ricoh. Wij ontwikkelden een oplossing waarmee organisaties zich kunnen verdedigen tegen ransomware. Griffiths: *“Tijdens ons due diligence-onderzoek en de evaluatie van Ricoh RansomCare kwamen we erachter dat er niets vergelijkbaars op de markt is. Geen ander product biedt zo'n effectieve laatste verdedigingslinie. Onze keuze was dan ook snel gemaakt.”*

Oplissing

De gemeente Coventry koos voor Ricoh RansomCare. Deze oplossing combineert BullWall-software met ondersteunende diensten van Ricohs Cybersecurity Practice. RansomCare is een agentloze toepassing, die wordt geïnstalleerd op een virtuele server in het centrale ICT-systeem van de gemeente. Dus niet op elk endpoint. Het controleert realtime de gegevens binnen de hele organisatie. Het kan overal in het netwerk een ransomware-aanval spotten, zelfs als deze de bestaande beveiligingssystemen al heeft omzeild. Meestal gebeurt dit via een laptop of desktop. RansomCare schakelt de locatie direct uit en stopt de verspreiding van ransomware.

De IT-afdeling volgt de activiteit realtime in een dashboard. Op elke aanval volgt direct een waarschuwing. Het systeem levert automatisch een aanvalsaudit en rapportage voor analyse en AVG-compliance. De oplossing werd aanvankelijk ingezet om de belangrijkste gemeentelijke data te beschermen, maar wordt nu ook uitgerold naar o.a. ter plekke gehoste SharePoint- en Microsoft 365-toepassingen. RansomCare kan ook cloudgegevens beschermen, hoewel dit niet de vraag was van Coventry.

Ricoh leaset de BullWall-software voor vijf jaar aan Coventry. De software-installatie duurde slechts een halve dag. Naast de software leverden we vijf dagen ondersteunend advies over installatie, toezicht en opleiding. De uiteindelijke oplossing werd in twee maanden gepland, getest en geïmplementeerd. Zodat Coventry in korte tijd kon rekenen op optimale bescherming tegen ransomware-aanvallen.

Resultaat

Ricoh RansomCare - powered by BullWall geeft Coventry een goede bescherming tegen ransomware. Het is makkelijk en snel te installeren, met minimale impact op de IT-infrastructuur en -prestaties. Zelfs als er een aanval is, stopt Ricoh RansomCare deze vóór er schade is. Het beschermt de gegevens waarmee de gemeente haar dienstverlening uitvoert. Van wegenbouw en onderwijs tot sociale zorg.

Griffiths zegt: *“Hopelijk krijgt onze gemeente nooit te maken met een ransomware-aanval. Maar mocht dit toch gebeuren, dan kunnen we vertrouwen op Ricoh RansomCare. We investeren graag in zekerheid - en houden grip op de impact van een mogelijke aanval. We willen absoluut voorkomen dat ons systeem maandenlang geblokkeerd wordt en er miljoenen worden besteed aan dataherstel. Dát is pas kostbaar.”*

Thuiswerken en hybride werken wordt meer en meer de norm. Ook in Coventry. De gemeente erkent dat er nieuwe risico's zijn nu veel mensen thuis en op eigen devices werken. Denk aan phishingmails, onbetrouwbare websites of geïnfecteerde USB-drivers. Hoe robuust de cybersecurityoplossingen ook zijn: er is meer kans op incidenten als mensen op hun eigen devices werken en minder bedacht zijn op veiligheidsprotocollen.

Griffiths voegt toe: *“Ricoh RansomCare beschermt het netwerk als er toch iets binnendringt. Hopelijk hoeven we het nooit te gebruiken. Maar onze bezorgdheid neemt toe nu er steeds meer ransomware-aanvallen plaatsvinden en cybercriminelen steeds creatiever worden. We willen doen wat mogelijk is om de gegevens van onze inwoners en medewerkers te beschermen - en de continuïteit van de dienstverlening te garanderen.”*

“Hopelijk krijgt onze gemeente nooit te maken met een ransomware-aanval. Maar mocht dit toch gebeuren, dan kunnen we vertrouwen op Ricoh RansomCare. We willen absoluut voorkomen dat ons systeem maandenlang geblokkeerd wordt en er miljoenen verloren gaan aan dataherstel. Dát is pas kostbaar. We investeren liever in zekerheid - en beheersen de impact van een mogelijke aanval.”

Gary Griffiths, ICT Engagement Lead bij gemeente Coventry

