RICOH
imagine. change.

Keeping essential public services running with robust protection against ransomware

With RICOH RansomCare powered by BullWall, this Danish Municipality can detect and contain ransomware threats, minimise the impact of incidents, and comply with stringent regulations.

COMPANY & CHALLENGE

The customer is responsible for the delivery of public services in an area of Denmark with a population of more than 20,000 people. The Municipality provides education, healthcare, waste and recycling, public transport, culture and leisure services, and much more.

Ransomware attacks are growing smarter and more sophisticated all the time. Across Europe, cybercriminals have successfully targeted many private companies and public sector organisations, including major enterprises, government ministries and municipal bodies. In many cases, the victim takes hours or even days to detect the data breach, by which time the malicious software has encrypted tens of thousands of sensitive files.

This Municipality is well aware of the growing threat. The organisation manages the systems that ensure many essential public services are available when people need them — from schools and council functions to healthcare facilities. A cyberattack could cause significant damage, not only knocking out key services and denting public confidence, but also forcing the Municipality to perform costly work to recover its data.

To mitigate these risks, the Municipality previously relied on a traditional perimeter cybersecurity model, with firewall and antivirus tools to prevent malicious traffic from entering its network. However, the organisation lacked a specialised solution for tackling ransomware incidents and set out to bolster its defences.

A spokesperson for the Municipality explains: "As an organisation, we are on a long-term digital transformation journey. For example, we are adopting more cloud solutions alongside our main on-premises infrastructure. We knew that this could potentially create new vulnerabilities and security gaps, and that even the latest firewall and antivirus systems often fail to detect ransomware attacks before it's too late."

As the next step, the Municipality planned to add an extra layer of protection to help detect and respond to ransomware attacks. Rather than simply trying the prevent an incident altogether — an impossible task — the aim was to contain attacks and prevent illicit encryption from spreading across the network.

> We have worked with Ricoh on multiple projects in the past, and the service has always been excellent. When Ricoh ran the demos of RansomCare, we quickly saw the value of the solution for tackling a ransomware incident.
>
> *Municipality Spokesperson*

"Previously, there was always the risk that a ransomware incident could cause lengthy downtime and disruption. RansomCare will help us to keep essential public services available, even in the event of a ransomware attack." Municipality Spokesperson

SOLUTION

To enhance its cybersecurity posture, the Municipality worked with long-term technology partner Ricoh. Following discussions involving senior management and IT teams, and a series of demonstrations, the Municipality decided to implement RICOH RansomCare powered by BullWall. The solution will provide 24/7 monitoring of the Municipality's infrastructure to detect and respond to emerging ransomware incidents.

The Municipality is working closely with Ricoh to roll out RansomCare across its on-premises and cloud file share environment. The agentless solution runs on a virtual server in the Municipality's data centre rather than on individual user devices and endpoints, helping to minimise the impact on network performance.

During the installation, embedded artificial intelligence (AI) in RansomCare learns to distinguish between normal file share activity and potentially malicious encryption. When the AI has been trained, 28 detection sensors in RansomCare will track activity across the Municipality's file and cloud shares and take immediate action whenever the number of simultaneous encryption tasks passes a predetermined threshold. At this point, the solution will isolate the appropriate user or device, and shut down their PC or revoke their network access.

The spokesperson continues: "We have worked with Ricoh on multiple projects in the past, and the service has always been excellent. When Ricoh ran the demos of RansomCare, we quickly saw the value of the solution for tackling a ransomware incident. The user interface and dashboards on RansomCare will be especially useful, enabling us to monitor all activity across our extensive file and cloud shares in real time."

BENEFITS

With RansomCare, the Municipality will significantly strengthen its cybersecurity posture, adding another layer of resilience. While the antivirus and firewall systems continue to monitor the network perimeter for malicious traffic, RansomCare acts as a last line of defence, on hand to shut down anything that slips through.

The spokesperson explains: "Previously, there was always the risk that a ransomware incident could cause lengthy downtime and disruption, and mean we would have to

complete a full data restore to get back up and running. RansomCare will help to minimise the impact, not only containing the attack but also providing a full record of any encrypted files, so we can recover rapidly. RansomCare will help us to keep essential public services available, even in the event of a ransomware attack."

In addition, RansomCare will ensure that the Municipality meets the requirements of the General Data Protection Regulation (GDPR) for reporting ransomware incidents. The regulation gives organisations hit by an incident 72 hours to provide a detailed report to the relevant supervisory authority. The Ricoh solution will automatically generate a GDPR-compliant report containing a full breakdown of the incident, including the source of the attack, how many users were affected, how many files were encrypted, and a time and date stamp.

The spokesperson concludes: "Having RansomCare in place will also offer real peace of mind for our management and IT team. We can all rest a little easier and feel more secure knowing that the Ricoh solution is working round the clock to monitor and protect us. As the threat landscape evolves, we know we have the high levels of protection we need to react and respond effectively when ransomware strikes."

ABOUT RICOH

Ricoh is a leading provider of integrated digital services and print and imaging solutions designed to support digital transformation of workplaces and workspaces, and to optimise business performance.

Headquartered in Tokyo, Ricoh's global operation reaches customers in approximately 200 countries and regions, supported by cultivated knowledge, technologies, and organisational capabilities nurtured over its 85-year history. In the financial year ended March 2023, Ricoh Group had worldwide sales of 2,134 billion yen (approx. 16.0 billion USD).

It is Ricoh's mission and vision to empower individuals to find Fulfillment through Work by understanding and transforming how people work so we can unleash their potential and creativity to realise a sustainable future.

To find out more please visit www.ricoh-europe.com

RICOH
imagine. change.

www.ricoh-europe.com