Fallstudie

Stadtverwaltung von Coventry
Kommunalverwaltung

Die Stadtverwaltung von Coventry schützt Bürgerinnen und Bürger, Angestellte und Services mit der RICOH RansomCare-Lösung

Der Stadtrat von Coventry war zunehmend besorgt über die wachsende Bedrohung durch Ransomware-Angriffe. Der Beginn des Corona-Lockdowns schärfte den Blick für das Risiko, da gute Sicherheitspraktiken nur schwer auf Mitarbeitende anzuwenden waren. Um den bestmöglichen Schutz zu gewährleisten, entschied sich die Stadtverwaltung für den Einsatz der RansomCare-Lösung von Ricoh – eine Entscheidung, die sie als „unschlagbar" bezeichnete.

Zusammenfassung

Name: Stadtverwaltung von Coventry
Ort: Coventry, West Midlands
Größe: 5.500 Mitarbeitende
Tätigkeit: Kommunalverwaltung

Herausforderungen

- Wachsende Bedrohung durch Ransomware-Angriffe
- Risiko für die Kontinuität des Dienstes und hohe Kosten für die Wiederherstellung
- Corona und Arbeiten von zu Hause aus verschärfen das Problem

Lösung

- Ricoh-RansomCare
- Ricoh-Fachberatung

Vorteile

- Eine der besten Schutzlösungen gegen Ransomware
- Schutz vor zusätzlicher Bedrohung durch Remote Working
- Gutes Kosten-Nutzen-Verhältnis im Vergleich zu den Schäden und Kosten eines Angriffs
- Einfach innerhalb eines halben Tages zu installieren
- Minimale Auswirkungen oder Eingriffe in die IT-Infrastruktur

Herausforderungen

Die Stadtverwaltung von Coventry ist eine Gebietskörperschaft, die für die Erbringung von kommunalen Dienstleistungen für 360.000 Menschen in der Stadt zuständig ist. Die Stadt wurde für 2021 zur britischen Kulturhauptstadt ernannt. Die Stadtverwaltung hat ein digitales Transformationsprogramm eingeführt, um den Betrieb und die Bereitstellung von Dienstleistungen für die Gemeinschaft zu verbessern. Mit innovativen Technologien wie Microsoft Office 365, Kommunikations- und Kollaborationstools und der Ausstattung aller Mitarbeitenden mit mobiler Technologie will die Stadtverwaltung ihre Belegschaft flexibler aufstellen.

Teil dieser digitalen Strategie ist ein robustes Cybersicherheitssystem mit verschiedenen Technologien, um den Schutz der Bürger, der Mitarbeitenden der Stadtverwaltung und der von der Stadtverwaltung erbrachten Dienstleistungen zu gewährleisten. Dank dieses mehrschichtigen Ansatzes für die IT-Sicherheit sind die Systeme der Stadtverwaltung sehr gut gegen bekannte und unbekannte Bedrohungen geschützt.

Aber wie viele andere Organisationen und Unternehmen ist auch die Stadtverwaltung von Coventry zunehmend besorgt über Ransomware. Dabei handelt es sich um bösartige Software, die von finanziell motivierten Kriminellen zum Angriff auf Daten eingesetzt wird.

Sobald Ransomware in das System eines Unternehmens eingedrungen ist, verschlüsselt sie die Dateien, sodass sie nicht mehr zugänglich sind. Sie ändert die Dateierweiterungen und nicht die Namen, sodass es schwierig ist, beschädigte Dateien zu finden. Ransomware kann bis zu 7.000 Dateien pro Minute infizieren. Die Kriminellen verlangen dann eine Zahlung und halten geschäftskritische Daten und Informationen als Geiseln fest.

Die Auswirkungen von Ransomware wurden deutlich, als Ende Februar eine andere britische Kommunalbehörde angegriffen wurde und es zwei Monate dauerte, bis die Daten wiederhergestellt und die Dienste wieder verfügbar waren. Ein internationales Unternehmen, das von Ransomware betroffen war, erlebte einen Einbruch seines Aktienkurses und die Wiederherstellung kostete Millionen von Pfund. Die andere Herausforderung, welche die Stadtverwaltung von Coventry zum Handeln veranlasste, war die Corona-Pandemie und damit verbundene erhöhte Anfälligkeit durch die hohe Anzahl von Mitarbeitenden im Homeoffice.

„Die traditionelle Abwehr gegen Cyberangriffe besteht aus Endpunkttechnologie wie Firewalls, Antivirensoftware und Netzwerkpenetration, die auf Prävention basiert, anstatt sich auf einen tatsächlichen Ausbruch der Verschlüsselung zu konzentrieren. Sie zielt darauf ab, zu verhindern, dass etwas in Ihr Netzwerk eindringt. Aber was passiert, wenn doch etwas eindringt? Das ist die wahre Gefahr von Ransomware. Die einzige Möglichkeit, sie zu stoppen, ist ein physischer Lockdown. Aber bis Sie das getan haben, ist bereits viel Schaden entstanden“, sagt Gary Griffiths, Leiter der ICT-Abteilung bei der Stadtverwaltung von Coventry. „Das große Problem sind Zeit und Kosten für die Wiederherstellung der Dienste, und dieses Problem nimmt zu.“

Die Stadtverwaltung von Coventry diskutierte das Problem mit Ricoh, einem der führenden strategischen Partner der Stadtverwaltung. Als Reaktion auf die Bedrohung hat Ricoh eine Lösung entwickelt, die Organisationen hilft, sich gegen Ransomware zu schützen. Griffiths sagt: „Bei unserer Due-Diligence-Recherche und Wettbewerbsanalyse der Ricoh-Lösung haben wir festgestellt, dass es auf dem Markt nichts Vergleichbares gibt, das eine so effektive letzte Abwehrstufe bietet. Es war also keine schwierige Entscheidung, die Ricoh-Lösung zu wählen.“

Lösung

Die Stadtverwaltung von Coventry hat die RansomCare-Lösung von Ricoh installiert, die auf der Ransomware-Software BullWall basiert und von der Cyber Security Practice von Ricoh unterstützt wird. RansomCare ist eine agentenlose Anwendung, die auf einem virtuellen Server im zentralen IT-System der Stadtverwaltung und nicht auf jedem Endpunkt installiert wird. Sie überwacht in Echtzeit die Daten im gesamten Unternehmen. Sie kann einen Ransomware-Angriff – in der Regel über einen Laptop oder Desktop – überall im gesamten Netzwerk erkennen, selbst wenn es gelungen ist, die vorhandenen Sicherheitssysteme zu umgehen. RansomCare blockiert den Angriffsort sofort und verhindert, dass sich die Ransomware ausbreitet.

Ein Dashboard zeigt der IT-Abteilung ein Echtzeitbild der Aktivitäten und löst bei einem Angriff sofort einen Alarm aus. Das System erstellt automatisch eine detaillierte Angriffsprüfung und einen Bericht zur Analyse und Einhaltung der DSGVO.

Die Lösung schützte zunächst die wichtigsten Daten der Stadtverwaltung, wird jetzt aber auch auf andere Daten wie vor Ort gehostete SharePoint- und Office-365-Anwendungen ausgeweitet. Obwohl diese Funktion von der Stadtverwaltung von Coventry nicht benötigt wird, kann RansomCare auch Cloud-Daten schützen.

Um die Stadtverwaltung zu unterstützen, waren im Service von Ricoh fünf Tage Beratung enthalten, die Installation, Überwachung und Schulung umfasste, die aus der Ferne durchgeführt wurden. Die Lösung wurde innerhalb von zwei Monaten evaluiert, geplant, getestet und implementiert. Die Softwareinstallation dauerte nur einen halben Tag. Die BullWall-Software wurde von Ricoh im Rahmen eines fünfjährigen Supportplans geleast.

Vorteile

Mit der Ricoh-RansomCare-Lösung verfügt die Stadtverwaltung von Coventry über eine der besten Schutzmaßnahmen gegen Ransomware, die derzeit auf dem Markt erhältlich sind. Sie ist schnell und einfach zu installieren und hat nur minimale Auswirkungen auf die IT-Infrastruktur und die Leistung. Verglichen mit den Auswirkungen auf Dienste, Geschäftskontinuität und Kosten, die ein Ransomware-Angriff mit sich bringt, bietet die Lösung ein sehr gutes Preis-Leistungs-Verhältnis. Selbst wenn es zu einem Angriff kommt, stoppt RansomCare ihn sofort, bevor größerer Schaden entsteht. RansomCare schützt die Daten, die die Stadtverwaltung für die Erbringung von Dienstleistungen nutzt, von Straßenbau und Bildung bis hin zu Sozialfürsorge und Finanzen.

Griffiths sagt: „Hoffentlich wird die Stadtverwaltung von Coventry nie von einem Ransomware-Angriff betroffen sein, aber die RansomCare-Lösung von Ricoh ist wie eine Versicherungspolice. Wenn wir das nicht getan hätten und es zu einem Angriff gekommen wäre, hätten wir uns rechtfertigen müssen, warum wir angesichts der Kosten für die Lösung eine monatelange Sperrung des Systems und Millionenausgaben für die Reparatur von Daten nicht vermieden haben. Jetzt haben wir etwas, das uns im Falle eines Ransomware-Angriffs, der unsere erste Abwehrstufe umgeht, zusätzliche Sicherheit gibt, wie wir die Auswirkungen bewältigen können."

Einer der wichtigsten Vorteile war die Bekämpfung der Auswirkungen des Corona-Lockdowns. Die Stadtverwaltung erkannte, dass ein erhöhtes Risiko bestand, da mehr Mitarbeitende im Homeoffice arbeiteten. Trotz robuster Sicherheitssysteme besteht das größte Risiko für jede Organisation in Benutzerfehlern wie dem Klicken auf einen Link in einer E-Mail, dem Zugriff auf gefährliche Websites oder dem Einstecken eines infizierten USB-Datenträgers. Dieses Risiko steigt, wenn die Mitarbeitenden nicht im Büro sind und weniger auf die Sicherheitspraktiken achten.

Griffiths fügt hinzu: „RansomCare ist dazu da, das Netzwerk vor Eindringlingen zu schützen. Vielleicht wird es niemals genutzt. Aber angesichts der weltweiten Besorgnis über die Zunahme von Ransomware-Angriffen und der Tatsache, dass Cyberkriminelle immer kreativer werden, tun wir mehr als die meisten, um die Stadtverwaltung, ihre Daten und die von ihr angebotenen Dienste zu schützen."

Ricoh-Lösung/Produkte

- RansomCare
- BullWall-Software
- Ricoh-Beratungs- und Schulungsservice

„Hoffentlich wird die Stadtverwaltung von Coventry nie von einem Ransomware-Angriff betroffen sein, aber die RansomCare-Lösung von Ricoh ist wie eine Versicherungspolice. Wenn wir das nicht getan hätten und es zu einem Angriff gekommen wäre, hätten wir uns rechtfertigen müssen, warum wir angesichts der Kosten für die Lösung eine monatelange Sperrung des Systems und Millionenausgaben für die Reparatur von Daten nicht vermieden haben. Sollte ein Ransomware-Angriff an unserer Abwehr vorbeigehen, haben wir jetzt eine weitere Sicherheit, wie wir die Auswirkungen bewältigen können."

Gary Griffiths, Leiter ICT-Abteilung, Stadtverwaltung von Coventry

Coventry City Council

RICOH
imagine. change.

2023 Ricoh UK Ltd. All rights reserved. Replication of part or all of this document requires the express written permission of Ricoh UK Ltd.