Caso di successo

RansomCare per il consiglio comunale di Coventry

Il consiglio comunale di Coventry protegge i cittadini, il personale e i servizi grazie alla soluzione Ricoh per la difesa dai ransomware

Il consiglio comunale di Coventry era sempre più preoccupato nei confronti della crescente minaccia di attacchi ransomware. Il lockdown imposto a causa del COVID-19 ha portato l'attenzione su questo rischio causato dalla difficoltà di applicare le "best practice" di sicurezza al personale in smart working. Per garantire la migliore difesa possibile, il consiglio ha deciso di implementare la soluzione RansomCare di Ricoh, una decisione che l'ente ha descritto come "un gioco da ragazzi".

In sintesi

Azienda: Consiglio comunale di Coventry
Localizzazione: Coventry, West Midlands, UK
Dimensioni: 5.500 dipendenti
Attività: Amministrazione Locale

Le sfide

- Crescente minaccia di attacchi ransomware
- Rischio per la continuità del servizio e costi di ripristino elevati
- Problema aggravato dallo smart working dovuto al COVID-19

La soluzione

- Ricoh RansomCare
- Consulenza di esperti Ricoh

I vantaggi della soluzione

- Garantisce una delle migliori difese contro i ransomware
- Protegge dalle crescenti minacce causate dal lavoro da remoto
- Offre un ottimo rapporto qualità-prezzo rispetto ai danni e ai costi di un attacco
- E' veloce e semplice da installare (mezza giornata)
- Ha un impatto minimo sull'infrastruttura IT

Caso di successo: consiglio comunale di Coventry

Le sfide

Il consiglio comunale di Coventry fornisce servizi amministrativi ai 360.000 abitanti della città. Di recente, Coventry è stata nominata Città della cultura del Regno Unito per il 2021. L'amministrazione ha avviato un programma di trasformazione digitale per migliorare la gestione e la fornitura dei servizi alla comunità. L'obiettivo era quello di sviluppare modi di lavorare più agili grazie a tecnologie quali Microsoft Office 365, a strumenti di comunicazione e collaborazione e a soluzioni per la mobility.

La sicurezza informatica rappresenta un aspetto importante di questa strategia ed è basata su molteplici tecnologie che garantiscono la protezione dei cittadini, del personale comunale e dei servizi forniti. Grazie a questo approccio stratificato e completo alla sicurezza IT, i sistemi sono molto ben protetti contro minacce note o sconosciute.

Come molte altre organizzazioni e aziende, il consiglio comunale di Coventry era sempre più preoccupato nei confronti della crescente minaccia di attacchi ransomware, software dannosi utilizzati da criminali per attaccare i dati ed estorcere denaro.

Una volta entrato nei sistemi, il ransomware cripta i file in modo che non sia più possibile accedervi e ne modifica le estensioni anziché i nomi, quindi è difficile individuare quelli danneggiati. Il ransomware può infettare fino a 7.000 file al minuto. I criminali chiedono il pagamento di un riscatto tenendo "in ostaggio" dati e informazioni business-critical.

Il pericolo del ransomware è diventato ancora più evidente quando un altro ente locale del Regno Unito è stato attaccato e ha impiegato due mesi per recuperare i dati e ripristinare i servizi. Un'azienda internazionale colpita da ransomware ha visto crollare il prezzo delle sue azioni e il ripristino è costato milioni di sterline. L'altro fattore che ha spinto il consiglio comunale di Coventry ad agire è stata la pandemia di COVID-19 e la maggiore vulnerabilità dovuta all'elevato numero di personale in smart working.

"La difesa tradizionale contro gli attacchi informatici poggia su tecnologie endpoint - come ad esempio firewall, software antivirus e network penetration - basate su un approccio preventivo anziché sul contrasto alla diffusione effettiva della criptazione. Il focus è rivolto ad impedire l'accesso alla rete. Ma cosa succede se una minaccia riesce ad entrare? Questo è il vero pericolo dei ransomware. L'unico modo per fermarli è un blocco fisico. Ma nel momento in cui si comincia ad agire, il danno è già avvenuto", afferma Gary Griffiths, ICT Engagement Lead del consiglio comunale di Coventry. "Il grande punto critico è rappresentato dal tempo e dal costo per il ripristino dei servizi e questo è un problema sempre più rilevante".

Il consiglio comunale di Coventry ha condiviso la propria preoccupazione con Ricoh, che ora è uno dei principali partner strategici del consiglio. In risposta a questa tipologia di minacce, Ricoh ha sviluppato una soluzione che aiuta le organizzazioni a difendersi dai ransomware. Griffiths afferma: "Durante l'attività di due diligence e la valutazione della soluzione Ricoh, abbiamo scoperto che non vi era nulla sul mercato in grado di fornire una linea di difesa così efficace. Quindi, scegliere la soluzione Ricoh non è stata una decisione difficile".

La soluzione

Oltre ad avvalersi dell'approccio "Cyber Security Practice" di Ricoh, il consiglio comunale di Coventry ha scelto la soluzione RansomCare di Ricoh basata sul software ransomware di BullWall. RansomCare è un'applicazione agentless - installata su un server virtuale nel sistema IT centrale del comune anziché su ogni endpoint - che monitora in tempo reale i dati dell'intera organizzazione. E' in grado di individuare un attacco ransomware - il cui punto di ingresso è di solito un laptop o un desktop - in qualunque punto della rete, anche quando il malware riesce a bypassare i sistemi di sicurezza esistenti. RansomCare blocca all'istante il punto in cui si trova l'elemento dannoso e ne impedisce la diffusione.

Grazie a una dashboard, l'IT può monitorare in tempo reale l'attività ricevendo un alert istantaneo in caso di attacco. Il sistema fornisce automaticamente un controllo dettagliato degli attacchi e un report per l'analisi e la conformità al GDPR.

La soluzione è stata inizialmente utilizzata per proteggere i dati più importanti del comune, ma è stata successivamente estesa ad altri ambiti come SharePoint in loco e applicazioni Office 365. Sebbene non sia richiesto dal consiglio comunale di Coventry, RansomCare può proteggere anche i dati archiviati nel cloud.

Per supportare il consiglio, Ricoh ha svolto per cinque giorni un'attività di consulenza inerente a installazione, monitoraggio e formazione, il tutto svolto in remoto. La soluzione è stata valutata, pianificata, testata e implementata in soli due mesi. L'installazione del software è stata ancora più rapida: solo mezza giornata. Il software BullWall è stato concesso in locazione da Ricoh in base a un piano di supporto della durata di cinque anni.

RICOH
imagine. change.

I vantaggi della soluzione

La soluzione Ricoh RansomCare offre al consiglio comunale di Coventry una delle migliori difese contro i ransomware attualmente conosciuti. È semplice e rapida da installare e ha un impatto irrilevante sull'infrastruttura IT e sulle prestazioni dei sistemi. Considerato il possibile impatto sui servizi, sulla continuità aziendale e sui costi di gestione di un attacco ransomware, la soluzione offre un ottimo rapporto qualità-prezzo. Qualora si verificasse un attacco, RansomCare è in grado di bloccarlo immediatamente prima che questo causi danni significativi. La soluzione protegge i dati che il comune utilizza per fornire i servizi in ambiti quali infrastrutture stradali, istruzione, assistenza sociale e servizi finanziari.

Griffiths afferma: "Ci auguriamo che il consiglio comunale di Coventry non subisca mai un attacco ransomware, ma la soluzione RansomCare di Ricoh è come una polizza assicurativa. Se non avessimo implementato questa soluzione e si fosse verificato un attacco, avremmo dovuto giustificare il mancato investimento e spendere somme ingenti per porre rimedio. Grazie a questa soluzione, se un attacco ransomware dovesse bypassare la nostra difesa perimetrale, avremmo la certezza di riuscire comunque a gestirne l'impatto".

Uno dei principali vantaggi è stato riuscire a mitigare l'impatto del lockdown imposto per il COVID-19. Il consiglio ha ritenuto che il rischio fosse maggiore a causa del numero elevato di dipendenti che lavoravano da remoto. Nonostante i solidi sistemi di sicurezza, il rischio principale per qualsiasi organizzazione è rappresentato dagli errori commessi dalle persone che per sbaglio, ad esempio, cliccano su un collegamento in un'e-mail, accedono a siti Web pericolosi oppure utilizzano un driver USB infetto. Questi rischi aumentano quando le persone non sono in ufficio e sono meno attente alla sicurezza delle informazioni.

Griffiths aggiunge: "RansomCare protegge la rete nel caso in cui un malware cercasse di accedere. Speriamo non sia mai necessario utilizzare questa soluzione, ma in tutto il mondo vi è una grande preoccupazione per la crescita degli attacchi ransomware e la proliferazione di criminali informatici sempre più "creativi". Per questo stiamo facendo il massimo per riuscire a proteggere il comune, i suoi dati e i servizi che offre".

Soluzioni/prodotti Ricoh

- RansomCare
- Software Bullwall
- Servizi di consulenza e formazione Ricoh

"Ci auguriamo che il consiglio comunale di Coventry non subisca mai un attacco ransomware, ma la soluzione RansomCare di Ricoh è come una polizza assicurativa. Se non avessimo implementato questa soluzione e si fosse verificato un attacco, avremmo dovuto giustificare il mancato investimento e spendere somme ingenti per porre rimedio. Grazie a questa soluzione, se un attacco ransomware dovesse bypassare la nostra difesa perimetrale, avremmo la certezza di riuscire comunque a gestirne l'impatto".

Gary Griffiths, ICT Engagement Lead del consiglio comunale di Coventry

Coventry City Council

RICOH
imagine. change.

www.ricoh.co.uk