RICOH
imagine. change.

Dansk kommune står nu endnu stærkere i kampen mod ransomware.

Med RICOH RansomCare powered by BullWall kan denne danske kommune opdage og inddæmme ransomware, minimere påvirkningen af hændelser og overholde compliance og lovgivning.

VIRKSOMHED & UDFORDRING

Kunden er ansvarlig for levering af offentlige ydelser i et område af Danmark med mere end 20.000 indbyggere. Kommunen tilbyder uddannelse, sundhedspleje, administration af affald og genbrug, offentlig transport, kultur, fritidstjenester og meget mere.

Ransomwareangreb bliver hele tiden mere intelligente og avancerede. På tværs af Europa er det lykkedes for cyberkriminelle at angribe mange private virksomheder og organisationer i den offentlige sektor ministerier og kommunale organer. I mange tilfælde kan det tage timer eller endda dage, før offeret opdager databruddet - og på dette tidspunkt har den ondsindede software allerede krypteret titusinder af følsomme filer.

Den omtalte kommune er fuldstændig klar over den voksende trussel. Organisationen administrerer de systemer, der sikrer, at mange vigtige offentlige tjenester er tilgængelige, når folk har brug for dem - lige fra skoler og kommunale funktioner til sundhedsvæsnet. Et cyberangreb kan forårsage betydelig skade, ikke kun ved at stoppe de vigtigste tjenester og ødelægge tilliden til offentligheden, men også ved at tvinge kommunen til at foretage et omkostningstungt arbejde for at gendanne data.

For at afbøde disse risici stolede kommunen tidligere på en traditionel perimeterbaseret cybersikkerhedsmodel med firewall- og antivirusværktøjer til at forhindre ondsindet trafik i at trænge ind på netværket. Organisationen manglede imidlertid en specialiseret løsning til at tackle ransomware og satte sig derfor for at styrke forsvarsevnen.

En talsmand for kommunen forklarer: "Som organisation er vi på en længerevarende digital transformationsrejse. For eksempel vedtager vi flere cloudløsninger sideløbende med vores primære infrastruktur på stedet. Vi var klar over, at dette potentielt kunne skabe nye sårbarheder og sikkerhedshuller, og at selv de nyeste firewall- og antivirussystemer ofte ikke opdager ransomwareangreb, før det er for sent."

Som næste skridt planlagde kommunen at tilføje et ekstra lag af beskyttelse for at hjælpe med at opdage og reagere på ransomwareangreb. I stedet for blot at forsøge helt at forhindre en hændelse, hvilket er en umulig opgave, var målet at begrænse angreb og forhindre ulovlig kryptering i at sprede sig over netværket.

> Vi har tidligere arbejdet sammen med Ricoh på flere projekter, og firmaets service har altid været fremragende. Da Ricoh kørte demoerne af RansomCare, blev vi hurtigt klar over værdien af sikkerhedsløsningen til at håndtere ransomware.
>
> *Kommunens talsmand*

"Tidligere var der altid risiko for, at ransomware kunne forårsage længerevarende nedetid og forstyrrelser. Ricoh RansomCare hjælper os med at holde vigtige offentlige tjenester tilgængelige, selv i tilfælde af et ransomwareangreb."

Kommunens talsmand

LØSNING

For at forbedre sikkerheden, arbejdede kommunen sammen med sin mangeårige teknologipartner Ricoh. Efter drøftelser med den øverste ledelse og IT-afdelinger, samt en række demonstrationer, besluttede kommunen at implementere RICOH RansomCare powered by BullWall.

Kommunen arbejder tæt sammen med Ricoh for at udrulle RansomCare på tværs af lokale og cloudbaserede fildelingsmiljøer. Den agentløse løsning kører på en virtuel server i kommunens datacenter i stedet for på individuelle brugerenheder og slutpunkter, hvilket hjælper med at minimere påvirkningen af netværkets ydeevne.

Under installationen lærer indlejret kunstig intelligens (AI) RansomCare at skelne imellem en normal fildelingsaktivitet og en potentielt ondsindet kryptering. Når AI'en er blevet oplært, vil 28 detektionssensorer i RansomCare-løsningen spore aktivitet på tværs af kommunens fil- og cloudshares. Systemet tager øjeblikkelig handling, når antallet af samtidige krypteringsopgaver passerer en forudbestemt grænse. På dette tidspunkt isolerer løsningen den relevante bruger eller enhed og lukker den pågældende PC ned eller tilbagekalder adgangen til netværket.

Talsmanden fortsætter: "Vi har tidligere arbejdet sammen med Ricoh på flere projekter, og firmaets service har altid været fremragende. Da Ricoh kørte demoerne af RansomCare, blev vi hurtigt klar over værdien af sikkerhedsløsningen til at håndtere ransomware. Brugergrænsefladen og de forskellige dashboards er yderst nyttige og gør os i stand til at overvåge al aktivitet på tværs af vores omfattende fil- og cloudbaserede delinger i realtid."

FORDELE

Med RansomCare tilføjer kommunen endnu et lag af modstandsdygtighed og styrker dermed deres cybersikkerhedsposition markant. Mens antivirus- og firewall systemerne fortsætter med at overvåge netværkets perimeter for ondsindet trafik, fungerer RansomCare som en sidste forsvarslinje, der er klar til at lukke alt ned, der måtte slippe igennem.

Talsmanden forklarer: "Tidligere var der altid risiko for, at et ransomwareangreb kunne forårsage en længerevarende nedetid og forstyrrelse – samt medføre at vi var nødt til at gennemføre en fuld datagendannelse for at komme i gang igen. Ricoh RansomCare hjælper med at minimere påvirkningen, ikke kun ved at tilbageholde angrebet, men også med at give en fuld registrering af eventuelle krypterede filer, så vi hurtigt kan

få overblik og komme tilbage på sporet. Det betyder, at vi kan holde grundlæggende offentlige tjenester og services tilgængelige, selv i tilfælde af et ransomwareangreb."

Derudover sørger RansomCare for, at kommunen opfylder kravene i databeskyttelsesforordningen (GDPR) vedrørende rapportering af ransomwareangreb. Forordningen giver organisationer, der er ramt af en hændelse, 72 timer til at levere en detaljeret rapport til den relevante tilsynsmyndighed. Ricohs løsning genererer automatisk en GDPR-kompatibel rapport, der indeholder en komplet oversigt over hændelsen, herunder kilden til angrebet, hvor mange brugere der blev berørt, hvor mange filer der blev krypteret, og en oversigt med præcis dato og tidspunkt.

Talsmanden konkluderer: "At have RansomCare på plads vil også give vores ledelse og IT-team langt mere ro i sindet. Vi kan alle slappe lidt mere af og føle os mere sikre, når vi ved, at Ricohs løsning overvåger og beskytter os døgnet rundt. Efterhånden som trusselsbilledet udvikler sig, ved vi, at vi har de høje beskyttelsesniveauer, vi har brug for, for at kunne handle og reagere effektivt, når vi rammes af ransomware."

OM RICOH

Ricoh er en førende leverandør af digitale tjenester, workflow- og dokumenthåndteringsløsninger samt kommercielle og industrielle printløsninger, der er designet til at understøtte digital transformation og optimere virksomhedens resultater.

Med hovedkontor i Tokyo når Ricohs globale aktiviteter ud til kunder i cirka 200 lande og regioner, understøttet af viden, teknologier og organisatoriske kompetencer, der er oparbejdet gennem dets 85-årige historie. I regnskabsåret, der sluttede marts 2023, havde Ricoh Group en omsætning på verdensplan på 2.134 milliarder yen (ca. 16,0 milliarder USD).

Ricoh Danmark A/S har hovedkontor i Vallensbæk Strand og filialer i Aarhus og Kolding. Ricoh Danmark har desuden eget landsdækkende servicenetværk, samt en række specialiserede partnere over hele landet.

Det er Ricohs mission og vision at give enkeltpersoner mulighed for at finde tilfredstillelse gennem deres arbejde ved at forstå og transformere, hvordan folk arbejder, så vi kan frigøre deres potentiale og kreativitet for at skabe en bæredygtig fremtid.

Besøg www.ricoh.dk for mere info.

RICOH
imagine. change.

www.ricoh.dk