Virksomheden fik lukket de kritiske huller i IT-sikkerheden

Virksomhedens drift og forretning er nu sikret mod angreb

IT-sikkerheden er nu både tidssvarende og fremtidssikret hos den store produktions-virksomhed – og det betyder, at forretningen ikke risikerer alvorlige nedbrud med store omkostninger til følge.

kaastrup|andersen har hjulpet en stor produktionsvirksomhed med at forberede og igangsætte udrulning af en helt ny connectivity-platform for at sikre netværket – og dermed hele virksomhedens infrastruktur og drift – mod kompromitterende cyberangreb, der potentielt kan true virksomhedens eksistens.

Virksomheder må i dag erkende, at det ikke er et spørgsmål, **om** sikkerheden bliver truet, det er et spørgsmål om **hvornår**. Konsekvenserne afhænger i høj grad af de sikkerhedsforanstaltninger, der er etableret i forhold til connectivity: netværksforbindelser i bredeste forstand. Og et IT-netværk rækker vidt, fra virksomhedens forskellige lokationer (både produktion og kontorer), til medarbejdernes hjemmearbejdspladser og mobile enheder, til eksterne samarbejdspartnere og cloud-udbydere.

Læs om, hvad der skulle til for at løfte virksomhedens IT-sikkerhed til et tidssvarende niveau.

Udfordring

As-Is situationen var et netværk opbygget gennem en længere årrække med netværksudstyr, som efterhånden var op til 10 år gammelt – og delvist endda endnu ældre. En af problemstillingerne i forhold til sikkerhed var, at noget af udstyret var gået ud af produktion (End of Service), så ved fejl på hardware var det afgørende, at virksomheden selv havde reservedele og udstyr på lager – og kompetencerne til at foretage reparationen. Det forældede udstyr ville på sigt blive ubrugeligt og udgøre sikkerhedsmæssige problemer.

For at kunne holde et kontinuert højt sikkerhedsniveau er det nødvendigt at opdatere software løbende og hyppigt på alle netværksenheder. Virksomheden havde ikke gennemført struktureret opdatering af software, og der blev heller ikke udgivet flere opdateringer fra producenternes side til de enheder, som var gået ud af produktion.

Den manglende sikkerhed havde potentiale til at udvikle sig til en kritisk situation for virksomheden, som producerer 24/7, og som er afhængig af connectivity: Det kan hurtigt blive meget dyrt at have længerevarende omfattende nedbrud på netværks-infrastrukturen og dermed stå overfor tabt produktion og måske manglende leverancer til kunderne.

Løsning

Forud for selve projektet var der blevet udarbejdet risiko-vurderinger herunder økonomiske konsekvensanalyser af forskellige scenarier for, hvordan virksomhedens netværk kunne blive kompromitteret.

De indledende vurderinger viste, at en opdatering af alt netværksudstyr isoleret set var en stor omkostning, men omkostningen svarede kun til et par dages tabt omsætning, hvis virksomheden blev ramt af et omfattende nedbrud på netværket.

Projektets mål blev derfor at forberede og påbegynde udrulning af en helt ny connectivity-platform, som led i en større digitaliseringsplan på overordnet virksomhedsniveau. Målet med den nye platform er en høj ydelse og driftsstabilitet og adgang til nødvendige services, med et kontinuert højt sikkerhedsniveau, baseret på NIS2-direktivet.

Løsningen på virksomhedens udfordring gik således ud på at implementere en connectivity-strategi med en række elementer og karakteristika:

- Lifecycle Management – løbende monitorering, opdatering og udskiftning af udstyr
- Automatiseret udrulning og opdatering – alle enheder får nye versioner af software automatisk, og det sker uden at forstyrre driften
- Segmentering og fleksibilitet – dele af netværket kan isoleres, så skader ved eventuelle angreb begrænses, for eksempel vel brug af lokale firewalls
- Cloud-ready – korrekt konfigurerede og altid opdaterede firewalls, der sammen med segmentering mindsker muligheden for indtrængen via cloudløsninger
- Certifikatbaseret wi-fi – kun godkendte enheder kan forbinde sig til virksomhedens wi-fi-netværk

Et andet afgørende aspekt i forbindelse med håndtering og opretholdelse af sikkerhed på netværket er brugeradfærd. Det er ikke nok at implementere en teknisk løsning: Brugerne skal løbende uddannes i og opdateres på, hvordan de skal anvende IT-systemerne på en sikker måde. Dette var dog ikke en del af projektets scope.

Resultat

Efter endt udrulning vil virksomheden stå med en række gevinster:

- Kontinuerlig høj sikkerhed overalt i netværket
- Øget sikkerhed specifikt omkring produktionen
- Bedre omkostningsoverblik og-styring i forhold til soft- og hardware
- Effektiv begrænsning af omfanget af et eventuelt sikkerhedsbrud, så hele produktionsfaciliteter ikke står stille på én gang
- Organisatorisk rammesætning, ansvars- og rollefordeling for både de driftsmæssige og strategiske opgaver

Virksomheden har lukket de farlige huller i IT-sikkerheden og har samtidig etableret en velfungerende, fremtidssikret platform, der gør, at både software, hardware og processer altid er opdaterede og kan modstå de efterhånden mange angreb på netværk i både små og store virksomheder. Det betyder, at driften og dermed forretningen nu er mere sikker – på både kort og langt sigt – og virksomheden undgår ubehagelige overraskelser med uforudsete omkostninger som konsekvens.

kaastrup|andersen hjalp kunden igennem processen frem mod en sikring af forretningen.

kaastrup|andersen som din samarbejdspartner

Har du brug for hjælp til en ISO 27001-proces? Vi hjælper dig gerne videre. Ud fra dine behov sammensætter vi et unikt team af fx IT-projektledere, sikkerhedskonsulenter og IT-arkitekter. De kan blandt andet hjælpe dig med at afdække, hvilke tiltag der skal til for at løse din udfordring og sørge for intelligent træk på dine interne ressourcer, når projektet gennemføres.

Kontakt Lasse for en uforpligtende snak om din IT-infrastruktur og sikkerhed. på

På www.kaastrupandersen.dk finder du alle vores cases, som du kan filtrere på forretningsområde.

Se alle cases her

Lasse Aaen Godtfredsen
Mail: lag@kaastrupandersen.dk.
Telefon: +45 70 27 77 19