
## Udfordringen

Cyberangreb bliver stadig mere sofistikerede og aggressive, så hvordan kan det danske forsyningsselskab NRGi forbedre sin evne til at beskytte sine forretningssystemer mod hackere og malware?

## Transformation

NRGi arbejdede sammen med IBM Gold Business Partner SecureDevice om at implementere et centralt overvågningssystem, der registrerer avancerede trusler automatisk, hvilket muliggør mere proaktive netværkssikkerhedssvar.

**Michael Warrer**
**CIO**
**NRGi**

### Fordele:

**Forbedrer**
**NRGi's evne til at opdage potentielle trusler mod sit netværk**

**Advarer**
**IT-teamet om mistænkelig aktivitet automatisk, hvilket muliggør hurtig handling**

**Frigør**
**personale fra gentagne overvågningsopgaver, hvilket giver dem mere tid til at undersøge og håndtere problemer**

# NRGi

# Forbedrer sikkerheden med centraliseret overvågning i realtid

NRGi er Danmarks fjerde største elleverandør, der leverer energi til mere end 220.000 husstande i hele landet. Virksomheden er forpligtet til at være en aktiv del af den nationale og internationale overgang til et mere bæredygtigt energisystem og forvalter sin egen portefølje af vedvarende aktiver. Med hovedkontor i Århus beskæftiger NRGi omkring 1.200 personer.

*"Før følte vi altid, at vi var lidt bagud med hensyn til skkerhed, men nu er vi meget mere produktive."*

Michael Warrer
CIO
NRGi

Share this

## Handling mod cyberkriminelle

Det er enhver virksomheds værste mareridt at blive ramt af et cyberangreb, der angriber nøglesystemer og efterlader organisationen med store problemer. For NRGi blev dette mareridt desværre til virkelighed.

Michael Warrer, som er CIO hos NRGi, siger: "For et par år siden blev vi offer for et målrettet angreb, som brugte ransomware til at ødelægge og kryptere et stort antal af vores back-office-systemer. Vi blev stort set holdt som gidsler. De cyberkriminelle bag angrebet ville have penge som betaling for at returnere kontrollen over de berørte systemer tilbage til os.

"Angrebet berørte 180 servere i vores datacenter. Heldigvis har vi robust backup-, gendannelses- og forretningskontinuitetsprocesser på plads, hvilket betød, at vi kunne genopbygge serverne og få alt i gang igen indenfor 60 timer. Men angrebet forårsagede store problermer og betød, at 1200 medarbejdere ikke kunne logge ind på vores forretningssystemer, indtil vi løste problemet.

"Angrebet var et stort realitetstjek - ikke kun for os, men for hele den danske forsyningssektor. Vi indså, at vi var nødt til at være langt mere proaktive i at beskytte os mod cyberangreb i fremtiden."

Tidligere havde NRGi flere værktøjer til overvågning af logfilerne, bl.a. tidsstemplede registreringer af netværksbegivenheder produceret af dets applikationer og systemer.

Manglen på en centraliseret visning af netværksbegivenheder gjorde det vanskeligt at opdage mønstre på mistænkelig aktivitet. For at forbedre synligheden ønskede NRGi et samlet overblik over sit netværk.

Warrer forklarer: "Selvfølgelig er der ingen måde at stoppe cyberkriminelle fra at forsøge at kompromittere dine it-systemer. I stedet skal du forsøge at være et skridt foran dem. Vi vidste, at hvis vi havde værktøjerne til at gøre os opmærksom på potentielle trusler, kunne vi reagere hurtigere for at undgå brud."

*"Vi indså, at vi var nødt til at være langt mere proaktive i at beskytte os mod cyberangreb i fremtiden."*

Michael Warrer, CIO, NRGi

## Blive mere proaktiv

For at styrke sin sikkerhedsstilling arbejdede NRGi sammen med IBM Gold Business Partner SecureDevice om at implementere IBM® QRadar® SIEM, som er et centraliseret overvågningssystem, der konsoliderer og analyserer loghændelser fra hele netværket.

I tæt samarbejde med SecureDevice konfigurerede NRGi IBM-løsningen til at registrere potentielt ulovlig aktivitet på deres netværk. Når IBM QRadar SIEM registrerer et mistænkeligt mønster, som f.eks. flere mislykkede loginforsøg og firewall afvisninger - advarer løsningen NRGi om at undersøge sagen yderligere.

"Da vi først implementerede systemet, fik vi ca. 10.000 advarsler om ugen, hvoraf de fleste var falske positiver, "siger Warrer.

"Teamet fra SecureDevice brugte ni måneder på at opdatere reglerne og programmere systemet til at genkende tegnene på et potentielt angreb og raffinere systemet, så det kun advarede os om alvorlige problemer. SecureDevice indarbejdede også IBM X-Force® Threat Intelligence i løsningen, som indeholder en liste over potentielt ondsindede IP-adresser, så vi er opmærksom på dem. Nu har vi fjernet de fleste falske positiver, og modtager ca. fem advarsler om ugen, som vi kan give vores fulde opmærksomhed."

NRGi bruger IBM QRadar SIEM til at overvåge alle webservere i sin DMZ (demilitariserede zone) samt alle primære servere i parameteren. Logdata sendes fra hele netværket og spænder over 30 steder i hele Danmark. Enhver mistænkelig aktivitet markeres øjeblikkeligt som en automatiseret alarm til det centrale dashboard, og udløser handling fra it-teamet.

*"SecureDevice hjalp os ikke blot med at forbedre vores regler under implementeringsprocessen, men fortsætter med at arbejde sammen med os for at opdatere dem efterhånden som truslerne udvikler sig."*

Michael Warrer, CIO, NRGi

Warrer tilføjer: "SecureDevice hjalp os ikke blot med at forbedre vores regler under implementeringsprocessen, men fortsætter med at arbejde sammen med os for at opdatere dem efterhånden som truslerne udvikler sig, hvilket sparer os tid og kræfter. Supporten fra SecureDevice har været fremragende i hele projektet. Vi var meget imponerede over deres personlige og professionelle tilgang og niveauet af ekspertise, som de leverede."

## Forberedt på alt

Med IBM QRadar SIEM får NRGi den nødvendige oversigt i realtid over netværksbegivenheder, som der kræves for at tage en mere proaktiv tilgang til sikkerhed. IT-teamet bliver nu automatisk opmærksom på betydelige hændelser, hvilket giver dem en tidlig advarsel om potentielle trusler.

Warrer siger: "Brug af IBM QRadar SIEM er som at have øjne bag i hovedet. Før følte vi altid, at vi var lidt bagud med hensyn til skkerhed, men nu er vi meget mere produktive. Hvis nogen prøver på og ikke kan logge på en af vores brugerkonti uden for vores netværk, har vi alle de oplysninger, vi har brug for til at forudsige præcist, om de udgør en trussel mod vores systemer. For eksempel kan vi se, om forsøgene er fra en brugers bærbar computer eller hjemme-pc eller fra en usikker enhed, hvilket kan tyde på, at nogen forsøger at få uautoriseret adgang.

"Disse automatiserede advarsler fortæller os med det samme, når noget måske kan være mistænkeligt. Hvis nogen har adgang til hundredvis af filer inden for et par minutter, kan det for eksempel være tegn på et ransomware-angreb. Vores tidlige advarselssystem giver os tid til at ringe til den person, der er tilknyttet brugerkontoen for at kontrollere, om de har tilgået filerne. Hvis det ikke er tilfældet, kan vi hurtigt lukke den kompromitterede konto og undersøge, hvad der skete i dybden."

I samarbejde med SecureDevice arbejder NRGi løbende på at optimere systemet og forbedre reglerne og alarmerne for at sikre, at it-teamet modtager en tidlig advarsel, hvis cyberkriminelle angriber. Virksomheden overvejer også muligheden for at forbedre sin løsning med kognitive evner.

"Vi er meget interesserede i at indarbejde IBM Watson® for Cyber Security i vores løsning, "siger Michael Warrer. "Vi har set, at IBM Watson-løsninger kan give værdifulde beslutningsstøttefunktioner til vores analytikere og hjælpe dem med at fjerne falske positiver hurtigere, så de kan bruge mere tid på at undersøge alvorlige potentielle trusler."

Han konkluderer: "Vores IBM QRadar SIEM-løsning, der leveres af SecureDevice, har forbedret vores netværksovervågningsmuligheder betydeligt. Det bedste forsvar mod cyberkriminalitet er årvågenhed, tilpasning og hastighed samt automatiserede advarsler, der giver os den dyrebare tid, vi har brug for til at tage en målrettet indsats for at holde systemer sikre."

*"Vores IBM QRadar SIEM-løsning, der leveres af SecureDevice, har forbedret vores netværksovervågningsmuligheder betydeligt."*

Michael Warrer, CIO, NRGi

## Løsningskomponenter

- IBM® QRadar® SIEM
- IBM X-Force® Threat Intelligence

## Næste skridt

SecureDevice er et førende it-sikkerhedstjenesteselskab med hjemsted i Gentofte, Danmark. Selskabet er en IBM Gold Business Partner, og SecureDevice-konsulenter tilbyder dyb teknisk ekspertise og har hjulpet virksomheder fra hele Skandinavien til at forbedre deres it-sikkerhed. Hvis du vil lære mere om produkter og tjenester fra SecureDevice, skal du besøge: securedevice.dk

Hvis du vil vide mere om IBM Security-løsninger, bedes du kontakte din IBM-repræsentant eller IBM Business Partner eller besøge følgende websted: ibm.com/security

## Kontakt os



WGC12515-DKDA-00