

Dit netværk er virksomhedens digitale rygrad

Sikker digital infrastruktur handler om langt mere end lovgivning og compliance. Her får du et overblik over, hvilke områder du bør prioritere, og hvordan du bygger et netværk, der understøtter drift, forretning og den teknologiske udvikling.

Hvad koster det? Det spørgsmål har hidtil ligget øverst på prioriteringslisten, når virksomheder skulle investere i sikkerheden af deres digitale infrastruktur og netværk. Men EU-direktivet for cybersikkerhed, NIS2, har fået flere virksomheder til i højere grad at investere efter kritikalitet. En vigtig udvikling, som handler om langt mere end lovgivning, spørger man Jeppe Ruokokoski, der er rådgivningschef hos IT-sikkerhedsvirksomheden nLogic.



Jeppe Ruokokoski
Rådgivningschef nLogic

“Det er min overbevisning, at mange virksomheder kan bruge deres eget netværk og data til at skabe en konkurrencefordel.

”At sikkerhed indtil nu primært har afhængt af budget, betyder, at mange virksomheder i dag ikke kan leve op til NIS2-kravene. Konsekvenserne er ikke bare en risiko for bøder. Det er også en risiko for at få ubudne gæster i sin virksomhed, siger Jeppe Ruokokoski.

ISO 27001 er en god start

Det er en stor del af danske virksomheder, der skal leve op til NIS2. Det påvirker ikke bare



dem, der hører under kritisk infrastruktur, men også indirekte deres leverandører. Det kan efterlade mange virksomheder med uro i maven. Men har din virksomhed i forvejen erfaring med den internationale standard for ledelsessystemer for informationssikkerhed ISO 27001, er du allerede mange skridt foran.

”Standarden ligger tæt op ad NIS2 og bygger på sund fornuft. Det handler ikke om at tage en aluminiumshat på og spille en masse penge bare for sikkerhedens skyld. Det handler om at tage stilling, indføre vigtige processer og sikre din virksomhed,” siger Jeppe Ruokokoski og tilføjer:

”De mange processer kan godt virke overvældende set udefra, men det er ikke til for at belejre. I stedet er formålet at gøre tingene nemmere. Jeg vil anbefale at kontakte en virksomhed, der er specialister i IT-sikkerhed, og tage en ærlig snak om hullerne i sikkerhedsnettet. Så kommer I godt fra start.”

Skab først en barriere

Når du skal skabe et sikkert digitalt netværk og infrastruktur er første skridt, og en afgørende del af fundamentet, den klassiske firewall. Sikker-

hedssystemet fungerer som en første barriere, der kontrollerer trafik ind og ud af virksomhedens netværk. Men den kan ikke stå alene.

“

Du ville aldrig give adgang til, at en gæst kan gå direkte fra lobbyen og op på direktørens kontor uden aftale, så hvorfor tillade den adgang digitalt?

Herefter kommer segmenteringen. Hvis alle enheder og systemer kan tale frit med hinanden, kan en computer med en uopdaget virus i princippet blive en genvej videre ind i virksomheden. Ved at dele netværket op i zoner kan man begrænse, hvor langt et angreb kan sprede sig.

”Det kræver adgangskontroller og access lister. Det er en statisk, manuel og meget tung proces, som ikke er skalerbar, men heldigvis er der kommet nye systemer og mere fleksible løsninger,” fortæller Jeppe Ruokokoski.

Digitale adgangskort – en overset disciplin

De fleksible løsninger, han taler om, kan sammenlignes med fysiske adgangskort. Hver medarbejder har sit ID i en snor om halsen klar til at blive scannet, når de bevæger sig ind og ud af virksomhedens interne områder. En sikkerhedsforanstaltning, hos især større virksomheder, som ingen sætter spørgsmålstegn ved.

”Du ville aldrig give adgang til, at en gæst kan gå direkte fra lobbyen og op på direktørens kontor uden aftale, så hvorfor tillade den adgang digitalt? Digitale adgangskort sikrer, at Ib fra bogholderiet ikke har adgang til samme netværk som direktøren,” forklarer Jeppe Ruokokoski.

Han ser desværre, at det er et område, hvor mange virksomheder fortsat er bagud.

”Digitale adgangskort bør komme lang højere på dagsordenen. Systemer som for eksempel Aruba ClearPass betyder, at dit personale ikke skal konfigurere IT-udstyr til det rigtige netværk. Et eksempel kunne være et hospital, der skal flytte en blodtransfusionspumpe fra et hospital til et andet. Det kan være en kritisk

5 SKRIDT. SÅDAN LUKKER DU HULLERNE I DIT DIGITALE SIKKERHEDSNET

1. Få fundamentet på plads

Kortlæg netværk, enheder, data og systemer – og identificér de største sårbarheder. En opdateret firewall er et grundlæggende første forsvarsværk, men den skal konfigureres, overvåges og vedligeholdes løbende.

2. Del netværket op

Segmentér netværket, så en kompromitteret computer eller enhed ikke automatisk giver adgang til resten af virksomheden. Mikrosegmentering kan begrænse, hvor langt et angreb kan sprede sig.

3. Gør adgang personlig

Behandl digitale adgange som fysiske adgangskort: Brugere og enheder skal kun have adgang til det, de har brug for. Network Access Control og Zero Trust-principper kan sikre, at identitet og enhed bliver verificeret, før der gives adgang.

4. Overvåg – og vær klar til at reagere

Sikkerhed er ikke en engangs-investering. Overvåg netværk, endpoints og cloud for mistænkelig aktivitet, og sørg for at kunne opdage, håndtere og gendanne efter et angreb. Løbende sårbarhedsscanning og centraliseret logning kan være en del af fundamentet.

5. Byg sikkerhed ind i fremtidens infrastruktur

Sikkerhed skal tænkes ind, når virksomheden tager ny teknologi i brug – fra cloud og AI til IoT og nye arbejdsformer. Vælg en arkitektur, hvor netværk, sikkerhed og data spiller sammen, og hvor løsningen kan udvikles i takt med virksomheden.



disciplin, hvis du manuelt skal åbne adgang til medicinsk IT hvor menneskefejl ikke må ske, men med ClearPass følger adgangen dig automatisk. Det gør mange processer nemmere og sikrer i hverdagen, så du slet ikke skal tænke over det,” siger Jeppe Ruokokoski.

Hver virksomhed sit sikkerhedsbehov

Nu er baseline på plads, og det er tid til at skrue op for og forfine sikkerheden. Der findes ikke én sikkerhedsmodel, der passer til alle. En produktionsvirksomhed med store maskiner har andre risici end et kontor med primært cloudbaserede tjenester. Og en virksomhed, der anvender AI-agenter eller andre automatiserede systemer, skal forholde sig til, hvilke data og systemer de får adgang til.

“

Det gælder om at skabe et forsvar i alle lag af dit netværk for også at være robust i fremtiden.

”Sikkerhed og netværksløsninger bør ikke være en samling af standardprodukter, men en del af virksomhedens samlede IT-arkitektur,” siger Jeppe Ruokokoski.

Dit netværk, dine fordele

Jeppe Ruokokoski ser ikke bare netværkssikkerhed som en pragmatisk foranstaltning. Han mener i langt højere grad, at det kan bruges som en værdiskabende investering.

”Virksomhedens netværk skal ikke bare være en passiv investering, som fornyes hvert femte år. Det kan blive en indtjeningskilde.

Et eksempel kunne være, hvis du arbejder med retail. Her kan du bruge dine data til at kortlægge hotspots i butikken, hvor kunderne bruger mest tid. Med den viden kan du få flere varer hen til kunden og sælge mere. Det er min overbevisning, at mange virksomheder kan bruge deres eget netværk og data til at skabe en konkurrencefordel,” fortæller han.

Det kræver dog, at data kan bruges på tværs af infrastrukturen, og at sikkerhed og adgang tænkes ind fra begyndelsen.

Et holistisk netværk er et robust netværk

Kigger man få år frem, ser Jeppe Ruokokoski en udvikling, der kommer til at stille endnu større krav til virksomheders netværk. AI udvider konstant sine muligheder og kvantetek-

nologi bliver snart en naturlig del af samfundets teknologi-værktøjskasse. Og sikkerheden? Ja den får kun et endnu større trusselsbillede.

”Udviklingen af kunstig intelligens øger konstant risikoen for hacking. Det gælder om at skabe et forsvar i alle lag af dit netværk for også at være robust i fremtiden. Hver gang du som virksomhed foretager en investering i dit netværk og datasikkerhed, skal det passe ind i det eksisterende IT-økosystem. Det nytter ikke noget, at din data kun kan bruges af en enkel komponent, det skal rundt i hele netværket.”

”Virksomheder der tænker netværk holistisk formår at styrke deres drift, sikkerhed, og evne til innovation. Det er fremtidens konkurrencemodell”



1. FIREWALL – HOLD UBUDNE GÆSTER UDE

En digital portvagt ved netværkets ydre grænse, som kontrollerer trafik ind og ud.

2. SEGMENTERING – BEGRÆNS SKADEN

Del netværket op i separate zoner, så et angreb ét sted ikke kan sprede sig til hele virksomheden.

3. DIGITALE ADGANGSKORT – GIV KUN ADGANG TIL DE RETTE

Vis brugere og enheder med forskellige adgangsniveauer – kun særligt godkendte får adgang til kritisk infrastruktur.

4. OVERVÅGNING – HOLD ØJE MED TRAFIKKEN

Et overvågningslag følger aktiviteten i hele netværket og reagerer på mistænkelig adfærd.

5. KRITISK INFRASTRUKTUR – BESKYT DET VIGTIGSTE

Placer virksomhedens vigtigste data og systemer inderst, beskyttet af de øvrige sikkerhedslag.

HVEM ER NLOGIC?

nLogic specialiserer sig i tilgængelige og robuste netværk, datacentre og IT-infrastruktur. Virksomheden er grundlagt i Norge og blev etableret i Danmark i 2022 med hovedkontor i København. Som en del af løsningerne tilbyder nLogic også rådgivning, konsulentytelser og support. Løsningerne er målrettet service, provider-segmentet og virksomheder, kommuner og regioner, som håndterer kritisk infrastruktur.

nLOGIC