Ulrik Ledertoug, Director of Business Development hos Orange Cyberdefense.

SÅDAN FÅR I MEST UD AF REGERINGENS CYBER-SIKKERHEDSTILSKUD

Hvis jeres virksomhed modtager 50.000 kroner til rådgivning om cybersikkerhed, så gælder det om at få tilskuddet til at række så langt som muligt. Det kræver både overblik og indsigt – samt en god plan! Hos Orange Cyberdefense er vi eksperter i at analysere virksomheders, myndigheders og organisationers it-sikkerhed og rådgive om, hvordan man bedst prioriterer de nødvendige indsatsområder i forhold til det aktuelle trusselsbillede.

I mange år har cybersikkerhed i dansk erhvervsliv mest handlet om at bygge høje mure omkring netværket, som holdt de cyberkriminelle ude. Men i dag står vi overfor et langt mere kompliceret trusselsbillede. Nu gælder det i højere grad om at være i stand til at holde kerneforretningen kørende, selvom cyberkriminelle trænger igennem det ydre forsvar.

"Vejen til et mere tidssvarende cyberforsvar varierer meget fra virksomhed til virksomhed. Den bedste strategi afhænger i høj grad af, hvor moden sikkerheden er. Det vil sige, hvilke sikkerhedslag der allerede er på plads, hvordan netværket og forretningen er bygget op, hvor store angrebsfladerne er og hvilke risici, man er villig til at løbe", forklarer Ulrik Ledertoug, Director of Business Development hos Orange Cyberdefense.

Vi ved, hvor skoen trykker

"Vores erfaring viser, at opmærksomheden omkring cybersikkerhed - og indsigten i området, halter hos mange SMV'er. Det er et stort problem, for det gør dem utrolig sårbare over for angreb", fortæller Ulrik Ledertoug.

I Orange Cyberdefense har vi adgang til enorme mængder af data intelligence indsamlet fra over 500 informationskilder 24/7. Når vi analyserer disse data, får vi et meget detaljeret billede af, hvordan det globale trusselsbillede udvikler sig. På den baggrund er vi stand til at rådgive offentlige myndigheder og virksomheder om, hvad det betyder for deres organisation og forretning - og hvordan de skal respondere og agere. "Som trusselsbilledet ser ud i dag, er det ikke muligt at sikre sig 100 procent mod hacker- og cyberangreb, men vi anbefaler, at man særligt prioriterer disse fem sikkerhedsområder højt, for så står man langt bedre rustet i den verden, vi lever i, i øjeblikket", siger Ulrik Ledertoug.

1) Få styr på, hvad I har i netværket

Kun de færreste virksomheder har fuldt overblik over al hardware og software i deres netværk – og man kan ikke beskytte, hvad man ikke ved, man har. I vores daglige arbejde finder vi gang på gang masser af "shadow IT", der ikke er patchet eller opdateret. Det er ulykker, der bare venter på at ske. Løsningen er at få styr på alle assets. Dvs. at du skal have skabt et overblik over, hvilke systemer der kører i netværket, og hvilke sårbarheder har de? Start med de eksterne systemer – altså dem der kan nås fra internettet. Næste skridt er at anvende sårbarhedsscannere til at finde sårbarheder og fejlkonfigurationer, som typisk er åbne døre for cyberkriminelle.

2) Beskyt kritiske systemer og IP-adresser

Tjek grundigt, at backups af Domain-controllere og kritiske assets er tilgængelige og fuldt beskyttet mod uautoriseret adgang. Backup-processer og -procedurer bør testes på kontinuerlig basis. Sikkerhedskopier bør altid opbevares, så de er fuldstændig beskyttet mod uautoriseret adgang.

3) Lad "hackere" angribe jeres netværk

Sørg for, at der bliver foretaget penetrationstest af en etisk hacker flere gange om året for at få verificeret jeres sikkerhedssetup og sikre at eventuelle fejlkonfigurationer opdages i tide. Hvis I kun vurderer jeres cybersikkerhed indefra, kan selv alvorlige sårbarheder være svære at få øje på. Det gælder om at sætte sig i angriberens sted, hvilket godt kan være rigtig svært, fordi de cyberkriminelle hele tiden bliver mere opfindsomme og kreative.

4) Indfør Zero Trust

Flade netværk med lav sikkerhed er opskriften på problemer, derfor skal du være yderst opmærksom på, hvem du giver adgang til hvad. Hvorfor give kantinepersonalet adgang til økonomisystemet? Vend logikken om: Ingen har adgang til noget – medmindre deres rolle i virksomheden kræver det. I så fald vil selv tyveri af en betroet medarbejders identitet give langt færre muligheder for at tilgå følsomme data og kritiske systemer.

5) Segmentér jeres netværk

Inddeling af netværket i "brandsikre rum" skaber langt bedre muligheder for at overvåge og kontrollere al trafik i netværket. Med segmentering kan man sætte mikroperimetre omkring følsomme data og systemer, som effektivt holder dem uden for hackernes rækkevidde, og dermed skaber langt mindre angrebsflader. Fordi den nye segmenteringsteknologi er softwarebaseret, behøver man ikke at lave tunge, manuelle access control lists og komplicerede routing-tabeller, som man hurtigt taber overblikket over. Med softwarebaseret segmentering er det muligt at styre trafikken i hele netværket ved hjælp af kun 10-20 policies – uanset hvordan det er bygget op rent fysisk.

Vælg en bred sikkerhedspartner

Da det er de færreste SMV'er, der råder over de nødvendige ressourcer internt, anbefaler vi altid, at I indleder et samarbejde med en sikkerhedsrådgiver. På den måde får I adgang til den nødvendige indsigt og viden, der kan få afgørende betydning for virksomheden på længere sigt. Vælg altid en rådgiver, som også kan assistere jer med implementering af de konkrete løsninger, I vælger at gå videre med – og som kan hjælpe med at administrere og overvåge løsningerne fremover. "Når vi indleder et samarbejde med en virksomhed, myndighed eller offentlig organisation, er det en kæmpe fordel for begge parter, hvis vi har haft mulighed for at lave en Security Assessment og analysere det eksisterende cyberforsvar. Det giver os de bedste forudsætninger for at komme med præcise anbefalinger til indsatsområder og forbedringer. Herudover hjælper vi naturligvis også med at levere, implementere, drifte, administrere og overvåge en lang række forskellige sikkerhedsløsninger og Managed Security Services på stort set alle områder inden for cybersecurity", fortæller Ulrik Ledertoug.

FAKTA

- Orange Cyberdefense er en af Europas ledende it-sikkerhedsleverandører med 25 års erfaring inden for cybersecurity og Managed Security Services. Kompetencerne spænder over alt fra overvågning, analyse, rådgivning og sparring til implementering, drift og administration af kundernes strategiske it-sikkerhedsplatforme og sikkerhedsløsninger.
- Orange Cyberdefense er eksperter i at analysere virksomheders, myndigheders og organisationers it-sikkerhed og rådgive om, hvordan man bedst prioriterer de nødvendige indsatsområder i forhold til det aktuelle trusselsbillede.
- Orange Cyberdefense råder over 250 af branchens bedste analytikere fordelt på 18 SOCs, 14 CyberSOCs og 4 CERTs i hele verden. De indsamler og analyserer data fra over 500 informationskilder 24/7, hvilket giver markedets bedste intelligencebasserede billede af, hvordan det globale trusselsbillede udvikler sig.
- Orange Cyberdefense har over 8.000 kunder i 160 lande og beskæftiger over 2.500 medarbejdere i hele verden, hvoraf ca. 60 er placeret i Danmark.
- Orange Cyberdefense er sammen med Orange Business Service en del af Orange Group – en af verdens førende teleoperatører med ca. 150.000 ansatte og 257 mio. kunder på verdensplan.

Læs mere her: 50.000 kr. i tilskud til digital sikkerhed og ansvarlig dataanvendelse - Orange Cyberdefense Denmark