Støvede planer for it-sikkerhed gør ondt, når angrebet rammer

Danske virksomheder og offentlige organisationer er i stigende grad offer for cyberkriminalitet. Alligevel har mange utilstrækkelige eller slet ingen beredskabsplaner for, hvordan de skal håndtere it-angreb, der på få sekunder kan gøre omfattende økonomisk skade og få langsigtede konsekvenser. Døgnovervågning kan være en del af løsningen

Cyberangreb bliver kun flere og mere avancerede. Man kan ikke beskytte sig 100 pct. mod truslerne - derfor er det nødvendigt, at der ligger en beredskabsplan klar, når ubeldet rammer. Det mener Lars Højberg, der er chef for NetDesign Security Operations Center. Foto: Peter Jarvad

Af Fredrik Malte Petersen for NetDesign

Mange danske virksomheder har ikke styr på beredskabsplanerne, hvis de skulle blive udsat for et it-angreb. Det kan føre til svære økonomiske tab, og gøre det svært at få gang i forretning og it-systemer igen, efter et angreb.

Det siger, Lars Højberg, der er chef for NetDesigns Security Operations Center (SOC) – et center, der overvåger kunders it-netværk mod ondsindet indtrængen og andre angrebstyper.

"Beredskabsplaner er sindssygt vigtige, fordi tid er en afgørende faktor ved f.eks. ransomware-angreb, cyberspionage, DDoS-angreb og anden it-relateret kriminalitet. Hvis du har en gennemarbejdet og indøvet beredskabsplan, sparer du værdifuld tid. Men den mangler i mange virksomheder," siger han.

Voksende behov for beredskab

Der er ellers god grund til at have en opdateret og indøvet beredskabsplan, som en del af sin cybersikkerhed.

Ifølge rapporten Cybercrime Survey 2020, der er udarbejdet af PWC i samarbejde med Bestyrelsesforeningen m.fl., har 58 pct. af danske virksomheder været udsat for minimum én sikkerhedshændelse inden for det seneste år. En klar stigning fra 2018, hvor andelen var 44 pct.

Mange virksomheder har slet ingen eller får ikke løbende opdateret deres beredskabs- og kommunikationsplaner for håndtering af hacking og andre ondsindede angreb. Den går ikke længere, siger Lars Højberg.

"Rigtig mange virksomheder har i alt for lang tid været af den overbevisning, at de kunne beskytte sig ud af trusselsbilledet ved at bygge en tilpas høj sikkerhedsmur," indleder han.

"Billedet er dog ved at ændre sig, og flere og flere er kommet til den erkendelse i dag, at man ikke kan beskytte sig ud af trusselsbilledet. I stedet må man forberede sig på den dag, hvor man bliver udsat for en sikkerhedshændelse. Derfor er det vigtigt med en god beredskabsplan, som inkluderer en række af de services et Security Operations Center kan levere. Med en SOC i ryggen, har man nemlig mulighed for at opdage og reagere hurtigt og effektivt på sikkerhedshændelser, og det er vigtigt, hvis man vil begrænse følgerne af ondsindede angreb."

Døgnovervågning er et godt fundament

Når en trussel opdages hurtigt, har man mulighed for at minimere skaden og forhindre, at størstedelen af truslen bliver til grim virkelighed. Derfor er det en god idé at etablere et samarbejde med en SOC, som har de rigtige tekniske værktøjer, processer og specialister, som giver optimale muligheder for at reagere på mistænkelig adfærd, før der ligger en mail med krav om løsepenge i virksomhedens indbakke.

"I vores Security Operations Center hos NetDesign kan vi overvåge kunders netværk og se, om der foregår aktivitet, der ikke skal være der. Ved at automatisere mange af vores processer, kan vi minimere reaktionstiden og f.eks lave en hurtig automatisk isolering af de kompromitterede systemer og enheder hos kunden. På den måde inddæmmer vi skaden og reducerer konsekvenserne," siger Lars Højberg.

Gammel plan fjerner tillid

"En gennemarbejdet og operationel plan, der afprøves regelmæssigt, kan være forskellen på, om virksomheden hurtigt får reageret og håndteret et cyberangreb, som ellers lynhurtigt kan udvikle sig til en krise i virksomheden. En krise, kan betyde et stort økonomisk tab og/eller massivt oprydningsarbejde. For eksempel reetablering af data og store dele af it-infrastrukturen," siger Jørgen Papadopoulos, der er Sikkerhedskonsulent og partner i Devoteam.

"En dårlig plan giver falsk tryghed og ekstra forvirring, når krisen sætter ind, og tid er det afgørende parameter. Vi ser alt for mange formelle planer uden konkrete anvisninger af handlinger og ansvar. Når der så opstår en situation, hvor de tager beredskabsplanerne frem, mister de hurtigt tilliden til den, fordi oplysningerne ikke passer. Det skaber en utryg situation og større forsinkelser og det er præcis det virksomheden skal undgå."

Planen skal blandt andet gøre det muligt hurtigt at sammenkalde relevante beslutningstagere og klæde dem på til at træffe en række svære beslutninger, som ofte har en række indbyggede dilemmaer, fortæller Lars Højberg.

"Det kræver f.eks., at personen, som har det endelig mandat til at lukke ned for forretningskritiske systemer, er til stede, når en teknisk rådgiver anbefaler at tage de ramte servere eller andre enheder af nettet for at forhindre angrebet i at brede sig."

Lang nedetid gør ondt på økonomien

Et cyberangreb er ofte forbundet med store økonomiske omkostninger – også efterfølgende, hvor virksomheden ikke kan servicere kunderne eller opretholde den sædvanlige omsætning pga. nedetid.

Prioriterer man ikke ressourcer til et sikkerhedsberedskab, men tager man det 'som det kommer', kan det derfor få store konsekvenser.

"Hvis man for eksempel ikke abonnerer på en eller anden form for døgnovervågning og ikke har en beredskabsplan, så er man på bagkant, når angrebet finder sted. Og så mister man vigtig tid, man kunne bruge til at komme bedre gennem angrebet, og lang nedetid koster mange penge," siger Lars Højberg.

OM NETDESIGN OG NETDESIGN SOC

- NetDesign er en it- og konsulentvirksomhed, som er ekspert i at designe, levere, vedligeholde og drifte løsninger inden for Cyber Security, Digital Infrastructure, Collaboration og Customer Engagement.
- NetDesigns Security Operations Center overvåger danske virksomheder, myndigheder og organisationers infrastruktur 24 timer i døgnet og beskytter dem mod alle typer cyberangreb fra hackere og andre it-kriminelle.
- NetDesign SOC udfører overvågning, alarmhåndtering, incident response, threat hunting og forensics.
- NetDesigns SOC-tjenester er i høj grad baseret på automatisering, hvilket gør det muligt at opdage og reagere hurtigt på sikkerhedshændelser.
- NetDesigns SOC er placeret i København og er bemandet 24/7 af erfarne og højt kvalificerede medarbejdere, godkendt af Forsvarets Efterretningstjeneste.
- NetDesign har eksisteret i over 30 år og har ca. 320 medarbejdere.

Annoncen er produceret af Børsen Creative i samarbejde med NetDesign