Cyberansvar og cyberangreb

Johannes Luef og Helen Kobæk, *associerede partnere, Faarup & Partners*

DEBAT Det er efterhånden hævet over enhver tvivl, at beskyttelse mod cyberangreb er et kæmpe problem for alle virksomheder og bør være topprioritet for bestyrelser i alle virksomheder. Mærsk har estimeret, at cyberangrebet i 2017 har kostet dem næsten 2 mia. kr. Demant har berettet om et tab på ca. 600 mio. kr. grundet et cyberangreb i 2019, og senest var ISS ramt af cyberangreb.

Relevante emner på bestyrelsens cyberagenda burde være en bæredygtig strategi med udgangspunkt i virksomhedens nuværende situation og plan for det videre arbejde, tekniske tiltag og organisatoriske aspekter. Sidstnævnte kunne handle om placeringen af CISO (chief security officer), etablering af et SOC (security operation centre), medarbejderuddannelse og træning og kontinuerlige krise- og beredskabs øvelser.

Hvordan skal bestyrelsen gribe opgaven med at holde styr på cybersecurity an? Der er ingen patentløsninger. Opgaverne kan outsources til eksterne firmaer og rådgivere, men det kan ansvaret ikke. Emner i forhold til cyberresilience er langhårede og meget tekniske. Kunne "board governance by committee", som man f.eks. kender på revisions-, risiko- og remunerationsområdet, være en løsning? Der er eksempler på at store organisationer, der har en sådan komité, som typisk samles under ledelse af en formand, som også er medlem af bestyrelsen. Komitéen samles forud for det egentlige bestyrelsesmøde og udarbejder en fremlæggelse på området for den samlede bestyrelse.