MARSH

SOCIAL ENGINEERING FRAUD

Nye trends inden for økonomisk kriminalitet og hvordan virksomheden kan begrænse sin risiko ved opdatering af interne kontroller.

Virksomheder verden over oplever i stigende omfang økonomisk kriminalitet i form af *Social Engineering Fraud*, en form for kriminalitet, hvor gerningsmanden udnytter en social relation hos virksomhedens medarbejdere ved at udgive sig for en person, som en given medarbejder kender eller ved, hvem er, og derved manipulerer denne medarbejder til at overføre et eller flere større beløb til sig selv.

Disse bedrag kommer i flere former, men navnlig to skiller sig ud:

DEN FALSKE DIREKTØR

Flere medarbejdere har oplevet et opkald efterfulgt at en mail fra en gerningsmand, der har udgivet sig for at være direktør i moderselskabet med besked om, at dette er i færd med et fortroligt projekt, som kræver overførsel af et større beløb uden om de sædvanlige retningslinjer for overførsel. I sådanne sager har gerningsmanden undersøgt virksomheden nøje og har oprettet en mailadresse, der indeholder navnet på direktøren og moderselskabet, og i mange tilfælde har medarbejderen først opdaget bedraget, når overførslen er sket.

MARSH ANBEFALER

Marsh anbefaler, at ledelsen indprenter og jævnligt gentager overfor alle medarbejdere, at en sådan henvendelse ikke vil kunne finde sted, og at enhver medarbejder, der modtager en sådan henvendelse eller nogen anden henvendelse om ekstraordinære overførsler straks kontakter direktionen telefonisk med henblik på verifikation af henvendelsen eller anmeldelse af bedrageriforsøget.

NYE BANK-OPLYSNINGER FRA EN SAMARBEJDS-PARTNER

En lang række virksomheder har oplevet, at en medarbejder har modtaget en henvendelse fra en gerningsmand, der har udgivet sig for at være en af virksomhedens leverandører eller samarbejdspartner med oplysning om, at denne har skiftet bankforbindelse, og at overførsler fremover skal ske til en nærmere angiven konto i et pengeinstitut. Også her har gerningsmanden et navn og en mailadresse, der tilsyneladende er autentisk inklusiv et autentisk logo. Disse tab kan være meget store, idet mange overførsler kan være sket, inden den rigtige samarbejdspartner rykker for betalingen.

MARSH ANBEFALER

For at undgå denne form for bedrageri anbefaler Marsh, at virksomheden udover de sædvanlige kontrolprocedurer også implementerer regler om opdaterede og godkendte leverandørlister med angivelse af bankdetaljer, samt at ændringer i en samarbejdspartners bankdetaljer kun kan foretages af en ledende medarbejder og kun efter telefonisk bekræftelse hos samarbejdspartneren på det telefonnummer, som lederen i forvejen var i besiddelse af.

FORSIKRINGS-DÆKNING

Sådanne bedragerier er som udgangspunkt omfattet af en kriminalitetsforsikring, herunder Marshs kriminalitetsfacilitet, men flere forsikringsselskaber er begyndt at betinge dækningen af, at virksomheden har implementeret ovenstående kontroller.

Marsh A/S
Teknikerbyen 1
2830 Virum
Danmark

CVR 87377016
+45 45 95 95 95
www.marsh.dk
Marsh.denmark@marsh.com

KONTAKT

Har du spørgsmål til risici, der relaterer sig til Social Engineering Fraud er du meget velkommen til at kontakte Marsh. Kontakten kan enten være via din sædvanlige kontaktperson hos Marsh eller direkte til Marsh Danmarks FINPRO Practice.

MARSH DANMARK FINPRO PRACTICE

Pernille Palsby
Senior Vice President
Insurance Broker, FINPRO
+45 45 95 95 95
pernille.palsby@marsh.com

Bernt Sandell
Senior Vice President
Head of Nordic
FINPRO Practice
+45 45 95 95 95
bernt.sandell@marsh.com