



8 gode råd til at undgå svindel i din virksomhed



**WHISTLEBLOWER
PARTNERS**

Svindel i virksomheder er et stort og fortsat stigende problem i takt med øget globalisering, digitalisering og en øget kompleksitet på mange felter, ligesom Coronaen har øget risikoen.

Svindel internt i virksomheder er et større problem, end mange tror. En virksomhed kan miste op til fem procent af sin årlige omsætning på grund af intern svindel. Det viser undersøgelser internationalt. Danske virksomheder oplever også en kraftig stigning inden for økonomisk it-kriminalitet, hvor medarbejderne bliver snydt til at udbetale penge til eksterne kriminelle.

Det er klart, at kontrol er uhyre vigtigt, men selvom man kan komme langt med fx revisionsværktøjer, er løsningen desværre ikke helt så enkel. Der er i lige så høj grad brug for en god arbejdskultur, hvor medarbejderne opfordres og påvirkes til at træffe de rigtige valg, så de ikke begår bevidste eller ubevidste fejl, der kan koste virksomheden dyrt.

Siden Covid-19 epidemien ramte os er hjemmearbejde blevet den nye normal, og tendensen må antages at fortsætte. Dermed er der også opstået nye risici for virksomheder.

Her er der nogle opmærksomhedspunkter i forhold til svindel i virksomheder:

1. Øget kontrol og opmærksomhed omkring procedurer i virksomheden

Færre på kontoret kan risikere at betyde, at procedurerne bliver slækket internt i virksomheden for at få dagligdagen til at glide. Passwords kan blive udlånt mellem kollegaer, og der er risiko for, at samme person både kan godkende regninger, ændre kreditoroplysninger og godkende betalingen.

Det giver gode muligheder for økonomisk svindel, hvor svindleren kan dække sine spor. Hvis det bliver gjort i det små over en længere periode, kan svindlen nå at blive ganske omfattende, før den – måske – bliver opdaget.

Virksomheder bør derfor ikke slække på procedurer internt i virksomheder, selvom medarbejderne måske i øget grad arbejder enkeltvis hjemmefra og hele tiden "regulere" kontrolaktiviteterne i takt med risikoen.

2. Høj opmærksomhed overfor hacking, phishing og anden it-svindel

Kriminelle forsøger i stigende grad at narre personlige koder eller oplysninger ud af virksomheder via opkald (vishing), sms (smishing) eller mails (phishing). Svindleren udgiver sig ofte for at være fra fx virksomhedens bank eller samarbejdspartner, offentlige myndigheder, NemID eller Nets.

Nogle virksomheder får deres mailsystem hacket direkte, andre it-svindlere bruger phishing, hvor et klik på et link eller fil i en falsk mail kan give adgang til virksomhedens it-systemer.

Det er meget vigtigt at indskærpe overfor medarbejdere, at de skal være skeptiske overfor uopfordret kontakt eller mails, der ser usædvanlige eller mærkelige ud, og medarbejdere bør indskærpes, at de aldrig skal udlevere personlige oplysninger eller koder. Er den enkelte medarbejder i tvivl, bør denne altid kontakte virksomhedens IT-afdeling - hellere en gang for meget end en gang for lidt.

3. Undgå CEO-fraud

CEO-svindel indtræffer, når en medarbejder bliver narret til at betale en falsk faktura eller til at foretage en uautoriseret overførsel med virksomhedskontoen til en konto ejet af svindleren. Svindleren udgiver sig for at være højtstående person inden for den pågældende virksomhed.

Det er vigtigt at indskærpe procedurer i virksomheden for betaling af regninger og overførsel af midler, og at alle forespørgsler, der ikke er normale, følges op med en kontrol, uanset hvor meget overførslen haster i mailen. Et telefonopkald til CEO'en kan ofte afsløre hele svindlen, og virksomheden kan spares for store tab.

4. Undgå fakturasvindel

Ved fakturasvindel eller -bedrageri udgiver svindleren sig for at repræsentere en virksomheds kunde eller leverandør, og beder om, at fremtidige fakturaer betales til en ny bankkonto - som tilhører svindleren.

Det er vigtigt at sørge for, at de relevante medarbejderne er informeret og opmærksomme på denne form for bedrageri, og hvordan man undgår det. Det er således væsentligt at instruere personale med ansvar for at betale fakturaer om altid at kontrollere dem for uregelmæssigheder, at etablere faste procedurer for håndtering af manuelle betalinger og at kontrollere af legitimiteten af betalingsanmodninger.

Det er en fordel at anvende et automatiseret betalingssystem for dermed at holde antallet af manuelle betalinger på et minimum.

5. Vær opmærksom på svindel ved ændringer i bankoplysninger

Det er vigtigt at være opmærksom på, at denne type svindel med ændring af bankoplysninger eksisterer, og at denne viden deles med de funktioner i virksomheden, som kan være potentielle ofre for sådanne ændringer i bankoplysninger.

Hvis virksomheden får en mail vedrørende ændringer i bankoplysninger, skal der altid ringes til leverandøren, med henblik på at få en bekræftelse fra virksomhedens sædvanlige kontaktperson på rigtigheden af kontoændringen.

6. Undgå momssvindel

Det er en væsentlig risiko for, at virksomheder bliver udsat for momssvindel ved handel i relation til momskaruseller. Momskarusseller er kendetegnet ved, at der handles med varer eller ydelser hen over landegrænser. Typisk forhandles varerne via en stråmand, der ikke angiver eller afregner moms, når varerne sælges videre. Derefter handles varerne gennem en eller flere mellemænd, inden de sendes ud af Danmark igen og fortsætter karusellen.

Disse mellemænd kan være helt reelle danske virksomheder. Det betyder, at danske virksomheder let kan ende i en fælde, der både kan give økonomisk tab fx i form af mistet momsfradrag, ukurante varer, et dårligt ry eller en unfair konkurrence i branchen. I nogle tilfælde kan et helt marked blive undermineret, inden svindlen opdages.

Hvis der er den mindste tvivl om leverandøren eller varerne, som virksomheden er i gang med at købe, så skal man holde sig fra handlen. Og det anbefales, at det altid tjekkes, om de virksomheder, som virksomheden handler med, er momsregistrerede. Det gør virksomheden ved at søge på leverandørens momsnumre.

På SKATs hjemmeside er der desuden opregnet en række specifikke opmærksomhedspunkter i forbindelse med køb og salg af varer.

7. Pas på printere

Printere i virksomheder kan udgøre en betydelig sikkerhedsrisiko for en virksomhed, hvis man ikke er opmærksom.

Udviklingen i teknologien i printere, herunder det forhold at printere indeholder de samme hardwarekomponenter som en computer, eksempelvis drev, kontrolpanel og tastatur betyder, at

virksomheder bør sikre printere mod angreb på lige fod med en PC. Dette bliver ofte overset, selvom danske virksomheder generelt er meget bevidste om cybertruslen.

8. Kontakt banken og anmeld svindel eller forsøg på svindel til politiet

Hvis svindlen er foregået gennem virksomhedens bank, bør denne altid kontaktes med henblik på muligheden for at tilbageføre beløbet. Kontakt desuden altid politiet i tilfælde af svindel eller svindelforsøg, selvom du ikke nåede at blive offer for svindel. Husk at gemme dokumentationen og medtag denne i anmeldelsen til politiet.