

GUIDE

Sådan bruger I actioncards ved digital og økonomisk svindel

Målerettet SMV'er



Styrelsen for
Samfundssikkerhed

Guide til brug af actioncards

Før hændelsen

Sørg for at alle i virksomheden kender til actioncards

Actioncards er et hændelsesredskab I kan bruge, hvis I oplever digital og økonomisk svindel, eller mistænker forsøg på svindel. Kortene virker kun, hvis alle i virksomheden kender til dem og ved, hvornår og hvordan de skal bruges.

Derfor er det vigtigt, at I gennemgår dem i fællesskab før, I oplever en hændelse.

I kan også bruge actioncards som del af virksomhedens awareness-træning og i oplæring af nye medarbejdere.

Gennemgå handlinger og rækkefølge

Tal kortene igennem og sørg for, at alle i virksomheden ved, hvordan de skal følge handlingsanvisningerne på de forskellige kort. Hvis jeres virksomhed eksempelvis har en procedure eller funktion til indrapportering af phishing-mails, er det vigtigt, at alle kender den.

Gennemgå også rækkefølgen af handlingerne på de forskellige kort. Det kan være, at der er en mere hensigtsmæssig rækkefølge for jeres virksomhed. Det kan eksempelvis være, at første handling hos jer altid vil være at kontakte jeres leverandør eller at orientere ledelsen.

Aftal, hvem der gør hvad

Det er også vigtigt at aftale, hvem i jeres virksomhed, der skal kontaktes og aktiveres, hvis I udsættes for en hændelse. Det er ikke sikkert, at det er den medarejder, som opdager hændelsen, der skal udfylde alle aktiviteter på kortet.

I kan lave en kontaktliste over de personer og funktioner, internt og eksternt, som skal kontaktes i tilfældet af et angreb eller svindel. Sørg for, at alle i virksomheden kender listen og ved, hvor de kan finde den.

Det kan f.eks. være oplysninger og telefonnummer til:

- Ledelse
- Økonomiansvarlig
- It-ansvarlig
- Bankens akutnummer
- Cyberhotline for digital sikkerhed
- It-leverandør
- Forsikringens akutnummer

Under hændelsen

Find det rigtige kort

De forskellige actioncards starter altid med en beskrivelse af den oplevelse og de tegn på svindel og angreb, som du ofte vil opleve. Det er ikke sikkert, at du oplever dem alle, men hvis du kan genkende et eller flere tegn, skal du reagere. Det er vigtigt, at alle i virksomheden er opmærksomme på de tegn, der er på digitale angreb og svindel.

OBS: Actioncards dækker for nuværende ikke ransomware og malware angreb. Her kan I bruge Nødplan ved cyberangreb (se side 5).

Se, hvad I skal gøre som det første

Det er en god idé at læse hele kortet igennem som det første. Kortene giver et hurtigt overblik over, hvilke handlinger man straks bør foretage sig – selv når I ikke genkender angrebstypen med det samme. Det er ikke en udtømmende liste, men et godt sted at starte for at afdække og bremse hændelsen. Handlingerne kan også foregå sideløbende, så man eksempelvis ringer til banken, imens en kollega hjælper med at kontakte den økonomiansvarlige.

Efter hændelsen

Lær af hændelsen og advar andre

Det er altid en god idé at dele oplevelsen med hele virksomheden. På den måde kan I skabe en fælles forståelse af digital svindel, og hvad I skal gøre, når I oplever noget mistænksomt.

Når I skal anmelde angrebet til myndighederne, er det vigtigt at have indsamlet og sikret beviser. I kan læse mere om sikring af beviser [her](#).

Ordliste

Hacking af mailkonto (BEC-angreb)

BEC-angreb (Business Email Compromise) er hacking af virksomhedens mailkonto, hvorfra hackeren kan kontakte kunder og andre med henblik på bedrageriforsøg i virksomhedens navn.

Digital svindel

Digital svindel dækker bredt over forsøg på at opnå fortrolige oplysninger, adgang til fx it-system, penge eller narre modtageren til at klikke på et inficeret link eller vedhæftet fil.

Det kan foregå via mail (phishing), sms/beskeder (smishing) eller opkald (vishing).

Flerfaktor-autentifikation/multifaktor-autentifikation

Flerfaktor-autentifikation er en loginproces, hvor brugeren får adgang på baggrund af sit brugernavn og to eller flere af:

- Noget brugeren **ved** (f.eks. pinkode eller password),
- Noget brugeren **har** (f.eks. ID-kort, mobiltelefon, nøglekort, eller USB-nøgler), eller
- Noget brugeren **er** (f.eks. ansigtsgenkendelse eller fingeraftryk), kaldes også biometrisk identifikation.

Oftest benyttes to-faktor-autentifikation, hvor eksempelvis et password (noget brugeren ved), suppleres med godkendelse på mobiltelefonen (noget brugeren har).

Phishing/smishing/vishing

Metode til forsøg på at narre modtageren af mailen/beskeden/opkaldet til i god tro at videregive personlige eller andre beskyttelsesværdige oplysninger eller give uretmæssig adgang til blandt andet it-systemer.

Ofte vil angriber ved hjælp af simpel social engineering (manipulation) forsøge at få ofrene til at klikke på links til falske hjemmesider eller åbne inficerede filer.

Spoofing

Er hackerens teknik til at udgive sig for at være en anden. Spoofing bruges f.eks. om forfalskning af afsenderadressen på e-mails eller SMS.

Vær opmærksom på, at mange smartphones sorterer beskeder ud fra afsendernavn. Det betyder eksempelvis, at en SMS med et falsk afsendernavn kan havne i samme beskedtråd som en rigtig SMS fra din leverandør.

Flere værktøjer til opbygning af et it-beredskab

Hvis I gerne vil arbejde mere med virksomhedens it-beredskab, kan I få hjælp på Sikkerdigital.dk med vores øvrige værktøjer og vejledninger.

Nødplan ved cyberangreb

Vi har udviklet en enkel skabelon til en nødplan, som beskriver de centrale roller og vigtigste kontaktinformationer, som kan hjælpe mindre virksomheder med at handle hurtigere ved et cyberangreb.

[Gå til nødplanen](#)

Skabelon og vejledning til it-beredskabsplan

For de virksomheder, der ønsker at tage skridtet videre, har vi lavet en skabelon og hjælp til at udarbejde en it-beredskabsplan. Med en it-beredskabsplan sikrer I, at de it-afhængige og forretningskritiske arbejdsprocesser i virksomheden kan reetableres og er funktionelle efter en kritisk hændelse.

[Få hjælp til at lave en it-beredskabsplan](#)

Sikkerdigital.dk

På Sikkerdigital.dk har vi samlet vejledninger og værktøjer, som hjælper virksomheder til at styrke [it-sikkerheden og forebygge cyberangreb](#).



**Styrelsen for
Samfundssikkerhed**

Datavej 20
3460 Birkerød
+45 45 16 16 66

Sikkerdigital.dk

Kontakt til Styrelsen for Samfundssikkerhed angående indhold, vejledning og værktøjer på Sikkerdigital.dk via sikkerdigital@samsik.dk

Cyberhotline for digital sikkerhed

Cyberhotline for digital sikkerhed er til borgere og virksomheder, som ønsker vejledning om, hvordan de bliver mere digitalt sikre samt håndterer og forebygger digital svindel og cyberangreb. Som borger kan du få hjælp, hvis din identitet er blevet misbrugt.

Ring 33 37 00 37