E-BOG Cyber Security

BUSINESS E-MAIL COMPROMISE

4 måder at forhindre svindlere i at få adgang til din virksomheds e-mailkonto

Building Todays and Tomorrow's IT. Together.

itm8®

Indhold

Business E-mail Compromise (BEC)-angreb er en voksende trussel mod organisationer.

Vil du gerne beskytte din virksomhed effektivt mod angreb via e-mail?

Så har vi udarbejdet denne guide som hjælp.

Hvad er et **BEC-angreb?**

Et BEC-angreb (Business E-mail Compromise) er et cyberangreb, hvor svindlere opnår adgang til en e-mailkonto i en organisation, hos en leverandør eller lignende.

Med denne adgang vil svindleren udgive sig for at være en leder, kollega eller leverandør – typisk for at manipulere medarbejdere til at overføre penge eller afsløre følsomme oplysninger ved at sende tilsyneladende troværdige mails til medarbejdere.

90%

af alle cyberangreb og datalækager involverer e-mail. Det gør e-mail til den største trussel mod din virksomheds IT.[1]

1: Cloudfare 2023 Phishing Report

Hvem er **potentielle mål** for manipulation?

Alle medarbejdere i en din virksomhed er potentielle mål. Angriberne anvender social engineering-teknikker, hvor de manipulerer din tillid for at opnå deres mål.

BEC-angreb er ofte sofistikerede og udføres af professionelle aktører, der kan operere ubemærket og undgå grundlæggende tekniske sikkerhedsforanstaltninger. Derfor er det vigtigt at være opmærksom på tegnene på et BEC-angreb, især for medarbejdere i finansielle funktioner eller andre med adgang til følsomme systemer og oplysninger.

10 tegn på et muligt BEC-angreb

Hvis du opdager uventede ændringer i dine normale workflows, bør du altid blive alarmeret. Derudover bør følgende ti scenarier altid udløse skepsis:

#01	Henvendelser, der beder dig om at ignorere interne procedurer eller sikkerhedsforanstaltninger (f.eks. at sende følsomme oplysninger via alternative kanaler).
#02	Henvendelser fra kolleger, du ikke normalt kommunikerer direkte med – herunder din direktør.
#03	Anmodninger om at omdirigere eller videresende følsomme oplysninger som f.eks. kontrakter, persondata eller forretningsdokumenter.
#04	Ændringer i betalingsoplysninger.
#05	Uventede anmodninger om betaling, information og lignende.
#06	Anmodninger om at sende betalinger på andre datoer end tidligere aftalt.
#07	E-mailvedhæftninger fra ukendte afsendere.
#08	Små eller store ændringer i kommunikationssprog.
#09	Øget pres fra afsender, som skaber en følelse af hastværk.
#10	Henvendelser modtaget uden for normal arbejdstid såsom aften, nat, morgen og ferieperioder.

Forbered dig før du bliver ramt af et BEC-angreb

Du har en vigtig rolle i at forhindre et BEC-angreb – sammen med resten af medarbejderne og organisationen.

Det er afgørende at din organisation implementerer de rette tekniske sikkerhedsforanstaltninger samt har etableret politikker og procedurer, som er tydeligt kommunikeret til organisationen.

Bliv klogere på de tekniske kontroller i vores tekniske guide "The CSIRT Guide for preventing Business Email Compromise"

Læs den her

4 måder at beskytte mod BEC-angreb

En effektiv beskyttelse mod BEC-angreb kræver klare retningslinjer. Dette er både for at kunne forebygge og hurtigt håndtere sikkerheds-hændelser.

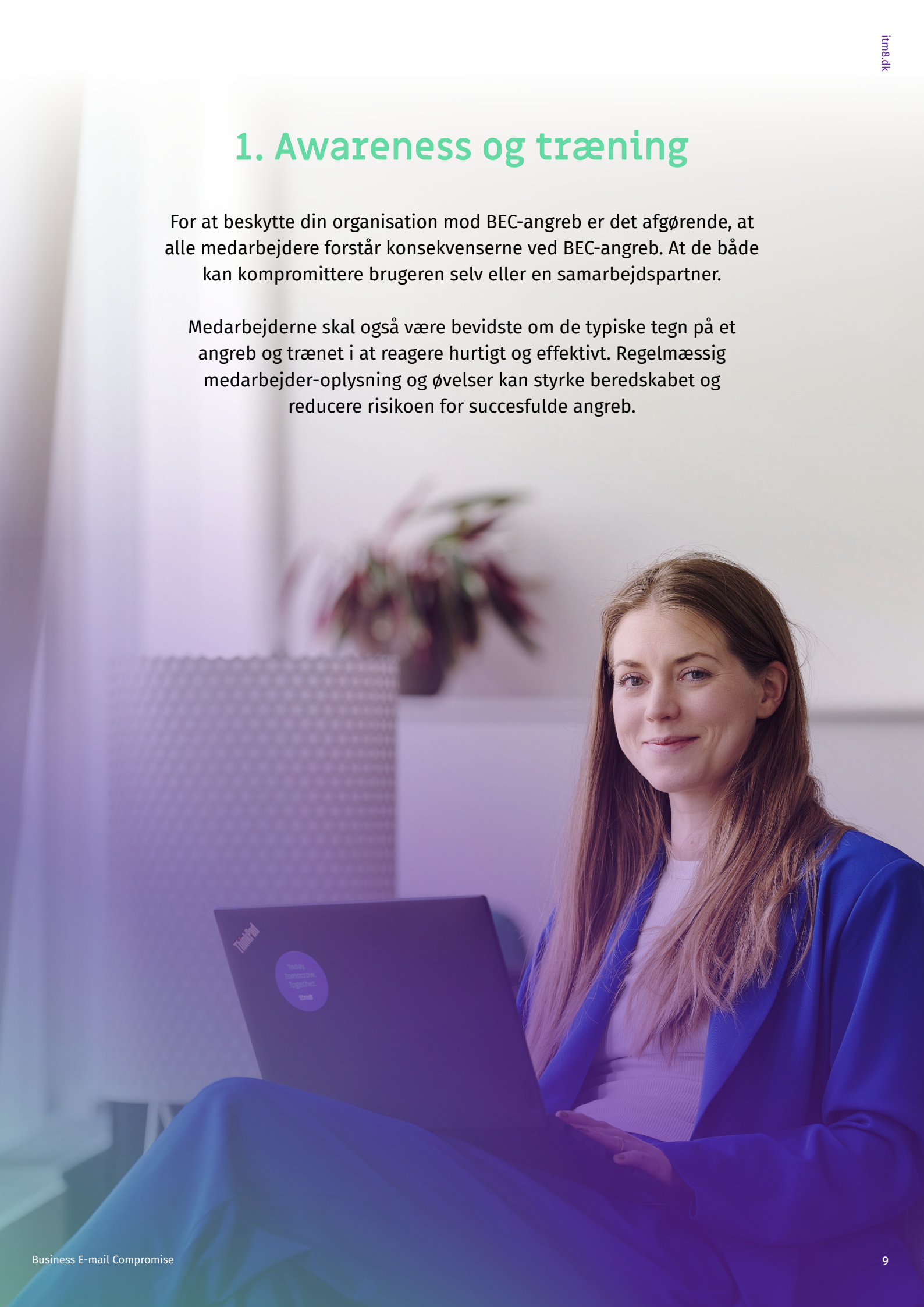
Der er fire centrale tiltag, som kan forbedre din organisations beskyt-telse mod BEC-angreb:

1. Awareness og træning
2. Håndtering af mistænkelige henvendelser
3. Rapportering og sikkerhedsprocedurer
4. Tekniske kontroller

1. Awareness og træning

For at beskytte din organisation mod BEC-angreb er det afgørende, at alle medarbejdere forstår konsekvenserne ved BEC-angreb. At de både kan kompromittere brugeren selv eller en samarbejdspartner.

Medarbejderne skal også være bevidste om de typiske tegn på et angreb og trænet i at reagere hurtigt og effektivt. Regelmæssig medarbejder-oplysning og øvelser kan styrke beredskabet og reducere risikoen for succesfulde angreb.



2. Håndtering af mistænkelige henvendelser

Medarbejderne skal kunne identificere og verificere mistænkelige e-mails samt straks informere IT-afdelingen om potentielle trusler.

Hvis der er mistanke om kompromittering, bør adgangskoder ændres med det samme.

3. Rapportering og sikkerhedsprocedurer

En tydelig rapporteringsproces bør være på plads, så usædvanlige betalings- eller købsanmodninger hurtigt kan blive undersøgt af relevante interessenter.

Medarbejdere bør opfordres til at bekræfte anmodninger om betaling via alternative – men i forvejen godkendte – kommunikationskilder f.eks. via telefon.

Derudover er det vigtigt at sikre, at medarbejdere følger faste procedurer for verifikation af kontooplysninger og vurderer økonomirelaterede henvendelser kritisk.

4. Tekniske kontroller

Tekniske kontroller er en central del i forhold til at forhindre BEC-angreb mod din virksomhed. Menneskelige fejl sker. Derfor er det vigtigt at implementere et lag af kontroller, som kan stoppe angreb, der slipper igennem.

Overvåg og opdag trusler i tide

Der er faktisk endnu et tiltag, som kan beskytte din organisation mod BEC-angreb. Det er noget så simpelt som overvågning.

Hvis du gerne vil stoppe et potentielt Business E-mail Compromise-angreb, handler det om at holde øje med mistænkelig mailaktivitet og reagere hurtigt, så angrebet kan stoppes, før skaden sker.

Men det kræver både tid og tekniske kompetencer at overvåge sin IT-infrastruktur for at kunne beskytte mod potentielle BEC-angreb. Fordi der skal indsamles og analyseres store mængder data fra forskellige sikkerhedskilder. Har du tid, ressourcer og kompetencer til det?

Security Operations Center:
En proaktiv sikkerhedsløsning

Et eksternt Security Operations Center (SOC) holder styr på din sikkerhed uden at du selv skal bruge tid på det. Et SOC er ansvarlig for at overvåge og reagere på IT-sikkerhedshændelser, der virker mistænkelige – heriblandt mulige BEC-angreb.

I tilfælde af unormal login-adfærd og mistænkelig mailaktivitet vil SOC-teamet blive alarmeret, så angrebet kan stoppes hurtigst muligt. Uden den overvågning kan kompromitteringen forblive ubemærket i længere tid og føre til alvorlige sikkerhedsbrud.

4 ting du får med et Security Operations Center

Det gør du ved mistanke om BEC-angreb

Hvad gør du, hvis du har mistanke om, at du selv er "faldet i fælden"? Eller hvis du frygter at blive involveret, fordi en leverandør er blevet angrebet?

Er du ramt af BEC?

Mistænker du, at din egen e-mailkonto er blevet kompromitteret? Så skal du logge af internettet med det samme.

Undlad så vidt muligt at kommunikere via e-mail, og kontakt din egen IT-afdeling/support for yderligere vejledning. Og kontakt eventuelt vores Incident Response Team på +45 91 95 95 95.

Er du under angreb? Kontakt os nu

Er din samarbejdspartner, leverandør eller kunde ramt af BEC?

Bliver du opmærksom på eller mistænker du, at en samarbejdspartner, leverandør eller kunde er ramt af et BEC-angreb? Og frygter du, at du er eller bliver involveret?

Hvis du mistænker, at en tredjepart er ramt af et BEC-angreb, fordi du har modtaget noget, som ser mistænkeligt ud, så anbefaler vi, at du gør følgende:

- Kontakt partneren eller kunden hurtigst muligt direkte f.eks. via telefon – brug andre kommunikationskanaler end e-mail.

- Kontakt din egen IT-afdeling/support for yderligere vejledning.

Vil du gerne **stå stærkere mod BEC-angreb** i fremtiden?

Så er forebyggelse og klare retningslinjer vejen mod mere sikkerhed.

Vil du høre, hvordan netop din organisation kan beskytte jer mod BEC-angreb? Eller har du andre spørgsmål relateret til Business E-mail Compromise eller andre cyberrelaterede emner? Så er er du altid velkommen til at række ud til os.

+45 6916 0004

information@itm8.com

itm8.dk/cyber-security

Today. Tomorrow. Together.

itm8®

Lad os bygge fremtidens IT. **Sammen.**

Kontakt os i dag

+45 6916 0004

information@itm8.com

www.itm8.dk