Velkommen til VELTEKs medlemswebinar

Vi gør opmærksom på, at webinaret bliver optaget med henblik på visning på VELTEKs hjemmeside bag medlemslogin.

HUSK at mute din mikrofon!

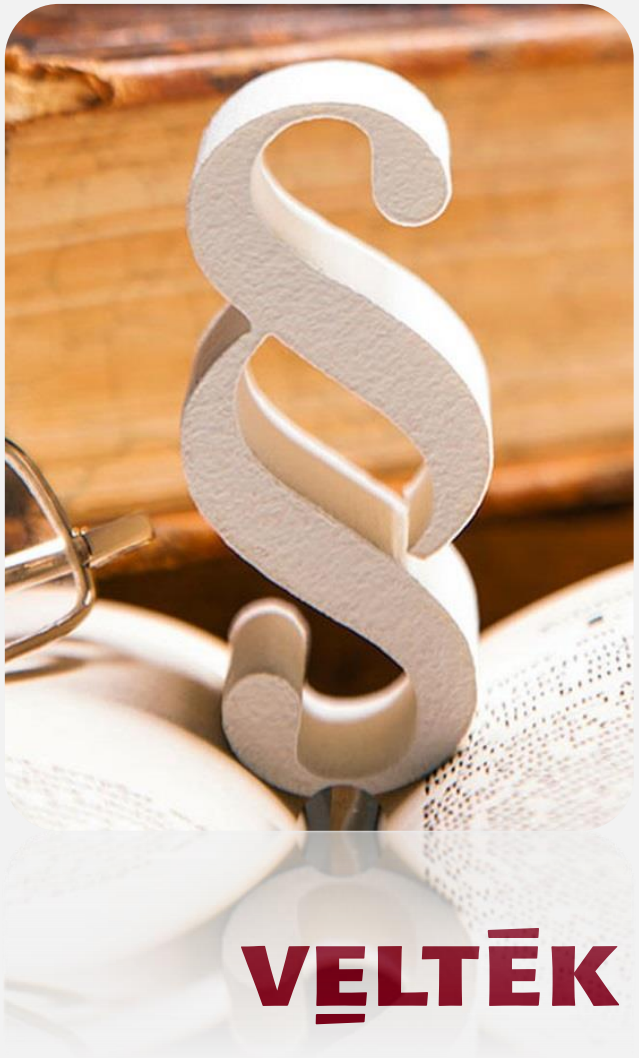
VELTĒK

VELTEKs compliance regler

Gennemgås og underskrives før alle møder

KONKURRENCELOV – TJEKLISTE TIL MØDER

DET MÅ DU IKKE:	DET MÅ DU GERNE:
Over for dine konkurrenter: **Du må ikke diskutere, afgive eller udveksle kommercielt følsomme oplysninger *med konkurrenter*, herunder for eksempel oplysninger om:** • ***Priser***, herunder individuelle prissætninger, påtænkte prisændringer, rabatter, godtgørelser, kreditvilkår etc. • ***Produktion og salg***, herunder individuelle virksomhedsplaner- og data vedr. produktion, omkostninger, kapacitet, lagerbeholdning, distribution, salgstal, markedsføringsstrategi, etc. • ***Transportsatser***, eksempelvis priser eller prispolitik for de enkelte forsendelser, herunder basing point systems, zone prices, fragt mv. • ***Markedsprocedurer***, herunder virksomhedens budstrategi ift. bestemte kontrakter, virksomhedens procedurer i udbudsprocesser, blacklistning eller boykot af kunder eller leverandører, oplysninger om sager der kan påvirke den forretningsmæssige adfærd overfor faktiske eller potentielle leverandører eller kunder, etc. **Over for dine forhandlere:** **Du må ikke direkte eller indirekte over for en *forhandler*:** • **Fastsætte *bindende videresalgspriser*** (herunder aftale faste videresalgspriser, mindste videresalgspriser eller giver rabatter mv. for at en forhandler fastholder en given pris). • **Forbyde *passivt salg***, dvs. eksempelvis at forbyde en forhandler at sælge til en kunde, der *uopfordret* henvender sig. • **Forbyde *generel reklame på internettet***, der er rimelig set i forhold til forhandlerens egne kundegrupper/-områder (betragtes som et forbud mod passivt salg).	**Sikre en striks håndtering inden for områder som:** ***Tilsyn / Supervision:*** Tilknyt en repræsentant på hvert møde. • Rådfør dig med passende ekspertise vedr. spørgsmål, der kan være relateret til konkurrenceloven. • Begræns drøftelser til emner på dagsordenen. • Udlever en kopi af denne tjekliste til alle mødedeltagere og hav en kopi til rådighed på alle møder. ***Journalføring:*** • Hav en agenda og et referat, der præcist afspejler de diskuterede emner. • Sørg for at passende personale gennemgår dagsordener, referater og andre vigtige dokumenter forud for udsendelse. • Beskrivelse af virksomhedens/koncernens formål, instanser og myndigheder. ***Agtpågivenhed:*** Ved emner til diskussion eller mødeaktiviteter der synes at overtræde denne tjekliste; bed om at dette stoppes, således at den korrekte retslige kontrol kan foretages evt. af en advokat, og træk dig fra denne diskussion eller aktivitet. Din indvending tages til referat over for deltagerne i et møde, hvor diskussioner synes at krænke denne tjekliste. Såfremt disse drøftelser fortsætter, så forlad mødet og få dette taget til referat. ***Uformel samling under større møder:*** • Vær særlig forsigtig såfremt konkurrencemæssige oplysninger udveksles i uformelle sammenkomster og tilknyttede møder før og efter møder i brancheforeningen. • Hvis konkurrencemæssige oplysninger diskuteres bør du tilkendegive din indsigelse, forlade samtalen og sikre beviser for din afstandtagen.



VELTĒK

CO WINS

CYBERFORSIKRING VED COWINS FORSIKRINGSMÆGLER

Hvad kan Cowins hjælpe med?

VELTEK AFTALE

- Indkøbe forsikringer på vores kunders vegne med adgang til en masse special forsikringsselskaber
- Virksomhedsbesøg og detaljeret gennemgang af alle forsikringspolicer og betingelser
- Udarbejdelse af rapport med Cowins' anbefalinger både på eksisterende og manglende forsikringer
- Rapporten leveres gratis til alle Veltek-medlemmer

CO'WINS

VELTĒK

CYBERFORSIKRING

Dækning

CYBER

- Cyberforsikringen dækker hackerangreb udført imod virksomheden
- Forsikringen dækker blandt andet omkostninger til IT-eksperter, reetablering af data og driftstab
- Der er krav om antivirusprogrammer, firewalls, kompleksitet af kodeord samt hyppighed for backup af data.

  Mange virksomheder lever ikke op til alle sikkerhedskrav i deres police, og risikerer at stå helt uden forsikringsdækning
- "Afledt drifstab" er ikke altid meddækket, men skal tilvælges. Dækningen er relevant for mange virksomheder, og dækker såfremt man får et driftstab grundet et cyberangreb hos en leverandør
- Bemærk at nogle af de klassiske forsikringsselskaber har en ret skrabet dækning i forhold til specialselskaberne. En billig cyberforsikring, kan ende med at koste virksomheden en formue

Typiske cyberangreb

CYBER

- Ransomware:
  Angreb hvor data og systemer tages som gidsel. Dette krypteres og gøres utilgængeligt og hackerne kræver en løsesum for at åbne igen

- Phishing:
  Angreb via e-mails og beskeder, der ikke er, hvad de udgiver sig for at være. Formålet er at få os til at videregive personlige oplysninger eller klikke på links til skadelige hjemmesider eller klikke på vedhæftede filer med skadeligt software

- DDoS-angreb:
  Angreb hvor hjemmesider udsættes for så meget trafik, at de ikke kan klare det og bliver utilgængelige. DDoS-angreb kaldes også overbelastningsangreb

CYBER

Fakta om Cyberangreb

- Hver fjerde modtager åbner phishing e-mails
- Antallet af anmeldte hackerangreb er steget med over 300 % siden 2010
- I ca. 60 % af hackerangreb er hackerne kun få minutter om at opnå systemadgang
- I en PwC undersøgelse af 300 virksomheder havde 69 % været udsat for et hackerangreb eller forsøg på hackerangreb.
  Flere vidste det ikke
- GDPR reglerne kræver at anmeldelse af databrud skal ske indenfor 72 timer
- Den generelle trusselsvurdering i Danmark for Cyberangreb vurderes "meget høj" ifølge Center for Cybersikkerhed
- Cyberangreb drevet via AI bliver mere udbredte og komplekse, og Institut for Cyber Risk spår at dette vil stige i løbet af 2024

Guldborgsund Komm
udsat for hackeran
kriminalitet

18.12.2023 13:15:00 CET | Guldborgsund Kommu

Del

DANMARK

Tusindvis af ku
hackerangreb

Dansk hostingselskab blev natten til fredag uds

Dansk ingeni
ramt af hacke

PLUS | Ransomware | 13. decem

DI: Truslen mod Danmark er på sit højeste i 84 år. Mange er for sårbare

Truslen mod Danmark har ikke været større siden Anden Verdenskrig, mener landets største erhvervsorganisation. Derfor opfordrer Dansk Industri nu alle virksomheder til at forberede sig bedre på krisesituationer.

peger på, at Danmark bør opruste it-sikkerheden.

Business

eb er eksploderet

Del artikel

Mest

onto – og kort efter blev

mme - formentlig russiske - hackerangreb, som brat lukkede det helt
e kommet ind ved at stjæle en ansats kodeord.

pe tager ansvaret for at
d: »Vi giver Danmark en
nd«

hjemmesider er søndag ramt af massive hackerangreb. Prorussisk

CYBER

Skadeseksempler

MÆRSK:
Angrebet ramte 27. juni 2017. Virussen kom ind via et angreb på deres software, og gik under navnet NotPetya. Den satte computere og software ud af drift. Mærsks containerhavne verden over stod stille, og mange kontorer kunne man end ikke ringe til. Mens skibene kunne sejle og navigere, var it-systemer ramt i en grad, så kunder ikke kunne få at vide, hvor deres fragt var.

Mærsk måtte lukke alle sine systemer ned. I 2017 var Mærsks containerskibsflåde på over 650 skibe, og selskabet håndterede 10,7 millioner 40-fodscontainere. Mærsks 74 havne håndterede gennemsnitligt flere end 10.000 containere om dagen.

Mærsk vurderede i sit halvårsregnskab, at hackerangrebet kostede selskabet 1,5 til 1,8 milliarder kroner.

OTICON:
Virksomheden Demant - der sælger høreapparater af mærket Oticon - blev ramt af hackerangreb 3. september 2019. Angrebet ramte selskabets servere og systemer og påvirkede både produktion og distribution. Ligeledes var alt virksomhedens interne kommunikation ramt.

Virksomheden måtte gendanne systemer og servere, og havde en nedetid på ca. 14 dage.

Hackerangrebet vurderes af Demant til at koste 750 mio. kr.

Skaden var dækket af Demants Cyberforsikring, som dog kun havde en dækningssum på 100 mio. kr.

CYBER

Skadeseksempler

EDC:
Ejendomsmæglerkæden EDC blev den 1. november 2023 ramt af et ransomware-angreb, hvor hackerne frigav kopier af pas, kørekort og sygesikringsbeviser for 1.300 personer online. Cirka 100.000 CPR-numre blev desuden offentliggjort. Hackergruppen fik fat på en backupfil som følge af en menneskelig fejl. Hackerne krævede en løsesum på ca. seks millioner dollars, men EDC betalte ikke løsesummen

NÆSTVED KOMMUNE:
Næstved Kommune meldte i juli 2022 ud, at kommunen var blevet svindlet for 277.000 kroner. En medarbejders kommunale mailkonto var blevet hacket og misbrugt til at sende falske fakturaer til en økonomimedarbejder i kommunen. Hackeren havde fået adgang til medarbejderens mail via en phishingmail sendt fra en lokal elektriker, som hackeren også havde kompromitteret. Medarbejderen havde tidligere haft kontakt til elektrikeren og mistænkte derfor ikke mailen for at være ondsindet.

EASY PARK:
I december 2023 blev parkeringsappen Easy Park angrebet, hvorefter kundedata blev lækket. Easy Park har meddelt, at det drejer sig om 'ikke-følsomme data', da der blev lækket informationer som e-mail, navn, adresse og telefonnummer, der har været tilknyttet kunderne i appen. På trods af at der ikke skulle have været lækket følsomme data, giver dette alligevel anledning til bekymring hos mange af Easy Parks kunder, hvilket illustrerer, at selv et 'mindre angreb' kan have indflydelse på forretningen og dens omdømme.

TJEK LISTE

CYBER

- <u>For lave dækningssummer</u>
  Mange virksomheder har utilstrækkelige dækningssummer

- <u>For lav selvrisiko</u>
  Det kan ofte godt betale sig at hæve selvrisikoen og hæve dækningssummen.

- <u>Risikobeskrivelse og aktiviteter</u>
  Ofte er forsikringsselskabets beskrivelse af de forsikrede aktiviteter ikke tilstrækkelig.

- <u>Klausuler</u>
  Policer indeholder ofte en hel del "med småt", der kan få stor betydning i en skadessituation.

- <u>Sikkerhedsforholdsregler</u>
  Der er krav om antivirusprogrammer, firewalls, kompleksitet af kodeord samt hyppighed for backup af data

SPØRGSMÅL

NIELS JØRGEN HASLEV
PROJEKTCHEF

NJH@COWINS.DK
TLF: 2753 8290

DANNIE SKOUV PEDERSEN
KUNDECHEF

DSP@COWINS.DK
TLF: 5455 6480