En håndbog i sikker IT-brug

NORLYS

Indhold
– genveje med et klik

Mange danske SMV'ere er sårbare, når det kommer til IT-kriminalitet

Hos Norlys gør vi meget ud af vores IT-sikkerhed, og vi er også underlagt krav og love inden for området, da Norlys ejer infrastrukturen til både fiber og strøm. Den viden, vi har, vil vi gerne dele med dig. Derfor giver vi dig i denne håndbog gode råd til, hvordan du bedst muligt kan sikre din virksomhed mod IT-kriminelle.

En stor del af de danske små og mellemstore virksomheder (SMV'er) er ifølge en undersøgelse foretaget for Erhvervsstyrelsen sårbare over for IT-sikkerhedsangreb. Dette skyldes blandt andet, at virksomhederne ikke har tilstrækkeligt fokus på virksomhedens IT-sikkerhedsniveau.

Over halvdelen af danske SMV'er vurderes at have et lavt IT-sikkerhedsniveau ifølge undersøgelsen. En hel del virksomheder har ikke implementeret de nødvendige IT-sikkerhedsforanstaltninger som fx systematiske og løbende opdateringer af firmaets IT-systemer, foranstaltninger som er helt centrale i forhold til at lukke sårbarheder. Hvordan ser det ud i din virksomhed?

Mange virksomheder har ikke fokus på IT-sikkerhed, selvom de er afhængige af IT-systemer og har/arbejder med følsomme data. Og dette på trods af at konsekvensen ved et læk af forretningskritiske data kan føre til, at virksomhederne mister deres forretningsgrundlag, hvis de IT-kriminelle fx lækker, sælger eller kopierer virksomhedens data. Antallet af IT-sikkerhedsbrud er stærkt stigende, og mange danske virksomheder har allerede oplevet sikkerhedsbrud.

En hurtig og stabil internetforbindelse er nødvendig for en virksomhed for at kunne følge med de digitale trends. Kunder er utålmodige og venter ikke på langsomme hjemmesider og webshops men finder hurtigt en alternativ hjemmeside. Med fibernet fra Norlys får du en lynhurtig og stabil internetforbindelse med hastighedsgaranti, så dine medarbejdere kan arbejde hurtigt og effektivt, og dine kunder komme sikkert til kassen.

God læselyst

Venlig hilsen
Norlys erhverv

IT-sikkerhed starter hos medarbejderen

Har din virksomhed sikkerhedsforanstaltninger, der skal beskytte IT-udstyr og systemer mod hackerangreb, phishing og andre trusler? Formentligt, men sikkerhedsforanstaltningerne kan ikke stå alene, og trusselbilledet ændrer sig hele tiden i takt med, at de IT-kriminelle bliver dygtigere og dygtigere. Derfor er det i sidste ende medarbejdere, der er det stærkeste værn mod udefrakommende trusler.

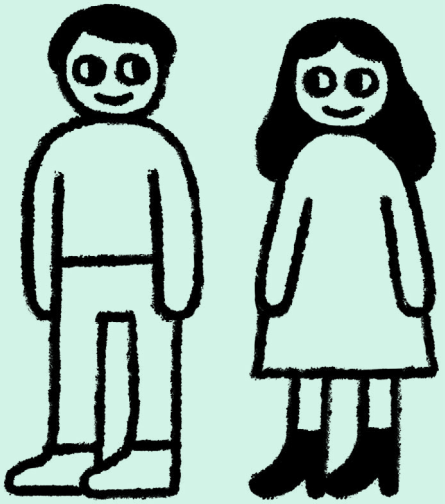
Som medarbejder er det vigtigt, at du altid har din sunde fornuft og kritiske sans med dig. Det betyder blandt andet:

- at din computer altid skal låses, når du forlader din plads.
- at du skal have en naturlig skepsis over for mistænkelige mails – hold øje med afsenderadressen, stavefejl og links.
- at du aldrig må klikke på et link, hvis du er i tvivl, men spørg en kollega fra IT.

Overvej hvor du sidder med din pc i det offentlige rum. Ser dine medpassagerer i toget eller menneskerne ved bordet bag dig på caféen, at du taster dit password? Gør de det, har du foræret dem adgang til dine programmer, e-mails og mapper på din pc.

Hvad gør du, når du er blevet hacket?

Har din virksomhed en procedure for, hvordan du og dine kollegaer skal handle, hvis I bliver hacket? Er du blevet hacket, skal du som det første **slå internettet fra** for at undgå spredning og derefter kontakte enten din IT-leverandør eller IT-sikkerhedsleverandør. Din leverandør vil herefter guide dig til, hvad du nu skal gøre.



Forskellige værktøjer IT-kriminelle bruger for at tilgå din computer

Bruger du også internettet til mange af dine arbejdsopgaver? I den moderne verden, hvor meget foregår digitalt, er vi alle nødt til at forholde os til IT-kriminalitet.

IT-kriminelle forsøger på forskellige måder at tilegne sig oplysninger eller ødelægge programmer. Herunder er forskellige typer trusler, du som virksomhed ikke ønsker at komme i nærkontakt med:

1. **Virus** er et lille computerprogram, som sammen med computeren og styresystemet kopierer sig selv ved at inficere filer uden din viden. En virus lægger sig typisk i starten af et eksisterende program, så den afvikles, inden det reelle program foretager sig noget. En virus kan ikke fungere alene. Virussen kan fx ødelægge vigtige filer samt holde sig i baggrunden og stjæle dine adgangskoder.

2. **Phishing** er en form for svindel, hvor IT-kriminelle forsøger at narre dig til at give dem fortrolige oplysninger som fx adgangskoder. Den typiske phishing-svindel foregår i to faser: E-mail og hjemmeside. Du modtager en e-mail, der ser ud til at komme fra nogen, du har tillid til (fx Skat eller din bank), som beder dig oplyse/bekræfte informationer på en falsk hjemmeside, som de linker til i e-mailen. Sender du de ønskede oplysninger, har de IT-kriminelle modtaget oplysningerne med henblik på at misbruge dem.

3. **Ransomware** er et ondsindet stykke kode, som låser din computer og forhindrer dig i at tilgå den, indtil du har betalt en løsesum. Bliver du ramt, krypteres dine filer og/eller dit operativsystem samt koden kan stoppe applikationer som fx din web browser i at virke. Du kan altså ikke tilgå programmer, dokumenter, billeder og lignende på din computer, mobil eller tablet. Som virksomhed kan det betyde et produktionstab og dermed en økonomisk krise. Medarbejdernes data vil gå tabt, og de vil ikke kunne fortsætte deres arbejde. Spredning af ransomware sker

oftest gennem e-mails med falske links. Når brugeren trykker på linket, omdirigeres de til en falsk webside, hvor de skal downloade noget software. Gør brugeren det, bliver hendes/hans computer inficeret, og virussen finder vej ind i computeren via smuthuller, hvis brugerens programmer fx ikke er opdaterede.

De IT-kriminelle går konsekvent efter virksomheder, og det er der en god grund til. Mange virksomheder fristes nemlig til at betale en løsesum for at få deres data dekrypteret, fx fordi deres backup ikke er opdateret. Løsesummen lander direkte i de IT-kriminelles lommer. Ved at betale løsesummen får de IT-kriminelle et incitament til at fortsætte kriminaliteten, og du ved ikke, om du reelt set får dit data tilbage, når du har betalt.

4. **Et DDoS-angreb** (Distributed Denial of Service) er, når IT-kriminelle sender store mængder af trafik til en bestemt IP-adresse – fx et website eller et netværk. Det kan websitets infrastruktur typisk ikke håndtere, og det betyder, at sitet bliver meget langsomt eller går helt ned. Konsekvensen er derfor, at virksomhedens kunder, samarbejdspartnere og andre reelle besøgende må gå forgæves.

DDoS er i praksis et overbelastningsangreb. Her bruger IT-kriminelle en gruppe af computere (kaldet et botnet), som de IT-kriminelle har inficeret med malware eller trojanske heste til at kontakte den udvalgte hjemmeside. Typisk ved de personer ikke, hvis computere er blevet en del af botnettet, at deres computere er inficeret og bruges til DDoS-angreb. Ofte vil den eneste mærkbare forskel være, at deres computer er lidt langsommere end normalt.

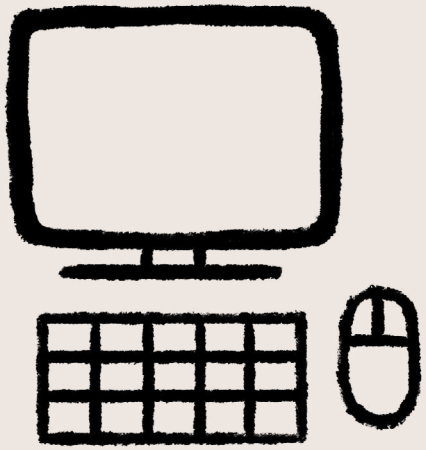
Hvad bruges DDoS-angreb til og hvorfor? DDoS-angreb bliver ofte brugt til en af tre ting:

- Til at skade virksomheder eller konkurrenter.
- Til hacktivisme, det vil sige til at skabe opmærksomhed om en bestemt mærkesag.
- Til afpresning.

Årsagen, til at stadig flere virksomheder rammes af DDoS-angreb, er blandt andet, at det ikke kræver stor teknisk viden at foretage den type angreb, da det kan købes på internettet til forholdsvis små penge. DDoS-angreb kræver dog store ressourcer i form af computerkapacitet fra angriberen, derfor er et angreb ofte relativt tidsbegrænset.

5. **CEO fraud** (direktørsvindel) er når IT-kriminelle udgiver sig for at være chefen i en virksomhed og beder en ansat om at betale en regning enten med kort varsel eller tys tys. De IT-kriminelle har typisk på forhånd hacket sig ind på direktørens e-mailkonto for at lære direktørens sprogbrug og interesser at kende, så deres e-mail til medarbejderen virker meget troværdig. Det er typisk den mindre virksomhed, der bliver ramt af CEO fraud, da de ofte ikke har processer omkring betalinger og overførsler.

   For at undgå CEO fraud bør du som medarbejder altid ringe til chefen, inden du overfører penge. Du bør også have klare procedurer for pengeoverførsler, som fx at der altid skal være to medarbejdere, der godkender en overførsel over et bestemt beløb.



Kender du de anbefalede retningslinjer omkring adgangskoder?

Vi har alle mange steder, hvor vi skal bruge adgangskoder for at logge ind både arbejdsmæssigt og privat. Den nemme løsning er at bruge den samme adgangskode eller én arbejdsmæssigt og én til private adgange. Men det er kun en fordel for IT-kriminelle, hvis uheldet er ude, så det bør du undlade.

Adgangskoder til IT-systemer og -enheder skal behandles fortroligt og må ikke deles med andre – heller ikke dine kolleger. Der kan dog i visse arbejdssituationer være behov for, at flere personer deler et brugernavn og en adgangskode.

Vil du have en stærk adgangskode, kan du følge nedenstående retningslinjer

Din adgangskode:

- Skal være minimum 10 karakterer langt.
- Skal indeholde både tal, store og små bogstaver samt gerne et specialtegn.
- Udløber efter 100 dage.

Husk:

- Brug ikke ord fra ordbogen. Ord fra ordbogen bør kombineres med andre tegn, hvis de skal indgå i din adgangskode.
- Genbrug aldrig adgangskoder men brug en unik adgangskode for hver af dine konti.
- Brug evt. flere sikkerheds-faktorer som fx engangkode over SMS.

Vælg originale adgangskoder og undgå at anvende samme brugernavn/adgangskode til eksterne adgange, som du bruger internt. Har du mistanke om, at andre har kendskab til din adgangs-

kode, bør du straks ændre den og orientere den IT-ansvarlige.

3 gode råd til, hvordan du opretter unikke adgangskoder

• Brug en sætning, hvor hvert ord starter med et bogstav i et navn på en, du kender og kan huske.
(Fx 1Mandmaledealdrig = Emma).

• Brug forbogstaverne i en sætning, du kan huske.
(Fx Db1bpN = "Der bor i en by på Nørregade").

• Lad hånden gå på tastaturet, og lav en kombination af bogstaver/ tal og tegn, der er naturligt for dig. Således "husker" dine hænder koden for dig. Det er dog en god idé også at lære koden udenad.

Er din e-mail adresse lækket?

Ved du, om din e-mailadresse er blevet lækket i forbindelse med et større sikkerhedsbrud hos leverandører som LinkedIn og Facebook? Tjek det på haveibeenpwned.com

Vidste du, at du kan gemme og generere sikre passwords via en Password Manager? Password Managere findes som app til både Android og IOS og opbevarer dine passwords sikkert. Du skal så kun huske ét password: det til Password Manageren.

Hvor sikkert er dit password?

Tjek det på howsecureismypassword.net

Er der retningslinjer omkring brug af sociale medier i din virksomhed?

Sociale medier er en integreret del af de fleste menneskers liv, og du bør altid tænke over, hvad du skriver og deler via sociale medier – både for din egen skyld men også for din virksomheds. Vær derfor varsom med, hvad du skriver om din arbejdsplads, din leder og kolleger, og tag højde for din virksomheds interesser og værdier.

Deltager du i en debat med din personlige profil, hvor du bruger din faglige viden, er det vigtigt at du tydeligt viser, at du udtaler dig som privatperson og ikke på vegne af din virksomhed. Du skal naturligvis altid overholde eventuelle tavshedspligter og ikke videregive følsomme data, også her er du omfattet af loyalitets-pligten over for din virksomhed.

Uanset om der er retningslinjer i din virksomhed eller ej, bør du altid forholde dig kritisk og bruge din sunde fornuft, når du er online på de sociale medier. Dine profiler på de sociale medier indeholder oplysninger, som kan være af høj interesse for IT-kriminelle. Får de fat i dit login til fx din private eller virksomheds Facebook eller e-mail, kan de sende beskeder fra din eller din virksomheds profil med inficerede links, der kan slippe en virus løs hos modtageren, hvis denne klikker på linket. Dette kaldes konto-hijacking og er en form for identitetstyveri, hvor de IT-kriminelle vil bruge de stjålne informationer til ulovlige formål.

Sådan forebygger du, at IT-kriminelle får adgang til din computer

Vil du undgå, at IT-kriminelle får adgang til dine data kræver det blot, at du forbereder dig, inden ulykken sker. Her er et par gode råd, du bør forholde dig til:

- Hav altid en nylig backup af alt din virksomheds data på en separat lokation.
- Åbn aldrig vedhæftninger fra uautoriserede e-mails.
- Informér dine kollegaer. Manglende viden er nemlig én af de største årsager til, at virksomheder bliver smittet.
- Hold al din software opdateret (ikke kun din Microsoft desktop).
- Forhold dig skeptisk til e-mails og websteder, der beder om følsomme oplysninger om dig.
- Hvis du er i tvivl om ægtheden af en e-mail eller webside, så kontakt afsenderen.
- Tjek at links til sider med fortrolig information begynder med https.
- Undgå at klikke på links i e-mails. Indtast i stedet selv web-adressen. Prøv eventuelt at holde musen over links for at se, hvor de peger hen. SKAT-dk, SKAT.nu eller SKAT.eu er eksempler på falske URL's.
- Vær opmærksom på stavefejl. Der sniger sig ofte stavefejl og haltende formuleringer ind i falske mails, selvom mange IT-kriminelle er blevet bedre til at undgå stavefejl og uheldige vendinger.
- Hvis du bruger cloud-løsninger, bør du sikre, at dine data i skyen er sikret via en back-up løsning.

SKAT, banker og andre myndigheder vil aldrig bede dig om personlige oplysninger, koder, kontooplysninger m.m. per mail eller telefon.

Ved du, hvordan du bør håndtere fortrolige og følsomme oplysninger?

Nedenfor har vi samlet en række gode råd til, hvordan du håndterer persondata og fortrolige oplysninger i dagligdagen. Brug generelt altid din sunde fornuft og vær ekstra varsom, hver gang du har med en personoplysning at gøre.

Deling og videregivelse af personoplysninger

Undgå at dele personoplysninger med kolleger, der ikke har et formål med oplysningerne. Undgå også at dele personfølsomme oplysninger med andre end den person, oplysningerne omhandler, medmindre personen har givet skriftligt samtykke til det. Personfølsomme oplysninger omfatter bl.a. oplysninger om helbred, racemæssig eller etnisk baggrund, politisk eller religiøs overbevisning.

E-mails og persondata

Har du behov for at sende personoplysninger til eksterne på e-mail, så bed dem slette e-mailen, når de er færdige med at bruge den. E-mails, der sendes til eksterne, er ikke altid krypterede og kan muligvis blive læst af uvedkommende. Du bør kun sende følsomme og fortrolige oplysninger over e-mail, hvis de er krypterede.

Skype, Messenger, Facebook etc.

Undgå at dele personoplysninger via Skype og andre tilsvarende programmer, hvor du kan kommunikere via internettet, da samtalehistorikken kan blive gemt automatisk.

Print

Overvej altid om det er nødvendigt at printe dit dokument med personoplysninger ud. Skal dokumentet printes, bør du stille dig ved printeren, når du printer og tag altid alle papirer med dig.

Generelt bør du ikke lade dokumenter med personoplysninger ligge frit tilgængelige på skriveborde (både pc og på kontoret), ved printere og lignende.

Gode råd
- kort og godt

1. Tænk før du klikker
2. Hold dine programmer og systemer opdateret
3. Lås din pc, når du forlader den
4. Pas på med at dele personoplysninger
5. Hold dine adgangskoder hemmelige
6. Lån ikke din pc ud
7. Skift jævnligt din adgangskode
8. Brug din sunde fornuft
9. Hold en god tone på de sociale medier
10. Tag fat i din IT-ansvarlige, hvis du oplever noget mistænkeligt

Hurtigt og stabilt internet er livsnerven i mange virksomheder. Gælder det også hos dig?

Vi håber, at du er blevet klogere omkring sikker brug på internettet og at du kan bruge nogle af de gode råd til at forbedre IT-sikkerheden i din virksomhed.

Har din virksomhed brug for en hurtig og stabil internetforbindelse, er fibernet fra Norlys en oplagt mulighed. En hurtig fiberforbindelse hjælper dig med holde dine programmer opdaterede uden at det påvirker den daglige drift. Samtidig kan du lynhurtigt up- og downloade tunge filer og arbejde i skyen, uden at det påvirker hastigheden for hverken dig eller dine kollegaer.

Kontakt os for at høre mere om vores forskellige erhvervsløsninger og hør, om vi kan levere fiber til din virksomheds adresse.

Vi ser frem til at høre fra dig.

Jeanette G. Warming
jeawar@norlys.dk

Brian Bech Hjarsen
brbhj@norlys.dk

Jakob Larsen Dalsgaard
jacdal@norlys.dk

Kildehenvisninger

Til denne håndbog har vi, udover at benytte os af vores interne viden, også fundet viden på forskellige relevante hjemmesider, blandt andet nedenstående:

www.klikikkeher.dk

www.erhvervsstyrelsen.dk

www.digitalsikkerhed.dk

www.datatilsynet.dk

www.it-borger.dk

www.it-blogger.dk

www.markedsforing.dk

www.smvdanmark.dk