

Sikkerhedshåndbog

3.2. Brugervejledning til låneformidlere

Tilslutning via Internettet

Det er e-nettet A/S mål, at e-nettet på alle områder skal betragtes som et sikkert og pålideligt system med et højt niveau af sikkerhed.

e-nettet bygger på en vifte af anerkendte teknikker og principper for sikkerhed – blandt andet benyttes stærk kryptering til sikring af oplysninger, der via Internettet sendes til og fra e-nettet. Derfor kan du trygt benytte e-nettet.

Som ansvarlig part på e-nettet skal du og de medarbejdere, du autoriserer til at benytte e-nettet, kende og følge denne sikkerhedsvejledning.

Sikkerhedsprincipper

Din adgang til e-nettet bygger på følgende generelle sikkerhedsprincipper:

- Dit bruger-ID og din adgangskode er fortrolig og identificerer dig som bruger af e-nettet
- Oplysninger, der sendes til og fra e-nettet, er hemmeligholdt, således at uvedkommende ikke kan læse disse
- Oplysninger, der sendes til og fra e-nettet er sikret mod at kunne blive ændret af uvedkommende

Disse principper giver et højt sikkerhedsniveau, som medvirker til, at din anvendelse af e-nettet kan ske sikkert og betryggende.

Det forholder sig dog sådan, at anvendelse af Internettet generelt kan påvirke sikkerheden i alle dine systemer, herunder din adgang til e-nettet. Ved anvendelse af e-nettet, skal du derfor følge de normale sikkerhedsregler for sikker anvendelse af Internet og e-post, som der forklares om senere i denne sikkerhedsbeskrivelse.

Det høje sikkerhedsniveau bygger også på din aktive medvirken og årvågenhed.

Sådan autoriserer du dine medarbejdere

Som ansvarlig bruger på e-nettet modtager du et bruger-id og en tilhørende opstartskode.

Har du mistanke om, at opstartskoden er kommet i forkerte hænder, eller at brevet ser ud til at have været åbnet, kan du spærre din adgang til e-nettet ved at taste din kode forkert 3 gange. e-nettet kan også spærre din adgang ved at du udfylder kontaktformularen 'Kontakt os' på www.e-nettet.dk eller på telefon 33 73 04 44 indenfor den almindelige kontortid.

Du skifter ved første logon til e-nettet opstartskoden til den adgangskode, du og dine medarbejdere fremover ønsker at anvende.

Det er vigtigt at vælge adgangskoden med omhu:

- Din adgangskode skal være på minimum 8 tegn og maksimalt 15 tegn, og skal bestå af

Sikkerhedshåndbog

en kombination af store og små bogstaver og tal.

- Undgå derfor at anvende navne eller andre værdier, som er lette at gætte.
- Vælg en kode der er let at huske, men svær at gætte for andre. Det kan for eksempel være første bogstav fra hvert ord i titlen på en sang, en linje skrevet af din yndlingsforfatter eller anden sætning, som du særligt kender.
- Videregiv brugerid og adgangskode til de medarbejdere, du ønsker at autorisere til at anvende e-nettet. Hvis en medarbejder med kendskab til adgangskoden forlader jobbet, skal du skifte adgangskoden.

Vælg adgangskoden omhyggeligt - som ansvarlig bruger er du ansvarlig for, at kun de medarbejdere, du autoriserer til at anvende e-nettet, anvender adgangen.

Når du og dine medarbejdere anvender e-nettet

For sikker anvendelse af e-nettet skal du og dine medarbejdere:

- sørge for at uvedkommende ikke ser adgangskoden, når den indtastes
- undgå at sende underskriftskodeordet i en e-post
- altid logge af e-nettet eller låse skærmen på computeren inden PC'en forlades
- sikre PC'en med adgangskontrol (f.eks. opstartskodeord og skærmlås)
- altid straks bede e-nettet om at spærre for adgang ved *enhver* mistanke om, at uvedkommende har fået viden om brugerid og adgangskode. Husk, at orientere dine kolleger.
- skifte adgangskoden minimum hver 2. måned, men du kan til enhver tid ændre adgangskoden ved behov. Husk, at skiftet skal koordineres med dine kolleger

Det er vigtigt at holde adgangskoden hemmelig. Notér aldrig adgangskoden ned.

Spør altid adgangen til e-nettet ved mistanke om misbrug.

Når du og dine medarbejdere anvender Internettet eller e-post

For bedst muligt at sikre adgangen til e-nettet skal der iagttages en række sikkerhedsforanstaltninger når Internettet eller e-post anvendes fra samme udstyr, der benyttes som adgang til e-nettet.

Det er et generelt sikkerhedsproblem, at programmer, der hentes fra Internettet, kan have virus eller anden skadelig kode. For at imødegå problemer er det derfor vigtigt, at du kun henter eller modtager programmer via browser eller e-post, hvor du kan være sikker på udbyderens eller afsenderens identitet og seriøsitet. Det kan være svært at afgøre, men det er en god rettesnor at holde sig til kendte udbydere og leverandører på Internettet.

På visse hjemmesider tilbydes du automatisk programmer til installation på din computer, hvis du ikke selv har bedt om et program, så sig altid nej til at installere disse programmer.

Sikkerhedshåndbog

E-nettet understøtter Microsoft Internet Explorer fra version 6.0 – der kan indstilles til at sikre, at der ikke uden din accept modtages programmer med adgang til din pc - f.eks. ActiveX komponenter eller Java applets (om ActiveX og Java se under: Ofte stillede spørgsmål). Af hensyn til din egen beskyttelse anbefaler vi dig altid at anvende sådanne indstillinger.

”Smart phones” er en computer og skal holdes opdateret ligesom en almindelig computer.

Du bør desuden foretage viruskontrol med et opdateret antivirusprogram med jævne mellemrum og altid ved installation/indlæsning af programmer, uanset om det er fra CD-ROM, e-mail eller Internet.

Ligeledes bør du sikre dig, at den software, du anvender til Internetadgang, til stadighed er opdateret med de seneste sikkerhedsmæssige opdateringer. På de store software-leverandørers hjemmesider kan du få informationer om rettelser til deres programmer. Hvis du benytter Windows kan du installere et auto-update program, der sikrer, at du automatisk henter og installerer de seneste opdateringer. Du kan alternativt hver måned kontrollere, om der ligger nye opdateringer klar til dit operativsystem, på adressen: windowsupdate.microsoft.com
Det anbefales at konfigurere operativsystemet til automatisk at hente opdateringer.

Vi vil foreslå, at du beskytter dit IT-miljø bedst muligt mod risikoen for angreb fra Internettet. Med anvendelse af en dedikeret firewall til netværket, samt sikkerhedspakke minimum bestående af applikationsfirewall og anti-virus på den enkelte brugers pc.

Forholdsregler ved Internet anvendelse:

- *Vær sikker på at sikkerhedsniveauet i din browser er sat korrekt*
- *Undgå generelt at indlæse programmer fra kilder du ikke har tillid til*
- *Anvend altid virusbeskyttelse*
- *Sørg for, at din software er opdateret*
- Beskyt dit IT-miljø med brug af firewalls
- Undgå at besøge ondsindet websider
- Kontrollere at URL'en matcher SSL certifikatet der vises i statusbaren nederst i browseren

Ofte stillede spørgsmål

Nedenfor kan du finde forskellige spørgsmål (med tilhørende svar), som kan opstå under brugen af e-nettet.

1. Den første logon

Hvad sker der ved den første logon?

Efter at have returneret "Tilslutningsaftalen" vil du efterfølgende modtage et brev med en opstartskode, der skal bruges ved første logon. Brevet skal opbevares betryggende, sådan at opstartskoden ikke kommer i forkerte hænder, inden du har anvendt den. Brevet indeholder endvidere en sikkerhedskode, der kan anvendes i forbindelse med situation 2, 3, og 4, se nedenfor.

Sikkerhedshåndbog

2. Glemmt adgangskode

Hvad gør jeg ved glemmt adgangskode?

e-nettet A/S har ingen mulighed for at oplyse en adgangskode. Du kan dog altid bede e-nettet om at blive igangsat ved at udfylde kontaktformularen 'Kontakt os' på www.e-nettet.dk, der herefter af sikkerhedsmæssige hensyn vil faxe en ny opstartskode såfremt sikkerhedskoden ikke kan oplyses. Bemærk, at der kun vil blive faxet tilbage til det faxnummer, som på forhånd er registreret i e-nettet A/S.

Det nye kodeord skal skiftes ved første login.

3. Forkert adgangskode

Hvad sker der, hvis jeg bruger forkert adgangskode?

Bruges der forkert adgangskode flere gange i træk, spærres din adgang til e-nettet. Adgangen spærres også, dersom du ved skift af adgangskode indtaster den gamle adgangskode forkert flere gange. e-nettet A/S har ingen mulighed for at oplyse en adgangskode. Du kan dog altid bede e-nettet om at blive igangsat ved at udfylde kontaktformularen 'Kontakt os' på www.e-nettet.dk. Såfremt sikkerhedskoden ikke kan oplyses, vil e-nettet af sikkerhedsmæssige årsager faxe en ny opstartskode. Bemærk, at der kun vil blive faxet tilbage til det faxnummer, som på forhånd er registreret i e-nettet A/S.

Det nye kodeord skal skiftes ved første login.

4. Spærring

Hvordan spærrer jeg min adgang til e-nettet?

Du kan selv spærre din adgang til e-nettet ved at taste din kode forkert 3 gange. e-nettet kan også spærre din adgang ved at du udfylder kontaktformularen 'Kontakt os' på www.e-nettet.dk eller på telefon 33 73 04 44, indenfor den almindelige kontortid.

5. Virus beskyttelse

Hvordan sikrer jeg mig mod virusangreb?

Du bør benytte et effektivt og opdateret antivirus program på din maskine. Konfigurer dit antivirus program til automatisk at opdaterer dagligt, samt at foretage en automatisk fuld scanning af din maskine, minimum en gang hver måned.

Der bør generelt kun installeres software fra kendte parter, som kan anses for at være troværdige, og hvor ægthed og oprindelse kendes. Husk som udgangspunkt at hvis du er i tvivl, er det bedre ikke at installere et program eller åbne en e-mail.

Hvis du er i tvivl om en e-mail med en vedhæftet fil kan indeholde virus, så kontakt afsender for verifikation eller slet beskeden uden at åbne den.

6. ActiveX Komponenter & Java applets

Hvad er ActiveX komponenter og Java applets?

ActiveX og Java applets er små programmer der kan afvikles på din computer. Både ActiveX og Java kan indeholde kode, der hvis den aktiveres, giver fuld adgang til dit system. Både Active

Sikkerhedshåndbog

X og Java kan benytte sig af elektroniske signaturer. En elektronisk signatur verificerer, hvem der har fremstillet koden du downloader og aktiverer. Vær opmærksom på at en elektronisk signatur ikke garanterer, at filen er fri for virus, men kun giver dig sikkerhed for hvem filen kommer fra. Det er derfor vigtigt, at du kun accepterer ActiveX komponenter eller Java applets fra software leverandører eller hjemmesider du stoler på.

ActiveX komponenter eller Java applets anvendes ikke af e-nettet, men kan altså alligevel udgøre en sikkerhedsmæssig risiko, dersom ActiveX komponenter eller Java applets indlæst under din øvrige anvendelse af Internettet viser sig at indeholde kode, der kan skade din computer og dermed din Realkreditnet adgang.

Både Internet Explorer og Netscape kan konfigureres, så de kun giver mulighed for at aktivere ActiveX eller Java, hvis de er elektronisk signerede. Den digitale signatur på ActiveX komponenten eller Java appletten sikrer yderligere, at koden ikke er ændret, siden den elektroniske signatur blev dannet. Dermed sikres, at den downloadede kode kun kan stamme fra den virksomhed, som har afgivet den elektroniske signatur.

7. Trådløse netværk

Må jeg benytte trådløst netværk sammen med e-nettet?

Flere benytter i dag trådløs teknologi, og der er flere ting du skal være opmærksom på hvis du benytter et trådløst netværk sammen med e-nettet.

Det er vigtigt, at benytte den indbyggede WPA eller WPA2 til kryptering af dit trådløse netværk. M.h.t. WPA2 skal det sikres at hardwaren supporterer dette. Vejledning for hvordan du sikrer, at WPA eller WPA2 krypteringen er aktiveret fås fra din forhandler, eller via den dokumentation der følger med det produkt, du har anskaffet. Hvis du ikke aktiverer WPA eller WPA2 krypteringen, er der risiko for dit trådløse net kan misbruges af andre end de tiltænkte brugere, og det kan teoretisk set aflyttes.

Anvender man WPA-PSK (Pre-Shared Key), er anbefalingen at man benytter mindst 20 karakterer som fælles kode, og de skal indeholde både specielle karakterer, såvel store og små bogstaver og cifre. Den mest sikre er WPA2 med CCMP i øjeblikket, idet nogle mindre svagheder i TKIP fornyeligt har vist sig.

Husk signalet fra din trådløse sender/modtager rækker langt ud over den lokation du benytter det fra. Den optimale løsning er derfor, hvis du både krypterer netværket og sikrer dine klientmaskiner med en software firewall. Derudover må SSID'en (Service Set Identifier - navnet på en basisstation) fra det trådløse netværk ikke indeholder referencer til din virksomhed. Vejledning for hvordan du sikrer, at SSID'en er korrekt konfigureret fås fra din forhandler, eller via den dokumentation der følger med det produkt, du har anskaffet.

Sørg også for at ændre eventuelle default passwords på din basisstation. Hvis dit trådløse netværk leveres med default brugere, som eks. en administrator konto, er det vigtigt at huske at ændre passwordet for denne konto. Benyt et stærkt password, på minimum 8 karakterer, med kombineret brug af store og små bogstaver og tal.