TJEKLISTE

6 TJEK TIL IT-CHEFEN

IT-sikkerhed på hjemmearbejdspladsen

Sådan sikrer du virksomhedens systemer, når medarbejderne arbejder hjemmefra.

CapaSystems
...because time matters

TJEKLISTE

Med hjemmearbejdspladserne er der opstået et hidtil ukendt land af risici, når vi taler om IT-sikkerhed. Vi er nemlig slet ikke vant til at håndtere – og huske – IT-sikkerheden, når vi sidder i hjemmets trygge rammer med en kop filterkaffe i hånden og havedøren på klem.

Derfor må du som IT-chef være ekstraopmærksom på din rolle og tage nogle ekstra sikkerhedsmæssige forbehold for at holde ubudne gæster ude af jeres IT-systemer.

Følg denne tjekliste, og få styr på IT-sikkerheden på hjemmearbejdspladsen.

- [ ] **Indkøb bærbare arbejdscomputere til alle medarbejdere**

  Sørg for at alle medarbejdere, der ønsker at arbejde hjemmefra, er udstyret med bærbare arbejdscomputere og arbejdstelefoner. Lader du folk arbejde fra private enheder, mister du kontrollen med software-versioner og Firewall-instillinger.

- [ ] **Installér lynhurtig VPN på alle maskiner**

  Bare fordi dine kolleger sidder i sofaen, bliver deres tålmodighed med systemerne ikke større. Sørg derfor for ultrahurtige VPN-forbindelser, så medarbejderne ikke fristes af fx WeTransfer eller Facebook Messenger til fildeling og kommunikation.

- [ ] **Minimér login-risikoen med 2FA og unikke kodeord**

  Antallet af logins stiger, når medarbejderne arbejder hjemmefra – både til virksomhedens systemer og til private tjenester. Sørg derfor for at anvende 2-faktor-autorisation og påtving allerhelst forskellige koder til forskellige tjenester. Så kan ét kodeord ikke åbne dørene til alle jeres systemer, og risikoen for et full blown hackerangreb falder betragteligt.

CapaSystems
...because time matters

TJEKLISTE

Kommunikér problemet med børns adgang til maskinerne

Når arbejdscomputeren alligevel står på bordet, er det bare nemmest at bruge den, når børnene skal underholdes med Gurli Gris på YouTube. Men børn tænker næppe over, hvilke links de klikker på. Kommunikér problemet til dine kolleger, og om nødvendigt kan du analysere aktiviteten på fx YouTube for at identificere overdreven brug.

Opsæt ekstra sikkerhedsforanstaltninger i krise

Hackere holder ikke Corona-fri. Tværtimod bliver kriser ofte brugt som madding i ondsindede phishing-kampagner. Det kan være phishing-mails forklædt som beskeder fra myndighederne eller NGO'ere. Dine kolleger vil være ekstra tilbøjelige til at hoppe i fælden, når der er krise, så du må være ekstra dygtigt til at forhåndssortere den elektroniske post for dem.

Analysér netværksaktivitet og service levels

Når medarbejderne sidder på distancen, er det sværere for dig at holde fingeren på pulsen og opsnappe problemer med jeres IT-systemer. Folk er simpelthen ikke lige så hurtige til at reagere og informere om problemerne.

Derfor må du selv sørge for, at holde øje med netværksaktiviteten, så I ikke udfordrer kapasiteten og systemernes hastighed. Hold øje med, hvilke requests der foretages, og hold overblik over, om jeres IT-leverandører lever op til de service-level agreements, I har indgået.

Skal vi også kigge på dit IT-system? Kontakt os i dag.

+45 70 10 70 55

sales@capasystems.com

CapaSystems A/S
Roskildevej 342C
DK-2630 Taastrup

CapaSystems
...because time matters