UNDGÅ AT BLIVE HACKET

HVORFOR ER IT-SIKKERHED VIGTIGT FOR DIN VIRKSOMHED?

Forestil dig, at du møder ind en morgen på din arbejdsplads – og alt er kaos. Ingen produktion, ingen aktivitet, PC`erne virker ikke, kunder ringer og skælder ud, ordrer er forsvundet ud i den blå luft, og folk kan ikke forstå, at de ikke kan få hjælp og få svar på spørgsmål. Og medarbejderne? De er stærkt forvirrede og prøver febrilsk at få tingene til at køre igen. Imens siver kunderne væk.

KORT SAGT:

ALT er kaos, og lynhurtigt kan situationen udvikle sig fare-truende for virksomheden, både på kort og længere sigt.

Et sådant kaos kan opstå, hvis din virksomhed bliver hacket eller på anden vis udsættes for avanceret IT-kriminalitet.

Sammenlign det med, at virksomheden er brændt ned til grunden i nattens løb. Tænk at møde ind om morgenen, og virksomhedens produktion og kontorer ikke længere eksisterer. Så er det du oplever at stå alene. I kaos ved du ikke, hvordan du kommer videre.

Men du kan faktisk gøre meget for at undgå kaos. Du kan forebygge og tage initiativer på it-området, som minimerer risikoen for, at kaos IKKE opstår.

På bagsiden er samlet 10 gode råd. Følger du dem, kan du sove roligt om natten.

Se mere på bagsiden ▶

HVAD KAN DU UMIDDELBART GØRE FOR AT BESKYTTE DIN VIRKSOMHED?

Du anbefales følgende 10 handlinger for at sikre en høj grad af IT-sikkerhed:

1 HOLD IT OPDATERET
Malware benytter ofte kendte huller i ældre udgaver af software

2 INSTALLER SIKKERHEDSPAKKE
Som minimum bør du have firewall, spamfilter og antivirus

3 UDNYT, AT MODERNE BROWSERE ADVARER OM PROBLEMER
Det kan være irriterende, men lad være med at slå det fra

4 BENYT SIKKERHED PÅ DET TRÅDLØSE NET
Brug WPA2-kryptering, som understøttes af stort set alt

5 BRUG STÆRKE PASSWORDS
Brug passwords med mindst 12 tegn, som er en blanding af tal, symboler samt store og små bogstaver

6 BRUG SUND FORNUFT PÅ NETTET
Alle skal opføre sig fornuftigt på nettet og reagere, hvis noget virker mistænkeligt

7 HAV EN EFFEKTIV BACKUPSTRATEGI
– og kontrollér jævnligt, at du og dine medarbejdere også kan gendanne data

8 SØG HJÆLP HOS EKSPERTER
Hvis du er i tvivl, så tag fat i en ekspert.

9 INGEN BØR BRUGE ADMINISTRATORRETTIGHEDER I HVERDAGEN
Lokale administratorrettigheder kan give en hacker let adgang til systemerne og bør kun bruges, når ingen anden metode virker

10 BESKYT MAIL OG DOMÆNER
Sørg for, at SPF, DKIM og DMARC er slået til. Er du i tvivl om hvad det er, så spørg din it-leverandør. Brug desuden altid digital signatur

HVAD BØR DU PÅ DEN LANGE BANE GØRE FOR AT ØGE SIKKERHEDEN?

På den lange bane bør du arbejde strategisk med IT-sikkerhed. Nedfæld en skriftlig IT-sikkerhedspolitik, der regelmæssigt - en eller to gange årligt - bliver gennemgået og ajourføres om nødvendigt.

Du bør overfor medarbejdere og andre relevante personer synliggøre, hvad acceptabel brug af IT er. Anvend den internationale standard ISO 27001, der er en ledelsesstandard for informationssikkerhed. Den udgør et effektivt styringsværktøj, der hjælper med at beskytte dine værdifulde informationer.

ISO 27001 indeholder krav til risikostyring, dokumentation af processer samt fordeling af roller og ansvar for informationssikkerhed. Det er nødvendigt med tekniske tiltag for at beskytte it-systemerne, og din virksomheds software skal derfor altid være opdateret. Husk at have installeret sikkerhedspakker med antivirus og firewall.

Mange persondata ligger elektronisk, og en god IT-sikkerhedspolitik kræver, at virksomheden sikrer de persondata, som du behandler. Du bør derfor medtage GDPR-reglerne som en del af IT-sikkerheds-politikken.

Serverrum og anden følsom elektronik er også af vital betydning for den daglige drift. Her skal man overveje hvem og hvor mange der har adgang til disse områder, så man minimerer risiko for at udefrakommende får adgang.

Tænk over den dårlige omtale og det imagetab, du risikerer at komme ud for, hvis din virksomheds navn opnår et dårligt omdømme på nettet. Det kan have vidstrakte konsekvenser, da dette kan tage meget lang tid at komme af med igen. Som dominobrikker risikerer din virksomhed at falde sammen for øjnene af dig. Tænk hvis du ikke er i stand til at sende regninger til kunderne! Din økonomi rammes lynhurtigt, så hav fokus på høj grad af IT-sikkerhed.

Sidst, men ikke mindst: stil krav til din IT-leverandør!

Heldigvis kan du gøre meget selv. Minimerer du risikoen, så vågner du ikke op til en morgen fyldt med kaos!

Udgivet august 2021 af de nævnte transportorganisationer

DTL Dansk Transport og Logistik · ITD · danske speditører · DI Transport · DANSK ERHVERV · ATL Transportens arbejdsgivere – en del af DI · 3F · POLITI