Er der hul igennem for hackerne?

TDC Erhverv

TIL SMÅ OG MELLEMSTORE VIRKSOMHEDER

6 fokus-områder til it-sikkerhed

Slå ring om jeres data,
og brug tiden på kunderne.

TDC Erhverv

Er der hul igennem for hackerne?

TIL SMÅ OG MELLEMSTORE VIRKSOMHEDER

6 fokusområder til it-sikkerhed

Slå ring om jeres data,
og brug tiden på kunderne.

4 ud af 10 tager chancen hver dag

Det halter med it-sikkerheden i SMV-Danmark. 40 % lever livet farligt ifølge Erhvervsstyrelsen[1]. Vi er sikrest sammen, så det skal vi lave om på.

Små og mellemstore firmaer har ikke et tilstrækkeligt it-sikkerhedsberedskab, og det truer forretningen i en tid, hvor det kun er et spørgsmål om, hvornår hackerne slår til. Den gode nyhed er, at I kan tage jeres forholdsregler allerede i dag.

Tænk sikkerhed på øverste etage

Første skridt: Sæt sikkerhed på dagsordenen. Dels som prioritet i ledelsen. Dels som bevidst adfærd hos alle ansatte. Et cyberangreb kan lamme jeres virksomhed, medføre tabt omsætning og i værste fald lukning. Og truslen er desværre reel.

Sæt ind nu på de 6 fokusområder

Næste skridt: Gå systematisk til værks med forholdsregler på de områder, hvor kriminelle leder efter sårbarheder. I TDC Erhverv ved vi, hvor skoen trykker.

1) https://erhvervsstyrelsen.dk/digital-sikkerhed-i-danske-smver-2021

Ud fra vores indsigter har vi defineret 6 fokusområder, I bør arbejde med:

- 01 Internetforbindelse
- 02 Arbejdscomputere
- 03 Mobiler og tablets
- 04 Backup af data
- 05 Viden og adfærd
- 06 Hjemmearbejde

På de næste sider ser vi på de 6 fokusområder med konkrete forslag, I kan bruge til at slå ring om jeres data og få mere tid til kunderne.

01
INTERNETFORBINDELSEN

Mandag morgen klokken 8:32 ...

Pludselig forsvinder internetforbindelsen. Medarbejderne får travlt med at gå på nettet via deres mobiler. Der er ikke adgang til kunder og leverandører. Det hele går i stå, for internetforbindelsen er livsnerven i virksomheden. Brug et øjeblik på at lægge en plan, så det ikke sker.

DET KAN I GØRE I DAG:

- Tjek virksomhedens firewall
- Vælg et stærkt kodeord til netværket
- Skift netværkskoden med mellemrum
- Overvej en ny generation firewall

Derfor hedder det en firewall

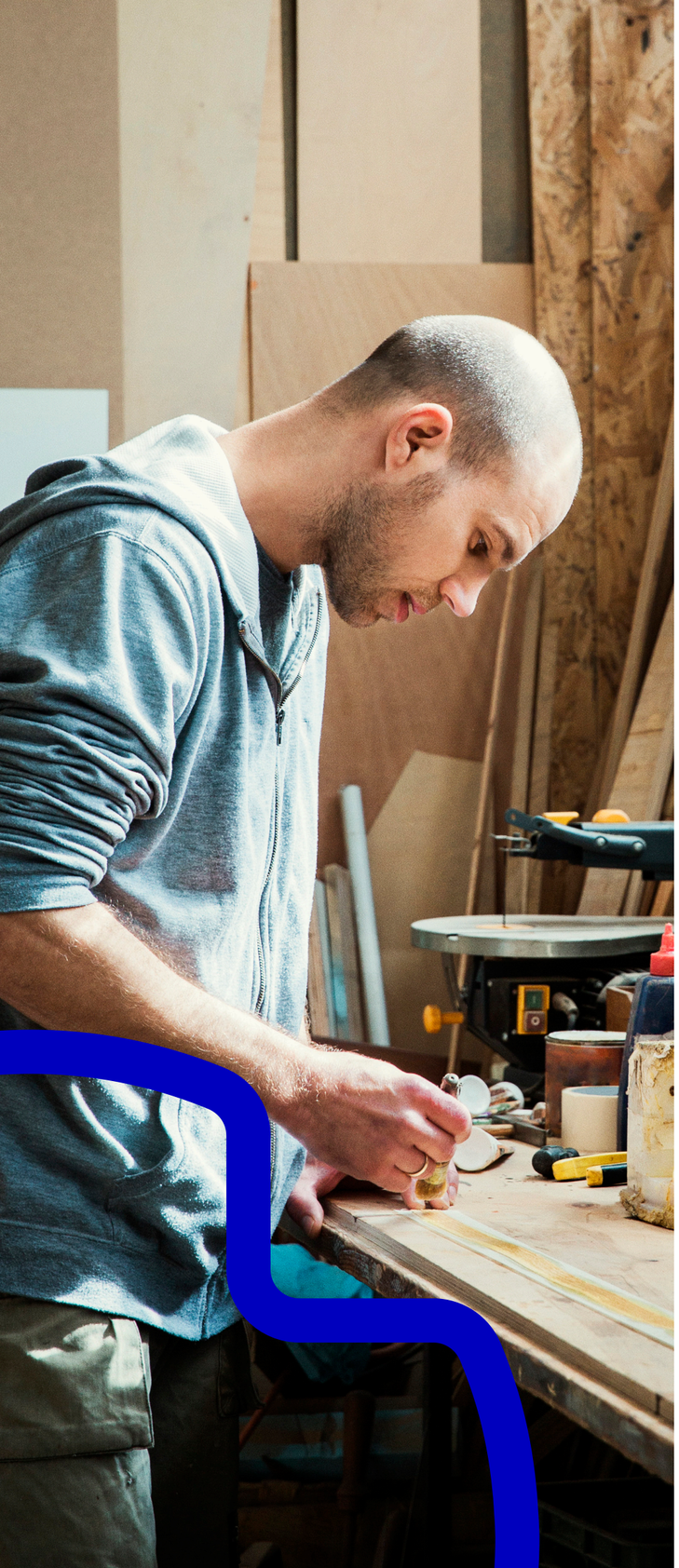
En firewall er afgørende for at sikre data og kritiske systemer. Den hjælper med at beskytte internetforbindelsen mod indtrængen, men kun hvis den er opdateret. De nyeste firewalls giver mulighed for at tjekke trafikken helt ned i detaljer.

Det duer ikke med 'Admin123'

Internetforbindelse og wi-fi på kontorerne sætter skub i produktiviteten. Medmindre en hacker knækker adgangskoden. Derfor skal netværkskoden være lige så unik og stærk som til arbejdscomputerne. Det er også en god idé at skifte den jævnligt.

En ekstra kommunikationslinje

Forbindelsen kan forsvinde af mange grunde. Det kan også være et kabel, der bliver gravet over. Under alle omstændigheder er det være en god idé at have en ekstra linje som fx mobilt bredbånd eller lignende. Så går forretningen ikke i stå.



02

ARBEJDSCOMPUTERNE

Se på pc'erne som et kasseapparat

Jeres virksomheds arbejdscomputere er omdrejningspunkt for forretningsudvikling, ordrebehandling, kundeservice, korrespondance og løbende drift. Tænk på hver pc som et kasseapparat, der sikrer omsætning og aldrig må svigte. Så ved I, hvor vigtigt det er at give sikkerheden et tjek.

DET KAN I GØRE I DAG:

- Vælg nogle stærke adgangskoder
- Skift jeres adgangskoder ofte
- Brug unikke koder til hver service
- Find en god password manager

Vælg stærke adgangskoder

Den enkleste måde at holde hackerne fra døren på: Unikke koder med specialtegn, tal, store og små bogstaver – plus unikke koder til hver tjeneste. Er de svære at huske? Så kan I bruge en password manager med én kode til alle andre koder.

Hold alle pc'er opdaterede

Husk de løbende sikkerhedsopdateringer af programmer og systemer. Så er jeres pc'er et skridt foran hackerne. Sæt computerne til at opdatere automatisk, når der er nye versioner. Så bliver bagdøren lukket, uden at nogen skal huske på det.

Brug to-faktor godkendelse

Når I logger på virksomhedens system, styrker I sikkerheden ved at tilføje et ekstra trin ud over brugernavn og adgangskode. Det kan fx være en kode sendt som en sms. Det tager et øjeblik ekstra, men kan spare kostbar tid til genoprettelse.

DET KAN I GØRE I DAG:

- Få et overblik over alle mobile enheder
- Sørg for, at de opdateres automatisk
- Indfør stærke, unikke adgangskoder
- Overvej at indføre to-faktor-godkendelse

03
MOBILER & TABLETS

Sikkerhed til fingerspidserne?

Mobiler og tablets gør livet lettere og mobilt. De fungerer som computere, og mange opgaver kan løses lige ved hånden. Men hvordan ligger det med sikkerheden? Har I jeres private enheder med på jobbet? Nogle få forholdsregler kan sikre tryg mobilitet for alle på kontoret og på farten.

Hold enhederne opdaterede

Ligesom arbejdscomputerne skal mobiler og tablets opdateres til de nyeste versioner af programmer og systemer. Gør det til fast rutine, at enhederne er indstillet til automatisk opdatering – også selv om det er jeres egne mobiler og tablets.

Hvad med touch og FaceID?

Mange enheder giver adgang med fingeraftryk eller ansigtsgenkendelse. Hvis I får direkte adgang til virksomhedens systemer på den måde, kan det udgøre en risiko. Har I overvejet to-faktor-godkendelse, som også omfatter mobile enheder?

Lås og backup på mobilen

Som minimum skal der være lås på mobiler og tablets, så uvedkommende ikke får adgang, hvis enheden bliver tabt eller stjålet. Af samme grund er det en god idé at tage backup, så man hurtigt kan genskabe en enhed, der går tabt.

04
BACKUP AF DATA

Hvor længe kan I undvære data?

Når data forsvinder eller bliver taget som gidsel i ransomware, står alting stille. Systemerne skal genetableres, og det kan tage tid, hvis der ikke er en frisk backup. Hvor længe kan jeres virksomhed holde til det? Timer, dage, uger? Backup er et kedeligt emne, der hurtigt kan blive brandvarmt.

DET KAN I GØRE I DAG:

- Tjek virksomhedens backuprutiner
- Sker det ofte og sker det sikkert nok?
- Kan I hurtigt komme i gang igen?
- Overveje backup til to lokationer

Etablér faste rutiner for backup

Backup af virksomhedens data kan ske internt eller eksternt, til datacenter eller skyen. Det kan ske på harddiske eller på bånd. Under alle omstændigheder er det en god idé at gøre det automatisk, regelmæssigt og ofte – bare det bliver gjort.

Husk at teste backup og recovery

Enhver backup- og recoveryløsning skal testes for at sikre, at det fungerer. Test regelmæssigt med genstart af systemet, så alle kan arbejde trygt til daglig og være hurtigt i gang, hvis uheldet er ude, eller angrebet er en realitet.

Nogle data er vigtigere end andre

Det koster penge at etablere og drive backup. Derfor vælger mange at prioritere, så de mest kritiske data bliver gemt ofte, måske hver dag eller få timer bagud i tiden. Så kan mindre vigtige data gemmes ugentligt eller endnu sjældnere.

05

VIDEN OG ADFÆRD

Kim er hackernes bedste ven

Der er sket en eksplosiv stigning i phishing-angreb, hvor kriminelle forsøger at lokke koder fra virksomhedens medarbejdere. Kim i kundeservice og Jytte i regnskab skal derfor være oppe på mærkerne, hvis der er tegn på angreb. Det kræver, at alle har viden om betydningen af sikkerhed.

Øjne og ører skal holdes åbne

Ser mailen mærkelig ud? Er et godt tilbud for godt til at være sandt? Skal chefen have overført ekstra mange penge på ferie? De cyberkriminelle bliver bedre og bedre til at fiske oplysninger. Det er på sin plads med sund skepsis hver dag.

Gør reklame for de gode rutiner

Automatisk sikkerhedskopiering, stærke adgangskoder, skepsis over for mails ... trusselsbilledet skifter og alle skal være bevidste om, at det kan gå galt, og at det kan have konsekvenser. Tag et fyraftensmøde om it-sikkerheden.

En printer kan også være en dør

Sikkerhedsbevidst adfærd omfatter ikke alene pc'er, tablets og routere. Printere, overvågningskameraer og andre enheder er også koblet på netværket, og kan gemme på data. Derfor skal alle netværksenheder omgås med sikkerhed.

DET KAN I GØRE I DAG:

- Hold et møde med sikkerhed på agendaen
- Tal om it-sikkerhed ofte i hverdagen
- Sørg for sund skepsis ift. mails og links
- Prøv at indføre nogle enkle rutiner

06
HJEMMEARBEJDE

Den nye filial på Tjørnevænget 32

Brugen af hjemmearbejdspladser er eksploderet under corona, og meget tyder på, at det er kommet for at blive. På fremtidens arbejdsmarked er der 'kontorer' overalt, og ofte er fjernarbejde et krav for at tiltrække nye medarbejdere. Hvis ikke it-sikkerheden flytter med ind, kan det give udfordringer.

DET KAN I GØRE I DAG:

- Undersøg markedet for VPN-løsninger
- Husk stærke koder på hjemme-pc'en
- Brug kun arbejds-pc'en til arbejde
- Sæt alle enheder til automatisk opdatering

Den sikreste vej hedder VPN

En VPN – *Virtual Private Network* – er en krypteret linje mellem hjemmet og firmaets netværk. Den beskytter trafikken og gør medarbejderen mere produktiv. Har I valgt to-faktor-godkendelse skal den også gælde for hjemme-pc'en.

Er der private med på linjen?

I sagens natur sidder mange på hjemmekontoret side om side med resten af familien. Det kræver disciplin. En VPN-forbindelse og sikker login på virksomhedens netværk er en god idé, og så bør arbejds-pc'en kun bruges til arbejde.

Opdatering og sikkerheds-kopiering

Der er risiko for, at medarbejderens setup på hjemmekontoret kan forsvinde ud af syne for de it-ansvarlige. Men når man logger på netværket, fungerer det, som om man sidder på kontoret. Husk derfor automatisk opdatering og backup.

TDC Erhverv

Vil I videre med sikkerhed?

Hos TDC Erhverv hjælper vi tusinder af danske virksomheder med at holde hackerne fra døren, så medarbejdere og ledelse kan koncentrere sig om at udvikle virksomheden og pleje kunderne. Kontakt os, og hør mere om, hvordan vi kan hjælpe jer.

Se mere på **tdc.dk/smartsecurity**
Ring til os på **70 70 90 90**