Det sker kun for min nabo….
NEJ! Cyberangreb er en stadig stigende trussel. Du tænker måske, at din virksomhed er for lille og ikke er interessant for en hacker, men der tager du fejl. Ifølge Ritzau har hver 4. danske mindre virksomhed oplevet brud på IT-sikkerheden i 2021.

Hvordan påvirkes de mindre virksomheder?
Et klik på et forkert link medførte, at en el-installatørs økonomisystem blev krypteret - hackerne krævede løsepenge for at låse filerne op. En webshop blev ramt af malware på hjemmesiden, og kunderne betalte nu direkte til hackeren i stedet for webshoppen. Et IT-system til håndtering af aftaler, opkrævning, betaling, ruteplanlægning mv. blev låst og kunne ikke tilgås, og virksomhedens eksistens blev dermed truet. En direktørs mail blev hacket, og brugt til at instruere økonomimedarbejderen i at overføre penge til "falske kunder".

Hændelserne kostede ikke kun tyveri af likvider, men også tabt driftstid og indtjening. Hændelserne øgede derudover omkostninger til reetablering af data og rensning af systemer fra de ubudne gæster.

Men hvorfor blev virksomhederne ramt, hvad gjorde dem interessante?

Stigende digitalisering af arbejdsgange, dokumentation mv. øger graden af IT-afhængighed i virksomhederne. Det er ikke en dårlig udvikling, da det fremmer effektivitet, produktivitet og gør hverdagen lettere, men det har en værdi for virksomhederne, og dermed også en værdi for en hacker.

Hvad skal de mindre virksomheder så gøre?
Oktober måned er cybersikkerhedsmåned og de danske myndigheder har øget fokus på praktiske råd om, hvordan virksomheder kan beskytte sig bedre. Ja det lyder ikke som det mest spændende at beskæftige sig med de organisatoriske it-sikkerhedsrammer i virksomheden, når man har valgt at blive vinduespudser, butiksejer eller ledelseskonsulent – ikke desto mindre er det vigtigt.

Nogle af de ting man som virksomhed skal forholde sig til er.

- Etablering af en specifik og virksomhedsrelevant it-sikkerhedspolitik
- Løbende vurdering af risikoprofil – fordi cyberangreb ændrer sig og det gør risikoen også
- Identificere og tydeliggøre de elementer, der ved angreb kan true virksomhedens eksistens
- Etablering sikkerhedsforanstaltninger mod trusler
- Fastlægge procedure ved it-sikkerhedsbrud og etablering af roller, opgave og ansvarsområder, som reaktioner på brud
- Fastlæggelse af regelmæssige information til medarbejdere om it-sikkerhed for at øge bevidstheden om trusler i hverdagen
- Kontrol af logning ved sikkerhedshændelser til vurdering af brud og om de eksisterende sikkerhedsprocedurer er tilstrækkelige eller om de skal forbedres.

Opgaven kan virke svær at gribe om og du vil måske efter evner og interesse have behov for rådgivning.

På SMV:digital.dk er det muligt at søge tilskud til rådgivning om digital sikkerhed og ansvarlige dataanvendelse på op til 50.000 kr. hvis du har mellem 2-249 ansatte (https://smvdigital.dk/content/ydelser/tilskudspuljer-i-smvdigital-i-2022/94225503-954b-40fb-95e5-43c7a1a8ffb3/)

Du kan herudover overveje en cyberforsikring, der oftest suppleres med rådgivning om IT-sikkerhed, ud over at du får erstatning ved rekonstruktion af IT-systemet ved angreb.

Her og nu

Det er fint at søge tilskud, igangsætte projekter og lignende for at øge sikkerheden – men hvad skal du gøre straks – her og nu – for at blive mere sikker.

De 4 absolut vigtigste råd er:

1. Backup
2. Softwareopdatering
3. Password og to-trin beskyttelse
4. Bevidsthed og træning

1. *Backup*

   Få styr på jeres backupprocesser:

   - Hvad skal der tages backup af?
   - Hvornår skal det gøres?
   - Hvem er ansvarlig for at gøre det?
   - Hvor skal det opbevares – måske hos ekstern part?
   - Test backuppen regelmæssigt – virker den som den skal?

2. *Softwareopdatering*

   Sørg for at jeres systemer er opdaterede – både grundlæggende operativsystemer og programmer, som Windows.
   Sørg for at antivirusprogrammet er opdateret og fungerer som planlagt.

3. *Password og to-trin beskyttelse*

   Brug stærke password – kombinationen af dine børns, kones eller kæledyrs navn og fødselsdag giver kun et mindre antal kombinationer for hackerens programmer at finde frem til og er derfor ikke særlig stærke.

   Et stærkt password består af mindst 12 tegn, store og små bogstaver, tal og med specialtegn. Det er et der ikke bruges flere steder, og som du ikke deler med andre. Herudover skiftes det jævnligt.

   Anvend en to-faktor godkendelse til beskyttelse af brugeroplysninger. En to-faktorgodkendelse er fx. at du modtager en sms med en kode der skal indtastes efter dit normale password ved login.

   På digitalsikkerhed.dk er det muligt at finde guides til forskellige tjenester med to-trin godkendelse, herunder Microsoft, Google og sociale medier jf. følgende link: https://sikkerdigital.dk/borger/tekniske-setup/guide-to-trins-login Listen er ikke udtømmende.

4. *Bevidsthed og træning*
   En stor del af cyberangreb lykkedes med hjælp fra virksomhedens egne medarbejdere – ganske ubevist naturligvis.

   Oplys medarbejderne om de mulige trusselstyper ifm. cyberangreb – det er ikke alle, der er lige beviste om, hvordan en hacker kan få adgang og hvordan man spotter en risiko.

   Rådgiv medarbejderne i hvordan man bedst undgår truslerne, fx:
   - At undlade at åbne mail og filer fra ukendte afsendere,
   - At undlade at klikke på links, uden først at holde musen over for at se, hvor linket fører til, og om det er som forventet.
   - At forholde sig kritisk til sproglige formuleringer i mails,
   - At bede om bekræftelse (telefonisk/face-to-face) på om overførsel af likvider i store mængder.

Center for cybersikkerhed (cfcs.dk), Sikkerdigital.dk og mange flere har gode råd, vejledninger og værktøjer at hente til hjælp i forbindelse med at øge sin it-sikkerhed.

Hvad nu hvis virksomheden er blevet angrebet?
Er skaden sket og er din virksomhed blevet ramt af et cyberangreb – så skal angrebet stoppes. Inden du trækker stikket ud af kontakten, så henviser politiet til at læse deres publikation om forholdsregler, således at det samtidig sikre indsamling af data til brug i efterforskningen: https://sikkerdigital.dk/media/8774/forholdsregler-ved-brud-paa-it-sikkerhedssystemer.pdf Det er naturligvis vigtigt at din virksomhed agerer efter hvad der er bedst for jer i situationen.

Uanset angrebets størrelse, så skal angrebet indberettes til Erhvervsstyrelsen på virk.dk: https://virk.dk/myndigheder/stat/ERST/selvbetjening/Indberetning_af_brud_paa_sikkerhed/ Herudover kan økonomisk svindel på nettet indberettes digitalt til politiet, https://politi.dk/oekonomisk-svindel-paa-nettet

Kontakt
Du er altid velkommen til at kontakte din daglige rådgiver hos Revision Vadestedet for drøftelse af den generelle IT-sikkerhed i din virksomhed. Vores særlige fokus er naturligvis på risikoen i forbindelse med økonomi og regnskabsaflæggelse, men vi involverer gerne specialister i det omfang du måtte have behov for det.