Cybersikkerhed – 5 tips til organisationer under coronavirus-lockdown

Marlene Winther Plas
Partner, Head of IPT, Denmark

Anders Nielsen
Advokat

Jon Lauritzen
Partner

Mange danske arbejdspladser har i disse tider – efter regeringens opfordring – givet deres medarbejdere besked om, at de skal arbejde hjemmefra. Generelt må det konstateres, at den pludselige stigning i mængden af hjemmearbejde – kombineret med den samfundsmæssige påvirkning af coronavirus – forøger virksomheders risikobillede i relation til cybersikkerhed. Center for Cybersikkerhed udkom i marts 2020 med en revideret trusselsvurdering. Her blev truslen fra cyberkriminalitet vurderet til at være "MEGET HØJ".

Vi giver derfor 5 råd til virksomheder, der er påvirket af den nuværende coronavirus-lockdown.

Tip 1: Opdater jeres risikovurdering

Risikobilledet i dag er væsentligt ændret i forhold til for få måneder siden. Kriser skaber normalt en øget efterspørgsel på information hos mennesker, hvilket ondsindede hackere forsøger at udnytte i form af phishing, falske hjemmesider og andre former for spredning af skadeligt indhold. Derudover åbnes der op for sårbarheder når størstedelen af virksomhedens medarbejdere – fra den ene dag til den anden – skal arbejde hjemmefra.

Det er derfor naturligt, at man som virksomhed skal forholde sig til det ændrede risikobillede – både i forhold til risici for hændelige uheld og ondsindede hændelser – og overveje hvilke foranstaltninger der bør iværksættes som konsekvens heraf.

Eksempler på overvejelser, som virksomheder i den forbindelse kan gøre sig, kan omfatte:

- Hvorvidt virksomheden er blevet et mere eller mindre interessant mål i lyset af COIVD-19 og lockdown
- At VPN-tjenester pludselig kan udgøre et forretningskritisk IT-aktiv, der eksempelvis lammer al virksomhedens produktivitet, hvis der sker overbelastning (fordi der ikke er indkøbt tilstrækkelig kapacitet i tilfælde af DDOS-angreb, etc.)
- Hvilken betydning hjemmearbejdspladser har for fysisk sikkerhed
- Hvorvidt medarbejderne har tilstrækkelige IT-ressourcer stillet til rådighed. Manglende ressourcer kan forøge risikoen for, at medarbejderne anvender uautoriserede IT-aktiver, såsom private computere, private e-mailkonti, private lagringsmedier (fx USB-nøgler), uautoriserede cloud-løsninger (fx Dropbox) etc.
- Den øgede risiko for phishing og anden udnyttelse af medarbejdernes bekymring, nysgerrighed og søgen efter information som følge af COVID-19
- Det skal også overvejes, hvorvidt smart-devices med stemmestyring som f.eks. Googles Nest Hello og Amazons Echo på hjemmekontoret er forenelig med virksomhedens sikkerhedspolitik

Vi anbefaler, at alle virksomheder foretager en midlertidig revidering af gældende risikovurderinger så længe den nuværende coronavirus-lockdown står på. Virksomhedens sikkerhedsniveau bør ikke sænkes som følge af den særlige situation.

Alle virksomheder bør desuden overveje om ekstra awareness-kampagner skal iværksættes, der er målrettet den særlige coronavirus-situation, og bør sørge for løbende at orientere medarbejdere om, hvilke risici de skal være opmærksomme på.

Tip 2: Sørg for, at risici håndteres i overensstemmelse med virksomhedens pligter

For visse sikkerhedsrisici er det en forretningsmæssig beslutning, hvordan disse skal håndteres – herunder om man vælger at være mere eller mindre risikovillig. For andre sikkerhedsrisici kan det være lovgivningsmæssige rammer, der påvirker de handlemuligheder (eller mangel på samme) som virksomheden har – navnlig databeskyttelsesforordningens artikel 32 for så vidt angår beskyttelse af persondata. Disse rammer kan særligt begrænse virksomhedens risikovillighed, og kan i visse tilfælde fastholde virksomhedens ansvar, hvis dette outsources til en ekstern leverandør uden at de rette foranstaltninger træffes.

Hvis din virksomhed agerer som databehandler på vegne af andre virksomheder, vil der typisk være indgået databehandleraftaler, der stiller krav til det niveau af sikkerhed der skal opretholdes – sikkerhedskrav der eventuelt skal kunne underlægges en revision. Her er det særligt vigtigt at være opmærksom på, at databehandleraftalen kan stille særlige krav eller helt afskære adgangen til brug af hjemmearbejdspladser. Står sådanne vilkår i vejen for hjemmearbejdet, kan en akut genforhandling være nødvendig.

Tip 3: Hvad står der i kontrakten med IT-leverandøren?

Mange virksomheder er generelt afhængige af deres IT-leverandører, der ofte betragtes som forretningskritiske. Dette gælder særligt i disse tider, hvor en stor del af virksomhedens medarbejdere arbejder hjemmefra.

I skrivende stund har størstedelen af alle europæiske virksomheder givet deres medarbejdere besked om, at de skal arbejde hjemmefra i videst muligt omfang. Dette er naturligvis en belastning for den eksisterende IT-infrastruktur og kapacitet – endda i en sådan grad, at nogle streaming-tjenester har valgt at reducere kvaliteten på indhold der leveres til forbrugere.

Derved opstår også en forøget risiko for, at IT-leverandøren ikke er i stand til at levere den lovede kapacitet – blandt andet fordi visse IT-leverandører sælger mere kapacitet end de egentlig har, ud fra en tese om, at samtlige kunder aldrig bruger 100% af den indkøbte kapacitet.

Visse IT-leverandører kan derfor finde det vanskeligt at leve op til de IT-kontrakter, som er indgået med deres kunder – eventuelt også fordi underleverandørerne er udfordret.

Eksempler på spørgsmål, som virksomheder i den forbindelse bør forholde sig til, er:

- Hvorvidt de krav, der stilles til IT-leverandøren, er klare og præcise. Regulerer SLA'en også svartider eller alene oppetider?
- Hvorvidt der anvendes underleverandører og hvilken betydning disse har
- Hvilke handlemuligheder virksomheden har, hvis leverandøren ikke kan levere (helt eller delvist)
- Hvorvidt IT-leverandøren kan påberåbe sig force majeure for manglende eller mangelfuld levering samt i hvor lang tid IT-leverandøren kan påberåbe sig force majeure
- Hvorvidt der stilles tilstrækkelige sikkerhedsmæssige krav til leverandøren samt om disse skal revideres i overensstemmelse med Datatilsynets retningslinjer herom
- Hvorvidt der kan leveres (reserve)hardware med kort varsel – særligt hvis virksomheden selv hoster sine tjenester

Tip 4: Forbered jer på det værste

Situationen med coronavirus-lockdown bør også give anledning til at genoverveje virksomhedens beredskabsplan og eventuelt udarbejde en midlertidigt revideret version af denne.

Mange beredskabsplaner tager udgangspunkt i, at medarbejderne har adgang til at møde fysisk og har uhindret fysisk adgang til servere og andre IT-aktiver. Virksomheden bør desuden overveje, om erstatnings-hardware kan skaffes uden problemer, og hvilken betydning hjemmearbejdspladser har for at kunne styre og lede en genopretning af IT-systemer, hvis disse rammes af et angreb.

Som led heri, bør virksomheden overveje, hvordan nødkommunikation til virksomhedens medarbejdere kan ske i tilfælde af, at virksomhedens gængse kommunikationsplatforme bliver utilgængelige. Hvor der tidligere var mulighed for hurtigt at kommunikere mundtligt til et større antal medarbejdere i tilfælde af et (hændeligt eller ondsindet) IT-nedbrud, eksisterer denne mulighed som udgangspunkt ikke under coronavirus-lockdown.

Det bør desuden overvejes, om mulighederne for at fremskaffe de rette kompetencer til tilfælde, hvor et IT-nedbrud er påvirket af corona-lockdown. Det må nok forventes, at de fleste IT-sikkerhedsfirmaer fortsat står til rådighed med virtuelle møder, hvis der er brug for deres hjælp - lige som vi i DLA Piper gør.

Endeligt bør virksomhedens medarbejderne mindes om, at kravene om at underrette om sikkerhedsbrud stadig gælder, selvom de arbejder hjemmefra. Sikkerhedsbrud der sker fra en hjemmearbejdsplads skal – som udgangspunkt – fortsat indberettes til Datatilsynet senest 72 timer efter at det opdages.

Tip 5: Følg myndighedernes råd og vejledning

En lang række offentlige myndigheder stiller i øjeblikket skarpt på den nuværende situation og de særlige omstændigheder, som coronavirus skaber. Vi henviser i den forbindelse særligt til Center for Cybersikkerhed (fe-ddis.dk), der flere gange om ugen udsteder nye vejledninger om informationssikkerhed til virksomheder og private.

Andre offentlige hjemmesider, der stiller gratis information til rådighed, omfatter sikkerdigital.dk og ENISA (Europearn Union Agency for Cybersecurity) – enisa.europa.eu.

Fagområder	IP og teknologi
Sektorer	Technology