nft

Nordisk Forsikringstidsskrift

Et samarbeid mellom forsikringsforeningene i Danmark, Norge og Sverige



**FORFATTER**

*Tom Engly*

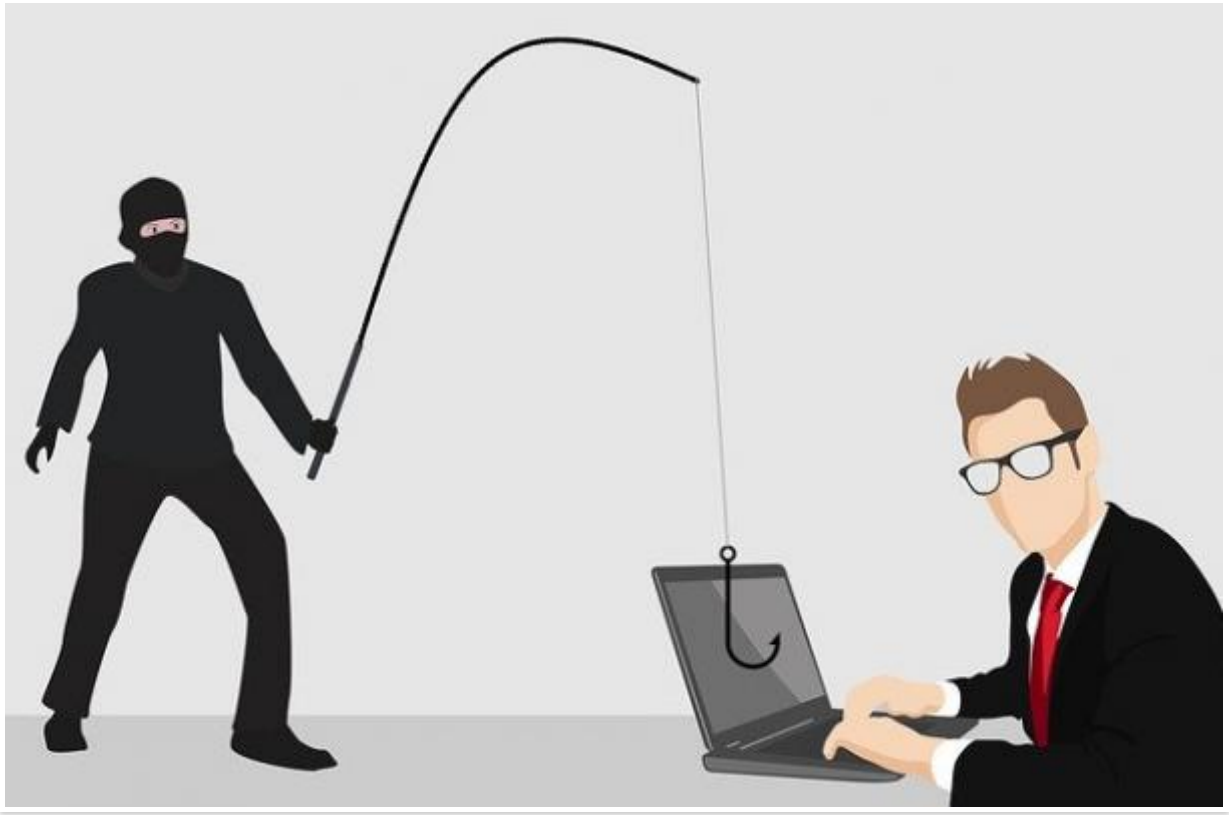
**FACTS**

*Udgave: 1 /2020*

*Språk: Dansk*

*Kategorier: Digitalisering, Risiko*

**SHARE ARTICLE**





# Cybercrime – en stigende trussel

De fleste kan sikkert nikke genkendende til ordet Cybercrime, men hvad ligger der egentlig i det?

Jeg var med til at starte den danske afdeling til bekæmpelse af denne type kriminalitet i Dansk Politi tilbage i 1990`erne, hvor det hed EDB-kriminalitet, siden IT-Kriminalitet, og nu altså Cybercrime. I bund og grund er det stadig det samme – nemlig kriminalitet ved brug af computere, netværk og Internettet.

I den tidlige start krævede det en stor teknisk viden at begå "Edb-kriminalitet", og der fandtes stort set ingen såkaldte hackerværktøjer til at understøtte det. Det var primært hacking for hackings skyld, der var fænomenet – altså ikke den økonomiske vinkel, der først kom til senere.

Det adskiller sig ikke fra den fysiske kriminelle verden, hvor f.eks. mafia, rockerbander og andet godtfolk kastede sig over f.eks. narkotikahandel, prostitution og lignende. Hvor der er økonomisk gevinst i sigte, er der altså også kriminelle, der involverer sig. Det er der, vi står i dag, hvor kriminaliteten blot er flyttet over på

de digitale platforme. Vi er med andre ord blevet digitale borgere i et digitalt samfund. Da vi digitaliserer alt, hvad er muligt er det altså blevet sværere at begå den konventionelle fysiske kriminalitet. Et godt gammeldags bankrøveri hører derfor til sjældenhederne.

I dag er hacking blevet allemandseje, og enhver, der måtte have kriminel hensigt og en smule indsigt i at finde ud på "Det mørke Internet", kan begå selv meget avanceret kriminalitet ved at købe sig til tjenester på det mørke Internet. Det er blevet en industri at udbyde – lad os bare kalde dem webshops – hvor man kan købe sig til at begå Cybercrime. I fagsproget kaldes det CaaS (Crime as a Service). Og så er risikoen for at blevet fanget minimal i forhold til at begå gammeldags fysisk kriminalitet.

Der findes utallige måder at begå svindel på ude på nettet, ligesom der er rigtig mange metoder til på anden vis at tvinge penge ud af sagesløse ofre. At liste dem op kræver en artikel i sig selv, så jeg vil nøjes med at nævne en af tidens største trends.

Ransomware
Ransomware er en kriminalitetsform, hvor de kriminelle krypterer dine filer, så de ikke er tilgængelige. I Tryg blev vi tidligt i 2015 ramt af et Ransomware angreb, hvor vi fik ca. 300.000 filer krypteret og blev afkrævet løsesum. Det var i den tidlige start af fænomenet Ransomware, og heldigvis kunne vi undgå at betale, da vi via backup kunne genskabe alt data – ganske vist forbundet med en del bøvl. Siden da er fænomenet blevet et så alvorligt problem, at det har haft meget store konsekvenser hos virksomheder, hvor nogen simpelthen har måttet lukke. 2019 var året, hvor Ransomware var den absolut største trussel. I Norden kan jeg f.eks. nævne Norsk Hydro, der havde en omkostning på ca. en ½ milliard kroner, og senest høreapparatfirmaet William Demant i Danmark, hvor angrebet jfr. Demant selv kostede ca. 650 millioner kroner. Over stort set hele verden – og værst i USA - er store virksomheder, offentlige institutioner og sundhedsvæsen blevet ekstremt hårdt ramt i 2019. Angrebene er blevet mere avancerede og ikke mindst målrettede, hvilket gør det sværere at beskytte sig. Tendensen forudsiges at fortsætte i 2020. Generelt kan man sige, at så længe der er nogen, der betaler løsesummen, holdes der gang i de kriminelles forretningsmodel.

## Phishing

Phishing er en af tidens andre store trends, og som ofte også indgangen til at få et Ransomware angreb til at bryde ud i en virksomhed. Phishing er en nørdet betegnelse for at "fiske" – altså fiske f.eks. brugernavne og passwords, lokke dig til at klikke på links eller vedhæftede filer, der enten inficerer din computer med såkaldt Malware (virus eller lignende) eller blot giver de kriminelle adgang til systemerne via dit afgivne brugernavn og password.

Phishing starter typisk med en e-mail eller SMS (smishing), og det anslås at 9 ud af 10 angreb starter med en e-mail. Hvorfor så det? – jo det er nemmere at få en medarbejder til, mod dennes viden, at hjælpe med

at give de kriminelle adgang til virksomhedens hellige haller, end at forsøge at bryde ind gennem hoveddøren. Analogt til den gamle verden, hvor vi i mine tidlige år i politiet så biltyve gå udenom biler med ratlåse. Det var ikke umuligt at stjæle en sådan, men ulige nemmere at stjæle den uden ratlås, der stod ved siden af.

## GDPR

British Airways var i 2018 udsat for et hackerangreb, hvor de kriminelle kopierede British Airways hjemmeside og dirigerede kunder over på en kopiplatform, hvor op mod 300.000 kunder så afgav en masse personlige oplysninger i den tro, at de var på den rigtige side. Det er her, GDPR kommer ind. British Airways blev indstillet til en bøde på op mod 1,3 milliarder kroner for at overtræde GDPR lovgivningen – alt sammen på grund af en dårlig sikkerhed på deres hjemmeside.

GDPR har været i kraft siden maj 2018, og ingen tvivl om at GDPR bliver taget ganske alvorligt ude blandt virksomheder m.v. Man kan diskutere om, det er pga. bødestørrelser og ikke et reelt ønske om sikkerhed. Det vil jeg lade op til andre at vurdere. En ting er sikkert, GDPR har betydet et væsentligt løft af IT-sikkerheden bredt i virksomhederne. Uanset det vil de fleste virksomheder alligevel blive ramt, da det er umuligt at sikre sig 100% mod hacker angreb.

## Hvad med de mindre virksomheder?

Som formand for den danske regerings Virksomhedsråd for IT-Sikkerhed arbejder jeg sammen med rådets øvrige medlemmer på at fremme sikkerheden hos de små og mellemstore virksomheder – simpelthen fordi disse halter alvorligt bagud med at få implementeret selv de mest banale sikkerhedstiltag. Det er manglende basissikkerhed, der er den altoverskyggende årsag til vellykkede angreb. Kan vi bare få virksomhederne til at sikre sig på basisniveau, så vil risikoen for, at de bliver udsat for et vellykket Cyberangreb mindskes ganske betydeligt. Det er f.eks. backup af data, opdatering af programmer (kaldes patching), to-faktor godkendelse på internetvendte systemer, lange og komplekse passwords, firewalls og antimalware systemer.
I rådet har vi overfor ministeren anbefalet, at der indføres et IT-Sikkerheds mærke, som kan gives netop hvis den grundlæggende IT-sikkerheds hygiejne er på plads.

## Awareness

Siden phishing nu er årsagen til mange angreb, er et vigtigt tiltag for borgere og ansatte i virksomheder awareness, eller viden om de faldgruber der findes. Det går nemlig ikke væk. I Tryg – som i mange andre virksomheder - kører vi awareness kampagner overfor medarbejderne. Vi simulerer bl.a. phishing overfor de ansatte med henblik på at lære dem, hvad de ikke skal klikke på eller åbne.  Igen et tiltag der ikke fjerner risikoen, men mindsker den. Det er i virkeligheden, hvad sikkerhed går ud på – nemlig at afdække sine

risici, prioritere dem, og nedbringe de væsentligste.
Jeg er selv meget glad for www.sikkerkollega.dk, som er en sjov App, der lærer dig om alle de væsentlige sikkerhedsmæssige faldgruber. Den er sponseret af Industriens Fond, og vi har bl.a. kørt den med succes blandt medarbejderne i Tryg. Den er gratis, så tag den endelig i brug.

## Videndeling og åbenhed

Som tidligere beskrevet kan vi ikke beskytte os 100% mod Cybercrime, men et af midlerne til at blive mere proaktive er at dele den viden, vi får om angreb. Vi kalder det "Indicators of Compromise" I den finansielle branche i Norden findes NFCERT – en sammenslutning af banker og forsikringsselskaber, der via en central platform deler netop denne viden. Det er altså af stor værdi at få detailoplysninger om et angreb på f.eks. et forsikringsselskab i Norden, så alle andre kan tage deres øjeblikkelige forholdsregler. Det kræver også åbenhed, og her er der stadig meget tilbage at ønske sig. Virksomheder holder stadig hændelser tæt ind til kroppen, hvis de er angrebet. – f.eks. ville William Demant ikke sige, hvilket angreb de var udsat for, kun at de var udsat for et alvorligt Cyberangreb. Først meget lang tid efter kom det frem, at det var Ransomware.

## Cyberforsikring

Kan man undvære en sådan? Selv hvis jeg ikke var ansat i et forsikringsselskab, ville jeg aldrig undlade at tegne en sådan. Det er nødvendigt at have professionel og økonomisk hjælp – ikke hvis, men når angrebet sker. I Danmark går diskussionen netop nu på, om vi på lige fod med andre lovpligtige forsikringer også skal kræve, at virksomheder har en Cyberforsikring. Jeg er overbevist om at det er den rigtige vej, med det jeg ser ske.

Man skal heller ikke negligere, at borgerne – som jo er vores kunder – også i stigende grad ser på, hvilken sikkerhed, der findes hos de virksomheder de entrerer med, ligesom alt også tyder på, at IT-sikkerhed vil blive et konkurrenceparameter fremover. Vi ser det allerede nu. Som virksomhed er vi forpligtet til at risikovurdere vores leverandører, hvis de skal behandle persondata for os. Ansvaret for sikkerheden ligger stadig hos os, uanset om vi vælger at lade andre virksomheder behandle data for os. Derfor vil vi i stigende grad være nødt til at fravælge leverandører, som ikke lever op til nødvendig sikkerhed.

## Afslutning

For første gang vurderes Cybercrime som den største risiko virksomhedsledere globalt ser, og derfor er emnet for alvor kommet på bestyrelser og direktioners agenda. Det kan lyde som en helt umulig opgave at sikre sig, men det er det bestemt ikke. Derfor er mit råd at tage den risikobaserede tilgang til at få lavet de nødvendige sikkerhedstiltag. Det vil nedbringe den såkaldte restrisiko, og dermed gøre det mindre sandsynligt, at man rammes. Så se at få en "ratlås" på dine digitale systemer. Uden indsats vinder de

kriminelle.

**Nordisk Forsikringstidsskrift**

Et samarbeid mellom forsikringsforeningene i Danmark, Norge og Sverige

Dataskydd

forsakringsforeningen.se • forsikringsforeningen.no • forsikringsforeningen.dk