Noter til IT-sikkerhed

Mikkel Boye Rasmussen

March 7, 2023

Indledning

Bogen består hovedsageligt af følgende 3 dele:

- **Trusler og risici:** Nærkig på sårbarheder, risikoanalyse og risikostyring. Definition af grundbegræber og koncepter som kan anvendes til konsulentopgaver.
- **Tekniske foranstaltninger:** Denne del af bogen omhandler minimering af risici, og er meget praktisk. Der berøres udvikling af sikker software, kryptografi, hacking og databeskyttelse.
- **Organisatoriske foranstaltninger og it-sikkerhedsledelse:** Den sidste del omhandler ledelse, NIST og ISO 2700x styringssystemer, de vigtigste dele af GDPR samt etiske overvejelser.

Definition af sikkerhedstyper

Informationssikkerhed - sikring af information, modvirk medarbejdere røber information, sikre kun adgang for specifikke individer.

IT-sikkerhed - primært systemets sikkerhed, både information, data, teknologi, brugerene og systemet selv. Eksempelvis er temperaturdata ikke vigtig at sikre, men at sikre systemet så temperaturen ikke kan justeres eksternt er.

Cybersikkerhed - hovedfokus er trusler fra cyberspace, altså netværksrelaterede angreb. Center for cybersikkerhed (CFCS) har til opgave at beskytte Danmark mod disse.

De 7 råd

Erhvervsstyrelsen opsatte i 2021 7 basale råd for at sikre basal IT-sikkerhed i virksomheder. De 7 råd er som følger:

1. Få overblik over vigtige data og systemer.
2. Opdater programmer løbende.
3. Køb antivirus og firewall.
4. Tag backup af data.
5. Lær at spotte mistænkelige mails.
6. Lav stærke adgangskoder.
7. Stil sikkerhedskrav til IT-leverandøren.

Kapitlet omhandlet hvorfor det er vigtigt at holde sig opdateret omkring aktuelle trusler, hvordan danmarks cyberforsvar udvikler sig, samt de to mest udbredte trusler; phishing og ransomware.

Hvad er IT-kriminalitet?

Hovedsageligt kan IT-kriminalitet beskrives som en bred vifte af kriminalitet forbundet med computere, typisk hvor netværk / internettet er benyttet.

der har været et domæneskift fra at fysiske værdigenstande har været værd at stjæle, til at det i høj grad nu er information og persondata der bedst kan svare sig.

Der er en mellemgrund mellem IT-kriminalitet og almen kriminalitet, eksempelvis svindelsannoncer på DBA ved brug af PayPal. Man kan stoppe overførsler efter et produkt for at snyde sælger for sine penge.

De 3 hovedtyper af IT-kriminalitet

Det kriminalpræventive råd har defineret hvad hører under begrebet *IT-kriminalitet*

- **Computer-integritetsforbrydelser:** Forbrydelser hvor selve computeren angribes, ofte med henblik på at hente data eller ødelægge/ændre IT-systemet
- **Computer-assisterede forbrydelser:** Hovedsageligt forbrydelser mod personer typisk igennem netværk, eksempelvis Phishing og identitetstyveri.
- **Computer-indholdsforbrydelser:** distribuering af ulovligt indhold igennem internettet, eksempelvis børneporno. En slags undergruppe af computer-assisterede forbrydelser.

IT-kriminalitet i vækst senest opståede type kriminalitet, men samtidigt den hurtigst voksende. Har oversteget narkokriminalitet som før var den største globale kriminalitetsform. For perspektiv blev 36 milliarder konti eksponeret i de første 3 kvartaler af 2020. Økonomisk set den dyreste form for kriminalitet, adskillige gange dyrere end narko.

IT-kriminalitet i tal

- 90% af verdens sundhedsorginisationer har haft mindst en IT-sikkerhedshendelse de sidste 3 år.
- Cyberkriminalitet koster i gennemsnit 2.9 millioner usd i minuttet, og tager 280 dage stoppe.
- Store virksomheder mister 25usd i minuttet, og i gennemsnit 3.86 mil usd pr angreb.

- IT-sikkerhedsmarkedet var i 2020 176.5 milliarder usd værd, forventet 403 milliarder usd i 2027.
- 15milliarder kontodetaljer hvoraf 5milliarder er unikke, er tilgængelige på *darkweb*
- flere enheder kobles til nettet, der forventes 55,7 milliarder devices på nettet inden 2025. 75% vil være IOT devices.
- DDoS angreb forventes at vokse til 15.4 millioner i 2023.
- DDoS 4.83 millioner angreb første seks måneder af 2020, 26.000 om dagen.
- 86% af sikkerhedsbrud i 2020 var økonomisk motiverede.
- tredobling af angreb mod Industrielle kontrolsystemer samt operationel teknologi.
- 70% af sikkerhedschefer forventer en mindskning i budget.
- i 2020 involverede 45% af sikkerhedsbrud hacking, 17% malware, 22% phishing.

Cyberkriminalitet

Man kan sige at al cyberkriminalitet er IT-kriminalitet, men ikke al IT-kriminalitet er cyberkriminalitet. (da man kun kan tilgå cyberspace igennem IT.)

Case: en større dansk hackersag (CSC-sagen)

Virksomheden opbevarede store mængder fortrolig data for den danske stat, herunder CPR numre i politiets kørekortsregister. Principielt kunne individers straffeattest være ændret. Hackerene havde adgang fra april 2012 til august 2012. Det danske politi ignorerede først en advarsel om databruden fra et revisionsfirma i juni, og dernæst det svenske politi i september. Det er først i februar 2013 politiet handler på informationen. Angrebet var formentligt inspireret af Gottfrid Svartholm Warg, samt en 21 årig dansker. Gottfrid blev anholdt under mistanke for samme angrebstype mod en lignende svensk virksomhed (Logica). Warg lærte danskeren at hacke mainframes igennem et simulatorprogram.

Retssagen

Hackerangrebet på CSC var en lækage af kørekort, CPR-numre og lignende. Det er usikkert om data er blevet misbrugt. De blev tiltalt for omfattende forstyrrelser af informationssystemer og groft hærværk (hacking af politiets registre) yderligere er de tiltalt for følgende paragraffer:

§193 - Omfattende forstyrrelse af drift på post, telefon, radio, fjernsyn, informationssystemer eller forsyning af vand, gas, strøm, varme - bøde eller fængsel på 6 år.

§263, stk 2 - halvandet års straf for uberettiget at skaffe adgang til en andens oplysninger eller pogrammer betemt til at bruges i et informationssystem.

§263, stk 3 - at skaffe adgang til en virksomheds erhvervshemmeligheder - fængsel på 6 år.

§291 stk.2 - øves der hærværk af betydeligt omfang kan straffen stige til 6 år.

CaaS - Crime as a Service CaaS er kommet til indenfor de sidste 5-7 år og har gjort det muligt for den almene mand at begå cyberkriminalitet. Der sælges software istand til at begå diverse typer angreb på dark web.

kapitlet er en kort grundig intro til kryptografi og starter med kryptografiens historie. Derefter en introduktion til fagtermer, koncepter samt moderne kryptografi. Dernæst gennemgås de 3 hovedfundamenter i kryptografi:

- symmetrisk kryptering
- asymmetrisk kryptering
- hashing

kapitlet indeholder opgaver, samt slutter med eksempler på brugen af moderne kryptografi.

Introduktion til kryptografi

Ordet kryptografi stammer fra det græske ord *kryptós* som betyder skjult. Hovedfokus er på kryptering og dekryptering.

Kryptoanalyse - teori og praksis vedrørende kryptering/dekryptering af beskeder.

Kryptologi - læren om hemmeligholdelse af information, en samlet definition for kryptografi og kryptoanalyse.

Historisk kryptografi

Caesar-algoritmen
forskydelse af bogstaver
vigenère-krypteringen
udvidelse af caesar-algoritmen, man starter med et at finde første bogstav fra sit kodeord i yderste kolonne, dernæst tager man det første bogstav i den krypterede besked. dernæst kan man aflæse det "rigtige" bogstav i øverste række.
One time pad
en slags "erstatnings-kryptering" bygger på en lang tilfældig engangskode. Både afsender og modtager skal bruge engangskoden, og beskeden skal mindst være lige så lang som koden.
Steganografi
et yderligere lag, eksempelvis at gemme en krypteret besked i et billede.
Enigma-maskinen