DIGITALISERINGSSTYRELSEN

CENTER FOR CYBERSIKKERHED

Trusselsidentifikation ved risikovurderingen af offentlige it-systemer – Kom godt i gang

2015

Oktober 2015

Trusselsidentifikation ved risikovurderingen af offentlige it-systemer – Kom godt i gang
Oktober 2015

Denne publikation er udarbejdet af
Digitaliseringsstyrelsen
Landgreven 4
Postboks 2193
1017 København K
Telefon 33 92 80 00
digst@digst.dk

og

Center for cybersikkerhed
Kastellet 30
2100 København Ø
Telefon: +45 33 32 55 80
cfcs@cfcs.dk

Elektronisk publikation:
ISBN: 978-87-93073-15-9

Publikationen kan hentes på
Digitaliseringsstyrelsens hjemmeside
www.digst.dk

og

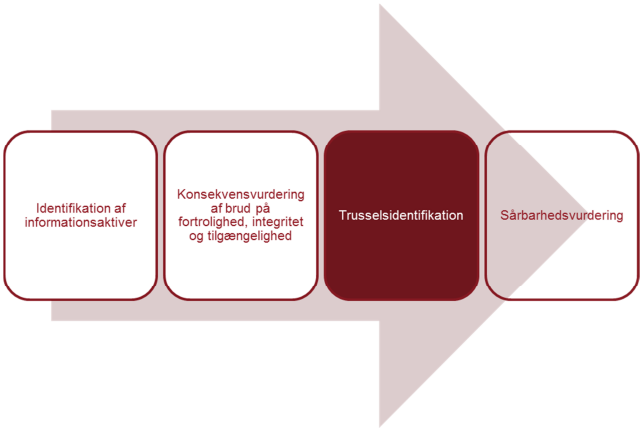
Center for cybersikkerheds hjemmeside
www.cfcs.dk

Indledning

Denne vejledning henvender sig til personer, som arbejder med informationssikkerhed, herunder specifikt risikovurdering og identifikation af trusler, og som har et grundlæggende kendskab til informationssikkerhed og begreberne fra ISO27000 og principperne i ISO27001.

Trusselsidentifikation er en vigtig del af arbejdet med risikovurdering og risikoledelse. Denne vejledning har til formål at give indsigt i, hvordan relevante trusler for informationssikkerheden kan identificeres. Vejledningen behandler ikke det videre arbejde med de identificerede trusler i forhold til sårbarhed og sandsynlighed.

Nedenstående figur illustrerer, hvor i processen man typisk befinder sig på det tidspunkt, hvor vejledning om trusler bliver efterspurgt. Forudsætningen for at kunne identificere relevante trusler er, at informationsaktiverne er kendt, og at der er foretaget en konsekvensvurdering af brud på fortrolighed, integritet og tilgængelighed i forhold til disse, så der er et klart billede af, hvad der er mest vigtigt for organisationen.



I ”vejledning i risikostyring og -vurdering” anbefales det, at der i grundlaget for identifikation af trusler mod informationssikkerheden er udarbejdet et passende grundlag at tage udgangspunkt i. Det anbefales at tage udgangspunkt i organisationens kritiske forretningsprocesser og understøttende informationsaktiver.

Trusselsidentifikation handler om at finde ud af, hvad der kan true informationssikkerheden, om det er relevant for organisationen at tage stilling til disse trusler, ud fra en vurdering af om en given trussel vil kunne påvirke fortrolighed, integritet eller fortrolighed.

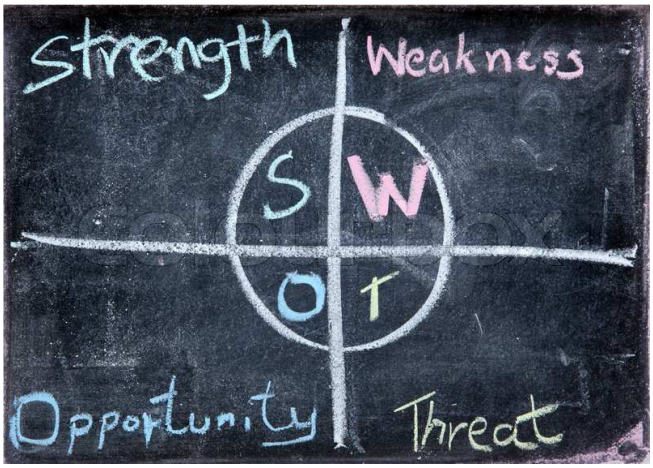
Brud på informationssikkerheden opstår som følge af en hændelse, der potentielt kan skade forretningen. En hændelse udløses af en trussel. Det er arbejdet med identifikationen af trusler, der behandles i denne vejledning.

Udbyttet af denne vejledning bør således være, at læseren er i stand til at identificere trusler, som kan påvirke informationssikkerheden for informationsaktiver i en organisation.

For yderligere information om risikostyring henvises til ”Vejledning i risikostyring og risikovurdering” (2015) samt ISO27005:2011.

Indhold

1. Trusselsidentifikation



En trussel kan betegnes som noget, der potentielt kan udnytte en sårbarhed ved den måde informationsaktivet håndteres eller opbevares. Dette kan resultere i kompromittering af informationsaktivets fortrolighed, integritet og tilgængelighed og dermed skade vigtige forretningsprocesser.

I denne vejledning er det primære fokus på trusler. Den grundlæggende forståelse af trusler er hentet fra den internationale standard for informationssikkerhed ISO27000:2014. Her defineres trusler således som:

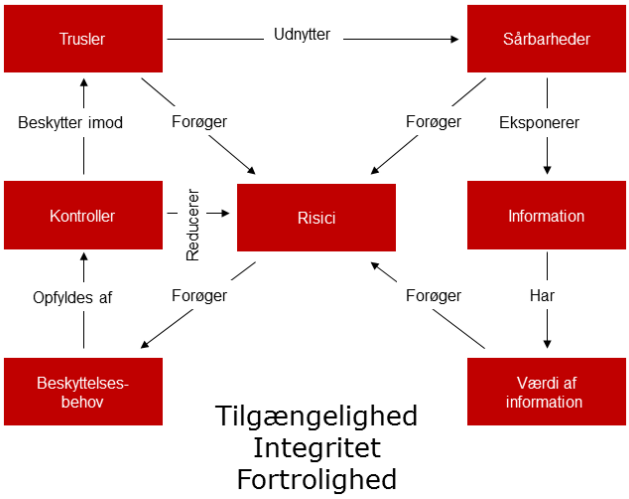
"Potentiel årsag til en uønsket hændelse, som kan forårsage skade på et system eller i en organisation."

Med udgangspunkt ISO27005 beskrives her sammenhængen mellem trusselsvurderingen og organisationens risikostyring af informationssikkerhed og foreslår en metode til at identificere trusler.

Arbejdet med identifikation af trusler handler om at finde ud af, hvad der kan påvirke organisationens informationssikkerhed.

Trusler er dynamiske, og derfor er det tilrådeligt at tilrettelægge arbejdet med identifikation af trusler i det løbende arbejde med informationssikkerheden og de processer, der relaterer sig til organisationens kritiske mål.

Informationssikkerhed skal ses som understøttende for indfrielse af organisationens mål og forretningsstrategi og samtidigt hjælpe ledelsen med at vurdere, om risici er for store til, at de bør accepteres. Trusler er de faktorer, som potentielt kan forhindre organisationen i at nå sine mål.



Figuren viser risikostyringens sammenhæng med begreberne trussel, sårbarhed og kontroller. Denne vejledning handler om at kunne identificere trusler. De øvrige elementer behandles i vejledningen til risikostyring og -vurdering.

Trusler mod informationssikkerheden kan opdeles i fire grupper:

1. Mennesker
   1.1. Medarbejdere
   1.2. Samarbejdspartnere/leverandører
   1.3. Hackere, hacktivister eller andre kriminelle
2. Naturkatastrofer
3. Ulykker
4. Nedbrud og tekniske fejl

1. Mennesker
Den menneskelige faktor udgør to former for trusler mod informationssikkerheden. Den ene er fejl, og den anden er forsætlige handlinger.

1.1 Medarbejdere
Insidere er betegnelsen på medarbejdere, som enten forsætligt eller uforsætligt er med til at forårsage en sikkerhedshændelse, som kan resultere i brud på informationssikkerheden.

Mange brud på informationssikkerheden skyldes medarbejderes mangel på viden eller arbejdsgange, hvor informationssikkerheden tilsidesættes pga. tidspres eller en opfattelse af, at det er for besværligt at arbejde sikkert. Fx deles kodeord mellem flere, eller kodeordene er alt for nemme at gætte.

1.2 Samarbejdspartnere og leverandører
Lige som med medarbejdere er samarbejdspartnere og leverandører ofte i "vennezonen" og betragtes derfor ikke umiddelbart som trusler mod informationssikkerheden. Det er blot vigtigt at orientere sig om, hvilke adgange disse interessenter gives, og nøjagtigt som med medarbejdere gives kun adgang til virksomhedens informationer ud fra princippet om kun at have adgang til det, der er nødvendigt for at udføre en given opgave.

1.3 Hackere, hacktivister og andre kriminelle
Truslen fra hackere, hacktivister og andre personer med hensigter, der er direkte rettet mod at nedbryde eller kompromittere informationssikkerheden, er efterhånden anerkendt.

Hackere og hacktivister er betegnelsen for personer, der udnytter sårbarheder til at bryde ind i computere og netværk, hvorefter de forsøger at få tilstrækkelig adgang til at udøve det, de har planlagt.

2. Naturkatastrofer
Udover menneskeskabte trusler findes også en række begivenheder, som kan påvirke informationssikkerheden. Jordskælv, vulkanudbrud og tornadoer er eksempler på naturkatastrofer. I Danmark er risikoen for naturkatastrofer meget lille, men har virksomheden informationsaktiver uden for Danmarks grænser, kan det være relevant at tage hensyn til dette ud fra en lokal betragtning.

De seneste 10 år har dog vist, at især oversvømmelser foranlediget af store nedbørsmængder kan udgøre en trussel for informationssikkerheden.

3. Ulykker
Udover naturkatastrofer kan informationssikkerheden også trues af andre katastrofer og ulykker, som er delvist er menneskeskabte, og som kan have lige så store konsekvenser. Som eksempler kan nævnes brande, gasudslip og fysiske skader på bygninger.

4. Nedbrud og tekniske fejl
Almindelig slitage og udstyr, der er enten er gammelt eller defekt, kan også true informationssikkerheden. Herudover er det også relevant at overveje konsekvensen af nedbrud på centrale leverancer, fx elektricitet, brændstof eller information. Ved information forstås fx svigt i en webservice, som leverer input til et it-system.

En risikovurdering for it-systemer og data er således en samlet vurdering af sandsynligheden for, at en sikkerhedshændelse indtræffer, samt en vurdering af hændelsens konsekvenser for opgavevaretagelsen i hele organisationen, hvis de pågældende it-systemer og data rammes af hændelsen.

I denne vejledning omtales hhv. vurdering af *trusler* og *sårbarheder:*

- Trusselsvurderingen identificerer og vurderer sandsynligheden for, at trusler vil medføre en sikkerhedshændelse ved at udnytte en sårbarhed. Identifikation og analyse af trusler gør det også muligt at finde eventuelle nye sårbarheder.
- Sårbarhedsvurderingen undersøger, om der er eller kan opstå svagheder, som de identificerede trusler kan påvirke, og derved potentielt forårsage brud på informationssikkerheden.

I det praktiske arbejde med identifikation af relevante trusler bør organisationen medtage nedenstående liste af trusselskilder for at sikre en så dækkende analyse som muligt:

- Den generiske trusselsliste fra ISO27005, Annex C.
- Informationer om trusler på specifikke hjemmesider herunder:
  - cfcs.dk
  - sans.org
  - enisa.europa.eu/
- Selv overveje, om der er andre trusler, som bør indgå.

2. Vurder relevante trusler for egen organisation

I arbejdet med identifikation af trusler mod informationssikkerheden fokuseres på at udpege de trusler, som er relevante for organisationen. Dette arbejde kan udføres helt enkelt ved at tage udgangspunkt i den bruttoliste af trusler, som er udarbejdet på grundlag af foregående kapitels arbejde med identifikation af mulige trusler. Resultatet bør være en nettoliste af trusler, som vurderes relevant for organisationen at forholde sig til.

For at kunne nå dertil, hvor organisationen har en liste over de trusler, som vurderes at kunne påvirke organisationens informationssikkerhed negativt, anbefales det at gennemgå bruttolisten over trusler sammen med andre, herunder kolleger og andre med viden om forretningen og anvendelse af informationsaktiver.

I arbejdet med at vurdere, om en trussel er relevant, kan det være svært at gennemskue, om en trussel har direkte eller indirekte mulighed for at påvirke informations-sikkerheden og kritiske forretningsprocesser. Det er vigtigt at sondre mellem trusler og sårbarheder i dette arbejde, så der udelukkende tages udgangspunkt i, *om* en given trussel kan påvirke informationssikkerheden. Arbejdet med sårbarhedsvurdering hører til senere i risikovurderingen.

Det anbefales, at der tages udgangspunkt i en overordnet konsekvensvurdering, som bør være lavet inden arbejdet med trusler går i gang. En detaljeret konsekvensvurdering er en del af arbejdet med risikovurdering og beskriver konsekvenserne af brud på fortrolighed, integritet og fortrolighed i forhold til de informationsaktiver, som bør være identificeret. I vejledningen om risikostyring og –ledelse beskrives konsekvensvurdering nærmere.

Identificerede trusler bør vurderes efter relevans, og der bør tages stilling til truslernes påvirkning af fortrolighed, integritet og tilgængelighed. Derved kan konsekvens-vurdering og trusselsliste sammenholdes for på den måde at få overblik over, hvilke trusler der potentielt har størst påvirkning på informationssikkerheden.

For overskuelighedens skyld kan det være nyttigt at gruppere de relevante trusler efter type, aktiv, proces eller en anden struktur, som kan give et hurtigt overblik i den videre behandling af trusselskataloget.

Relevans er hægtet til sandsynlighed. Sandsynligheden bør overvejes for at kunne vurdere om en trussel er relevant. I kontekst af vurdering af, om en trussel er relevant at forholde sig til overhovedet, introduceres begrebet ’en **iboende sandsynlighed**’ som sandsynligheden for, at en trussel eksisterer.

Der er fx ikke vulkaner i Danmark. Den iboende sandsynlighed vurderes derfor meget lav eller som ”ingen”. Udfaldet af denne vurdering vil højst tænkeligt blive, at denne trussel ikke vil blive behandlet yderligere, uagtet at skulle der indtræffe et vulkanudbrud ud af det blå, ville der sandsynligvis være behov for at sikre sig i mod det.

Iboende sandsynlighed er ikke er det samme som vurdering af sandsynligheden for konkrete forretningsmæssige konsekvenser for organisationen.

Sandsynlighed behandles ikke yderligere i denne vejledning, men der kan findes mere information om emnet i ISO27005:2011, Annex E.

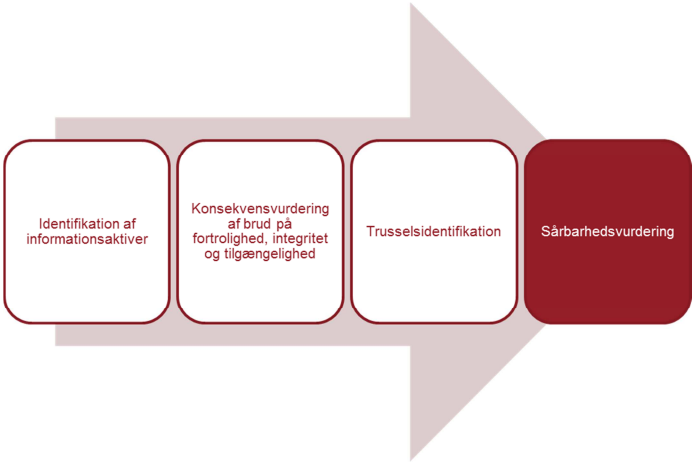
På næste side er der et eksempel på en tabel, som illustrerer en måde at strukturere den indledende behandling af trusler, hvor der udelukkende tages stilling til, hvorvidt en identificeret trussel vurderes relevant for organisationen.

I tabellen er der til inspiration indsæt en række eksempler på trusler fra de forskellige kategorier af trusler:

Trussel:	**Relevant: (JA/NEJ)**	**Påvirker**		
		Fortrolighed	Integritet	Tilgængelighed
Ved en fejl videresendes e-mail til forkerte modtagere	JA	X		
En medarbejder åbner en vedhæftet fil med virus/malware/cryptoware	JA	X	X	X
En medarbejders PC hos en leverandør/samarbejdspartner er inficeret med virus/malware og forbundet til organisations netværk	JA	X	X	X
En medarbejder hos en leverandør har fået nyt job og har fortsat adgang til organisationens informationsaktiver	JA	X	X	
En hacktivist finder en svaghed på organisationens webserver efter en opdatering og laver en defacement	JA			X
En hacker får via social engineering informationer, som kan bruges til at finde sårbarheder	JA	X	X	X
Vulkanudbrud	Nej (nærmeste aktive vulkaner er Island og Italien)			
Brand i serverrum	Nej (Har outsourcet al drift)			
Elforsyning fejler pga. nedbrud hos leverandør	JA			X
Brand i kontorlokaler eller naboejendom	JA			X

3. Afslutning

Identifikation af trusler mod organisationens informationssikkerhed og dermed evne til at udføre sine forretningskritiske processer skal efterfølgende føre til arbejdet med sårbarhedsvurderingen og herunder imødegå disse trusler på en balanceret måde.



Sidste del af denne vejledning handler om det udbytte, der gerne skulle være produktet af en grundig trusselsidentifikation.

Formålet med arbejdet med trusselsidentifikation er at få et klart overblik over, hvad der kan true forretningen, og hvilke trusler der kan gøre skade, hvor.

Afhængig af, hvordan vurderingen af truslers relevans for forretningen er udarbejdet, er næste skridt at foretage en sårbarhedsvurdering i forhold til de identificerede trusler.

Arbejdet med sårbarhedsvurdering og den efterfølgende mitigering beskrives ikke i denne vejledning, men der henvises til den generelle vejledning i risikostyring og -vurdering som findes her.

I arbejdet med sårbarhedsvurdering kan der endvidere findes inspiration i ISO27005:2011, Annex D, hvor emnet omtales yderligere sammen med konkrete metoder.