# Bedre brug af indberettede data om sikkerhedshændelser

**Initiativets indhold**

IT-Branchen og Rådet for digital sikkerhed foreslår, at der i forbindelse med den kommende Strategi for Cyber- og Informationssikkerhed igangsættes et arbejde, der skal sikre at indberetninger om hændelser til bl.a. Datatilsynet samt Politiets Landsdækkende center for økonomisk it-kriminalitet (LCIK) kan systematiseres og anvendes til at øge vores viden om sikkerhedshændelser.

Initiativet består af seks aktiviteter:

* Der skal sikres en brugbar tilbagemelding til de aktører som foretager indberetning.
* Der skabes et overblik over alle de forskellige kilder, hvor der indberettes og deles oplysninger om sikkerhed til og med offentlige myndigheder – f.eks. Datatilsynet, LCIK, Finanstilsynet og DCIS-samarbejdet.
* Der etableres datavarehuse, hvor data fra kilderne kan samles og systematiseres. Datavarehusene bør placeres hos den pågældende dataejer for at sikre bedst mulig kvalitetssikring og anvendelse af data
* Der igangsættes en normalisering og anonymisering af data, så de kan fritstilles og anvendes sammen med andre data om sikkerhedshændelser, f.eks. fra private sikkerhedsleverandører. På denne måde kan initiativet være første led i etablering af en egentlig hændelsesdatabase
* Der igangsættes et arbejde, der skal sikre, at der er hjemmel til at anvende de indberettede data i denne sammenhæng og udstille dem i anonymiseret form.
* Der igangsættes et arbejde, der skal undersøge, om der i forbindelse med indberetninger til kilderne kan stilles mere præciserede spørgsmål, der kan give mere relevant viden om sikkerhedstruslerne.

**Baggrund**

Det ligger værdifuld viden om cybersikkerhedshændelser og -trusler, som ikke anvendes i tilstrækkeligt omfang.

GDPR, NIS-direktivet og lovgivning på flere sektorområder (bl.a. tele og finans) gør det obligatorisk for rigtig mange offentlige og private aktører at indberette brud på informationssikkerheden. Selvom alle indberetningerne ikke direkte omhandler sikkerhedshændelser, indeholder de fleste af disse alligevel værdifuld viden, som kan bruges i den sammenhæng.

Lovene er som udgangspunkt myndighedscentrerede og har fokus på, hvad myndighederne skal have, og hvad myndighederne kan bruge det, de får, til. Dem, der indberetter, har generelt en oplevelse af, at data sendes ind i et sort hul, fordi der ikke sker en tilbagemelding fra myndigheden som beskriver, om data er blevet brugt, til hvad de er blevet brugt, og om virksomhedernes bidrag på nogen måde har haft gavn - f.eks. til at opklare en kriminel handling.

Derfor har mange virksomheder ikke incitament til at bruge ressourcer på at foretage anmeldelsen. I stedet bliver anmeldelsen alene betragtet som en administrativ byrde. Det betyder bl.a., at alt for få virksomheder og myndigheder deler deres erfaringer om digitale trusler, angreb og løsninger. Center for Cybersikkerhed modtog fx kun 38 indberetninger om sikkerhedshændelser i 2019. Der bør derfor arbejdes med at sikre en fornuftig tilbagemelding til de aktører, der skal bruge eller frivilligt bruger deres tid på at indsamle data og indberette disse. På den måde sikrer man et incitament til flere indberetninger.

For at sikre flere indberetninger, og for at gøre bedre brug af de indberetninger som allerede modtages, foreslår IT-Branchen og Rådet for digital sikkerhed en indsats, der skal normalisere, anonymisere og udstille de indsamlede data, så de kan komme flest muligt til gavn. Det vil være oplagt at starte de steder, hvor vi i dag har flest indberetninger,

* LCIK modtager hvert år over 20.000 indberetninger fra borgere og virksomheder.
* Datatilsynet har siden GDPR trådte i kraft modtaget over 18.000 indberetninger om databrud.

Disse indberetninger bruges intensivt til det specifikke formål, de er indsamlet til, men den store værdi ift. at skabe ny viden om sikkerhedshændelser og trusler udnyttes ikke i dag. Der vil være stor værdi for anmelderne i adgang til anonymiserede data om hændelser fra lignende aktører, eller aggregerede data i form af statistikker om typer af sikkerhedshændelser. Det vil også være af stor værdi for professionelle aktører i form af sikkerhedsvirksomheder og brancheorganisationer, at kunne udnytte data til at vejlede om mitigerende foranstaltninger.

For at øge værdien af de indsamlede data bør man endvidere undersøge, om det er muligt at revidere indberetningsskemaerne, så der i højere grad indsamles data, der giver værdi til virksomhedernes og myndighedernes indsats for bedre sikkerhed. Det kan fx være yderligere oplysninger om sikkerhedshændelsen i form af tidsstempler, IP-adresser og anvendt skadelig kode, hvad der forsagede den og hvilke sikkerhedsforanstaltninger man har anvendt.