

Sterk økning i risiko for eksponering av helsedata i USA

Forfattere: Makhlysheva A, Bellika JG, Bakkevoll PA.

Bakgrunn

Risiko er et mål som kombinerer sannsynligheten for og virkningen av en uønsket hendelse. I risikoanalyser angis risiko som produktet av sannsynligheten for at hendelsen skal skje og konsekvensen av hendelsen: $\text{risiko}(x) = \text{sannsynlighet}(x) \cdot \text{konsekvens}(x)$. I risikoanalyser deles normalt konsekvens og sannsynlighet inn i ulike kategorier som gir grunnlag for gradering av risikonivå. Estimert av risikonivå danner igjen grunnlag for vurdering av tiltak for å redusere risiko.

I USA skal brudd på personvernet innenfor helsesektoren, som er regulert av Health Insurance Portability and Accountability Act (HIPAA)(1), rapporteres til U.S. Department of Health and Human Services, Office for Civil Rights. Hendelser som representerer brudd på denne loven og som omfatter flere enn 500 personer offentliggjøres i et bruddregister på bruddportalen til departementet(2).

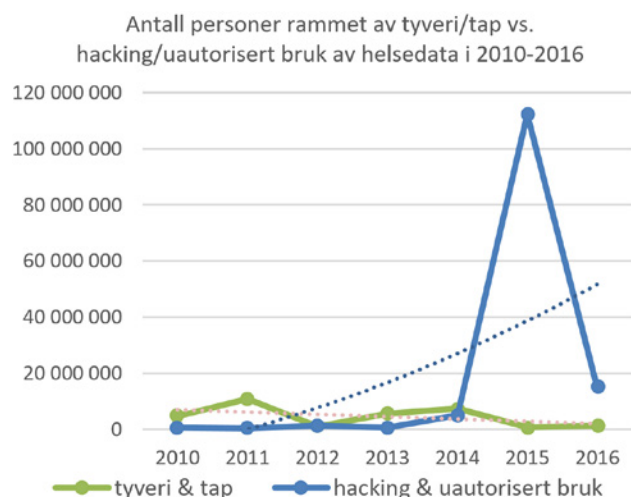
Ved Nasjonalt senter for e-helseforskning har man analysert innholdet i bruddregisteret for å kartlegge sannsynligheten for, og konsekvensen av de omfattende bruddene på informasjonssikkerheten i den amerikanske helsesektoren.

Funn

Ifølge registeret kan alle angrep på helserelaterte data grovt skilles i tre kategorier: 1) hacking og uautorisert bruk, 2) tap og tyveri, og 3) feilaktig bruk.

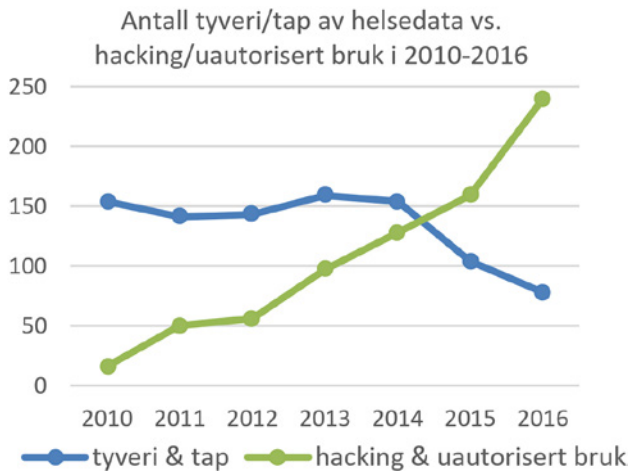
Ifølge data rapportert til registeret fra 1. januar 2010 til 31. desember 2016 ble helsedata for 171 074 016 personer eksponert. Selv om noen kan ha fått sine helsedata eksponert flere ganger eller ha helsedata i flere helseinstitusjoner(3), betyr dette at omtrent 54% av USAs befolkning på 318,9 millioner

- 79% av alle personvernbrudd på helserelaterte data i USA skyldes hacking eller uautorisert bruk.
- 19% av alle personvernbrudd på helserelaterte data i USA skyldes tap eller tyveri.
- 171 074 016 personer totalt ble rammet av brudd på helserelaterte data i perioden 2010-2016, noe som tilsvarer 54% av den amerikanske befolkningen.
- Ca. 4,6 millioner personer i gjennomsnitt rammes av tyveri eller tap av helserelaterte data årlig.
- Ca. 19,4 millioner personer i gjennomsnitt rammes av hacking eller uautorisert bruk av helserelaterte data årlig.
- Antall hackingangrep ble 15-doblet fra 2010 til 2016.
- 78,8 millioner er det største enkelttapet av pasientrelaterte data så langt.



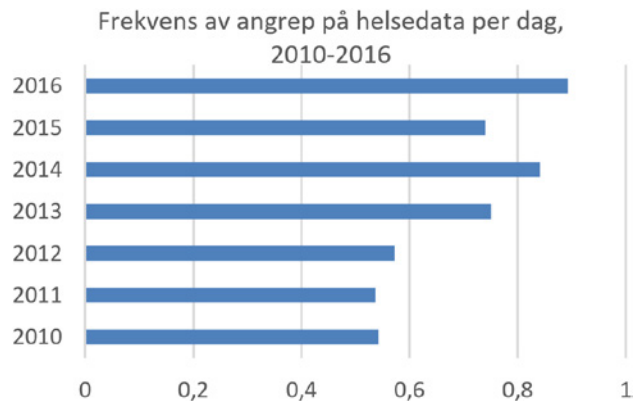
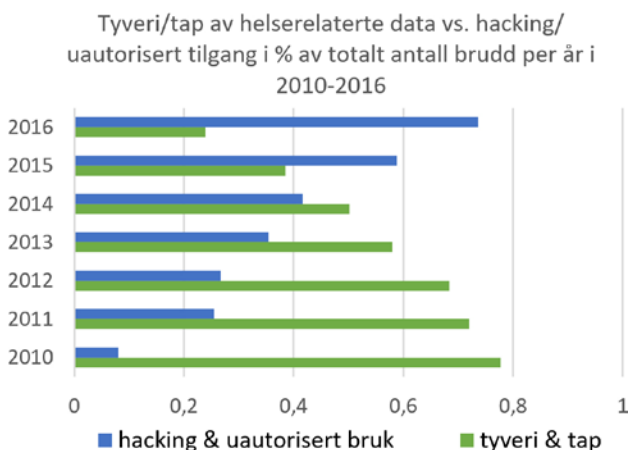
har vært utsatt for eksponering av sine medisinske data. Dette omfatter 135 775 362 personer som har vært rammet av hacking eller uautorisert bruk av helserelaterte data og 31 908 209 personer rammet av tyveri eller tap av helsedata i denne perioden. I gjennomsnitt ble helsedata for 19 396 480 personer årlig berørt av hacking eller uautorisert bruk, mot

4 558 316 personer som ble berørt av tyveri eller tap av helsedata. Dette betyr at det i perioden 2010 til og med 2016 var 4,26 ganger så stor sannsynlighet for å bli rammet av cybertyveri sammenlignet med fysisk tyveri.



Antall hendelser i kategorien hacking/uautorisert bruk økte fra 16 tilfeller i 2010 til 240 i 2016. I samme periode falt antall tilfeller av tyveri/tap fra 154 til 78. Som frekvensgrafen nederst viser, var gjennomsnittlig antall brudd per dag i USA i 2016 0,83. Det betyr at det i gjennomsnitt forekom brudd på personvernbestemmelsene oftere enn annenhver dag.

Den påfølgende grafen viser andeler av tyveri/tap og hacking/uautorisert bruk av helsedata i % av alle angrep på helserelaterte data årlig i perioden 2010-2016. Det er en jevnt økende trend for hacking og uautorisert bruk, og en nedadgående trend for tyveri/tap. I 2016 f.eks. var 10 ganger så mange personer omfattet av hacking/uautorisert bruk av helsedata sammenlignet med tyveri/tap.



Oppsummering

Gjennomgangen av USAs bruddregister viser at sannsynligheten for brudd er økende og nærmer seg i gjennomsnitt å bli en daglig hendelse. Omfanget eller konsekvensen av brudd viser også en økende trend. I sum betyr dette at risikoen for brudd på personvernlovgivingen for helsedata i USA er veldig høy og sterkt økende. I norske omgivelser ville en slik risiko kreve tiltak for å redusere både sannsynlighet for og konsekvensen av brudd. Omfanget av brudd på personvernlovgivningen skaper bekymring blant helsepersonell for at pasienter vil holde tilbake informasjon fra helsearbeidere, og dermed undergrave mulighetene til å forbedre helse og helsetjenester(4).

Referanser

- 45 CFR Parts 160 and 164. <https://www.hhs.gov/hipaa/for-professionals/privacy/>
- U.S. Department of Health and Human Services Office for Civil Rights. Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
- Liu V, Musen MA, Chou T. Data Breaches of Protected Health Information in the United States. JAMA. 14. april 2015;313(14):1471.
- Blumenthal D, McGraw D. Keeping personal health information safe: the importance of good data hygiene. JAMA. 14. april 2015;313(14):1424.

For mer informasjon, kontakt:

Johan Gustav Bellika, Professor
957 48 049
johan.gustav.bellika@ehealthresearch.no