Status på vores sektor
En trusselsvurdering
En risikovurdering
Et katalog af tiltag

V. Kurt Gammelgaard Nielsen

Formand for Danske Universiteters IT-sikkerhedsudvalg

Statsrevisorernes beretning nr. 8/2018 om universiteternes beskyttelse af forskningsdata.

1. Uddannelses- og Forskningsministeriets arbejde med at inddrage universiteternes implementering af ISO 27001 i det systematiske tilsyn
2. Uddannelses- og Forskningsministeriets arbejde med at etablere en tværgående trusselsvurdering for universiteterne
3. Resultatet af Uddannelses- og Forskningsministeriets bestræbelser i forhold til, at universiteterne får identificeret og rettet op på eventuelle kritiske it-sikkerhedsbrister.

Den overordnede trusselsvurderingen for den danske universitetsforskningssektor:

- Truslen fra cyberspionage mod den danske uddannelses-og forskningssektor er meget høj. Fremmede stater og kriminelle har stor interesse i at stjæle forskningsdata og intellektuel ejendom fra sektoren.
- Truslen fra cyberkriminalitet er meget høj. Det er muligt, at angreb fra cyberkriminelle kan forstyrre den daglige drift eller skade forskningsdata.
- Truslen fra cyberaktivisme er lav. Truslen er ofte motiveret af enkeltsager, og truslen mod sektoren kan derfor stige uden eller med kort varsel.
- Det er mindre sandsynligt, at fremmede stater vil rette destruktive cyberangreb mod dansk samfundsvigtig infrastruktur, herunder uddannelsessektoren.

Den overordnede trusselsvurderingen -2.del

- Insidertruslen mod uddannelses-og forskningssektoren er meget høj. Der er manglede awareness blandt forskere vedrørende truslen og konsekvenserne heraf, hvilket øger sandsynligheden for menneskelige fejl, uanset om disse er bevidste eller ubevidste.
- Truslen for fysiske forskningsdata er lav. Det er mindre sandsynligt at fysiske forskningsdata bliver udsat for destruktive angreb, og der er ikke registreret hændelser i denne kategori det senest år. Der er større sandsynlighed for at truslen udgøres af lokale fysiske eller miljømæssige trusler som brand, vand, natur eller forureningsskade samt tyveri, som der er registreret for det seneste år. Idet der ikke er en generel trussel mod sektorens fysiske forskningsdata, og der er få indrapporterede hændelser, vurderes truslen som lav.

Overordnet risikovurdering*

- Der er generelt en større risikoappetit i sektoren sammenlignet med andre sektorer med samme trusselsniveau.
- Universitetsforskningen er karakteriseret ved brede samarbejdsflader nationalt som internationalt, og det er af væsentlig betydning for forskningens fortsatte udvikling, at universiteterne fortsat kan fungere som åbne organisationer med mange samarbejdsrelationer, hyppige besøg af gæsteforskere mm.
- Sektoren har som helhed inden for rammerne af ISO27001 valgt en risikobaseret tilgang til valg af sikkerhedsforanstaltninger for forskningsdata. En risikobaseret tilgang skaber en optimering af forbruget af ressourcer samtidig med at det skaber et systematisk og gennemgående princip.
- *Baserer sig på internationale og nationale vurderinger, DKcert

Overordnet risikovurdering

- I forhold til den fysiske sikring af forskningsdata, så gør nogle af de samme forhold sig gældende. Der er en generel risikobaseret styring, således at sektorens bygningsmasse generelt er overvåget af ventilations, -varme-, køle- og brugsvandsanlæg (CTS), beskyttet med adgangskontrol (ADK), tyverianlæg (AIA) og branddetektionsanlæg.

- Inde i sektorens bygningsmasse er der generelt en fri adgang og et åbent miljø som anses som en forudsætning for universitetets forsknings- og undervisningsmiljø. Sektoren har dog principper for fysisk sikring, der typisk deler aktiviteterne op i nogle sikringszoner, gående fra en helt åben zone hvor studerende, ansatte og gæster kan færdes frit, til særlig kontor- og laboratorieområder som altid er aflåst og hvor adgang er overvåget og auditeret. Fysiske forskningsdata opbevares generelt kun i de særlige kontor- og laboratoromåder. Der er en accepteret restrisiko ved at adgang typisk ikke auditeres, og der i mange lokaler er adgang for forskningsmiljøets ansatte, gæster og studerende.

Katalog af mitigerende foranstaltning

- Forskeres rettigheder som lokaladministratorer.
- *Alle universiteter tillader forskere rettigheder som lokaladministratorer, hvilket betyder, at de selv kan installere software og har ansvar for at sikkerhedsopdatere. Dette kan, ifølge Rigsrevisionen, give et efterslæb på sikkerhedsopdatering af software. Rigsrevisionen bemærker, at hver enkelt forsker som har lokaladministratorrettigheder udgør en risiko for både sin egen og de øvrige forskeres it-sikkerhed. Tildelingen af lokaladministratorrettigheder bør derfor afgrænses til et konkret behov og kort tidsinterval.*

- Sektoren har påbegyndt mitigerende foranstaltninger som fra en centralt styret politik styrer installering af software og sikkerhedsopdateringer. Det er forskelligt hvordan de enkelte institutioner har valgt den konkrete implementering, men generelt er det en blanding af forhåndsgodkender/whitelister muligheden for at installere software samt reduktion af at brugerne ikke er permanent lokaladministratorer, men tildeles rettighederne efter behov og i et begrænset tidsrum.

Ukendt hardware på universiteternes netværk og politikker vedr. bring your own device.

- *Flere universiteter tilbyder forskerne, at de selv kan medbringe, anskaffe og tilslutte it-udstyr på universitetets netværk. Dette kan, ifølge Rigsrevisionen, udgøre en sikkerhedsmæssig risiko, hvis det ikke sikkerhedsopdateres. Rigsrevisionen vurderer, at det ikke er muligt at have en tilstrækkelig it-sikkerhed og løbende overblik over sikkerhedshændelser, hvis der ikke er overblik over det anvende it-udstyr.*

- Sektoren har segmenteret de interne netværk og er påbegyndt udrulning af den anbefalede tekniske standard (802.1x) som styrer udstyrs adgang til netværket.
- Sektoren har stort fokus på it-udstyr som ikke kan sikkerhedsopdateres. Dette udstyr bliver forsøgt udfaset, men hvis det ikke kan lade sig gøre så opsættes mitigerende foranstaltninger således at udstyr kun er tilgængeligt på lukket netværk.
- Nogle institutioner er også påbegyndt microsegmentering som isolerer den enkelte server indenfor det samme netværkssegment. For begge løsninger gælder at man fra en risikobaseret betragtning kan fastholde et brugbart instrument samtidig med at man ikke udsætter forskningsapparatet for cyberangreb.

Ansvar fra centralt hold

- Sektoren har fastsat ansvaret for beskyttelse af forskningsdata. Der er for de enkelte institutioner valgt forskellige politikker, men der er ledelsesmæssigt vedtaget og gennemført oplysningsindsatser overfor forskerne.

Næste skridt

- Udarbejde et katalog af tiltag