BLOG | Kim Tiedemann

EMNER *Digital forvaltning, Digitalisering, Offentlig it, Sikkerhedshuller*

Vi trykker enter - og så kører det...

Af Kim Bjørn Tiedemann 18. december 2014 kl. 11:36

Regeringen præsenterede den nye digitale strategi for cyber- og IT sikkerhed (http://www.fmn.dk/nyheder/Documents/National-strategi-for-cyber-og-informationssikkerhed.pdf) . Efter at have læst den igennem må jeg konstatere, at der ikke er meget nyt under solen - specielt ikke for leverandører.

Klare krav til leverandøren

I afsnit 3.0 beskrives hvorledes der skal stilles klare krav til leverandører i forbindelse med fx outsourcing af IT drift. Strategien beskriver 2 initiativer, som skal sikre, at der stilles krav til leverandørerne, samt at myndighederne løbende følger op på sikkerheden hos leverandøren.

Initiativ 7- Sikkerhedsmæssige krav i udbud og ved indgåelse af kontrakter på it-området

I de offentlige kontrakter og udbud, som jeg har læst, har der allerede været krav om overholdelse af ISO27001 eller lignende sikkerhedsstandarder. Men krav gør det ikke alene. Jeg er sikker på, at der har været lignende krav hos de leverandører, hvor vi har set datalæk eller decideret hacking (http://www.version2.dk/interaktiv/csctidslinje) .

Opfyldelse af sikkerhedskrav er, i modsætning til funktionelle krav, svære at teste. En lille bitte kode- eller konfigurationsfejl (https://www.imperialviolet.org/2014/02/22/applebug.html) kan kompromittere hele løsningen, og disse fejl er yderst svære at finde ved almindelige penetrationstest. På mange af de projekter, som jeg har været involveret i, så blev sikkerhedskravene kun kontrolleret ved, at der blev foretaget et eksternt sikkerhedsreview og en penetrationstest. Hvis dette var positivt, så blev boksen afkrydset, og alt var herefter fint.

Initiativ 8 - Løbende opfølgning på den sikkerhedsmæssige leverandørstyring

Igen er der allerede i offentlige kontrakter mulighed for, at myndighederne kan lave audits af leverandørens sikkerhedspolitik samt implementeringen i form af deres sikkerhedssystem. Det nye er dog, at det nu centraliseres, og Digitaliseringsstyrelsen nu skal følge op på, om myndighederne efterlever disse audits.

Forslag til andre initiativer

Jeg mener ikke, at ovenstående gør den store forskel i forhold til, hvad vi allerede har. Det er ikke nok at stille krav til leverandøren og efterfølgende følg op. Det er selvfølgeligt meget bekvemt, at man efterfølgende kan pege på en leverandør og sige, "vi har sagt, I skal gøre det", men det øger ikke sikkerheden. Det øger heller ikke sikkerheden, at man laver kontrol af kontrollen, hvis det ikke har en konsekvens at bryde sikkerhedssystemet.

Jeg foreslår derfor, at man ved etablering af et nyt projekt eller en ny driftsutsourcing også etablerer en sikkerhedsorganisation, som består af repræsentanter fra myndighed og leverandøren. Begge parter har som henholdsvis databehandler og dataansvarlig en

et projekt, men i stedet for at sikre fremdriften for et projekt, så rhold til plan og økonomi. Gruppen skal bestå af ledelsen fra myndighed og virksomhed, således at ansvaret placeres højt nok oppe i organisationerne til, at der kan træffes nødvendige beslutninger.

Medicinalindustrien kunne være et udemærket sted at lære fra, når man ønsker at følge op på leverandørens (og myndighedernes) efterlevelse af sikkerhedspolitikken. Medicinalbranchen er dødsensangste for FDA audits, fordi FDA har autoriteten til at lukke produktionen af et lægemiddel og dermed stoppe for en milliardomsætning. Lignende bemyndigelse kunne man indføre på IT sikkerhedsområdet, således at leverandører og myndigheder bliver tvunget til, at tage sikkerhedsområdet alvorligt. Man kunne også overveje, at gøre antallet af succesfulde sikkerhedsaudits en del af offentlige lederes KPI.

Det er dog ikke gratis for myndighederne, når sikkerheden skal prioriteres højere. Når der til medicinalindustrien udvikles GxP compliant IT systemer (http://en.wikipedia.org/wiki/GxP#Consequences_of_GxP_for_information_technology) , så er der et ikke ubetydeligt overhead for at sikre, at systemet lever op kravene. Det samme vil gøre sig gældende for IT systemer til det offentlige.

Andre forslag

Man bør indføre en ordning, hvor det er muligt at indrapportere sikkerhedshændelser, som man er blevet opmærksom på. Det kunne fx være, at man har opdaget et sikkerhedshul i en offentlig løsning. Det bør være muligt at indrapportere anonymt og dermed give mulighed for en whistleblower-ordning, hvor offentlige ansatte eller ansatte hos leverandører har mulighed for, at informere om kritisable forhold.

Derudover bør man indføre et centralt register over sikkerhedshændelser, som selvfølgelig er blevet rettet, men så det dokumenteres hvilke hændelser der har været. Public shaming vil give et klart incitament til at rette op på eventuelle sikkerhedsproblemer.

Der er lang vej fra regeringen har trykket enter og til at det kører...

Om Kim Bjørn Tiedemann

Kim er udviklingschef hos Schultz og arbejder også som løsningsarkitekt og scrum coach. Han har arbejdet med agil udvikling de seneste 5 år, teknologi er hans store passion, og i sin fritid koder han på en Windows 8-app. Han er uddannet i datalogi fra AAU.

Følg @kimtiede 124 følgere