OPENBAAR
Tweede Kamer
t.a.v. Parlementaire werkgroep ICT-projecten bij de overheid

Delft, 28 mei 2012

Bijdrage van Fox-IT / Ronald Prins t.b.v. parlementair onderzoek n.a.v. ICT-problemen bij de overheid
1 juni 2012

Inleiding

Fox-IT is een bedrijf dat gespecialiseerd is ICT-Security problematiek. Wij worden typisch ingehuurd op het moment dat de veiligheid gefaald heeft, en door organisaties die meer dan gemiddeld zich realiseren dat ICT security voor hun organisatie belangrijk is.
Onze bijdrage zal zich merendeels beperken tot privacy en veiligheidsaspecten van ICT-projecten.

Tav het onderzoeksvoorstel

U geeft aan de gestelde onderzoeksvragen per project te bestuderen. Ik zou graag meegeven om ook mee te nemen hoe nationale initiatieven op cyber security gebied een actieve bijdrage kunnen leveren aan veiligere ICT projecten. Denk daarbij bijvoorbeeld aan een mandaat voor het Nationaal Cyber Security Centrum, de invloed van meldplicht(en) op publieke organisaties, etc.

Zienswijze op het onderwerp

Uw onderzoeksvoorstel is binnen Fox-IT verspreid. Diverse medewerkers hebben hun reactie gegeven op basis van hun eigen ervaringen. Hieronder een bloemlezing van een aantal (anekdotische) reacties in willekeurige volgorde. Mogelijk komen ze soms (onbedoeld) generaliserend over.

1. Door gebrek aan inhoudelijke kennis bij het inkoopproces wordt vooral gestuurd op kosten. Voorzover veiligheidselementen al relevant zijn, wordt vooral gesproken over de beschikbaarheid van systemen en niet confidentialiteit er van (geheimhouding). Beschikbaarheid is immers eenvoudig uit te drukken in getallen, en daarmee een goed control mechanisme tussen opdrachtgever en leverancier. De niet-hackbaarheid is veel moeilijker te definiëren en wordt vooral afgedaan met de aanwezigheid van een aantal beveiligingsmechanismen zonder daarbij de werkelijke toegevoegde waarde daarvan te kunnen beoordelen. De drang om beschikbaarheid zo goed mogelijk te doen werkt daarnaast ook de “niet-hackbaarheid” tegen. Immers het up-to-date houden van een systeem gaat gepaard met downtime. Kortom overheidsinkopers zijn in de regel niet in staat “veilige” systemen te verwerven.

2. Het domein van bescherming van staatsgeheimen en dep. vertrouwelijke gegevens wordt beschreven in het VIR-BI (Voorschrift Rijksoverheid - bescherming bijzondere informatie). De formele eisen hierin beschreven zijn erg sterk. Voor veel behoeften zijn er geen producten en ontwerpen die daar aan voldoen. Er zijn geen aanbevelingen voor het beste alternatief waardoor organisaties vaak niet weten wat ze er mee moeten en deze eisen dan maar negeren en daarmee apparatuur aanschaffen met een veiligheidsniveau ver onder een acceptabel niveau. In de praktijk merk je als land daar direct niet veel van omdat dit een kwetsbaarheid is die vooral door inlichtingendiensten wordt uitgebuit. Hun succes worden zelden breed uitgemeten.

3. (politieke) tijdsdruk van projecten hebben tot gevolg dat concessies worden gedaan aan de beveiligingsmaatregelen zonder te kijken naar de security impact.

4. Overschat vertrouwen in de claims van security leveranciers. Vooral in het VIR-BI domein kunnen kosten behoorlijk oplopen waardoor vaak een “niet goedgekeurd” product gekozen wordt. Pas bij een penetratietest blijkt dat het gekozen alternatief inderdaad niet voldoet aan de gestelde eisen, waarna

FOX-IT BV
Olof Palmestraat 6, Delft
POSTBUS 638, 2600 AP Delft
T +31 (0)15 284 79 99
F +31 (0)15 284 79 90
ABN AMRO 554697041
KVK Haaglanden 27301624

alsnog de duurdere oplossing geïmplementeerd moet worden.

5. tav juridische aspecten rondom privacy. Privacyaspecten worden vaak vergeten bij het design. Op de kosten voor de formele zaken die daarbij geregeld moeten wordt zelfs zodanig bezuinigd dat daar liever adviseurs opgezet worden dan juristen van een gerenommeerd bureau. Ook waarbij juridisch advies minder dan 0,1% zou kosten van de ict kosten van het project.

6. vasthouden aan ouderwets projectmatig werken. Door de lange doorlooptijd van ICT projecten verandert de omgeving soms significant tijdens een project. De nieuwe omgeving (nieuwe techniek, nieuwe dreigingen) maken het dat in het project dan andere keuzes gemaakt moeten worden onderweg. Stuurgroepen blokkeren dit vaak. “Zo hebben we het afgesproken, zo zal het gebeuren ook”

7. Liever iets maken dat werkt, dan iets goeds. Doordat medewerkers van leveranciers vaak tijdelijk betrokken zijn bij een project zijn ze erg gericht op het ‘oplevermoment’. Extra kwaliteit (voorzorgsmaatregelen om incidenten tegen te gaan) krijgen daardoor minder aandacht dan als die personen zelf nog verantwoordelijk zouden zijn voor het product tijdens het daadwerkelijk gebruik.

8. De genoemde problemen komen zowel in het bedrijfsleven als bij de overheid voor. Desondanks lijkt binnen het bedrijfsleven dankzij concurrentie steeds meer het besef te komen dat ze IT security goed geregeld moet zijn. Banken en mobiele operators willen niet dat consumenten overstappen. Daardoor wordt security langzaam aan meer een strategisch element voor bedrijven. Binnen de overheid ontbreekt deze “concurrentie prikkel”.

9. Gebrek aan kennis op alle fronten. Zowel bij ICT leveranciers, ICT security bedrijven, inkopers, en gebruikers.

10. Centrale ICT systemen (GBA, EPD) worden vaak via decentrale partijen ontsloten. Deze decentrale partijen wordt veel vrijheid geboden aan de invulling van hun eigen systemen. Daarmee worden heel veel verschillende sloten aan een dezelfde kluis verbonden. Honderden organisaties moeten proberen deze sloten veilig te houden, maar de hacker hoeft er maar een te vinden die hij open krijgt. Gezien de schaarsheid van security expertise bij al deze organisaties lijkt dit niet de juiste weg om te bewandelen.

Tot zover onze opmerkingen. We beseffen ons dat ze erg gericht zijn op het aanwijzen van oorzaken en daarmee hooguit een indirecte oplossingsrichting schetsen. Mogelijk dat u verderop in uw onderzoek nog over de oplossingszijde wilt discussiëren.

Met vriendelijke groet,

Ronald Prins