Questafette

`Vakmanschap van overwegend belang binnen informatiebeveiliging'

Informatiebeveiliging, nr. 6, nov. 2004, p.4-5.
<http://www.gvib.nl/infobev/informatiebeveiliging.htm>

Naam:
Bart Jacobs

Beroep:
Hoogleraar beveiliging en correctheid van programmatuur

Werkzaam bij:
Radboud Universiteit Nijmegen

Ervaring met informatiebeveiliging sinds:
1998.

Vindt ten aanzien van de stelling
'Informatiebeveiliging is vakmanschap, geen wetenschap':

"Goed academisch gebruik vraagt allereerst om een analyse van de betekenis van de begrippen die in de stelling voorkomen. Een filosofische discussie over wat er precies verstaan dient te worden onder `wetenschap' gaat hier waarschijnlijk iets te ver, maar een nadere duiding van `informatiebeveiliging' lijkt wel op z'n plaats. Gaat het hier om informatiebeveiliging als discipline of als activiteit? Vooralsnog is dat onduidelijk. Daarnaast is het goed even stil te staan bij de retoriek. Waarschijnlijk poogt de stellingnemer enige spanning te creeren via de impliciete aanname dat ondergetekende, als academicus, waarschijnlijk een zo groot mogelijke bereik voor de wetenschap wil claimen. Die aanvechting is mij echter vreemd. Tevens zou men met een kwaadwillend gemoed in de stelling kunnen lezen dat wetenschap geen vakmanschap zou behelsen. Deze enigszins gezochte interpretatie wil ik echter volledig negeren.

De discipline-aanduiding informatiebeveiliging wordt soms gebruikt als alomvattend alternatief voor computerbeveiliging of computer security. Dat het hier niet om wetenschap zou gaan is evident onjuist. Veel van de basistechnieken en protocollen van het vakgebied (zoals RSA of Kerberos) zijn in de wetenschappelijke wereld onstaan.

Is informatiebeveiliging als activiteit dan de juiste interpretatie? Het lijkt zo te zijn. Voordat de prangende vraag of het hier gaat om vakmanschap of wetenschap zinvol beantwoord kan worden lijkt ook nu een nadere analyse van deze activiteit gepast. Mijn favoriete omschrijving van computerbeveiliging is: regulating access to assets. Bij dit reguleren onderscheid men idealiter de volgende vijf fasen.

1. Opstellen van een security policy. Hierbij brengt men nauwkeurig in kaart wat de `assets' zijn die beveiliging vereisen en wie daar (op welk moment, vanwaaruit, met welke handelingen) toegang toe zou mogen hebben. In grote lijnen gaat het hierbij om het nauwkeurig opstellen van een grote toegangsmatrix, volledig los van een implementatie mbv. specifieke beveiligingstechnieken. Bij dit opstellen is een scherpe blik en open houding nodig. Het is belangrijk, maar enigszins saai werk, waarbij het mij lijkt dat enige vorm van vakmanschap (speciaal ervaring) van belang is, maar dat een beroep op creatieve wetenschappelijke vermogens niet direct noodzakelijk is.

2. Uitvoeren van een bedreigingsanalyse. In deze fase probeert men de

mogelijke aanvallers en hun strategieen te identificeren, nog steeds op zo abstract mogelijk niveau. Weer gaat het vooral om ervaring, en ondermijnend inlevingsvermogen. Bij dat laatste is enige creativiteit wel nuttig, maar niet in wetenschappelijk opbouwende zin.

3. Ontwerpen van een security architectuur. Deze architectuur moet niet alleen recht doen aan de bovengenoemde security policy, maar ook de geidentificeerde bedreigingen het hoofd kunnen bieden. Vaak zal vakmanschap in deze fase voldoende zijn voor het gebruik van bekende technieken, maar mogelijk dient een geheel nieuwe architectuur met eigen protocollen ontworpen te worden. In dat geval is meer dan alleen vakmanschap vereist. Het komt dan aan op een wetenschappelijke aanpak, waarin creativiteit, bekendheid met de laatste inzichten in de literatuur, en een analytische houding van doorslaggevend belang zijn voor succes.

4. Implementatie van de architectuur. Hierbij gaat het vooral om vakmanschap, met passende inzet van bewezen cryptografische technieken in veilige protocollen. Nauwkeurigheid is bij implementatie van groot belang, zodat de gehele beveiligingsinfrastructuur uiteindelijk niet gecompromitteerd kan worden door bijv. een onbenullige buffer overflow.

5. Certificatie door een onafhankelijke derde partij. Hierbij kan het gaan om een spectrum van activiteiten, op verschillende niveaus. Bijvoorbeeld in de Common Criteria standaard bestaan er zeven ``evaluation assurance levels'' EAL1 -- EAL7. Op het laagste niveau gaat het vooral om het nalopen van een aantal formele eisen, maar op de hoogste twee niveaus is het gebruik van formele (wiskundige) methoden vereist om adequate beveiliging vast te stellen. Het gebruik van zulke methoden is onderwerp van intensief wetenschappelijk onderzoek, waarbij de aansluiting op de praktijk vooralsnog moeizaam is. Inderdaad zijn certificaties op zulke hoge niveaus zeldzaam, en beperken ze zich vooral tot een militaire context. Ik zie het als een van de grote uitdagingen voor het vakgebied om de kloof tussen de praktijk van het braaf nalopen van checklists en de theorie van abstracte security logica's te verkleinen. Wanneer dergelijke wetenschappelijke theorieen hun nut eenmaal bewezen hebben, kunnen ze worden vastgelegd in tools, die met vakmanschap gebruikt kunnen worden. Het gaat dan niet langer om nieuwe, maar om bestaande, techniek.

Samenvattend is voor informatiebeveiliging (als activiteit) vakmanschap van overwegend belang. Wetenschappelijke methoden zijn vooral relevant in ontwerp en certificatie, maar zijn op het laatste gebied vooralsnog onvoldoende ontwikkeld om direct aan te sluiten bij de complexiteit van de huidige praktijk. Ik zie dit vooral als een uitdaging in een jong vakgebied, en meen dat inspanningen en een open houding van twee kanten---theorie en praktijk---noodzakelijk zijn om deze kloof te kunnen dichten."

Geeft estafettestokje door aan:
Maurice Wessling van Bits of Freedom

Met de stelling:
De in opkomst zijnde sterke authenticatiemiddelen (zoals het paspoort met biometrie) zijn goed voor de burger omdat hiermee het risico van identiteitsfraude afneemt.