

Sentinels-event: verslag workshop A

Pascal van Eck

1 Deelnemers

De volgende personen hebben deelgenomen aan de workshop:

- J. van den Bosch (KPN): eerste spreker
- J. Akkerhuis (NLnet Labs): tweede spreker
- M. Dasselaar (SenterNovem): moderator
- P. van Eck (Universiteit Twente): rapporteur
- E. Luijff (TNO Defensie en Veiligheid)
- P. Veugen (TNO ICT)
- R. Staallekker (IBM Nederland B.V.)
- W. Segeth (STW)
- H. Meeuwissen (Lucent Technologies)
- M. Lagerberg (Lucent Technologies)
- J. van Ginkel (Universiteit van Amsterdam)
- H. Bos (Vrije Universiteit Amsterdam)
- P. van Rossum (Radboud Universiteit Nijmegen)
- S. Mauw (TU Eindhoven)
- P. de Jager (TNO ICT)
- P. Hartel (Universiteit Twente)
- A. Haccou (KPN)
- A.W. Duthler (Duthler Associates)

2 Structuur workshop

De workshop bestond uit twee delen:

- Deel 1 (voor de lunch): presentaties van de heren J. van den Bosch (KPN) en J. Akkerhuis (NLnet Labs). Van dit deel is geen verslag gemaakt; voor de inhoud van deze presentaties wordt verwezen naar de slides.
- Deel 2 (na de lunch): discussie met als doel het vinden van onderzoeksvragen voor toekomstige Sentinels-projecten, plenair te presenteren middels een korte presentatie na afloop van de workshop.

3 Verslag deel 2 (discussie)

De discussie werd ingeleid met een vraag n.a.v. de presentaties die tijdens deel 1 van de workshop gegeven waren. Deze vraag was gericht aan in het bijzonder de presentatoren maar in het algemeen aan de aanwezige vertegenwoordigers van het bedrijfsleven en luidde: aan welke methodes, technieken en gereedschappen heeft het bedrijfsleven behoefte bij het uitvoeren van projecten op het gebied van IT-beveiliging? De rationale achter deze vraag is dat het bedrijfsleven in het algemeen succesvol is in het oplossen van beveiligingsproblemen van alledag, maar dat dat wellicht efficiënter en effectiever kan met nieuwe methodes, technieken en gereedschappen. Het ontwikkelen van dergelijke methodes, technieken en gereedschappen is een natuurlijke bezigheid voor de academische wereld.

Vanuit deze vraagstelling werden gedurende deel 2 van de workshop een drietal onderwerpen besproken:

- Het ontwikkelen van een algemeen kader waarin de nu nog onbekende “bedreigingen van morgen” geanalyseerd kunnen worden.
- Inventarisatie van fundamentele problemen in de huidige IT-infrastructuur: deze inventarisatie werd gezien als meer fundamenteel dan een inventarisatie van huidige bedreigingen: huidige bedreigingen maken gebruik van de fundamentele problemen.
- De “echte kansen”: waar liggen mogelijkheden om zinvol onderzoek te doen.

3.1 Algemeen kader

Geconstateerd werd dat het inventariseren van huidige bedreigingen nuttig is, maar dat het veel belangrijker is om over algemene kennis, methoden en technieken te beschikken waarmee gereageerd kan worden op de (nu nog onbekende) bedreigingen van (over)morgen. Er is een “algemeen kader” nodig waarmee de bedreigingen van morgen geanalyseerd kunnen worden. Randvoorwaarden hiervoor zijn:

- Het kader moet snel, flexibel en goedkoop zijn.
- Er is een spanningsveld tussen enerzijds snel, flexibel en goedkoop en anderzijds goede bescherming. Het kader moet de benodigde afwegingen in dit spanningsveld expliciet maken, bijv. via risico-analyse.
- Het kader moet van toepassing zijn op zowel producten als protocollen en moet analyse van continue beschikbaarheid (24x7) ondersteunen.

Er werd voorgesteld om het kader zo op te stellen dat afwegingen in het genoemde spanningsveld gekoppeld worden aan het onderliggende *business model* van het product of dienst.

De discussie werd concreter gemaakt door een plan voor te stellen om tot een dergelijk kader te komen:

- Als eerste wordt het kader ontwikkeld gebaseerd op scenarios.
- Daarna wordt dit ingevuld voor het security-domein.
- Het uiteindelijke doel is om met dit kader devices, netwerkarchitecturen en –topologieën te kunnen testen. Als laatste stap in de ontwikkeling kan dit voor een aantal voorbeelden gedaan worden.

3.2 Inventarisatie fundamentele problemen

De volgende fundamentele problemen werden genoemd:

- Het fundament van het Internet rammelt. Dit maakt zaken als *DNS spoofing* mogelijk. Voor een aantal rammelende onderdelen zijn oplossingen voorhanden, maar die worden vaak slecht of helemaal niet in gebruik genomen.
- We hebben te maken met *zero-day exploits*: het tijdstip waarop een beveiligingslek bekend raakt valt zo goed als samen met het tijdstip waarop voor het eerst misbruik van dit lek gemaakt wordt. Dat betekent dat er geen ruimte meer is voor de traditionele aanpak (ingrijpen door systeembeheerders).
- Er is zowel vraag naar het beschermen van privacy op het Internet als het openstellen van de infrastructuur, bijv. voor terrorismebestrijding en forensisch onderzoek. Deze twee zaken lijken elkaar volledig tegen te spreken; dit roept om een nieuw aandachtsgebied dat we “contradictiemanagement” noemen.
- Er is grote behoefte aan benchmarks, tests en testomgevingen.

3.3 Echte kansen

In de voorgaande paragraaf zijn fundamentele problemen in de huidige IT-infrastructuur geïnventariseerd. Het ligt voor de hand aan te nemen dat kansen voor Sentinels-onderzoek liggen op het vlak van het oplossen van die problemen. Het is echter niet realistisch om aan te nemen dat in het kader van een onderzoeksproject zomaar de huidige, wereldwijde infrastructuur aangepast kan worden. Daar liggen dus geen kansen. Kansen zijn er wel op de volgende gebieden:

- Secure overlays. Het fundament van het Internet kan niet (makkelijk) aangepast worden, maar er kan wel een betere laag bovenop gelegd worden. Er zijn kansen voor Sentinels om aan te sluiten bij het ontwikkelen van die laag. Een voorbeeld van zo’n secure overlay is VPN. Een mogelijke andere functionaliteit van zo’n laag is verkeersprioritering in het geval van uitval van een significant deel van de normale bandbreedte.

- Er zijn ook kansen in gebieden waar veel minder sprake is van een gevestigd fundament. Gedacht kan worden aan allerlei protocollen die nog ontwikkeld moeten worden voor nieuwe vormen van wireless communication. Sentinels kan hierbij aansluiten.
- Er zijn kansen op het gebied van het detecteren en isoleren “bad guys”.
- De vitale infrastructuur in Nederland voor zaken als de energievoorziening wordt meer en meer digitaal bestuurd. Er zijn kansen op het gebied van het ontwikkelen van veilige monitoring en besturing van deze infrastructuur.

4 Afsluiting

Besloten werd om tijdens de plenaire presentatie alleen in te gaan op de onderwerpen genoemd bij 3.2 en 3.1 (in die volgorde). De geïnventariseerde “echte kansen” (3.3) werden uiteindelijk beschouwd als te weinig precies en te weinig concreet.

Er werd ook geïnventariseerd wie bereid is om aan de bediscussieerde onderwerpen verder te werken. Besloten werd om op een termijn van ong. 1 maand verder te praten over deze onderwerpen; KPN bood aan om als gastheer op te treden.