

JOOP BAUTZ INFORMATION SECURITY AWARD JURY RAPPORT 2014

De Jury van de Joop Bautz Information Security Award 2014 is na ampel beraad tot de eenstemmige conclusie gekomen dat zij voor de Joop Bautz Information Security Award 2014 nomineert:

Stef Schinagl en Keith Schoon

voor hun werkstuk getiteld:

"Security Operations Center, Modelleren en meten van effectiviteit" ¹

De Jury overweegt hierbij het volgende:

In 2014 werd het voor de dertiende maal mogelijk om kandidaten voor te dragen voor de Joop Bautz Information Security Award, een prijs ingesteld door 3 instituten, actief op het gebied van informatiebeveiliging in Nederland (PvIB, ISACA en NOREA).

De toetsingscriteria hiervoor luiden:

- **Theoretische diepgang:** bronnengebruik, diepgang, aanpak, presentatie, nauwkeurigheid
- **Praktische Relevantie:** originaliteit, effectiviteit & efficiency, "zitten we er op te wachten"
- **Vernieuwing:** originaliteit, gemak, vernieuwend
- **Toepasbaarheid:** maatschappelijk draagvlak, kostenfactoren, werkingsfeer, acceptatie

Na bestudering van de in totaal 10 voordrachten heeft de jury er 3 genomineerd, waaronder de voordracht van de heren Schinagl en Schoon. De Jury overweegt daarbij het volgende.

Elke moderne werkorganisatie (overheid of niet) worstelt met de vraag hoe de eigen IT infrastructuur en daarmee vitale belangen van burgers en klanten beschermd moeten worden tegen bedreigingen, intern dan wel extern. De afkorting SOC voor Security Operations Centre is het nieuwe buzzword om activiteiten aan te duiden die elke organisatie uitvoert bij beheersing van bekende en onbekende IT gebonden risico's. Schinagl en Schoon hebben met frisse blik dit uitermate woelige gebied in kaart gebracht in hun afstudeerwerkstuk (als bij product van een daadwerkelijke onderzoeksopdracht voor de Rijksoverheid). De druk vanuit de werkorganisaties enerzijds, de krapte van de budgetten voor IT beveiliging anderzijds maakten dat de overheid als sponsor wilde weten wat de standaarden zijn waaraan zo'n SOC behoort te voldoen. Gegroeide afhankelijkheden gecombineerd met ernstige incidenten (Diginotar voorop, maar denk ook aan het platleggen van IDEAL en DigiD) vormden de voedingsbodem voor de studie van Schinagl en Schoon. In hun werkstuk beschrijven zij hoe een SOC eruit pleegt te zien, aan welke eisen bemensing en instrumentatie moet worden voldaan maar vooral ook dat er geen panacee "textbook" SOC denkbaar is: elke organisatie zal op eigen wijze het SOC concept inhoud moeten geven en daarbij keuzes moeten maken. Hun onderzoek leverde nieuwe inzichten op, die vooral liggen op het raakvlak tussen IT levering en afname. Middels dit type beoordeling krijgt de betrokken organisatie een spiegel voorgehouden, die – zoals de spiegel uit het sprookje – een realistisch beeld geeft van de eigen status. Vooral gericht op de vraag: hoe effectief is dit allemaal en krijg ik waar voor mijn geld.

De Jury beoordeelde het werkstuk als potentieel prijswinnend op de criteria van de Award. De Jury overwoog daarbij dat beide auteurs het concept SOC uitstekend in kaart hebben gebracht, ontdaan van de hype, met de nodige aandacht voor de praktische aspecten.

Kortom, het betreft een goed onderbouwd werkstuk over een actueel thema met hoge maatschappelijke relevantie, met een aantal vernieuwende inzichten, te nomineren als mogelijk winnaar van de Award.

De Jury van de Joop Bautz Information Security Award 2014,

Mr. P. van Dijken (voorzitter)

ing. K.F. Rorive MSc CISSP CISA CISM (secretaris)

¹) Afstudeeronderzoek Vrije Universiteit Amsterdam, PGO IT Audit Compliance & Advisory, begeleiding Prof.dr.ir. Ronald Paans RE en Jerry Fasten BEc RE QSA CISA. Prof. Paans is lid van de Joop Bautz Jury, heeft geen aandeel gehad in de beoordeling van de Jury van dit werkstuk.