Rijksdienst voor Ondernemend Nederland

Samenvatting SBIR-winnaars 2e fase tender SBIR Cyber Security II

Intrinsic-ID, Innovalor, Coblue, IC3D Media, Digital Intelligence Group en Ziuz Forensics krijgen de kans om hun voorstellen voor het vergroten van de digitale veiligheid in Nederland verder uit te werken tot een prototype. In het kader van SBIR Cyber Security II geeft het ministerie van Economische Zaken deze zes winnende ondernemers van de 2e fase tender 1,5 jaar de tijd en een budget van maximaal 2 ton mee.

Lees hieronder een samenvatting van de zes SBIR-winnaars van Cyber Security II.

Lees ook het nieuwsbericht 6 SBIR-Winnaars voor Cyber Security II onderzoek.

Intrinsic ID: project BYOS (SBIR15C028)

Het beoogde product is een smartphone die fungeert als een universeel toestel voor twee-factorauthenticatie: phone as a token. Het R&D-traject omvat samenwerking met smartphone fabrikanten voor de integratie van innovatieve PUF technologie* van Intrinsic-ID in nieuwe smartphones. Voor smartphones zonder deze technologie worden cloud services gecombineerd met intrinsieke karakteristieken van de smartphone om een sterke sleutel te genereren. Softwareontwikkelaars kunnen de SDK** gebruiken om veilige apps te ontwikkelen voor deze toestellen. Toepassingen zijn o.a. veilige toegang tot clouddiensten en bedrijfsnetwerken, elektronisch betalen en bankieren, en authenticatie in het algemeen. Het project sluit aan op het onderzoeksthema Management van identiteit, privacy en vertrouwen van de NCSRA-II*. Intrinsic-ID komt voort uit het voormalige Natlab van Philips.

**PUF = Physically Unclonable Function (dit is de "fingerprint" van de chip)*

***SDK = Software Development Kit*

**** National Cyber Security Research Agenda II*

Innovalor: project mobiele app voor identiteitsvaststelling (SBIR15C048)

Identiteitsdocumenten bevatten een chip als één van de echtheidskenmerken. Smartphones hebben steeds vaker Near Field Communication (NFC) technologie waarmee deze chips contactloos uitgelezen kunnen worden. Dit project leidt tot een prototype voor mobiele software die van een NFC-capable smartphone een mobiel, gebruikersvriendelijk en relatief goedkoop apparaat maakt om de echtheid van identiteitsdocumenten te verifiëren, attributen uit te lezen en gezichtsherkenning te doen. Deze software kan toegepast worden in situaties waarbij gebruikers online hun eigen identiteit moeten aantonen, bijvoorbeeld bij het openen van een bankrekening. Het project sluit aan op het thema 'Identity, privacy, and trust management' van de NCSRA-II onderzoeksagenda. InnoValor komt voort uit het voormalige Novay / Telematica Instituut en werkt samen met de Universiteit Twente.

Coblue: Cryptovaluta-inlichtingen (SBIR15C021)

Het gebruik van cryptovaluta – zoals Bitcoin – is de laatste jaren sterk toegenomen. Zowel voor legitieme doeleinden, als voor criminele activiteiten (witwaspraktijken, fraude, handel in illegale goederen en diensten). Zowel wetshandhavings-, opsporings-, en inlichtingendiensten als toezichthouders en beleidsmakers hebben behoefte aan inzicht in Bitcoin-transacties, -geldstromen en -actoren. Dit inzicht is nodig om criminaliteit tegen te gaan, daders op te sporen, en het legale gebruik van cryptovaluta in goede banen te leiden. Het primaire doel van het project is het ontwikkelen van analyse-software voor het verschaffen van inzicht in cryptovaluta-transacties. Het project draagt vooral bij aan onderzoeksthema 'Cybercrime and the underground economy' van de NCSRA-II. In 2012 is Coblue gekozen tot de Kairos50, een prijs die wordt uitgereikt aan de 50 meest innovatieve universiteit start-ups wereldwijd.

22 januari 2015

IC3D Media: project Cybercheck (SBIR15C045)

Een onderzoek van IBM in 2014 toont aan dat menselijke fouten of onwetendheid de oorzaak zijn van 95% van de digitale beveiligingsincidenten. De huidige trainingen die medewerkers van organisaties bewuster moeten maken van digitale veiligheidsrisico's zijn echter algemeen en niet afgestemd op de afdeling of de functie van medewerkers. Het resultaat is dat de menselijke schakel zwak blijft. Medewerkers zijn onvoorzichtig met het delen van bestanden, nog steeds gevoelig voor phishing mails en niet echt bewust van de risico's in cyberspace.

IC3D media ontwikkelt een open platform, Cybercheck, waarmee bedrijven zelf snel een trainingspakket kunnen samenstellen. Zij leren in levensechte scenario's hoe cybersecurity impact heeft op hun dagelijkse werk. Het project draagt vooral bij aan onderzoeksthema's 'Opsporing en voorkoming van aanvallen en monitoring' en 'Risk Management, economie en regelgeving' van de NCSRA-II. IC3D Media won in 2012 de Accenture Innovation Award (2012) met haar trainings-software InterACT en ontwikkelt o.a. virtuele trainingen voor Defensie, G4S en de overheid van Indonesië.

Digital Intelligence Group: CyberSCAN (SBIR15C014)

De gecombineerde inzet van conventionele en cybercapaciteiten kan de effectiviteit van een militaire operatie vergroten. Per 25 september 2014 heeft Defensie het Cyber Commando opgericht. Daarmee is cyber een volwaardig onderdeel van militaire operaties geworden, inclusief de ontwikkeling van offensieve cybercapaciteiten. Defensie heeft onder andere behoefte aan software die de infrastructuur van een land in kaart brengt. De huidige producten hebben daar maanden voor nodig. Het CyberSCAN_project gaat een scanmethodiek opleveren die in enkele dagen de netwerkinfrastructuur van een groot gebied nauwkeurig in kaart brengt. Het project draagt vooral bij aan onderzoeksthema 'offensieve cyber capaciteiten' van de NCSRA-II. De Digital Intelligence Group verzorgt trainingen en producten op het gebied van digitale recherche en beveiliging op het internet en richt zich op personeel van overheidsorganisaties.

Ziuz Forensics: VCR (SBIR15C010)

De vele organisaties die betrokken zijn bij het opsporen van malafide content hebben eigen initiatieven en processen die niet met elkaar verbonden zijn. ZiuZ wil samen met Web-IQ en de Landelijke Eenheid een Visuele Contentrechercheur ontwikkelen. Dit platform zal geautomatiseerd en proactief webdomeinen detecteren waar beeldmateriaal van onder meer kinderpornografie wordt gehost en verspreid. Daarmee wordt de slagkracht van opsporingsdiensten die dergelijke malafide content bestrijden, significant vergroot. Het project draagt vooral bij aan de onderzoeksthema's 'Forensics en incident management', 'Cybercrime en de underground economy' en 'Offensieve cyber capaciteiten' van de NCSRA-II. ZiuZ ontwikkelt beeldtechnologie gericht op classificatie, registratie en detectie van beeldmateriaal. De oplossingen van ZiuZ vormen de standaard voor de Nederlandse politie en vele andere opsporingsdiensten.