Persbericht

BSA-onderzoek Europese cyber security-wetgeving: lidstaten wisselend voorbereid

Brussel, 3 maart 2015 – Niet elke EU-lidstaat is even goed voorbereid als het gaat om cyber security. Dat blijkt uit een onderzoek van BSA | The Software Alliance, dat voor het eerst Europese wet- en regelgeving op het gebied van cyber security analyseerde. De BSA | The Software Alliance toetste de nationale wet- en regelgeving in alle 28 EU-lidstaten aan de hand van 25 criteria die als essentieel worden beschouwd voor effectieve bescherming van cyber security. Doel van dit onderzoek was de EU-landen een mogelijkheid te bieden om hun eigen policy's af te zetten tegen key metrics. Daarnaast zet BSA hiermee een stap vooruit door de belangrijkste bouwstenen voor een krachtig juridisch kader voor cyber security te bepalen.

"Als het gaat om cyberbescherming, is er in Europa sprake van grote verdeeldheid. De meeste lidstaten erkennen dat cyber security een prioriteit is. Toch blijft de volledige interne markt kwetsbaar voor bedreigingen vanwege de inconsistenties in hun aanpak", zegt Thomas Boué, Director of Policy EMEA bij BSA. "De Europese richtlijn voor netwerk- en informatiebeveiliging kan helpen bij het verstevigen van het basisniveau van cyber security en cyberweerbaarheid, als die richtlijn zich richt op het in lijn brengen van de bescherming van de meest kritische Europese infrastructuur en op het introduceren van geharmoniseerde rapportage- en kennisdelingsprocessen binnen de gemeenschappelijke markt."

Een aantal van de belangrijkste onderzoeksresultaten op een rij.

- De meeste EU-lidstaten zien cyber security als een nationale prioriteit – vooral als het gaat om kritische infrastructuren.
- Er zijn aanzienlijke hiaten tussen de cyber security-policy's, juridische kaders en operationele mogelijkheden van alle lidstaten, met als gevolg een grote achterstand in algehele cyber security-bescherming in Europa.
- Bijna alle EU-lidstaten hebben incident response-teams samengesteld om cyberincidenten aan te pakken, maar het doel en de ervaring van deze eenheden verschillen.

- Er is op het gebied van cyber security een zorgwekkend gebrek aan systematische samenwerking tussen overheid en bedrijfsleven, en tussen Europese regeringen en niet-gouvernementele organisaties (ngo's) en internationale partners.

Op basis van het onderzoek raadt de BSA EU-lidstaten aan te focussen op vier belangrijke onderdelen van een krachtig juridisch kader voor cyber security.

- Creëer en onderhoud een uitgebreid juridisch kader met policy's, gebaseerd op een nationale cyber security-strategie die is aangevuld met branchespecifieke cyber security-plannen.
- Geef operationele eenheden duidelijke verantwoordelijkheden voor operationele computerbeveiliging en emergency response en incident response.
- Kweek vertrouwen en werk samen met het bedrijfsleven, ngo's en internationale partners en allianties.
- Stimuleer het onderwijs en het bewustzijn rondom risico's en prioriteiten op het gebied van cyber security.

Verder waarschuwt de BSA Europese regeringen ervoor om nutteloze beschermingsregelingen te voorkomen, die afbreuk kunnen doen aan cyberbeschermingsinitiatieven in plaats van ze te verbeteren. Lidstaten moeten in het bijzonder:

- onnodige of onredelijke eisen vermijden, die de keuze kunnen beperken en kosten verhogen, zoals unieke, landspecifieke certificerings- of testeisen, mandaten voor lokale content, voorschriften voor gevoelige informatie als broncode en encryptiesleutels, en beperkingen aan buitenlands eigendom en intellectueel eigendom;
- standaarden niet manipuleren, maar juist toonaangevende, internationaal erkende, technische standaarden ondersteunen;
- datalokalisatieregels vermijden en ervoor zorgen dat data vrij tussen de verschillende markten kan bewegen;
- niet de voorkeur geven aan eigen technologieën die buitenlandse concurrentie belemmeren en schadelijk zijn voor wereldwijde innovatie.

Het onderzoeksrapport vermeldt dat de overheid in 2012 de Belgische Cyber Security Strategy bekrachtigde. Echter, het juridische kader voor cybersecurity in België blijft onduidelijk en er is beperkte informatie over de implementatie van de strategie. België heeft wel een gevestigd computer emergency response-team, CERT.be, en een goed ontwikkelde structuur voor het rapporteren van cybersecurity-incidenten. Daarnaast introduceerde België onlangs een nieuw Cybersecurity Centre. Overal in het land is er actieve ondersteuning voor partnerships tussen overheid en bedrijfsleven. Dit is mogelijk door BeINIS, een overheidsorgaan dat nauwe contacten onderhoudt met private en semi-private organisaties.

Het volledige onderzoeksrapport met de 28 landen en gedetailleerde samenvattingen van alle EU-lidstaten zijn te vinden op www.bsa.org/EUcybersecurity.

Over BSA | The Software Alliance

BSA | The Software Alliance (www.bsa.org) is de belangrijkste pleitbezorger van de software-industrie ter wereld. De aangesloten leden van de BSA investeren jaarlijks miljarden dollars in de ontwikkeling van softwareoplossingen die de economie stimuleren en het moderne leven verbeteren. De BSA verbreedt de horizon van de digitale wereld door relaties met internationale overheden, het naleven en afdwingen van intellectueel eigendom, en onderwijsactiviteiten. Daarnaast vergroot de organisatie het vertrouwen in de nieuwe technologieën die deze wereld stimuleren. Meer informatie: www.bsa.org/netherlands of www. bsa.be.

Voor meer informatie:

LVTPR
Luc Gyzels
Telefoon: 02 474 17 40
E-mail: bsa@lvtpr.com