Zur Veröffentlichung

Pressekontakt:
Michael Höppner
Michael.hoeppner@vibrio.de

BSA gibt Empfehlungen zur besseren Organisation und warnt vor nationalem Protektionismus

Analyse der Gesetze zur Cybersicherheit: EU nur lückenhaft gerüstet

Brüssel, 3 März 2015 — Die Bereitschaft, auf Bedrohungen der Cybersicherheit zu reagieren, ist innerhalb Europas lückenhaft und zersplittert, so eine aktuelle Analyse der gesetzlichen Lage. Die Untersuchung, welche die BSA | The Software Alliance heute vorstellt, bewertet die nationalen Gesetze, Regeln und Richtlinien in allen 28 Mitgliedsstaaten der EU. Sie begutachtet dabei 25 Kriterien, die für die effektive Cybersicherheit von zentraler Wichtigkeit sein dürften. Die Ergebnisse sollen die EU Mitgliedsstaaten in die Lage versetzen, ihre Vorgehensweise zu prüfen und die weitere Entwicklung mit Hilfe der wesentlichen Bausteine starker Cybersicherheits-Gesetze zu definieren.

Thomas Boué, Director of Policy EMEA der BSA: "In Punkto Cybersicherheit ist die Ausgangslage in Europa höchst uneinheitlich. Die meisten Mitgliedsstaaten haben erkannt, dass der Schutz oberste Priorität hat, aber die unterschiedlichen Herangehensweisen machen den gemeinsamen Markt anfällig für Bedrohungen. Die Richtlinie zur Informations- und Netzsicherheit könnte eine solidere Basis der Cybersicherheit und der Widerstandsfähigkeit schaffen. Darüber hinaus muss sie dazu beitragen, die wichtigsten Infrastrukturen in der EU harmonisieren und einheitliche Berichts- und Informationsprozesse im Binnenmarkt schaffen."

Die wesentlichen Ergebnisse der Analyse sind:

- Die meisten EU-Mitgliedsstaaten erkennen die Cybersicherheit als eine nationale Priorität, insbesondere in Bezug auf kritische Infrastruktur.
- Es bestehen erhebliche Unterschiede zwischen den Herangehensweisen, Gesetzen und Kapazitäten der Cybersicherheit in den Mitgliedssaaten. Die Konsequenz sind deutliche Lücken in der Cybersicherheit Europas.
- Nahezu alle 28Mitgliedsstaaten haben unabhängige Krisenstäbe eingerichtet, um Cyber-Vorfällen zu begegnen. Die Aufgabenstellung und die Erfahrung dieser Organisationen jedoch sind unterschiedlich.

- Bei der Cybersicherheit herrscht ein systematischer Mangel an „public-private“-Abstimmung zwischen Behörden und Organisationen des privaten Sektors sowie internationalen Partnern.

Der Bericht bestätigt Deutschland eine umfassende Strategie im Bereich Cybersicherheit, die 2011 eingeführt wurde und durch eine robuste Gesetzeslage im Sicherheitsbereich ergänzt wird. Das Bundesamt für Sicherheit in der Informationstechnik (BSI), im Auftrag der deutschen Regierung verantwortlich für den Schutz von Computern und Kommunikation, ist ein klarer Beleg für die hohe Priorität, die Cybersicherheit für die deutsche Regierung hat. Deutschland verfügt auch über ein Netz von Krisenreaktionsteams (CERT), deren nationaler CERT-BUND eng mit den behördlichen und regierungsunabhängigen CERTs zusammen arbeitet. Weiterhin bestehen gute Partnerschaften zwischen öffentlichen und privaten Einrichtungen, so etwa die Allianz für Cyber-Sicherheit und die Kooperation UP KRITIS. Die nationale Politik und die Gesetze unterstreichen den Fokus auf die Zusammenarbeit zusätzlich.

In ihrer Analyse fordert die BSA alle EU-Mitgliedsstaaten dazu auf, sich auf vier Pfeiler zu konzentrieren, um ein stabiles Cybersicherheits-Konzepts zu realisieren:

- Aufbau und Erhalt eines umfassenden rechtlichen und politischen Rahmens auf Basis nationaler Cybersicherheits-Strategien, der von branchenspezifischen Cybersicherheits-Plänen ergänzt wird.
- Die Schaffung von Organisationen mit klar umrissenen Verantwortungsbereichen zur Sicherheit von Computern und zur Reaktion auf Vorfälle und in Notfällen.
- Die Förderung von Vertrauen und Zusammenarbeit mit der Privatwirtschaft, mit NGOs, internationalen Partnern und Verbündeten.
- Aufklärung und Ausbildung über Cybersicherheits-Risiken und -Prioritäten.

Zudem warnt der Bericht die europäischen Regierungen vor Protektionismus, welcher der Cybersicherheit eher schadet denn sie fördert. Insbesondere sollten die Mitgliedsstaaten:

- davon absehen, unnötige oder übertriebene Anforderungen zu stellen, welche bei der Wahl von Lösungen und Anbietern einschränken und die Preise in die Höhe treiben. Dazu zählen etwa nationale Zertifizierungen oder Test-Anforderungen, die Forderung einheimischer Herstellung („local content“), der Zwang zur Heraushabe sensibler Informationen wie Sourcecode oder Verschlüsselungskey sowie Beschränkungen ausländischen Rechts am geistigem Eigentum.
- sich beim Eingriff in Standards zurückhalten, und stattdessen aus der Branche entstandene, international akzeptierte technische Standards unterstützen.
- Regeln zur regionalen Speicherung von Daten vermeiden, um den freien Verkehr von Daten über Grenzen hinweg zu sichern.
- von der Bevorzugung einheimischer Technologien Abstand nehmen, welche den internationalen Wettbewerb behindern und die weltweite Innovation hemmen.

Der vollständige Bericht mit Details für alle 28 Länder ist erhältlich unter www.bsa.org/EUcybersecurity.

Informationen zur BSA*BSA | The Software Alliance (www.bsa.org) ist die globale Stimme der Software-Industrie. In der BSA sind weltweit führende Unternehmen versammelt, die jährlich Milliardenbeträge in neue Softwarelösungen investieren, welche die Wirtschaft antreiben und das moderne Leben von heute prägen. Durch internationale Zusammenarbeit mit Regierungen, die Verfolgung von Urheberrechtsverletzungen und breite Aufklärungsmaßnahmen arbeitet die BSA daran mit, den Horizont der digitalen Welt zu erweitern und das Vertrauen in neue Technologien zu stärken. BSA-Website: EU: http://www.bsa.org/EU International: http://www.bsa.org Twitter: @BSANewsEU und @BSAnews*

Avenue des Arts 44
Brussels 1040

P +32 (0) 2 274 13 1
W bsa.org

EU Register of Interest Representatives:
75039383277-48