Der Geschäftsführer von ENISA für Netzwerk- und Informationssicherheit spricht auf der EP-Konferenz von einer ausgewogenen Annäherung an die Online-Privatsphäre zusammen mit einem bewährten EU ICT Sektor.

„Die Herausforderung für Politiker ist es, eine ausgewogene Annäherung zur Privatsphäre mit möglichst wenig negativen Auswirkungen auf die Interessen und Industriegeschäfte der Bürger zu schaffen“, sagte Udo Helmbrecht, der Geschäftsführer von ENISA, auf der Konferenz des Europäischen Parlamentes in Brüssel. Die Konferenz, welche gemeinsam vom Komitee für bürgerliche Freiheiten und der Luxemburgischen Präsidentschaft des Europäischen Rates zusammen mit den Komitees IMCO und ITRE organisiert wird, diskutiert den Schutz der Online-Privatsphäre, indem sie die IT-Sicherheit verbessert und die IT-Fähigkeiten der EU stärkt.

ENISA begrüßte die einzeln besprochenen Politikfelder der Einführung der Privatsphäre verbessernder Technologien, die Soft- und Hardware-Schwachstellen und die Infrastruktur des Internets sowie das Potenzial der EU für die Entwicklung einer starken, lebendigen IT-Industrie. ENISA hofft auf einen anregenden Effekt der Konferenz in der politischen Diskussion zu diesen eng verknüpften Politikfeldern.

Privatsphäre verbessernde Technologien – Standardisierung und Zertifizierung sind die Basis für die IT-Industrie

Der Gebrauch Privatsphäre verbessernder Technologien, wie beispielsweise „privacy by design“, sind Teil der IT-Funktionalität; sie bieten vereinbaren Schutz der Privatsphäre an und bauen Eigenschaften des Sicherheitsstandards aus und werden dazu ermutigt, als Standard eingesetzt zu werden. Des Weiteren können EU-Richtlinien, welche die Entwicklung sicherer Soft- und Hardware sowie die Standardisierung und Zertifizierung betreffen, die ENISA ebenfalls entwickelt, in allen EU-Mitgliedsstaaten beworben und eingesetzt werden um Schwachstellen anzusprechen.

Die Einführung des „Internet of Things“ ist ein Beispiel, welches die immer mehr wachsende Wichtigkeit betreffend Herausforderungen der Sicherheit, die zum Teil vom Aspekt der Netzwerkelastizität gelindert werden, demonstriert. Indessen stellt das Zusammenspiel des „Internet of Things“ mit Software- und Hardware-Komponenten mehr Risiken und Gefahren vor. Dies betrachtend spielen gewisse Komponenten der Internetstruktur eine wichtige Rolle. Daher ist es wichtig, Informationen zu Vorfällen und Schwachstellen zu teilen und einen Dialog zwischen den Akteuren herzustellen, der zu einer gemeinsamen Annäherung zur Sicherheit verhilft.

Mit Empfehlungen, die Kritikalität der IT-Infrastruktur der EU anzusprechen haben EU-Mitgliedsstaaten spezifische Maßnahmen entwickelt, diese zu schützen. Der neue vereinbarte Text über die Weisung in die Netzwerk- und Internetsicherheit ist ein positiver Schritt für eine übereinstimmende Annäherung und Kooperation zwischen allen Akteuren und Sektoren, die die Sicherheit der digitalien Infrastruktur (egal ob Energie, Gesundheit, Transport oder Finanzen) ansprechen, um eine hohe Ebene der Sicherheit kritischer Systeme, der Infrastruktur und der Bürger zu gewährleisten. ENISA hat in diesen Bereichen umfangreiche Erfahrung. Durch diese Erfahrung wurden starke Kooperationsmechanismen entwickelt (durch CSIRTs und die Übungen der Cyber Europe Serie), die maßgebenden Regierungen zusammen mit dem privaten Sektor erlauben, auf Vorfälle zu reagieren (Artikel 13a, TSPs)[1]. „Wir freuen uns auf die weitere Verbesserung und Stärkung unserer Zusammenarbeit in diese Richtung“, sagte Helmbrecht.

[1] TSPs (Trust Service Providers). ENISA schlägt neues Reporting Schema für TSPs vor Artikel 13a: Art. 13a, aus Richtlinie 2009/140 EC, ist Teil des Telekom-Pakets und strebt die Sicherstellung der Sicherheit und

ENISA hebt den Zuwachs des Marktes für Cyber-Sicherheit hervor

Die aus der Cyber-Sicherheit hervorgehenden Werte, die bis zu 640 Milliarden Euro für die EU-Wirtschaft erreichen könnten, wurden in der Diskussion hervorgehoben. Der EU-Markt für Cyber-Sicherheit ist mit einem geschätzten Wert von 20 Milliarden Euro wachsend um 6% CAGR[2] unterentwickelt. Es ist wichtig, dass die EU Cyber-Vertrauen unter den Bürgern und der Industrie schafft, um einen wettbewerbsfähigen EU-basierten ICT-Sektor aufzubauen, welcher die Position der EU zusätzlich stärkt.

Für weitere Informationen zu diesem Thema und Presseanfragen kontaktieren Sie bitte press@enisa.europa.eu,
Tel.+30 2814 409576

Für weitere Informationen zum Treffen des EP besuchen Sie bitte folgende Links:

http://www.europarl.europa.eu/committees/en/libe/events.html?id=20151208CHE00191
http://www.stoa.europarl.europa.eu/stoa/cms/home/events/workshops/privacy

Integrität elektronischer Kommunikationsnetzwerke und –dienste (Telekom) an. In diesem Bereich hat ENISA die Verantwortung, Vorfälle und Handlungen, die innerhalb des Telekom-Sektors der Mitgliedsstaaten getätigt wurden, zu sammeln und zur „Harmonisierung angemessener technischer und organisatorischer Sicherheitsmaßnahmen beizutragen, indem Expertenratschläge angeboten warden“ und indem „der Austausch von guten Beispielen iniziiert wird “.
[2]Cyber-security market size in Europe – Gartner 2014