

05/02/2014

EPR09/2014  
[www.enisa.europa.eu](http://www.enisa.europa.eu)

## Standardisierte Betriebsabläufe, um multinationale Cyber-Krisen zu managen, zusammengestellt von der EU, EFTA-Mitgliedsstaaten und ENISA

**Mit der Entwicklung der EU-Standards für Betriebsabläufe (EU-SOPs), wurde ein Meilenstein, um multinationale Cyber-Krisen zu managen, erreicht. Die Abläufe wurden von der EU und Mitgliedsländern der Europäischen Freihandelsassoziation (EFTA) in Zusammenarbeit mit der EU Agentur ENISA entwickelt. Die EU-SOPs bieten Leitlinien über die Bewältigung von großen Cyber Vorfällen, die sich ansonsten zu einer Krise entwickeln würden. Besonders der direkte Link zu Entscheidungsträgern und politischer Führungsebene, um Cyber-Krisen erfolgreich zu bewältigen, wird durch die EU-SOPs hervorgehoben.**

Das Ziel der EU-SOPs ist die Unterstützung bei der Reaktion auf große Cyber Vorfälle, die sich zu Krisen entwickeln könnten.<sup>1</sup> Insbesondere werden diese Verfahren helfen, das Verständnis über Ursachen und Auswirkungen von multinationalen Cyber-Krisen (Situationsbewusstsein) zu verbessern und ermöglichen eine schnelle und effektive Milderung. Durch eine Kombination von Kontaktstellen, Richtlinien, Workflows, Vorlagen, Tools und bewährten Praktiken, bieten die EU-SOPs Krisenmanager die Möglichkeit, international verbreitete technische und nicht technische Informationen zu benutzen, um integrierte operative Zusammenhänge und effektive Aktionspläne zu identifizieren. Diese können auf politischer Ebene für die Entscheidungsfindung präsentiert werden.

Multinationales Cyber-Krisenmanagement erfordert die starke Beteiligung von technischen Experten, während der operative Krisenmanager über Zeit wichtiger wird, je höher die Kritikalität der Vorfälle ist. Auch entscheidend sind die direkten Verbindungen zu Entscheidungsträgern auf strategischer und politischer Ebene.

Der [Generaldirektor](#) der ENISA, Professor Udo Helmbrecht, merkte an: *“Eine effektive Antwort auf multinationale Krisen erfordert grenzübergreifende Zusammenarbeit für eine schnelle Bewertung und Milderung. Diese Verfahren werden die Notwendigkeit eines Handbuchs für vordefinierte, allgemein vereinbarte und operative Kontakte, Verfahren und Prozesse adressieren.”*

### [Für mehr Informationen über ENISA Cyber-Krisenkooperation](#)

#### Hintergrund:

---

<sup>1</sup> Eine Cyber-Krise ist ein Ereignis oder eine Reihe von Ereignissen, natürlicher Art oder von Menschen geschaffen, die als solche von einem Land deklariert wird. Bei einer multinationalen Cyber-Krise betreffen die Ursache oder die Auswirkung mindestens zwei Länder.



05/02/2014

EPR09/2014  
[www.enisa.europa.eu](http://www.enisa.europa.eu)

Der EU-SOPs Entwurf wurde über die letzten drei Jahre, inklusive einer europaweiten Übung organisiert von ENISA getestet: [Cyber Atlantic](#) in 2011 und [Cyber Europa](#) in 2012. Die Verfahren sind für alle öffentlichen Behörden der EU/ EFTA Mitgliedsländer, die in der Bewältigung von multinationalen Cyber-Krisen involviert sind, verfügbar.

Siehe auch die vorgeschlagene [EU Cyber Sicherheitsstrategie und die vorgeschlagene NIS Richtlinie](#).

**Für Interviews:**

Ulf Bergström, Pressesprecher, [press@enisa.europa.eu](mailto:press@enisa.europa.eu), mobil: + 30 6948 460 143, oder Dr. Panagiotis Trimintzios, Experte, [c3e@enisa.europa.eu](mailto:c3e@enisa.europa.eu)

*Übersetzung. Das Englische Original ist die einzige maßgebliche Fassung.*

<http://www.enisa.europa.eu/media/enisa-auf-deutsch/>  
[www.enisa.europa.eu](http://www.enisa.europa.eu)

ENISA is a Centre of Expertise in Network and Information Security in Europe

Securing Europe's Information Society

The European Union Agency for Network and Information Security

Follow the EU cyber security affairs of ENISA on [Facebook](#), [Twitter](#), [LinkedIn](#) [YouTube](#) [Pinterest](#) [Slideshare](#) & [RSS feeds](#)