

ENISA stellt die Cyber-Bedrohungslandschaft 2014 dar: die 15 wichtigsten Cyber-Bedrohungen, Cyber-Bedrohungsagenten, Cyber-Angriffsmethoden und Bedrohungstrends für Bereiche der neuen Technologien.

Der heute veröffentlichte Bericht [ENISA Bedrohungslandschaft 2014](#) (ETL 2014) ist der dritte Jahresbericht in Folge, der die wichtigsten Cyber-Bedrohungen und die 2014 stattgefundenen Entwicklungen zusammenfasst und analysiert. Der Bericht ENISA Bedrohungslandschaft 2014 trägt zur Erreichung der in der Cyber-Security-Strategie für die EU formulierten Ziele bei und betont die Bedeutung der Bedrohungsanalyse und die Identifizierung der neuen Trends in der Cyber-Sicherheit.

Neuerungen der ETL 2014 sind:

- Informationen zu den Angriffsvektoren, die anfängliche Informationen dazu liefern, „wie“ ein Cyber-Angriff stattfindet
- Die Erarbeitung von Anwendungsfällen für Bedrohungsintelligenz, die zeigen, wie die Bedrohungsanalyse in Phasen des Security-Managements eingesetzt werden kann und
- Die Einbeziehung von Interessensvertretern, bestehend aus 13 Experten von CERTs, Lieferanten, Mitgliedstaaten und Nutzern.

2014 waren bei den wichtigsten Bedrohungen größere Veränderungen zu beobachten: eine erhöhte Komplexität der Attacken, erfolgreiche Angriffe auf wesentliche Sicherheitsfunktionen des Internets, jedoch auch erfolgreiche, international koordinierte Operationen durch Strafverfolgungsbehörden und Sicherheitsunternehmen. Viele der Veränderungen im Bereich Cyber-Bedrohungen sind exakt dieser Koordination und der Mobilisierung der Cyber-Community zu verdanken. Jedoch gibt es Hinweise darauf, dass die künftigen Cyber-Bedrohungslandschaften eine hohe Dynamik beibehalten werden.

2014 kann als Jahr des Datenmissbrauchs charakterisiert werden. Die massiven Datenschutzverstöße bedeuteten massive Angriffe auf wichtige Sicherheitsfunktionen des Internets und zeigten, wie effektiv Cyber-Bedrohungsagenten die Sicherheitsmängel bei Unternehmen und Regierungen ausnutzten. Zu den wichtigsten Erkenntnissen aus der ETL gehört, dass „Nachlässigkeit“ in Bezug auf Cyber-Sicherheit die häufigste Ursache für Datenmissbrauch darstellt und in 50 % der Fälle der Grund dafür ist. Überdies zeigt sich eine positive Entwicklung in der Zunahme der Qualität sowie der Quantität der erhobenen Informationen, was eine bessere Bedrohungsbeurteilung und detaillierteres Material für Endnutzer zur Folge hat.

In der ETL 2014 werden Angaben zu diesen Entwicklungen anhand der wichtigsten Cyber-Bedrohungen und der neuen Bedrohungstrends in verschiedenen Technologie- und Anwendungsbereichen unter Verweis auf mehr als 400 relevante Bedrohungsquellen dargestellt, um Entscheidungsträger, Sicherheitsexperten und interessierte Privatpersonen auf ihrem Weg durch die Cyber-Bedrohungslandschaft zu unterstützen.

Die neuen Technologien, die einen Einfluss auf die Bedrohungslandschaft ausüben werden, sind: Cyber Physical Systems (CPS), mobiles und Cloud Computing, Trust Infrastructure, Big Data und das Internet der Dinge. CPS hat großen Einfluss im Bereich Schutz kritischer Infrastrukturen und stellt eine deutliche Gelegenheit dar, um für die europäische Industrie und Forschung Wettbewerbsvorteile zu erzielen.

28.01.2015

EPR04/2015

www.enisa.europa.eu

Der geschäftsführende Direktor der ENISA, Professor [Udo Helmbrecht](#), kommentierte das Projekt wie folgt: *„Die Identifizierung und das Verständnis der Dynamik von Cyber-Bedrohungen entwickelt sich zu einem äußerst wichtigen Instrument der Cyber-Sicherheit. Die Dynamik der Cyber-Bedrohungslandschaft legt die Parameter für flexible und dennoch effektive Schutzmaßnahmen fest, die an das tatsächliche Risiko angepasst werden. Das Verständnis der wechselseitigen Abhängigkeiten zwischen allen Komponenten der Bedrohungslandschaft ist eine wichtige Erkenntnis und ermöglicht aktive und flexible Maßnahmen des Sicherheitsmanagements. Mit ETL 2014 leistet ENISA einen weiteren Beitrag zum öffentlich verfügbaren Know-how im Bereich Cyber-Bedrohungen.“*

In diesem Jahr hat ENISA zwei thematische Bedrohungslandschaften entwickelt: eine im Bereich [Internet-Infrastrukturen](#) und eine weitere für Smart Home-Umgebungen, die im nächsten Monat veröffentlicht werden sollen. Individuelle, thematische Bedrohungslandschaften liefern einen Leitfaden für die Entwicklung von Schutzmaßnahmen zur Minimierung des Bedrohungsrisikos für wertvolle Vermögenswerte in verschiedenen Sektoren.

Der vollständige Bericht (in englischer Sprache) ist hier abrufbar: [ENISA Threat Landscape 2014](#)

Hinweise für Redakteure:

- **Tabelle 1** gibt einen ‘Überblick über die 15 wichtigsten bewerteten aktuellen Cyber-Bedrohungen und die neuen Trends’ der ENISA Bedrohungslandschaft’ 2014. **S.iv**
- **Tabelle 2** ‘Überblick und Vergleich der aktuellen Bedrohungslandschaften 2014 und 2013’ zeigt Veränderungen sowohl hinsichtlich der Trends als auch des Rankings der bewerteten Cyber-Bedrohungen, **S.39**
- **Tabelle 3:** ‘Beteiligung der Bedrohungsagenten bei den wichtigsten Bedrohungen’, **S.49**
- ETL-Bericht nach Kapiteln: Zweck, Umfang und Methode **S.5**, ETL 2014 **S.13**, Bedrohungsagenten **S.41**, Angriffsvektoren **S.51**, Die neue Bedrohungslandschaft **S.59**, Denkanstöße und Schlussfolgerungen **S.79**

Für Interviews: Dr. Louis Marinos, Experte für Netzwerk- und Informationssicherheit der ENISA
E-Mail: louis.marinos@enisa.europa.eu, **Telefon:** (+30) 2814 409 682