ENISA bildet die Bedrohungslage der IT-Infrastruktur 2014 ab und legt einen Good Practice-Leitfaden für verbesserte Sicherheit vor

Der heute von der ENISA veröffentlichte Bericht „Bedrohungslage und Good Practice-Leitfaden für IT-Infrastruktur“ bildet den Umfang, aus dem die IT-Infrastruktur besteht, sowie die entsprechenden Bedrohungen ab; gleichzeitig wird eine Übersicht über sich abzeichnende Trends gegeben und es werden entsprechende Sicherheitsmaßnahmen dargelegt. Der Bericht richtet sich in erster Linie an Inhaber von IT-Netzweken sowie Internet-Organisationen, Sicherheitsexperten, Entwickler von Sicherheitsleitfäden und Entscheidungsträger.

Der Bericht legt die Anlagen, aus denen eine IT-Infrastruktur besteht, dar und klassifiziert die entsprechenden Bedrohungen; dabei werden „wichtige spezifische Bedrohungen“ hervorgehoben, die die Konnektivität unterbrechen. Hierzu gehören Routing-Bedrohungen, DNS-Bedrohungen und (Distributed) Denial-of-Service. Jede Bedrohung lässt sich direkt mit den risikobehafteten Anlagen verknüpften. Insgesamt ist ein verstärktes Auftreten dieser Bedrohungen zu beobachten.

Der Bericht nimmt eine Bestandsaufnahme öffentlich verfügbarer Sicherheitsmaßnahmen zum Schutz der IT-Infrastruktur-Anlagen vor und erlaubt es den Eigentümern, ihre IT-Infrastruktur durch eine Risikobewertung und Evaluierung des Risikos spezifischer Bedrohungen sorgfältig zu analysieren. Zudem enthält der Bericht eine Liste an Good Practices, mit denen eine IT-Infrastruktur sicherer gemacht werden kann.

Darüber hinaus werden mittels einer Gap-Analyse bestehende Mängel der aktuellen Good Practices festgestellt. Anhand der Analyse werden die Lücken mit der Anwendung von Skill-Sets bei allen wichtigen spezifischen Bedrohungen, die analysiert wurden, sowie mit der Systemkonfiguration und wichtigen Adressierungsprotokollen für (Distributed) Denial-of-Service verknüpft.

Fünf technische Empfehlungen und vier organisatorische Empfehlungen werden für ein erhöhtes Sicherheitsniveau durch die Entwicklung und Anwendung von Good Practices vorgeschlagen, wobei die Bedeutung der Zusammenarbeit in der Gemeinschaft betont wird.

Udo Helmbrecht, geschäftsführender Direktor der ENISA, kommentierte das Projekt wie folgt: *„Die in der aktuellen Studie analysierten Bedrohungen deuten darauf hin, dass sie weltweit zunehmen. Es ist wichtig, Good Practices anzuwenden und den Austausch von Informationen zu fördern, um Bedrohungen zu vermindern und die IT-Infrastruktur zu sichern. Der Leitfaden der ENISA gibt einen aktuellen Überblick über aufkommende Bedrohungen und bildet das Fundament für die Gemeinschaft im Hinblick auf eine sicherere IT-Infrastruktur durch angemessene Risikoeinschätzung, -schulung und -bewertung.“*

Die Veröffentlichung ist Teil der ENISA Bedrohungslandschaft 2014, eine Initiative zur Erreichung der in der Strategie für Cyber-Sicherheit für die EU formulierten Ziele, und betont die Bedeutung der Bedrohungsanalyse und sich entwickelnder Trends im Bereich Cyber-Sicherheit.

Der vollständige Bericht (in englischer Sprache) ist hier abrufbar: Threat Landscape and Good Practice Guide for Internet Infrastructure

Für Interviews: Dr. Louis Marinos, Netz- und Informationssicherheit – Experte für Forschung und Analyse, ENISA, **E-Mail:** louis.marinos@enisa.europa.eu, **Telefon:** (+30) 2814409682