2013/09/19

EPR10/2013

www.enisa.europa.eu

Zwischenbericht: Top-Cybergefahren – intelligenter gesteuerte Angriffe, Bedrohungen für mobile Geräte und Social-Media-Identitätsdiebstahl durch Cyberkriminelle mit Hilfe von Cloud-Services

ENISA präsentierte heute eine Liste der Top-Cybergefahren, als Vorgeschmack auf den Zwischenbericht "Bedrohungslandschaft 2013". Die Studie analysiert 50 Berichte und identifiziert einen Zuwachs an Bedrohungen für: IT-Infrastrukturen durch gezielte Angriffe, mobile Geräte und Social Media durch Identitätsdiebstähle mit Hilfe von Cloud-Services.

Zu den in der Studie identifizierten entscheidenden Trends zählen:

- Cyberkriminelle verwenden zunehmend fortgeschrittene Verfahren, um nicht nachvollziehbare und schwer rückgängig zu machende Angriffstechniken (Vektoren) umzusetzen. Anonymisierungstechnologien und Peer-to-Peer-Systeme (sogenannte verteilte Technologien) spielen hierbei eine wichtige Rolle. Es besteht kein Zweifel, dass mobile Technologien immer mehr von Cyberkriminellen genutzt werden. Gefahren aller Art, welche bisher im Zusammenhang mit traditionellen IT-Bereichen bekannt waren, werden in Zukunft auch mobile Geräte und verschiedene, auf den Plattformen angebotene Leistungen betreffen.
- Die weite Verbreitung von mobilen Geräten führt zu einer Zunahme von Missbrauch, asierend auf Knowledge/Attack-Methoden, welche sich gegen Social Media richten.
- Die Verfügbarkeit von Malware sowie Werkzeugen und Dienstleistungen für Cyberhacking, in Kombination mit digitalen Währungen (z.B. Bitcoins) und anonymen Zahlungsmethoden, bieten neue Möglichkeiten für Cyberbetrug und erleichtern somit kriminelle Aktivitäten maßgeblich.
- Es besteht die reelle Gefahr, dass erfolgreich durchgeführte Angriffe, welche verschiedene Bedrohungsarten miteinander verbinden, schwerwiegende Auswirkungen haben.
- Wie von ENISA in ihrem Bericht über ernste Cybergefahren (20.7.2013) ausgeführt, stellen Cyberattacken den sechstgrößten Grund für Ausfälle von Telekommunikationsstrukturen dar, eine Tatsache, die eine beträchtliche Anzahl von Benutzern betrifft. Wenn man all diese Vorfälle, sowie die Denial-of-Service-Entwicklungen in Betracht zieht, können wir im Jahr 2013 einen signifikanten Anstieg von IT-Infrastrukturbedrohungen feststellen.

Die Studie identifiziert folgende Hauptbedrohungen, welche seit 2012 große Auswirkungen haben.

Drive-by-exploits: browserbasierende Angriffe stellen nach wie vor die meist gemeldete Bedrohung dar, Java bleibt für diese Art von Bedrohung die am häufigsten ausgenutzte Software.

Code Injektion: Angriffe gegen Content-Management-Systeme (CMS) sind besonders häufig. Aufgrund ihrer weiten Verbreitung stellen beliebte CMS eine nicht zu unterschätzende Angriffsfläche für Cyberkriminelle dar. Netze von Cloud-Service-Anbietern werden zunehmend für automatisierte Angriffe genutzt.

Botnets, Denial-of-Service, Rogueware/Scareware, gezielte Attacken, Identitätsdiebstahl und Search-Engine-Poisoning stellen weitere, verbreitete Bedrohungen dar.

Der vollständige ENISA „Bedrohungslandschaftsreport 2013" wird Ende des Jahres veröffentlicht.

Der geschäftsführende Direktor der ENISA, Professor Udo Helmbrecht kommentierte: „Dieser kurze Zwischenbericht informiert Sicherheitsakteure so früh wie möglich über Cybergefahrenentwicklungen, damit sie entsprechende Gegenmaßnahmen ergreifen können."

Zum Report: ENISA-Bedrohungslandschaft-Halbjahresreport 2013

Für Interviews: Graeme Cooper, Leiter der Public Affairs Einheit, E-Mail: press@enisa.europa.eu, Mobil: + 30 6951 782 268, oder Dr. Louis Marinos, Experte, louis.marinos@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