Cybersicherheit in Anlehnung an Winne the Pooh/Puuh den Bären: der neue Bericht der EU-Agentur ENISA über “digitale Fallen” (honeypots) für das Aufdecken von Cyberangriffen

Die EU-Agentur für Cybersicherheit ENISA veröffentlicht eine detaillierte Studie über 30 unterschiedliche “digitale Fallen” oder ‚Honeypots‘ die von Computer Emergency Response Teams (CERT, eine Gruppe von IT-Sicherheitsfachleuten, die bei der Lösung von konkreten IT-Sicherheitsvorfällen mitwirkt) und bundesweiten/staatlichen CERTs verwendet werden können, um proaktiv Internetangriffe ermitteln zu können. Die Studie enthüllt Hindernisse beim Verstehen der grundlegenden ‘honeypot’-Konzepte und beinhaltet Empfehlungen, in welchen Fällen ‚Honeypots‘ anzuwenden sind.

Eine zunehmende Anzahl von komplexen Internetangriffen erfordert verbesserte Frühwarn- und Erkennungsressourcen für die CERTs. ‚Honeypots‘ sind, vereinfacht erklärt, Fallen mit der einzigen Aufgabe, Angreifer abzulenken, indem sie eine reale Computerquelle nachahmen (z.B. eine Dienstleistung, eine Anwendung, ein System oder eine Datei). Jedes Objekt, das mit einem ‚Honeypot‘ in Verbindung steht, ist verdächtig. Daher wird jede Bewegung beobachtet, um bösartige Aktivitäten zu erkennen.

Diese Studie ist eine Nachfolge zum kürzlich erschienenen ENISA-Bericht über proaktive Erkennung von Störungen der Cybersicherheit. Der vorhergehende Bericht beschloss, dass CERTs die ‘Honeypots’-Fähigkeiten, welche entscheidende Einblicke in Hackerverhalten geben, anerkennen würden. Dennoch sei deren Einsatz für das Aufdecken und die Ermittlung von Angriffen noch nicht so weit verbreitet wie erwartet. Dies zeige, dass es Hindernisse in der Verwendung gibt.

Diese neue Studie stellt praktische Verwendungsstrategien und wichtige Themen für CERTs vor. Insgesamt wurden 30 ‚Honeypots‘ unterschiedlicher Kategorien getestet und bewertet. Das Ziel ist hier, Einblick darin zu gewähren, welche frei zugänglichen Lösungen und welche ‚Honeypot‘-Technologie sich am besten für die Verwendung und den Gebrauch eignen. Da es keine Wunderwaffe gibt, hat diese neue Studie einige Defizite und Hindernisse in der Verwendung von ‚Honeypots‘ identifiziert: die Anwendungsschwierigkeit, die geringe Dokumentation, Mangel und Software-Stabilität sowie Entwicklerunterstützung, eine geringe Standardisierung, der Bedarf an höchst qualifizierten Leuten sowie Probleme beim Verständnis von grundlegenden ‚Honeypot‘-Konzepten. Die Studie stellt eine Gliederung der ‚Honeypots‘ vor und behandelt deren Zukunft.

The Geschäftsführer von ENISA Professor Udo Helmbrecht nimmt wie folgt Stellung:

“Honeypots bieten für CERTs ein leistungsfähiges Werkzeug um Informationen zu Bedrohungen zu sammeln ohne die Produktionsinfrastruktur zu beeinflussen. Korrekt angewandt, bieten ‚Honeypots‘ wesentliche Vorzüge für CERTs: bösartige Aktivitäten in einem CERT-Bereich können verfolgt werden um frühzeitig Warnungen vor bösartiger Software, neuen Angriffen, Schwachstellen und schädlichem Verhalten zu senden. Außerdem bieten ‚Honeypots‘ auch die Möglichkeit, über Angreiftaktiken zu lernen. Wenn die CERTs in Europa ‚Honeypots‘ zunehmend als eine geschmackvolle Möglichkeit anerkennen, könnten sie ihre Bereiche besser verteidigen.“

Der ganze Bericht hier.
Für Hintergrundinformationen: COM(2009)149 und Legal Implications of Countering Botnets der NATO.

Für Interviews kontaktieren Sie bitte: Ulf Bergstrom, Sprecher, press@enisa.europa.eu oder Mobiltelefon: +30 6948 460 143, oder Cosmin Cioabanu, ENISA-Experte, unter opsec@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