LKA Niedersachsen

Projekte des LKA Niedersachsen zur Bekämpfung von Botnetzen

Vortrag anlässlich der Veranstaltung
zum Thema Botnetze
des eco-Verbandes

Jens Kolpack

Frankfurt am Main, 04.02.2009

LKA Niedersachsen

Vorschau

- Vorstellung AuR
  - ± Allgemeines
  - ± Tätigkeiten
- Rechtliche Grundlagen
  - ± Strafverfolgung
  - ± Gefahrenabwehr
- Projekte
  - ± Spam-Analyse
  - ± Bot-Analyse

LKA Niedersachsen

Vorstellung AuR

- AuR: Anlassunabhängige Recherche in Datennetzen
  → Internetstreife
- Einrichtung Oktober 2006
- LKA Niedersachsen, Standort Hannover
- Ausbau geplant
- Ähnliche Dienststellen bei anderen LKA, BKA, Zoll

LKA Niedersachsen

Gesetzliche Aufgaben

- Gefahren***abwehr***
  Schutz von Rechten / Gesetze

- Straf***verfolgung***
  Tatverdacht beim Vorliegen eines Rechtsbruchs.

- Je schwerwiegender Tatverdacht oder Gefahr, desto gravierender sind die Eingriffsmöglichkeiten

LKA Niedersachsen

Arbeitsablauf

- Internetstreife wie normale Streife
- Prüfung auf Relevanz
- „Erster Angriff“
  - ± Sicherung flüchtiger Beweise
  - ± Einleitung unaufschiebbarer Maßnahmen
- Weiterleitung an zuständige Stellen zur abschliessenden Bearbeitung

LKA Niedersachsen

Tätigkeitsfelder

Strafverfolgung

- Kinderpornografie
- Links- / Rechtsextremismus
- Anleitung oder Anstiftung zu Straftaten
- Verbotene Medien, verbotener Verkauf von Waffen
- Handel mit Medikamenten und BTM

Gefahrenabwehr

- Thematische Recherchen (z. B. G8-Gipfel, Chaostage)
- Botnetze

LKA Niedersachsen

Projekte mit Botnetzen

- Projekte zum Einstieg in das Thema Botnetze
- Spam-Analyse
  - ± Dezember 2006 bis Mitte 2007
- Bot-Analyse
  - ± November 2007 bis Februar 2008
- Ziel jeweils Gefahrenabwehr
- Beschränkung auf deutsche IP-Adressen

LKA Niedersachsen

Spam-Analyse

Arbeitshypothesen

- Verteilung von Spam fast ausschließlich über Botnetze
- Eintrag im E-Mail-Header
- Auslesen der IP-Adresse des Botrechners
- Gefahrenabwehr
  - ± Lokalisierung der Botrechner, Information der Besitzer
  - ± Ziel: Entfernung aus dem Botnetz

LKA Niedersachsen

Spam-Analyse

Durchführung

- Auswertung der E-Mail-Header über Skripte
- Benachrichtigung der Provider per E-Mail mit Anschreiben
- Ziel: Provider informieren ihre Kunden über potentielle Viren-Infektion
- Probleme

LKA Niedersachsen

Bot-Analyse

- Auslösen von Trojanern in virtueller Umgebung oder ungesichertem PC
- Protokollieren und Analysieren des Netzverkehrs, Struktur-Prüfung, geografische Verteilung
- Ermittlung von verdächtigen Bot-Rechnern oder gehackten Servern in Deutschland
- Ziel: Informierung des Providers und ggfs. Inhaber, Aufklärung und Prävention

LKA Niedersachsen

Schlussbetrachtung

- Erste Versuche zur Bekämpfung von Botnetzen
- Weitere Projekte geplant
  - ± Probebetrieb Honeypot
- Erfahrungsaustausch mit anderen Institutionen
- Rechtliche Möglichkeiten der Polizei

LKA Niedersachsen

Kontakt

Bei Fragen nehmen Sie Kontakt mit uns auf

Jens Kolpack

Tel.: 0511/26262-3123

jens.kolpack@polizei.niedersachsen.de

sg31-aur@lka.polizei.niedersachsen.de