

# Neues aus dem DFN-CERT

**51. DFN-Betriebstagung - Forum Sicherheit  
06. Oktober 2009  
Torsten Voss, DFN-CERT**

- Veranstaltungen
- Aktuelle Schwachstellen
- Aktuelle Vorfälle

IT-Sicherheitskriterien im Vergleich  
05.11.09 – 06.11.09 in Berlin

Incident Response unter Unix und Windows  
19.11.09 – 20.11.09 in Hamburg

<http://www.dfn-cert.de/veranstaltungen.html>

Seit Februar 2009:

- Schwachstellen in MS Office, Internet Explorer, Firefox und Java gehen nicht aus
- Schwachstellen in Adobe PDF und Flash
- Schwachstellen in Microsoft ATL
- Einige Schwachstellen im Linux Kernel, Lokal Root Exploits verfügbar

- Shared Library Rootkit bei einer Uni
- Verschiedene Trojaner z.B. Mebroot, Torpig, Zeus, Mariposa
- Phishing Emails gegen Unis
- Conficker

Sehr geehrte uni-xxx.de Account Benutzer,

Es wird eine allgemeine Aktualisierung in unserem System zwischen 7. bis 29. August 2009. Durch die anonyme Registrierung von uni-xxx.de und die Zahl der ruhende Konten, werden wir mit diesem Upgrade, um die genaue Anzahl der Teilnehmer haben wir derzeit.

Sie sind beauftragt, um sich in Ihrem uni-xxx.de und überprüfen, ob Ihre Konto ist nach wie vor gültig, und senden Sie sofort die folgenden

Username :.....(Obligatorische)

Passwort :.....(Obligatorische)

Geburtsdatum :.....(Optional)

Staat :.....(Optional)

Weitere Entwicklung seit Feb. 2009:

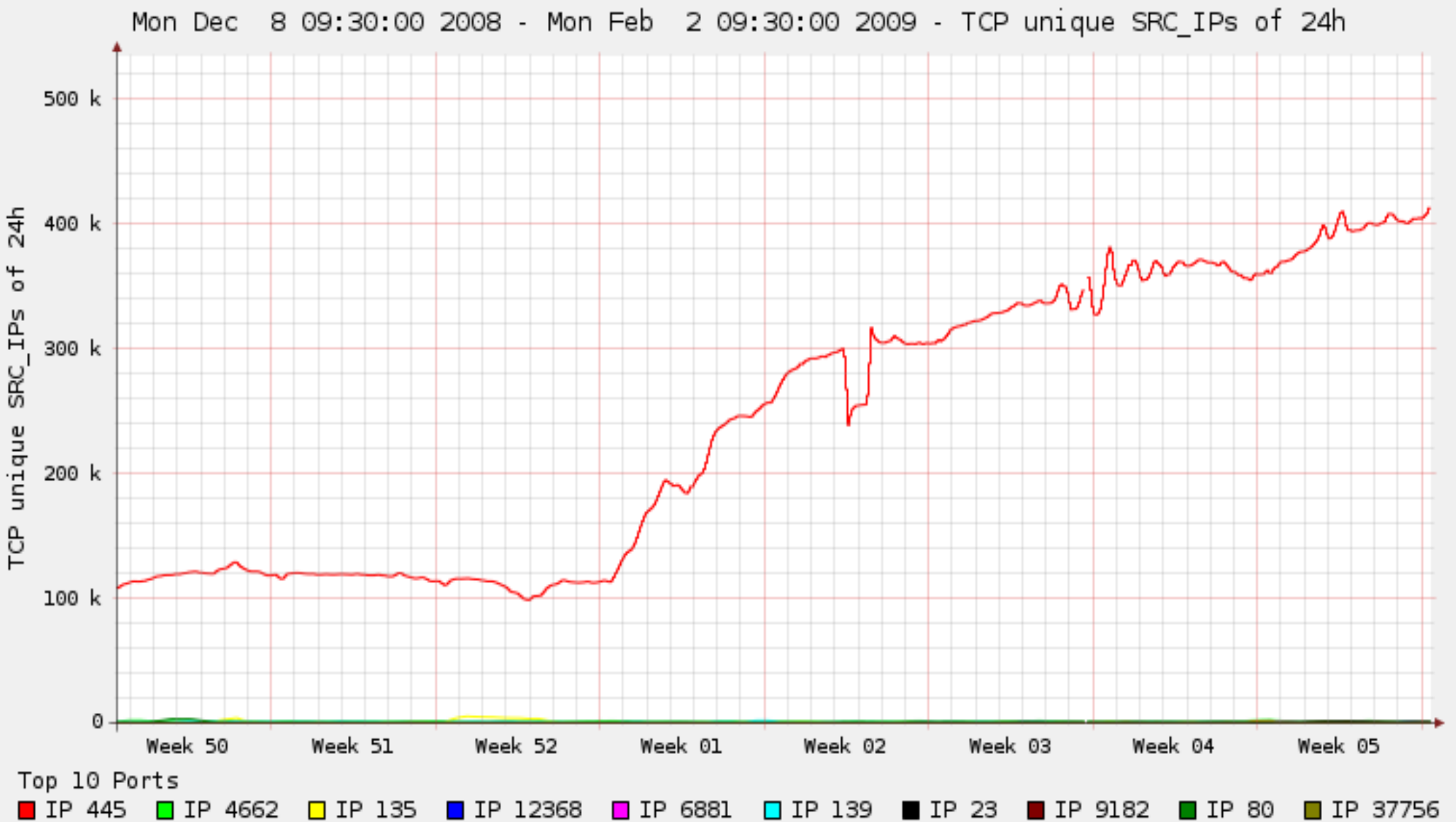
- Neue Versionen Conficker C-E
- Beendet Anti-Malware-Software
- Verbreitung/Updates über P2P-Verbindung
- Zeitweise Funktion für Vertrieb von Spam und Scareware

Referenzen:

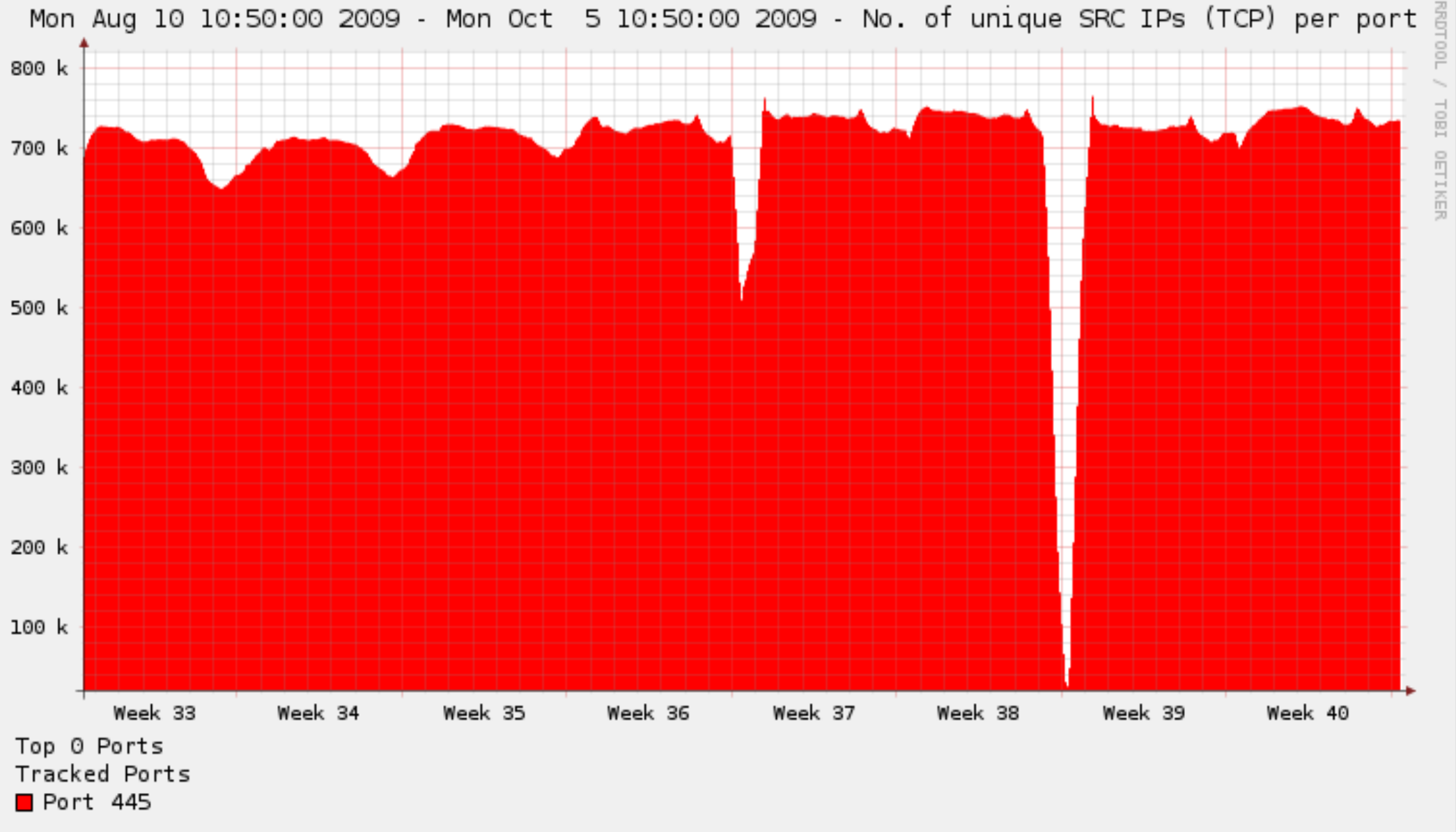
[www.confickerworkinggroup.org](http://www.confickerworkinggroup.org)

<http://iv.cs.uni-bonn.de/wg/cs/applications/containing-conficker>

<http://en.wikipedia.org/wiki/Conficker>

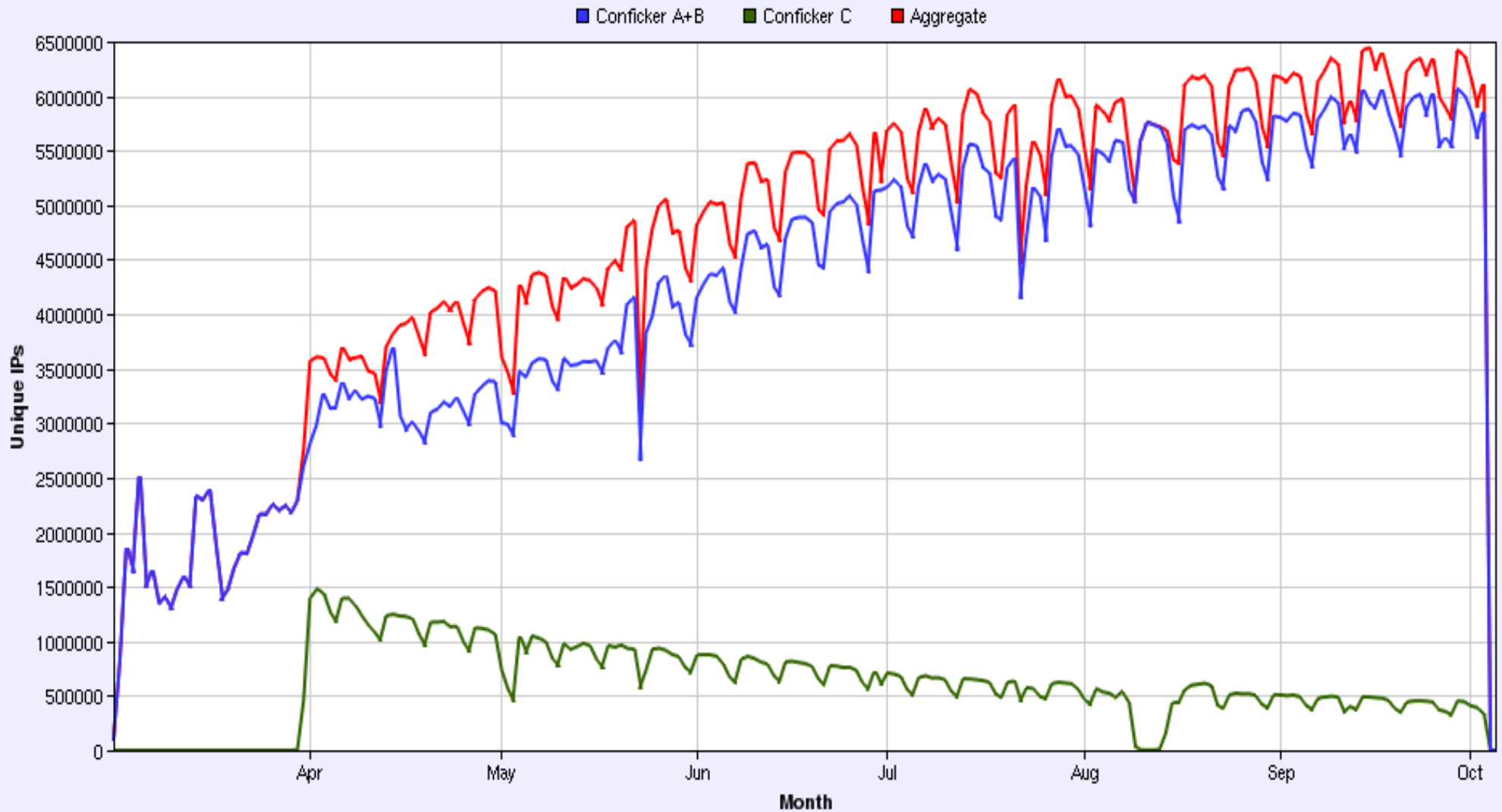


Quelle: Carmentis 02.02.2009



Quelle: Carmentis 05.10.2009

## Yearly Conficker Population



Quelle: [confickerworkinggroup.org](http://confickerworkinggroup.org) 05.10.2009

- Große Anzahl noch infizierter Systeme
- Einige Registrare hören auf die generierten Domains zu sperren
- Nicht mehr im Fokus der Öffentlichkeit
  
- Gute Lösung: Umlenkung der täglich neu generierten Update-Domains auf einen lokalen Server
- Dort können die Anfragen ausgewertet werden und betroffene Benutzer informiert werden
- **False-Positiv Meldungen möglich!**

# Vielen Dank für Ihre Aufmerksamkeit!

- Hilfe bei Vorfällen bei der DFN-CERT Hotline  
cert@dfn-cert.de oder 040 / 8080 77555
- Anmeldung für die Automatischen Warnmeldungen per  
Mail an: **cert@dfn.de**
- Weitere Informationen unter: **<https://www.cert.dfn.de/>**