DFN CERT

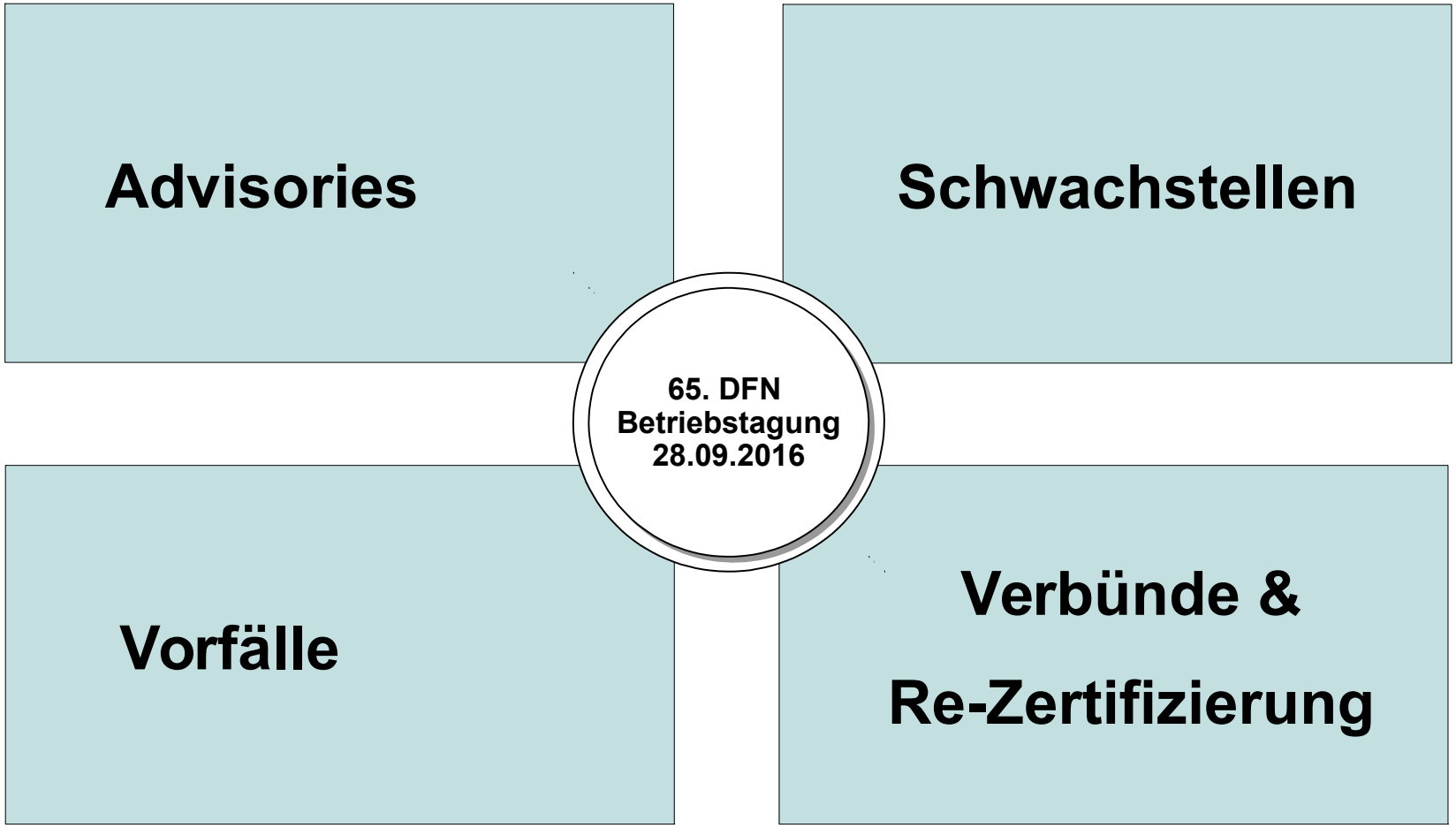
DFN Deutsches Forschungsnetz

Neues aus dem DFN-CERT

65. DFN-Betriebstagung - Forum Sicherheit
28. September 2016
Christine Kahl

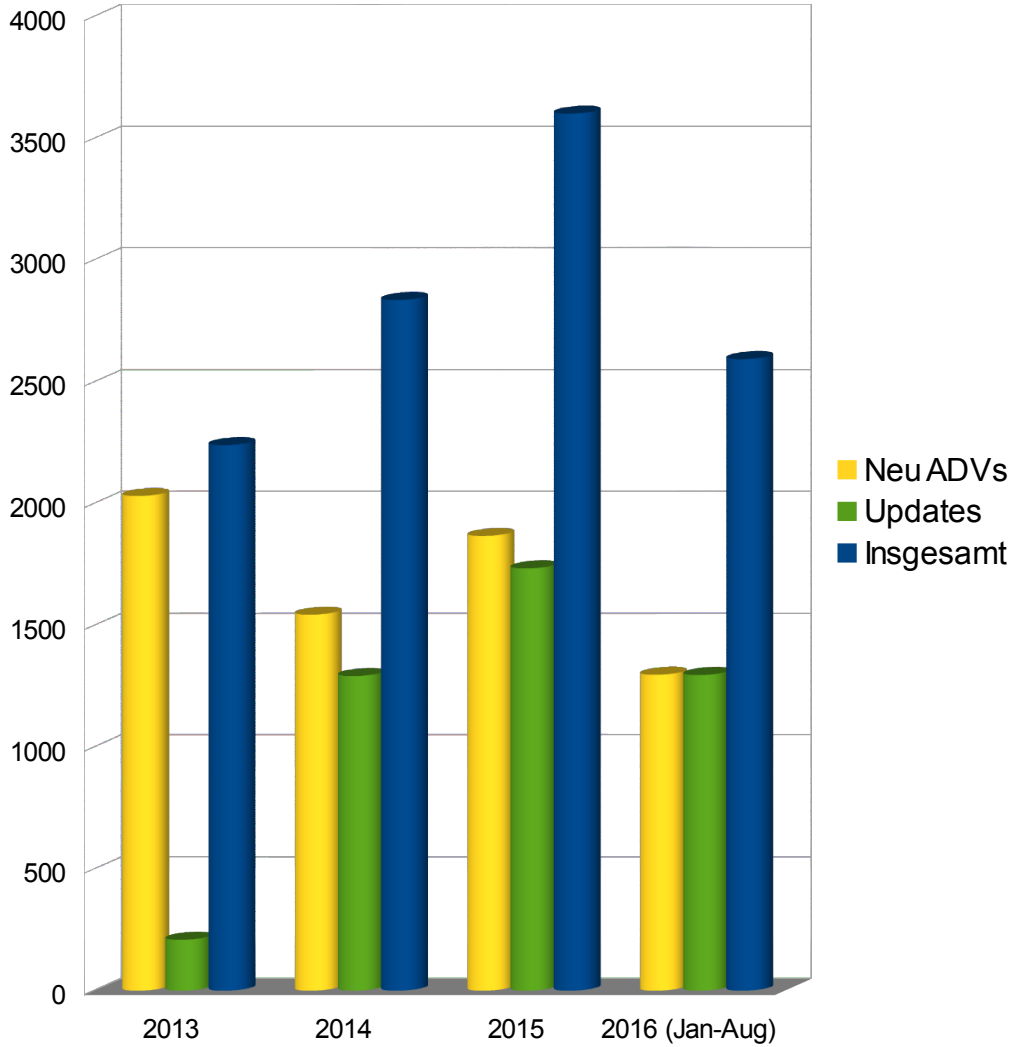
DFN Deutsches Forschungsnetz

Neues aus dem DFN-CERT



Advisories

Aktuelle Advisory Zahlen



Gesamtzahl ADVs

2013 = 2240

2014 = 2836

2015 = 3601

2016(Jan-Aug) = 2593

(neu: 1297, Update:1296)

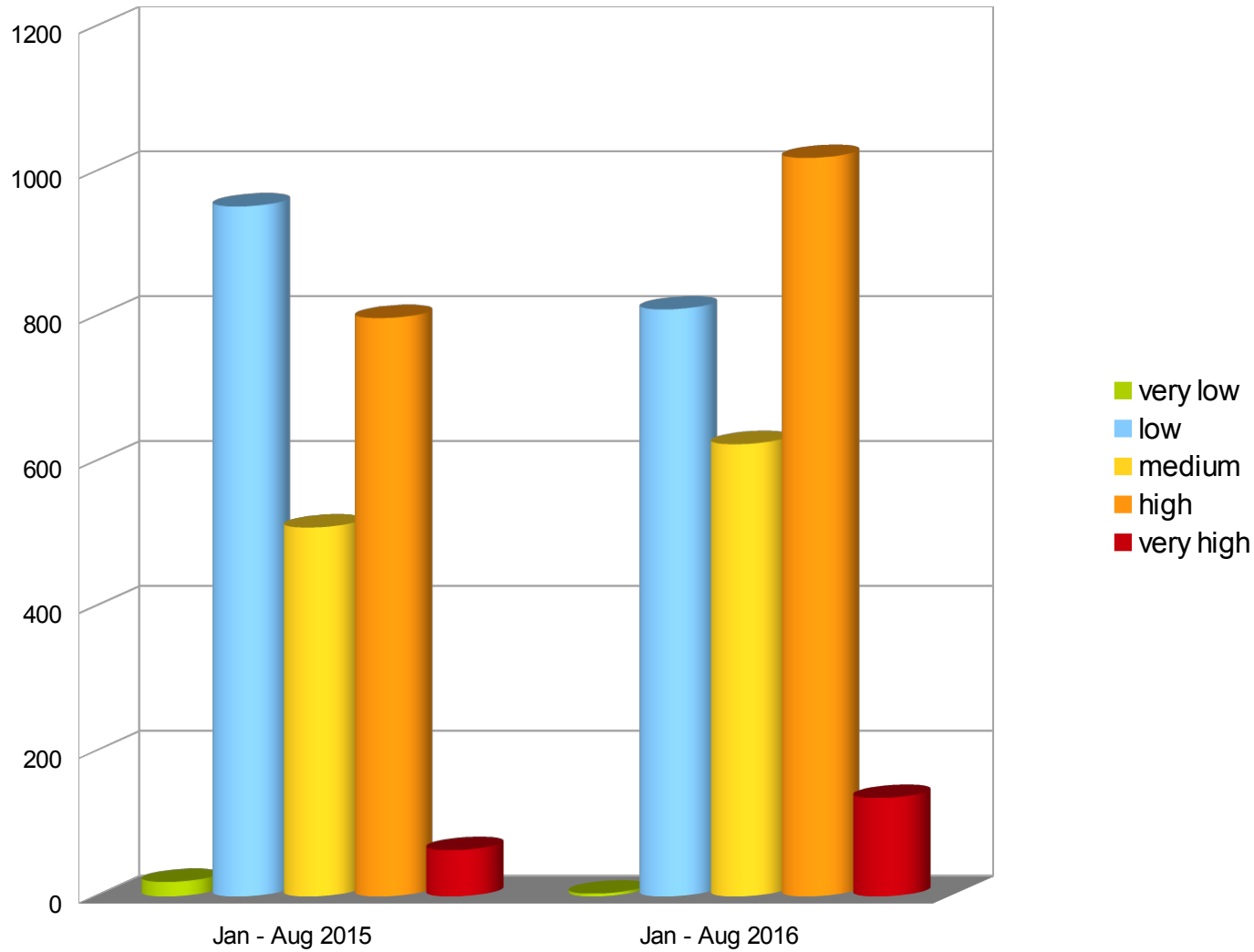
Anstieg:

2013 → 2014: 26,6%

2014 → 2015: 27,0%

2015 → 2016: < 10%

ADVs nach Schweregrad
Jan – Aug 2015 und 2016 im Vergleich



very high:

Anzahl verdoppelt im Vergleichs-zeitraum

low → high

Verschiebung des Schwerpunktes

DFN Deutsches Forschungsnetz

Abonnement: → Netzwerk

- **Primäre Unterstützung für FortiGate und FortiOS**

  Die FortiGate-Firewall ist eine integrierte Netzwerksicherheitslösung, die eine Firewall, Unified Threat Management und verschiedene Next-Generation-Firewall-Technologien wie VPN, Anwendungskontrolle, Anti-Malware, Intrusion Prevention ... beinhaltet.

- Damit hängen eng zusammen:
  - FortiClient → Endpunktsicherheit
  - FortiManager → Kontrolle der Sicherheitsrichtlinien, Sicherheitsupdates
  - FortiAnalyser → Logging, Reporting und Analysieren von FortiGate-Geräten

DFN Deutsches Forschungsnetz

Abonnement: → AIX, Linux, Solaris, Unix, Windows

- **IBM WebSphere Application Server (WAS)**

  Der IBM WAS ist ein Software-Framework und eine Middleware, die dazu dient, auf Java basierende Webanwendungen zu hosten. IBM WAS wurde unter Verwendung offener Standards wie Java EE und XML entwickelt.

- Nur die 'Core'-Version wird unterstützt. Für Produkte wie den WebSphere Application Server for Bluemix (Bluemix ist eine Cloud-Plattform) erstellen wir keine Advisories.

ADVs allgemein

Distributionen werden vollständig unterstützt, aber:

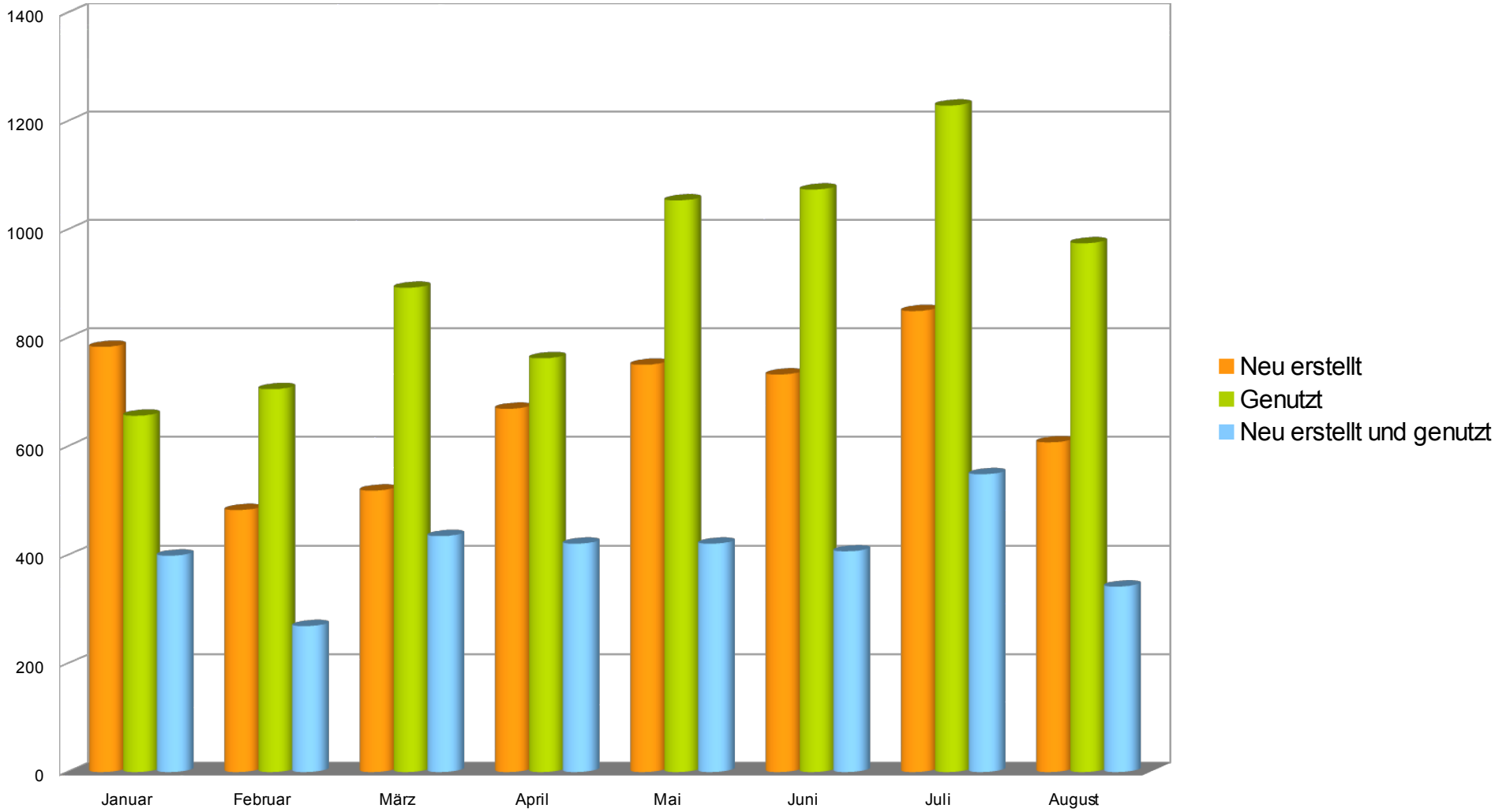
- **Keine Spiele**
- **Keine absoluten Spezialanwendungen**
  - z.B. Navigationsanwendung für Piloten
- **Sicherheitshinweise erstellen wir nur, wenn es sich wirklich (erkennbar) um Sicherheitsupdates handelt**
  - Manchmal werden Updates als 'Security' klassifiziert, es lässt sich aber nicht erkennen, dass mit dem Update wirklich Schwachstellen behoben wurden.
  - Mittels Bug Fix Releases oder Feature Enhancements werden zuweilen Schwachstellen adressiert.

Schwachstellen

Schwachstellen – Jan bis Aug 2016

Neu erstellt: 5398 **Genutzt 2015 gesamt: 7962** **Genutzt 2016: 7351**

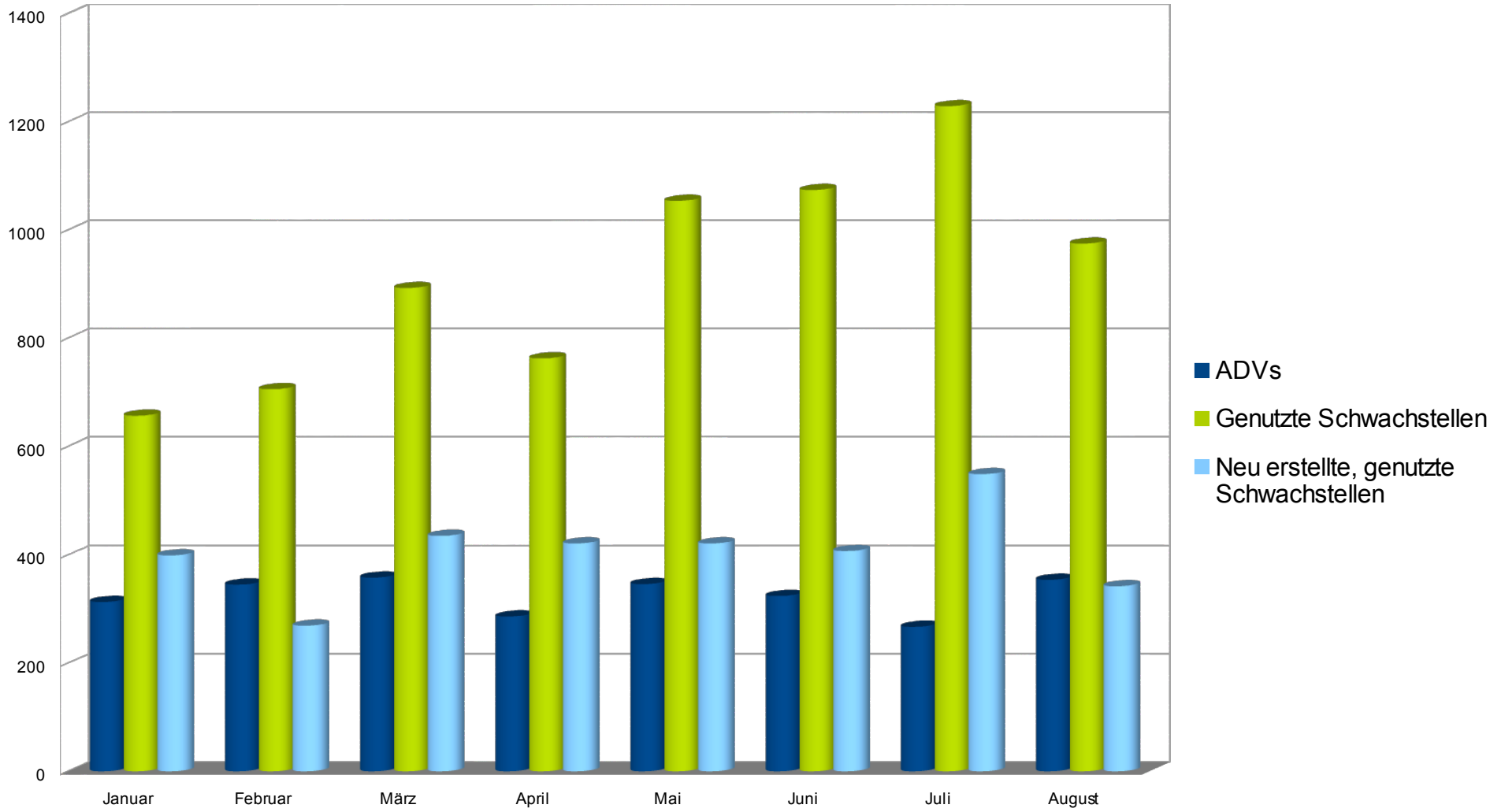
Neu erstellt und genutzt: 3243



Vergleich: ADVs und Schwachstellen

2015: ca. 2,2 CVEs pro ADV.

2016: ca. 2,8 CVEs pro ADV.



Spezielle Schwachstellen - httpoxy

CVE-2016-5385 (PHP, Skriptsprache),

CVE-2016-5386 (Go, kompilierbare Programmiersprache),

CVE-2016-5387 (Apache HTTP-Server),

CVE-2016-5388 (Apache Tomcat),

CVE-2016-1000212 (lighttpd Webserver),

CVE-2016-6286, CVE-2016-6286 (nicht spez. nach NVD),

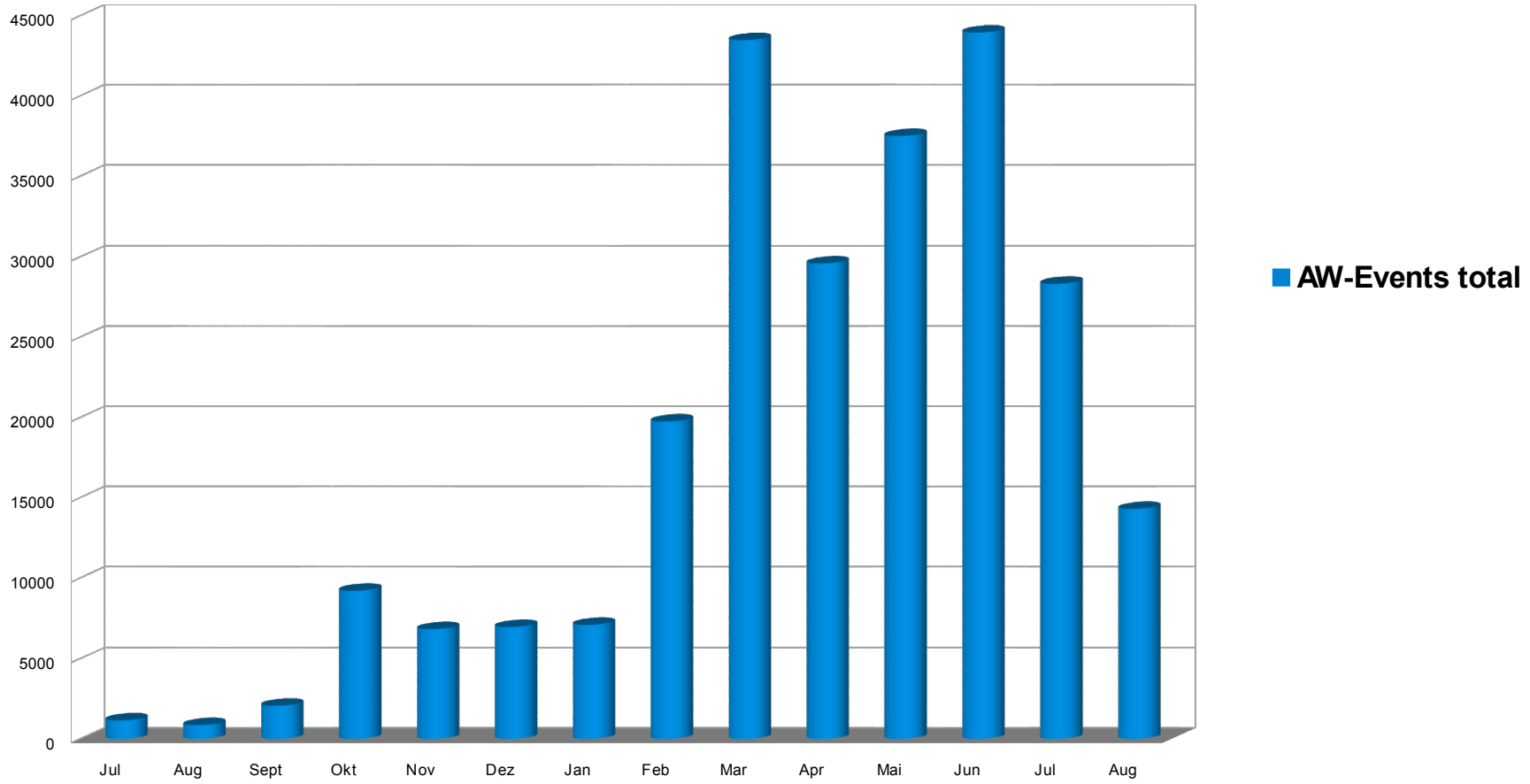
CVE-2016-1000104 (Apache HTTP-Server, mod_fcgi)

- Eigentlich keine Schwachstelle, Verhalten konform zu RFC 3875 Sektion 4.1.18 (The Common Gateway Interface, CGI).
- Durch einen präparierten Proxy-Header in einem HTTP-Request kann der ausgehenden HTTP-Verkehr einer Anwendung auf einen beliebigen, schädlichen Proxy-Server umgeleitet werden.

Vorfälle

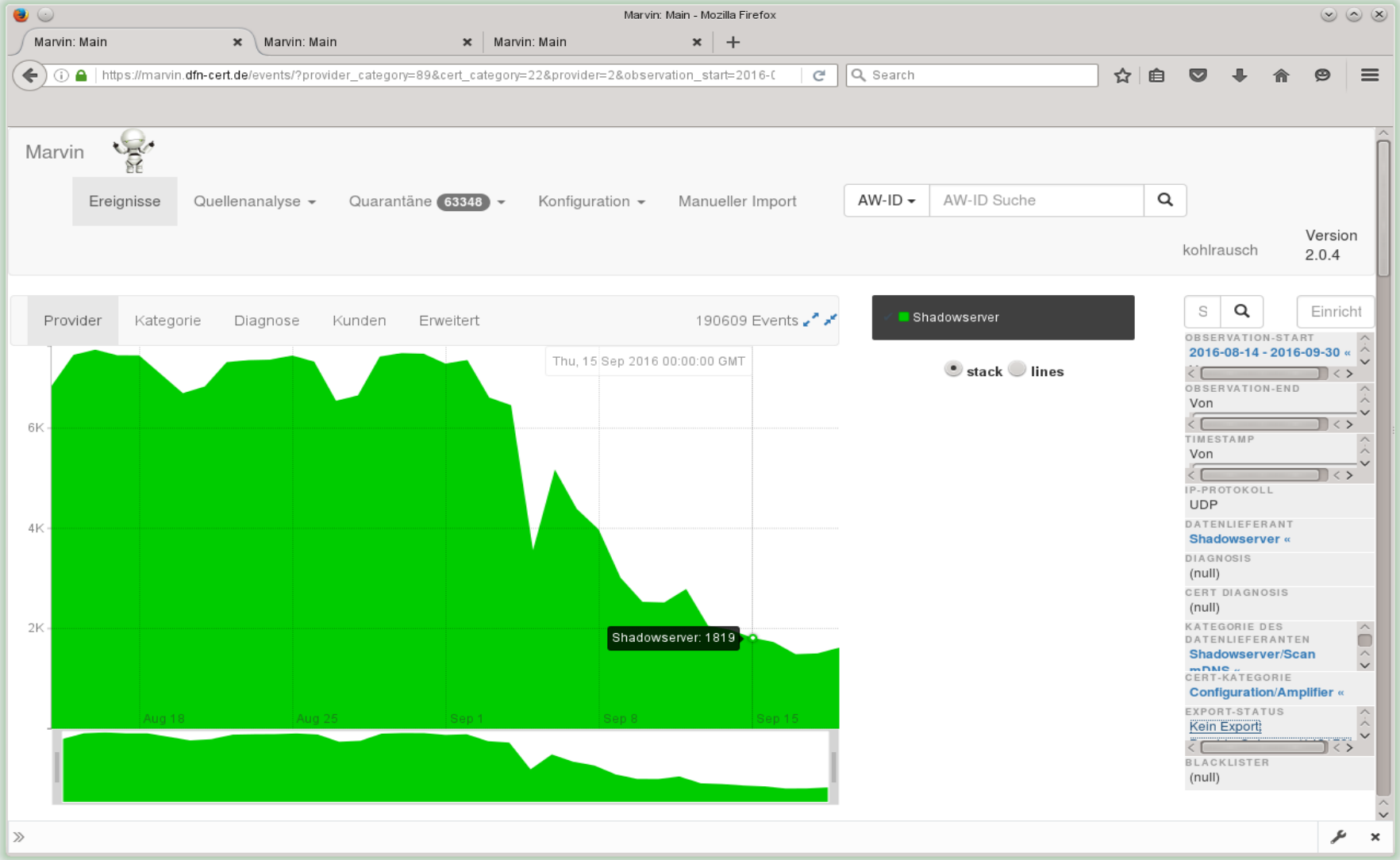
AW-Dienst, Gesamtzahl der Events

- **Anzahl Meldungen: seit Juli rückläufig**
- **Verschiebung: bisher Bot bei 90%, im August Bot und Konfig-Probleme fast gleich gewichtet**



Kleine Erfolgsgeschichte

DDoS-Reflektor-Angriffe, die auf Multicast DNS (mDNS) Anfragen beruhen



Verbünde & Re-Zertifizierung

DFN-CERT ist Mitglied

im CERT-Verbund

- Allianz deutscher Sicherheits- und Computer-Notfallteams, bzw. deutschsprachiger Teams
- Teams aus der öffentlichen Verwaltung (Bund, Land), von Großunternehmen und Mittelständlern und aus der Forschung
- Keine kommerziellen Interessen, sondern Verbesserung der operativen Sicherheit
  - Prüfung der fachlichen Qualifikation im Rahmen des Aufnahmeprozesses
  - NDA und gute Vertrauensbeziehung, um offen kommunizieren zu können
  - Zweimal jährlich Arbeitstreffen (im November in Hamburg)
- Lebt durch das Engagement der Mitglieder
- Wer sich mehr engagieren möchte und den Code of Conduct unterschreibt, kann im Lenkungskreis mitarbeiten

DFN-CERT ist Mitglied

bei FIRST

- **F**orum for **I**ncident **R**esponse and **S**ecurity **T**eams
- Globaler Verbund mit mehr als 300 Mitgliedern
- 1x jährlich FIRST-Konferenz (General Meeting) + sehr viele weitere Konferenzen und Meetings

bei TF-CSIRT Trusted Introducer

- Europäischer Verbund (plus Ausnahmen aus dem asiatischen Raum)
- Wie die beiden anderen Verbände nimmt TI eine Basisüberprüfung der Teams vor, die aufgenommen werden möchten, **aber** zusätzlich gibt es ein Akkreditierungs- und Zertifizierungs-Schema, das etwas über den Reifegrad eines Teams aussagt
- i.d.R. 3x jährliche Arbeitsmeetings
- Wichtiger Aspekt: Weiterbildung

DFN-CERT wird Re-Zertifiziert

- **Erstmalig zertifiziert 2012**
  - Prüft die Reife des **S**ecurity **I**ncident **M**anagements (**SIM**)
  - SIM3 → Maturity Parameters, Quadrants und Levels
  - 45 Parameter aus den Bereichen 'Organisation', 'Human', 'Tools' und 'Processes'
  - 5 Bewertungslevel von
    - 'not available'
    - 'implicit' (bekannt aber nicht aufgeschrieben)
    - 'explicit internal' (aufgeschrieben aber nicht formalisiert)
    - 'explicit formalised' (veröffentlicht)
    - 'subject to control process'

DFN-CERT wird Re-Zertifiziert

- **'Organisation'**
  - Rückhalt im Management
  - Auftrag von welchem Kundenkreis
  - Dienstbeschreibung
  - Incident Klassifikationsschema
  - Vernetzung
  - Sicherheitsrichtlinie

- **'Human'**
  - Code of Conduct
  - Vertretungsregelungen
  - Skillset
  - Trainings intern und extern

DFN-CERT wird Re-Zertifiziert

- **'Tools'**
  - Eingesetze Werkzeuge
    - Insbesondere Tracking von Incidents
      → seit Ende August: OTRS
  - Quellen
  - Erreichbarkeiten per E-Mail und Telefon (das wird auch geprüft)

- **'Processes'**
  - Eskalationsprozesse
  - Prävention
  - Detektion
  - Lösungsprozess
  - Verbesserungsprozesse
  - Umgang mit vertraulichen Informationen

Status aktuell: 'all is fine now for re-certification'

Vielen Dank für Ihre Aufmerksamkeit!

DFN-CERT Hotline:

- cert@dfn-cert.de
- 040 / 808 077-590

Weitere Informationen unter:
https://www.cert.dfn.de/