

# Neuer Dienst im DFN-CERT Portal

51. DFN-Betriebstagung Berlin

6. Oktober 2009

Marcus Pattloch (cert@dfn.de)

- Das DFN-CERT Portal (Stufe 1)
  - Überblick / Automatische Warnmeldungen
- Neuer Dienst: Information über Schwachstellen
  - bisher über win-sec-ssc (aber einige Defizite)
  - jetzt stark verbessert
- Das DFN-CERT Portal (Stufe 2)
  - Information zu Schwachstellen integriert  
(Archiv, Konfiguration, etc.)
- Zusammenfassung

# Das DFN-CERT Portal (Stufe 1)

## DFN-CERT Portal

### Automatische Warnmeldungen



Deutsches  
Forschungsnetz

Willkommen **Automatische Warnmeldungen** Hilfe

**Übersicht** Konfiguration Informationen

#### Automatische Warnmeldungen - AW-Dienst

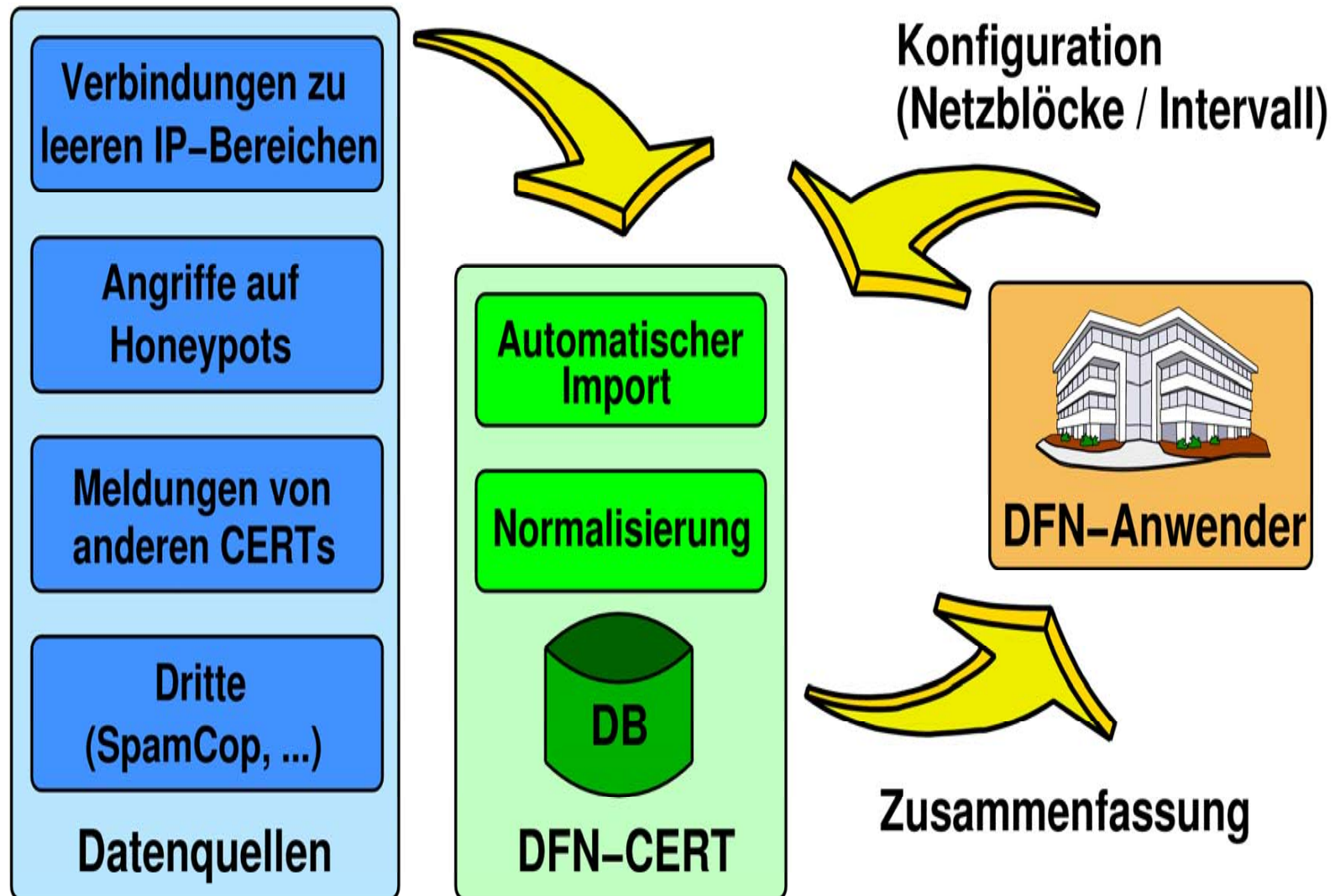
- Bitte wählen Sie **Konfiguration**, um Ihre Netzbereiche für den AW-Dienst zu konfigurieren oder zu ändern. Kurze Erläuterungen zu den Möglichkeiten finden Sie als Tooltips in der Konfigurationstabelle.
- Bitte wählen Sie **Informationen** für weitere Informationen und eine ausführliche Anleitung zum AW-Dienst.

[Impressum](#)

- Ziel des DFN-CERT Portals
  - einheitlicher Zugriff auf Dienste des DFN-CERT
  - flexible Konfiguration je Einrichtung
- Eingeführt im Rahmen der letzten DFN-BT
  - 1. Dienst: Automatische Warnmeldungen (AW)
  - Zugriff mit Zertifikat der DFN-PKI Global
  - Möglichkeit der passgenauen Konfiguration
- Statistik der Nutzung
  - großer Erfolg: seit Einführung auf letzter BT nehmen bereits mehr als 150 Einrichtungen teil

- Grundlegende Idee des Dienstes
  - das DFN-CERT sammelt Informationen zu möglichen Sicherheitsproblemen
    - Registrierung bei SPAM- / Security-Communities
    - automatisierte Suche in Foren / Listen
    - Auswertung der Daten aus eigenen Sensoren
  - Überführung in einheitliches Format
  - Korrelation und Zusammenfassung der Daten
  - Benachrichtigung der DFN-Anwender mit genauer Angabe der betroffenen Systeme

# Schema des AW-Dienstes



# Beispiel Warnmeldung

Liebe Kolleginnen und Kollegen,

dies ist eine automatische Warnmeldung des DFN-CERT. In den letzten Tagen erhielten wir Informationen über mögliche Sicherheitsprobleme auf Systemen in ihrem Netzwerk.

IP	Meldungstyp	Zuletzt gesehen
xxx.xxx.149.100	Virus/Wurm: Stormworm	2009-01-29 09:00:01
xxx.xxx.149.33	Spam-Beschwerde	2009-01-29 19:20:03

Weitere Informationen zu den Meldungstypen finden Sie auf den Seiten des DFN-Vereins unter: [www.cert.dfn.de/autowarn](http://www.cert.dfn.de/autowarn)

Wir bearbeiten den Vorfall als DFN-CERT#33277 und stehen natürlich für Rückfragen unter [<cert@dfn-cert.de>](mailto:cert@dfn-cert.de) zur Verfügung.

- DFN-Dienst „Automatische Warnmeldungen“
  - mehr als 150 Einrichtungen nehmen bisher teil
  - umfasst ca. 70% der IP-Adressen im X-WiN
  - Anwender bisher über mehr als 30.000 Vorfälle informiert, ca. 200 neue Vorfälle pro Tag
- Wichtigste Kategorien von Vorfällen
  - übernommener Rechner ist aktiver Teil eines Botnetzes („Conficker“)
  - übernommener Rechner versendet Spam
- Erkenntnis: Der Dienst wird angenommen

# **Neuer Dienst: Information über Schwachstellen**

Liebe Kolleginnen und Kollegen,

soeben erreichte uns nachfolgende Warnung des Microsoft Product Security Notification Service. Wir geben diese Informationen unverändert an Sie weiter.

CVE-2009-2496 - Schwachstelle in WC10.Spreadsheet.BorderAround()

Die Microsoft Office Components (OWC) Spreadsheet ActiveX Control ueberprueft die Parameter der Methode BorderAround() nicht ...

Betroffen sind die folgenden Software Pakete und Plattformen: ...

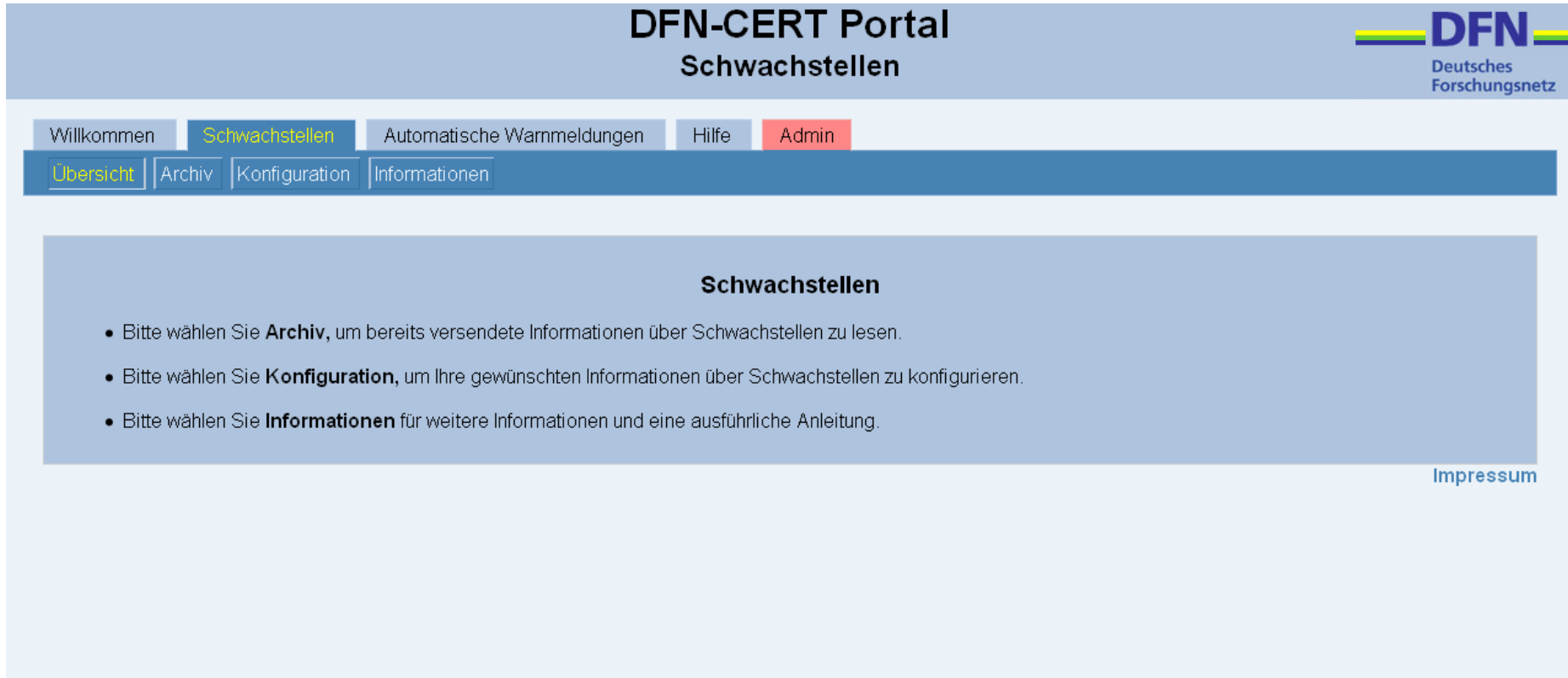
Vom Hersteller werden ueberarbeitete Pakete zur Verfuegung gestellt ...

- Seit Jahren etabliert
  - Mailingliste „win-sec-ssc“
  - Tausende von Nutzern (oft lokale Listen)
  - mehr als 1.000 Infos pro Jahr
- Defizite erkannt
  - man bekommt alles oder nichts (damit auch viele Meldungen zu Systemen, die man gar nicht hat)
  - nur ein Format verfügbar (manchmal überladen)
  - kein Archiv

- Grundidee gleich, aber viele Verbesserungen
  - gezielte Auswahl, d.h. man bekommt nur das, was man auch haben will
  - Archiv
  - Lang- und Kurzformat
- Und: integriert in das DFN-CERT Portal
  - Dienst kann ab sofort von „allen“ genutzt werden
  - Oktober 2009: Pilotphase
    - grundsätzlich alle Funktionen vorhanden
  - ab November 2009 Regelbetrieb

# **Das DFN-CERT Portal (Stufe 2)**

# Screenshot: Übersicht



The screenshot shows the DFN-CERT Portal interface for the 'Schwachstellen' (Vulnerabilities) section. The page has a light blue header with the title 'DFN-CERT Portal Schwachstellen' and the DFN logo. Below the header is a navigation bar with buttons for 'Willkommen', 'Schwachstellen', 'Automatische Warnmeldungen', 'Hilfe', and 'Admin'. A secondary navigation bar contains buttons for 'Übersicht', 'Archiv', 'Konfiguration', and 'Informationen'. The main content area features a blue box with the heading 'Schwachstellen' and a list of instructions. A link for 'Impressum' is located in the bottom right corner of the content area.

## DFN-CERT Portal Schwachstellen

Willkommen Schwachstellen Automatische Warnmeldungen Hilfe Admin

Übersicht Archiv Konfiguration Informationen


### Schwachstellen

- Bitte wählen Sie **Archiv**, um bereits versendete Informationen über Schwachstellen zu lesen.
- Bitte wählen Sie **Konfiguration**, um Ihre gewünschten Informationen über Schwachstellen zu konfigurieren.
- Bitte wählen Sie **Informationen** für weitere Informationen und eine ausführliche Anleitung.

[Impressum](#)

# Screenshot: Archiv

## DFN-CERT Portal Schwachstellen



Willkommen **Schwachstellen** Automatische Warnmeldungen Hilfe Admin

Übersicht **Archiv** Konfiguration Informationen


Hier können Sie das Archiv der bisher vom DFN-CERT verschickten Informationen über Schwachstellen durchsuchen.

Alle Systeme

Die neuesten Schwachstellenmeldungen:

- [17.09.2009 DFN-CERT-2009-1309: \[Linux, Debian\] Schwachstelle in den International Components for Unicode \(ICU\)](#)
- [16.09.2009 DFN-CERT-2009-1308: \[Linux, Unix, Solaris, Windows\] Schwachstellen in StarOffice/StarSuite](#)
- [16.09.2009 DFN-CERT-2009-1307: \[Linux, Mandriva\] Mehrere Schwachstellen im SILC-Client und -Toolkit](#)
- [16.09.2009 DFN-CERT-2009-1306: \[Unix, HP-UX\] Schwachstelle im bootpd](#)
- [16.09.2009 DFN-CERT-2009-1305: \[Linux, Debian\] Schwachstelle in OpenSSL](#)
- [16.09.2009 DFN-CERT-2009-1304: \[Linux, Debian\] Schwachstelle in Ruby on Rails](#)
- [16.09.2009 DFN-CERT-2009-1303: \[Linux, Fedora\] Schwachstelle in nginx](#)
- [16.09.2009 DFN-CERT-2009-1302: \[Linux, Fedora\] Schwachstelle in Planet](#)
- [16.09.2009 DFN-CERT-2009-1301: \[Linux, Fedora\] Schwachstelle in Dovecot](#)
- [15.09.2009 DFN-CERT-2009-1300: \[Linux, Debian\] Mehrere Schwachstellen in Iceweasel](#)
- [15.09.2009 DFN-CERT-2009-1299: \[Linux, Debian\] Mehrere Schwachstellen in Xulrunner](#)
- [15.09.2009 DFN-CERT-2009-1296: \[Linux, RedHat\] Schwachstelle in der KDE 4 SSL Bibliothek](#)
- [15.09.2009 DFN-CERT-2009-1297: \[Linux, SuSE\] SuSE Sammeladvisory für die 38 KW](#)
- [15.09.2009 DFN-CERT-2009-1291: \[Linux, Fedora\] Schwachstellen in der Mozilla Browser Engine vor Version 3.5.3](#)
- [15.09.2009 DFN-CERT-2009-1295: \[Linux, RedHat\] Schwachstellen im RedHat Enterprise 4 Linux Kernel](#)
- [15.09.2009 DFN-CERT-2009-1294: \[Linux, Debian\] Schwachstelle in nginx](#)
- [15.09.2009 DFN-CERT-2009-1293: \[Linux, Mandriva\] Schwachstelle im Mandriva Linux Kernel](#)
- [15.09.2009 DFN-CERT-2009-1292: \[Unix, Solaris\] Schwachstelle in Pidgin](#)
- [15.09.2009 DFN-CERT-2009-1290: \[Linux, Fedora\] Schwachstellen in der Mozilla Browser Engine vor Version 3.0.14](#)
- [14.09.2009 DFN-CERT-2009-1289: \[Linux, Fedora\] Schwachstellen in puppet](#)

# Screenshot: Konfiguration



DFN  
Deutsches  
Forschungsnetz

## DFN-CERT Portal Schwachstellen

Willkommen Schwachstellen Automatische Warnmeldungen Hilfe Admin

Übersicht Archiv Konfiguration Informationen

Hier können Sie konfigurieren, welche Meldungen Sie erhalten möchten. Die Meldungen werden an die in Ihrem Zertifikat eingetragene E-Mail-Adresse geschickt.

Systeme	Format	Empfänger
<input type="checkbox"/> Linux <input type="checkbox"/> Debian <input type="checkbox"/> Fedora <input type="checkbox"/> Mandriva <input type="checkbox"/> RedHat <input type="checkbox"/> SuSE		
<input type="checkbox"/> Unix <input type="checkbox"/> AIX <input type="checkbox"/> FreeBSD <input type="checkbox"/> HP-UX <input type="checkbox"/> NetBSD <input type="checkbox"/> OpenBSD <input type="checkbox"/> Solaris	Langformat	ra@dfn.de <input type="button" value="Hinzufügen"/>
<input type="checkbox"/> Windows		
<input type="checkbox"/> Cisco		
<input type="checkbox"/> Grid		

# Umfang der Nutzung

	Archiv	Abo - Adresse aus Zertifikat	Abo - Adresse frei wählbar
Alle Nutzer ohne Zertifikat	✓	✗	✗
Alle Nutzer mit Zertifikat	✓	✓	✗
handlungsberechtigte Person mit Zertifikat	✓	✓	✓

Alle Zertifikate der DFN-PKI Global können genutzt werden.

- Der bisherige Dienst über die Mailingliste „win-sec-ssc“ wird von vielen genutzt
- Empfehlung zum Vorgehen
  - erst eigene Konfiguration über das DFN-CERT Portal einrichten
  - dann aus der „win-sec-ssc“ austragen (lassen)
    - Mail an [win-sec-ssc@lists.dfn-cert.de](mailto:win-sec-ssc@lists.dfn-cert.de)
    - Betreff: unsubscribe <Mailadresse>
    - also z.B.: unsubscribe pattloch@dfn.de
  - Achtung: oft über lokalen Verteiler abonniert
    - dann muss auch dort ausgetragen werden!

# Zusammenfassung

- Automatische Warnmeldungen
  - einer Ihrer Rechner ist kompromittiert
  - Rechner ist im Netz auffällig geworden
  - wir können die betroffene IP-Adresse benennen
  - reaktiver Dienst
- Information über Schwachstellen
  - grundsätzliches Problem ist bekannt geworden
  - Lösung meistens: Patches einspielen
  - proaktiver Dienst

- Portal: <https://portal.cert.dfn.de>
- DFN-CERT Portal nun mit zwei Diensten
  - Automatische Warnmeldungen (erweitert)
  - Information über Schwachstellen (neu)
- (Pilot)Nutzung des neuen Dienstes ab sofort
  - Funktionsumfang abhängig von Zertifikat
- Mehr Infos im AK Sicherheit heute um 14:30 Uhr in diesem Raum und unter
  - Web: [www.cert.dfn.de/schwachstellen](http://www.cert.dfn.de/schwachstellen)
  - Mail: [cert@dfn.de](mailto:cert@dfn.de)