

Delivering services in a user-focussed way - The new DFN-CERT Portal -

29th TF-CSIRT Meeting in Hamburg

25. January 2010

Marcus Pattloch (cert@dfn.de)

How do we deal with the ever growing workload?

29th TF-CSIRT Meeting in Hamburg

25. January 2010

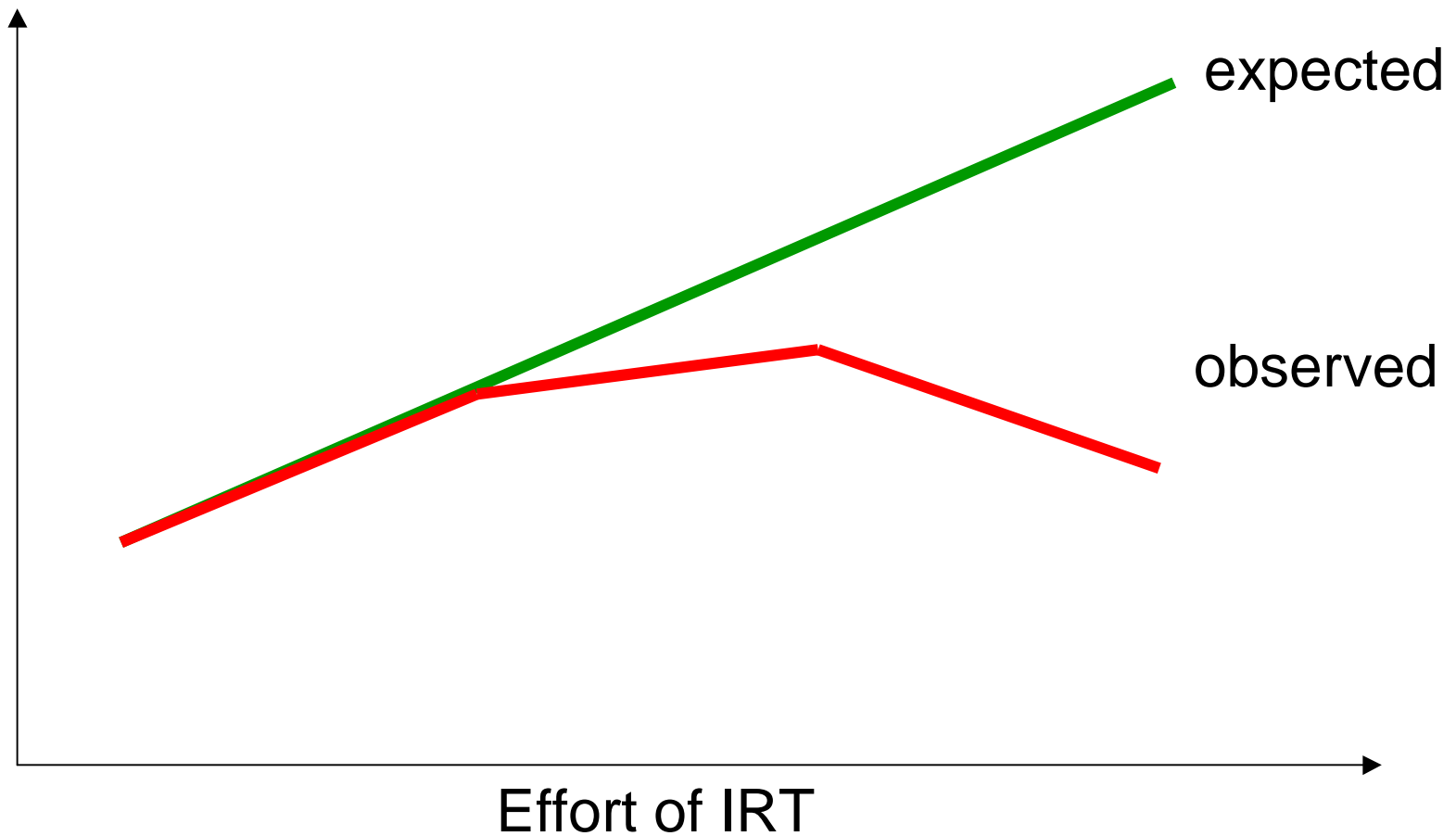
Marcus Pattloch (cert@dfn.de)

- DFN-CERT supports sites since 1993 with security related services
 - proactive (advisories, info on vulnerabilities)
 - reactive (incident response)
 - training (workshops, tutorials, ...)
 - national and international integration
- Well-established service for many years
 - e.g. security site contacts at all sites
 - but ...

- For some years there has been a problem with the sheer number of events, e.g.
 - several 1.000 new vulnerabilities per year
 - several 10.000 compromised computers per year just in our constituency
- As a result we have been sending out more and more information to our constituency
 - expecting our services to become better
 - but observing that the usefulness for our sites went down

work harder = better service?

“Usefulness” for
Constituency



- Only half a person works on security issues
 - few mails per day are OK
 - but 20 mails per day lead to „resignation“
- Local workflow / trouble-ticket systems in place
 - few mails per day are manually imported
 - (too) many mails are ignored
- Different people responsible in departments
 - few mails are redirected by site security contact
 - too many mails for other departments are dropped

Willkommen im DFN-CERT Portal, Marcus Pattloch.

Hier können Sie DFN-CERT Dienste für Ihre Einrichtung konfigurieren.

Zur Zeit stehen Ihnen folgende Möglichkeiten zur Verfügung:

- **Automatische Warnmeldungen** konfigurieren
- Informationen über **Schwachstellen** lesen und für sich konfigurieren
- **Hilfe** und Informationen zur Nutzung des DFN-CERT Portals anzeigen

Bitte wählen Sie eine Registerkarte

[Impressum](#)

<https://portal.cert.dfn.de>

- Configuration and information point for all sites.
- Customization per site based on user's certificate.

1. Advisories (proactive)

Example: Advisory

DFN-CERT-2009-1630: **Designschwäche im SSL/TLS Protokoll betrifft OpenSSL**

Betroffene Software:

Paket openssl

Betroffene Plattformen:

openSUSE 11.0

...

Aufgrund einer Designschwäche im SSL- und TLS-Protokoll sind verschiedene Programme, die die OpenSSL Bibliothek verwenden, anfällig für Man in the Middle Angriffe.

Weitere Informationen finden sie unter:

[<https://portal.cert.dfn.de/adv/DFN-CERT-2009-1630/>](https://portal.cert.dfn.de/adv/DFN-CERT-2009-1630/)

No one needs them all ...

- More than 2.000 advisories per year because of new vulnerabilities
 - esp. Windows, Linux, Unix
 - “Applications” (Java, VMware, Adobe, Office, ...)
 - Network (Cisco, Juniper, ...)
- Many sites only have a small amount of systems in house
 - thus they are not interested in all advisories
 - different departments have different systems in use; they want to configure that

Willkommen | **Schwachstellen** | Automatische Warnmeldungen | Hilfe

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.

Neues Abonnement anlegen

Systeme	Format	Empfänger	
<input checked="" type="checkbox"/> Linux <input type="checkbox"/> Debian <input type="checkbox"/> Fedora <input type="checkbox"/> Mandriva <input type="checkbox"/> RedHat <input type="checkbox"/> SuSE <input checked="" 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 <input type="checkbox"/> Windows <input type="checkbox"/> VMWare <input type="checkbox"/> Netzwerk <input checked="" type="checkbox"/> Cisco <input type="checkbox"/> HP	Kurzformat	pattloch@dfn.de	<input type="button" value="Ändern"/> <input type="button" value="Löschen"/>
<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 <input checked="" type="checkbox"/> Windows <input type="checkbox"/> VMWare <input type="checkbox"/> Netzwerk <input type="checkbox"/> Cisco <input type="checkbox"/> HP	Langformat	pattloch@dfn.de	<input type="button" value="Ändern"/> <input type="button" value="Löschen"/>

... configuration of systems, formats and recipients

Willkommen **Schwachstellen** Automatische Wammeldungen Hilfe Admin

Übersicht Archiv Konfiguration Konfiguration (HP) Informationen

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

Ihre Suchergebnisse (83 Treffer):

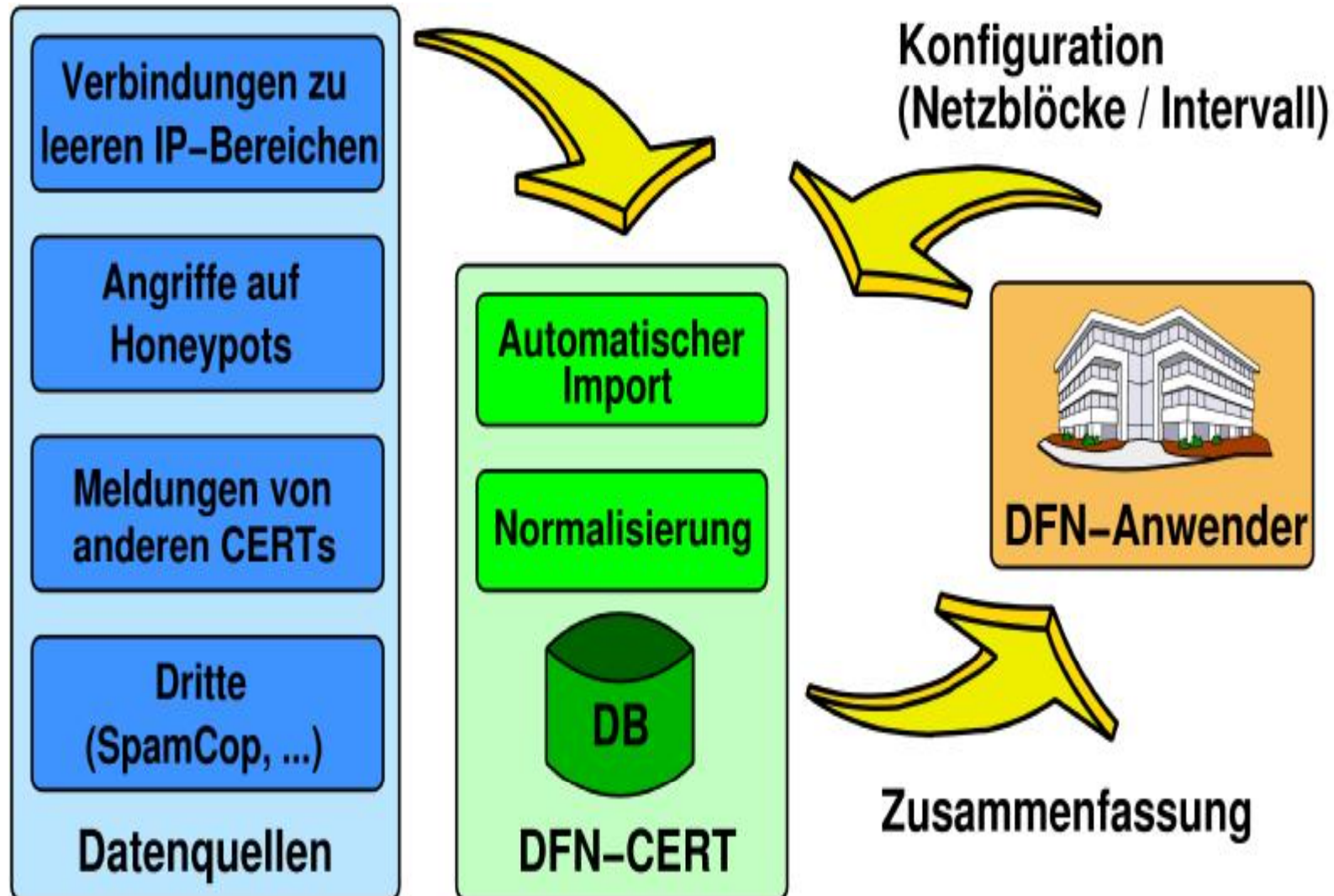
[erste Seite](#) | [vorherige Seite](#) | [1 / 5](#) | [nächste Seite](#) | [letzte Seite](#)

Datum	Titel	Systeme
17.11.2009	DFN-CERT-2009-1620: Mehrere Schwachstellen in OpenJDK bis einschließlich Version 1.6.0	Linux, RedHat
16.11.2009	DFN-CERT-2009-1616: Mehrere Schwachstellen in SUN Java bis einschließlich Version 1.6.0	Linux, Fedora
13.11.2009	DFN-CERT-2009-1609: Mehrere Schwachstellen in IBM Java bis Version 1.6.0	Linux, RedHat
11.11.2009	DFN-CERT-2009-1598: Mehrere Schwachstellen in SUN Java bis Version 1.6.0	Linux, RedHat
11.11.2009	DFN-CERT-2009-1597: Mehrere Schwachstellen in SUN Java bis Version 1.5.0	Linux, RedHat
10.11.2009	DFN-CERT-2009-1581: Mehrere Schwachstellen im Java Runtime Environment für HP-UX	HP-UX
10.11.2009	DFN-CERT-2009-1580: Mehrere Schwachstellen in Apache Tomcat	Linux, RedHat
10.11.2009	DFN-CERT-2009-1579: Mehrere Schwachstellen in Apache Tomcat	Linux, RedHat
06.11.2009	DFN-CERT-2009-1564: Schwachstellen in Mozilla Firefox vor Version 3.5.4	Linux, Mandriva
05.11.2009	DFN-CERT-2009-1563: Schwachstellen in der Mozilla Browser Engine vor Version 3.0.15	Linux, RedHat
05.11.2009	DFN-CERT-2009-1554: Schwachstellen in Mozilla Firefox vor Version 3.0.15	Linux, SuSE
05.11.2009	DFN-CERT-2009-1552: Schwachstellen in IBM Java	Linux, SuSE
04.11.2009	DFN-CERT-2009-1543: Schwachstellen in JDK und JRE vor Version 6 Update 17	Linux, Unix, Solaris, Windows
03.11.2009	DFN-CERT-2009-1541: Schwachstelle im GlassFish Server bei der Auswertung von XML Signaturen	Linux, RedHat, Unix, AIX, Solaris, Windows
30.10.2009	DFN-CERT-2009-1535: Diverse Schwachstellen in Mozilla Firefox vor Version 3.0.15	Linux, Mandriva
29.10.2009	DFN-CERT-2009-1531: Schwachstellen in der Mozilla Browser Engine vor Version 3.0.15	Linux, RedHat
29.10.2009	DFN-CERT-2009-1532: Schwachstellen in Xulrunner / Mozilla Browser Engine vor Version 3.0.15	Linux, Debian
28.10.2009	DFN-CERT-2009-1530: Schwachstelle in Expat	Linux, Debian
28.10.2009	DFN-CERT-2009-1525: Mehrere Schwachstellen in Seamonkey vor Version 2.0	Linux, RedHat
28.10.2009	DFN-CERT-2009-1524: Diverse Schwachstellen in Mozilla Firefox vor Version 3.0.15	Linux, RedHat

... searchable archive of all advisories

2. Incident Warning (reactive)

How we know about incidents ...



Example: Incident Warning

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	2009-10-29 09:00:01
xxx.xxx.149.33	Spam-Beschwerde	2009-10-29 19:20:03

<„*detailed information follows*“>

...

... we have about 10.000 incident warnings per year just for our constituency!

Willkommen Schwachstellen **Automatische Warnmeldungen** Hilfe

Übersicht **Konfiguration** Informationen

Name Ihrer Einrichtung: DFN-Geschäftsstelle

Netzbereiche anzeigen

Neue Regel einfügen

Die Regeln werden in der angegebenen Reihenfolge von oben nach unten bearbeitet. Nur die erste passende Regel wird angewendet.

Aktiv?	Netzbereiche	Intervall	Leermeldungen?	Empfänger	Betreff	
↓ Ja	193.174.247.0/24 193.174.1.160/28 194.95.237.0/24 194.95.247.0/24 195.37.61.224/27 195.37.209.100/30 195.37.209.112/30	Mo - Fr	Nein	admin@sgs.dfn.de cert@dfn.de	DFN-SGS	Ändern Löschen
↑ ↓ Ja	194.95.240.0/24	Mo - Fr	Nein	admin@sgs.dfn.de cert@dfn.de	DFNVC	Ändern Löschen
↑ Ja	193.174.167.0/24	Mo - Fr	Nein	cert@dfn.de	CASG Adressraum	Ändern Löschen
Ja	Alle übrigen	Mo - Fr	Ja	cert@dfn.de	Alles Regel	Ändern

... configuration of network ranges and recipients

Automatically processable

```
<?xml version="1.0" encoding="utf-8" ?>
<warning incidentid="11023">
<message ip="183.22.xx.yy" timestamp="2009-11-01 21:45:05"
type="Bot">
<logrecord> TCP Quellport Malwaretyp
Zeitstempel(GMT+0000)
```

```
-----
unbekannt   Conficker      2009-11-01 21:45:05
unbekannt   Conficker      2009-11-01 20:57:23
```

```
</logrecord>
```

```
<description>Auf dem System scheint eine Bot-Software betrieben zu
werden, die versucht, einen HTTP- oder IRC-basierten Bot-Netz
Control-Server zu erreichen. Zu den unterschiedlichen Malwaretypen
finden Sie unter der folgender Webseite mehr Informationen:
http://www.cert.dfn.de/index.php?id=bot</description> ....
```

3. “Network Scanner” (due in spring 2010)

Willkommen Schwachstellen Automatische Warnmeldungen **Netzwerkprüfer** Hilfe Admin

Übersicht **Scan-Auftrag** Scan-Ergebnisse Informationen

Name Ihrer Einrichtung: DFN-Geschäftsstelle

Netzbereiche anzeigen

Bitte geben Sie die zu prüfende IP-Adresse oder den zu prüfenden Netzbereich ein.

IP-Adresse oder Netzbereich:

Type in IP-addresses of your site to be “checked” ...

Willkommen Schwachstellen Automatische Warnmeldungen **Netzwerkprüfer** Hilfe Admin

Übersicht Scan-Auftrag **Scan-Ergebnisse** Informationen

Name Ihrer Einrichtung: DFN-Geschäftsstelle

Auftragsdatum	Netzbereich	Status	
18.11.2009	192.76.176.1	Fertig	 
19.11.2009	192.76.176.1	Fertig	 
19.11.2009	192.76.176.3	Fertig	 
19.11.2009	192.76.176.0/24	Fertig	 

... results will show open ports, services, their versions, vulnerabilities, links to patches, etc

- DFN-CERT Portal central configuration and information point for all DFN-sites
 - consolidate information in a consistent portal structure
 - offer mechanisms to configure services per site
 - send each site (each department) only information that is relevant to them
 - data can easily be integrated into local processes
- The Portal cannot replace direct support in severe cases, but it gives the IRT-experts the time to give that support!