QUO VADIS, IT-SICHERHEIT?

Dr. Thomas Eisenbarth

Was wird das hier?

IT-Security-Comedy

Was war 2014, was wird 2015. Und: Industrie 4.0!

IT-SICHERHEIT?
WIR KAPITULIEREN!

IT-SICHERHEIT?

~~WIR KAPITULIEREN~~

WIR HABEN KAPITULIERT!

Microsoft Security Bulletin MS15-011

"Vulnerability in Group Policy Could Allow Remote Code Execution (3000483)"

THIS SECURITY UPDATE IS RATED CRITICAL FOR ALL SUPPORTED EDITIONS OF...

- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Windows 7
- Windows Server 2008 R2
- Windows 8
- Windows Server 2012
- Windows RT
- Windows 8.1
- Windows Server 2012 R2 und Windows RT 8.1.

"SECURITY BY ANTIQUITY"

OHNE WORTE.

WIR KAPITULIEREN, EHRLICH!

JAVA

"Oracle’s update brings Java 7 to Update 75 and Java 8 to Update 31, and fixes at least 19 security vulnerabilities in the program."

"Security vendor Qualys notes that 13 of those flaws are remotely exploitable, with a CVSS score of 10 (the most severe possible score)."

1.7.0.72 kam im Oktober 2014 raus,
1.7.0.75 dann am 20. Januar

GOOGLE SECURITY-TEAM

...veröffentlich 0-day für Windows & OS X.

Project Zero, which Google officially launched in mid-2014, tasks researchers with uncovering any software flaws that have the potential of leading to targeted attacks on people's computers.

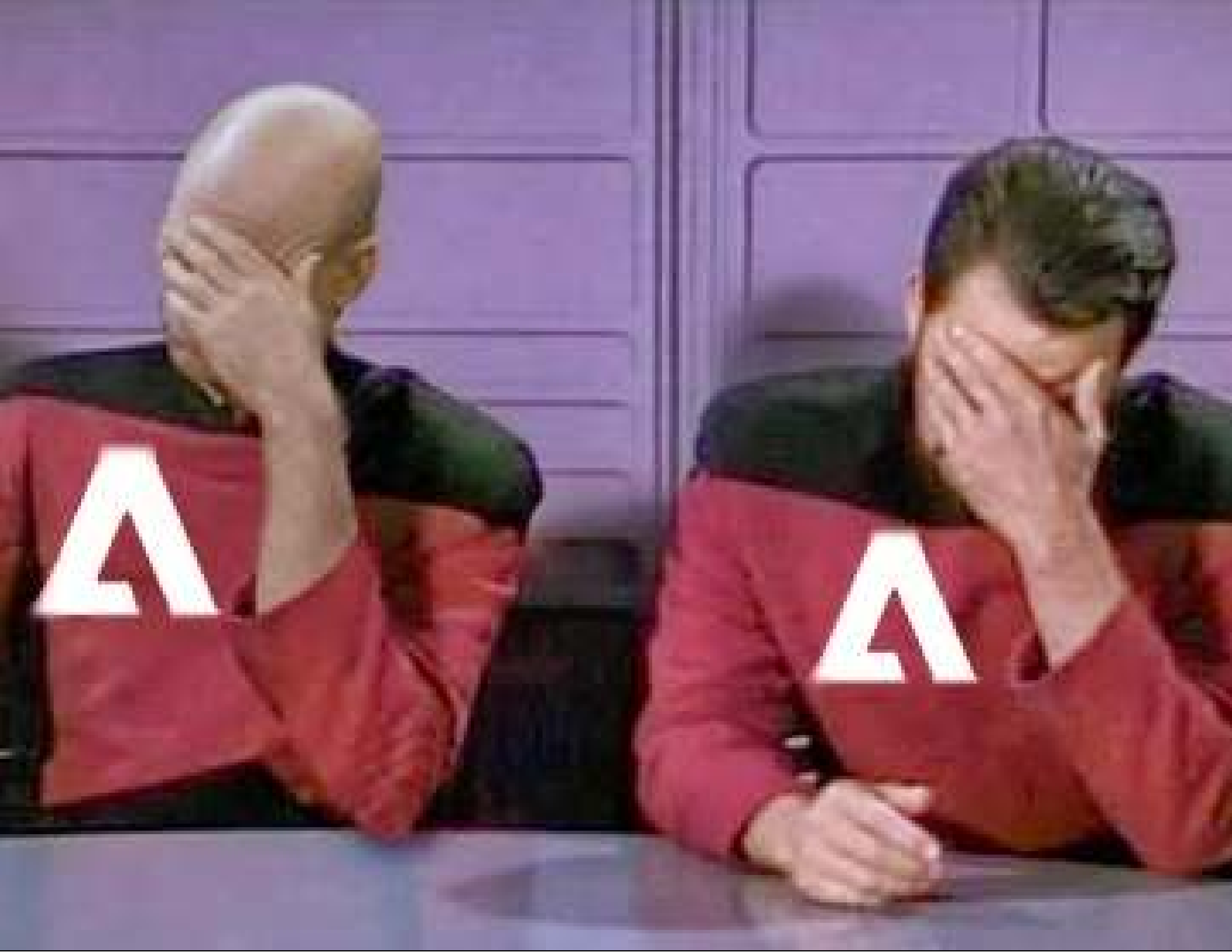
SECURITY-PARTY GOES ON!

KA-PI-TU-LIERT

FLASH

"Sicherheitslücke: Experten raten zum sofortigen Abschalten des Flash-Players" [SPON]

"Flash-Player deaktivieren! Schon wieder Angriffe auf ungepatchte Lücke" [heise.de]



Bonn


BONN
tagesschau

"Rund 40.000 MongoDB-Datenbanken standen völlig ungesichert im Internet."

NEIN!

Chef: "Wir müssen dieses NoSQL jetzt auch machen!"

```
sudo apt-get install mongodb redis riak memcached bigtable
voldemort

0 upgraded, 638 newly installed, 0 to remove and 2 not
upgraded. Need to get 67,7 GB of archives. After this
operation, 181 GB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Läuft!


FAIL

Socket auf 0.0.0.0 (oder ::) ist meistens nicht cool.

Schaut halt **einmal** mit nmap von aussen drauf.

... bevor es das BSI macht.

NEUES VON DER SSL-FRONT...
HEUTE: LIVE.FI

Gefälschtes Microsoft-Zertifikat im Umlauf

Microsoft warnt davor, dass Unbekannte es geschafft haben, ein SSL-Zertifikat für die Domain **live.fi** zu fälschen.

"Diese Domain wird dafür benutzt, die finnische Version der Windows Live Services bereitzustellen. Mit dem gefälschten Zertifikat könnte sich ein Angreifer in die gesicherte Verbindung zu den Microsoft-Servern einklinken und Daten abgreifen."

WIE KANN DAS DENN PASSIEREN?

WIE KOMMT MAN EIGENTLICH AN SSL-ZERTIFIKATE?

- Verkäufer und Produkt aussuchen (Thawte, Verisign, COMODO)
- CSR bauen und an Verkäufer schicken
- Domain verifizieren
- Zertifikat installieren

WIE KOMMT MAN EIGENTLICH AN SSL-ZERTIFIKATE?

- Domain validation
  E-Mail an bestimmte Adressen an Wunsch-Domain (z.B. ssladmin@your-domain.tld)
- Organization Validation
  Handelsregisterauszug, oft per Fax
- Extended Validation
  Telefonischer Kontakt, Unterschriften, Firmenstempel

LIVE.FI

"Diese Domain wird dafür benutzt, die finnische Version der Windows Live Services bereitzustellen."

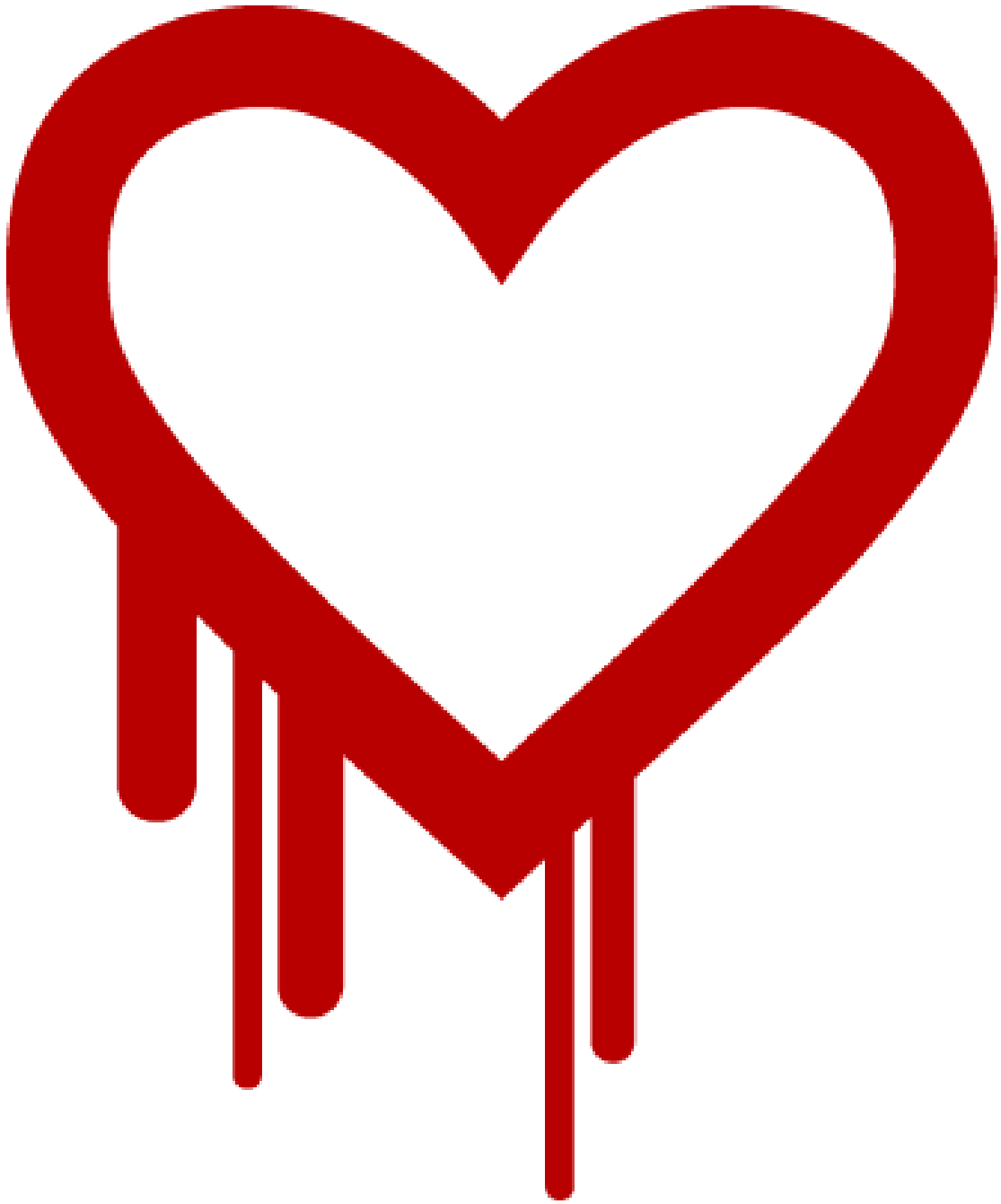
?

"Die Windows-Live-Dienste waren Windows Live Hotmail (vormals MSN Hotmail), Windows Live SkyDrive ..."

HACK!

- E-Mail bei live.fi registrieren,
  z.B. hostmaster@live.fi oder ssladmin@live.fi
- SSL-Zertifikat für live.fi beantragen, Validierung per E-Mail
- H4><0r3d.


MARCY



HEARTBLEED

Sicherheitslücke mit dem besten Marketing **ever.**

HEARTBLEED

Die Sau ist ja schon längst durchs Dorf.

Die Fragen die sich dennoch stellen...

- Warum gabs da so einen Wirbel drum?
  (das stand auf SPON!!!1)
- Wie konnte das denn schon wieder passieren?

OpenSSL ist verbreitet wie Hölle

Praktisch alles was SSL oder TLS terminiert (und nicht auf Windows läuft) ist mit relativ hoher Wahrscheinlichkeit OpenSSL. (Nicht böse sein, GnuTLS)

- nginx, Apache (HTTPs)
- Exim, Dovecot, Courier, ...
- OpenSSH
- diverse Appliances

WIE KONNTE DAS PASSIEREN?

OpenSSL ist eine C-Bibliothek

PUNKT

COMMIT

96DB9023B881D7CD9F379B0C154650D6C108E9A3

```
-       /* Read type and payload length first */
-       hbtype = *p++;
-       n2s(p, payload);
-       pl = p;
-
  if (s->msg_callback)
    s->msg_callback(0, s->version, TLS1_RT_HEARTBEAT,
      &s->s3->rrec.data[0], s->s3->rrec.length,
      s, s->msg_callback_arg);

+       /* Read type and payload length first */
+       if (1 + 2 + 16 > s->s3->rrec.length)
+               return 0; /* silently discard */
+       hbtype = *p++;
+       n2s(p, payload);
+       if (1 + 2 + payload + 16 > s->s3->rrec.length)
+               return 0; /* silently discard per RFC 6520 sec. 4 */
+       pl = p;
```

```
+       if (1 + 2 + 16 > s->s3->rrec.length)
+               return 0; /* silently discard */
+       hbtype = *p++;
+       n2s(p, payload);
+       if (1 + 2 + payload + 16 > s->s3->rrec.length)
+               return 0; /* silently discard per RFC 6520 sec. 4 */
+       pl = p;
```

Wo sind die Tests?


LOL

Das mit SSL geht weiter, keine Sorge.

POODLE, FREAK, BEAST, ...

```
# OpenSSL 1.0.1m:

Totals grouped by language (dominant language first):
ansic:       272198 (76.01%)
perl:         69147 (19.31%)
asm:           9007 (2.52%)
cpp:           4375 (1.22%)
sh:            3346 (0.93%)
lisp:            24 (0.01%)

Total Physical Source Lines of Code (SLOC) = 358,097
```

OPENSSL 1.0.1M ≈ 0,4 MIO SLOC

Year	OS	SLOC (Mio)
1994	Windows NT 3.5	7–8
1996	Windows NT 4.0	11–12
2000	Windows 2000	> 29
2001	Windows XP	45
2003	Windows Server 2003	50

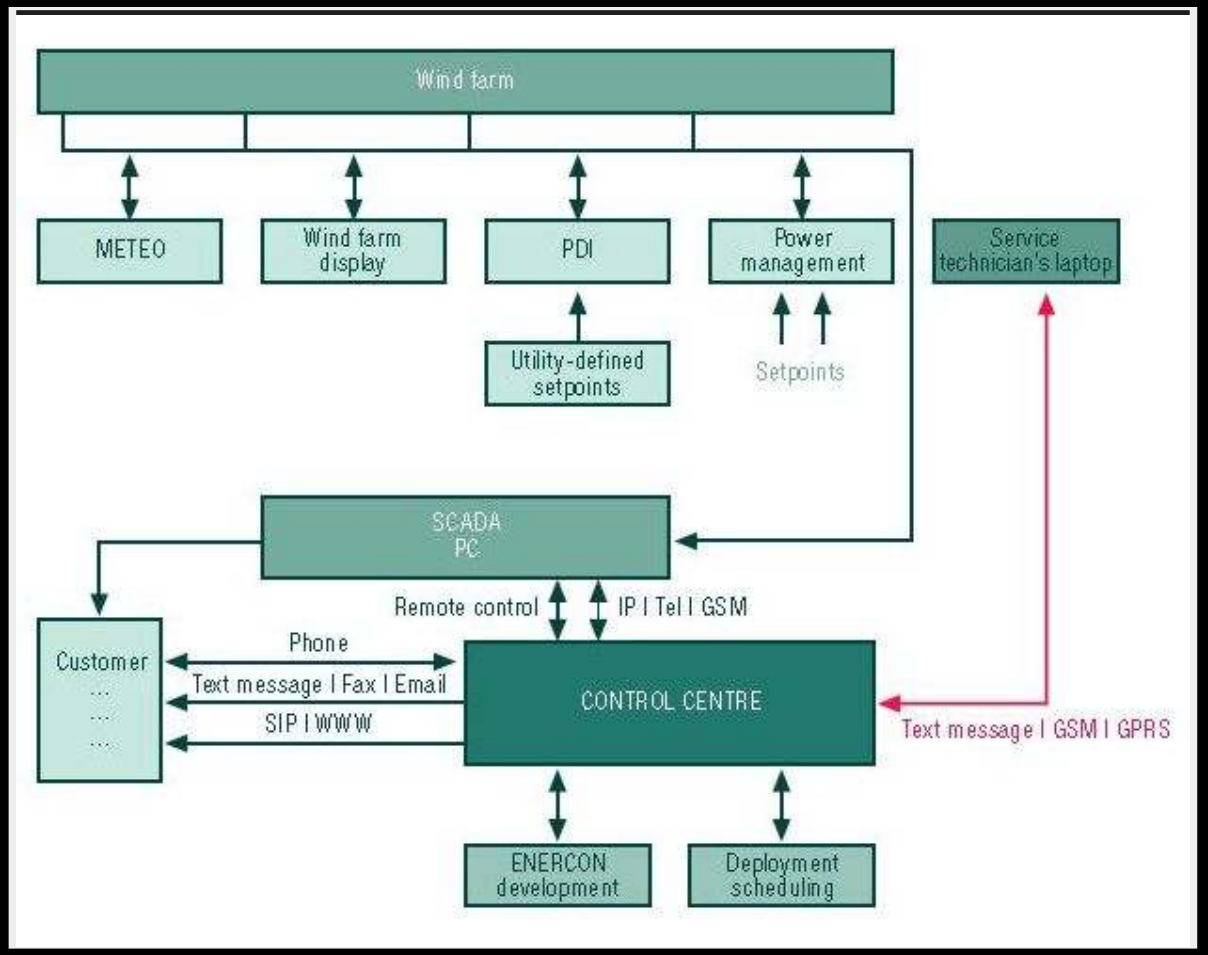
Year	OS	SLOC (Mio)
2010	Linux kernel 2.6.35	13.5
2012	Linux kernel 3.6	15.9
2000	Debian 2.2	55-59
2012	Debian 7.0	419

AUSBLICK

INDUSTRIE 4.0

Heisst dass wir künftig auf die offenen Redis und MongoDBs
auf Windrädern kucken können.
Oder so.

INDUSTRIE 4.0



Google ist so hilfreich!

"wind farm portal" 11.06.11
193.253.196.156
http://www.thewindpower.net/windfarm_de_586_les-moulins-de-boulay.php

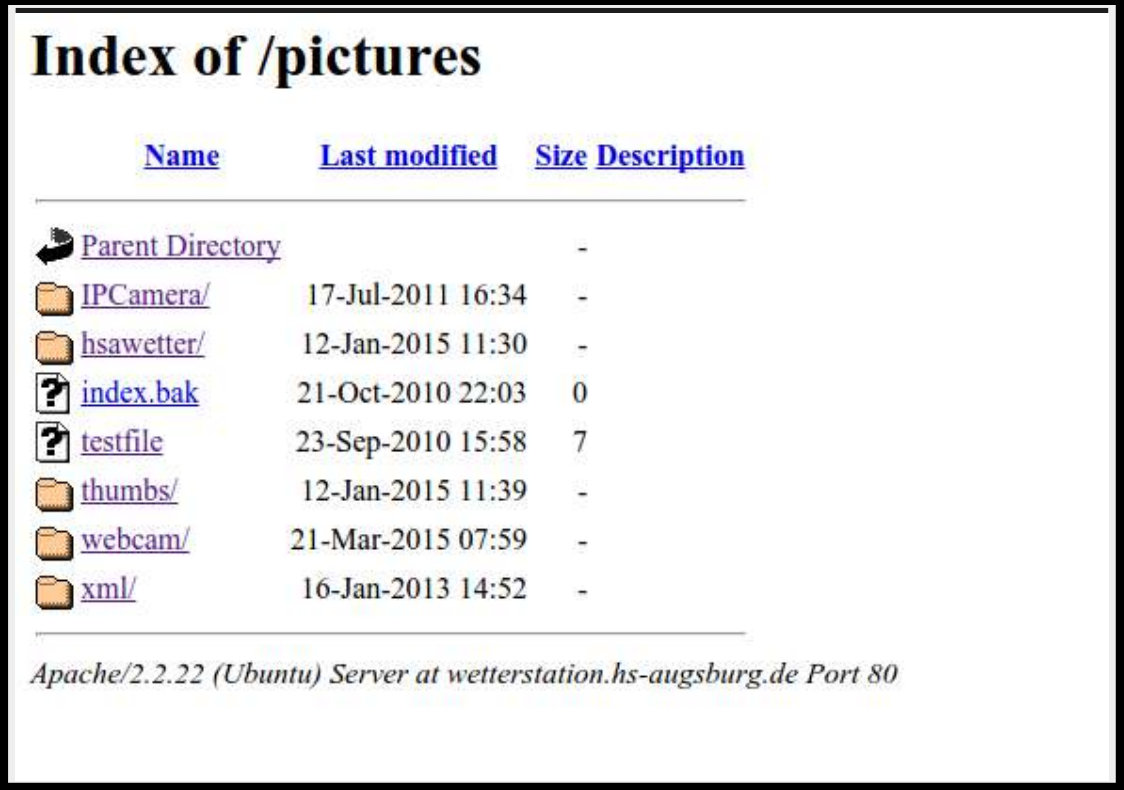
WETTER IN AUGSBURG...

http://wetterstation.hs-augsburg.de

```
rDNS record for 141.82.59.1: wetterstation.Informatik.FH-Augsburg.DE

Not shown: 809 closed ports, 188 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
3306/tcp open  mysql
8180/tcp open  unknown
```

ACH SCHAU AN



Index of /pictures

Name	Last modified	Size	Description
Parent Directory		-	
IPCamera/	17-Jul-2011 16:34	-	
hsawetter/	12-Jan-2015 11:30	-	
index.bak	21-Oct-2010 22:03	0	
testfile	23-Sep-2010 15:58	7	
thumbs/	12-Jan-2015 11:39	-	
webcam/	21-Mar-2015 07:59	-	
xml/	16-Jan-2013 14:52	-	

Apache/2.2.22 (Ubuntu) Server at wetterstation.hs-augsburg.de Port 80

INTERESSANT, EIN PHP-SCRIPT... "DATABASE.PHP"

```php
/*
 * Schnittstelle zum Zugriff auf die Wetterstationsdatenbank und zur Rückgabe als JSON Datei
 *
 * Autor: Markus Görlich
 *
 */

error_reporting(E_ALL);
```

AHA!

```
$Messdaten_Wetter = array("Temperatur", "Luftfeuchtigkeit",
                          "Luftdruck", "Windrichtung", "Ozon",
                          "Niederschlag", "Globalstrahlung", "PHWert");

$Messdaten_Solar = array("Pac", "ETotal", "Betriebszeit");

$Messdaten_Ceilometer = array("Wolkenhoehe", "Aerosol");
```

```
...
```

```
$db = mysql_connect("localhost", "root", "wetter") or
      die (mysql_error());
```

AUTSCH!

OH.

```
11:34:00 ✘ fnordomat ~ > mysql -uroot -p -h wetterstation.hs-augsburg.de
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 260523
Server version: 5.5.41-0ubuntu0.12.04.1 (Ubuntu)

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| Wetterdaten        |
| mysql              |
| performance_schema |
| test               |
| wikidb             |
+--------------------+
6 rows in set (0.55 sec)
```

```
mysql> use Wetterdaten;
mysql> select * from User;
+----+-------+----------------------------------+-------+-------------+-------------+------------+
| ID | Name  | Passwort                         | admin | wetterdaten | solaranlage | ceilometer |
+----+-------+----------------------------------+-------+-------------+-------------+------------+
|  1 | Admin | 3858f62230ac3c915f300c664312c63f |     1 |           1 |           0 |          0 |
+----+-------+----------------------------------+-------+-------------+-------------+------------+
```

DAS WIRD INDUSTRIE 4.0

UND NU?

"YOU ARE UNDER ATTACK"

WEITER VERSCHLÜSSELN!

Die Nachrichtendienste sollen sich ja nicht langweilen.

Apropos langweilen...

Informatiker/in (Master/Diplom) (TA/002-15)

Der Bundesnachrichtendienst (BND) sucht für die Abteilung Technische Aufklärung (TA) im Groß eine/n Informatiker/in (Master/Diplom).

Die Abteilung Technische Aufklärung (TA) gewinnt nachrichtendienstlich relevante Erkenntnisse durch die gezielte Filterung der internationalten Kommunikationsströme.

Aufgabenschwerpunkte

- Softwareentwicklung
- Projekt- / Entwicklungsdurchführung / Modifikation von Systemen
- Projektierung / Planung / Konzeption
- Planen, Koordinieren und Durchführen von Integrationsmaßnahmen
- Erstellung von Fachbeiträgen und Systemexpertisen

Anforderungsprofil

- abgeschlossenes Studium in der genannten Studienrichtung (Master/Diplom)

Informatiker/in (Master/Diplom) (TA/002-15)

Der Bundesnachrichtendienst (BND) sucht für die Abteilung Technische Aufklärung (TA) im Groß eine/n Informatiker/in (Master/Diplom).

Die Abteilung Technische Aufklärung (TA) gewinnt nachrichtendienstlich relevante Erkenntnisse durch die gezielte Filterung der internationalten Kommunikationsströme.

Aufgabenschwerpunkte

- Softwareentwicklung
- Projekt- / Entwicklungsdurchführung / Modifikation von Systemen
- Projektierung / Planung / Konzeption
- Planen, Koordinieren und Durchführen von Integrationsmaßnahmen
- Erstellung von Fachbeiträgen und Systemexpertisen

Anforderungsprofil

- abgeschlossenes Studium in der genannten Studienrichtung (Master/Diplom)

WERBUNG

makandra.de

www.buch7.de

Web & Wine

Nerdnight

CREDITS

www.flickr.com/photos/neolao/3105372669
ENERCON__11_Scada_Remote.png
www.bnd.de
www.flickr.com/photos/gaylon/28051605 / 28051605_288674c4c2_b
www.flickr.com/photos/robboudon/3040333241/ / 3040333241_839ef40ed3_o
www.flickr.com/photos/eyeliam/2539194260/ / 2539194260_67c3b3443a_o
Heartbleed-Logo

DANKE!