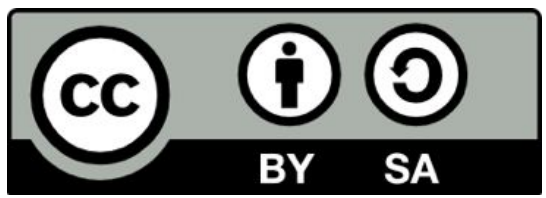
Security of Legacy Systems

Ing. DI(FH) Herbert Dirnberger, MA
Florian Brunner, MSc.

Security Forum 2014
9. - 10. April 2014
Hagenberg im Mühlkreis



CYBER SECURITY AUSTRIA

Verein zur Förderung der Sicherheit Österreichs strategischer Infrastruktur

- gemeinnützig
- unabhängig
- Sensibilisieren und Bewusstsein schaffen

”Sicherheit geht uns alle an!”

http://www.cybersecurityaustria.at

Herbert Dirnberger

- Automatisierung/Mechatronik
- Wirtschaftsinformatik/Security
- Automatisierungs- und Systemtechniker
- Leiter der AG ICS Security
- **Sensibilisieren und Bewusstsein schaffen für ICS Security – Industrie/Infrastruktur**

herbert.dirnberger@cybersecurityaustria.at @dirnberg

Florian Brunner

- Studium Sichere Informationssysteme
- Software Consultant
- seit 2011 HolisticSec
- Penetration Testing u. Sicherheitsberatung
- Schwerpunkt: Überprüfung von Systemen, Anwendungen und Konzepten, Sicherheitsberatung

florian.brunner@holisticsec.com @dosbart

1 alt, gut und sicher?

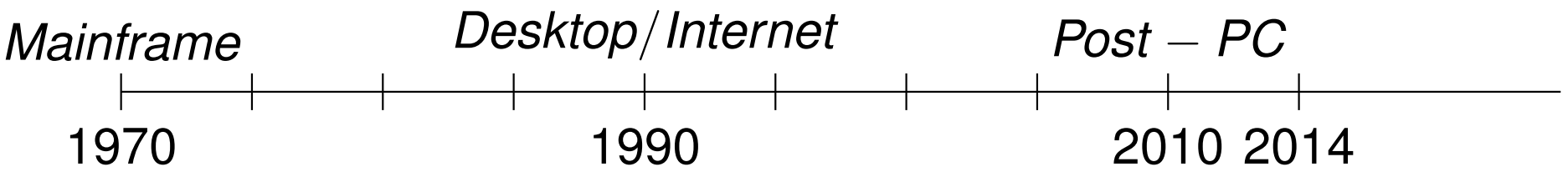
2 Legacy

3 Umgang mit Legacy

4 Praxis

5 Empfehlungen

schneller, stärker und cooler



Lawrence Livermore National Laboratory [Attribution], via Wikimedia Commons from Wikimedia Commons
`http://commons.wikimedia.org/wiki/File%3AIBM_704_mainframe.gif`

IBM PC 5150 with keyboard and green monochrome monitor (5151), running MS-DOS 5.0 I, Boffy b took this photo of my IBM PC, and release it under the GFDL and CC-BY-SA. `http://upload.wikimedia.org/wikipedia/commons/6/69/IBM_PC_5150.jpg`

By LG [CC-BY-2.0 (http://creativecommons.org/licenses/by/2.0)], via Wikimedia Commons from Wikimedia Commons
`http://commons.wikimedia.org/wiki/File%3ANexus_5.png`

Einsatzdauer

Monate

Jahrzehnte

By Tedeytan (Flickr) [CC-BY-SA-2.0 (http://creativecommons.org/licenses/by-sa/2.0)], via Wikimedia Commons from Wikimedia Commons `http://commons.wikimedia.org/wiki/File%3AGoogle_Glass.jpeg`

By Ikar.us (Karlsruhe:Raffinerie) [CC-BY-2.0-de (http://creativecommons.org/licenses/by/2.0/de/deed.en)], via Wikimedia Commons from Wikimedia Commons `http://commons.wikimedia.org/wiki/File%3AMiRO8.jpg`

Bruce Sterling (2010)

”Today’s bleeding-edge technology is tomorrow’s broken legacy system.”

By Dirk Ingo Franke (Own work) [CC-BY-3.0 (http://creativecommons.orghelicenses/by/3.0)], via Wikimedia Commons
`http://upload.wikimedia.org/wikipedia/commons/4/47/Berlin_NEXT_bruce_sterling_24.04.2013_16-07-00.JPG`

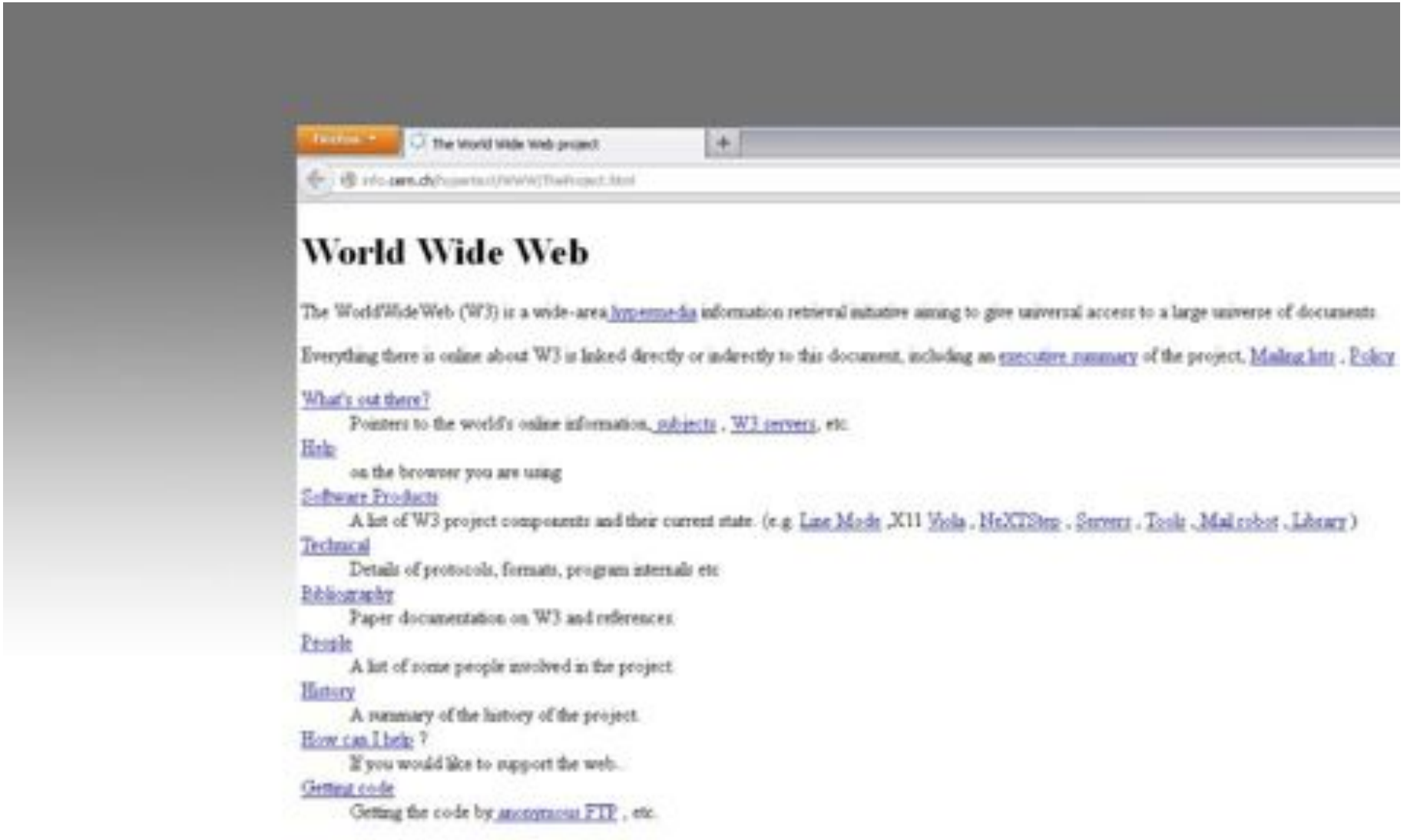
`http://paradox1x.org/2010/01/todays-bleeding/`

1989

Other 'BBS' systems

St	Name	Phone	Baud	Storage	Software
NE	THE YOYODYNE BBS		1200	2	FoReM ST
NE	COMPU CONNECTION		300	1.5	COMMODORE
NJ	TRANSFER STATION BLUE		1200	2	COMMODORE
NY	SUPER COMMODORE WARES		3/12	1/4	COMMODORE
NJ	BUCKAROO BONZAI'S BBQ		2400	80	OTHER
IL	PROTECTO SUPPORT		2400	lot	COMMODORE
RI	INFOMANIACK		2400	2	ATARI 8 BIT
CA	FORBIDDEN ZONE		2400	2.5	COMMODORE
NJ	THE CIA		1200	1	IBM
CT	ONE BYTE		2400	60	PC BOARD
CA	LUNATIC LABS		1200?	60	PC BOARD
CT	YANKEE INGENUITY		1200	30+	PC BOARD
CT	INFOMANIACK		1200	1	ATARI 8 BIT
CA	MR. ED'S STABLE		2400	30	PC BOARD
VA	THE BEEHIVE BBS		2400	170	IBM
CT	THE DEN OF INEQUITY		2400	65	IBM

1990



World Wide Web

The WorldWideWeb (W3) is a wide-area hypermedia information retrieval initiative aiming to give universal access to a large universe of documents

Everything there is online about W3 is linked directly or indirectly to this document, including an executive summary of the project, Mailing lists , Policy

What's out there?
Pointers to the world's online information, subjects , W3 servers, etc.

Help
on the browser you are using

Software Products
A list of W3 project components and their current state. (e.g. Line Mode ,X11 Viola , NeXTStep , Servers , Tools , Mail robot , Library)

Technical
Details of protocols, formats, program internals etc

Bibliography
Paper documentation on W3 and references.

People
A list of some people involved in the project.

History
A summary of the history of the project.

How can I help ?
If you would like to support the web..

Getting code
Getting the code by anonymous FTP , etc.

Quelle: `http://www.pc-magazin.de/news/erste-webseite-der-welt-online-internet-geburtstag-1502650.html`

1993 – 1999

1993 Internet öffentlich zugänglich

1996 `http://www.ey.com`

1997 `http://www.ikarus.at`

1998 `https://www.brz.gv.at`

`http://www.softwarepark.at`

`http://www.bacher.at`

1999 `http://www.xortex.com`

2000 – 2003

2000 http://www.kpmg.at

2001 http://www.t-systems.at

http://www.hagenbergerkreis.at

http://www.uninet.at

http://www.fh-ooe.at

2002 http://www.staatsdruckerei.at

2003 https://www.sec-consult.com

http://www.securityforum.at

2006 – 2012

2006 http://www.rewe-group.at

http://www.zt-prentner-it.at

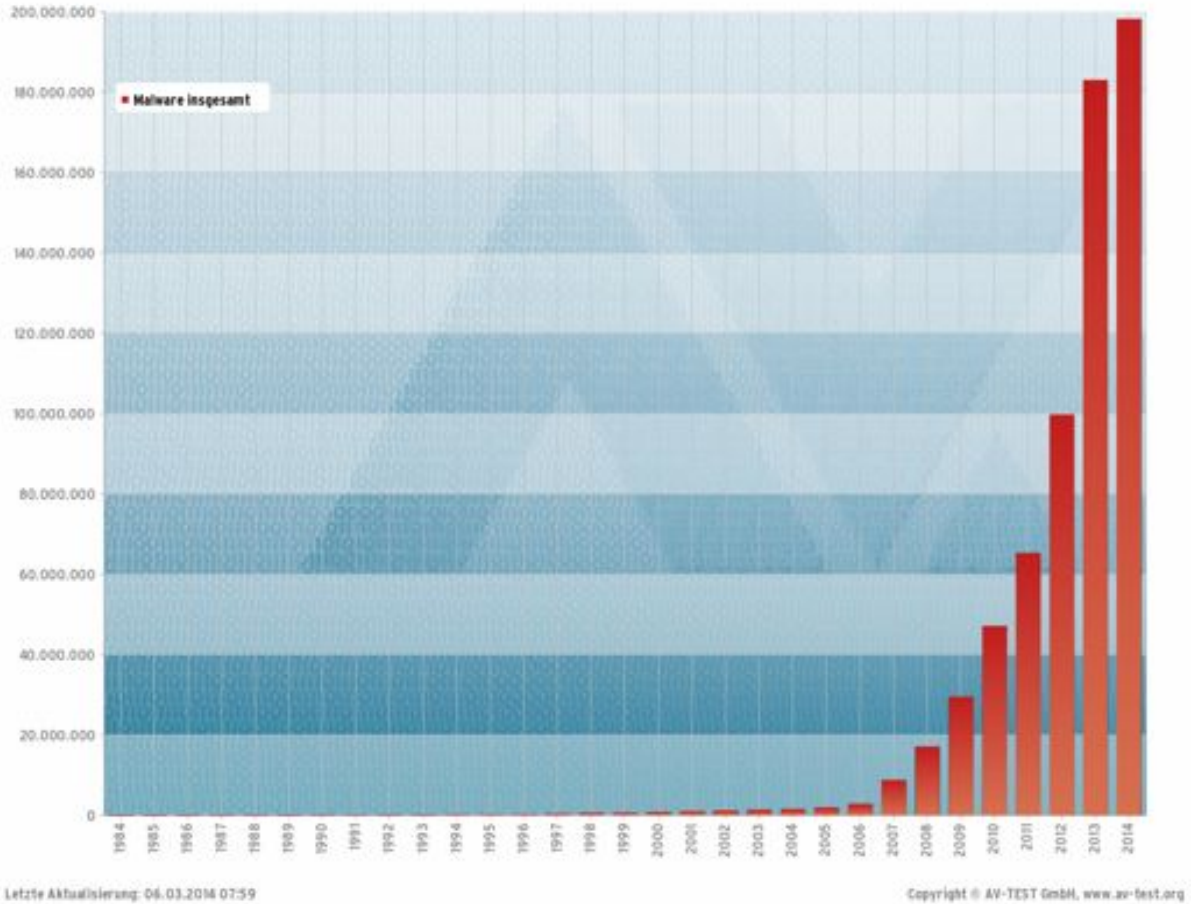
2008 http://www.arz.at

2009 http://www.sba-research.org

2011 http://www.iqsol.biz

2012 http://www.cybersecurityaustria.at

25 Jahre Internet



3 Mrd. User vs 200 Mill. Malware (Quelle: www.av-test.org)
komplex, rasantes Wachstum & veraltert!

Quelle: `http://www.av-test.org/typo3temp/avtestreports/print_malware-all-years_sum_de.png`

Legacy=Altlast?

- veraltert
- nicht mehr Stand der Technik
- nicht mehr zeitgemäß
- gewachsene und unüberschaubare Systeme
- kein Support durch Hersteller/Lieferant
- Weiterentwicklung nicht möglich

Legacy=Vermächtnis?

- hoher Vermögenswert
- teuer im Unterhalt

By Luckyprof Luckyprof (talk) 11:01, 11 March 2013 (UTC) (Eigenes Foto) [CC-BY-SA-3.0 (http://creativecommons.org/licenses/by-sa/3.0)], via Wikimedia Commons from Wikimedia Commons `http://commons.wikimedia.org/wiki/File%3ASchloss_Hagenberg.jpg`


Interfaces
Bussysteme
Sicherheitsprotokolle
Betriebssysteme
LEGACY
Data
Protokolle
Applikationen
Code
Informationen
Komponenten
Industrieanlagen

Ökonomische Betrachtungen

- so lange betreiben wie möglich
- Funktion laufend verbessern
- Umstellung ist teuer und bringt keinen direkten Nutzen
- Austauschen, nur wenn unbedingt notwendig

Sicherheitsbetrachtung?

- Altsysteme können nicht mehr gepatcht werden
- somit ein Risiko
- Vorwurf der Fahrlässigkeit
- Unternehmerische Sorgfaltspflichten
- Schadensersatz

Erneuern und Modernisieren

- Big Bang, alles neu, ”Rip & Replace”
- kleine Änderungen
- Schrittweise Weiterentwicklung
- große Anpassungen, Reengineering
- Belassen ”mit schlechten Gewissen”
- Ignorieren, nichts tun

By Stefan Kühn (Own work) [GFDL (http://www.gnu.org/copyleft/fdl.html) or CC-BY-SA-3.0-2.5-2.0-1.0 (http://creativecommons.org/licenses/by-sa/3.0)], via Wikimedia Commons from Wikimedia Commons `http://commons.wikimedia.org/wiki/File%3AAbrissbirne.jpg`

Gründe für nicht Erneuerung

- mangelnde ”Politik”
- Geld
- Zeit
- fehlendes Know How
- ”nicht trauen” da zu komplex
- Riskio von Fehlverhalten nach Umstellung
- aus Funktionssicht nicht notwendig

Praktische Erfahrungen

1. Legacy Code
2. Industrieanlagen, Medizintechnik und Infrastruktur
3. anno 1989

”Grundproblematik”

- Ökonomie verlangt Legacy
- Geld steht über Sicherheit
- verschiedene Zeithorizonte
- Abwarten bis System veraltert ist

Empfehlungen

- von Anfang bis Ende denken
- ”Long Term” Serviceverträge
- laufend Sicherheit nachbessern
- aktuell dokumentieren
- Härten, sicher konfigurieren,...
- nicht abwarten
- erreichbare Ziele, Schritt für Schritt

By Nicor (Own work) [GFDL (http://www.gnu.org/copyleft/fdl.html) or CC-BY-SA-3.0-2.5-2.0-1.0 (http://creativecommons.org/licenses/by-sa/3.0)], via Wikimedia Commons from Wikimedia Commons `http://commons.wikimedia.org/wiki/File%3ASanierung_Doppelhaush%C3%A4lfte.JPG`

CYBER SECURITY AUSTRIA

http://www.cybersecurityaustria.at