Bundesamt
für Sicherheit in der
Informationstechnik

Auswirkungen des IT-Sicherheitsgesetzes auf den IKT-Sektor

Dirk Häger
Operative Netzabwehr

eco Internet Security Days / 16.9.2015

Die Regelungskomplexe des IT-SiG

- Verbesserung der IT-Sicherheit in Unternehmen
- Verbesserung der IT-Sicherheit des Bundes
- Stärkung des BSI
- Schutz der Bürger/Unternehmen in einem sicheren Netz

➡ Das IT-SiG ist mehr als ein KRITIS-Gesetz

Schutz der Bürger/Unternehmen in einem sicheren Netz

- Verpflichtung TK-Betreiber (Änderungen TKG)
  - Stand der Technik bei der Sicherheit berücksichtigen
  - Informationspflicht gegenüber den Nutzern
  - Regelmäßige Überprüfung des Sicherheitskonzepts durch BNetzA

- Recht der TK-Betreiber

  Verwendung von Nutzungsdaten zur Störungserkennung

Verbesserung der IT-Sicherheit in Unternehmen

- WER wird reguliert
  - Betreiber kritischer Infrastrukturen
  - Ausnahme: Kleinstunternehmen
  - Vorrang von spezialgesetzlichen Regelungen
- WAS wird reguliert
  - Einhaltung von Sicherheitsstandards (inkl. Nachweispflicht)
  - Meldepflicht für Sicherheitsvorfälle
- WIE wird reguliert
  - Kooperativer Ansatz
  - Sanktionsmöglichkeit (OWi) bei Kooperationsverweigerung

IT-Sicherheitsgesetz: Wo nachlesen?

Artikelgesetz

- Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)
- Atomgesetz (AtomG)
- Energiewirtschaftsgesetz (EnWG)
- Telemediengesetz (TMG)
- Telekommunikationsgesetz (TKG)
- Bundesbesoldungsgesetz (BBG)
- Bundeskriminalamtgesetz (BKAG)

Rechte

- BSIG: Das Bundesamt kann **Betreiber Kritischer Infrastrukturen** auf deren Ersuchen bei der Sicherung ihrer Informationstechnik beraten und **unterstützen** oder auf qualifizierte Sicherheitsdienstleister verweisen.
- BKAG: Das Bundeskriminalamt nimmt die polizeilichen Aufgaben auf dem Gebiet der Strafverfolgung wahr [...] in den Fällen von Straftaten nach **§§ 202a, 202b, 202c, 263a, 303a** und 303b des Strafgesetzbuches, soweit tatsächliche Anhaltspunkte dafür vorliegen, dass die Tat sich gegen [...] **Stellen von lebenswichtigen Einrichtungen**, bei deren Ausfall oder Zerstörung eine erhebliche Bedrohung für die Gesundheit oder das Leben von Menschen zu befürchten ist oder die für das Funktionieren des Gemeinwesens unverzichtbar sind, richtet.

Rechte

- BSIG (kein Zitat): **Das BSI hat** die für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik wesentlichen **Informationen zu sammeln und auszuwerten**, insbesondere Informationen zu Sicherheitslücken, zu Schadprogrammen, zu erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und zu der dabei beobachteten Vorgehensweise, deren potentielle Auswirkungen zu analysieren **und unverzüglich die Betreiber Kritischer Infrastrukturen über sie betreffende Informationen zu unterrichten.**

Pflichten

Bundesamt
für Sicherheit in der
Informationstechnik

www.sicherheitstest.bsi.de

2014/01/21

SPIEGEL ONLINE NETZWELT

Login | Registrierung

Politik | Wirtschaft | Panorama | Sport | Kultur | Netzwelt | Wissenschaft | Gesundheit | einestages | Karriere | Uni | Schule | Reise | Auto

Nachrichten > Netzwelt > Web > Computersicherheit > BSI warnt vor Identitätsdiebstahl: 16 Millionen Nutzerkonten betroffen

Warnung des BSI: 16 Millionen Online-Konten geknackt

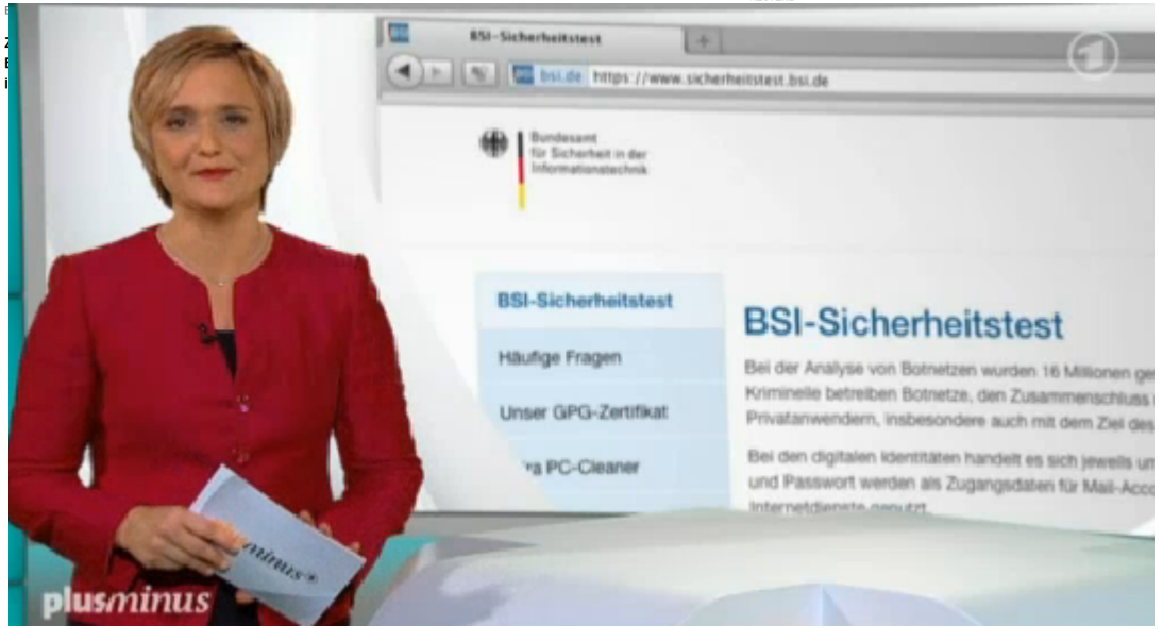
REUTERS

21. Januar 2014 - 11:18 Uhr

Millionen Online-Zugangsdaten gekapert

Bei der Analyse von Botnetzen sind Experten auf Millionen übernommene Zugangsdaten von zumeist deutschen Usern gestoßen. Dabei handelt es sich vorwiegend um Mail-Adresse und Passwort. Eine Testseite soll möglicherweise Betroffenen Klarheit bringen.

| Artikel auf tagesschau.de



16.09.15

Bundesamt für Sicherheit und Informationstechnik

Hacker spähen 16 Millionen E-Mail-Konten aus

Mehrere Millionen Zugangsdaten für Online-Dienste sind nach Angaben des Bundesamt für Sicherheit in der Informationstechnik (BSI) gekapert wurden. Betroffen seien 16 Millionen Benutzerkonten.

(Foto: DPA)

Hacker haben 16 Millionen E-Mail-Konten ausgespäht. Auf einer Website können die Bürger prüfen, ob sie betroffen sind. BSI-Präsident Hauge warnt und spricht von einer "beachtlichen Dimension".

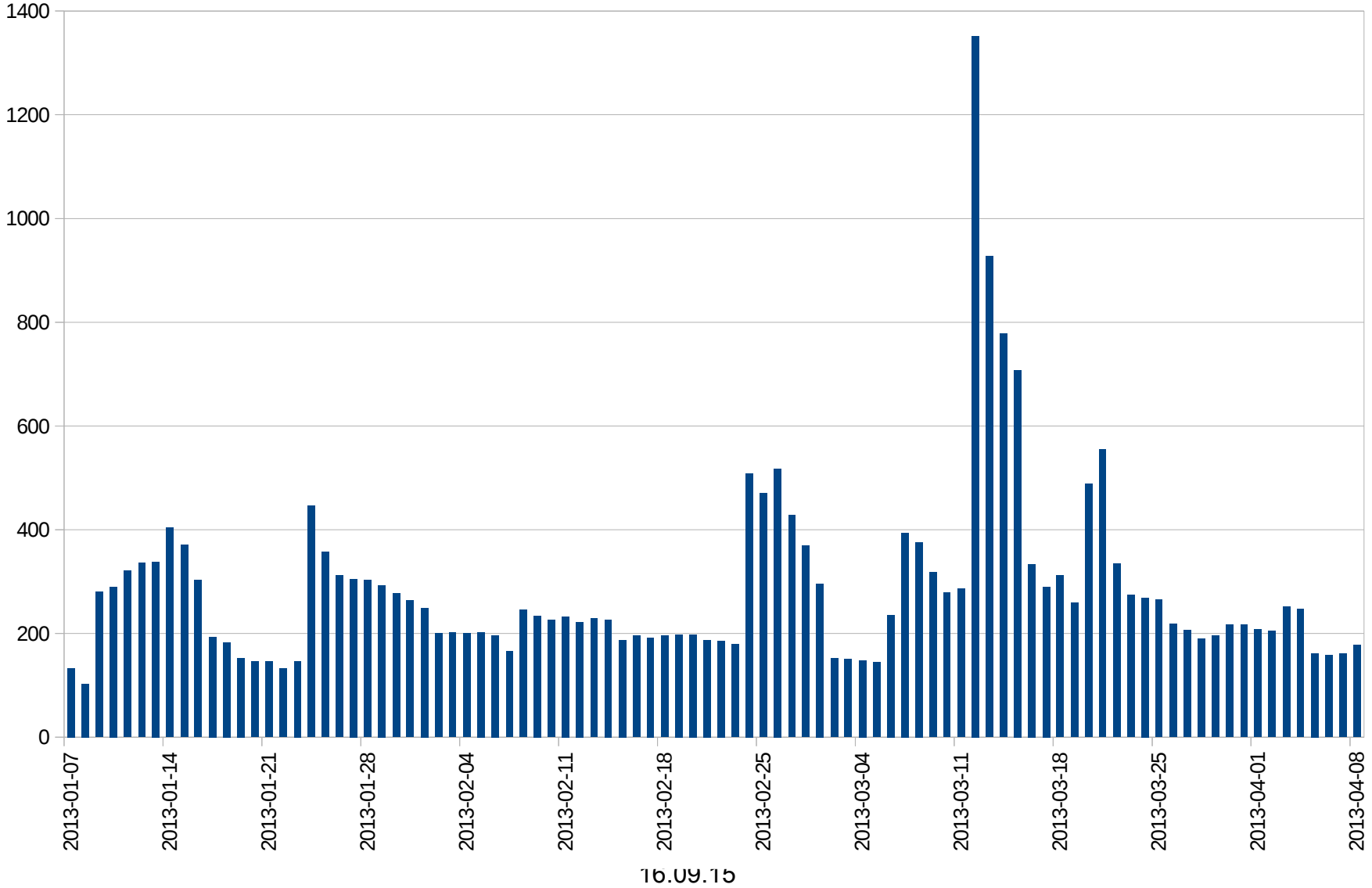
ISPs: Mitwirkungspflicht bei Warnungen

- BSIG: Das BSI darf bei IT-Sicherheits-Warnungen Dritte mit einbeziehen.

- TKG: Werden dem Diensteanbieter [...] Störungen bekannt, die von Datenverarbeitungssystemen der Nutzer ausgehen, so hat er die Nutzer, soweit ihm diese bereits bekannt sind, unverzüglich darüber zu benachrichtigen. Soweit technisch möglich und zumutbar, hat er die Nutzer auf angemessene, wirksame und zugängliche technische Mittel hinzuweisen, mit denen sie diese Störungen erkennen und beseitigen können.

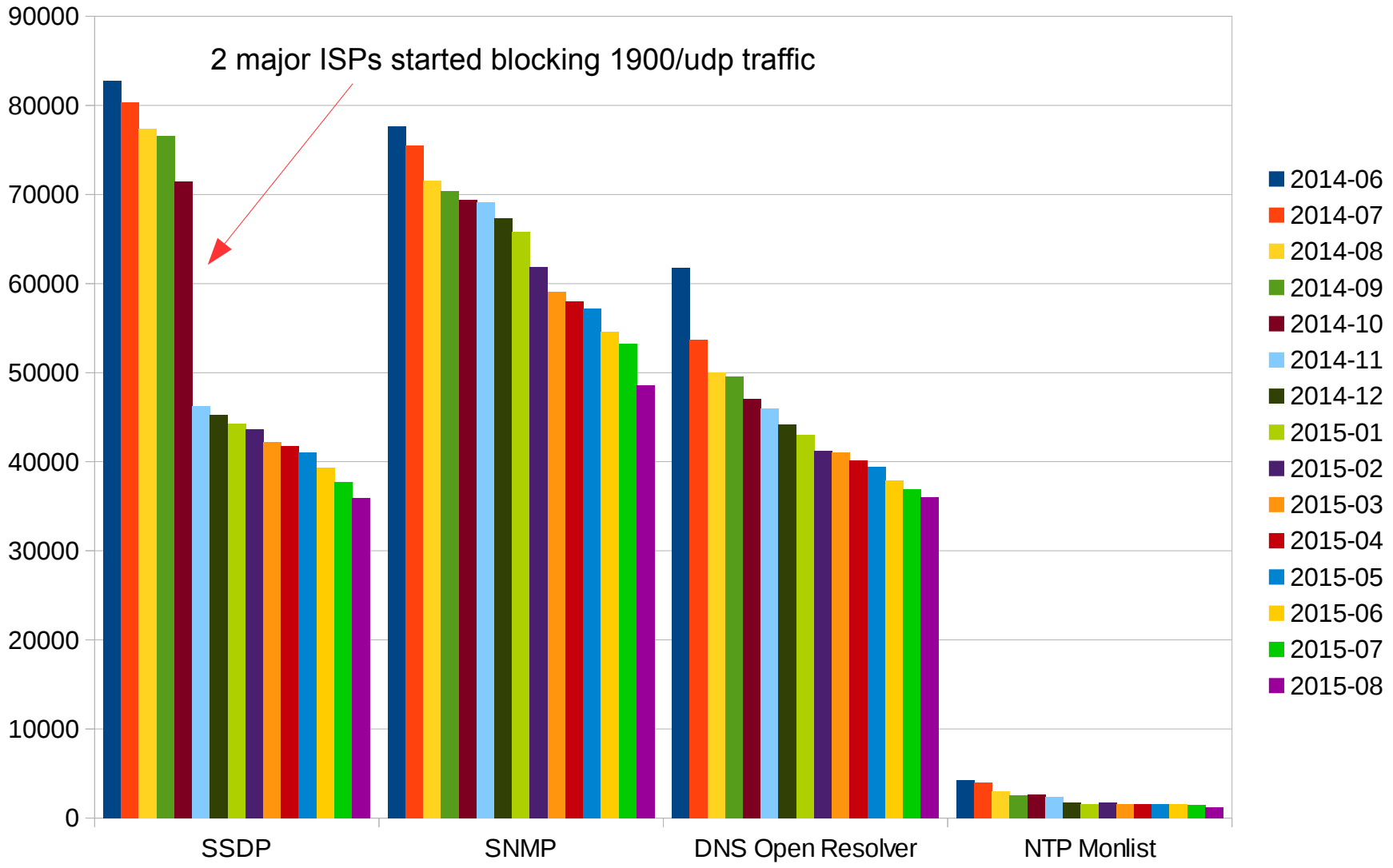
Brobot
DDoS-Angriffe gegen US-Banken

Anzahl täglich aktiver bekannter Bots in DE



Bundesamt
für Sicherheit in der
Informationstechnik

DDoS-Reflection geeignete Dienste in Deutschland



Verpflichtung zur Einhaltung grundlegender Sicherheitsmaßnahmen

- TMG: Diensteanbieter haben, soweit dies technisch möglich und wirtschaftlich zumutbar ist, im Rahmen ihrer jeweiligen Verantwortlichkeit für geschäftsmäßig angebotene Telemedien durch technische und organisatorische Vorkehrungen sicherzustellen, dass
  1. kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und
  2. diese
     a) gegen Verletzungen des Schutzes personenbezogener Daten und
     b) gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind, gesichert sind. [...]

Absicherung kritischer IT-Prozesse

- BSIG: Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden. […]
- Erstellung branchenspezifischer Sicherheitsstandards
- Nachweispflicht

Bekanntwerden eines Angriffs

From: Vikki Doss [mailto:vikki.doss@yahoo.co.uk]
Sent: Thursday, September 23, 2010 1:24 PM
To: Duke, Roger; Klein, Scott; Smith, Brooke; Williams, Chilly; Malmgren, Michael; Fox, Deborah; Hynes, Tim; Ty.Schieber@QinetiQ-NA.com; Crouch, JD
Subject: A Good Chance

Dear Sir,
It is a conference that you may possibly be interested in.
More information is attached below.

Yours sincerely,
Vikki Doss

ISSNIP

The Sixth International Conference on Intelligent Sensors, Sensor Networks and Information Processing

ISSNIP 2010 Call for Papers

The Sixth International Conference on Intelligent Sensors, Sensor Networks and Information Processing ISSNIP 2010 (http://www.issnip.org/2010) held under the umbrella of the ARC Research Network on ISSNIP is an annual forum for sensor network research. Recent advances in both theory and applications of intelligent sensors and smart systems in diverse areas ranging from manufacturing and defence to medical science and environmental monitoring will be presented by the leading researchers in the field. The conference will be held in Brisbane, Australia during the 7th-10th of December 2010.

Papers are sought addressing the theory, implementation, and applications of intelligent sensors, sensor networks, and intelligent information processing systems. Topics include:

- Sensor Network Security
- Network Scheduling and Optimization
- Sensor Fusion, Tracking and Localization
- Protocols in Sensor Networks
- Multimedia Sensor Network
- Environmental Monitoring
- Distributed Information Processing
- Data Aggregation, Storage & Management
- Middleware in Sensor Networks
- Fault Tolerance and Identification
- Networked Sensing and Control
- Embedded Software for Sensor Networks
- Energy Efficiency and Management
- Sensor Networks for Smart Grids
- Applications of Sensor Networks in Healthcare, Infrastructure, Defence, Environment

The papers can be nominated under the following symposiums and workshops (see the website for respective details and topic scope).

- Sensor Networks
- Sensor Network Security
- Advances in Optimization for Distributed Control, Information Fusion and Sensor Network Applications
- Sensor Networks for Healthcare
- WSN's for Structural Health Monitoring.
- Cognitive Wireless Sensing Systems for Factory and Logistics Automation
- Smart Cities for Sustainable Living
- ISSNIP/CREON Workshop - Building coral reef sensor networks as systems of systems

Paper Submission:
Prospective authors are invited to submit full papers (up to 6 pages in length) electronically through the EDAS system (http://edas.info/N8067) and must be original material not currently under review by another conference or journal. Author guidelines are available on the conference website. All submitted papers will be subjected to multiple independent peer reviews. All accepted papers will be published by the IEEE Press and appear in the Conference Proceedings and on IEEE Xplore.

Important Dates :
Title and Abstract Submission: **15 August 2010**
Paper Submission: **31 August 2010**
Notification of Acceptance: **30 September 2010**
Final Paper Submission: **7 October 2010**
Conference Dates: **7-10 December 2010**

Contact Information:
ISSNIP 2010
Dept of Electrical and Electronic Engineering,
University of Melbourne, Victoria - 3010, Australia
Email: issnip2010 (at) issnip (dot) org

Technical Co-Sponsorship
IEEE Sensors Council

Sponsors
Australian Government
Australian Research Council

Organised by
ARC Research Network on Intelligent Sensors, Sensor Networks and Information Processing
ISSNIP
The University of Melbourne
QUT

General Co-Chairs:
M. Palaniswami, University of Melbourne
Peter Corke, Queensland University of Technology
Steven Manolis, University of Melbourne

IEEE Sensors Council Liaison:
S C Mukhopadhyay, Massey University

Symposia Chairs/Organizers:
Paul Havinga, University of Twente
Roberto di Pietro, Universita di Roma Tre
Yee Wei Law, Uni of Melbourne
Adrian N. Bishop, NICTA
Iman Shames, ANU
Ahsan N. Khandoker, Uni of Melbourne
Daniel T. H. Lai, Victoria University
Rezaul K. Begg, Victoria University
Priyan Mendis, University of Melbourne
Tuan Ngo, University of Melbourne
Laurent Herault, CEA-LETI
Alexander Gluhak, University of Surrey
Srdjan Krco, Ericsson
Sally Holbrook, University of California Santa Barbra
Scott Bainbridge, Australian Institute of Marine Science
Supriyo Chatterjea, University of Twente
Özlem Durmaz İncel, Bogazici University
Raluca Marin-Perianu, Uni of Twente

Publication Chair:
Jayavardhana Gubbi, University of Melbourne

Manuscripts will be made available on
IEEE Xplore

www.issnip.org/2010

Bundesamt
für Sicherheit in der
Informationstechnik

Bekanntwerden eines Angriffs

From: Vikki Doss [mailto:vikki.doss@yahoo.co.uk]

Re: FW: A Good Chance

Von: Phil Wallisch <phil@hbgary.com>
An:
Kopie:
Blindkopie:
Datum: 24.09.2010 07:27

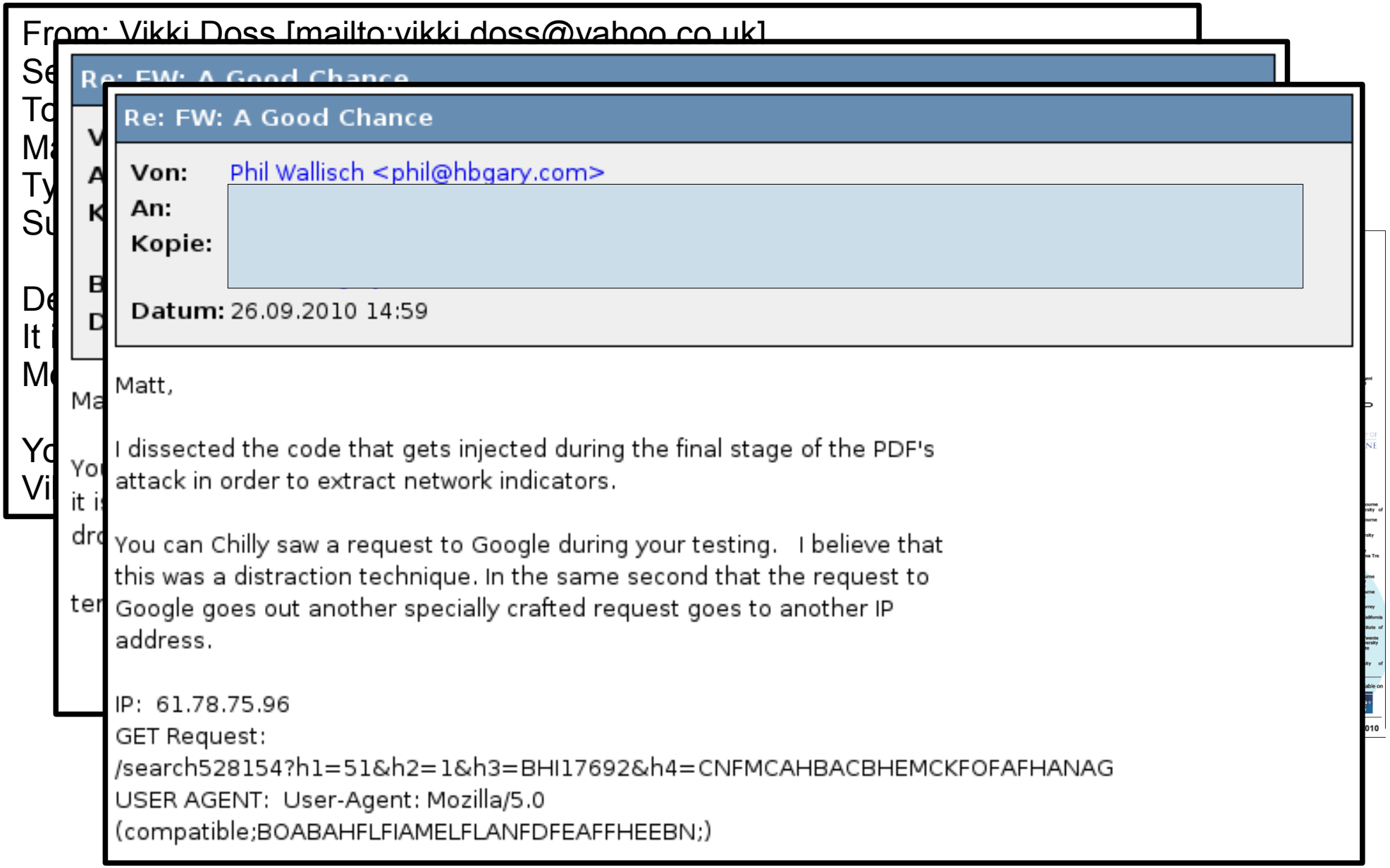
Matt,

You were right to be concerned. This is a very complicated PDF. I believe it is exploiting a recent Adobe buffer overflow vulnerability. The PDF drops:

temp.exe-->
-->setup.exe
-->msupdater.exe and FAVORITES.DAT

Bundesamt
für Sicherheit in der
Informationstechnik

Bekanntwerden eines Angriffs



Kommunikationsdefizite

03.02.2012 00:07 « Vorige | Nächste »

MSUpdate-Trojaner attackierte Rüstungsfirmen

vorlesen / MP3-Download

Mit einer Einladung zu renommierten Fachkonferenzen haben Unbekannte versucht, einen Trojaner bei Firmen der Rüstungsindustrie einzuschleusen. Wer den angehängten

2010 erreicht haben. Noch vor wenigen Wochen habe man kompromittierte Rechner entdeckt, von denen einige seit zwei Jahren infiziert waren, erklärte Aviv Raff, CTO von Seculert,

Ziel der Angriffe waren den Angaben zufolge vor allem europäische und amerikanische Firmen im Regierungsumfeld, darunter Rüstungs- und Luffahrtunternehmen. Die Angriffe sollen bereits 2009 begonnen und ihren Höhepunkt im Herbst 2010 erreicht haben. Noch vor wenigen Wochen habe man kompromittierte Rechner entdeckt, von denen einige seit zwei Jahren infiziert waren, erklärte Aviv Raff, CTO von Seculert, gegenüber heise Security.

Meldepflicht

- TKG: Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat der Bundesnetzagentur unverzüglich Beeinträchtigungen von Telekommunikationsnetzen und -diensten mitzuteilen, die
  1. zu beträchtlichen Sicherheitsverletzungen führen oder
  2. zu beträchtlichen Sicherheitsverletzungen führen können.

Meldepflicht

- BSIG: Betreiber Kritischer Infrastrukturen haben erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können oder bereits geführt haben, über die Kontaktstelle unverzüglich an das Bundesamt zu melden.

Wer hätte zuhören müssen?

- TMG-Änderungen: alle Inhalteanbieter
- TKG-Änderungen: alle ISPs
- BSIG: nur die Großen
  - Sprach- und Datenübertragung
  - Datenspeicherung und -verarbeitung

- Wer genau? Rechtsverordnung durch Innenministerium (Identifikation nach Qualitäts- und Quantitätskriterien)

Bundesamt
für Sicherheit in der
Informationstechnik

Kontakt

Bundesamt für Sicherheit in der
Informationstechnik (BSI)

Dirk Häger
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)228 99 9582-5304
Fax: +49 (0)228 99 10 9582-5304

dirk.haeger@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de