Hochschule
Bonn-Rhein-Sieg

Prof. Dr. Hartmut Pohl
Informationssicherheit

Innenausschuss

A-Drs. 16(4)570 C

Hochschule Bonn-Rhein-Sieg
Postfach 1255, 53730 Sankt Augustin

Grantham-Allee 20 53757 Sankt Augustin
Tel. 02241/865-204
0172-9437-329
Hartmut.Pohl@sang.net
http://www.inf.h-brs.de/pohl

Innenausschuss des Deutschen Bundestags - Sekretariat

Platz der Republik

11011 Berlin

5. Mai 2009

Stellungnahme zum Entwurf eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes. BT-Drucksachen 16/11967, 16/12225. Öffentliche Anhörung am Montag den 11. Mai 2009

Ihre Einladung zu einer persönlichen Stellungnahme als Sachverständiger vom 23. April 2009

Sehr geehrter Herr Vorsitzender, sehr geehrte Damen und Herren,

Unterzeichner hat den Gesetzentwurf seit den ersten Referentenentwürfen begleitet; so u.a. als Sprecher des Präsidiumsarbeitskreises der Gesellschaft für Informatik e.V. (GI), die eine - zusammen mit Fachkollegen erarbeitete - Stellungnahme Ihnen als Vorsitzendem und allen Ausschussmitgliedern mit Schreiben vom 23. Januar 2009 zugeleitet und auch veröffentlicht[1] hat. Die wichtigsten Aspekte zu Artikel 1 des Gesetzentwurfs will ich hier aktualisiert nennen.

1 Überwachung der gesamten Sprach- und Datenkommunikation mit Bundesbehörden und Verletzung des Fernmeldegeheimnisses

Der Gesetzentwurf sieht in § 5 Abs. 1 die ständige verdachtslose und sogar anlasslose (!) vollständige Überwachung (Verbindungsdaten und Inhalte) der gesamten Sprach- und Datenkommunikation aller Unternehmen und Bürger[2] vor, die mit Bundesbehör-

[1] Informatik-Spektrum 32/2 (2009) Seiten 188-190.

[2] Erfasst werden durch die Überwachung ausschließlich deutsche (oder europäische) Unternehmen und Bürger; Unternehmen und Bürger aus Drittstaaten sowie Kriminelle wie Terroristen sind nur schwer zu erfassen und zu überwachen; insbesondere letztere wissen sich zu schützen durch praktisch nicht rückverfolgbare Absenderadressen und/oder Angriffsprogramme, die z.B. unveröffentlichte Sicherheitslücken ausnutzen.

den kommunizieren! Die vollständige Überwachung jeglicher Kommunikation mit der Bundesverwaltung ist eine untaugliche Sicherheitsmaßnahme – soweit sie über die technisch üblichen Virensuchprogramme und Intrusion Detection/Protection Systeme hinausgeht. Nach Medienberichten ist der Bundesregierung bekannt, wie Kriminelle tatsächlich aus dem Internet unerkennbar angreifen (vgl. die folgende Ziffer).

Der in der Begründung angeführte Zeitverzug zur Erkennung von Schadprogrammen "von mehreren Tagen oder Wochen" ist hier nicht bekannt. Grundsätzlich sind nicht neue Schadprogramme problematisch – vielmehr sollte die Bundesregierung die zugrundeliegenden Sicherheitslücken ausmerzen (lassen).

Empfehlung: Alle Überwachungsregelungen streichen. Vielmehr ergänzen: Die Bundesregierung wird ab Ende 2009 ausschließlich hoch zertifizierte Systeme einsetzen.

2 Geheimhaltung von Sicherheitslücken in IT-Programmen und –Systemen

In § 7 wird es in das nicht näher spezifizierte Ermessen des BSI gestellt ("kann"), Erkenntnisse über Schadprogramme und Sicherheitslücken an die Betroffenen weiterzugeben und die Öffentlichkeit zu warnen.

Unveröffentlichte Sicherheitslücken werden in einschlägigen Kreisen im Internet gehandelt; einige können allgemein sogar bei einem Internet-Auktionshaus ersteigert werden. Gleichwohl sollen aber unveröffentlichte, der Bundesregierung aber bekannte Sicherheitslücken deutschen Unternehmen und Privaten vorenthalten werden!

In diesem Zusammenhang muss auf § 9 (4) hingewiesen werden: Ein Sicherheitszertifikat braucht nicht erteilt zu werden, wenn dem "öffentliche Interessen, insbesondere sicherheitspolitische Belange" entgegenstehen. Eine Begründung liegt nicht vor. Dies nährt den Verdacht, dass die Bundesregierung in Standardprogramme heimlich Sicherheitslücken einbauen (lassen) will.

Da durch neue Schadprogramme und insbesondere unveröffentlichte Sicherheitslücken[3] sehr große Schäden entstehen (können), muss vielmehr – u.a. vor dem Hintergrund der durch die im BKA-Gesetz vorgesehene Online-Durchsuchung induzierten Interessenkollision im Dienstbereich des Innenministeriums, dem BSI und BKA unter-

---

[3] Unveröffentlichte Sicherheitslücken werden von Kriminellen, gegnerischen Nachrichtendiensten und auch zur heimlichen Online-Durchsuchung eingesetzt. Vgl.:

Pohl, H.: Zero-Day und Less-Than-Zero-Day Vulnerabilities und Exploits - Risiken unveröffentlichter Sicherheitslücken. Erschienen in: Zacharias, C.; ter Horst, K. W.; Witt, K.-U.; Sommer, V.; Ant, M.; Essmann, U.; Mülheims, L. (Hrsg.): Forschungsspitzen und Spitzenforschung. Innovationen an der Fachhochschule Bonn-Rhein-Sieg. Festschrift für Wulf Fischer. Heidelberg 2008 http://www.inf.fh-bonn-rhein-sieg.de/data/informatik_/fb_informatik/personen/pohl/Aufsaetze/Less_Than_Zero_Day_Vulnerabilities.pdf

Pohl, H.: Zero-Day and Less-Than-Zero-Day Vulnerabilities and Exploits in Networked Infrastructures. European Network and Information Security Agency: ENISA Quarterly Review Vol. 4, No. 2, Apr-Jun, 7 – 9, 2008 http://www.enisa.europa.eu/doc/pdf/publications/enisa_quarterly_07_08.pdf

Pohl, H.: Zur Technik der heimlichen Online-Durchsuchung. Datenschutz und Datensicherung 31, 9, 684 – 688, 2007 http://www.dud.de/binary/DuD_Pohl_907.pdf

stehen - eine **Pflicht** zur Warnung und Veröffentlichung von Sicherheitslücken und diese ausnutzenden Schadprogrammen gefordert werden. Anderenfalls sind Unternehmen und Private Spionage- und Sabotage-Angriffen aus dem Internet völlig schutzlos ausgeliefert.

Empfehlung: Die Bundesregierung muss alle ihr bekannten Sicherheitslücken und die sie ausnutzenden Angriffs- und Schadprogramme unverzüglich veröffentlichen.

3 Zu § 9: Zertifizierung nur ausgewählter IT-Systeme (Software und Hardware)

Die Sicherheitszertifizierung nach § 9 (4) 2. sowie § 9 (6) 2. ist eine international standardsisierte nützliche Aktivität des BSI. Allerdings ist die (deutsche) Einschränkung Systeme nicht zu zertifizieren, für die 'das Bundesministerium des Innern festgestellt hat, dass überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, der Erteilung nicht entgegenstehen." völlig kontraproduktiv. Hier **muss** der Eindruck entstehen, dass das Bundesinnenministerium Schadprogramme in diese IT-Systeme eingebaut hat und diese Tatsache dem BSI und den Evaluatoren verheimlichen will.

Im Gegenteil müssen **alle** IT-Systeme, für die ein Zertifikat beantragt wird, evaluiert und zertifiziert werden.

Empfehlung: Die Absätze § 9 (4) 2. und § 9 (6) 2. sind zu streichen.

4 Zu: § 2 (5) Schadprogramme

Den formulierten Zweck erfüllen (fast) alle Programme wie z.B. Betriebssysteme, Datenbanksoftware, Anwendungssoftware wie Bürosoftware etc. etc. Schadprogramme können nur an Sicherheitslücken ansetzen und Schaden anrichten - ohne Sicherheitslücken sind sog. Schadprogramme völlig wirkungslos.

Empfehlung: Definition korrigieren.

5 Zu: § 2 (6) Sicherheitslücken

Sicherheitslücken stellen (naturgemäß) keine Eigenschaft von Programmen dar, Sicherheitslücken sind vielmehr **Fehler** in Programmen.

An dieser Stelle fehlt ein Hinweis auf mögliche Fehlkonfigurationen von IT-Systemen, die unberechtigte Zugriffe auf IT-Systeme des Bundes erlauben, weil Sicherheitseigenschaften nicht oder nur unzulänglich parametrisiert sind,.

Empfehlung: Definition erweitern: Fehlkonfigurationen von Hardware und Software stellen Sicherheitslücken i.S. des Gesetzentwurfs dar.

6 Zu: § 5 (1)

Die hier geforderte "sofortige und spurenlose Löschung" ist bekanntlich technisch nicht möglich.

Zum Löschen stellt sich weiterhin die Frage, worin sich diese Forderung vom "unverzüglichen Löschen" in § 5 Ziff. 6 und § 6 unterscheidet.

Empfehlung: Denselben Begriff verwenden: Sofortige nachhaltige Löschung.

7 Zu: § 5 (3)

Hinsichtlich der Erkennbarkeit von Schadprogrammen wird in der Begründung zu § 5 Abs. 2 unbegründet "von einem zeitlichen Verzug von mehreren Tagen oder Wochen (abhängig von deren Verbreitung)" ausgegangen sowie ausgeführt "Derzeit liegen zwi-

schen dem Auftreten eines neuen Schadprogramms und deren Erkennbarkeit im Rahmen der Maßnahmen nach Absatz 1 in der Regel etwa 3 Monate." Offensichtlich sind hier andere Schadprogramme als Viren, Würmer und Trojanische Pferde gemeint, die binnen weniger Stunden mit einschlägigen kommerziell erhältlichen Produkten erkannt werden. Gemeint sein dürften hier die sog. Less-Than-Zero-Day Exploits, die z.T. erst nach Jahren bekannt werden.

Sofern sich ein Hinweis auf ein Schadprogramm nicht sofort ergibt, kann das Bundesministerium nicht zuwarten, bis sich nach einiger Zeit evtl. vielleicht doch noch ein Hinweis auf ein Schadprogramm ergibt.

Empfehlung: § 5 (3) 3. muss unverzichtbar gestrichen werden.

8 Zu: Begründung des Gesetzentwurfs

In B. Besonderer Teil, zu Artikel 1, § 2, Absatz 3 werden Geräte angesprochen, bei denen "Sicherheitslücken in der Regel keine Auswirkungen auf die Sicherheit der übrigen Informationstechnik" haben. Derartige Geräte dürften kaum existieren.

Empfehlung: Satz streichen.

Eine Unterscheidung zwischen beabsichtigten und "unbeabsichtigten" Sicherheitslücken dürfte auch dem BMI technisch, organisatorisch und personell nicht möglich sein – genauso wie die zwischen "normalen" und anderen Programmen.

Empfehlung: Die Begriffe 'beabsichtigt', 'unbeabsichtigt' und normal' streichen.

Mit besten Grüßen