Mattias Schlenker · IT-Consulting

Mattias Schlenker · IT-Consulting · Kochstr. 21 · 04275 Leipzig

Ihr Zeichen	Ihr Schreiben vom	Mein Zeichen	Datum
		MFS	10. Juni 2009

DNNSEC-Einführung durch BSI, resultierende Wirkungslosigkeit von Internetsperren

Sehr geehrte Damen und Herren,

wie Sie wissen koordiniert das Bundesamt für Sicherheit in der Informationstechnologie viele Initiativen des Bundes für ein sicheres Internet. Ausschlaggebend für viele Projekte ist der Schutz des Bürgers vor Cyberkriminalität und die effektive Abwehr von Wirtschaftsspionage. Finanziert werden die Projekte größtenteils aus dem Bundeshaushalt. In diesem Schreiben möchte ich Diskrepanzen zwischen der vom Bundesfamilienministerium und BMWi vorangetriebenen ,,Internetsperren gegen Kinderpornographie" und laufenden Projekten des BSI für ein sicheres Internet aufzeigen.

Einer der verwundbarsten Punkte des Internets ist das Domain Name System, eine Art Auskunftssystem, das einem Host- oder Domainnamen eine IP-Adresse zuordnet. Dieses System ist mit regulären Telefonauskünften vergleichbar, denen ich den Namen eines Teilnehmers nenne und dann dessen Telefonnummer erhalte. Gelingt es einem Angreifer, den Internet-Surfer dazu zu bringen, eine Auskunft anzufragen, die falsche Telefonnummern herausgibt oder die Antworten auf dem Übertragungsweg zu maniulieren, können beispielsweise beim Banking oder Login auf Auktions- oder Micropaymentseiten Daten abgefangen werden.

In den letzten fünf Jahren wurden verschiedene Angriffsformen auf das Domain Name System in freier Wildbahn beobachtet, einige setzten am lokalen Rechner an, indem sie in den Systemeinstellungen durch Kriminelle betriebene DNS-Server (,,Auskunftssrechner") eintrug, andere manipulierten Daten auf dem Transportweg. Entsprechend hoch ist das Interesse der Wirtschaft an Gegenmaßnahmen. Eine solche Gegenmaßnahme ist DNSSEC, ein Verfahren, bei dem das Paar aus angefragtem Hostnamen und zurückgelieferter IP-Adresse kryptografisch signiert ist. In der Offline-Welt ist das tatsächlich vergleichbar mit einer Signatur, die quer über ein Dokument geschrieben ist und so eine Verfälschung verunmöglicht.

Der Bund unterstützt über das BSI derzeit die flächendeckende Einführung von DNSSEC[1], zunächst im Bereich der DE-Domains, über deutsche Provider auch zwangsläufig über weite Teile des rest-

[1] Pressemitteilung des BSI zum DNSSEC-Feldversuch http://www.bsi.de/presse/pressinf/initiativeinternetsicherheit.htm

Mattias Schlenker
IT-Consulting
Redaktionsbüro
DVD-Konzepte

Adresse:
Kochstraße 21
04275 Leipzig

Telefon:
Festnetz: +49 341 3032616
Telefax: +49 341 3032616
Mobil: +49 1577 1530427

Internet:
ms@mattiasschlenker.de
news.mattiasschlenker.de
blog.rootserverexperiment.de

lichen Internets. Dieses Vorangehen ist im Sinne eines sicheren Internets absolut begrüßenswert.

Allerdings stützt sich auch das vom Bundesfamilienministerium auf den Weg gebrachte Gesetz für Internetsperren kinderpornografischer Websites auf DNS-Manipulationen: Wer eine Seite ansurfen möchte, die auf der Sperrliste steht, erhält die IP-Adresse des (voraussichtlich beim BKA beheimateten) Stoppseitenservers und nicht vom ursprünglich vorgesehenen Server. Bei flächendeckendem Einsatz von DNSSEC und Abstimmung der Software auf den Clientrechnern wird der Surfer entweder eine Fehlermeldung erhalten oder – was wahrscheinlicher ist – sein Browser wird mehrere Nameserver („Auskünfte") anfragen, bis er eine Antwort mit gültiger Signatur erhält.

Die Folge der Einführung von DNSSEC ist eine weitgehende Wirkungslosigkeit der angedachten Sperren. Es bleibt die theoretische Möglichkeit, die Einführung von DNSSEC durch Stoppen des Pilotprojektes so zu verzögern, dass das geplante Gesetz zunächst für einige Zeit seine Wirkung entfalten kann. Dies hätte jedoch den Nachteil, dass unsere IT-Infrastruktur an einem neuralgischen Punkt stark gefährdet bleibt. Zudem ist es nicht mehr möglich, eine international begonnene Entwicklung zu stoppen – die von BMWi und BSI getroffenen Entscheidungen können sich lediglich bremsend oder beschleunigend auf die weltweite Einführung von DNSSEC auswirken.

Folglich benötigt es zur Umgehung der angedachten Internetsperren nicht – wie von Frau von der Leyen vermutet – profunde Kenntnisse. Es genügt, darauf zu vertrauen, dass BSI, Provider und Registrare DNSSEC schnell und konsequent einführen. Ich möchte betonen, dass es keine Möglichkeit gibt, zwischen „guten" und „bösen" DNS-Manipulationen zu unterscheiden, das Verfahren sieht keine Hintertüren für staatliche Stellen vor. Es gibt objektiv betrachtet keine wirksame Möglichkeit, Zugriffe auf Transportebene umzuleiten, ohne sich Methoden zu bedienen, die auch Cyberkriminelle anwenden. Folglich bleibt der einzig wirkungsvolle Weg die Abschaltung der Server auf denen die illegalen Inhalte angeboten werden. Verschiedene Initiativen von Kinderschutz- und Bürgerrechtsorganisationen in den letzten Wochen haben gezeigt, dass „Löschen statt Sperren" möglich ist, aber eine sehr gute Ausbildung der Ermittler hinsichtlich der Topologie des Internets und der verwendeten Protokolle erfordert.

Ich appelliere daher an Sie, den geplanten Gesetzentwurf zu stoppen: Durch die schnell fortschreitende Einführung von DNSSEC hat das Gesetz bald nur noch Symbolcharakter. Alleine die Einführung des Gesetzes, erst recht die regelmäßige Pflege der „Listen zu manipulierender DNS-Einträge" bindet jedoch massiv personelle und finanzielle Ressourcen bei BKA und Providern. Diese könnten effizienter zur Ermittlung der Serverstandorte, Aufspürung der Betreiber, Ermittlung der Hintermänner und dem Ausbau der internationalen Kooperation zwischen Providern und Strafverfolgungsbehörden aufgewandt werden.

Sollten Sie detaillierte Fragen zu den Auswirkungen von DNSSEC auf die Wirksamkeit Ihrer Gesetzesinitiative haben, dürften Sie in dem für den DNSSEC Praxisversuch zuständigen Abteilungsleiter beim BSI, Herrn Dr. Hartmut Isselhorst einen kompetenten und neutralen Ansprechpartner in den eigenen Reihen finden. Für die Beantwortung allgemeiner technischer Aspekte zu Fragen des Domain Name Systems stehe selbstverständlich auch ich zur Verfügung.

Mit freundlichen Grüßen

Mattias Schlenker