Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
16(4)570 G

Anhörung zum BSI-Gesetz, 11.5.2009

Stellungnahme Prof. Dr. Jörg Schwenk, Ruhr-Universität Bochum

1. Einleitung

In meiner Stellungnahme möchte ich die folgenden drei Aspekte der diskutierten Gesetzesvorlage unterscheiden:

- Aspekt 1: Notwendigkeit der Abwehr von Angriffen
- Aspekt 2: Benachrichtigung der von Angriffen Betroffenen
- Aspekt 3: Strafverfolgung

2. Aspekt 1: Notwendigkeit der Abwehr von Angriffen

Die Notwendigkeit der Abwehr von Angriffen auf die IT-Infrastruktur des Bundes scheint unbestritten. Es stellt sich somit lediglich die Frage, ob hierzu die Speicherung von Daten erforderlich ist.

Entwicklung seit 2004

Seit dem Jahr 2004 (Beginn der Phishing-Angriffe auf Online-Banking) hat eine Kommerzialisierung der Malware-Szene eingesetzt. Schadsoftware wird nicht mehr primär mit dem Ziel entwickelt, eine möglichst große Verbreitung zu erzielen, sondern mit dem Ziel, unentdeckt zu bleiben. Hierzu werden verschiedene Techniken angewandt:

- **Erzeugung einer Vielzahl von Varianten einer Schadsoftware**, mit unterschiedlichen Antiviren-Signaturen. So hat die Firma Symantec in einer Studie[1] eine Anzahl von 1.656.227 neuen Schadsoftware-Varianten für 2008 genannt, im Vergleich zu 624.267 im Jahr 2007, und 140.690 im Jahr 2006. Dies hat zur Folgen, dass Schadsoftware häufig unerkannt beliebt. Einer Studie[2] von Google aus dem Jahr 2008 zufolge hat klassische AV-Software daher nur eine Erkennungsrate von maximal ca. 70%.
- **Drive-by-Downloads: Der Browser wird zum Hauptangriffsziel**. Durch die Anstrengungen von Microsoft im Rahmen von Windows Vista, die Entwicklung von Schadcode deutlich zu erschweren, und die Einführung und Aktivierung von Personal Firewalls auf den PCs der Endnutzer, hat sich der Browser zum Hauptangriffsziel für Schadsoftware entwickelt. Im Detail wird dies in der bereits oben zitierten Studie[2] der Firma Google ausgeführt, aber auch die Berichte verschiedener Anti-Viren-Firmen (z.B. Sophos[3] oder Symantec[4]) bestätigen dies. Da ein Browser meist viele verschiedene Software-Erweiterungen (für PDF, Audio, Video, Grafik, ...) enthält, die sich oft auf einem veralteten Softwarestand befinden, bieten sich hier vielfältige Ansatzpunkte für Angriffe.

[1] http://www.symantec.com/business/theme.jsp?themeid=threatreport
[2] N. Provos, P. Mavrommatis, M. A. Rajab, F. Monrose: All Your iFrames Point to Us. Google Technical Report provos-2008a
[3] Sophos Security threat report: 2009
[4] http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf

Neue Analysemethoden

Zur Erkennung möglichst vieler Malware-Varianten sind neue Erkennungsmethoden erforderlich, die eine kurz- bis mittelfristige Speicherung potenzieller Schadprogramme erforderlich machen:

- **Verhaltensbasierte Analyse**. Hier wird eine Schadsoftware anhand typischer Verhaltensmuster entdeckt, z. B. anhand des Verbindungsaufbaus zu bestimmten Servern im Internet, oder anhand von typischen Manipulationen im Betriebssystem. Hier kann allerdings eine Zeitverzögerung eingebaut sein, um z.B. Angriffe auf Online-Banking nur am Wochenende zu starten, wenn die Banken telefonisch nicht zu erreichen sind. Probleme kann hier die Detektion von Analyseumgebungen durch die Malware bereiten. Hier verhält sich die Schadsoftware unauffällig, wenn sie eine bekannte Analyseumgebung (z.B. virtuelles Betriebssystem, keine Verbindung zum Internet) erkennt.
- **Strukturanalyse**. Hier wird die Struktur der potenziellen Schadsoftware durch Disassemblierung und Vergleich der Aufruf- und Ablaufgraphen mit bekannten Malware-Varianten eine Erkennung durchgeführt. Dies ist zeitaufwändig und benötigt eine Spezialsoftware. Probleme kann hier z.B. die Verschlüsselung der Schadsoftware bereiten. (Im Extremfall werden nur diejenigen Teile der Schadsoftware entschlüsselt, die gerade ausgeführt werden.)

Für diese Analysen ist es jedoch nur notwendig, die potenzielle Schadsoftware selbst zu speichern. Um die Aspekte 2 und 3 abzudecken, kann die Speicherung weiterer Daten erforderlich sein.

Art der zu untersuchenden Daten

Untersucht werden muss potenzielle Schadsoftware, die in Form von ausführbaren Dateien oder in Form von Scriptcode (z.B. Javascript) vorliegen kann. Dieser potenzielle Schadcode kann auf folgenden Wegen zum Opfer gelangen:

- **E-Mail**: Als Anhang zu einer E-Mail, oder in Form eines Hyperlinks in der E-Mail, der auf die Malware zeigt. Hier ist überwiegend nur der so genannte „Body“ der E-Mail betroffen, der keine regulären E-Mail-Adressen enthält.
- **WWW**: Als Javascript-Code (der auch unkenntlich gemacht sein kann), in Form von kompilierter Schadsoftware, in Form von Multimedia-Komponenten, in Form von eingebetteten Hyperlinks, aber auch in URL (Adresszeile) selbst. Hier besteht die Problematik darin, dass neben dem „Body“ der http-Nachricht auch der „Header“ betroffen sein kann.

3. Aspekt 2: Benachrichtigung von Betroffenen

Es ist sinnvoll, die von einem Angriff Betroffenen auch im Nachhinein zu informieren. Für die beiden betrachteten Infektionswege können die beiden folgenden Vorgehensweisen sinnvoll sein:

E-Mail

Die E-Mail-Adresse des Empfängers/der Empfänger sollte in verschlüsselter Form gespeichert werden. Dies ist möglich, da sich diese Daten an einer klar definierten Position im E-Mail-Header befinden, und diese Positionen für die Malware-Analyse nicht mit herangezogen werden müssen.

WWW

Im WWW definiert die IP-Adresse einen Sender, Empfänger oder Übermittler (http-Proxy). Auch IP-Adressen können in verschlüsselter Form für die Dauer der Analyse gespeichert werden. Ob eine Speicherung der IP-Adressen Sinn macht, ist allerdings fraglich, wie die nachfolgenden Beispiele zeigen:

- Beispiel 1: Der WWW-Datenverkehr in einer Bundesbehörde wird über einen http-Proxy geleitet. In diesem Fall müsste der Administrator dieses Proxys die Warnungen an die betroffenen Nutzer weitergeben, wozu er allerdings selbst wieder die IP-Adressen protokollieren müsste.
- Beispiel 2: Der WWW-Datenverkehr kommt ohne aktives Zutun des Nutzers zustande, z.B. durch ein manipuliertes Werbebanner. In diesem Fall würde der Nutzer die Warnmeldung ignorieren, da er die in der Warnung genannte Adresse ja nicht aktiv angewählt hat.

Eine alternative Vorgehensweise könnte hier sein, nach einem Malware-Funde die Malware-Signatur und die zugehörige URL an alle Dienststellen zu senden, ohne die IP-Adresse des Empfängers zu protokollieren.

4. Aspekt 3: Strafverfolgung

Zu den Bestimmungen zur Strafverfolgung im vorliegenden Gesetzentwurf wurden bereits in der Bundestagsdebatte wichtige Einwände geltend gemacht. Ich möchte mich hier auf technische Aspekte beschränken.

- Im Bereich der Strafverfolgung von Malware-Angriffen sind protokollierte E-Mail-Adressen nur von beschränktem Nutzen, da sie leicht gefälscht werden können. E-Mail-Adressen von potenziell interessanten Empfängern werden zudem in Malware-Kreisen gehandelt. Sie sollten daher prinzipiell nur verschlüsselt gespeichert werden.
- IP-Adressen von Servern können von infizierten Rechnern stammen (Botnetze, hier kann Aspekt 2 greifen.). Sie sollten verschlüsselt gespeichert werden.
- IP-Adressen von Clients, die beim Aufruf bestimmter, Malware-infizierter Webseiten protokolliert werden, können ohne Zutun des Nutzers automatisch durch den Browser aufgerufen werden (eingebettete Bilder, Javascript, XMLHttpRequest, ...). Sie sollten verschlüsselt gespeichert werden.

Für die Ermittlung der Hintergründe eines Angriffs mit Schadsoftware ist die Malware selbst der wichtigste Ausgangspunkt. Da die Malware selbst, oder die Hyperlinks, von denen die Malware geladen wird, an vielen verschiedenen Stellen sowohl im Body einer E-Mail, als auch in einer WWW-Seite positioniert sein kann, sind generelle Vorgaben zum Schutz Datenschutz-relevanter Daten nicht einfach machbar; nach Möglichkeit sollten alle Nachrichtenbestandteile, die nicht zur Analyse benötigt werden, in verschlüsselter Form gespeichert werden. Es kann möglich sein, hier für bestimmte Fallklassen Vorgaben zu machen. Dies erfordert aber eine genauere Untersuchung.

Da sich die Angriffsmethoden im Bereich Malware relativ schnell ändern können, scheint eine Festlegung der genauen technischen Vorgehensweise zur Analyse derjenigen Nachrichtenteile, die Malware oder Verweise auf Malware enthalten können, im Gesetzestext nicht zielführend. Stattdessen sollte die Festlegung der zu protokollierenden Daten periodisch aktualisiert werden, unter Hinzuziehung der Experten aus Datenschutz (z.B. dem Bundesdatenschutzbeauftagten) und der Malware-Forschung. Eine Verpflichtung zur Anonymisierung/Verschlüsselung bestimmter, unkritischer Nachrichtenteile (z.B. der E-Mail-Adressen) ist hingegen sinnvoll.

Bochum, den 11.5.2009 Prof. Dr. Jörg Schwenk