idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Pressemitteilung

Gesellschaft für Informatik e.V.
Cornelia Winter

23.09.2013
http://idw-online.de/de/news552741

Buntes aus der Wissenschaft, Forschungs- / Wissenstransfer
Gesellschaft, Informationstechnik, Medien- und Kommunikationswissenschaften, Wirtschaft
überregional

NSA: Back-Doors in 80.000 strategischen Servern weltweit

Nachrichtendienste haben eine Infrastruktur geschaffen, mit der sie das gesamte Internet und jede über öffentliche Netze abgewickelte Telefon- und Handy-Kommunikation überwachen sowie gespeicherte und übertragene Daten manipulieren können: Unternehmen und Behörden werden auch intern überwacht, Daten und Dokumente können manipuliert werden. Davon sind nicht nur vernetzte Computer betroffen; über Datenträger sowie über optische und akustische Ausspähung (z.B. Abhören von Tastenklicks) sind auch nicht vernetzte Rechner potenziell verwundbar.

Der Präsidiumsarbeitskreis „Datenschutz und IT-Sicherheit“ der Gesellschaft für Informatik e. V. (GI) warnt deutsche und europäische Unternehmen, Behörden und Private vor der z.B. von der NSA vorgenommenen Installation von Hintertüren auf den wichtigsten Internet-Servern mit dem Ziel, auch in die angeschlossenen Unternehmens- und Behördennetze einzudringen. Dies belegen jedenfalls die von Edward Snowden vorgelegten Dokumente. Wenn wir davon ausgehen, dass ausschließlich die Industriestaaten der G8 betroffen sind, entspricht das durchschnittlich 10.000 Servern pro Nation.

Die angegriffenen strategischen Computer sind neben den Vermittlungsrechnern der Telekommunikation weltweit die zentralen Server und Router der wichtigsten Unternehmen und Branchen wie Automobil, Energie (Kraftwerke und Strom- und Gasversorgung), Nahrungsmittel, Finanzen und Versicherungen, Telekommunikation, Medien, Transport und Verkehr, Gesundheit, Wasserversorgung, Chemie- und Pharmaproduktion.

Hartmut Pohl, Sprecher des Arbeitskreises: „Wir müssen davon ausgehen, dass diese Angriffstechniken auch von anderen Ländern wie z.B. England, Frankreich, Schweden, Russland, China, Japan und Korea, aber auch der organisierten Kriminalität eingesetzt werden.“

Die Angriffe nutzen bisher nicht bekannte und unveröffentlichte Sicherheitslücken (zero-day vulnerabilities) in weit verbreiteter Standardsoftware und auch Individualsoftware aus. Betroffen ist insbesondere Sicherheitssoftware wie Firewalls, Virensuchprogramme, Verschlüsselungs-Software, Systeme zur Intrusion Detection/Protection, außerdem (Open Source und proprietäre) Betriebssysteme. Daneben werden auf „Anraten“ der Nachrichtendienste ggf. auch schon von den Herstellern Sicherheitslücken eingebaut, die jederzeit gezielte Angriffe ermöglichen (z.B. "Security Updates" zu Betriebssystemen). Während dieser Angriffe – die praktisch nicht erkannt werden können - werden Back Doors installiert, die einen sofortigen oder zukünftigen Zugriff auf alle gespeicherten und kommunizierten Daten in Echtzeit ermöglichen. Alle Kommunikationsvorgänge können dann protokolliert, aufgezeichnet und zur Auswertung an die Nachrichtendienste übermittelt werden. Inhalte werden genauso gespeichert wie Verkehrsdaten: Sender, Empfänger, Datum, Ortsangaben etc.

Mit einem Aufwand von jährlich ca. 250 Mio. Dollar können mit HTTPS, PGP, GnuPGP, Skype, SSH, VPN/IPSec, Public Key Encryption verschlüsselte Daten offenbar auf 3 Wegen entschlüsselt werden:
- Die Algorithmen ‚schwacher‘ Verschlüsselungsverfahren werden gebrochen.

- In ‚starken' Verschlüsselungsverfahren werden Hintertüren oder unveröffentlichte Sicherheitslücken eingebaut oder ausgenutzt.
- Standardsoftware wie Skype wird dazu benutzt, Spionagesoftware auf dem Zielrechner zu installieren und mit deren Hilfe Kommunikation abzuhören bevor sie verschlüsselt wird.

Zu den damit möglichen Angriffen gehören Überwachung, Ausspionieren und Manipulation von:
- Banken - insbesondere von Kontendaten, Überweisungen und Geldanlagen (SWIFT) sowie Kurs- und Börsendaten.
- vermittelten und durchgeleiteten Nachrichten (Mails, Dateien, Dokumente) auf Servern von Telekommunikationsunternehmen.
- Kraftwerken, Strom- und Gasversorgung, Pipelines, Chemieprozesse, Wasserversorgung, Fehlsteuerung von Robotern.
- in Clouds gespeicherten Daten (bis hin zur Löschung), Benachteiligung bestimmter Benutzer, Abschalten von Clouds.
- Eindringen in die Rechner von Zeitungen, Zeitschriften und Sendern: Auslesen geplanter Sendungen, Manipulation von Dokumenten, Kommunikation mit Informanten.

Diese Fälle zeigen die akute Gefahr für Leib und Leben der Bürgerinnen und Bürger – so besteht z.B. die Manipulationsmöglichkeit der Steuerungsdaten in Kernkraftwerken.
Angesichts dieser Fakten empfiehlt der Arbeitskreis Unternehmen und Behörden sowie Privatpersonen dringend die folgenden Maßnahmen:
1. Die wichtigsten Programme – insbesondere die Sicherheitsprogramme – müssen systematisch auf Sicherheitslücken überprüft und gepatcht werden.
2. Ausschließlich hoch abgesicherte Computer und Netze dürfen an andere interne und externe Netze oder gar an das Internet angeschlossen werden.
3. Sicherheitsmaßnahmen wie Grundschutz und Umsetzung der Normen der ISO 27000 Familie (inklusive z.B. Verschlüsselung) stellen nur absolute Mindeststandards dar.
4. Nur betrieblich notwendige Daten sollen erfasst, gespeichert und übertragen werden (Datensparsamkeit).
5. Unverzichtbar sind systematische Security Tests der wichtigsten Anwendungen zur Identifizierung von bislang nicht erkannten Sicherheitslücken (Zero-Day-Vulnerabilities), Covert Functions und Back Doors .

Der Präsidiumsarbeitskreis fordert insbesondere die deutschen Unternehmen aber auch die Behörden auf, stärker in Forschung und Entwicklung wirksamer IT-Sicherheitstechnik zu investieren. Die bisher verfolgte Gedanke der ex-post Betrachtung von Angriffen und der reine Austausch über bereits erfolgte IT-Angriffe und Sicherheitsbedrohungen zwischen Wirtschaft und Regierung reicht jedenfalls nicht mehr aus.

Zu weiteren Details der Überwachungsaffäre 2013 verweisen wir ausdrücklich auf die FAQ der GI https://www.gi.de/themen/ueberwachungsaffaire-2013.html.

Die Gesellschaft für Informatik e.V. (GI) ist eine gemeinnützige Fachgesellschaft zur Förderung der Informatik in all ihren Aspekten und Belangen. Gegründet im Jahr 1969 ist die GI mit ihren heute rund 20.000 Mitgliedern die größte Vertretung von Informatikerinnen und Informatikern im deutschsprachigen Raum. Die Mitglieder der GI kommen aus Wissenschaft, Wirtschaft, öffentlicher Verwaltung, Lehre und Forschung.

Bei Veröffentlichung Belegexemplar erbeten. Vielen Dank!

Cornelia Winter

Stellvertreterin des Geschäftsführers
Gesellschaft für Informatik e.V. (GI)
Wissenschaftszentrum
Ahrstr. 45
53175 Bonn

Tel.: +49 (0)228/302-145 / Fax: +49 (0)228/302-167
E-Mail: gs@gi.de / WWW: http://www.gi.de

Cornelia Winter
Tel.: +49 (0)228/302-147 / E-Mail: cornelia.winter@gi.de

URL zur Pressemitteilung: http://www.gi.de