NSA-Überwachung – und kein Ende?

Nachrichtendienste überwachen weltweit vollständig jeden Computer, das gesamte Internet und jede Telefon- und Handy-Kommunikation und manipulieren gespeicherte und übertragene Daten weil sich Unternehmen und Behörden nicht ausreichend absichern.

Internationaler Stand der IT-Sicherheit

Nach Berichten von Edward Snowden wird das Internet mit der gesamten Telefonkommunikation im Festnetz, Mobil- und Satellitenfunk etc. vollständig überwacht, auch können alle Daten manipuliert werden. Von der NSA erfolgreich angegriffen und mit Back Doors versehen sind die weltweit wichtigsten 35.000 sog. strategischen Server – bis zum Jahresende 2013 sollen es 85.000 sein. Diese Angriffstechniken werden auch von den Nachrichtendiensten anderer EU- und G20-Staaten wie England, Frankreich, Russland, China, Japan, Korea etc. und der organisierten Kriminalität genutzt – und auch von der Organisierten Kriminalität als Trittbrettfahrer. Aber auch stand-alone Systeme werden seit Jahren erfolgreich angegriffen, Daten werden ausgelesen und manipuliert.

Die sog. strategischen Computer sind die zentralen Server, Switches und Router der weltweit wichtigsten Unternehmen wie Automobil, Energie (Kraftwerke und Strom- und Gasversorgung), Nahrungsmittel, Finanzen und Versicherungen, Telekommunikation (Internet-Infrastruktur), Medien, Transport und Verkehr, Gesundheit, Wasserversorgung, Chemie- und Pharmaproduktionen. Von diesen zentralen Servern wird in die internen Netze von Unternehmen (und Behörden) eingedrungen.

Diese Angriffe nutzen bisher nicht-bekannte, unveröffentlichte Sicherheitslücken (Zero-Day-Vulnerabilities), in jeder Art Software wie Anwendungen, Standardsoftware, Betriebssysteme (Open Source und proprietäre – auch ‚gehärtete') und auch Suchmaschinen, Industriesteuerungen etc. – insbesondere aber auch in Sicherheitssoftware wie Firewalls, Virensuchprogramme, Verschlüsselung (!), Intrusion Detection und Protection Systeme. Derartige Angriffe können praktisch nicht erkannt werden. Während der Angriffe werden Back Doors installiert, die einen sofortigen und auch jeder Zeit zukünftigen (!) Zugriff auf alle gespeicherten und kommunizierten Daten in Echtzeit ermöglichen. Alle Kommunikationsvorgänge werden protokolliert, aufgezeichnet, ausgewertet, Inhalte werden genauso gespeichert wie Verkehrsdaten: Sender, Empfänger, Datum, Lokationsdaten etc. Verschlüsselung wird geknackt (z.B.: Skype) oder der fragliche Rechner ist bereits kompromittiert.

Die Angriffe erfolgen nicht breitgestreut wie bei Viren, sondern sind vielmehr gezielt gegen ausgewählte Unternehmen und Behörden gerichtet. Eine der ersten dieser Targeted Attacks stellt der ca. 2006 entwickelte Wurm stuxnet dar; seitdem konnten etwa 10 Nachfolger identifiziert werden.

Beispiele sind die folgenden internationalen Fälle:

- Ausspionieren der Finanztransaktionen von Banken und auch Manipulation der Kontendaten, Überweisungen, Geldanlagen, Manipulation von Kurs- und Börsendaten
- Überwachung und Manipulation von vermittelten und durchgeleiteten Nachrichten (Mails, Dateien, Manipulation ausgetauschter Dokumente) auf Servern von Telekommunikationsunternehmen
- Störung von Industriesteuerungen und Prozessen: Kraftwerke, Strom- und Gasversorgung, Pipelines, Chemieprozesse, Wasserversorgung, Fehlsteuerung von Robotern
- Manipulation von in Clouds gespeicherten Daten (bis zur Löschung), Benachteiligung bestimmter Benutzer, Abschalten von Clouds
- Eindringen in die Rechner von Zeitungen, Zeitschriften und Sendern: Auslesen geplanter Sendungen, Manipulation von Dokumenten, Adressdaten von Informanten

Diese Fälle zeigen auch die akute Gefahr für Leib und Leben der Bundesbürger, Europäer und der Menschen in praktisch allen Industriestaaten! Gegen derartige erfolgreiche (!) Angriffe soll kein Kraut gewachsen sein?

Vollkommener Schutz gegen Advanced Persistent Threats (APT) u.a. Angriffe

Angesichts der umfangreichen internationalen Überwachung und Manipulation von Daten ist in Unternehmen und Behörden eine zeitnahe Initiative zur Abwehr dieser APTs u.a. komplexer, zielgerichteter Cyberangriffe unverzichtbar.

Mindeststandards: Grundsätzlich müssen die folgenden vorbeugenden Sicherheitsmaßnahmen ergriffen werden – sie stellen allerdings nur das absolute Minimum dar:

1. Ausschließlich hoch abgesicherte Computer und Netze dürfen an andere interne und externe Netze oder gar an das Internet angeschlossen werden.
2. Implementierung von BSI-Grundschutz und Umsetzung der ISO 27000 Familie (inklusive z.B. Verschlüsselung).
3. Nur unverzichtbar notwendige Daten sollen erfasst, gespeichert und übertragen werden (Datensparsamkeit).
4. Die wichtigsten Programme – insbesondere die Sicherheitsprogramme – müssen methodischen Sicherheitsprüfungen unterzogen werden:

Security Testing

Alle Angriffe benötigen zu ihrem Erfolg notwendig eine Sicherlücke, die sie ausnutzen können. Werden alle Sicherheitslücken identifiziert und gepatcht, kann kein Angriff mehr erfolgreich sein. Zur Identifizierung der Sicherheitslücken werden international die folgenden 3 Methoden eingesetzt.

1. Threat Modeling

Conformity Testing: In der Designphase wird die Übereinstimmung des Produktdesigns mit den Anforderungen, Richtlinien o.ä. geprüft. Vorgehen:

- Sichtung der Produkt-Dokumentation, Sichtung technischer Richtlinien und Erstellen einer Prüfliste mit relevanten Prüfkriterien
- Erstellung einer Mängelliste: Fehlende Übereinstimmung der Dokumentation mit den Anforderungen. Die

zugehörigen Hinweise auf Fehlerquellen werden ergänzt durch vorgeschlagene Behebungsmaßnahmen.

Threat Modeling ist die methodische Überprüfung der Sicherheitsarchitektur in der Designphase der Softwareentwicklung. Es ist nützlich, Sicherheitslücken in der Designphase zu beheben, weil die Fehlerbehebungskosten in dieser Phase noch sehr gering sind. Sicherheitslücken werden systematisch identifiziert durch die Prüfung aller Datenflüsse auf Threats (Bedrohungen) und Gegenüberstellung den vorgesehenen Sicherheitsmaßnahmen. Bleibt ein Threat ungesichert, stellt er seine Sicherheitslücke dar.

2. Static Source Code Analysis

Dieses Verfahren analysiert den Quellcode, ohne ihn auszuführen. In der Implementierungsphase wird die Konformität des Quellcodes der Zielsoftware (White-Box Test!) mit formalen Methoden auf Einhaltung syntaktischer und auch semantischer Programmierkonventionen und auf Einhaltung der Programmierrichtlinien überprüft - vergleichbar einem Parser, der eine lexikalische, syntaktische und semantische Analyse des Programmcodes durchführt.

Aufgrund lexikalischer Regeln der verwendeten Programmiersprache und den semantischen Zugehörigkeiten ist einen nachfolgender manueller Audit nötig, um false Positives auszuschließen und entsprechende Behebungsmaßnahmen zu entwerfen. Die Qualität und Quantität der Analyse-Resultate hängt somit maßgeblich von der Auswahl geeigneter Tools und geschultem Fachpersonal: Experten ab.

In dieser Phase muss auch auf undokumentierte Funktionen und Back Doors geprüft werden.

3. Dynamic Analysis: Fuzzing

Sicherheitsprüfung des Binär-Codes eines Systems auf bislang nicht identifizierte Sicherheitslücken sowie die Analyse, Dokumentation und Bewertung des Schweregrads (severity) identifizierter Sicherheitslücken. Eingesetzt werden bis zu 60 (!) kommerzielle und Open Source Tools.

Zuerst werden die Schnittstellen der Zielanwendung identifiziert. Hierbei kann es sich um eine Mensch-zu-Maschine-Schnittstelle (Webinterface, Clientinterface, etc.) oder um eine Maschine-zu-Maschine-Schnittstelle handeln, Schnittstellen, die nur für programminterne Abläufe notwendig sind. Dazu wird die Dokumentation herangezogen: Die Schnittstellen sind im Rahmen des technischen Entwurfs festgelegt entsprechend dokumentiert.

Die für die identifizierten Schnittstellen relevanten Fuzzing-Tools werden aus ca. 300 weltweit verfügbaren Fuzzing-Tools ausgewählt. Je nach Schnittstelle kommen davon bis zu 60 Tools zum Einsatz.

Die Identifizierung von Sicherheitslücken erfolgt beim Fuzzing-Prozess durch ein umfassendes Monitoring. Einige Fuzzing-Tools verfügen bereits über eine integrierte Monitoring-Funktionalität. Neben der Überwachung der Zielsoftware können auch ein System-Monitoring und eine so genannte „Valid Case Instrumentation" infrage kommen. Eine notwendige Voraussetzung für eine Vulnerability ist ihre Reproduzierbarkeit sowie das Erreichen eines sicherheitsrelevanten Zustands im Zielprogramm (Buffer Overflow, Code Injection etc.).

Erst der Einsatz mindestens dieser 3 Methoden im Rahmen des systematischen Security Testings ermöglicht erfahrungsgemäß die Identifizierung aller Sicherheitslücken.

Key Words: NSA, Sicherheitslücke, Vulnerability Security, Testing, Threat Modeling, Dynamic Analysis, Fuzzing

Prof. Dr. Hartmut Pohl
Geschäftsführender Gesellschafter softScheck GmbH Köln/Sankt Augustin

softScheck
we identify vulnerabilities others don't