Von guter, schlechter und böser Software

Bugs, die Nahrung für Malware

Software stellt heute in allen Branchen einen immer größeren Wertschöpfungsanteil dar. Wir nutzen Software in Großrechnern, PCs, Notebooks, Smartphones, aber auch immer mehr in Autos, Industrieanlagen, Kühlschränken etc. Waren zum Beispiel bei Autos in der Vergangenheit nur mechanische Bauteile für die Funktion verantwortlich, steigt der Wertschöpfungsanteil der Software in Autos immer mehr. Auch verfügen die Autos über immer mehr Sensoren, die von Software ausgelesen werden, um für mehr Sicherheit und Komfort zu sorgen. Das bedeutet aber auf der anderen Seite, dass die Software eine sehr hohe Qualität aufweisen muss, damit wir uns darauf verlassen können. Bei der Software in Autos wurde und wird sehr viel Aufwand in die Qualität und Verifikation von Software gesteckt, um diesem Anspruch zu genügen. Leider trifft dies für IT-Software oft nicht zu. Folgender Beitrag beleuchtet das Softwareproblem und die Konsequenzen daraus.

Eine gute Software erreicht ein hohes Maß an Qualität, das heißt, die Anzahl der Softwarefehler ist minimal. Eine gute Software ist gegeben, wenn sie eine hohe Funktionalität aufweist und alle Funktionen korrekt und zuverlässig arbeiten. Außerdem stellt eine gute Software eine einfache und verständliche Benutzerschnittstelle zur Verfügung. Eine gute Software erfüllt in einem hohen Maße Datensicherheits- und Datenschutzansprüche und weist so wenig wie nur möglich Softwarefehler (Schwachstellen, Bugs …) auf und ist damit resistent gegen Malware-Angriffe. Zwischen guter und bösartiger Software gibt es so etwas wie „gutartige" Software – in der Regel gängige Produkte wie Treiber, Betriebssysteme, Applikationen und Ähnliches, die Anwender wissentlich und aktiv nutzen. Bei gutartiger Software bestehen von Seiten der Hersteller keine kriminellen Hintergedanken wie etwa bei Malware. Trotzdem kann gutartige Software „gut" oder „schlecht" sein!

Eine schlechte Software hat viele Softwarefehler (Schwachstellen, Bugs …) und ist damit ideales Einfallstor für Angriffe auf Rechnersysteme. Das Risiko für die Ausnutzung der Schwachstellen und damit für Schäden ist entsprechend groß. Kriminelle Organisationen konzentrieren sich zunehmend auf dieses Problem, weil die Erfolgsaussichten eines positiven Angriffes auf unsere Rechnersysteme und die gespeicherten Werte hier sehr groß sind. Aus diesem Grund ist eine schlechte Software die Wurzel allen Übels und letztlich dafür verantwortlich, dass Betrüger bei der Infizierung von Rechnersystemen mit Malware so leichtes Spiel haben!

Ursachen für schlechte Software

Die Ursachen für schlechte Software sind: steigende Komplexität der Software, kein Sicherheitsbewusstsein der Softwareentwickler, fehlende Expertisen der Softwareentwickler (schlechter Programmierstil, mangelnde Informationen über eingesetzte Bibliotheken und Komponenten), fehlendes Wissen über aktuelle Sicherheitsbedrohungen, der Zeitdruck für die Fertigstellung der Software (Time-to-Market) und damit verbunden unzureichendes Testen und kurze Anforderungsphase und daraus resultierender unsystematischer Entwurf. Diese Liste der Gründe für schlechte Software ist nicht vollständig und daher noch erweiterbar.

Der Softwareentwicklungsprozess verläuft häufig unsystematisch und für heutige Anforderungen an die Software nicht professionell genug. Leider sind sehr viele Softwareentwickler heute nicht gut genug ausgebildet, um gute Software zu schreiben. Sehr negativ ist auch, dass viele Hersteller von Software viel zu wenig Verantwortung übernehmen, um dieses Problem nachhaltig zu lösen.

Die Hersteller arbeiten daran, die Anzahl der Schwachstellen in ihrer Software zu minimieren, aber die Angreifer machen oft einen besseren „Job". Aus heutiger Sicht ist festzustellen, dass sich dieser Zustand auch nicht kurzfristig ändern wird, das heißt, die Fehlerdichte von Software wird zwar kleiner, Fehlerfreiheit ist zurzeit aber für große Software nicht erreichbar. Die kleiner werdende Anzahl der Software-Schwachstellen wird wegen ihrer professionellen Nutzung durch kriminelle Organisationen immer bedrohlicher.

Ein besonderes Risiko sind sogenannte Zero-Day-Attacken. Entdeckt jemand eine Sicherheitslücke und meldet diese nicht dem Software-Hersteller, so wird die Schwachstelle der Software erst nach dem ersten Angriff bekannt. Zero-Day-Attacken sind daher sehr effizient, weil sie großflächig neue Sicherheitslücken ausnutzen, bevor Sicherheitsprodukte wie etwa Virenscanner die benötigten Signaturen zum Erkennen der Angriffscodes bereitstellen oder die Hersteller der Betriebs- und Anwendungs-Software in der Lage sind, entsprechende Patches zu liefern. Schlechte Software ist die Basis für bösartige Software, die Malware.

Bösartige Software: Malware

Malware ist der Oberbegriff für „Schadsoftware" wie Viren, Würmer, Trojanische Pferde etc. Angreifer (kriminelle Organisationen) nutzen Software-Schwachstellen von schlechter Software aus, um Malware auf Rechnersysteme zu installieren. Malware wird dann zum Beispiel über E-Mail-Anhänge oder Webseiten mit Schadcode, auf denen die Nutzer surfen und auf Links klicken, auf die Rechnersysteme geladen und verdeckt zur Ausführung gebracht. Das if(is) geht zurzeit davon aus, dass auf jedem 25. Rechnersystem ungewollte Malware vorhanden ist, die über ein Botnetz gesteuert wird. Mit Hilfe von Malware auf fremden Rechnersystemen können Angreifer diese vielfältig manipulieren und nutzen:

Eine Keylogger-Funktion in Malware speichert alle Informationen, die zum Beispiel über die Tastatur vom Nutzer auf dem eigenen Rechnersystem eingegeben werden. Diese Informationen, Ziel sind primär Identitäten und Passwörter, werden dann von der Malware regelmäßig in sogenannte Drop-Zonen im Internet gesendet. Drop-Zonen sind Speicherbereiche von beliebigen Servern im Internet, von denen sich die Angreifer die wertvollen Informationen holen und damit Angriffe auf die Internet-Dienste der Opfer durchführen.

Außerdem hat Malware Funktionen, mit denen sie in der Lage ist, das infizierte Rechnersystem beliebig zu steuern und zum Beispiel vertrauliche Dateien auszulesen. Damit ist unter anderem auch gezielte Industriespionage möglich. Weitere typische und nutzbare Funktionen von Malware sind: Spam-Verteilung, Beteiligung an DDoS-Angriffen und Click Fraud. Intelligente Malware ist sehr flexibel. Kriminelle Organisationen sind in der Lage, sie aus der Ferne zu steuern und auch neue Funktionen nachzuladen sowie weitere Rechnersysteme zu infizieren.

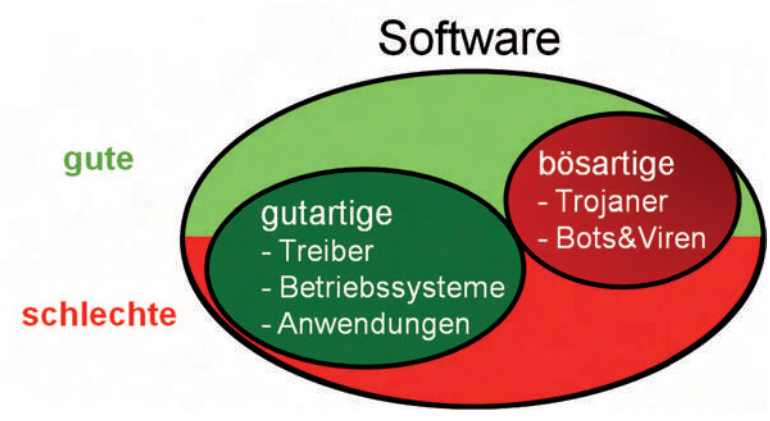
Eine weitere Herausforderung in diesem Bereich ist, dass zunehmend Malware gezielt für Personen und deren Rechnersysteme geschrieben und genutzt wird. Mit solchen „Targeted Attacks" sollen typischerweise Informationen wie Strategiepläne von Vorständen/Politikern/Generälen, Entwicklungsdaten von neuen Produkten usw. entwendet werden. Die Motivation dafür ist wirtschaftliche, politische oder militärische Spionage. Da bei solchen gezielten Angriffen Anti-Malware-Produkte konzeptionell schlecht wirken, muss hier nach neuen wirkungsvollen Sicherheitskonzepten gesucht werden. Malware ist sehr oft sehr gute Software (im Sinne der guten Programmierung)!

Intellige Malware – Stuxnet

Cyberwar wird eine immer realere Bedrohung in Form von gezielten Angriffen auf kritische Infrastrukturen. Neben den DDOS-Angriffen wie die auf Estland, ist Stuxnet eine weitere potentielle Bedrohung des Staates. Stuxnet bezeichnet ein Botnet mit einer qualitativ sehr hochwertigen Malware, die speziell für Produkte zur Überwachung und Steuerung technischer Prozesse (SCADA-System) der Firma Siemens entwickelt wurde. Es wird spekuliert, dass diese Malware mit dem Ziel geschrieben wurde, die Leittechnik einer Anlage zur Uran-Anreicherung im Iran zu sabotieren. Stuxnet hat eine neue Qualität von Malware eingeleitet, die sehr viel intelligenter ist, viel gezielter vorgeht und vor allem einen sehr viel größeren Schaden anrichten kann als frühere Malware. Stuxnet markiert den Startpunkt der Entwicklung von qualitativen Cyberwaffen, die Industrien und Infrastrukturen ganzer Länder lahmlegen können.

Mittel gegen Malware (bösartige Software)

Das beste Mittel gegen Malware ist die Entwicklung von guter Software. Da die Entwicklung von guter Software aber mittelfristig nicht zufriedenstellend gelöst werden kann, brauchen wir weitere Sicherheitsmechanismen, um die Auswirkung von Mal-



Gute und schlechte sowie gutartige und bösartige Software

ware nachhaltig zu verhindern. Die meisten der dafür heute angebotenen Lösungen arbeiten reaktiv – das heißt erkennen und dann entsprechend darauf reagieren.

Software-Updates
Eine effiziente Abwehr von Malware-Angriffen ist nur möglich, wenn sich die Software auf dem aktuellen Stand befindet. Sehr viele Software-Updates haben das Ziel, bekannte Schwachstellen schnell zu stopfen und dadurch die Angriffspunkte zu verringern. Leider gibt es viele Nutzer, die diese Software-Updates nicht oder nicht schnell genug einspielen und damit leicht angreifbar sind. Die Bekanntgabe der Software-Updates ruft auch die Angreifer auf, schnelle Strategien zu entwickeln und umzusetzen, um mit dem Software-Update bekannt gewordene Schwachstellen zu nutzen.

Anti-Malware
Anti-Malware-Lösungen wie Virenscanner sorgen auf den Rechnersystemen dafür, dass Malware, die Schwachstellen ausnutzt, erkannt und verhindert wird. Dies geschieht in der Regel mit Hilfe von Signaturen, die die Malware eindeutig identifiziert. Die Hersteller müssen die Malware kennen, damit sie in der Lage sind, diese Signaturen zu erstellen. Dazu haben die Hersteller von Anti-Malware sogenannte Malware-Traps im Internet positioniert und arbeiten sehr eng mit ihren Kunden zusammen, die beim ersten Auftreten von neuer Malware diese direkt an den Herstellen senden. Hier sind in Zukunft innovative Ideen gefragt, wie diese Angriffsfläche insgesamt effektiv verkleinert werden kann.

Erkennung von Malware im Kommunikationsverhalten
Eine weitere und neue Idee, Malware zu erkennen, besteht darin, dass in der Kommunikation von Rechnersystemen nach typischem Kommunikationsverhalten von Malware gesucht wird. Falls eine Malware-Kommunikation erkannt wird, ist das Rechnersystem mit einer Malware infiziert und es können Maßnahmen eingeleitet werden (siehe dazu auch: http://www.internet-sicherheit.de/forschung/aktuelle-forschungsprojekte/botnetze/).

Proaktive Sicherheitsmaßnahmen

IT-Sicherheitsmechanismen wie Anti-Malware und Software-Upgrades sind sicher sinnvoll, rennen den Angriffen jedoch immer hinterher und sind ohne nachhaltigen Erfolg. Wünschenswert sind proaktive IT-Sicherheitsmechanismen, die deutlich robuster gegen Angriffe sind [1].

Personal Firewall
Eine Personal Firewall sorgt dafür, dass nur bestimmte Kommunikations-Ports eines Rechnersystems vom und zum Internet genutzt werden, und sie kontrolliert auch, welche Programme auf den Rechnersystemen diese Ports nutzen. Sie sorgt dafür, die Angriffsfläche auf Rechnersysteme deutlich zu reduzieren.

Trusted Computing (Sicherheitsplattform)
Trusted Computing ist der Begriff für die Idee, IT-Technologie grundsätzlich vertrauenswürdiger zu machen. Eine der Hauptideen ist die Nutzung einer manipulationssicheren Hardware-Komponente, das Trusted Platform Module (TPM). Das TPM mit seinen Funktionen soll softwarebasierten Angriffen entgegenwirken. Die TPM-Spezifikationen wurden bereits von vielen Herstellern umgesetzt. Fast jedes aktuelle Notebook hat einen solchen Sicherheitschip. Das TPM wirkt als vertrauenswürdiger Anker in einem Rechnersystem (Root of Trust). Beginnend mit dem Startvorgang werden alle Hardware-Elemente und Software-Komponenten (BIOS, Betriebssystem, Anwendungsprogramme etc.) mit Hilfe von Hash-Funktionen gemessen und ihre Zustände im Platform Configuration Register (PCR) des TPM gespeichert. Die Systemkonfiguration des Rechnersystems ist also jederzeit komplett mess- und damit auch überprüfbar [2]. Damit können sich Rechnersysteme gegenüber einem Nutzer oder anderen Rechnersystemen hinsichtlich ihrer Systemkonfiguration „ausweisen". Dieser Vorgang wird Attestation genannt. Außerdem bietet das TPM die Möglichkeit, Daten zu versiegeln und vertraulich zu speichern. Dabei werden die Daten während der Verschlüsselung an die Systemkonfiguration gebunden. Dieser Vorgang wird Sealing genannt. Er stellt sicher, dass auf versiegelte Daten nur wieder zugegriffen werden kann, wenn sich das IT-System in einem bekannten Zustand (Systemkonfiguration) befindet.
Trusted Computing, genutzt in einer Sicherheitsplattform, die auch eine Virtualisierung auf Rechnersystemen ermöglicht, bietet sehr viele Vorteile. Es wird einfach möglich, Rechnersysteme so zu modellieren, dass Probleme isoliert und damit die Rechner gezielter geschützt werden können.

Fazit

Schlechte Software ist die Basis für die starke Verbreitung und Nutzung von Malware. Die Softwarehersteller müssen dieses Problem ernster nehmen und deutlich mehr tun, um bessere Softwareprodukte zu produzieren. Die Nutzer müssen nachhaltiger reaktive und zunehmend proaktive Sicherheitsmaßnahmen nutzen, um sich gegen Softwareangriffe zu schützen. ■

Literatur
[1] M. Linnemann, N. Pohlmann: „Sicher im Internet: Tipps und Tricks für das digitale Leben", orell füssli Verlag, Zürich 2010
[2] N. Pohlmann, Helmut Reimer: „Trusted Computing – Ein Weg zu neuen IT-Sicherheitsarchitekturen", Vieweg-Verlag, Wiesbaden 2008

Prof. Dr. (TU NN) Norbert Pohlmann, Informatikprofessor für Verteilte Systeme und Informationssicherheit im Fachbereich Informatik und Leiter des Instituts für Internet-Sicherheit – if(is) – an der Fachhochschule Gelsenkirchen.