AUSZUG AUS...
IT DIRECTOR
AUSGABE 1-2|2017

Security by Design als Wunderwaffe

Jede Woche neue Meldungen von Hackerangriffen. Die Unternehmen und vor allem die Entwickler stehen mit dem Rücken zur Wand. Abhilfe soll das Konzept „Security by Design" schaffen. Aber was steckt dahinter?

> Buffer Overflows zählen immer noch zu den 25 gefährlichsten Schwachstellen einer Software und zwar seit zwei Jahrzehnten. Dabei werden durch Fehler in den Programmen per „Pufferüberlauf" zu große Datenmengen in einen dafür zu kleinen reservierten Speicherbereich geschrieben. Auch Angriffsarten wie SQL-Injection und Cross-Site Scripting (XSS) sind zwar seit Jahren bekannt, aber noch sehr effektiv. Insbesondere bei einer stark verbreiteten Software können Schwachstellen dieser Art verheerende Auswirkungen haben. Ein Hacker kann durch eine einzelne Sicherheitslücke oft mehrere tausend User angreifen.

Allerdings besteht auch bei weniger stark verbreiteter Software ein hohes Schadenpotential. Der Grund dafür ist, dass bei der Software-Entwicklung vor allem darauf geachtet wird, dass das Programm die definierten Anforderungen erfüllt und alle Funktionen fehlerfrei ausführbar sind. Sicherheitsaspekte stehen nicht im Vordergrund und müssen sich der Wirtschaftlichkeit unterordnen. Das führt dazu, dass im Lebenszyklus einer Anwendung immer neue Lücken gefunden werden. Diese werden dann schnellstmöglich in teuren und aufwendigen Patch-Zyklen beseitigt. Auch das Zurückgreifen auf altbewährte Mittel (Firewalls, Intrusion Detection oder Malware-Schutz) bietet Unternehmen und deren Kunden kaum Schutz. Daher erkennen mittlerweile immer mehr Verantwortliche, wie wichtig es ist, schon von Beginn der Software-Entwicklung über den gesamten Prozess hinweg die Sicherheit im Blick zu haben.

Die Komplexität reduzieren

Die Lösung könnte das „Security by Design"-Prinzip sein. Dieses Prinzip gewährleistet eine integrierte, nachhaltige Anwendungssicherheit und unterstützt zudem den gesamten Entwicklungsprozess. Security by Design sollte nicht als Technik verstanden werden, sondern als eine Maßnahme während des Entwicklungsprozesses. Als Vorbild kann das „Security by Design"-Prinzip von Microsoft gelten. Microsoft entschloss sich 2002 als Reaktion auf eine stark ansteigende Zahl an Sicherheitslücken, seinen Entwicklungsprozess zu ändern. Es wurde ein 14-stufiger Plan entwickelt, an dem bis heute festgehalten wird.

Die Verantwortlichen sollten sich jedoch bewusst sein, dass die Einführung von Security by Design eine komplexe Aufgabe darstellt. Meist geht damit eine Änderung der Entwicklungskultur einher. Da sich die Umsetzung eines 14-stufigen Plans als sehr umfangreich gestaltet, sollte man sich anfangs auf wenige Stufen beschränken. Die Einführung erfolgt jedoch sehr individuell. Das bloße Adaptieren einer bestehenden Lösung ist nicht empfehlenswert. Die abgespeckte Variante sollte in kleinen Schritten eingeführt und im Laufe der Zeit erweitert und ausgebaut werden.

Die Einführung einer sichereren Entwicklung benötigt zudem die Unterstützung des Managements. Mit ihr steht und fällt der gesamte Prozess. Fehlt dieser Rückhalt, besteht die Gefahr, unter Zeitdruck zu geraten und Sicherheitsmaßnahmen zu vergessen. Ist die Management-Unterstützung aber gewährleistet, sollte sichergestellt werden, dass alle Entwickler über alle Sicherheitsgefahren aufgeklärt sind und diese bewältigen können. Durch Schulungen kann den Entwicklern ein besseres Wissen vermittelt und eigenes Know-how aufgebaut werden. Daraus resultierend lassen sich Leitfäden und Vorgaben definieren. Diese Maßnahmen sind vor dem Start der Anwendungsentwicklung durchzuführen und müssen immer wieder neu geprüft und definiert werden. Sind diese Maßnahmen aber alle ergriffen, kann die Entwicklung starten.

Als Erstes steht eine Risikoanalyse des Software-Entwurfs an. Hierfür wird das Verfahren „Threat Mode-

Sichere Programmierung

- Ein- und Ausgabenprüfung (Sanity Checks)
- Korrekte Handhabung/Schutz von sensiblen Daten
- Verhinderung von Informationsweitergabe
- Authentisierung/Zugriffskontrolle
- Befolgen des „Least Privilege"-Prinzips

Quelle: Voquz

ling" angewendet. Es erlaubt die Identifikation von Risiken und Gefahren im Entwurfsstadium. Falls Sicherheitslücken entdeckt werden, gilt es diese schnellstmöglich zu beheben. Die Durchführung des Threat Modelings ist neben der sicheren Programmierung einer der effektivsten Ansatzpunkte. Wird der Ansatz der sicheren Programmierung befolgt, lassen sich SQL-Injection, Cross-Site Scripting oder Fehler bei der Zugriffskontrolle in der Implementierungsphase verhindern.

Im letzten Schritt wird getestet, ob alle Vorgaben eingehalten wurden oder ob sich nicht doch noch Lücken eingeschlichen haben. Hierbei empfiehlt sich ein gründlicher Source-Code-Test. Dieser kann entweder intern durchgeführt oder als Managed Service beispielsweise an einen IT-Dienstleister wie Voquz IT Solutions in Ismaning ausgelagert werden. Die Weitergabe an einen externen Partner spart neben Zeit auch Kosten. Desweiteren hilft die Source-Code-Analyse den Entwicklern, zum einen die Konventionen und Qualität zu prüfen und zum anderen die Sicherheitslücken aufzudecken, zu dokumentieren und letztlich zu beheben. Da viele Sicherheitslücken bei der Eingabe auftreten, ist Fuzzing zu verwenden. Mit dieser wirksamen Maßnahme wird die Eingabeschnittstelle so lange mit generierten Eingaben beschickt, bis diese sicher ist und auch bei unerwarteten Eingaben keine Probleme auftreten. Mithilfe des gekürzten „Security by Design"-Prinzips lässt sich ein System implementieren, welches im Laufe der Zeit immer weiter ausgebaut werden kann. Das gekürzte Prinzip ist in den ersten Schritten ausreichend und behindert somit auch nicht das bestehende System.

Unternehmen können mit diesem Prinzip ihre Anwendungssicherheit verbessern und damit die Kosten für Entwicklung und Patches senken. Dadurch verbessert sich auch die Wettbewerbsfähigkeit. Die Vorteile überwiegen, jedoch hat die Umstellung auf Security by Design für Firmen weitreichende mittel- bis langfristige Konsequenzen. Von einer solchen Entscheidung ist stets der gesamte Betrieb betroffen und gerade am Anfang müssen einige Investitionen getätigt werden. Diese machen sich aber durch eine gesteigerte Produktqualität und künftige Kosteneinsparungen bezahlt. <

KRISTIN KALITT