Hintertür, wozu?!

Gastkommentar über Geheimdienstzugänge und ganz normalen Wahnsinn

Sorgen Geheimdienste gezielt für Hintertüren in kommerzieller Security-Software und Sicherheits-Systemen? Oder handelt es sich bei den mit (un-)schöner Regelmäßigkeit aufgedeckten Unzulänglichkeiten um den ganz normalen Wahnsinn heutiger Entwicklerarbeit?

Von Stefan Strobel, Heilbronn

Immer wieder kommen Diskussionen über Backdoors in Sicherheitssoftware auf – die Fans von Verschwörungstheorien werden nicht müde, auf angeblich vorsätzlich von Geheimdiensten oder Anbietern versteckte Hintertüren hinzuweisen, die eine heimliche Überwachung deutscher Firmen und unbescholtener Bürger ermöglichen sollen.

Nach fast 20 Jahren in der IT-Sicherheitsbranche habe ich den Glauben an solche Theorien größtenteils verloren. Nicht, dass ich an der Überwachung des Internets durch die Geheimdienste zweifeln würde: Dass die Geheimdienste Telefongespräche mitschneiden, Internetverbindungen anzapfen und auswerten, war vermutlich allen Sicherheitsexperten seit vielen Jahren klar. Eine gespielte Überraschung oder sogar Empörung über die Inhalte der Snowden-Enthüllungen mag für Politiker zweckmäßig sein, aber in der Sicherheitsbranche muss man sich fragen lassen, warum man zuvor an so etwas gezweifelt hatte.

Wenn es um angebliche Hintertüren in Software geht, dann habe ich andere Erfahrungen gemacht: Als Geschäftsführer einer IT-Sicherheitsfirma, die sehr viele Penetrationstests für große Kunden durchführt, sehe ich täglich Schwachstellen in Software-Produkten, bei denen man auf die Idee kommen könnte, dass hier bewusst Hintertüren eingebaut wurden. Die Ursache für diese Schwachstellen ist in den allermeisten Fällen jedoch ein unglückliches Zusammentreffen menschlicher Fehler mit mangelndem Sicherheitswissen und -bewusstsein sowie eng bemessenen Ressourcen. Trotz Schulungen und Entwicklungsrichtlinien werden immer noch regelmäßig Web-Anwendungen mit SQL-Injection-Schwachstellen implementiert – Sicherheitskonzepte fehlen oft ganz oder sind unvollständig.

Schwieriger Status quo

Müssen die Hersteller von Netzwerkkomponenten oder sogar Sicherheitsprodukten das besser machen? Schön und wünschenswert wäre das ohne Zweifel. Aber leider wird auch in dieser Branche oft mehr Wert auf funktionelle Weiterentwicklung gelegt als auf Sicherheit – und die Entwickler müssen unter hohem Druck ihr Releasedatum einhalten.

Als Felix Lindner (alias FX) die chinesischen Router von Huawei analysiert und die Ergebnisse auf verschiedenen Konferenzen vorgestellt hat, war die Liste der Schwachstellen lang. Auf die Frage eines Teilnehmers auf der IT-Sicherheitskonferenz IT-Defense, ob er Hintertüren der chinesischen Regierung gefunden hat, antwortete er sinngemäß: „Wofür braucht man bei der Menge an Schwachstellen noch Hintertüren?"

Dieser Zustand lässt sich vermutlich auf weite Teile der Softwareindustrie übertragen. Der Hersteller Barracuda beispielsweise geriet mit seinen Anti-Spam- und auch WAF-Produkten in den letzten Jahren mehrfach in die Kritik, da er Wartungszugriffe auf die bei Kunden installierten Appliances theoretisch auch ohne Freigabe des betroffenen Kunden durchführen konnte. Auch hier waren die Ursachen offensichtlich ein wenig durchdachtes Konzept für die Freischaltung der Wartungstunnel und eine schlechte Implementation, nicht aber eine versteckte Hintertür.

Natürlich wird man kaum jemals final beweisen können, dass eine Schwachstelle nicht doch von einem Geheimdienst beauftragt wurde. Solange die Softwareentwickler in aller Welt aber keinen fehlerfreien

Code implementieren – und das ist wohl eine Utopie –, besteht solcher Bedarf gar nicht. Mit genügend Ressourcen und Zeit kann man vorhandene Schwachstellen finden und ausnutzen, bevor sie öffentlich werden. Dass nicht nur „Hacker" nach solchen Verwundbarkeiten suchen, um sie selbst auszunutzen, war auch noch nie ein Geheimnis. Selbst zahlreiche deutsche Sicherheitsexperten verkaufen die von ihnen gefundenen Schwachstellen an amerikanische Firmen, die sie ihrerseits weiterverkaufen – auch an entsprechende Behörden. Und selbstverständlich gibt es bei den Militärs zahlreicher Länder Abteilungen, die sich mit der Suche und Ausnutzung von Sicherheitslücken beschäftigen.

Wozu also sollte ein Geheimdienst darüber hinaus noch mit hohem Aufwand und einem gewissen Risiko Hintertüren in „fehlerfreie" Software einschleusen?!

Die Cloud hilft

Wo die Software selbst „zu sicher" wird, bieten Hersteller freundlicherweise Cloudservices an, die es den Geheimdiensten im jeweiligen Land ermöglichen, die Daten bei Bedarf direkt am Speicherort abzuholen. Auch hier wird typischerweise keine geheime Hintertür in der Software selbst benötigt: Die Rechtslage in den USA, aber auch in anderen Ländern, sieht solche Zugriffe durch die Behörden ja offiziell vor.

Und wenn Unternehmen aus diesem Grund eine Verlagerung ihrer Daten in Cloudservices ablehnen, dann nutzen doch typischerweise ihre Mitarbeiter Dienste wie DropBox, YouSendIt, SourceForge und vieles mehr, ohne dass die IT-Abteilung dies bemerkt oder verhindert. Sogar Analysen bei Unternehmen, die Cloudservices per URL-Filter blockieren, haben gezeigt, dass Mitarbeiter dennoch eine kaum kontrollierbare Schatten-IT in der Cloud etablieren konnten.

Unabhängig von Clouddiensten sind in den letzten Jahren zudem viele Unternehmen dazu übergegangen, den Betrieb ihrer IT in die Hände von Drittfirmen zu geben, die ihrerseits viele Aufgaben in Ländern mit billigerem Lohnniveau erbringen oder erbringen lassen. Auch in diesem Fall benötigen Geheimdienste für das Ausspähen von Daten wohl kaum geheime Hintertüren in Softwareprodukten. ■

Stefan Strobel ist geschäftsführender Gesellschafter und Gründer der cirosec GmbH.