HANSER

Stille im Netz

Michael Zalewski

Ein Praxishandbuch zu passiver Reconnaissance und indirekten Angriffen

ISBN 3-446-40800-2

Vorwort

Vorwort

Was braucht es, um einen Roman zur Computersicherheit zu schreiben? Oder besser: Um überhaupt einen Roman zur modernen Datenverarbeitung zu schreiben?

Einen jungen und doch sehr erfahrenen Autor mit Begabungen in vielen Bereichen wie Computing, Mathematik und Elektronik, vielleicht der Robotertechnik als Hobby, zahlreichen anderen, auf den ersten Blick fachfremden Interessen (wie beispielsweise der fatalistischen erotischen Fotografie) und dem ausgeprägten Wunsch, zu schreiben – wobei diese Begabung gleichermaßen ausgeprägt ist.

Es war einmal in einem dunklen und weitgehend unerforschten Wald. Dort gebaren die (Hirnzellen-)Bäume dank Zauberwerk ein Datenbit. Sie sandten es einen reißenden Fluss hinab, bis es das riesige Meer (des Internets) erreichte. Dort fand es ein neues Heim, sein Grab oder vielleicht auch einen Platz in einem Museum.

Und so beginnt unsere Geschichte. Ob unser kleines Bit gut oder böse ist, spielt keine Rolle: Bereits in jungen Jahren wird es den Strom erreichen, der in eine strahlende Burg führt, welche aus weißem Metall gebaut ist (und den meisten doch nur als schwarzer Kasten gilt). Es wird durch das Portal treten und sich zum Schalter begeben, um sich anzumelden. Wäre es nicht so naiv und blauäugig, es hätte die Gruppe verkommen aussehender Bits längst bemerkt, die den Schalter von Ferne beäugen und zur Kenntnis nehmen, wann immer Bits ein- oder auschecken; allerdings hätte es sowieso keine andere Wahl gehabt, als mit der Anmeldung fortzufahren.

Nach einer kurzen Erholung würde unser Held gebeten, sich seinen Geschwistern oder einer anderen Gruppe von Bits beizugesellen. Gemeinsam würden sie ihre Leiber dann sämtlichst in ein gebrauchtes Schlauchboot quetschen. Ein vorsichtiges Bit könnte Abfallbits im Boot bemerken, die mutmaßlich von einer vorherigen Fracht übrig geblieben sind. (Aber ist das eigentlich wirklich Abfall?)

Nach einer langen und beengten Fahrt durch Staus und vorbei an vielen Verkehrsampeln (deren Lichtzeichen selbstverständlich beachtet werden) gelangen unsere Bits in einen sicheren Hafen und schippern dort zu den Landungsbrücken. Wird man sie von den Burgen und Leuchttürmen in der Nähe aus wahrnehmen? Wird jemand hingehen und verzeichnen, wann die Ampeln umschalteten – nur um genau sagen zu können,

wann unser Trupp fuhr? Wird irgendjemand Scheinwerfer auf den Pier richten und dort Fotos machen? Werden die anderen bösen Bits die Identität unserer Haudegen übernehmen und zuerst absegeln? Unsere Bits würden es nicht wissen.

Und so wechseln sie am Pier das Gefährt und stechen erneut in See. Die Fahrt unserer Helden geht weiter, und es stehen ihnen noch viele Gefahren bevor …

Nein, Michal Zalewskis Buch verbirgt die technischen Abläufe nicht hinter einer Mär, wie ich es gerade getan habe. Stattdessen beschreibt es alle Fakten klar und deutlich und vermittelt die Lösungen für die größten Herausforderungen gleich zu Anfang jedes Kapitels. Und trotzdem macht es Spaß, dieses Buch zu lesen.

Stille im Netz ist in vielerlei Hinsicht einmalig. Zwei Aspekte aber treten besonders deutlich zutage: Zunächst bietet es eine ausführliche Beschreibung fast aller wesentlichen Phasen der Datenverarbeitung, die das moderne „Internetworking" ermöglichen – von der ersten Tastaturbetätigung bis zum gewünschten endgültigen Ergebnis dieser Handlung. Zweitens skizziert es die weitgehend vernachlässigten, zu wenig erforschten und inhärenten Sicherheitsfragen, die mit der Netzwerktechnologie im Ganzen und mit jeder ihrer einzelnen Phasen verbunden sind. Die hier behandelten Sicherheitsprobleme eignen sich gut, um die verschiedenen Formen der Erforschung von Schwachstellen sowohl aus der Perspektive des Angreifers als auch aus der des Verteidigers zu demonstrieren, und bestärken den Leser darin, weitere Untersuchungen in diesem Bereich anzustellen.

Natürlich kann ein Buch über Computersicherheit niemals vollständig sein. In *Stille im Netz* provoziert Zalewski durch seinen Ansatz, all die vertrauten, hochgradig gefährlichen und weitverbreiteten Sicherheitslücken und Angriffe, die heutzutage von fast allen Mitgliedern der Datensicherheits-Community beschrieben werden, außen vor zu lassen. Er erzählt Ihnen vielmehr etwas über subtile tastaturbasierte Timingangriffe, erwähnt aber nicht, dass Trojanische Pferde, die Tastatureingaben protokollieren können, derzeit nicht nur wesentlich häufiger auftreten, sondern generell auch einfacher zu realisieren sind, als es die von ihm beschriebene Angriffsform je sein wird.

Man ist zu fragen versucht, warum Timingangriffe erwähnt werden, Trojaner jedoch nicht. Nun, solche auf Ablaufmustern basierenden Angriffe werden auch von den Profis im Bereich IT-Sicherheit weitgehend unterschätzt, während Trojanische Pferde eine Bedrohung darstellen, die weithin bekannt und offenkundig ist. Die Anfälligkeit gegenüber Timingangriffen ist eine strukturelle Eigenschaft zahlreicher häufig eingesetzter Komponenten, während die Implantation eines Trojaners entweder einen Softwarefehler oder ein Fehlverhalten des Endbenutzers erfordert.

Von nur sehr wenigen Ausnahmen abgesehen werden Sie in *Stille im Netz* konsequenterweise nicht die kleinste Einlassung zu vielfach ausgenutzten Softwarebugs finden – nicht einmal universelle „Bugklassen" wie Pufferüberläufe werden hier mit einem Wort erwähnt. Wenn Sie mit den gängigen Computersicherheitsrisiken nicht vertraut sind und dieses Wissen erwerben wollen, dann müssen Sie sich unter Umständen auch weniger spannendes Material (insbesondere zu den von Ihnen verwendeten Betriebssystemen) zu

Gemüte führen, welches Sie im Internet und in anderen Büchern finden. Dann aber wird dieses Buch sie mitnehmen auf eine spannende Reise.

Warum aber sollte man sich der Stille widmen, fragen Sie sich? Die Stille ist doch ein Nichts! In gewissem Sinne schon. Eine Null ist in diesem gewissen Sinne auch ein Nichts. Aber sie ist auch eine Zahl – ein Konzept, ohne welches wir die Welt nicht verstehen können.

Genießen Sie die Stille – so gut wie möglich.

Alexander Peslyak

Gründer und technischer Direktor von Openwall, Inc.

besser bekannt unter dem Namen

Solar Designer

Leiter des Openwall-Projekts