2014/16 Lifestyle

https://shop.jungle.world/artikel/2014/16/software-mit-herzfehler

Der Heartbleed-Bug

Software mit Herzfehler

Von **Boris Mayer**

Mehr als zwei Jahre lang blieb der Heartbleed-Bug unbemerkt. Das heißt aber nicht, dass niemand davon wusste.

Er ist zwar nicht der erste Bug mit eigenem Logo, aber Heartbleed ist der erste Softwarebug, der zeigt, wie verwundbar die Strukturen des verschlüsselten Datenverkehrs sein können. Und er ist eine Katastrophe. Der nicht eben für Alarmismus bekannte Computersicherheitsexperte und Kryptologe Bruce Schneier schreibt auf seinem Blog über den Bug mit dem blutigen Herzchen-Logo: »Katastrophal ist das richtige Wort. Auf einer Skala von Eins bis Zehn ist das eine Elf.« Eine halbe Million Server sind bisher betroffen, wie viele es auf Clientseite sind, ist bisher unbekannt.
Bei Heartbleed handelt es sich um einen Fehler im Programmcode von OpenSSL. Dieses ist nicht einfach nur ein eigenständiges Programm, sondern eine Softwarebibliothek, die ihre Funktionen anderen Programmen zur Verfügung stellt. Viele Programme nutzen OpenSSL, wenn sie eine verschlüsselte Verbindung über das Internet aufbauen wollen, anstatt sich selbst um die Sicherheit zu kümmern. Im Normalfall ist eine solche Übernahme einer Aufgabe durch eine spezialisierte Fremdsoftware wie OpenSSL auch das richtige Vorgehen, denn jeder kleinste Programmierfehler könnte potentiell dazu führen, dass eine verschlüsselte Verbindung nicht mehr sicher ist. Wird eine Standard-Implementierung verwendet, die auch noch Open Source ist – bei der der Programmcode für jedermann einsehbar ist – sollten Fehler in der Regel sehr schnell entdeckt werden. Die Entwickler von OpenSSL haben die Regelung, dass ein neues Stück Programmcode vor der Veröffentlichung in einer neuen Version noch von einem anderen Kollegen geprüft werden muss – aber bei Heartbleed haben weder der Autor selbst noch der Reviewer den Fehler entdeckt.

Seinen Namen hat der Softwarebug daher, dass er in der Heartbeat-Funktion von TLS (das ist die Abkürzung für Transport Layer Security) in OpenSSL gefunden wurde. Ein Heartbeat – also ein Herzschlag – dient bei netzwerkbasierten Programmen dazu, die Gegenseite der Verbindung in regelmäßigen Abständen darüber zu informieren, dass diese Verbindung noch besteht und man für weitere Befehle oder Datenübertragungen bereit

ist. Durch den Fehler kann nun diese Funktion dazu gebracht werden, einen kleinen Speicherblock von 64 kB Größe an die Gegenstelle zu übertragen. Und auch wenn dieser Datenblock ziemlich klein ist, ist er tückisch: Bestimmt werden kann nämlich, welcher Datenblock übertragen werden soll – und so könnte eine dazu nicht befugte Person (oder ein Programm) mit einigen hunderttausend bis Millionen Abfragen den ganzen Arbeitsspeicher eines Servers auslesen.
Dieser Datenspeicher wiederum kann wichtige Dinge enthalten. Wenn sich gerade jemand auf dem Server einloggt, wird zu einem bestimmten Zeitpunkt, zumindest kurz, dessen Username und Passwort unverschlüsselt im Speicher des Servers stehen. Noch wichtiger aber ist, dass der sogenannte private Schlüssel des Servers irgendwo im Speicher sein muss, da der Server ohne diesen privaten Schlüssel den an diesen Server gerichteten Datenverkehr nicht entschlüsseln könnte.
Fällt einem Angreifer aber dieser private Schlüssel in die Hände, so kann er den kompletten Datenverkehr, der an diesen Server gerichtet ist, ebenfalls entschlüsseln – und das gilt nicht nur für den aktuellen Datenverkehr, sondern auch für den, den ein Lauscher vielleicht in den vergangenen zwei Jahren zufällig mitgeschnitten und auf einer Festplatte abgelegt hat.
Eine Auswirkung der Heartbleed-Katastrophe ist also, dass man nicht mehr sicher sein kann, ob der verschlüsselte Datenverkehr aus den letzten Jahren wirklich zwischen den beiden Endpunkten – Server und Client – geheim geblieben ist oder eben nicht doch noch irgendwo nachgelesen wird.

Hinzu kommt, dass der Bug ganze 27 Monate unentdeckt blieb. Unentdeckt bedeutet bei Bugs nicht, dass niemand davon wusste, sondern lediglich, dass ihre Existenz nicht öffentlich oder zumindest dem Hersteller bekannt war – so kommt es beispielsweise immer wieder vor, dass User solche Fehler entdecken, aber nicht weitermelden, um gegebenenfalls von ihnen profitieren zu können. Schnell kamen deshalb Gerüchte auf, die NSA habe Heartbleed schon seit vielen Monaten gezielt genutzt, um sich viele private Schlüssel zu beschaffen und möglichst viel Datenverkehr mitlesen zu können. Das Weiße Haus und die NSA via Twitter haben dies schon dementiert, mit der Begründung, die NSA sei dazu verpflichtet, eine solche Lücke sofort bekannt zu machen, wenn sie Kenntnis davon erlange. Das stimmt aber nur zum Teil, denn die NSA muss nicht veröffentlichen, wenn eine Veröffentlichung klar die nationale Sicherheit oder eine Strafverfolgung gefährden würde – also eben jene Begründung vorliegt, auf der letztlich das gesamte Abhörprogramm der NSA basiert.
Unabhängig davon, wer eventuell mitgelesen haben könnte, sind die Folgen von Heartbleed drastisch: Alle Computer, die eine der betroffenen OpenSSL-Versionen einsetzen, brauchen ein Update und ein neues Sicherheitszertifikat, während das alte für ungültig erklärt werden muss. Ein Großteil der Firmen, die solche Zertifikate ausstellen, zeigte sich zwar sofort bereit, die Zertifikate ihrer Kunden kostenlos auszutauschen – aber schon jetzt steht fest, dass sie gar nicht die Kapazitäten haben, so viele in kürzester Zeit auszustellen. Eine halbe Million Zertifikate werden normalerweise über mehrere Monate ausgestellt, nicht innerhalb weniger Tage.
Und dann sind da noch die kleinen Computer, die von ihren Benutzern meist nur für smarte Telefone gehalten werden. Android-Handys mit dem System Android 4.1.1 könnten betroffen sein – ein Update gibt es bislang noch nicht. Schlimmer sieht es noch bei

Embedded-Systemen wie manchen Routern und DSL-Modems aus, in denen der Bug auch vorhanden sein könnte und bei denen es keine Möglichkeit für ein Softwareupdate gibt – sie können nur weggeworfen werden.

Das Ganze erinnert ein wenig an das Y2K-Problem, besser bekannt als »Millenium Bug«. Damals, kurz vor Anfang des neuen Jahrtausends, wurde überall vor der großen Computerkatastrophe gewarnt, doch die blieb aus. Für Experten ist klar, dass dies an der guten Vorbereitung der IT-Industrie lag, in den Augen der Gesellschaft aber war es nur ein künstlich aufgeblasenes Problem, es war ja schließlich nichts passiert. Ähnlich könnte es auch mit Heartbleed enden: Bleibt die Datenkatastrophe aus, haben die Experten gut an der Eingrenzung gearbeitet und wir hatten auch ein bisschen Glück. Ein Ausbleiben der Katastrophe würde aber nicht bedeuten, dass der Bug keine Schäden angerichtet hat.