Der monatliche Security Awareness Newsletter für Computeranwender

OUCH!

IN DIESER AUSGABE...

- **Was ist Heartbleed?**
- **Muss ich handeln?**
- **Vorsicht vor Phishing Angriffen**

Heartbleed - Warum sollte mich das kümmern?

Überblick

Am Montag, dem 7. April 2014, wurde eine schwerwiegende Schwachstelle in einer der meistgenutzten Implementierungen des SSL Protokolls, OpenSSL, veröffentlicht. SSL ist ein sehr wichtiges Sicherheitsprotokoll, dass im ganzen Internet verwendet wird. SSL schützt nicht nur Ihre Onlinekommunikation; es stellt auch sicher dass Sie sich zu legitimen Webseiten verbinden wenn Sie online einkaufen oder Onlinebanking betreiben. In diesem Newsletter geben wir einen kompakten Überblick der Bedeutung dieser Schwachstelle, wieso Sie betroffen sind und wie Sie sich schützen können.

Gastautor

Jake Williams (**@MalwareJake**; **malwarejake.blogspot.com**) ist wissenschaftlicher Leiter bei CSRgroup, einem auf Beratung im Kontext IT-Sicherheit spezialisierten Unternehmen. Er ist zudem der Co-Autor der Kurse Memory Forensics (FOR526) und Malware Reverse Engineering (FOR610) des SANS Institute.

Was its Heartbleed?

Die Heartbleed genannte Schwachstelle erlaubt es Angreifern, durch eine einfache Verbindung zu einem Webserver äusserst sensible Informationen zu sammeln, darunter z.B. Ihre Benutzernamen und Passwörter. Wenn ein Angreifer an diese Informationen gelangt, kann er sich damit an jedem Ihrer Benutzerkonten anmelden, dass diese Benutzernamen-Passwort-Kombination verwendet. Die Schwachstelle in OpenSSL existierte bereits seit gut 2 Jahren, wurde jedoch erst vor kurzem von Sicherheitsforschern entdeckt und am 7. April öffentlich kommuniziert. Heartbleed betrifft keine Windows oder Mac Computer; es betrifft primär Webseiten die von Ihnen genutzt werden wie z.B. Facebook, Gmail und viele mehr. Nicht jede Webseite im Internet ist betroffen, aber sehr viele von ihnen. Sie können z.B. mittels der Prüfseite von Lastpass nachsehen, ob ein von Ihnen genutzter Dienst darunter ist:
https://lastpass.com/heartbleed/.

Was sollte ich tun?

Es gibt mehrere Maßnahmen die zum Schutz ergriffen werden können. Diese Maßnahmen sind nicht nur gegen die Heartbleed Schwachstelle hilfreich, sie werden Sie ebenfalls gegen weitere, zukünftige Angriffe schützen:

- Als erstes sollten sie all Ihre Passwörter der Webseiten, von denen sie wissen, dass sie verwundbar waren und dass die Schwachstelle entfernt worden ist, ändern, angefangen mit den für Sie wichtigsten Zugängen. Falls Sie nicht wissen ob eine Webseite verwundbar war, ändern Sie die Passwörter dennoch, es ist eine gute Gelegenheit Ihre Passwörter zu erneuern und damit die Sicherheit online zu erhöhen.
- Stellen sie sicher, dass sie beim Erneuern der Passwörter gute, schwer zu erratende Passwörter auswählen. Zusätzlich sollten sie die 2-Faktor Authentifizierung auf Webseiten, die diese anbieten, aktivieren. Dies ist ein weiterer Schritt, der ihre Konten zusätzlich absichert.

Heartbleed - Warum sollte mich das kümmern?

- Stellen Sie auch sicher, dass Sie separate, einzigartige Passwörter für jedes Ihrer Konten nutzen. Auf diese Weise bleiben im Falle einer Kompromittierung eines Anbieters Ihre übrigen Konten sicher. Sie können sich nicht all Ihre Passwörter merken? Glückwunsch, das bedeutet nämlich, dass Sie gute Passwörter benutzen. An dieser Stelle möchten wir ihnen die Nutzung eines Passwort Managers empfehlen, der Ihre Passwörter sicher aufbewahrt. Ein solcher kann ihre Online Aktiväten nicht nur vereinfachen, sondern auch deutlich sicherer machen.
- Vergessen sie nicht Ihre E-Mail Programme. Wenn ihr E-Mail Prgramm, wie Microsoft Outlook oder Apple Mail, SSL bei der Verbindung zum E-Mail Server benutzt, könnte es sein, dass Sie diese Passwörter ebenfalls ändern sollten.

Mehr Informationen zu diesen Maßnahmen finden sie bei den weiterführenden Informationen am Ende dieses Newsletters.

Der beste Schutz besteht darin, zeitnah die Passwörter für wichtige Online-Konten zu ändern und dabei starke, einzigartige Passwörter für jeden Dienst zu verwenden.

Vorsicht vor Phishing Angriffen

Unglücklicherweise sind Angreifer ”Abstauber”. Sie wissen, dass die Heartbleed Schwachstelle in den Nachrichten war und dass viele Menschen, Sie eingeschlossen, davon gelesen haben. Sie werden daher gefälschte E-Mails erstellen, die so aussehen als kämen sie von legitimen Webseiten die Sie benutzen (wie Banken oder Onlineshops). Sie geben vielleicht sogar vor, für eine Sicherheitsfirma zu arbeiten die kostenlose Hilfsprogramme gegen Heartbleed anbieten.

Diese Taktik, gemeinhin Phishing genannt, ist nicht neu. Angreifer versuchen Sie dazu zu bringen, auf Links zu klicken die auf manipulierte Webseiten führen, oder Sie zum Ausführen infizierter Dateianhänge zu bewegen. Wenn Sie diesen Angriffen zum Opfer fallen, kann Ihr Computer infiziert werden. Statt diesen Pseudo-Handreichungen zu folgen, rufen Sie Webseiten einfach durch Eintippen der Webseitenadresse im Browser auf, wenn sie dort ihr Passwort ändern wollen. Auf diesem Weg können Sie sicher sein, sich zur richtigen Webseite zu verbinden.

Weiterführende Informationen

Welche Seiten sind verwundbar (englisch):	https://lastpass.com/heartbleed/
OUCH! Passwörter:	http://www.securingthehuman.org/ouch/2013#may2013
OUCH! Passwortmanager-Programme:	http://www.securingthehuman.org/ouch/2013#october2013
OUCH! Zwei-Wege-Authentifizierung:	http://www.securingthehuman.org/ouch/2013#august2013
OUCH! Phishing:	http://www.securingthehuman.org/ouch/2013#february2013
Technische Details:	http://www.heise.de/security/artikel/So-funktioniert-der-Heartbleed-Exploit-2168010.html

Redaktionsleitung: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis