15. Apr. 2014

von Martin

in Cyber Security, Sicherheitskultur

Kommentare (5)

Blutende Herzen und gebrochenes Vertrauen: Was folgt aus dem Heartbleed Bug?

von Martin Schmetz

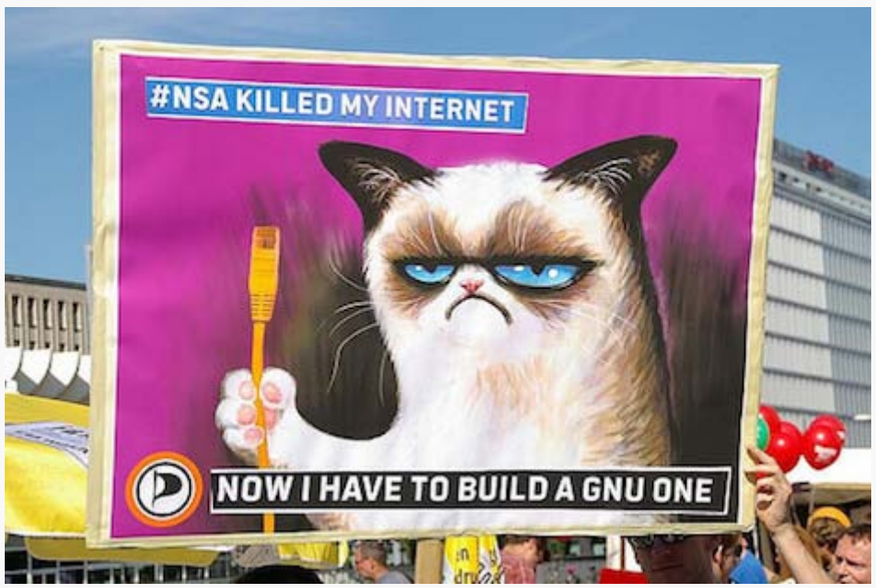
Der Heartbleed Bug hat das Internet aufgeschreckt. Ein zentrale Software (OpenSSL), zuständig für verschlüsselte Verbindungen, hat seit etwa 2 Jahren eine riesige Lücke, die den Zugriff auf Daten von anderen Nutzern erlaubt. Inzwischen ist die Lücke zwar gestopft und die meisten Nutzer sollten ihre Passwörter geändert haben, aber das Vertrauen ist nachhaltig geschädigt. Und damit ist nicht nur das Vertrauen in die offene Software gemeint, die viele der zentralen Funktionen des Internets ermöglicht, oder die ganzen Webdienste, die darauf setzen. Wenig überraschend kam auch sofort der Vorwurf auf, dass die NSA den Bug seit fast 2 Jahren ausnutzt. Die NSA hat dies sofort bestritten, aber um ihre Glaubwürdigkeit ist es nach den Enthüllungen von Edward Snowden nicht besonders gut bestellt. Fakt ist zudem, dass der Bug offensichtlich anderen im Netz bereits bekannt war und aktiv ausgenutzt wurde – vermutlich von einem Geheimdienst. Zum ersten mal hat die weitere Öffentlichkeit im Netz es also mit einem derart weitreichenden Bug zu tun. Was folgt politisch daraus?

Um diese Frage anzugehen, macht es Sinn, den Blick etwas zu erweitern: Im Grunde geht es um zwei Dinge: Erstens geht es um die Frage des Umgangs staatlicher Organe mit Zero Day Exploits, also dem Ausnutzen von Lücken in Software, die dem Hersteller noch nicht bekannt sind. Solche Lücken können folglich auch mit der aktuellsten Software ausgenutzt werden, was sie wiederum für Geheimdienste und Strafverfolgung attraktiv macht. Gleichzeitig besteht immer die Chance, dass mehr als eine Partei die Lücke entdeckt und ebenso ausnutzt – einen sicherheitsrelevanten Bug nicht dem jeweiligen Entwickler oder Hersteller zu melden macht also alle Nutzer der betroffenen Software unsicher. Wenn es sich dabei, wie im Fall des Heartbleed Bugs, um einen großen Teil der Webnutzer handelt, ist das umso dramatischer. Zweitens folgt daraus ein erheblicher Schaden für Vertrauen sowohl in die staatlichen Organe (auch von anderen Staaten) als auch das Internet an sich.

Im Rahmen der Berichterstattung rund um den Heartbleed Bug wurde bekannt, dass Präsident Obama bereits im Januar eine Direktive erlassen hatte, die den staatlichen Umgang mit Zero Days regelt. Demnach sollen grobe Fehler in für die Sicherheit des Internets relevanter Software öffentlich

gemacht werden. Das ist grundsätzlich gut, denn bisher gab es gar keine entsprechende Regelung, und es ist bekannt dass amerikanische Sicherheitsbehörden, allen voran die NSA, auf einem ganzen Haufen derartiger ungepatchter Exploits sitzen. Dies sollte also erst einmal unser Vertrauen in die amerikanischen Behörden und die Sicherheit des Netzes an sich stärken.

Leider beinhaltet die Direktive auch eine Ausnahme: Die Veröffentlichung kann verzögert werden, wenn es einen klaren Bedarf der nationalen Sicherheit oder bei der Strafverfolgung gibt. Diese Ausnahme ist ziemlich umfangreich, und es steht zu befürchten, dass sie in den meisten Fällen ausgenutzt werden wird. Dafür spricht auch, dass die Geheimdienstcommunity in den USA sich an der Direktive immens stößt – sie hält sie für einseitiges Abrüsten. In Anbetracht der Tatsache, dass andere Länder wie China ihrerseits die Cyberspionage ausbauen und ebenfalls auf der Suche nach Zero Days sind, mag diese Position aus Sicht der amerikanischen Behörden sogar nachvollziehbar sein. Der Rest der Internetnutzer profitiert von diesem Wettrüsten aber nicht.



Hoffentlich kommt es nicht wirklich soweit, Grumpy Cat. (Quelle: Frerk Meyer auf Flickr)

Problematisch ist außerdem, dass nicht klar ist, ob die Direktive für schon gefundene Lücken gilt, oder nur für neue. Die amerikanischen Behörden verfügen aber bereits über eine ganze Reihe von diesen Lücken, die noch nicht gestopft sind, und können diese aktiv ausnutzen – wie etwa im Fall von Stuxnet geschehen. Und selbst wenn im spezifischen Fall von Heartbleed die NSA tatsächlich den Bug nicht ausgenutzt hat, ist dank Snowden bekannt, dass sie an der Unterminierung von OpenSSL arbeiteten.

Das Ergebnis könnte fatal für die Zukunft des Internets sein: Das Vertrauen in die Infrastruktur als solche steht in Frage. Dass Kriminelle, die auf derartige Lücken stoßen, diese nicht veröffentlichen, mag einleuchten. Dass Staaten aber die Sicherheit ihrer eigenen Bürger aufs Spiel setzen ist schwerer zu vermitteln. Noch unangenehmer ist aber, dass andere, auch

BELIEBT KOMMENTARE NEU

Hell yeah, it's Political Science! Wissenschaftliche Podcasts

Das Internet darf ein cyberfreier Raum sein

Deutschlands Irak-Politik – Verantwortung nach außen, Intransparenz nach innen.

Wir haben Geburtstag!

„Mit Sicherheit nicht!“ Sexuelle Gewalt als politisches Mittel

KATEGORIEN

Außenpolitik (59)
Bürgerkriege (16)
Cyber Security (40)
Demokratisierung (9)
Drohnen (15)
Humanitäre Interventionen (15)
Innere Sicherheit (24)
Interviews (10)
Katastrophen (4)
Konferenz (20)
Militär (27)
Pandemien (2)
Podcast (7)
Popkultur (20)
Sanktionen (8)
Security Culture (13)

verbündete, Staaten die eigene Sicherheit im Netz gefährden. Damit ist nicht einmal gemeint, dass man direkt im Ziel ausländischer Geheimdienste landet. Vielmehr ist das Problem, dass einem kleine Kreis bekannte Lücken nicht gestopft werden und diese daher potenziell von Dritten ausgenutzt werden können. Das Vertrauen in das Internet als transnationales Konstrukt verschwindet, denn seine grenzüberschreitende Natur sorgt gerade dafür, dass Staaten in ihrem Drang sich gegenseitig auszuspionieren die Sicherheit aller gefährden – letztlich sogar die eigene.

Da sich die meisten Bürger aber ein Leben ohne das Internet kaum mehr vorstellen können, könnte damit der Ruf nach einem vermeintlich sicheren, lokalen Netz laut werden, das wenigstens nicht direkt von ausländischen Diensten unsicher gemacht werden kann. Man möchte schließlich seine Daten und die kritische Infrastruktur schützen. Das Ergebnis wäre die zunehmende Balkanisierung des Netzes und, im Falle Deutschlands, die Rückkehr der Idee des Schlandnetzes. Es liegt nun an den Regierungen, international genau gegen diese Gefahr vorzugehen. Denn das Internet als Ansammlung von nationalen, fein säuberlich abgetrennten Netzen, wäre nicht nur netzpolitisch und demokratisch eine Katastrophe, sondern auch ökonomisch. Mögliche Initiativen dafür könnten etwa im Rahmen der UN oder von ICANN stattfinden. Aber dabei muss schnell und vor allem grenzübergreifend gehandelt werden – denn jede staatlich ausgenutzte Lücke erodiert das Vertrauen weiter.

Tags: Cyber Security, Cyber Spionage, cybersicherheit, Hearbleed, ICANN, nsa, Sicherheit, USA, Vertrauen

« Koordination in der europäischen Netzpolitik, die zweite: Vorratsdatenspeicherung

Medienevent Klimawandel – Affenbabys und der IPCC-Bericht »

5 Kommentare zu “Blutende Herzen und gebrochenes Vertrauen: Was folgt aus dem Heartbleed Bug?”

seditioni | 15. Apr. 2014 um 13:52 | **#1**

Du schreibst, es könne der Ruf nach einem nationalen Internet laut werden. Von wem?
Wie wir bei den Snowden-Enthüllungen gesehen haben, kommt dieser Ruf definitiv nicht von den Bürgerinnen und Bürgern. Die meisten von ihnen scheinen sich nämlich nicht betroffen zu fühlen, was bei Heartbleed nicht anders sein wird.
Auch die deutsche Politik wurde in den post-Snowden-Monaten nicht gerade aktiver was den Datenschutz angeht. Wenn man sich schon kaum traut, die USA wegen dem NSA-Skandal angemessen zu kritisieren, wieso sollte dann jetzt jemand ernsthaft ein Schlandnet wollen? Ich sehe die Gefahr eines nationalen Netzes nicht – wo siehst du sie

Sicherheits-Kommunikation (14)
Sicherheitskultur (204)
Sozialwissenschaft Online (57)
Stellenangebote (42)
Strategie (10)
Terrorismus (14)
Theorie (2)
Umwelt (1)
Versicherheitlichung (21)
Visualisierung (5)
Whistleblowing (8)
WikiLeaks (17)
WMD (10)
Zivilgesellschaft (48)

BLOGROLL

Arbeitskreis soziale Bewegungen
Augen geradaus
Dan Drezner
Dart-Throwing Chimp
David Campbell
de.hypotheses.org
Demokratieforschung Göttingen
Duck Of Minerva
Future and Politics
Hylaean Flow
Internet und Politik
IR Blog
Just Security Blog
justsecurity.org
Killer Apps
Kings Of War
netzpolitik.org

genau?

ANTWORTEN

Martin | 15. Apr. 2014 um 14:01 | **#2**

Der Ruf nach einem nationalen Internet ist nie so richtig verstummt, er ist nur in Deutschland nicht mehr besonders laut. Derartige Rufe verorte ich eher in Ländern wie China oder Russland – der Unterschied ist, wie überzeugend die Argumente im jeweiligen Kontext sind. Im Prinzip war die Zero Day Problematik auch schon vorher bekannt, Heartbleed hat sie nur auf die Agenda gesetzt weil der Bug so viele betroffen hat.
Dass Bürgerinnen und Bürger dort einstimmen halte ich auch eher für unwahrscheinlich. Für wahrscheinlicher halte ich da schon Experten und Vertreter staatlicher Institutionen. In dem Zusammenhang sollte man sehen, dass die USA im letzten Monat langsam angefangen haben, die Kontrolle über ICANN abzugeben. Das ist zwar grundsätzlich gut, erlaubt es Ländern wie Russland und China aber auch, nicht mehr nur in der ITU ihre Agenda voranzutreiben.
Im Zuge des NSA Skandals und der Direktive von Obama zusammen mit einem dramatischen Bug, der der weiteren Öffentlichkeit grob vor Augen hält, dass es dort Probleme gibt, sehe ich durchaus das Potenzial für eine stärkere Bewegung in Richtung nationaler Netze. Momentan sind einfach die Kontextbedingungen für derartige Bestrebungen recht gut.

ANTWORTEN

seditioni | 22. Apr. 2014 um 16:34 | **#3**

Dazu http://www.collaboratory.de/w/Der_Digitale_Wandel_-_Magazin_f%C3%BCr_Internet_und_Gesellschaft, Seite 15: “Nationalgrenzen im Internet provozieren? Ein abschreckender Gedanke...” von Leslie Daigle.

ANTWORTEN

benkamis | 15. Apr. 2014 um 16:45 | **#4**

2 Sachen:
1. Für Chromenutzer gibt es eine Extension, die bei betroffenen Seiten warnt. Hier klicken. Es gibt auch eine Liste, auf die man schauen kann: http://mashable.com/2014/04/09/heartbleed-bug-websites-affected/ Gern geschehen.
2. OpenSSL ist Opensource, betrieben von einem kleinen Kader begeisterter Menschen und vielen freiwilligen Helfer. Wer ist hier der Hersteller? Wie schwer für die NSA wäre es, eigene Mitarbeiter in solchen Projekten einzubringen und Lücken bei der Entstehung neuer Platformen einzubauen? Bei Zero-day exploits geht man idR von unbekannten Problemen und Bugs aus, aber -X day exploits sind auch denkbar, oder?
Nur weil du paranoid bist, heißt es nicht, dass sie dir nicht hinterher sind.

ANTWORTEN

shabka.org
Terrorismus in Deutschland
theorieblog.de
Verfassungsblog
Vom Bohren harter Bretter
whistleblower-net.de

ARCHIV

Wähle den Monat

Martin | 15. Apr. 2014 um 16:48 | **#5**

Wie schwer es wäre, Leute bei einem derartigen Projekt einzuschleusen? Im Fall von OpenSSL nicht besonders. Die Codebase gilt als ziemlich schwer lesbar und das Projekt ist konstant unterfinanziert und hat nicht genug Programmierer, die dort aktiv über einen längeren Zeitraum Arbeit reinstecken können (da sie ja auch nicht dafür bezahlt werden). Was nicht zwingend heißt, dass genau das geschehen ist. Genauso kann es sich wirklich um einen Fehler handeln, der aus Versehen gemacht wurde und dann einfach entdeckt und nur nicht zwingend sofort der Öffentlichkeit und vor allem dem OpenSSL Projekt mitgeteilt wurde.

ANTWORTEN

Einen Kommentar hinterlassen

Name

Email

Webseite

Kommentar

Geben Sie den Text ein.

reCAPTCHA

Bestätigen

Datenschutz - Nutzungsbedingungen

Kommentar senden

☑ Benachrichtige mich über nachfolgende Kommentare per E-Mail.