Heartbleed in Österreich: 100 Tage danach

6. 8. 2014

Zusammenfassung

Der „Heartbleed“ – Bug in OpenSSL hat viele Systeme in Österreich betroffen. Ein großer Teil der Systemverwalter hat prompt reagiert und ihre Server aktualisiert. Mit dem Start der domainbasierten Messungen von CERT.at am 19. April 2014 waren unter der Top-level Domain Österreichs (.at) 1850 Webserver (https, TCP Port 443) und 1000 Mailserver (smtp, TCP Port 25) verwundbar. Bis Ende Juli 2014 hat sich die Zahl auf 740 Webserver und 520 Mailserver rund halbiert. Bezogen auf alle Web- oder Mailserver sind das 0,59 bzw. 0,73 Prozent. Von den untersuchten Servern die SSL/TLS unterstützen, sind das noch 1,31% (https) bzw. 1,28% (smtp).

Ende Juli sind noch 2030 .at - Domains bei https, und 1740 bei smtp für Heartbleed anfällig.

Die Zahlen zeigen, dass die Kombination aus einem nationalen CERT, das Informationen über Sicherheitsprobleme einholt und weitergibt, und einer gut funktionierenden Abuse-Abteilung bei ISPs, einen deutlichen, messbaren und positiven Effekt auf die Netzwerksicherheit hat.

Als Seiteneffekt dieser Messungen ergaben sich auch Werte, wie weit unter .at der Einsatz von verschlüsselter Datenübertragung angeboten wird. So etwa erlauben 79% der .at – Domains die Übermittlung von Email mittels SMTP/STARTTLS.

Autor:

Otmar Lendl <lendl@cert.at>

Feedback:

Kommentare oder Rückfragen bitte an team@cert.at.

Inhalt

Hintergrund

Am 7. April 2014 wurde ein schwerer Fehler in OpenSSL[1] bekannt. OpenSSL ist eine frei erhältliche Bibliothek für kryptografische Algorithmen und Protokolle. Unter anderem wird OpenSSL zur Absicherung von Netzwerkverbindungen auf Basis von SSL/TLS[2] benutzt. Insbesondere die Kombination mit dem Webserver Apache ist auf Linux Systemen sehr verbreitet.

Die CERT.at Warnung[3] vom 8. April 2014 hat das Thema so zusammengefasst:

> **Beschreibung**
>
> Durch einen Fehler in OpenSSL können Angreifer Teile des Hauptspeichers eines betroffenen Systems (in Schritten von 64kB) lesen. Dadurch ist es den Angreifern möglich, an diverse Informationen, unter Umständen inklusive der "Private" Keys/X.509 Zertifikate, zu gelangen.
>
> Eine ausführliche Beschreibung des Problems findet sich auf http://heartbleed.com/ (englisch).
>
> Eintrag in der CVE-Datenbank: CVE-2014-0160.
>
> **Auswirkungen**
>
> Da davon auszugehen ist, dass Angreifer über die Private Keys von mit verwundbaren OpenSSL-Versionen gesicherten Services verfügen, sind prinzipiell alle über solche Services übermittelten Informationen als kompromittiert zu betrachten.
>
> Falls die Services mit "Perfect Forward Secrecy" konfiguriert sind, können Angreifer allerdings nicht Informationen aus in der Vergangenheit mitprotokollierten Sitzungen entschlüsseln. Aktuell übertragene Informationen sind trotzdem betroffen.
>
> **Betroffene Systeme**
>
> Der Fehler betrifft alle OpenSSL Versionen von 1.0.1 bis inklusive 1.0.1f, die erste verwundbare Version 1.0.1 wurde am 14. März 2012 veröffentlicht.

Da es sich um einen „einfachen“ Programmierfehler handelte, wurde eine korrigierte Version von OpenSSL mit Bekanntgabe des Fehlers veröffentlicht. Sowohl für Open Source Betriebssysteme / Distributionen als auch für kommerzielle Produkte, die auf OpenSSL aufbauen, waren bald Updates erhältlich, die den Fehler behoben haben.

Über den „Heartbleed-Bug“ wurde nicht nur in der Fachpresse diskutiert, sondern dieser war auch ein Thema in den allgemeinen Medien.

[1] https://www.openssl.org/
[2] Secure Socket Layer / Transport Layer Security
[3] https://www.cert.at/warnings/all/20140408.html

Aktivitäten von CERT.at

Der Heartbleed-Bug war ein typischer Fall für CERT.at als nationales CERT, da hier mehrere der klassischen CERT-Aufgaben zu erfüllen waren:

- Veröffentlichung einer offiziellen Warnung
- Pressearbeit: CERT.at gab viele Interviews, in denen es meist um folgende Fragen ging:
    - Wie schlimm ist das Problem wirklich?
    - Wie sollen sich Serverbetreiber verhalten?
    - Was kann der Bürger machen?
- Sammlung von weiteren Informationen, Bereitstellung eines konsolidierten Status des Problems[4]
- Einholen von Informationen, welche Systeme in Österreich betroffenen sind
    - Externe Quellen
    - Eigene Nachforschungen
- Laufendes Informieren der Betroffenen
- Messen des Fortschritts der Bereinigung

Messungen

Der Heartbleed-Bug betrifft die Behandlung von „Heartbeat“ Nachrichten im SSL/TLS Protokoll. Ob ein Server anfällig ist, lässt sich sehr einfach testen – vorausgesetzt, dass man eine SSL/TLS-Verbindung zu diesem Server aufbauen kann. Es wurden schon sehr früh Testprogramme veröffentlicht, die genau dieses machen: Eine TLS Verbindung aufbauen, den Fehler auszulösen versuchen und zu testen, ob die Reaktion des Servers eine Verwundbarkeit vermuten lässt. Diese Testprogramme wurden noch über Tage hinweg optimiert, um wirklich alle Fälle abzudecken.

Scans nach IP-Adressen

Damit war es dann technisch relativ einfach, alle im Internet erreichbaren Server auf Heartbleed zu testen. Techniker, die eingehende Tests protokollierten, haben festgestellt, dass global von vielen Seiten alle IPv4-Adressen gescannt wurden.

Die vier Milliarden IP-Adressen von IP Version 4 sind mit aktueller Software und guter Netzanbindung innerhalb von wenigen Minuten durchsuchbar. Bei IP Version 6 ist das auf Grund des deutlich größeren Adressraumes nicht so einfach möglich.

Da die Zuordnung von IP-Adressen auf Staaten (mit Unschärfe) bekannt und öffentlich ist, kann man auch leicht einen Scan gezielt auf Heartbleed-verwundbare Server in einzelnen Staaten durchführen.

Domain-basiert Scans

Eine andere Variante ist es, nicht mit IP-Adressen zu starten, sondern mit Listen von Domains. Mittels ganz normaler DNS[5]-Lookups ergeben sich daraus die IP-Adressen der Server, die Dienste für diese Domains anbieten. Diese kann man dann gezielt auf den Heartbleed-Bug testen.

[4] https://cert.at/warnings/specials/20140411.html
[5] https://de.wikipedia.org/wiki/Domain_Name_System

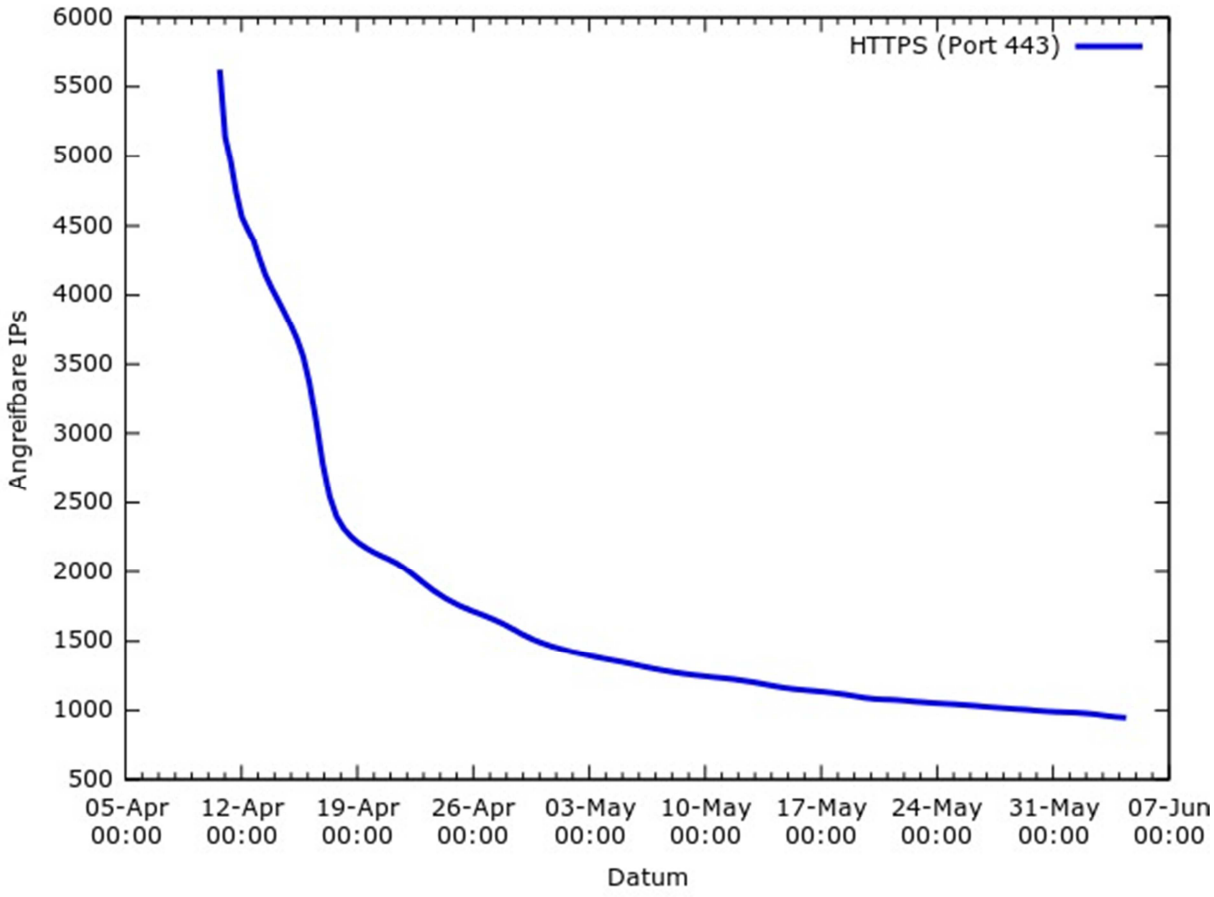
Das hat primär den Vorteil, dass auf diese Weise deutlich weniger Tests ausgeführt werden müssen. Das spart Aufwand auf der Seite des Testers, und ist auch auf der anderen Seite angenehmer, da unnötige Anfragen an unbenutzte oder reine Client-IP-Adressen vermieden werden.

Andererseits kann es so kein komplettes Inventar geben, da nicht alle Hostnamen, unter denen Dienste angeboten werden, bekannt sind. Auch werden so die Server in Österreich nicht erfasst, die für keine .at – Domain zuständig sind.

Ergebnisse der Scans nach Netzblöcken

In den ersten Tagen wurden von einigen Seiten aus IP-basierte Scans durchgeführt. Speziell für Österreich waren das die SBA Research gGmbh und CERT.at.

Die Zahlen von SBA Research werden auf http://www.sba-research.org/2014/04/15/heartbleed-bedrohungslage-in-osterreich/ veröffentlicht. Bei der ersten Messung am 10. April waren noch über 5000 IP-Adressen anfällig, bis zum Juni ist die Zahl dann unter 1000 gefallen. Am 28. Juli waren noch 663 IP-Adressen übrig. Die folgende Grafik (Quelle: SBA Research gGmbH) gibt die Entwicklung über die Zeit wieder:



Auch CERT.at hat initial die Österreich zugeordneten IP-Adressen gescannt (ab dem 9. April, nachdem schon global Scans beobachtet wurden). Basierend auf diesen Ergebnissen gingen ab 15. April Warnungen an die Netzbetreiber mit genauen Angaben, welche IP-Adressen aus deren Netzen für Heartbleed auf TCP-Port 443 (https) anfällig waren.

Ergebnisse der domain-basierten Scans

Da CERT.at eine Initiative von nic.at (der ccTLD Registry von .at) ist, war als Datenbasis die komplette Liste aller Domains unter .at verfügbar. Aufgrund früherer Untersuchungen war schon ein Framework zur Erhebung der SSL/TLS Fähigkeiten der Server, die .at-Domains betreuen, vorhanden. Dieses wurde um die Erkennung von Heartbleed erweitert und liefert seit dem 17. April Daten. Ab dem 18. April wurden zuerst die Betreuer der (wenigen) noch verwundbaren Server zu gv.at – Domains[6] informiert, ab dem 13. Mai wurde dann diese Datenbasis für die generischen Warnungen von CERT.at herangezogen.

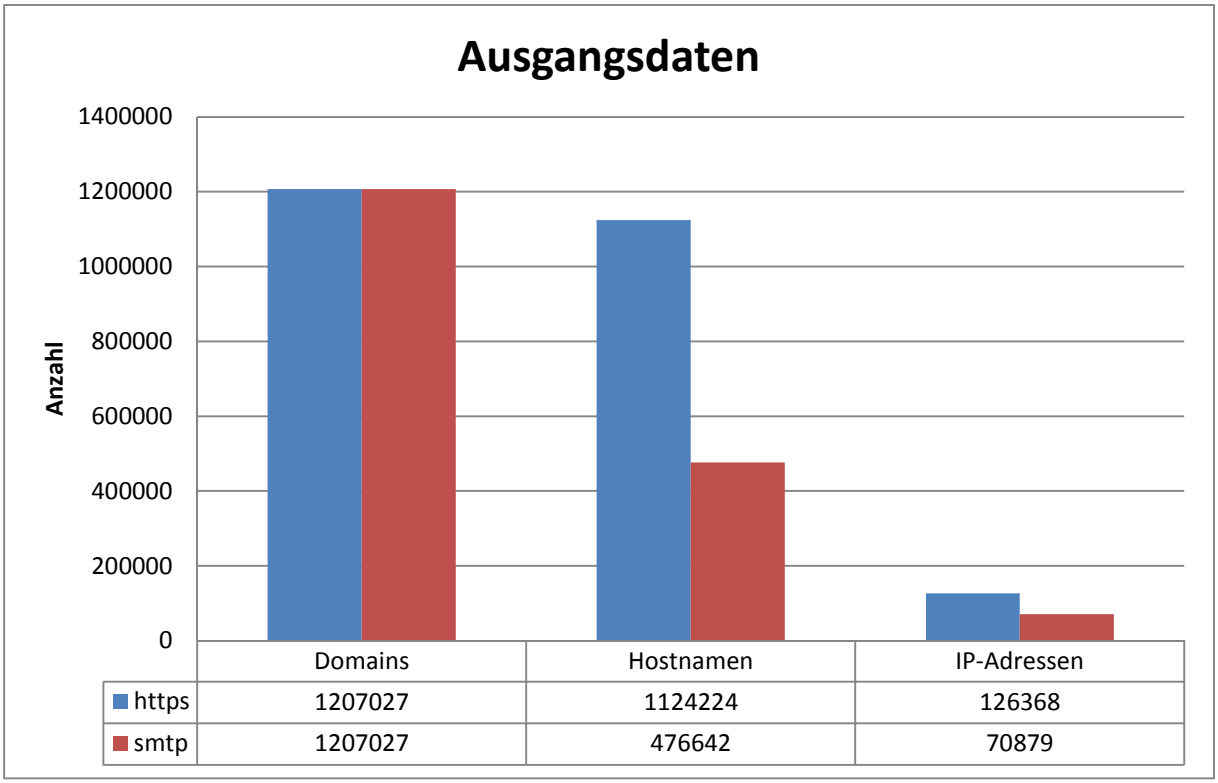
Betrachtet wurde sowohl https (TCP Port 443) als auch smtp (TCP Port 25, nach STARTTLS).

Datenbasis

Der Ausgangpunkt war eine Liste der rund 1,2 Millionen Domains unter .at, .gv.at, or.at und co.at. Von diesen wurden Hostnamen abgeleitet, die Dienste für diese Domains anbieten.

Für http wurde im DNS nach A – Records zur Domain selber und den Namen „www“ und „secure“ unter der Domain gesucht. Zum Beispiel: zu „nic.at“ waren das „nic.at“, „www.nic.at“ und „secure.nic.at“. Die A Records im DNS haben dann die IP-Adressen der entsprechenden Server ergeben. Hostnamen unter einer Domain, die auf die gleiche IP-Adresse verwiesen haben, wurden als redundant herausgenommen.

Im Falle von smtp wurden die zuständigen Hostnamen aus den MX – Records zur Domain genommen. Die Übersetzung auf IP-Adressen basierte wieder auf den A – Records im DNS.



	Domains	Hostnamen	IP-Adressen
https	1207027	1124224	126368
smtp	1207027	476642	70879

Es ist klar ersichtlich, dass der durchschnittliche Server für mehr als eine Domain zuständig ist.

[6] Für Systeme der öffentlichen Verwaltung agiert das Team von CERT.at unter der Fahne des GovCERT Austria.

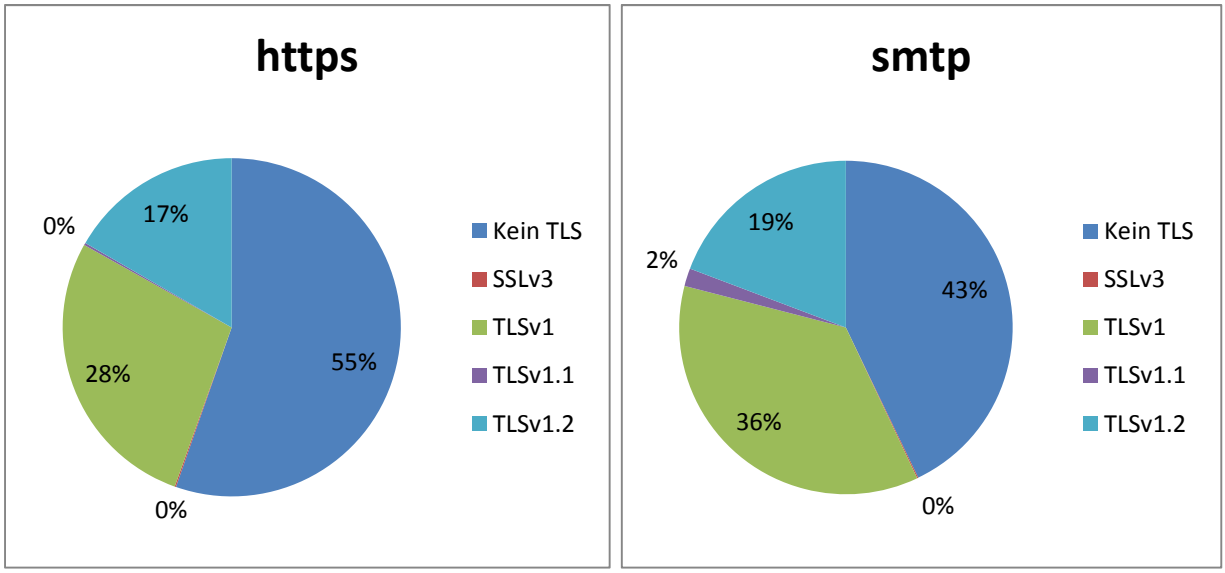
Für eine Erhebung des Status zu Heartbleed von 1,2 Millionen Domains ist es daher nicht nötig, auch eine Million Server zu testen: 126.368 plus 70.879, also rund 200.000 IP-Adressen/Ports sind ausreichend.

Im Folgenden können die Ergebnisse immer auf zwei Arten dargestellt werden: basierend auf Domains oder basierend auf IP-Adressen.

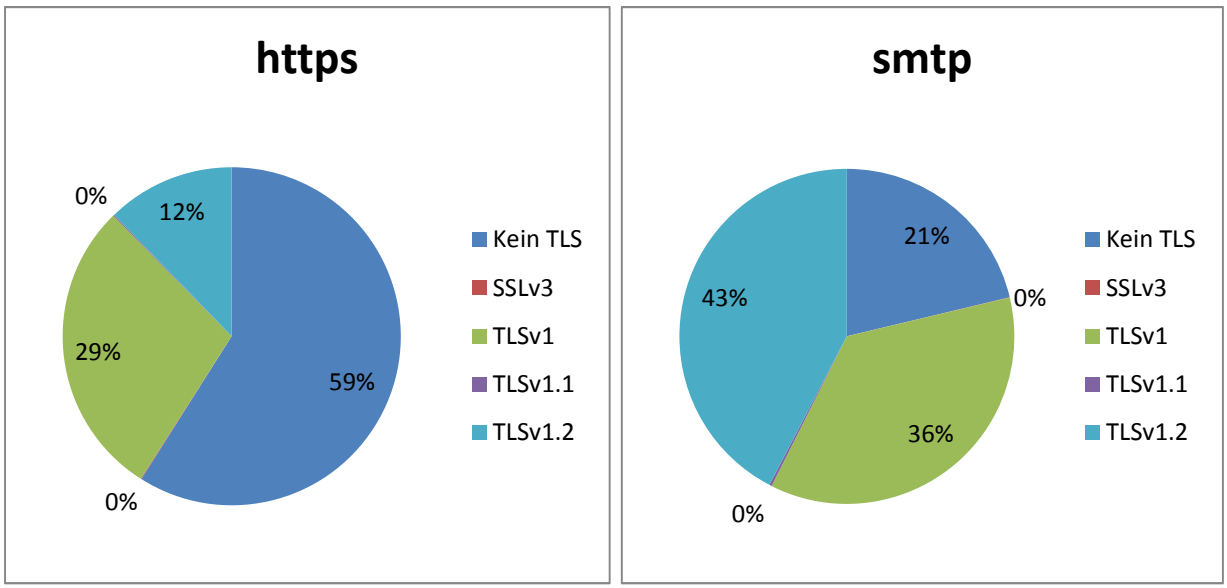
TLS Status

Nicht alle Domains bieten Webserver und Mail-Transfer mit TLS an: ein erster Test war daher, welche der rund 200.000 Dienste (https und smtp) verschlüsselten Datentransfer unterstützen.

Gerechnet in IP-Adressen



Gerechnet in Domains



Zur Interpretation dieser Grafiken sind folgende Punkte wichtig:

- Dass die IP-Adresse des Webservers zu www.example.at auch auf https antwortet, heißt nicht notwendigerweise, dass auch https://www.example.at/ wie erwartet funktioniert. Virtual Hosts (d.h. Webserver zu mehreren Domains auf einer IP-Adresse) für https waren

lange fast nicht machbar, erst mit SNI[7] wird das möglich. In der Praxis ist das aber noch kaum angekommen.

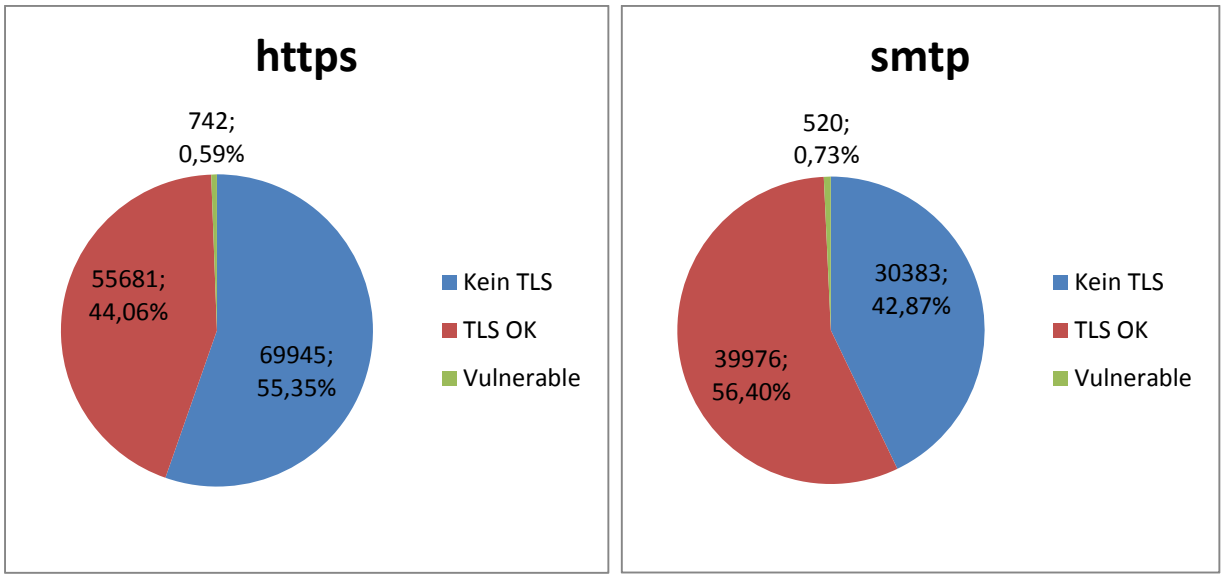
- Der große Unterschied im Anteil der TLS-Unterstützung für smtp zwischen den beiden Graphen deutet darauf hin, dass Mailserver, die viele Domains bedienen, tendenziell eher TLS unterstützen, als kleine Mailserver.
- Gegenstand dieser Untersuchung war nur, ob der Server TLS spricht, nicht aber, ob er auch ein gültiges X.509 Zertifikat von einer anerkannten Certification Authority vorweisen kann.

Da die Server ohne TLS-Unterstützung für Heartbleed nicht relevant sind, sind im weiteren nur noch rund 56.000 Webserver und 40.000 Mailserver zu betrachten.

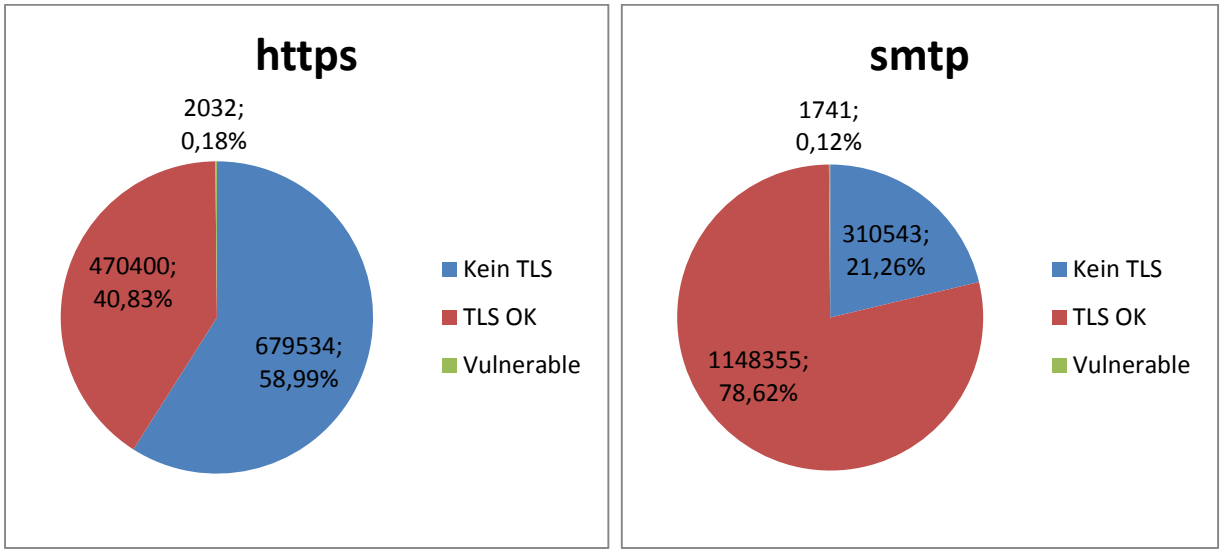
Heartbleed Status

Der Scan am 31. Juli 2014 ergab folgendes Ergebnis:

Gerechnet in IP-Adressen



Gerechnet in Domains



[7] https://en.wikipedia.org/wiki/Server_Name_Indication

Betrachtet man nur die Server, die TLS unterstützen, so sind Ende Juli noch 1,31% der https und 1,28% der smtp Server (gemessen nach IP-Adressen) für Heartbleed anfällig.

Diese Messung behandelt nur den aktuellen Stand der TLS-Implementation auf diesen Servern. Ob die Betreuer eines vormals betroffenen Servers – wie von vielen empfohlen – auch den privaten Schlüssel des Servers ausgetauscht und das alte Zertifikat widerrufen haben, wird hier nicht erfasst.

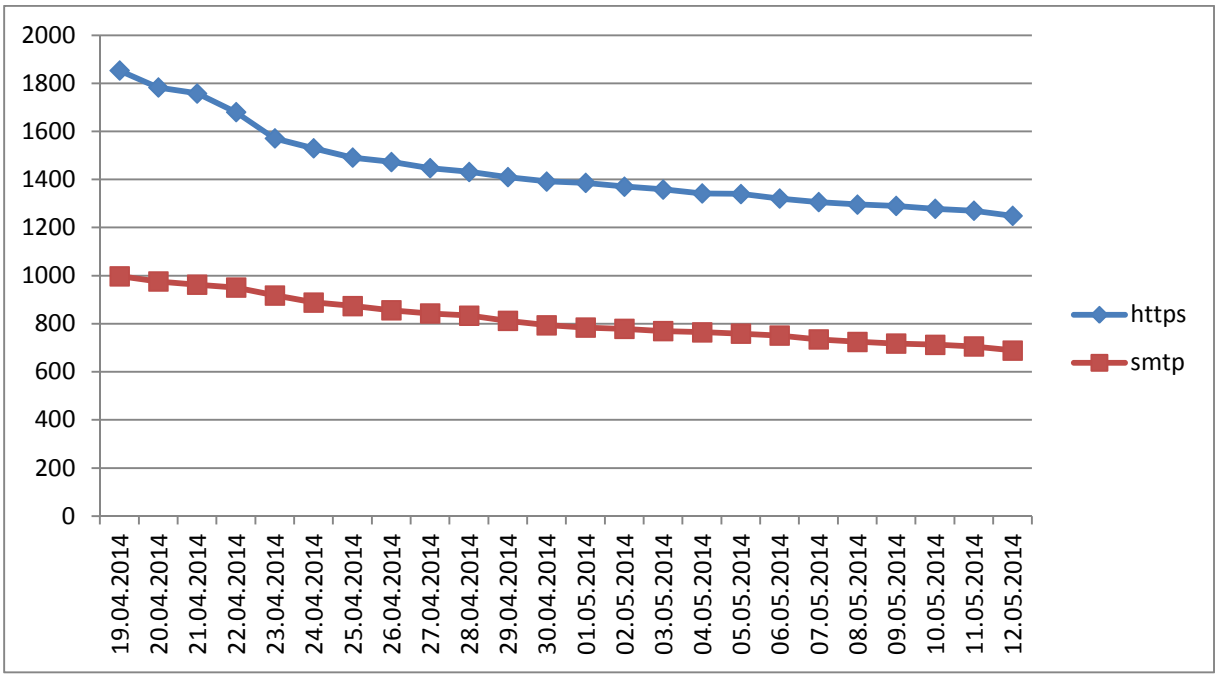
Entwicklung seit April

Typischerweise werden gut gewartete Server schnell aktualisiert: Kurz nach dem Bekanntwerden eines Fehlern werden daher sehr schnell viele Updates durchgeführt. Danach wird es immer langsamer: manche Betreiber warten ihre Server in einem Monatszyklus, andere überhaupt nur sehr sporadisch. Am Ende bleiben die Server übrig, um die sich schlicht gar niemand kümmert. Diese werden erst dann gefixt, wenn es entweder einen externen Druck gibt, oder die natürliche Lebensdauer der Hardware einen Ersatz (hoffentlich mit aktueller Software) nötig macht.

In der Kurve der SBA Research (siehe Seite 4) kann man den initial starken Rückgang der betroffenen System noch gut sehen. Da die Domain-basierten Messungen erst ab 19. April konsistente Werte geliefert haben, ist dort nur noch der flache Teil der Kurve sichtbar.

Initiale Messungen

Die Messwerte ergaben folgende Kurve für die ersten Wochen (gemessen nach IP-Adressen):



Initial kann man noch eine stärkere Verbesserung sehen, dann flacht die Kurve sehr ab.

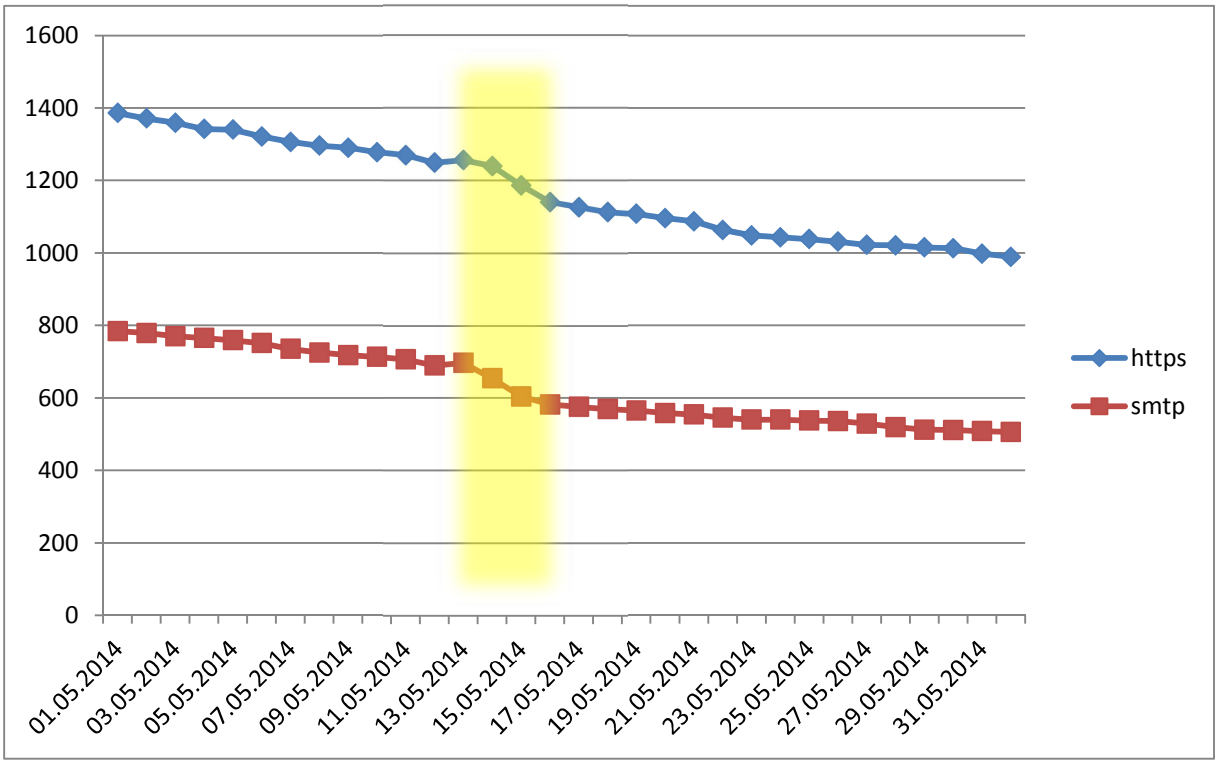
Zwei Ereignisse haben die Kurve dann später beeinflusst:

Effekt der CERT.at Meldungen an Netzbetreiber

Die ersten Mails von CERT.at an die Betreiber beruhten auf den IP-basierten Scans des österreichischen Internets auf Port 443/https. Am 13. Mai (für smtp, am 14. auch für https) stellte CERT.at die Grundlage der Meldungen auf die domainbasierten Scan um. Damit wurden auch Server außerhalb Österreichs erfasst, die für .at Domains zuständig sind. Gerade die in Deutschland

gehosteten .at - Domains machen einen erheblichen Anteil an der Gesamtzahl aus. Weiters wurden damit zum ersten Male auch die Betreiber von verwundbaren Mailservern angeschrieben. Diese Meldungen enthielten nicht nur die Betroffenen IP-Adressen, sondern auch einige der Domains, für die der Server zuständig ist.

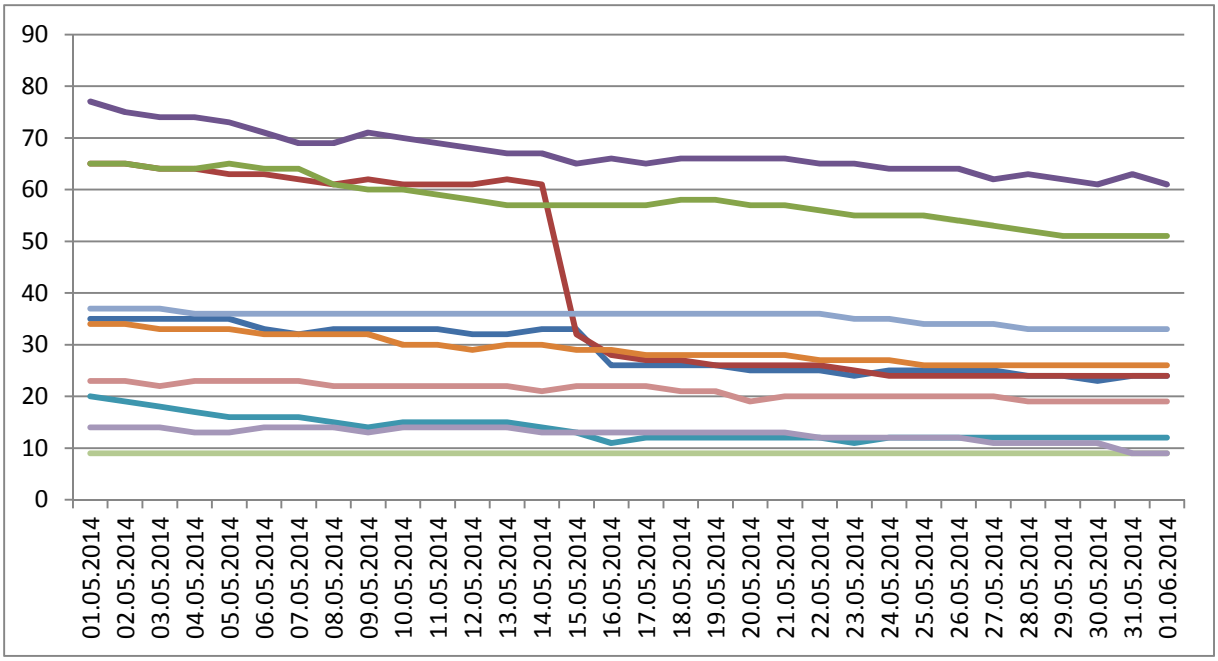
Da für smtp seit 19. April gemessen wurde, aber erst ab 13. Mai Mails versendet wurden, kann man den Effekt der Arbeit von CERT.at anhand der Entwicklung rund um den 13. Mai beurteilen:



Man kann eine klare Stufe in der Zahl der betroffenen IP-Adressen erkennen.

CERT.at hat in diesem Fall nicht den Domaineigentümer, sondern den Netzbetreiber (genauer: das Abuse-Team des Autonomen Systems, zu dem die IP-Adresse gehört) angeschrieben. Da nicht alle ISPs gleich effektiv auf solche Meldungen reagieren war es naheliegend, diese Kurve auf die einzelnen ISPs aufzuteilen.

Nimmt man die zehn ISPs, bei denen die meisten .at Domains gehostet werden, so ergibt sich folgendes Bild in diesem Zeitraum:



Die Verbesserung rund um den 14. Mai konzentriert sich auf nur zwei der Top 10 ISPs. Wir können hier keinen Namen nennen, aber der ISP, der innerhalb von zwei Tagen die Zahl seiner verwundbaren Server halbiert hat, ist bekannt dafür, dass er Meldungen an seine Abuse-Abteilung mit Nachdruck an seine Kunden weitergibt.

Von anderen ISPs haben wir auf Nachfrage erfahren, dass die CERT.at Meldungen zu Heartbleed nicht (sofort) weitergegeben wurden. Daher ist verständlich, dass es keinen positiven Effekt auf die Statistik dieser ISPs gegeben hat.

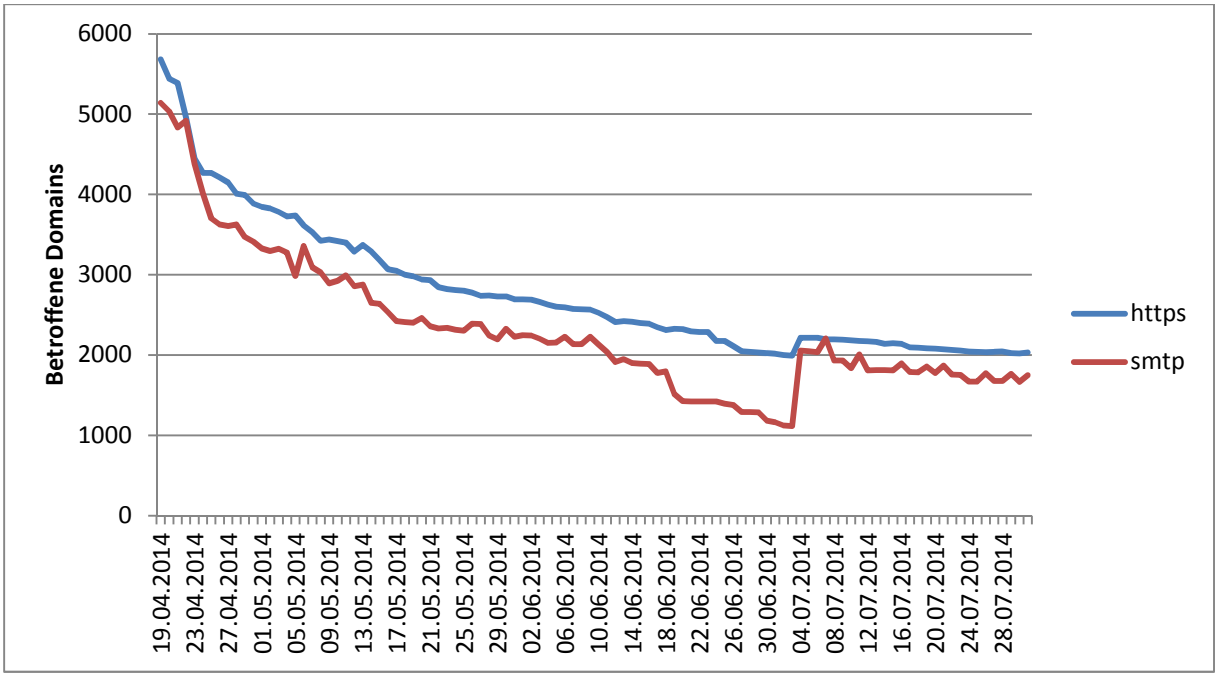
Update der Datenbasis

Die Übersetzung von Domains auf Hostnamen und weiter auf IP-Adressen wurde nur einmal initial am 17. April durchgeführt. Alle Tests der darauf folgenden Wochen bezogen sich auf die hier ermittelten IP-Adressen.

Das DNS ist aber nicht statisch: Webserver werden umgesiedelt, Domains wandern mit ihren MX - Records zu einen anderen Mailprovider und die Domainliste selber ist auch nicht statisch.

Wir haben daher am 2. Juni 2014 die Datenbasis der Scans aktualisiert. Dabei wurde auch mit deutlich großzügigeren Timeouts gearbeitet. In Summe hat sich damit die Menge der ab 3. Juni getesteten Server deutlich verändert. Damit kam es auch zu einem Anstieg der Zahl der als verwundbar eingestuften Systeme:

Aus dem Blickwinkel „betroffene Domains“ stellt sich die Kurve so dar:



Die Datenbank, in denen die Scanergebnisse verwaltet werden, implementiert nur eine statische Zuordnung von Domains auf IP-Adressen, diese Graphik basiert auf den DNS-Daten vom 2. Juni. Die Zahlen sind daher nicht exakt.

Basierend auf diesen Graphen ist nicht klar feststellbar, in wie weit die laufende, langsame Verbesserung nicht auch ein Effekt der DNS-Änderungen ist, die das Scan-System nicht laufend mitberücksichtigt.

Meldungen von CERT.at an ISPs

In einigen Fällen hat CERT.at (bzw. GovCERT Austria) direkt die Betreiber von relevanten Servern angeschrieben, die meisten Meldungen gingen aber – wie oben erwähnt – an die Abuse-Teams der ISPs.

Um diese Teams aber nicht mit Daten zu überladen, unterdrückt CERT.at Wiederholungen von Meldungen zu dem gleichen Vorfall innerhalb einer gewissen Zeit. Für Heartbleed wurde eine Woche als Frist zwischen zwei Meldungen zur gleichen IP-Adresse konfiguriert.

CERT.at hat bis zum 6. August in Summe 4366 Meldungen an 694 verschiedene ISPs (genauer: Autonome Systeme) versendet. Davon betrafen 3121 https und 1245 smtp. Über die Zeit ergibt sich folgende Grafik: