


ID: 01

Group: 

E-Mail sent: 06-03-2024, 12:50

Response to: first email / reminder

Date: 06-03-2024, 13:04

[deleted due to data protection reasons, person explicitly opted out]

*# Response 06 (2024-03-07, 10:50)*

Hallo,

keine Sorge - Ihre Emails werden in keiner Forschungsarbeit auftauchen.

Mit freundlichen Grüßen



ID: 02

Group: [REDACTED]

E-Mail sent: 06-03-2024, 12:49

Response to: first email / reminder

Date: 06-03-2024, 14:31

#Response 01

Guten Tag [REDACTED]

Danke für die Information.

Für Ihre Studie analysieren Sie bestimmt auch die Gründe, warum es zu einer Fehlfunktion kam. In diesem Fall waren die DNS-Einträge veraltet und die IP-Adresse eines mittlerweile abgeschalteten Servers an einen anderen Kunden des Providers vergeben. Da dort wohl auch ein SSH-Server lief, stimmten die Fingerprints nicht mit denen meines alten Servers überein.

Viele Grüße und Erfolg bei der Studie  
[Absender]

*# Response 02 (2024-03-06, 17:08)*

ID: 03

Group: [REDACTED]

E-Mail sent: 06-03-2024, 13:02

Response to: first email / reminder

Date: 06-03-2024, 13:33

Guten Tag [REDACTED]

schön, dass Sie sich um Sicherheit kümmern. Die gefundenen Subdomains sind allerdings Leichen.

Mit freundlichen Grüßen

[Absender]

*# Response 02 (2024-03-06, 17:09)*

ID: 04

Group: [REDACTED]

E-Mail sent: 06-03-2024, 13:00

Response to: first email / reminder

Date: 06-03-2024, 13:36

Hallo [REDACTED]

- > Sie setzen auf den folgenden Domains DNS-Einträge vom Typ SSHFP, um
- > DNS-basierte HostKey-Verifizierung für SSH zu nutzen:
- >
- > [DOMAINS]
- >
- > Im Rahmen unserer Untersuchung haben wir festgestellt, dass die von Ihnen
- > gesetzten Einträge nicht korrekt konfiguriert sind.

vielen Dank für den Hinweis!

Ich habe die Einträge (hoffentlich) korrigiert.

Viele Grüße

[Absender]

*# Response 02 (2024-03-06, 17:10)*

ID: 05

Group: 

E-Mail sent: 06-03-2024, 12:41

Response to: first email / reminder

Date: 06-03-2024, 13:46

Hi,

vielen Dank für die Information. Ich werde das demnächst beheben.

Viele Grüße

[Absender]

*#Response 02 (2024-03-06, 17:11)*

ID: 06

Group: [REDACTED]

E-Mail sent: 06-03-2024, 13:02

Response to: first email / reminder

Date: 06-03-2024, 13:53

Hallo [REDACTED]

> Am Mittwoch, 6. März 2024 um 13:02:34, schrieb :

>

> [DOMAIN]

das ist ja nett ☐

Das war ein übrig gebliebener DNS-Eintrag, ist jetzt weg.

Viele Grüße,

[Absender]

*#Response 02 (2024-03-06, 17:13)*

ID: 07

Group: [REDACTED]

E-Mail sent: 06-03-2024, 14:10

Response to: [first email](#) / reminder

Date: 06-03-2024, 14:15

[double, same as ID XX]

ID: 08

Group: [REDACTED]

E-Mail sent: 06-03-2024, 12:47

Response to: [first email](#) / reminder

Date: 06-03-2024, 16:00

Hallo [REDACTED],

Am Mi den 6. Mär 2024 um 12:47 schrieb [REDACTED]:

- > Im Rahmen eines Forschungsprojekts identifizieren wir
- > Fehlkonfigurationen in Zusammenhang mit Ihrer DNS-Infrastruktur.
- >
- > # Was ist das (Problem)?
- > Sie setzen auf den folgenden Domains DNS-Einträge vom Typ SSHFP, um
- > DNS-basierte HostKey-Verifizierung für SSH zu nutzen:
- >

[DOMAIN]

Das ist mir bekannt und leider nicht zu ändern.

Hetzner bietet keine Möglichkeit, Domains mit DNSSEC zu versehen und die eigentliche Lösung für das Problem, DLV, wird leider nicht mehr von isc unterstützt.

Gruß

[Absender]

Ps. Meine anderen Domains, beispielsweise [DOMAIN], funktionieren.

*#Response 02 (2024-03-06, 17:25)*

ID: 09

Group: [REDACTED]

E-Mail sent: 06-03-2024, 12:28 - 13:05

Response to: [first email](#) / reminder

Date: 07-03-2024, 01:33

Sehr geehrter [REDACTED],

mir wurde Ihre E-Mail weitergeleitet und ich habe einige Fragen:

Auf dem betreffenden Server [IP+Domain] sind mehrere Websites daheim und, wie der ns1-Name suggeriert, fungiert dieser Server gleichzeitig als Nameserver für eine Reihe an Domains, davon einige mit, einige ohne DNSSEC, da besonders die Denic es ein wenig umständlicher macht DNSSEC anzulegen (was nicht gut ist, aber ein fehlschlagender DNSSEC macht Reachability-mäßig mehr Schaden als kein DNSSEC), daher die Frage, ob HostKey überhaupt von gängigen Libraries genutzt wird in Abwesenheit von DNSSEC.

Während dig zwar vier SSHFP-Entries zurückgibt, so sind es von ssh-keyscan nur drei:

[Technische Details]

Diese sind wiederum nur die, die auch übereinstimmen. Entsprechend wundert es mich echt, ob es da ein Gefahrenpotenzial gibt, welches nicht durch OpenSSH negiert wird. Die Antwort darauf würde vermutlich konkretere Handlungsbereitschaft erwirken, als dass lediglich gesagt wird "passt auf euer SSH ist blöd und wenn euch wer MITM'd könnten eure Keys abfließen."

DNSSEC ist blöd bei Abwesenheit und werd ich so nochmal weitergeben, aber das tatsächliche Abuse-Potential von HostKey-Verification, scheint mir dann eher abstrakt und nicht wirklich ein Problem in der echten Welt zu sein.

Ich würde mich sehr über eine Antwort freuen, gerne auch mit Referenzen zu Papers oder irgendein Proof-of-Concept, der das ganze nochmal veranschaulicht.

Beste Grüße,[Absender]

# Response 02 (2024-03-07, 10:12)



ID: 10

Group: [REDACTED]

E-Mail sent: 06-03-2024, 12:56

Response to: first email / reminder

Date: 07-03-2024, 12:41

Hallo [REDACTED],

Vielen Dank für deine Nachricht mit Tipps zur Verbesserung der Sicherheit unserer Webseiten. Mich interessiert: wie kommst du darauf [Domain] zu prüfen? Ist das Zufall?

Beste Grüße

[Absender]

*#Response 02 (2024-03-07, 15:17)*

ID: 11

Group: [REDACTED]

E-Mail sent: 06-03-2024, 12:35

Response to: first email / reminder

Date: 07-03-2024, 21:23

Hallo [REDACTED],

danke für die Info!

(Ich hoffe ich habe diese Subdomains nicht mehr mit SSH in Verwendung.)

Viele Grüße

[Absender]

*#Response 02 (2024-03-11, 09:38)*

ID: 12

Group: [REDACTED]

E-Mail sent: 06-03-2024, 12:45

Response to: [first email](#) / reminder

Date: 09-03-2024, 12:09

Guten Tag, [REDACTED],

Danke für Ihren Hinweis.

Der Dienst unter [DOMAIN] wurde eigentlich schon vor geraumer Zeit aus Nachfragemangel eingestellt; fehlende Unterstützung von SSHFP und DNSSEC bei populärer (grafischer) SFTP-Software hat den Einsatz unpraktisch gemacht. Für SSH wurde es auch nicht verwendet, da es nur einen SSH-Administrator/Nutzer für die Systeme unter dieser Domain gibt.

Das Entfernen des DNS-Eintrages wurde dabei nicht berücksichtigt, dies habe ich jetzt nachgeholt.

DNSSEC scheint aber korrekt zu funktionieren, und der mit der Domain assoziierte Mailserver hat bisher erfolgreich Nachrichten über mit SMTP DANE gesicherte Verbindungen übertragen und empfangen, hauptsächlich mit Anbietern wie WEB.DE und GMX.

TLSA-Einträge stehen theoretisch ebenfalls für HTTPS-Verbindungen zu der Domain zur Verfügung, aber es gibt meines Wissens nach keine HTTPS-Clients, die dies unterstützen.

Mit freundlichen Grüßen,  
[Absender]

*#Response 02 (2024-03-11, 09:40)*

ID: 13

Group: [REDACTED]

E-Mail sent: 06-03-2024, 12:38

Response to: first email / reminder

Date: 09-03-2024, 15:26

Hallo [REDACTED]

vielen Dank für die Warnung. Ich habe jetzt DNSSEC bei inwx.de für meine\* Domains eingerichtet. Zusätzlich habe ich noch den einen Fehler in meinem SSHFS-Record gefunden und korrigiert. Ihr Live-Check-Tool hat mir sehr dabei geholfen!

\* Domains die mir gehören oder ich im Auftrag verwalte

e-Mail-Adressen: Meine e-Mail-Adresse [EMAIL] haben Sie von meiner Webseite. Haben Sie daran gedacht nach e-Mail-Adressen im DNS CAA-Record zu schauen? dig CAA thju.de | grep -i mailto  
Der Eintrag ist eigentlich für CAs, könnte Ihnen aber helfen technische Ansprechpartner zu Informieren.

Sollten Sie noch Fragen an mich haben die Ihnen bei Ihrer Studie helfen, schreiben Sie mich gerne an.

PS: Sollte es im Rahmen Ihrer Studie eine Umfrage geben, werde ich gerne daran Teilnehmen.

Domains, die von Ihnen gefunden wurden:  
[DOMAINS]

*#Response 02 (2024-03-11, 09:47)*

ID: 14

Group: [REDACTED]

E-Mail sent: 06-03-2024, 12:39

Response to: [first email](#) / reminder

Date: 10-03-2024, 19:17

Hallo [REDACTED],

vielen Dank für den Hinweis.

Allerdings bin ich mit Ihrer Analyse und Schlussfolgerung nicht so ganz einverstanden.

Für meine Domain sind zwei SSHFS Einträge vorhanden. Einer für RSA und einer für Ed25519. Beide mit einem SHA256 Hash. Diese stimmen auch. Ich habe das gerade nochmal nachgeprüft. Also ein Eintrag mit "1 2 <hash>" und ein Eintrag mit "4 2 <hash>".

Ihre Überprüfung versucht aber wohl teilweise eine Validierung mit SHA1. Soweit ich die entsprechenden RFCs verstehe sind SHA256 Hashes den SHA1 Hashes aber immer vorzuziehen. Dies entspricht auch meinem Verständnis von state-of-the Art Security. Ich sehe keinen Grund warum ich noch SHA1 Hashes für SSHFS bereitstellen sollte.

Vielleicht können Sie ihr Tool nochmal auf diesen Umstand hin überprüfen bzw. weitere Hinweise an mich geben.

Vielen Dank.

Mit freundlichen Grüßen

[Absender]

*# Response 02 (2024-03-11, 11:38)*

ID: 15

Group: [REDACTED]

E-Mail sent: 06-03-2024, 13:01

Response to: first email / reminder

Date: 11-03-2024, 11:23

Lieber [REDACTED],

vielen Dank für den Hinweis. Das Problem ist bekannt, die Behebung verzögert sich etwas, die Sicherheitsimplikationen sind uns bekannt.

Viele Grüße aus dem IT-Service (-Homeoffice)

[Absender]

*# Response 02 (2024-03-11, 14:51)*

ID: 16

Group: [REDACTED]

E-Mail sent: 06-03-2024, 12:47

Response to: first email

Date: 11-03-2024, 19:29

Hallo [REDACTED]

vielen Dank für diese Information. Die von Ihnen gefundene Domain ist nicht mehr in Betrieb und die im DNS hinterlegten Daten sind daher stale.

Der aktuell korrekte Name des (neu aufgesetzten Servers) lautet [DOMAIN]. Zu dieser Domain sind auch korrekte SSHFP records hinterlegt.

Mit freundlichen Grüßen  
[Absender]

*#Response 02 (2024-03-11, 22:43)*

*Hallo Herr [Kontakt],*

*vielen Dank für die Rückmeldung!*

*Wenn diese Domain nicht mehr in Betrieb ist, könnten Sie auch in Erwägung ziehen, die dazugehörigen DNS-Einträge (oder die Domain) aus dem DNS zu entfernen.*

*Mit freundlichen Grüßen*

[REDACTED]

*#Response 03 (2024-03-11, 22:46)*

Hallo [REDACTED]

> Wenn diese Domain nicht mehr in Betrieb ist, könnten Sie auch in Erwägung ziehen, die dazugehörigen DNS-Einträge (oder die Domain) aus dem DNS zu entfernen.

Sicher, anfangs war aber nicht klar, ob die Domain noch wieder reaktiviert wird und das alte VM-Image wieder aufgespielt wird, oder nicht, daher existiert die Domain so noch.

Mit freundlichen Grüßen  
[Absender]

*# Response 04 (2024-03-11, 22:48)*

ID: 17

Group: [REDACTED]

E-Mail sent: 06-03-2024, 12:59

Response to: first email

Date: 12-03-2024, 17:20

Hallo [REDACTED]

zunächst vielen Dank für den Hinweis.

Die Domains [DOMAIN-A DOMAIN-B] zeigen auf dieselbe IP. Für beide Domains sind unterschiedliche SSHFP-Records hinterlegt. Über SRV-Einträge wird jeweils darauf hingewiesen, wie der SSH-Dienst für die jeweilige Domain zu erreichen ist. Dadurch kann einem auffallen, dass der SSH-Dienst für die Domain [DOMAIN-A] auf dem Port 22 erreichbar ist, zu welchem dann hoffentlich auch die SSHFP-Einträge passen und der SSH-Dienst für die Domain [DOMAIN-B] auf dem Port 2222 erreichbar ist mit hoffentlich passenden SSHFP-Einträgen. Um den Schaden einer Sicherheitslücke des einen Diensts nicht auf den anderen Dienst zu übertragen, besitzen beide Dienste separate Hostkeys.

Meine DNS-Zone ist per DNSSEC abgesichert. Das könnten sie eigentlich automatisiert ermitteln. Daher verstehe ich entweder Ihren Hinweis auf die DNSSEC-Absicherung nicht, oder sitze einem Irrglauben auf.

Nach meinem Kenntnisstand ist diese Form des Deployments erstmal nicht anfällig für die von Ihnen genannten Risiken. Ich wäre aber über detailliertere Hinweise dankbar.

Sollten Sie die SRV-Einträge bei ihrem Scraping nicht berücksichtigen, würde ich eine Ergänzung empfehlen.

Mit freundlichen Grüßen  
[Absender]

*# Response 2024-03-12, 21:38*



ID: 18

Group: [REDACTED]

E-Mail sent: 06-03-2024, 12:45

Response to: first email

Date: 26-03-2024, 20:47

Am Mittwoch, 6. März 2024, 12:45:33 CET schrieben Sie:

> Guten Tag,

Guten Tag [REDACTED],

vielen Dank für den Hinweis.

- > Im Rahmen eines Forschungsprojekts identifizieren wir
- > Fehlkonfigurationen in Zusammenhang mit Ihrer DNS-Infrastruktur.
- >
- > # Was ist das (Problem)?
- > Sie setzen auf den folgenden Domains DNS-Einträge vom Typ SSHFP, um
- > DNS-basierte HostKey-Verifizierung für SSH zu nutzen:
- >
- > [DOMAIN]
- >
- > 2) Die SSHFP DNS-Einträge werden nicht ausreichend gesichert übertragen,
- > weil DNSSEC nicht konfiguriert ist.

Das ist mir bewusst, ich habe kein DNSSEC ausgerollt, aber mit den entsprechenden DNS-Einträgen experimentiert.

Gruß

[Absender]

# Response 02 (2024-03-27, 07:39)

ID: 19

Group: [REDACTED]

E-Mail sent: 27-03-2024, 17:41

Response to: reminder

Date: 27-03-2024, 18:42

Moin [REDACTED]!


Danke für deinen Input, wir haben das intern weitergeleitet. Wir als Vorstand haben jedoch keinen Einfluss darauf ob die DNS Admins sich bei dir zurückmelden.

Danke und Gruss

— [Absender]

*# Response 02 (2024-03-27, 19:21)*

ID: 20

Group: 

E-Mail sent: 27-03-2024, 18:03

Response to: reminder

Date: 27-03-2024, 18:51

Die angegebenen Domains haben mit mir nichts zu tun.

# *Response 02 (2024-03-27, 19:37)*

ID: 21

Group: 

E-Mail sent: 27-03-2024, 18:02

Response to: reminder

Date: 27-03-2024, 18:56

Die Konfiguration ist beabsichtigt. Kontaktieren Sie mich bitte nicht weiter - eine E-Mail zum Thema hätte m.E. genügt.

ID: 22

Group: [REDACTED]

E-Mail sent: 27-03-2024, 18:03

Response to: reminder

Date: 27-03-2024, 19:14

Hallo [REDACTED]

- > Im Rahmen eines Forschungsprojekts an der [REDACTED]
- [REDACTED] identifizieren wir mögliche Fehlkonfigurationen in Zusammenhang mit
- > Ihrer DNS-Infrastruktur.
- > Dazu haben wir Sie am 06.03.2024 bereits kontaktiert.

Die erste Mail zu dem Thema habe ich gelesen, für mich bewertet und ignoriert.  
Diese jetzt weitere Mail hat schon einen gewissen Nerv-Faktor. Aber es ist ja die letzte.

- >
- > Mit dieser Nachricht wollen wir Sie lediglich über ein von uns beobachtetes
- > Verhalten informieren. Falls Sie bereits Änderungen an den SSHFP-Einträgen
- > vorgenommen haben, bezieht sich diese Nachricht vermutlich auf nicht
- > konfiguriertes DNSSEC.

Und dann die Adressaten noch raten lassen, worauf sich Ihre Mail bezieht. Sie, beziehungsweise Ihr Script, sollten das doch wissen.  
Das halte ich im Rahmen Ihrer Forschungsarbeit für ethisch durchaus fragwürdig, denn ich gehe davon aus, dass Sie testen und retesten werden und dann ihr entsprechender "Erfolg" auch Teil Ihres Forschungsberichts bzw. Ihrer DA wird. Im Gegensatz zu ihrem (unzureichenden) automatischen Script mit automatischer Mail muss ich als Mensch Zeit aufwenden, um Ihre Mail zu lesen und zu bewerten. Ihre Ethikkommission weiss das?

- > Sie denken, dass unsere E-Mail ein Fehler ist? Oder Sie wissen bereits um
- > das Problem? Dann würden wir uns sehr über Ihr Feedback als kurze Antwort
- > auf diese E-Mail freuen.

Nun, ich denke folgendes:

RFC 4255 Sec 2.4 verbietet ausdrücklich einem Client, einem Key zu vertrauen, wenn er nicht durch DNSSEC abgesichert ist.

Die endgültige Entscheidung ob ich den Key akzeptiere liegt dann wieder beim Nutzer (also mir).

Die Situation mit vorhandenen SSHFP-Eintrag ist also niemals schlechter als ohne SSHFP-Einträge. Deswegen halte ich es für legitim, SSHFP-Records automatisch einfach aus Prinzip zu deployen, unabhängig davon ob auf der Domain DNSSEC aktiv ist oder nicht. Die Entscheidung für oder gegen DNSSEC fällt aus anderen Gründen...

Viele Grüße,  
und noch viel Erfolg...

[Absender]

# *Response 02* (2024-03-27, 19:59)

ID: 23

Group: [REDACTED]

E-Mail sent: 27-03-2024, 18:03

Response to: reminder

Date: 27-03-2024, 19:26

Guten Abend [REDACTED]

und vielen Dank für Ihre Emails. Ich bin in der Tat noch nicht dazu gekommen mir die Konfiguration im Detail anzuschauen.

Meines Wissens habe ich die DNSSEC-Konfiguration nicht vorgenommen.

Da die Konfiguration aber nicht hart in zonefiles codiert ist muss ich mir die Skripte einmal genauer anschauen, welche diese konfigurieren.

Dies werde ich mal demnächst tun.

Vielen Dank und Beste Grüße nach [REDACTED]

Geben Sie gerne mal bescheid, wenn sie aus der Studie ein Paper veröffentlicht haben.

Mit freundlichen Grüßen

[Absender]

*# Response 02 (2024-03-27, 21:26)*

ID: 24

Group: [REDACTED]

E-Mail sent: 27-03-2024, 17:41

Response to: reminder

Date: 28-03-2024, 01:58

Hallo,

entschuldigt, wir sind nur ein paar Leute, die ehrenamtlich als Admins [REDACTED] arbeiten. Eine grobe Erklärung für die noch nicht vollständig korrigierten DNSSEC-Einträge ist folgende: wir haben uns vor ca. zwei Jahren nach einer größeren technischen Panne entschieden, alle Server neu aufzusetzen, und sind seitdem nicht dazu gekommen, die SSHFP-Einträge nachzuziehen. SSHFP wurde in den vergangenen Jahren aber auch nur von einem einzigen Menschen [REDACTED] aktiv genutzt/beachtet (und auch tatsächlich schon bemängelt) und von allen anderen (der Standard-Einstellung der meisten SSH-Clients entsprechend) ignoriert, deshalb hatten wir das Thema mit einer sehr niedrigen Priorität auf dem Schirm. Als Reaktion auf eure Mail neulich haben wir jetzt tatsächlich mal ein kleines Bash-Script begonnen, das unsere SSH-Fingerprints automatisiert prüfen und bei Bedarf anlegen/korrigieren soll, hatten die letzten drei Wochen dann aber noch andere Dinge zu tun, deshalb kam es nur zur Korrektur des einen ED25519-Fingerprints. Euer Web-Tool haben wir auch schon ausprobiert, um die richtige Änderung dieses einen Eintrags zu testen, das hat gut geklappt und war tatsächlich sehr nützlich.

In jedem Fall vielen Dank für eure Anfrage, wir werden schauen dass wir auch die restlichen SSHFP-Einträge demnächst korrigieren (und bei dem einen bereits bearbeiteten Eintrag den aktuellen RSA-Fingerprint vmtl wieder einfügen). Euch weiterhin viel Erfolg bei eurer wissenschaftlichen Arbeit!


Viele Grüße

[Absender]

*# Response 2024-03-28, 01:10 (Zeitzone ggf. Unterschiedlich?)*



ID: 25

Group: 

E-Mail sent: 06-03-2024, 12:41

Response to: reminder (first email?)

Date: 28-03-2024, 09:04

Hallo,

Vielen Dank für den Hinweis. Die von Ihnen bemerkte Fehlkonfiguration ist in meinem Fall die fehlende DNSSEC-Absicherung. Die Hürde das zu korrigieren ist, dass mein Registrar (Hetzner, auf Cc:) leider keine Möglichkeit bietet DNSSEC zu konfigurieren. In der Dokumentation[1] steht nur, dass das zwar nützlich wäre um das Sicherheitsniveau anzuheben, aber zu teuer im Vergleich zur niedrigen Nachfrage ist. Auf meiner Langzeit-Todo-Liste steht aus diesem Grund ein Registrar-Wechsel, der Punkt hat es aber in der Priorisierung noch nicht nach oben geschafft. Bis es so weit ist, finde ich unabgesicherte DNS-Einträge besser als gar keine.

Wenn Ihre Arbeit die Wichtigkeit von DNSSEC mehr in den Fokus der Technikbranche bringt, fände ich das hervorragend. Wenn Ihre Ergebnisse veröffentlicht sind, würde ich mich über einen entsprechenden Hinweis und einen Link freuen.

Mit freundlichen Grüßen

[Absender]

[1] <https://docs.hetzner.com/de/dns-console/dns/general/dnssec/>

*# Response 2024-03-28, 10:15*

ID: 26

Group: [REDACTED]

E-Mail sent: 27-03-2024, 17:54

Response to: reminder

Date: 28-03-2024, 08:27

#Response 01

Hallo.

Danke für die Info.

Mir war das Problem allerdings grundsätzlich bekannt. Nach einem Server-Umzug hatte ich die FP noch nicht angepasst im DNS.

DNS-SEC mache ich bisher nicht, muss ich mir mal bei Gelegenheit nochmal ansehen. "Zuletzt" war mein Fazit, dass es aufgrund der Probleme, die durch die Benutzung von DNS-SEC entstehen können, keinen Sinn ergibt. Das ist aber auch schon Jahre her...

Ich habe Tickets in meinem Trac für beide Probleme, das geht also nicht verloren... □

Viele Grüße,

[Absender]

*# Response 02 (2024-03-28 10:13)*

*[Dankeschön]*

#Response 03 (2024-03-28, 12:36)

On 2024-03-28 10:13, [REDACTED] wrote:

[vielen Dank für die positive Rückmeldung!](#)

Danke Ihnen für den kostenlosen Service! □

ID: 27

Group: 

E-Mail sent: 27-03-2024, ?

Response to: reminder

Date: 04-04-2024, 13:56

Hi!

Danke für die Info.

Die [DOMAIN]-Domain ist nur noch legacymäßig im Betrieb und bekommt daher kein DNSSEC.

Der Zoneninhalt ist aber synchron mit unseren aktuellen Domains, in denen die SSHFP-Einträge angelegt werden.

Für eure Untersuchungen (und auch die Warnmails) würde es vermutlich helfen, fehlendes DNSSEC von falschem SSHFP zu unterscheiden.

Der wichtigste Hinweis zu möglichen Sicherheitsproblem fehlt meiner Ansicht nach in eurer Mail: ☐

`VerifyHostKeyDNS yes` akzeptiert die manipulierten hostkeys nur, wenn die DNS-Antwort auch korrekt signiert ist also das Authentic Data (AD) flag in der Antwort gesetzt ist. Sonst wird weiterhin gefragt ob man sich mit dem unbekannten Hostkey verbinden will.

Wir haben noch einen weiteren Mechanismus im Einsatz - SSH-Zertifikate.

Der Betreff dass unsere Website falsch konfiguriert sei ist leider irreführend - die Webseiten betreut eine völlig andere Abteilung ☐

Danke für eure Untersuchungen - wenn dazu mal ein Paper oder Ergebnisse rauskommen würden die mich interessieren!

Cheers

[Absender]

ID: 28

Group: [REDACTED]

E-Mail sent: 2024-03-06, 13:13

Response to: first email / reminder

Date: 2024-03-06, 13:35

Respondent: male

# Response 1

Hallo [REDACTED],

danke für die Information. Allerdings laufen auf der IP mehrere SSH-Server auf verschiedenen Ports. Soweit ich weiß gibt es keine Möglichkeit, SSHFP entsprechend zu unterscheiden. Die DNS-Einträge bei den jeweiligen kanonischen Hostnamen sind allerdings korrekt. Vielleicht möchten Sie das in Ihrer Forschungsarbeit als Szenario 3 mit unterbringen.

Beste Grüße

[Vorname Nachname, anonymisiert]

# Response 2 [2024-03-06, 15:09]

ID: 29

Group: 

E-Mail sent: 2024-03-06, 12:49

Response to: first email / reminder

Date: 2024-03-06, 15:37

Respondent: male

# Response 1

Moin,

danke für den Hinweis. Hintergrund für die "Fehlkonfiguration" ist meine Faulheit, da ich noch nicht die DNSSEC-Keys gesetzt habe. Ist jetzt entfernt, da die Überprüfung in OpenSSH per Default deaktiviert ist und eine manuelle Überprüfung weniger Angriffsfläche bietet. Danke!

*Für Szenario 2: DNS ist ein Klartext-Protokoll, welches ohne DNSSEC keine Garantien zur Authentizität der übertragenen Daten bietet. Der SSHFP-Standard erfordert, dass diese DNS-Einträge gesichert (bspw. per DNSSEC) übertragen werden sollen. Ist dies nicht der Fall, so können netzwerkbasierte Angreifer die übertragenen SSHFP-Einträge manipulieren oder entfernen. Das bedeutet, dass die automatisierte HostKey-Verifizierung scheitert oder vom Angreifer manipulierte HostKeys akzeptiert werden.*

Nach meinem Verständnis wäre diese Aussage nur dann korrekt, wenn das benutzte Programm die SSHFP-Einträge unzureichend überprüft. Dann wäre man, auch bei korrekter Konfiguration der DNS-Einträge, immer angreifbar. Eine fehlende Signatur sollte immer wie eine ungültige Signatur behandelt werden. Ist dies nicht der Fall, könnte ein Angreifer einfach die Signatur entfernen und die Einträge manipulieren. Generell können also unter keiner Konfiguration vom Angreifer manipulierte HostKeys akzeptiert werden.

Auch in dem verlinkten Paper von Neef und Wisiol wird nur das Fehlen von DNSSEC überprüft aber keine Folgen davon genannt.

Es sollte also immer Szenario 1 eintreten.

Gibt es tatsächlich Angriffe, die das irgendwie ausnutzen können?

Liebe Grüße

[Vorname, anonymisiert]

# Response 2 [2024-03-06, 15:54]

ID: 30

Group: [REDACTED]

E-Mail sent: 2024-03-06, 12:41

Response to: first email / reminder

Date: 2024-03-06, 16:00

Respondent: male

# Response 1

Sehr geehrte [REDACTED],

vielen Dank für Ihre Nachricht und die erkannte Schwachstelle in unserem System. Darf ich fragen, wie sie unsere Domains ausgewählt haben? Die Information ist auf jeden Fall hilfreich und wir werden uns um die Behebung des Problem kümmern,

Vielen Dank und viele Grüße,  
[Vorname Nachname, anonymisiert]

# Response 2 [2024-03-06, 16:22]

Hallo Herr [Nachname, anonymisiert],

vielen Dank für Ihre Rückmeldung!

*Die Frage zu unserer Methodik will ich Ihnen gerne beantworten. Zunächst haben wir aus verschiedenen, öffentlichen Quellen Domains mit deutscher Top-Level-Domain (".de") gesammelt. Insgesamt konnten wir so 27.5 Millionen aktiv genutzte deutsche Domains inklusive Subdomains ermitteln. Diese Domains haben wir anschließend auf das Vorhandensein und die korrekte Konfiguration von SSHFP gemäß der Methodik von Neef et al. [1] untersucht. Die Domains, die durch unsere Analyse als nicht korrekt konfiguriert eingestuft wurden, haben wir anschließend informiert.*

*Melden Sie sich gerne, wenn Sie noch Fragen haben!*

*Beste Grüße,*

[REDACTED]

[1] <https://arxiv.org/abs/2208.08846>

# Response 3 [2024-03-06, 17:17]

Hallo [REDACTED],

vielen Dank für die Rückmeldung und die Beschreibung der Methodik. Dadurch haben Sie sicherlich einigen Leuten helfen können.

Viele Grüße,  
[Vorname Nachname, anonymisiert]

*# Response 4 [2023-03-06, 19:02]*

ID: 31

Group: [REDACTED]

E-Mail sent: 2024-03-06, 13:06

Response to: first email / reminder

Date: 2024-03-06, 14:10

Respondent: male

# Response 1

Guten Tag,

ich habe einige Fragen zu Ihrer Test-Methode:

- Haben Sie sowohl IPv4 als auch IPv6 getestet?
- Wie sind Sie genau auf diese beiden Domains (unabhängig voneinander) gestoßen?  
Das sind alles CNAMEs auf den selben Host.
- Von welchem SSH-Port sind Sie bei dem Test ausgegangen und weshalb?
- Welche E-Mail-Adresse haben Sie für die anhängige Mail verwendet? Owner-C? Tech-C? Admin-C? Zone-C?
- Wie viele dieser E-Mails haben Sie insgesamt verschickt?
- Gibt es öffentliche Ressourcen zu Ihrem Projekt?

In diesem Fall befindet sich unter der v4-Adresse ein Honeypot mit anderem Host-Key.  
Mein Eindruck hier ist, dass es potentiell eine enorm hohe False-Positive-Rate bei diesen Tests gibt.

Viele Grüße,

[Vorname Nachname, anonymisiert] (auch tätig [REDACTED], [Dienststelle, anonymisiert])

# Response 2 [2023-03-06, 14:15]

Guten Tag,

die selben Fragen richte ich auch nochmals an [REDACTED] von [REDACTED], der  
offenbar andere Teile meiner privaten Domains gescannt hat.

Viele Grüße,

[Vorname Nachname, anonymisiert]



# Response 4 [2023-03-06, 14:46]

Guten Tag,

anhand des Links und der verschiedenen Infos auf der [REDACTED] konnte ich zumindest herausfinden, dass Sie ausschließlich IPv4 und ausschließlich Port 22. Aus meiner Sicht ist der Test so nicht für eine repräsentative Studie tauglich. Ich bitte Sie, Daten die ggf. aus meinen Domains erhoben wurden, nicht für eine entsprechende Studie/Paper zu verwenden. Außerdem Bitte ich Sie, den Mailversand betreffend des Hosts mit der IP [IP Adresse, anonymisiert] (via CNAME auf [Domain, anonymisiert]) \*umgehend\* einzustellen. Ich und andere Nutzer der Domains haben mittlerweile 21 Mails an verschiedene Adressen erhalten.

Viele Grüße,

[Vorname Nachname, anonymisiert]

# Response 5 [2023-03-06, 15:06]

Hallo Herr [Nachname, anonymisiert],

vielen Dank erst einmal für Ihre Rückmeldung. Wenn ich das richtig verstanden habe, sind ja ein Teil Ihrer Fragen bereits beantwortet?

Ansonsten kann [REDACTED] Ihnen gerne mehr Informationen zu den technischen Fragen geben!

Zu der Frage bezüglich unserer Methodik:

Wir haben die Personen angeschrieben, die wir entsprechend auf Domain-Ebene als Ansprechpartner:in identifizieren konnten. Dazu haben wir entweder die Informationen aus dem Impressum der entsprechenden Website genommen oder, wenn wir diese nicht aufrufen konnten, an hostmaster@DOMAIN geschrieben. Das führte in Ihrem Fall dazu, dass Sie, wie beschrieben, mehrere E-Mails und auch mehrere E-Mails zu unterschiedlichen (Sub-) Domains bekommen haben.

Um unsere Methodik reproduzierbar zu gestalten, haben wir bewusst nur solche Subdomains zusammengefasst, von denen wir sicher wussten, dass wir damit ein und dieselbe Person erreichen. Entsprechend haben wir auch nicht gesammelt Ansprechpersonen des CNAME-Hosts angeschrieben, was bei Ihnen ebenfalls noch einmal zu mehr Anschreiben führte. In der Auswertung werden wir diese Zusammenhänge - soweit nachvollziehbar - natürlich berücksichtigen.

Wir werden selbstverständlich in den Ergebnissen keine Daten veröffentlichen, die sich in irgendeiner Weise Rückschlüsse auf Sie oder Ihre Domain(s) zulassen. Sie bzw. die von Ihnen definierten Kontakte werden wir entsprechend nicht weiter kontaktieren.

Melden Sie sich gerne, wenn noch Fragen offen sind! Ich bin sicher, dass wir alles gut klären können. Im Zweifel im persönlichen Gespräch vor Ort [REDACTED];)

Beste Grüße,

[REDACTED]

# Response 6 [2023-03-06, 17:43]

Hallo Herr [Nachname, anonymisiert],

ich beantworte Ihnen gern die technischen Nachfragen.

- Haben Sie sowohl IPv4 als auch IPv6 getestet?

Nein, IPv6 haben wir aufgrund von technischen Limitierungen nicht geprüft. Alle Tests beziehen sich auf IPv4 Adressen (bzw. A-Records).

- Wie sind Sie genau auf diese beiden Domains (unabhängig voneinander) gestoßen?  
Das sind alles CNAMEs auf den selben Host.

Wir haben aus verschiedenen Quellen (Censys Certificate Dataset [0], CertStream [1], usw.) einen großen Datensatz deutscher (Sub)Domains (TLD:.de) generiert und diesen entsprechend analysiert.

- Von welchem SSH-Port sind Sie bei dem Test ausgegangen und weshalb?

Getestet wurde gegen den Standard-SSH-Port "22/tcp", um eine möglichst hohe Trefferrate zu erzielen.

Ich hoffe das hilft Ihnen weiter. Die anderen Fragen hatte meine Kollegin bereits beantwortet. Falls trotzdem noch welche offen sind, schreiben Sie uns.

Mit freundlichen Grüßen

[REDACTED]

[0] <https://support.censys.io/hc/en-us/articles/360038761891-Research-Access-to-Censys-Data>

[1] <https://certstream.calidog.io/>

# Response 7 [2024-03-12, 08:25]

Hallo [REDACTED],

Sie haben ja letzte Woche eine Nachfrage von [Vorname Nachname, anonymisiert] zu dem SSHFP-Scanning beantwortet und haben dann ein persönliches Gespräch angeboten. Die betreffenden Domains/Server werden von ihm gemeinsam mit mir

verwaltet, und ich hätte Interesse an einem Gespräch. Ich war bis jetzt aber leider unterwegs und kann daher erst jetzt reagieren.

Morgen hätte ich, bis auf einen Termin zwischen 13:00 und 14:00, den ganzen Tag Zeit, bei Ihnen vorbeizukommen, wenn Sie auch Interesse hätten. Was mich besonders interessiert wäre das Sicherheits-/Angreifermodell, das sie hier zugrunde legen und nach dem Sie Konfigurationen als "falsch" bewerten.

Viele Grüße,  
[Vorname Nachname, anonymisiert]

# Response 8 [2024-03-12, 16:27]

Hallo Herr [Nachname, anonymisiert],

*da haben wir diesmal ja interessante Kontakte aus dem direkten Umfeld dabei! Gerne können wir morgen sprechen, ich habe bis ca. 14.30 Uhr Termine, aber danach würde es bei mir passen. Ich muss allerdings leider zugeben, dass ich von den technischen Details eher oberflächliche Kenntnisse habe. Mein Forschungsgebiet liegt im Bereich der Benachrichtigung, weniger der Schwachstelle :) Daher kann ich Ihnen zwar sehr gerne erklären, warum mich das Thema interessiert, für alles andere wäre aber [REDACTED] von [REDACTED] der bessere Ansprechpartner.*

*Daher zwei Vorschläge: Wir könnten einen Online-Termin mit [REDACTED] vereinbaren, das wäre dann allerdings erst nächste Woche möglich. Einen Termin müssten wir dann noch mal zu Dritt absprechen. Ansonsten wäre [REDACTED] morgen in [REDACTED] Ihn kennen Sie vielleicht auch aus dem [Projektname]-Kontext, er betreut meine Arbeiten mit und kann sicher auch noch mal die eine oder andere eher technische Frage beantworten. Hier könnten wir uns morgen 10.30 und 11.30 Uhr bei uns am Institut treffen, wenn das passt!*

Beste Grüße,

[REDACTED]

# Response 9 [2024-03-12, 16:38]

Hallo,

Die Technik (im Sinne von, "wie der Mechanismus funktioniert" und "Was getestet wurde"), hab ich, glaub ich, recht gut verstanden. Mich würde da tatsächlich eher die Frage interessieren, mit welchem Gedankengang man was genau als "Fehlkonfiguration" bezeichnet. Das hängt auch direkt mit der Formulierung der Benachrichtigung zusammen. D.h. ich denke, dass ich Ihnen schon einiges interessante diskutieren könnte.

Die Zeiten, die Sie angegeben haben, passen für mich gerade nicht ganz zusammen. Sie schreiben, dass Sie Termine bis ca. 14:30 haben, aber bieten dann auch noch einen

Termin um 10:30 und/oder 11:30 an (oder wären Sie dann bei den zwei Zeiten nicht dabei?).

Mir wären diese Zeiten alle passend, ich kann also zu einer beliebigen dieser 3 Optionen kommen. Mit [REDACTED] hab ich bisher noch nicht zusammengearbeitet, wenn er dazukommen will, gerne. Das ist aber von mir aus nicht unbedingt notwendig. Wenn das allen passt, wäre dann ja morgen 10:30, eine gute Option.

Über einen Online-Termin würde ich mir dann nur Gedanken machen, wenn nach dem Gespräch morgen noch Fragen offen bleiben.

Viele Grüße,  
[Vorname, anonymisiert]

*# Response 10 [2024-03-12, 16:46]*

*Hallo [Vorname, anonymisiert],*

*(ich nutze jetzt einfach mal das „Du“, wenn das in Ordnung ist?)*

*Ach, tut mir Leid, wir waren den ganzen Vormittag in Meetings, ich wollte heute morgen gleich antworten und habe die Mail aber eben erst zu Ende geschrieben. In der Zwischenzeit haben sich Terminverschiebungen morgen Vormittag ergeben, sodass 10.30 Uhr wieder passt. Gerne auch 10.45 Uhr, wenn das bei dir geht, dann bleibt für uns noch eine kurze Pause zwischen den Terminen. Nur zur Sicherheit: Wir sitzen [REDACTED]*

*Beste Grüße,*

[REDACTED]

*# Response 11 [2024-03-12, 16:49]*

Hallo [REDACTED],

(ja, gerne "Du" :) )

Gut, dann bin ich um 10:45 [REDACTED]. Ich bin mir nicht sicher ob ich ins Gebäude komme, wenn ich an der Tür hänge, melde ich mich.

Viele Grüße,

[Vorname, anonymisiert]

*# Response 12 [2024-03-12, 16:55]*

*Ah, ja, das kann sein! Dann gerne kurz durchrufen: [REDACTED]. Dann komme ich runter! Schön, dann auf jeden Fall bis morgen!*

*[Persönliches Treffen am 13.03.2024, 10:45]*

*# Response 13 [2024-03-14, 13:32]*

Hallo,

Ich habe nach unserem Gespräch nochmal genauer über verschiedene Aspekte dieser SSHFP-Verifizierung nachgedacht. Vorab hab ich nochmal überlegt, was denn das Sicherheitsziel des SSHFP-Mechanismuses sein könnte, weil die Auswahl des Ziels natürlich Einfluss darauf hat, welche Konfiguration gewählt wird, und von welchem Nutzerverhalten man ausgehen würde. Ich hätte 3 Varianten:

- "Ziel ist es, die Wahrscheinlichkeit für erfolgreiche SSH-MitM-Angriffe zu senken, indem Nutzern nicht mehr dazu aufgefordert werden einen SSH-Key manuell zu verifizieren. Sie haben ihren SSH-Client so konfiguriert, dass er nicht mehr erlaubt, SSH-Keys manuell zu verifizieren." (Ziel 1)
- "Ziel ist es, die Wahrscheinlichkeit für erfolgreiche SSH-MitM-Angriffe zu senken, indem Nutzern seltener dazu aufgefordert werden SSH-Keys manuell zu verifizieren, und dadurch die Chance höher ist, dass sie eine manuelle Verifikation als Angriff erkennen, und dann vorsichtiger sind." (Ziel 2)
- "Ziel ist es, die Wahrscheinlichkeit für erfolgreiche SSH-MitM-Angriffe zu senken, indem Nutzern, die sich erstmalig mit einem SSH-Dienst verbinden, eine weitere Option zu geben wie sie den SSH-Fingerprint verifizieren können, wenn sie keine andere Möglichkeit haben den gültigen SSH-Fingerprint zu ermitteln." (Ziel 3)

Vor allem in Situationen in denen viele Leute auf viele verschiedene Hosts zugreifen (z.B. ein Rechencluster), ist wohl "Ziel 1" das passendste. Wenn nur wenige Leute sich mit demselben Server häufiger verbinden, dann trifft wohl "Ziel 3" zu. Seid ihr von einem dieser Sicherheitsziele (oder einem anderen) ausgegangen, bei der Überlegung, wie Leute SSHFP in ihrem client konfigurieren?

Ich habe mir auch nochmal die möglichen Konfigurationen für den openssh-Client genauer angeschaut (andere ssh-clients die sshfp verifizieren können, sind mir nicht bekannt). In allen Fällen kann diese Option nur mit einem lokalen, DNSSec-validierenden resolver die Sicherheit potentiell erhöhen. Wenn der resolver nicht lokal ist, bringt aktivieren von "VerifyHostKeyDNS=yes" sogar einen Sicherheitsnachteil. Die folgende Liste deckt natürlich nicht alle möglichen Kombinationen der Situation ab, aber ich denke die relevantesten sollte ich dabei haben.

- VerifyHostKeyDNS=no (Als "Ausgangssituation")
  - Korrekter SSH-Key in "KnownHosts" -> keine Aufforderung
  - Falscher SSH-Key in "KnownHosts" -> Große Warnung ohne Möglichkeit zu diese "direkt" zu ignorieren. Um sich trotzdem zu verbinden, muss man den SSH-Key händisch aus der "KnownHosts" datei entfernen. Das Kommando um das zu tun, wird dem Nutzer hierbei ausgegeben

- Kein SSH-Key in "KnownHosts" -> Nutzer wird zur manuellen Verifikation aufgefordert, und kann den Key mit "yes" (oder durch Eingabe des korrekten Fingerprints) bestätigen.

- VerifyHostKeyDNS=ask

- Korrekter SSH-Key in "KnownHosts" -> keine Aufforderung
  - Falscher SSH-Key in "KnownHosts" -> Große Warnung ohne Möglichkeit zu diese "direkt" zu ignorieren. Um sich trotzdem zu verbinden, muss man den SSH-Key händisch aus der "KnownHosts" datei entfernen. Das Kommando um das zu tun, wird dem Nutzer hierbei ausgegeben

- Kein SSH-Key in "KnownHosts" + gleicher SSHPF -> Manuelle Aufforderung zur Verifikation zusammen mit der Aussage, dass der SSH-Key auch in DNS gefunden wurde ("Matching host key fingerprint found in DNS.").

- Kein SSH-Key in "KnownHosts" + falscher SSHPF -> "Große Warnung" + Manuelle Aufforderung zur Verifikation, mit der man das überschreiben könnte.

- => In dieser Konfiguration ist es interessanterweise egal ob der resolver behauptet DNSSec geprüft zu haben

- VerifyHostKeyDNS=yes

- Korrekter SSH-Key in "KnownHosts" -> keine Aufforderung

- Korrekter SSH-Key in "KnownHosts" aber falscher SSHFP -> "Große Warnung", aber die Verbindung wird trotzdem ohne weitere Nachfrage hergestellt.

- Falscher SSH-Key in "KnownHosts" + gleicher SSHFP -> keine Aufforderung

- Falscher SSH-Key in "KnownHosts" + falscher SSHFP -> zwei mal "Große Warnung" direkt hintereinander (ohne Möglichkeit zu ignorieren)

- Kein SSH-Key in "KnownHosts" + gleicher SSHPF + ein Resolver der behauptet der DNS-Record ist signiert -> Direkte Verbindung ohne Nachfrage. Der SSH-Key wird nicht in "KnownHosts" aufgenommen.

- Kein SSH-Key in "KnownHosts" + falscher SSHPF + ein Resolver der behauptet der DNS-Record ist signiert -> "Große Warnung" + Manuelle Aufforderung zur Verifikation, mit der man das überschreiben könnte.

- VerifyHostKeyDNS=yes StrictHostKeyChecking=yes

- Dasselbe wie bei "VerifyHostKeyDNS=yes StrictHostKeyChecking=no", außer:

- Kein SSH-Key in "KnownHosts" + falscher SSHPF -> "Große Warnung", keine Möglichkeit fortzufahren, ohne Konfiguration zu ändern.

Wenn DNSSec zwar korrekt konfiguriert ist, aber diese Zone nicht signiert, denke ich, ist das Verhalten so:

- Jeder nicht-angreifer-kontrollierte DNS-Resolver wird nicht die Bestätigung zurückgeben, dass der Eintrag signiert war. Dadurch wird der SSH-Key zwar bei "VerifyHostKeyDNS=ask" angezeigt, leider ununterscheidbar von einem der signiert war ("Matching host key fingerprint found in DNS."). Und bei "VerifyHostKeyDNS=yes" wird nicht automatisch verbunden.

Diese Überlegungen kann man, glaub ich, wie folgend zusammenfassen: Bei den Konfigurationen, die ihr als "Fehlkonfigurationen" bezeichnet, kann man mit diesen Optionen den SSH-Client nicht so konfigurieren, dass er unbekannte SSH-Keys automatisch akzeptiert, da er diese nicht durch SSHFPs prüfen kann, wenn sich ein Nutzer über IPv4 zu den genannten Domain-Names verbindet. Das gilt sowohl für eine

nicht-DNSSEC-signierte Zone als auch für einen nicht-passenden SSHFP. Ich glaube eine solche Zusammenfassung wäre in der Informationsmail gut gewesen, ohne das als "Fehler" zu bezeichnen (aber das wäre dann natürlich eine technischere Erklärung, als die, die ihr hattet).

Diese nicht-passende Konfiguration unterscheidet sich von typischen "Fehlkonfigurationen" (Schwache Cipher erlaubt, Berechtigungen zu breit gesetzt, ...) dadurch, dass hier sowohl die Konfiguration des Servers als auch die Konfiguration der Clients relevant ist.

Was genau ein nicht-passender SSHFP/eine fehlende DNSSec-Signatur für den Nutzer bedeutet, hängt von der lokalen Konfiguration ab. Sollten Nutzer aber trotz diese nicht-zusammenpassenden Konfiguration die Verbindung aufbauen, ist sie (bei VerifyHostKeyDNS) aber nicht von einem Angriff zu unterscheiden.

D.h. wenn Nutzer sich trotz dieser nicht-zusammenpassenden-Konfiguration mit dem SSH-Dienst verbinden, dann würden sie das auch tun, wenn ein Angriff vorliegt.

Daraus schließe ich, dass wenn hier ein Problem vorliegt, es auf jeden Fall nicht nur ein Konfigurationsproblem des Servers ist, sondern auch ein Konfigurationsproblem der Clients.

(Ich habe übrigens inzwischen von einigen weiteren Leuten erfahren, die tatsächlich eine ähnliche Konfiguration verwenden wie wir, also verschiedene SSH-Dienste per IPv6 und IPv4 erreichbar machen. Dabei läuft auf IPv4 nicht unbedingt ein Honeypot, wie bei uns, sondern z.B. auch Weiterleitungen zu anderen, internen SSH-Servern, o.ä. So wie ich diese Personen verstanden habe, haben sie euch aber keine Rückmeldung gegeben. Ich kann natürlich keine quantitative Aussage treffen, aber glaube jetzt schon, dass ihr, zumindest für die identifizierten Domains für die ihr Mails schreibt, noch den IPv6-Dienst hätten prüfen sollen. Das schließt natürlich nicht aus, dass es eine andere mögliche Art zu verbinden gibt, bei der der SSHFP korrekt wäre [z.B. "interne" domains die extern anders auflösen], aber es reduziert die Chance schonmal. Habt ihr eigentlich auch SSHFP-Records gefunden, zu denen auf der IP überhaupt kein SSH-Server geantwortet hat?)

Wir hatten ja auch eine kurze Diskussion, was genau das Ziel der Informationsemail war. Die typische Abschätzung wann man so eine Mail sendet, wäre ja:

- Wir glauben, dass die Arbeitszeit, sich mit diesen E-Mails zu beschäftigen, die Erhöhung der Sicherheit "im Schnitt" wert ist. D.h. z.B. die Quote von "false positives" ist so gering, dass wir glauben, der gesamte Nutzen für alle Informierten überwiegt weit gegenüber ihrer verwendeten Arbeitszeit (Weil wir ja hier die Arbeitszeit der Leute mit "false positives" indirekt dazu verwendet wird, die Sicherheit anderer zu erhöhen, denke ich, dass hier der Vorteil stark überwiegen muss).

So eine Abschätzung kann man ja an einer Stichprobe versuchen zu validieren/plausibilisieren, bevor man Mails an alle schickt.

Ich mir nicht mehr sicher, was genau eure Antwort darauf war, welches Ziel die Informationsmail genau verfolgt. Hier mal mögliche Ziele:

- (Mail-Ziel 1) Wir wollen die Sicherheit von SSH-Nutzern dieser Dienste gegen MitM Angriffe erhöhen. Die Tatsache, dass bereits ein SSHFP-Record vorhanden ist, legt

nahe, dass diese Nutzer die SSHFP-Konfiguration beeinflussen können, und nach Anpassung von einer korrekten SSHFP-Konfiguration profitieren würden. Das sorgt nach dem "allgemeinen Ziel" für eine positive Abschätzung des Sicherheitsgewinns, da wir davon ausgehen, dass viele der angeschriebenen Nutzer daraus einen Sicherheitsgewinn ableiten.

- (Mail-Ziel 2) Wir wollen die Sicherheit von SSH-Nutzern dieser Dienste gegen MitM Angriffe erhöhen, indem wir Administratoren darauf hinweisen, dass ein Sicherheitsmechanismus, auf den sie sich möglicherweise verlassen, nicht so funktioniert wie sie denken (und möglicherweise ihre Sicherheit schwächt, anstatt sie zu stärken). Dadurch können sie das Sicherheitsbedürfnis ihrer Anwendung neu evaluieren, und entscheiden welche Schritte hier am passendsten sind (ob sie die Konfiguration anpassen oder entfernen, Schulung/Information für ihre Nutzer/...). Die Erhöhung des Sicherheitsniveaus derer, die erkennen, dass die Konfiguration nicht so ist, wie sie sich das vorstellen, ist den gesamten Arbeitsaufwand wert.

Ich glaube, ihr hattet euer Ziel für die Informationsmail anders formuliert (vielleicht näher an Mail-Ziel 2?), daher würde mich hier noch interessieren, wie genau ihr das Ziel der Mail formulieren würdet, und wie ihr basierend darauf zu der Entscheidung kommt, dass hier eine automatisierte Mail an alle gerechtfertigt ist. Aus der Tatsache, dass ihr Personen aus dem Impressum angeschrieben würde ich aber eher vermuten, dass "Mail-Ziel 1" beabsichtigt war, denn damit erreicht man ja eher "Inhaltlich verantwortliche" und nicht unbedingt "Technisch verantwortliche".

Sorry, dass es so viel Text geworden ist.

Viele Grüße,  
[Vorname, anonymisiert]

*# Response 14 [2024-03-22, 12:46]*

*Hallo [Vorname, anonymisiert],*

*Danke noch einmal für deine ausführliche Nachricht, ich habe unten mal unsere Antworten formuliert.*

*Ich hoffe, damit können wir die alle deine Fragen beantworten.*

*Beste Grüße,*



Vor allem in Situationen in denen viele Leute auf viele verschiedene Hosts zugreifen (z.B. ein Rechencluster), ist wohl "Ziel 1" das passendste. Wenn nur wenige Leute sich mit demselben Server häufiger verbinden, dann trifft wohl "Ziel 3" zu. Seid ihr von einem dieser Sicherheitsziele (oder einem anderen) ausgegangen, bei der Überlegung, wie Leute SSHFP in ihrem client konfigurieren?

*Prinzipiell sind alle Ziele denkbar. Da die Konfigurationen, wie du ja selbst weißt, sehr*



*individuell sein können, haben wir uns da vorher nicht festgelegt. Unser primäres Ziel war erst einmal, die Betroffenen über die mögliche Fehlkonfiguration zu informieren.*

Was genau ein nicht-passender SSHFP/eine fehlende DNSSec-Signatur für den Nutzer bedeutet, hängt von der lokalen Konfiguration ab. Sollten Nutzer aber trotz diese nicht-zusammenpassenden Konfiguration die Verbindung aufbauen, ist sie (bei VerifyHostKeyDNS) aber nicht von einem Angriff zu unterscheiden. D.h. wenn Nutzer sich trotz dieser nicht-zusammenpassenden-Konfiguration mit dem SSH-Dienst verbinden, dann würden sie das auch tun, wenn ein Angriff vorliegt. Daraus schließe ich, dass wenn hier ein Problem vorliegt, es auf jeden Fall nicht nur ein Konfigurationsproblem des Servers ist, sondern auch ein Konfigurationsproblem der Clients.

*Spannende Zusammenstellung, werden wir im Kopf behalten.*

(Ich habe übrigens inzwischen von einigen weiteren Leuten erfahren, die tatsächlich eine ähnliche Konfiguration verwenden wie wir, also verschiedene SSH-Dienste per IPv6 und IPv4 erreichbar machen. Dabei läuft auf IPv4 nicht unbedingt ein Honeypot, wie bei uns, sondern z.B. auch Weiterleitungen zu anderen, internen SSH-Servern, o.ä. So wie ich diese Personen verstanden habe, haben sie euch aber keine Rückmeldung gegeben. Ich kann natürlich keine quantitative Aussage treffen, aber glaube jetzt schon, dass ihr, zumindest für die identifizierten Domains für die ihr Mails schreibt, noch den IPv6-Dienst hätten prüfen sollen.

*Das Prüfen von IPv6 war aus technischen Gründen nicht möglich, da unsere Research Sever das nicht unterstützt haben. Diese Limitation ist uns bewusst und wir werden das entsprechend diskutieren.*

Das schließt natürlich nicht aus, dass es eine andere mögliche Art zu verbinden gibt, bei der der SSHFP korrekt wäre [z.B. "interne" domains die extern anders auflösen], aber es reduziert die Chance schonmal. Habt ihr eigentlich auch SSHFP-Records gefunden, zu denen auf der IP überhaupt kein SSH-Server geantwortet hat?)

*Ja, das haben wir. Im Rahmen dieser Studie waren diese Ergebnisse aber nicht relevant für uns, deshalb haben wir da aktuell keine Zahlen zu.*

Wir hatten ja auch eine kurze Diskussion, was genau das Ziel der Informationsemail war. Die typische Abschätzung wann man so eine Mail sendet, wäre ja:  
- Wir glauben, dass die Arbeitszeit, sich mit diesen E-Mails zu beschäftigen, die Erhöhung der Sicherheit "im Schnitt" wert ist. D.h. z.B. die Quote von "false positives" ist so gering, dass wir glauben, der gesamte Nutzen für alle Informierten überwiegt weit gegenüber ihrer verwendeten Arbeitszeit (Weil wir ja hier die Arbeitszeit der Leute mit "false positives" indirekt dazu verwendet wird, die Sicherheit anderer zu erhöhen, denke ich, dass hier der Vorteil stark überwiegen muss).

So eine Abschätzung kann man ja an einer Stichprobe versuchen zu validieren/plausibilisieren, bevor man Mails an alle schickt.

*Interessante Herangehensweise. Auch hier war es aufgrund der individuellen Möglichkeiten und Einschätzungen unser primäres Ziel, Awareness zu schaffen, dass möglicherweise ein Problem vorliegt. Eine Kalkulation, wie du sie vorschlägst ist in diesem Zusammenhang wenig sinnvoll, da ggf. die Bedrohungslage und damit der Nutzen unserer Nachricht individuell anders eingeschätzt wird.*

Ich glaube, ihr hattet euer Ziel für die Informationsmail anders formuliert (vielleicht näher an Mail-Ziel 2?), daher würde mich hier noch interessieren, wie genau ihr das Ziel der Mail formulieren würdet, und wie ihr basierend darauf zu der Entscheidung kommt, dass hier eine automatisierte Mail an alle gerechtfertigt ist. Aus der Tatsache, dass ihr Personen aus dem Impressum angeschrieben würde ich aber eher vermuten, dass "Mail-Ziel 1" beabsichtigt war, denn damit erreicht man ja eher "Inhaltlich verantwortliche" und nicht unbedingt "Technisch verantwortliche".

*Siehe oben, unser Ziel war es, primär erst einmal Awareness zu schaffen. Wir hatten ja auch schon gesagt, dass wir jede mögliche Aktion oder Nicht-Aktion als Ergebnis gleichwertig sehen. Bezüglich der Kontaktdaten haben wir uns an vorangegangene Arbeiten orientiert, in denen gezeigt wurde, dass durch manuelle Adressdatensuche (z.B. im Impressum) Bounces verringert [1] und E-Mail-Zustellungen verbessert werden [2, 3], während generierte Kontaktdaten [4, 5] oder WHOIS Daten (nicht mehr verfügbar) [1, 4, 6] weniger effektiv sind.*

[1] Ben Stock, Giancarlo Pellegrino, Frank Li, Michael Backes, and Christian Rossow. Didn't You Hear Me? - Towards More Successful Web Vulnerability Notifications. In Proceedings of the 25th Annual Symposium on Network and Distributed System Security (NDSS '18), pages 1 – 15, 2018.

[2] Anne Hennig, Heike Dietmann, Franz Lehr, Miriam Mutter, Melanie Volkamer, and Peter Mayer. "Your Cookie Disclaimer is Not in Line with the Ideas of the GDPR. Why?". In Human Aspects of Information Security and Assurance (HAISA 2022), volume 658 of IFIP Advances in Information and Communication Technology, pages 218–227, Cham, 2022. Springer.

[3] Max Maass, Alina Stöver, Henning Pridöhl, Sebastian Bretthauer, Dominik Herrmann, Matthias Hollick, and Indra Spiecker. Effective notification campaigns on the web: A matter of Trust, Framing, and Support. In 30th USENIX Security Symposium (USENIX Security 21), pages 2489–2506. USENIX Association, 2021.

[4] Ben Stock, Giancarlo Pellegrino, Christian Rossow, Martin Johns, and Michael Backes. Hey, You Have a Problem: On the Feasibility of Large-Scale Web Vulnerability Notification. In 25th USENIX Security Symposium (USENIX Security 16), pages 1015–1032, Austin, TX, 2016. USENIX Association.

[5] Orcun Cetin, Mohammad Hanif Jhaveri, Carlos Ganan, Michel van Eeten, and Tyler Moore. Understanding the role of sender reputation in abuse reporting and cleanup. Journal of Cybersecurity, 2(1):83–98, 2016.

[6] Eric Zeng, Frank Li, Emily Stark, Adrienne Porter Felt, and Parisa Tabriz. Fixing HTTPS Misconfigurations at Scale: An Experiment with Security Notifications. In The 2019 Workshop on the Economics of Information Security (2019), pages 1 – 19, Boston, MA, 2019.

ID: 32

Group: [REDACTED]

E-Mail sent: 06-03-2024, 12:55

Response to: first email / reminder

Date: 06-03-2024, 20:41

Respondent: male

# Response 1

Guten Abend [REDACTED],

vielen Dank für Ihre Nachricht. Mir ist bewusst, dass der SSHFP-Einsatz für besagten DNS-Record nicht vollständig den Ausführungen aus RFC 4255 entspricht, da die relevante DNS-Zone [Subdomain, anonymisiert] nicht mit DNSSEC abgesichert ist. Die Einführung von DNSSEC ist beabsichtigt, jedoch aufgrund unserer Stellung als ehrenamtliches Projekt von [Berufsbezeichnung, anonymisiert] aufgrund der Risiken bei Fehlkonfiguration sowie geringere Prioritäten im Vergleich zu anderen Aufgaben, aber noch nicht umgesetzt worden.

Für Nachfragen stehen ich ihnen gern zur Verfügung.

Beste Grüße / Best Regards

[Vorname Nachname, anonymisiert]

# Response 2 [2024-03-07, 09:37]

ID: 33

Group: 

E-Mail sent: 06-03-2024, 12:44

Response to: first email / reminder

Date: 06-03-2024, 14:12

Respondent: male

# Response 1


Eine sehr ungewöhnliche Mail :D

Etwas irreführend, da für [Subdomain, anonymisiert] die Verifizierung nicht fehlschlägt, sondern einfach die SSHFP records absichtlich nur für SHA256 und ed25519 gesetzt sind.

Viele Grüße,  
[Vorname Nachname, anonymisiert]

*# Response 2 [2024-03-07, 09:39]*

ID: 34

Group: 

E-Mail sent: 06-03-2024, 12:44

Response to: first email / reminder

Date: 06-03-2024, 22:08

Respondent: male

# Response 1

Wow, vielen Dank!

Ich habe mit der Einrichtung von DNSSec mit PowerDNS begonnen, dann ist beim automatischen synchronisieren zwischen meinen eigenen DNS-Servern irgendwas schief gelaufen und ich habe schon länger auf der TODO-Liste einmal zu verstehen, wie das eigentlich genau funktioniert mit dem DNS signieren.

Mir ist nur nicht ganz klar wie man meine SSH keys dadurch klauen könnte? Dann müsste ich doch in einem Netzwerk sein, in dem ein DNS Server die Anfragen an meinen eigenen Server manipuliert (was nicht passiert, weil mein Rechner über VPN namen auf dem Server auflöst). Oder gibt es noch ein anderes Angriffsszenario?

Beste Grüße und Danke nochmal

[Vorname Nachname]

*# Response 2 [2024-03-07, 12:31]*

ID: 35

Group: [REDACTED]

E-Mail sent: 06-03-2024, 13:10

Response to: first email / reminder

Date: 06-03-2024, 22:08

Respondent: male

# Response 1

Guten Tag [REDACTED],

On 6. Mar 2024, at 13:10, [REDACTED] wrote:

*Im Rahmen eines Forschungsprojekts identifizieren wir Fehlkonfigurationen in Zusammenhang mit Ihrer DNS-Infrastruktur.*

dürfte ich hier nach Hintergründen fragen? Insbesondere überrascht mich die persönlich/manuell verschickte Mail und die Formulierung "Ihrer DNS-Infrastruktur". Ist an meiner Infrastruktur etwas Besonderes, oder wie bin ich in den Fokus dieses Forschungsprojektes geraten? :-)

*Im Rahmen unserer Untersuchung haben wir festgestellt, dass die von Ihnen gesetzten Einträge nicht korrekt konfiguriert sind. Hierbei gibt es 2 mögliche Szenarien:*

Ich kenne zwar das Ziel des Forschungsprojektes nicht, aber die Hintergründe könnten für Sie interessant sein: Die veröffentlichten Einträge sind durchaus korrekt – jedoch nicht für den SSH-Dienst, der auf Port 22 erreichbar ist (SSHFP-Einträge sehen leider keine Angabe des TCP-Ports vor).

Viele Grüße aus [Stadtname, anonymisiert]  
[Vorname Nachname, anonymisiert]

PS: Ich freue mich über alle Projekte, die der Verbreitung von DNSSEC zuträglich sind. Wenn ich unterstützen kann ...

# Response 2 [2024-03-06, 16:13]

Hallo Herr [Nachname, anonymisiert],

vielen Dank für Ihre Rückmeldung und Ihren Hinweis!

*Sie haben Recht, die Formulierung ist tatsächlich etwas zu spezifisch. Ihre Infrastruktur konkret weist lediglich Merkmale der Fehlkonfiguration auf, die wir bei mehreren Domains finden konnten. In der Arbeit von Neef et al. [1] wurde das bereits für Domains weltweit untersucht. Unser Ziel ist es nun, die Betroffenen darüber zu informieren und generell zu untersuchen, wie wir solche Benachrichtigungen und Benachrichtigungen zu Schwachstellen im Allgemeinen möglichst effektiv gestalten können.*

*Daher sind wir natürlich über Hinweis jeder Art dankbar, insbesondere auch Ihre Erläuterung. Da wir nur auf Port 22 getestet haben, sind uns die anderen Einträge entgangen.*

*Beste Grüße,*



*# Response 3 [2024-03-06, 16:15]*

*Ah, sorry, Link zum Paper fehlte...*

*Anbei: <https://arxiv.org/abs/2208.08846>*

*# Response 4 [2024-03-06, 17:04]*

*Hallo* 

*danke für die schnelle Antwort!*

*Bezüglich "Benachrichtigungen zu Schwachstellen im Allgemeinen" fällt mir spontan das CERT-BUND (BSI) ein, das vergleichbare Sicherheitsbenachrichtigungen (verdächtige offene Ports etc.) regelmäßig an AS-Betreiber sendet. Vielleicht ist ein Erfahrungsaustausch ja interessant.*

*[https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/cert-bund\\_node.html](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/cert-bund_node.html)*

*Viele Grüße*

*[Vorname Nachname, anonymisiert]*

*# Response 5 [2024-03-06, 17:04]*

*Hallo Herr [Nachname, anonymisiert],*

*ja, mit dem CERT Bund sind wir tatsächlich schon im Rahmen von einem anderen Projekt in Kontakt :) Wir verstehen natürlich, dass es für Behörden immer schwierig ist, „auf Zuruf“ solche Schwachstellenbenachrichtigungen auszusenden, aber wir hoffen, dass wir mit unserer Forschung hier gezielt Hinweise liefern können. Aber danke für den Tipp! Haben Sie hier konkrete Erfahrung mit dem Melden oder Empfangen anderer Schwachstellen gemacht? Ich habe - leider - die Erfahrung gemacht, dass weniger technisch versierte Betroffene mit dem CERT Bund als Absender teilweise nichts anfangen können. Daher nur aus Interesse die Frage, was Ihre Verbindung ist.*

*Beste Grüße,*

*Anne Hennig*

# Response 6 [2024-03-07, 07:02]

Guten Morgen [REDACTED],

*On 6. Mar 2024, at 17:04, [REDACTED] wrote:  
Haben Sie hier konkrete Erfahrung mit dem Melden oder Empfangen anderer  
Schwachstellen gemacht? Ich habe - leider - die Erfahrung gemacht, dass weniger  
technisch versierte Betroffene mit dem CERT Bund als Absender teilweise nichts  
anfangen können. Daher nur aus Interesse die Frage, was Ihre Verbindung ist.*

ich habe auch beruflich viel mit IT-Sicherheit zu tun; insbesondere war ich früher bei einem Managed Hosting-Anbieter für die Technik mitverantwortlich, und in dem Rahmen auch für die Bearbeitung der Meldungen vom CERT-Bund und anderen Quellen, sowie Umsetzung von BSI/IT-Grundschutz etc. -- und zufälligerweise haben wir auch einige Jahre lang das Webhosting für cert-bund / WID betrieben.

Zur Bearbeitung der Meldungen gehörte auch die Beurteilung und ggf. das Weitermelden an unsere betroffenen Kunden; im Rahmen einer bestehenden Geschäftsbeziehung ist das deutlich einfacher als ein "cold call" von unbekanntem E-Mail-Absender.

Der Vorteil bei der aggregierten Meldung an AS-Betreiber ist natürlich, dass "weniger technisch versierte" Empfänger sehr unwahrscheinlich sind, da nur sehr wenige Privatpersonen ein eigenes AS betreiben. Bei Privatpersonen ist das wohl schwieriger. Ist Ihre Sorge, dass solche Empfänger die Meldungen eher als Spam abtun und ignorieren?

Viele Grüße  
[Vorname Nachname, anonymisiert]

# Response 7 [2024-03-07, 13:00]

Hallo Herr [Vorname, anonymisiert],

*ja, sehr spannend!  
Und ja, ich denke, die Gefahr, als Spam betrachtet zu werden ist auf jeden Fall da. Mein aktuelles Forschungsinteresse besteht aktuell darin, wie wir es schaffen können, den „täglichen Spam“ zu durchdringen. Wir haben das Problem bereits in anderen Settings untersucht und sehen natürlich auch, dass eine (mehr oder weniger persönliche) Beziehung zum Absender die Behebungsraten deutlich erhöht. Leider ist das etwas, was man nur schwer übertragen kann. Daher wäre die Frage, was man (noch) tun kann. Ich bin aktuell daran, alle „losen Enden“ zusammenzufassen und bin gespannt, ob wir am Ende eine Liste mit Empfehlungen haben oder eher eine Liste voller Parameter, die nicht wirksam sind.*

Beste Grüße,  
[REDACTED]



# Response 8 [2024-03-07, 13:29]

Hallo [REDACTED],

*On 7. Mar 2024, at 13:00, [REDACTED] wrote:  
Ich bin aktuell daran, alle „losen Enden“ zusammenzufassen und bin gespannt, ob wir  
am Ende eine Liste mit Empfehlungen haben oder eher eine Liste voller Parameter, die  
nicht wirksam sind.*

das Ergebnis wäre natürlich auch für Benachrichtigungen an Kunden spannend.  
Vielleicht denken Sie ja an mich, wenn die Ergebnisse vorliegen :-)

Danke für den angenehmen Austausch und viele Grüße  
[Vorname Nachname, anonymisiert]

# Response 9 [2024-03-07, 14:02]

*Sehr gerne! Und danke Ihnen auch :)*

ID: 36

Group: [REDACTED]

E-Mail sent: 2024-03-06, 12:55

Response to: first email / reminder

Date: 2024-03-07, 13:38

Respondent: female

# Response 1

Liebe [REDACTED],

vielen Dank für Ihre ausführliche Rückmeldung. Diese Seite ist gar nicht mehr in Benutzung, erstaunlich, dass Sie darauf gestoßen sind.

Unser Programmierer nimmt sie nun ganz vom Netz.

Vielen Dank für Ihre Mühe und allerbeste Grüße  
[Vorname Nachname, anonymisiert]

*# Response 2 [2024-03-07, 14:04]*

ID: 37

Group: [REDACTED]

E-Mail sent: 2024-03-06, 12:35

Response to: first email / reminder

Date: 2024-03-07, 14:18

Respondent: male

# Response 1

Guten Tag [REDACTED],

vielen Dank für den Hinweis. Wir werden der Sache nachgehen. Uns stellt sich noch die Frage wie Sie auf die Domain gekommen sind, da diese eigentlich nicht öffentlich zugänglich sind.

Des Weiteren hatten Sie noch 2 weitere Domains in Ihrer E-Mail erwähnt – können Sie uns sagen um welche es sich handelt?

Mit freundlichen Grüßen

[Vorname Nachname, anonymisiert]

[Berufsbezeichnung, anonymisiert]

# Response 2 [2024-03-07, 14:51]

Hallo Herr [Nachname, anonymisiert],

vielen Dank für Ihre Rückmeldung!

*Ihre Fragen will ich Ihnen gerne beantworten.*

*Finden: Wir haben aus verschiedenen, öffentlichen Quellen Domains mit deutscher Top-Level-Domain (".de") gesammelt (u.a. Censys Certificate Dataset [1], CertStream [2]). Insgesamt konnten wir so 27.5 Millionen aktiv genutzte deutsche Domains inklusive Subdomains ermitteln.*

*Weitere Domains: Aus Gründen der Lesbarkeit haben wir maximal 4 Subdomains dargestellt. In Ihrem Fall wären das noch [Subdomain1] und [Subdomain2].*

*Melden Sie sich gerne, wenn Sie noch Fragen haben!*

*Beste Grüße,*

[REDACTED]

[1] <https://support.censys.io/hc/en-us/articles/360038761891-Research-Access-to-Censys-Data>

[2] <https://certstream.calidog.io/>

# Response 3 [2024-03-07, 15:44]

Hallo .

vielen Dank für die schnelle Rückmeldung und die Auskunft! Wir werden uns um die notwendigen Schritte kümmern.

Mit freundlichen Grüßen

[Vorname Nachname, anonymisiert]

[Berufsbezeichnung, anonymisiert]

ID: 38

Group: [REDACTED]

E-Mail sent: 2024-03-06, 12:32

Response to: first email / reminder

Date: 2024-03-08, 09:36

Respondent: male

# Response 1

Hallo [REDACTED],

vielen Dank fuer den Hinweis.

Die detektierte Fehlkonfiguration werden wir schnellstmoeiglich beseitigen.

MfG

[Vorname Nachname, anonymisiert]

# Response 2 [2024-03-08, 09:42]

ID: 39

Group: [REDACTED]

E-Mail sent: 2024-03-06, 12:47

Response to: first email / reminder

Date: 2024-03-06, 18:25

Respondent: male

#### # Response 1

Hallo,

On 3/6/24 12:47, [REDACTED] wrote:

dabei handelt es sich um eine geduldete Fehlkonfiguration:

Spielwiesendomain, d.h. nicht produktiv. DNSSEC ist nicht implementiert.

Die betroffenen Server akzeptieren nur SSH Public Key Auth in Kombination mit MFA, sodass ich das Risiko bzgl. MITM-Szenarien für minimal halte.

Wird es später eine Veröffentlichung zu der Studie geben?

Weil ich werde aus der Motivation noch nicht so ganz schlau:

- Fokus der Studie liegt eher auf Benachrichtung?

Dann wäre natürlich interessant, ob und wie ich trotz Ignoranz

bzgl. der gemeldeten Schwachstelle den Test (nicht) bestanden habe ;-)

- oder doch Evaluation Sicherheitsniveau? SSHFP ist meinem Kenntnisstand nach aber eher eine Nischenlösung und nicht breitflächig umgesetzt.

Anmerkungen zu der FAQ-Seite:

\* "Wieso haben Sie mich angeschrieben?"

Die Antwort stimmt meistens, aber für die Domain [Domainname, anonymisiert] nicht.

Es gibt keinen Webauftritt und kein Impressum.

Vermutlich war es hier der laut DNS Zoneneintrag

verantwortliche Ansprechpartner (RFC1035, SOA RNAME).

\* "Wie wurde meine Domain gefunden?"

Daraus wird nicht so ganz klar, welche Beschaffenheit die verwendeten

Ausgangsdatensätze hatten. Es würde mich überraschen, wenn die Domain

[Domainname, anonymisiert] eine der Top Domains ist. Wortgenerator könnte ich mir eher vorstellen.

Gruß

[Vorname Nachname, anonymisiert]

# Response 2 [2024-03-06, 20:25]

Hallo Herr [Nachname, anonymisiert],

*vielen Dank für Ihre Rückmeldung und die Erklärung.*

*Wir können ja nur ein bestimmtes Verhalten beobachten und wissen ja nicht, aus welchem Grund dieses Verhalten besteht. Solche zusätzlichen Informationen helfen uns daher sehr!*

*Veröffentlichung: Ja, eine Veröffentlichung der Ergebnisse ist geplant. Wenn Sie das möchten, können wir Sie gerne informieren, was unsere Ergebnisse sind.*

*Motivation: In erster Linie geht es uns tatsächlich darum, wie die Betroffenen mit unserer Benachrichtigung umgehen, bzw. darauf reagieren. Entsprechend wollen wir eigentlich mehr lernen, ob wir „bestanden“ haben und Sie entsprechend mit unseren Informationen etwas anfangen konnten ;) In Ihrem Fall hilft Ihre Antwort uns sogar zusätzlich dabei, zu verstehen, warum Betroffene ggf. keine Änderungen vornehmen.*

*Vielen Dank auf für Ihre Anmerkungen zu unserer FAQ-Seite. Wenn wir - wie in Ihrem Fall - die Informationen nicht aus dem Impressum nehmen konnten, haben wir uns am RFC 2142 orientiert und hostmaster@DOMAIN angeschrieben. Das müssen wir ergänzen! Was das Finden betrifft: Hier haben wir aus verschiedenen öffentlichen Quellen versucht, möglichst alle Domains mit TLD „de“ zu sammeln. Wir haben uns also explizit nicht auf z.B. die Top-1M beschränkt, damit unser Sample möglichst repräsentativ ist. Auch hier sollten wir am besten die Formulierung anpassen.*

*Ich kann mich nur noch einmal bei Ihnen für die sehr nette Rückmeldung und das Feedback bedanken. Sollten noch Fragen aufkommen oder offen geblieben sein, melden Sie sich gerne!*

*Beste Grüße,*



# Response 3 [2024-03-09, 15:17]

Hallo .

On 3/6/24 20:25,  wrote:

Hallo Herr [Nachname, anonymisiert],

*vielen Dank für Ihre Rückmeldung und die Erklärung.*

*Wir können ja nur ein bestimmtes Verhalten beobachten und wissen ja nicht, aus welchem Grund dieses Verhalten besteht. Solche zusätzlichen Informationen helfen uns daher sehr!*


*Veröffentlichung: Ja, eine Veröffentlichung der Ergebnisse ist geplant. Wenn Sie das möchten, können wir Sie gerne informieren, was unsere Ergebnisse sind.*

ja, gerne!

Gruß

[Vorname Nachname, anonymisiert]

ID: 40

Group: 

E-Mail sent: 2024-03-06, 13:11

Response to: first email / reminder

Date: 2024-03-10, 21:44

Respondent: male

# Response 1

Guten Abend 

vielen Dank für Ihren Einsatz für ein sichereres Internet :-)

Mir hätte es geholfen, direkt eine Mail mit entweder nur 1) oder 2) gesendet zu bekommen, da dadurch eine weitere Analyse der Fehlerursache überflüssig wäre.

Weiterhin hätte ich mich über einen kurzen Kommandozeilenbefehl oder einen Link zu einem Webtool gefreut, mit dem die Fehlkonfiguration direkt nachvollziehbar und nach Behebung auch die Korrekturbar überprüfbar geworden wäre.

In meinem Fall habe ich jetzt bspw. die Einträge mit den Werten aktualisiert, die ssh-keyscan -D [Domainname, anonymisiert] ausgespuckt hat. Offensichtlich sind dies aber die gleichen Werte, die auch vorher im DNS standen. Es kann also nur 2) die Fehlerursache sein - eine Abfrage via delv sshfp [Domainname, anonymisiert] gibt mit aber auch "fully validated" aus. Entweder war DNSSEC aus irgend einem Grund temporär kaputt, oder ich prüfe die Konfiguration falsch.

Viele Grüße

[Vorname Nachname, anonymisiert]

# Response 2 [2023-03-11, 14:14]

Hallo Herr [Nachname, anonymisiert],

*vielen Dank für Ihre Rückmeldung und Ihre wertvollen Hinweise! Das werden wir gerne mit aufnehmen.*

*Zu Ihrer Frage: Auf Ihre Domain trifft Szenario 1 zu. Wir schauen uns Ihren Fall aber noch einmal genauer an, ggf. liegt auch ein Fehler unsererseits vor. Mein Kollege, der unsere Logs überwacht, ist allerdings gerade verhindert, es kann daher sein, dass wir erst gegen Ende der Woche genauere Ergebnisse haben. Ich melde mich auf jeden Fall noch einmal bei Ihnen!*

*Beste Grüße,*





ID: 41

Group: [REDACTED]

E-Mail sent: 2024-03-06, 12:31

Response to: first email / reminder

Date: 2024-03-11, 11:41

Respondent: male

# Response 1

On 3/6/24 12:31, [REDACTED] wrote:

*Im Rahmen eines Forschungsprojekts identifizieren wir Fehlkonfigurationen in Zusammenhang mit Ihrer DNS-Infrastruktur. # Was ist das (Problem)? Sie setzen auf den folgenden Domains DNS-Einträge vom Typ SSHFP, um DNS-basierte HostKey-Verifizierung für SSH zu nutzen: grid.rrze.uni-erlangen.de 1) Die HostKey-Fingerabdrücke in den SSHFP DNS-Einträgen stimmen nicht mit den tatsächlichen HostKeys bzw. HostKey-Fingerabdrücken von dem SSH-Server überein.*

Danke fuer den Hinweis, die fehlerhaften Eintraege fuer [Subdomain 1, anonymisiert] / [Subdomain 2, anonymisiert] wurden korrigiert.

Entstanden sind sie uebrigens durch einen kaputten Automatismus, der faelschlicherweise die Eintraege erzeugt und dann aber nie mehr aktualisiert hat.

Gruss,

[Signatur, anonymisiert]

# Response 2 [2024-03-11, 14:16]

ID: 42

Group: [REDACTED]

E-Mail sent: 2024-03-06, 12:42

Response to: first email / reminder

Date: 2024-03-12, 13:34

Respondent: male

# Response 1

Guten Morgen [REDACTED],

Vielen Dank für Ihre Meldung! Wir haben die gemeldeten Probleme geprüft und kommen zu einem anderen Schluss und sehen nicht dass wir angreifbar sind, nehmen uns aber durchaus einige ToDos zum Verbessern unseres Standings mit.

Zu aller erst: Wir sehen keine Angreifbarkeit, da wir zwar SSHFP records auf diesen Hostnamen haben, diese aber nicht verwenden. Für Kommunikation mit diesen Hosts über SSH verwenden wir den selben Namen, nur in der [Domainname, anonymisiert] Zone statt in [Domainname, anonymisiert]. Dort liegen die selben SSHFP records, dort werden die records aber mit DNSSEC abgesichert. Um diesen Irrtum zu vermeiden, hätten wir die records aber ausschließlich in der [Domainname, anonymisiert] Zone setzen sollen. Das konnten Sie aber natürlich nicht Wissen, also geht dieses Missverständnis vollständig auf unsere Kappe.

Bezüglich der nicht übereinstimmenden HostKeys bzw HostKey-Fingerabdrücken: Die SSH keys auf dem Host stimmen überein. Die drei Records die gesetzt sind sind korrekt. Gesetzt sind nur SHA256 hashes der public keys, vom SSH Server werden auch SHA1 hashes zurück gegeben. Dadurch kommt die Übereinstimmung von nur 3/6 Fingerabdrücke zustande. Das ist jedoch kein Sicherheitsproblem. Wir werden hier im SSH Server explizit SHA1 abschalten, dass der SSH Server keine Fingerabdrücke zurück liefert die nicht über die SSHFP records verifiziert werden können. Hier bin ich der Meinung, dass der Security Check nicht korrekt ist: Jeder Key der vom Server zurück gegeben wurde, konnte mit SHA256 verifiziert werden, das sollte das Tool meiner Meinung nach nicht als Problem werten.

Ein Anliegen hätte ich noch: Derartige Meldungen von Sicherheitsforschenden erhalten wir i.d.R. über security@[Domainname, anonymisiert].com und nicht info@[Domainname, anonymisiert].com. Diese E-Mail Adresse bewerben wir gemäß RFC 9116 auch unter [https://\[Domainname, anonymisiert\]/.well-known/security.txt](https://[Domainname, anonymisiert]/.well-known/security.txt). Ist dieser Standard so wenig verbreitet, dass es sich nicht lohnt zu prüfen ob Unternehmen eine security.txt ausliefern?

Zu guter letzt: Vielen Dank für ihr Arbeit in diesem Bereich! Trust on first use ist für SSH Verbindungen leider viel zu verbreitet, und ich bin froh, dass hier Forschung zur Verbreitung und korrekten Nutzung von Sicherheitsmechanismen durchgeführt wird.

Ich wurde letzts auf eine Alternative zu SSHFP + DNSSEC aufmerksam gemacht: <https://codeberg.org/wiktor/ssh-openpgp-auth>. Dieses Projekt nutzt OpenPGP

Zertifikate für die Validierung von SSH Host Keys. Das kann für Unternehmen die sich vor der Verwendung von DNSSEC sträuben eine potentiell einfacher umzusetzende Alternative sein.

Mit freundlichen Grüßen  
[Name Vorname, anonymisiert]

*# Response 2 [2024-03-12, 16:38]*

ID: 43

Group: [REDACTED]

E-Mail sent: 2024-03-06, 12:31

Response to: first email / reminder

Date: 2024-03-26, 12:34

Respondent: male

# Response 1

Sehr geehrte [REDACTED],

die Problematik (es ist das Szenario 2) ist bekannt. Die Zone [Subdomain, anonymisiert] <http://[Subdomain, anonymisiert]/> ist mit DNSSEC abgesichert -- die Zone[Domain, anonymisiert] <http://[Domain, anonymisiert]/> aber leider nicht.

Die Personen, die auf diese(n) Rechner zugreifen haben entweder den Schlüssel für [Subdomain, anonymisiert] <http:// [Subdomain, anonymisiert]/> als vertrauenswürdig konfiguriert oder verlassen sich auf OpenSSH, wo SSHFP Schlüssel ohne DNSSEC nicht ohne Nachfrage akzeptiert werden.

Gruß,

[Signatur, anonymisiert]

# Response 2 [2024-03-26, 21:01]

Guten Tag Herr [Nachname, anonymisiert],

*vielen Dank für Ihre Rückmeldung! Es ist für uns immer sehr interessant, zusätzliche Informationen zu bekommen, die wir ja so aus den Daten nicht ablesen können. Mich würde aus Ihrer Antwort tatsächlich noch eine Sache interessieren: Gibt es einen Grund (den Sie mir nennen dürfen), warum [REDACTED] nicht durch DNSSEC abgesichert ist? Ist das eine bewusste Entscheidung oder einfach eine Ressourcen-/Zeitfrage?*

*Falls Sie im Gegenzug noch Fragen an mich haben - immer gerne!*

*Beste Grüße,*

[REDACTED]

# Response 3 [2024-03-27, 09:37]

Sehr geehrte [REDACTED],

die Zone [Domain, anonymisiert] <http://[Domain, anonymisiert]/> wird von unserem [Eigenname, anonymisiert]-IT-Zentrum ([E-Mail-Adresse, anonymisiert] <mailto: [E-Mail-Adresse, anonymisiert]>) betrieben. Vielleicht kann Ihnen da weitergeholfen werden.

Gruß,

[Signatur, anonymisiert]

# Response 4 [2024-03-27, 14:11]

*Vielen Dank!*

ID: 44

Group: [REDACTED]

E-Mail sent: 2024-03-27, 17:46

Response to: first email / reminder

Date: 2024-03-27, 18:46

Respondent: male

# Response 1

Sehr geehrte [REDACTED],

vielen Dank für den Hinweis, ich habe das an die DNS-Administration weitergegeben.


Da auf unserem SSH-Server Authentifikation via Paßwort generell deaktiviert ist, gehe ich jedoch nicht davon aus, daß das Risiko so hoch ist, wie von Ihnen dargestellt.

Sie haben uns im Übrigen auch diese Erinnerung für [Domainname, anonymisiert] geschickt, für diese Domain sind wir jedoch nicht verantwortlich.

Mit vielem Dank und freundlichen Grüßen  
[Vorname Nachname, anonymisiert]

# Response 2 [2024-03-27, 19:54]

ID: 45

Group: 

E-Mail sent: 2024-03-27, 17:26

Response to: first email / reminder

Date: 2024-03-27, 18:55

Respondent: male

# Response 1

Hi!

Besten Dank für den Hinweis.

Tatsächlich ist die Konfiguration korrekt. Aus Sicherheitsgründen läuft der ssh Server jedoch auf einem anderen Port als 22. auf Port 22 antwortet ein ssh Server, dieser läuft jedoch auf einer anderen Maschine die keine Daten hostet.

Viele Grüße,

[Vorname, anonymisiert]

# Response 2 [2024-03-27, 19:54]

ID: 46

Group: [REDACTED]

E-Mail sent: 2024-03-27, 17:31

Response to: first email / reminder

Date: 2024-03-28, 11:13

Respondent: male

# Response 1

Hallo [REDACTED],

Vielen Dank für die Mail. Die genannten DNS-Einträge sind allesamt CNAMEs auf einen Shared-Host des Anbieters [Anbietername, anonymisiert], den ich nicht selbst verwalte. Daher bin ich auch der falsche Ansprechpartner, da mir die Ziel-Domain nicht gehört.

Viele Grüße

[Vorname, anonymisiert]

# Response 2 [2024-03-28, 13:58]



ID: 47

Group: [REDACTED]

E-Mail sent: 2024-03-27, 17:28

Response to: first email / reminder

Date: 2024-03-28, 13:58

Respondent: male

# Response 1

Guten Tag [REDACTED],

besten Dank für den Hinweis, ich habe die SSHFP Einträge entfernt.

Mit freundlichen Grüßen

[Vorname Nachname, anonymisiert]

*# Response 2 [2024-03-28, 16:40]*

ID: 48

Group: [REDACTED]

E-Mail sent: 2024-03-27, 17:46

Response to: first email / reminder

Date: 2024-03-28, 15:49

Respondent: male

# Response 1

Sehr geehrte [REDACTED],

leider ist ihr Forschungsprojekt fehlerhaft. Ich habe SSHFP auf meinen Nameserver lediglich für eine einzige per DNSSEC abgesicherten Domain konfiguriert und dies auch nur für die zu den jeweiligen Servern zugordneten Subdomains:

```
$ host -a -t sshfp [Subdomain, anonymisiert]
```

```
Trying "[Subdomain, anonymisiert]"
```

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41023
```

```
;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 0
```

```
;; QUESTION SECTION:
```

```
; [Subdomain, anonymisiert].      IN      SSHFP
```

```
;; ANSWER SECTION:
```

```
[Subdomain, anonymisiert]. 300 IN      SSHFP 4 2
```

```
402E63D59A5B6F57DD837FFDADE6E6C9E23AF0125BD3E6E884921D93 E9406097
```

```
[Subdomain, anonymisiert]. 300 IN      SSHFP 1 1
```

```
F5782F88D6331CC6DEA4C46F7BE9FFF1C15022CD
```

```
[Subdomain, anonymisiert]. 300 IN      SSHFP 3 1
```

```
2CA4356249F7DF49380F3C1C455414B17042AAFE
```

```
[Subdomain, anonymisiert]. 300 IN      SSHFP 4 1
```

```
C6364E30CE149791A585B5D62914D10B7F25A448
```

```
[Subdomain, anonymisiert]. 300 IN      SSHFP 2 2
```

```
EE367B5F69576395EB2D81E25C595B95FFED634176882F20BCA214E9 327C830E
```

```
[Subdomain, anonymisiert]. 300 IN      SSHFP 1 2
```

```
20383EE306FF4FCA2ACB6152073A00AF151DD210285087594CE07D9E 4201A130
```

```
[Subdomain, anonymisiert]. 300 IN      SSHFP 3 2
```

```
0D2EBE1DC3F547AF93A16093FE3F355E2832622B25EE34360326AE69 DB571B9A
```

```
[Subdomain, anonymisiert]. 300 IN      SSHFP 2 1
```

```
83B2E205FD5014739CAE8B04AE8BC52FE92ABDBA
```

Für die Domains [Domainname, anonymisiert], [Domainname, anonymisiert], [Domainname, anonymisiert], [Domainname, anonymisiert], [Domainname, anonymisiert] und weitere, die sie in schöner Regelmäßigkeit mit „Spammails“ ;) überziehen ist \_kein\_ SSHFP konfiguriert:

```
$ host -a -t sshfp [Domainname, anonymisiert]
```

```
Trying "[Domainname, anonymisiert]"
```

:: ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25014  
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

:: QUESTION SECTION:  
; [Domainname, anonymisiert]. IN SSHFP

Ich bitte sie darum, von weiteren E-Mails zu Domains mit den Nameservern  
[Nameservername 1, anonymisiert] + [Nameservername 2, anonymisiert] abzusehen.

Mit freundlichen Grüßen  
[Vorname Nachname, anonymisiert]

*# Response 2 [2024-03-28, 16:48]*

ID: 49

Group: [REDACTED]

E-Mail sent: 2024-03-27, 17:46

Response to: first email / reminder

Date: 2024-04-02, 10:04

Respondent: male

# Response 1

Sehr geehrte [REDACTED],

vielen Dank für den super Service! Ich denke, ihr Skript könnte insofern verbessert werden, als dass es CNAMEs separat ausweist, weil jetzt sehr viele Virtual Hosts als betroffen gemeldet wurden, wobei es sich ja aber nur um einen Host handelt. (Vermutlich, es heißt ja nur "und [Anzahl Subdomains, anonymisiert] andere".)

Aber vielen Dank für Ihre Mitteilung, in der Tat schieben wir das Upgrade auf DNSSEC schon zu lange vor uns her...

Mit freundlichen Grüßen,

[Vorname Nachname, anonymisiert]

# Response 2 [2024-04-02, 10:37]

ID: 50

Group: [REDACTED]

E-Mail sent: 2024-03-27, 17:29

Response to: first email / reminder

Date: 2024-04-02, 10:04

Respondent: undefined

# Response 1

Guten Tag [REDACTED],

wir sind ein Verein ([Vereinsname, anonymisiert]). Unsere Mitglieder haben die Möglichkeit, Server einzurichten und dafür u.a. die Domain [Domainname, anonymisiert] zu nutzen. Das von Ihrer Recherche betroffene Mitglied ist der Meinung, sshfp korrekt eingerichtet zu haben.

DNSSEC haben wir für unsere Zone nicht eingerichtet, da wir die dafür erforderliche personelle Kapazität, Kontinuität und Dokumentation nicht gewährleisten können. Wer das heute einrichtet, könnte morgen weg sein.

Das Mitglied nutzt sshfp auf eigenes Risiko und weiß das auch. Ob wir DNSSEC machen oder nicht, diskutieren wir seit längerem. Im Moment haben wir andere Prioritäten.

Mit freundlichen Grüßen  
[Name, anonymisiert]

# Response 2 [2024-04-03, 09:39]