(/)

It's all about domains... mit Klaus Darilion von nic.at

25.06.2021

Was ist DNS Security und wie kann uns Technologie dabei helfen, eine Domain zu schützen? Heute beantwortet Klaus Darilion (nic.at) unsere Fragen, damit wir das beschützen können, was uns allen besonders am Herzen liegt: Domains!

Dank des DNS (Domain Name System), einem hierarchisch aufgebauten und dezentralisierten System, das numerische Informationen mit Domains (/fileadmin/_processed_/8/6/csm_Interview_KD_Blogbild_ffa2b05100.png)

(https://www.internetx.com/domains/) verknüpft, bietet das Internet eine benutzer- freundliche Umgebung. DNS ist seit 1985 ein wesentlicher Bestandteil des Internets! Haben Sie sich jemals die Frage gestellt, wie die Funktionsfähigkeit und Sicherheit eines solch wichtigen und grundlegenden Systems langfristig gesichert werden?

In der Domain-Branche (https://de.domainreport.global/) widmen sich Organisationen und Fachleute der Aufgabe, allen Internetnutzern über das DNS ein nachhaltiges und zuverlässiges System zur Verfügung zu stellen. Einer dieser Fachkräfte ist Klaus Darilion, Head of Operations bei nic.at, (https://www.nic.at/de) gemeinsam mit seinem Team. Im Einzelnen sichert das Team die Stabilität und Performance von .at, der österreichischen ccTLD (/domains/at-domains/). Klaus, der eine akademische Ausbildung in Elektrotechnik und Forschungserfahrung im Bereich der paketorientierten Sprachkommunikation, vor allem mit SIP, aufweist, ist seit 2004 Teil von nic.at. Zu seinem Aufgabenbereich gehören Network Design, Network Security, VoIP Security, DNSSEC und Anycast DNS. Seit Ende 2014 ist er Leiter des nic.at Betriebsteams. Er ist zweifelsohne die Ansprechperson, wenn es um DNS Security geht. Durchleuchten Sie zusammen mit uns einige technische Aspekte rund um DNS Security!

Was bedeutet es, an der DNS Security mitzuwirken?

Der Schutz des DNS ist ein breitgefächerter Bereich: dieser beginnt bei der Registrierung und endet mit den eigentlichen Domain-Daten, die von Internetnutzern empfangen werden. Hinsichtlich des DNS bedeutet Sicherheit, dass niemand in der Lage ist, diese Daten zu manipulieren und Informationen jederzeit ohne Störungen zur Verfügung stehen.

Eine Domain wird in der Regel über ein Webportal (oder API) eines Registrars angemeldet. Wer Zugang zu diesem Portal hat, kann die entsprechenden Domains bearbeiten, übertragen oder löschen. Aus diesem Grund sollten Domain-Besitzer solche Daten sicher verwahren und sofern möglich eine Zwei-Faktor-Authentisierung nutzen. Registrare müssen zudem sicherstellen, dass ihre Portale keine Sicherheitslücken aufweisen, die von Angreifern ausgenutzt werden könnten, um das Portal zu knacken und administrierte Domains zu manipulieren.

Ein weiterer Bestandteil ist der Domain-Name. Die Nameserver-Software muss stets auf dem neuesten Stand sein, um mögliche Sicherheitslücken im Protokoll zu vermeiden. Ferner muss das Set-up des Nameservers so konfiguriert sein, dass es mit 100% Uptime läuft; damit das gelingt, werden mehrere Nameserver eingesetzt, sodass genügend Kapazitäten bereitstehen, um hohen DNS-Abfragen standzuhalten und DDoS zu verringern. Leider sind DDoS-Angriffe heute im Internet an der Tagesordnung.

(https://www.internetx.com/news/zwei-faktor-authentifizierung-so-schuetzen-sie-ihre-accounts/)

Erfahren Sie mehr über die Zwei-Faktor-Authentisierung (2FA) (https://www.internetx.com/news/zwei-faktor-authentifizierung-so-schuetzen-sie-ihre-accounts/) und wie Sie Ihre Domains mit AutoDNS schützen können.

DNS ist ein wesentlicher Bestandteil des Internets: Warum ist es heute noch so anfällig für Angriffe?

Bei DNS handelt es sich um ein veraltetes Protokoll aus einer Zeit, in der nur „gute“ Menschen das Internet nutzten. Seither wurden viele Schwachstellen entdeckt, mit denen Eindringlinge das DNS mit falschen Daten füttern konnten, um auf diese Weise Internetnutzer auf falsche Webseiten umzuleiten. Dies geschah meistens mit der Absicht, Malware zu verbreiten oder Login-Informationen zu stehlen. Sobald ein solcher Angriff ermittelt wurde, behob man – sofern möglich – die Sicherheitslücke im DNS-Protokoll.

Eine Erschwernis ist jedoch, dass die meisten DNS-Protokolle nicht einfach geändert werden können, ohne dass Inkompatibilitäten entstehen, wodurch ältere Geräte von dem System ausgeschlossen würden. Somit mussten Workarounds implementiert werden, um solchen Angriffen entgegenzuwirken. Ein Beispiel hierfür: Das DNS verwendet eine 16-Bit Transaction-ID, die nur 65.536 unterschiedliche IDs zulässt. Die Anzahl der Bits zu erhöhen ist nicht möglich, denn das würde das Protokoll verletzen. Daher erweiterten Workarounds wie Random Source

Ports und 0x20 Verschlüsselungen (mit gemischter Groß- und Kleinschreibung) die tatsächliche Transaction-ID auf 32+ Bits. Da DNS hauptsächlich das User Datagram Protocol (UDP) verwendet, ist es anfällig für Angriffe, die auf IP-Fragmentierung beruhen.

Der „DNS Flag Day 2020 (https://dnsflagday.net/2020/)“ schaffte ein Bewusstsein für diese Problematik. Dies führte dazu, dass viele DNS-Provider ihre Nameserver für kürzere DNS-Antwortzeiten konfigurierten, um IP-Fragmentierung zu vermeiden. Jeder festgestellte Angriff könnte durch Implementierung von Workarounds in der Nameserver-Software entschärft werden.

(https://www.nic.at/de)

Mit DNSSEC könnten solche Angriffe einfacher entdeckt oder vollständig verhindern werden. Wie funktioniert DNSSEC?

DNSSEC nutzt Public-Key-Verschlüsselungsverfahren, um DNS-Antworten vor Missbrauch zu schützen. Wenn ein bestimmter Domain-Name angefragt wird, antwortet ein autoritativer Nameserver, auf dem der Dienst DNSSEC aktiviert ist, nicht nur mit den angeforderten Daten, sondern versieht diese Daten auch mit dem Private Key der Domain. Ein auflösender Nameserver nutzt den Public Key der Domain, um die Signatur zu überprüfen. Zur Verifizierung des Public Keys wird eine sogenannte Chain-of-trust eingesetzt, anhand derer der Fingerprint des Public Keys in der übergeordneten Zone der Domain veröffentlicht wird. Zum Beispiel wird der Fingerprint des Public Keys der Domain nodesecure.com von der .com Domain veröffentlicht und signiert. Der Fingerprint des Public Keys der .com Domain wird wiederum in dem Root-Bereich der DNS veröffentlicht und signiert.

Ein Angreifer, dem es gelingt, DNS-Antworten zu fälschen, wird nicht in der Lage sein, dies auch mit der Signatur zu bewerkstelligen. Im Falle, dass eine gefälschte Antwort von einem Resolver ohne Validierung nicht festgestellt werden könnte, würde ein Resolver mit einem Validierungsverfahren eine gefälschte Antwort sofort erkennen und ignorieren. Heutzutage wird DNSSEC-Validierung bei allen großen DNS-Diensten wie 8.8.8.8 und 1.1.1.1 genutzt, doch bei vielen Internetzugangsprovidern ist die DNSSEC-Validierung auf den auflösenden Nameservern nicht aktiviert.

Auch wenn DNSSEC ausgereift und stabil ist, gibt es noch immer einige Probleme:

1. Zum einen hängt dies mit alten Firewalls und CPE (Customer Premise Equipment, dt. Teilnehmernetzgerät) zusammen, d.h. DSL/Kabel-Modems. Solche Geräte weisen oft fehlerhafte DNS-Implementierungen auf, die versagen, wenn DNSSEC verarbeitet werden muss. So kann es vorkommen, dass Internetnutzer keine E-Mails mehr von Nutzern solcher älteren Geräte empfangen, sobald DNSSEC für die Domains aktiviert wurde.

2. Zum anderen ist das Keymanagement ein Problem. Sobald Kryptografie zur Anwendung kommt, ist eine Erneuerung der Keys unverzichtbar. Beispielsweise bei einem Leak von Private Keys oder wenn eine Schwachstelle in dem verwendeten Algorithmus vorliegt und die Keys geändert werden müssen. In solchen Fällen müssen der Einsatz neuer Keys und die Stilllegung alter Keys mit einem bestimmten Timing erfolgen. Ansonsten schlägt die DNSSEC-Validierung fehl. Die Voraussetzungen für das Timing sind sehr komplex und anfällig für Fehler.

Heutzutage kann Nameserver-Software wie Bind oder Knot die Key-Erneuerung unterstützen – das Hauptproblem ist jedoch nach wie vor menschliches Versagen.

(https://www.nic.at/de)

Wie können Registrys wie nic.at sicherstellen, dass die Registranten einen sicheren Domain-Namen erhalten?

Sicherheitsfunktionen sind heute unerlässlich. Im Allgemeinen müssen Änderungen für .at Domains von dem Domain-Inhaber signiert werden, um sicherzugehen, dass die Änderungen an ihrer Domain auch beabsichtigt sind. Sicherheit ist für uns als Registry ein zentrales Thema, das ständig weiterentwickelt wird. Meine Kollegin Katharina Hackl, Head of Customer Service, weist auf die unterschiedlichen Sicherheitsfunktionen von nic.at für .at Domains (/domains/at-domains/)hin:

Security Lock: Dieser Dienst schützt Domains vor unbefugten Transaktionen. Mit Security Lock erhält jede Änderung einen ausstehenden Status; diese Änderung wird von dem System zurückgehalten, bis sie schließlich von dem Domain-Inhaber ausdrücklich überprüft und bestätigt wurde.

Anycast DNS: Sollte der Domain-Inhaber seine Domain nicht nur gegen unerwünschte Transaktionen schützen wollen, bietet nic.at auch den RcodeZero DNS Anycast Service. Mit weltweit mehr als 40 Nameservern gewährleisten wir, dass der Online-Dienst unserer Kunden stets zugänglich und möglichst unter der gleichen IP-Adresse verfügbar ist.

DNSSEC: Mit diesem Dienst wird Domain-Inhabern garantiert, dass Nutzer auch wirklich auf ihre Webseites gelangen.

Registrar Lock: Zusätzlich wird derzeit ein weiterer Dienst ausschließlich für Registrare eingerichtet. Vor einer gewünschten Änderung in der .at Domain muss der Registrar den Registrar-Lock von der Domain entfernen. Sobald alle Änderungen vorgenommen wurden, wird das Registrar-Lock wieder eingesetzt. Der Vorteil dieses Dienstes liegt darin, dass es von den Registraren als Selbstschutz genutzt, aber auch vom Domain-Inhaber angefordert werden kann.

Kann Automationstechnologie das DNS sicherer machen?

Fehlfunktionen des DNS sind häufig auf menschliches Versagen zurückzuführen, wie z. B. Copy/Paste-Fehler bei der Domain-Konfiguration oder Domain-Übertragung. Dies kann vor allem dann vorkommen, wenn Internetnutzer eine Domain bei Registrar A anmelden, das DNS jedoch beim Anbieter B oder eigenhändig verwaltet wird. Solche Fehler können meistens vermieden werden, wenn der DNS-Service des Registrars genutzt wird, da der Registrar hoch automatisierte Prozesse für die Domain-Konfiguration nutzt. Und erst recht, wenn DNSSEC zum Einsatz kommt – in diesem Fall ist Automation der Schlüssel zum Erfolg. Der Registrar hat die Key-Management-Prozesse automatisiert, wodurch die Einhaltung der Timing-Voraussetzungen sichergestellt wird. Außerdem kann der Registrar die Chain-of-trust mit der übergeordneten Domain, d.h. mit dem TLD-Register, automatisch aktualisieren.

Was sind die innovativsten Techniken, die derzeit zum Einsatz kommen, um die Sicherheit des DNS zu erhalten?

Laut meines Kollegen Alexander Mayrhofer, Head of R&D bei nic.at, ist im DNS-Ökosystem Sicherheitsschutz in den folgenden zwei Bereichen notwendig:

Einer der Bereiche ist das Ökosystem der Registrierungs-/Namespace-Verwaltung, in dem Registrys und Registrare die Vergabe und Konfiguration von Domains vornehmen. Der Schlüssel für mehr Sicherheit ist in diesem Fall, Domains vor unbefugten Änderungen oder Löschungen zu schützen, sei es aufgrund von Verlust der Zugangsdaten, Social-Engineering oder einem Angriff auf der Systemebene. Immer mehr Registrare erweitern ihre Login-Portale mit einer Zwei-Faktor-Authentifizierung; die meisten Endnutzer kennen diese Technologie bereits vom Online-Banking oder sogar von ihrem Gmail-Konto. Ferner bieten Registrys Optionen für zusätzliche Verifikationsmöglichkeiten, wie etwa Registrar Lock und Security Lock, die für noch mehr Sicherheit sorgen.

Der zweite Teil der DNS-Technologie ist der Auflösungspfad – also das eigentliche Abrufen der Informationen entsprechend dem Domain-Namen. Hierbei werden sowohl die Authentizität als auch der Datenschutz berücksichtigt. DNSSEC sorgt für die Authentizität der Informationen; dieser Dienst wird schon seit einiger Zeit angeboten, daher kann man hier nicht mehr von einer „Innovation“ sprechen. Eine Innovation wäre jedoch, diese Funktion von den IT-Administratoren an die Kunden weiterzureichen. Und zwar in der Art und Weise, wie es mit Let’s Encrypt bei der Verwaltung von Zertifikaten gehandhabt wird. Bezüglich des Datenschutzes wird immer mehr DNS-Traffic zwischen Stub Resolvern und Recursor verschlüsselt und es scheint, als würde sich dieser Trend fortzusetzen. Im Laufe der Zeit wird sich dies auch auf die Kommunikation zwischen Recursorn und autoritativen Servern ausweiten. DNS over QUIC ist eine Innovation, die wir alle gespannt mitverfolgen.

Wie glauben Sie wird sich DNS in den kommenden Jahren entwickeln?

In Übereinstimmung mit meinem Kollegen Alexander Mayrhofer erwarten wir seitens des Registrierungs-/Namespace-Managements keine großen Änderungen im Vergleich zu heute. Für Registrare und Registrys können zusätzliche Anforderungen an die Validierung und Verifizierung von Kundendaten entstehen. Beispielsweise die Anforderungen aus der NIS-2-Richtlinie der Europäischen Union (https://digital-strategy.ec.europa.eu/en/library/proposal-

directive-measures-high-common-level-cybersecurity-across-union). Schließlich wird es eine neue new gTLD-Runde geben, aber es ist damit zu rechnen, dass viel ruhiger als beim ersten Mal verlaufen wird, und die Erwartungen im Vergleich zu 2012 realistischer sein werden. Im Hinblick auf die Auflösung wird mehr und mehr Traffic verschlüsselt; es werden neue Protokolle und neue Auflösungswege entstehen.

Trotzdem können wir mit Gewissheit sagen, dass DNS von Dauer sein wird – Soziale Netzwerke gewinnen und verlieren an Popularität, Domains sind jedoch die einzigen vom Menschen lesbaren Identifier im Internet, die nicht von Richtlinien, der Popularität und dem Betrieb abhängen.

Eine Reihe von Sicherheitslücken im Softwarestack hat zu einer erneuten Verbreitung des klassischen DNS-Cache-Poisoning-Angriffs geführt. Erfahren Sie, was einen SAD DNS Angriff ausmacht und wie diese Bedrohung in der DNS verringert werden kann (https://www.internetx.com/news/sad-dns-das-comeback-des-dns-cache-poisoning/).

InterNetXPress Newsletter

Werden Sie jetzt Teil von tausenden InterNetXPress-Lesern!

✔ 2x im Monat ✔ Jederzeit kündbar

E-Mail-Adresse

Ich habe die Datenschutzerklärung (https://www.internetx.com/rechtliches/datenschutz/) zur Kenntnis genommen. Durch Anklicken „Abonnieren" willige ich ein, dass meine E-Mail-Adresse elektr. erhoben und gespeichert wird.

ABONNIEREN

Hinweis: Sie können Ihre Einwilligung jederzeit ohne Angabe von Gründen für die Zukunft per E-Mail datenschutz@internetx.com (mailto:datenschutz@internetx.com?Subject=Einwilligung%20widerrufen) widerrufen.

(/news/das-muessen-sie-ueber-dnssec-wissen/)

Das müssen Sie über DNSSEC wissen (/news/das-muessen-sie-ueber-dnssec-wissen/)

(/news/code-signing-mehr-authentizitaet-und-integritaet/)

Code Signing: Mehr Authentizität und Integrität ... (/news/code-signing-mehr-authentizitaet-und-integritaet/)

(/news/wie-laesst-sich-domain-parking-mit-domain-investing-vereinbaren/)

Wie lässt sich Domain-Parking mit Domain-Investing... (/news/wie-laesst-sich-domain-parking-mit-domain-investing-vereinbaren/)

(/news/domain-hijacking-wie-kommt-man-wieder-an-gekaperte-domains/)

Domain Hijacking – Wie kommt man wieder an... (/news/domain-hijacking-wie-kommt-man-wieder-an-gekaperte-domains/)

Autor

Simone Catania

Global Content & Communications Manager

E-Mail: presse@internetx.com

Social Media

(https://www.facebook.com/InterNetX)
(https://twitter.com/InterNetX)
(https://www.youtube.com/user/InterNetXGmbH)
(https://www.linkedin.com/company/internetx-gmbh)
(https://www.xing.com/companies/internetxgmbh)

Domains (/domains/)

Server (/server/)

SSL-Zertifikate (/ssl-zertifikate/)

InterNetX (/ueber-uns/)

Rechtliches (/rechtliches/impressum/)

Social Media

Blog (blog/)

Facebook (https://www.facebook.com/InterNetX)

Twitter (https://twitter.com/InterNetX)

YouTube (https://www.youtube.com/user/InterNetXGmbH)

Instagram (https://www.instagram.com/internetx_official/?hl=de)

Spotify (https://open.spotify.com/show/3A5BxhZmxi7pPmJmWs65s9?si=d7lvkgutTXK69VViHGJiwA)

iTunes (https://itunes.apple.com/de/podcast/snapshot-digitale-themen-auf-den-punkt-gebracht/id1331011109?mt=2)

Impressum (https://www.internetx.com/rechtliches/impressum/) | Datenschutz (https://www.internetx.com/rechtliches/datenschutz/)