Sachverständigengutachten

IT-Sicherheit im Kontext registrierter Domains

Erik Sy und Rainer Rehak

12. Juni 2017

Mit dem Internet verbundene IT-Systeme sind professionellen IT-Angriffen und den damit verbundenen Risiken ausgesetzt. Die Angreifer wählen die attackierten IT-Systeme oft anhand von Sicherheitslücken aus, wie zuletzt bei den bekannteren Angriffen auf die Telekom-Router oder „Wannacry“ geschehen. Dies führt zu der Situation, dass die Angreifer teilweise IT-Systeme attackieren ohne die Identität der Besitzer dieser Systeme zu kennen. Auch bei Nichtveröffentlichung von registrierten Domains sind die betroffenen IT-Systeme bereits im Internet über ihre IP-Adresse erreichbar und damit gefährdet. Mit der Geheimhaltung der registrierten Domains kann die Unverkettbarkeit zwischen dem Bundesministerium für Gesundheit und den entsprechenden Domains teilweise geschützt werden, ein Vorteil für die IT-Sicherheit der betriebenen Systeme lässt sich hieraus nicht ableiten.

Kontaktdaten der Verfasser

Erik Sy, M. Sc.
Universität Hamburg
Fachbereich Informatik
Sicherheit in verteilten Systemen
Vogt-Kölln-Str. 30
22527 Hamburg

Telefon: 040-42883-2008
E-Mail: sy@informatik.uni-hamburg.de

Rainer Rehak, Dipl. Inf.
Hochschule für Technik und Wirtschaft Berlin
Fachbereich Informatik, Kommunikation und Wirtschaft
Angewandte Informatik
Campus Wilhelminenhofstraße
12459 Berlin

E-Mail: rehak@htw-berlin.de

1 Grundlagen des Domain Name Systems

Damit die Kommunikation zwischen zwei Systemen über das Internet zielgerichtet erfolgen kann, werden IP-Adressen zur Identifikation der Systeme eingesetzt. So verwendet beispielsweise jeder erreichbare Computer im Internet eine IP-Adresse, deren Vergabe von der Internet Corporation for Assigned Names and Numbers (ICANN) beaufsichtigt wird.

Damit sich Nutzer nicht die Zahlenfolgen der IP-Adressen für verschiedenste Onlinedienste merken müssen, wurde das Domain Name System (DNS) eingeführt. Eine Domain ist ein administrativer Namesraum, welcher weltweit einmalig und eindeutig ist, wie etwa „www.beispiel.de“. Die Vergabe von Domainnamen für die Top-Level-Domain „.de“ wird durch die DENIC e.G. vorgenommen. In den Nameservern des DNS werden Einträge vorgehalten, die die Domains mit den IP-Adressen der zugehörigen Server verknüpfen. Beim Surfen im Internet werden diese Einträge im DNS beispielsweise vom Webbrowser abgefragt, so liefert eine Anfrage für die Domain „www.beispiel.de“ die IP-Adresse 5.100.155.211, welche dann für die Verbindung zum Webserver verwendet wird.

Die Registrierung von Domains im DNS ermöglicht es, für die erworbene Domain eine Verknüpfung zu einer IP-Adresse zu definieren. Gleichwohl kann ein Webserver auch ohne Kenntnis der eventuell verknüpften Domain direkt über seine IP-Adresse im Internet kontaktiert werden.

2 Grundlagen der IT-Sicherheit

Die Anzahl der möglichen IP-Adressen im Internet ist begrenzt. So kann der gesamte Adressraum des populären Internet Protokoll Version 4 (IPv4) binnen 45 Minuten durchsucht werden.[1] Dies bedeutet für die IT-Sicherheit, dass schwachstellenbehaftete IT-Systeme leicht von potentiellen Angreifern erkannt werden können. Mit dem Onlinedienst „www.shodan.io“ wird die Identifikation verwundbarer IT-Systeme weiter vereinfacht, weil der Angreifer dort bereits gesammelte Daten über im Internet erreichbare Geräte auswerten kann.

In den Medien wurden in den vergangenen Monaten beispielsweise die Angriffe auf Telekom-Router[2] sowie der Krypto-Trojaner „Wannacry“[3] thematisiert. Bei diesen Angriffen haben infizierte IT-Systemen anschließend selbstständig im IP-Adressraum des Internets nach weiteren verwundbaren Geräten gesucht und zur Ausbreitung des Angriffs beigetragen. Diese Beispiele belegen die Notwendigkeit, dass IT-Systeme grundsätzlich abgesichert werden müssen, bevor sie mit dem Internet verbunden werden.

Üblicherweise erfolgen solche professionellen und automatisierten Angriffe auf Basis von IP-Adressen, sodass eventuell auf die IT-Systeme verweisende DNS-Einträge keinen Einfluß auf den Verlauf des Angriffs haben.

Für IT-Systemen mit besonderen Sicherheitsanforderungen eignet sich ein Betrieb in vom Internet entkoppelten Computernetzwerken, welche sich auch über große Entfernungen, mittels sogenannter Standleitungen, realisieren lassen.

1. Siehe Tools wie ZMap, masscan oder Scanrand.
2. https://www.heise.de/security/meldung/Grossstoerung-bei-der-Telekom-Was-wirklich-geschah-3520212.html
3. https://www.heise.de/newsticker/meldung/WannaCry-Angriff-mit-Ransomware-legt-weltweit-Zehntausende-Rechner-lahm-3713235.html

3 Verknüpfung von Ministerium und Domain (Verkettbarkeit)

Das Bundesministerium für Gesundheit (BMG) schützt durch die Geheimhaltung der registrierten Domains die betroffenen Systeme nicht, weil diese bereits ohne Kenntnis der spezifischen Domains einer Vielzahl von professionellen IT-Angriffen ausgesetzt sind. Die Nichtveröffentlichung dient vielmehr der Unverkettbarkeit zwischen BMG und registrierten Domains.

Aufgrund der öffentlichen Architektur und Verwaltung des Internets, kann diese Unverkettbarkeit zwischen zwischen dem BMG und den registrierten Domains jedoch grundsätzlich nur teilweise aufrecht erhalten werden. So wird beispielsweise die Website „www.bundesgesundheitsministerium.de“ vom Deutschen Institut für Medizinische Dokumentation und Information (DIMDI) betrieben. Die für das DIMDI registrierten IP-Adressen liegen im Bereich von 194.153.219.0 bis 194.153.219.255.[4] Für diesen Adressbereich sind ohne Anspruch auf Vollständigkeit zusätzlich die folgenden Domains durch sogenannte Rückwärtsauflösung (PTR-Records) der DNS-Einträge öffentlich und daher direkt einsehbar:

- ns1.dimdi.de
- watson.dimdi.de
- mailin.dimdi.de
- mailin.bzga.de
- mailin2.dimdi.de
- mailin3.dimdi.de
- holmes.dimdi.de
- proxy.dimdi.de
- ns2.dimdi.de
- extranet.dimdi.de
- sslvpn.dimdi.de
- caweb.dimdi.de
- mrpdb.dimdi.de
- web01cluster.dimdi.de
- jira.dimdi.de
- z3950gw.dimdi.de
- portal.dimdi.de
- resources.pharmnet-bund.de
- collaboration.dimdi.de
- federation.dimdi.de
- bzweb01.dimdi.de
- services.dimdi.de
- srv01mailgw.dimdi.de
- srv02mailgw.dimdi.de
- onlineassist1.dimdi.de
- onlineassist2.dimdi.de
- www.organspende-geschichten.de
- anwendungen-spiegel.pharmnet-bund.de
- web01spiegelcluster.dimdi.de
- web01testcluster.dimdi.de
- services-test.dimdi.de
- web01rproxy.dimdi.de
- spc.dimdi.de
- www.cts-mrp.eu
- webshop.dimdi.de
- www.bzga.de
- marlowe.bzga.de
- bmgks3web.dimdi.de
- www.dimdi.de
- www.pharmnet-bund.de
- versandhandel.dimdi.de
- www.drugcom.de
- www.telemedizin-journal.de
- spade3.bzga.de
- www.europsychology.de
- biosci.dimdi.de
- pdfextra.fruehehilfen.de
- www.ops-301.de
- www.amg-zulassung.de
- www.nachzulassung.de
- web01drkstest.dimdi.de
- bmweb01svrg.dimdi.de
- www.uaw-bfarm.de
- epay.dimdi.de
- sso.dimdi.de
- sso-test.dimdi.de
- sso-spiegel.dimdi.de
- various.dimdi.de
- bzweb01testtypo3.-dimdi.de
- services-spiegel.dimdi.de
- piwik.dimdi.de
- www.cts-server.net
- www.wir-gegen-viren.de
- hammer.dimdi.de
- booker.dimdi.de
- misc.dimdi.de
- chat.bzga-rat.de
- bzweb01sunset-test.dimdi.de
- sunset-clause.dimdi.de
- www.zentrale.gutdrauf.net
- www.uaw-pei.de
- spade.bzga.de
- spade2.bzga.de
- eunetdev.dimdi.de
- www.egms.de
- www.sexualaufklaerung.de
- iris-frontend.dimdi.de
- www.check-dein-spiel.de

4. https://apps.db.ripe.net/search/lookup.html?source=ripe&key=194.153.219.0-194.153.219.255&type=inetnum

4 Zusammenfassung

Domainnamen sind administrative Bereiche des Internet, denen IP-Adressen zugeordnet werden, um darüber Internet-Dienste in Anspruch zu nehmen. Dabei sind IP-Adressen und Domainnamen dem öffentlichen Teil des Internet zuzurechnen. Sie können durch Abfrage von DNS-Servern oder dem eigenen Betrieb eines solchen erhalten werden, siehe obiges Beispiel des registrierten IP-Adressbereiches des BMG. IT-Systeme mit besonderen Sicherheitsanforderungen können über dedizierter Standleitungen verbunden werden, um einen Schutz vor Angriffen aus dem Internet zu gewährleisten.

IT-Systeme im Internet sehen sich permanent gezielten und ungezielten Angriffen ausgesetzt, weshalb jedes mit dem Internet verbundene System gegen nicht-berechtigte Zugriffsversuche, also Angriffe, abgesichert werden sollte.

Ein Geheimhaltung der Verkettung zwischen dem BMG und den registrierten Domains kann IT-Angriffe gegen die betroffenen Systeme nicht verhindern und nur marginal erschweren. Ferner sind bereits eine Vielzahl möglicher Angriffspunkte gegen die IT-Systeme des BMGs, beziehungsweise beauftragter Stellen, öffentlich bekannt, sodass auch für gezielte Angriffe eine erhebliche potentielle Angriffsoberfläche besteht. Aufgrund der hohen Professionalität und Anzahl von ungezielten IT-Angriffen wie dem „Wannacry“-Wurm kann kein qualitativer Unterschied zwischen gezielten und ungezielten IT-Angriffen belegt werden, sodass ein IT-Sicherheitskonzept gegen ungezielte Angriffe auch eine Verteidigung gegen gezielte Attacken (ohne Insiderwissen) einschließen wird.