Reise ins Herz des Internets

Der Schlüssel zur Macht

21 Keyholder schützen im Auftrag der Internet Corporation for Assigned Names and Numbers (ICANN) das Domain Name System (DNS), eine Kerninfrastruktur des Internets. Große Teile der privaten und geschäftlichen Kommunikation hängen davon ab. Doch die eigenen Server müssen Unternehmen immer noch selbst schützen – und bei der Domainwahl ist ein strategisches Vorgehen sinnvoll.

► Es ist eine bizarre Zeremonie, die alle paar Monate in den USA vollzogen wird – und die ein wenig an einen Agententhriller erinnert: Eine Gruppe von Technikern, genannt „Crypto Officers", besitzt Schlüssel für ein Schließfach in einem mehrfach gesicherten Rechenzentrum in Culpeper im US-Bundesstaat Virginia. Der Ort liegt an der amerikanischen Ostküste, ein paar Kilometer außerhalb jener Zone, die nach einem Atombombenangriff auf die US-Hauptstadt Washington, D.C. vom radioaktiven Fallout betroffen wäre. In jenen Schließfächern befinden sich Computer, die sich nur starten lassen, wenn eine bestimmte Zahl der Schlüsselträger anwesend ist. Die Schlüssel sind über die Welt verteilt, und die Schlüsselträger dürfen nie im selben Flugzeug reisen – damit im Falle eines Absturzes nicht alle tot sind. Sieben Schlüssel gibt es für Culpeper an der amerikanischen Ostküste. Zur Sicherheit steht an der Westküste, in der Nähe des Flughafens von Los Angeles, ein fast identisches Datenzentrum mit sieben anderen Schlüsselträgern. Für die Zeremonie müssen mindestens drei Schlüsselträger alle drei Monate abwechselnd in Ost und West zusammenkommen, um einen sogenannten Masterschlüssel zu erzeugen, einen digitalen Code, der die Einträge des DNS-Servers aufs Neue absichert. Ohne diesen Sicherheitsschlüssel könnten sonst Hacker Millionen von Websites kapern und Schadsoftware verbreiten. Für den – ziemlich unwahrscheinlichen – Fall, dass allen 14 Schlüsselträgern etwas zustößt oder beide Rechenzentren gleichzeitig zerstört werden, gibt es zusätzlich noch sieben „Recovery Key Share Holders". Sie verfügen über spezielle Speicherkarten, die das System im Notfall an einem geheimen Ort wiederherstellen könnten. Beauftragt sind die insgesamt 21 Schlüsselhüter von der Non Profit Organisation ICANN mit Sitz in den USA. Die Abkürzung steht für „Internet Corporation for Assigned Names and Numbers", die Organisation verwaltet seit ihrer Gründung 1998 das System der internationalen Top-Level-Domains mit Endungen wie .com, .de oder .net und weist ihnen IP-Adressen zu. Das System, um das es dabei geht, ist so etwas wie das Herz des Internets. Es heißt Domain Name System – kurz: DNS – und wird häufig auch als „Telefonbuch des Internets" bezeichnet. Seine Aufgabe ist es, Buchstabenfolgen wie etwa www.diruj.net in einmalige, aber schwer zu merkende IP-Adressen zu übersetzen, die aus einer Zahlen-Punkte-Kombination bestehen, und die Anfrage

„Unternehmen sollten unbedingt über Risiken und Angriffsarten aufklären und Hinweise für das richtige Verhalten geben."

Simran Mann
Referentin für Sicherheitspolitik
Bitkom

über mehrere Ebenen an jenen Server weiterzuleiten, auf dem die Internetseite liegt. Von dort kann der Browser dann die Inhalte der Seite herunterladen und anzeigen.

Katastrophale Folgen eines DNS-Ausfalls

Das Ganze passiert so schnell und so häufig, dass es die meisten Menschen als völlig selbstverständlich betrachten. Und doch ist es essenziell, dass dieses System stets funktioniert. „Große Teile unserer privaten und kommerziellen Kommunikation basieren auf diesem System", erklärt Dominik Eickemeier, Fachanwalt für gewerblichen Rechtsschutz und Partner am Kölner Standort der Kanzlei Heuking Kühn Lüer Wojtek und Co-Leiter der Praxisgruppe IP, Media & Technology der Kanzlei. „Ein DNS-Blackout dürfte fast ähnlich katastrophale Folgen haben wie der Ausfall der Stromversorgung." Und Sicherheitslücken kennt auch das DNS: Cache Poisoning und der Kaminsky Bug sind nur zwei davon. Ihre Gemeinsamkeit ist, dass sie das Aufrufen von Internetseiten zu einem Glücksspiel machen würden: Anfragen nach IP-Adressen könnten auf falsche Server umgeleitet, E-Mails unterwegs abgefangen und mitgelesen werden. Um das auszuschließen, brauchte das DNS eine zusätzliche Sicherheitsebene. Die gibt es seit 1997, sie heißt Domain Name System Security Extensions, kurz DNSSEC. Stark vereinfacht ausgedrückt setzt DNSSEC auf digitale Signaturen, mit denen große Teile des Internet-Telefonbuchs unterschrieben werden. Diese Unterschrift kann bei jedem Abruf einer Website vom Provider des Internetnutzers überprüft werden. Der Provider erkennt dann, ob die Daten, die an den Nutzer gesendet werden, vom richtigen Server kommen und ob sie unterwegs manipuliert wurden – und bricht die Anfrage gegebenenfalls ab, um den Nutzer zu schützen. Das Herzstück von DNSSEC sind kryptografische Schlüssel, die zum Erstellen der Signaturen notwendig sind. Die wichtigsten Schlüssel heißen Zone Signing Key (ZSK) und Key Signing Key (KSK). Mit dem ZSK wird die sogenannte Root Zone des Internets unterschrieben, das ist die oberste Hierarchie-Ebene des DNS. Jede Anfrage nach einer IP-Adresse landet zuerst dort und wird dann über die niedrigeren Ebenen bis zum Zielserver weitergeleitet. Damit DNSSEC vertrauenswürdig sein kann, muss auch dieser oberste Teil des Telefonbuchs unterschrieben werden. Das geschieht alle drei Monate mit einem erneuerten Root Zone ZSK. Der wiederum wird mit dem KSK signiert. Der KSK ist damit sozusagen der Schlüssel aller Schlüssel – und wird eben in den beiden Rechenzentren in Culpeper und Los Angeles aufbewahrt, wo die vierteljährlichen Zeremonien stattfinden, in denen jeder neue ZSK mit dem KSK signiert wird.

Warnung vor Aufsplitterung des Internets

„Man kann dem vertrauen, das läuft transparent ab", sagt Kristian Ørmen, Vice President Registry Services bei der schwedischen Stiftung Internetstiftelsen. Er gehört zu jenem erlauchten Kreis der Keyholder, die sich vierteljährlich treffen und über die Sicherheit des Systems wachen. Die technische Überwachung des DNS sei durch die verschiedenen Sicherheitsebenen und die vierteljährliche Key-Signing-Zeremonie gewährleistet, sagt Ørmen. Ob die Zeremonie wirklich notwendig ist, um die Sicherheit des DNS zu gewährleisten, ist unter Experten allerdings umstritten. David Huberman, Technikbeauftragter der ICANN für Europa und Nordamerika, sieht durch die Zeremonie das Vertrauen in das System gewährleistet. „Als Maßnahme von innen heraus scheint sie mir nicht geeignet, das Vertrauen deutlich zu erhöhen", meint hingegen Heuking-Experte Eickemeier. Wichtiger als die Zeremonie an sich sei es aber ohnehin, die Aufsplitterung des globalen Internets zu verhindern, sagt Huberman. „Die potenzielle Fragmentierung des Internets ist ein beunruhigendes Thema." Gerade autoritären Regierungen etwa in Russland, China oder dem Iran seien die Freiheiten, die das Internet biete, ein Dorn im Auge. Umgekehrt wehrt sich Huberman auch gegen Forderungen, einzelne Länder vom Internet abzukoppeln. So hatte der ukrainische Präsident Wolodymyr Selenskyj zu Beginn des Krieges im vergangenen Jahr gefordert, Russland aus dem Internet auszuschließen. Die ICANN hat das wiederholt zurückgewiesen. „Wir müssen neutral bleiben", so Huberman.

Prinzip der Eigenverantwortlichkeit

Eben jene Neutralität ist auch die Grundidee der ICANN. „Die ICANN ist praktisch entstanden, um den Wettbewerb zu verstärken und etwas unabhängiger von den Machtgefügen

„Die potenzielle Fragmentierung des Internets ist ein beunruhigendes Thema."

David Huberman
Technikbeauftragter für Europa und Nordamerika
ICANN

„Ein DNS-Blackout dürfte fast ähnlich katastrophale Folgen haben wie der Ausfall der Stromversorgung."

Dominik Eickemeier
Fachanwalt für gewerblichen Rechtsschutz und Partner
Heuking Kühn Lüer Wojtek

der Weltpolitik zu sein", erläutert Heuking-Jurist Eickemeier. „Bisher scheint dies aus meiner Sicht erfolgreich gewesen zu sein." Eine Alternative wäre höchstens, die ICANN den Vereinten Nationen zu unterstellen. Doch auch wenn die ICANN die Sicherheit des DNS gewährleistet und so die Weiterleitung von Anfragen an die Server von Unternehmen, Organisationen und Behörden gewährleistet – um die Sicherheit der Daten auf eben jenen Servern muss sich jeder selbst kümmern. „Jedes Unternehmen kann Opfer von Cyberattacken werden, unabhängig von Branche und Größe", warnt Simran Mann, Bitkom-Referentin für Sicherheitspolitik. „Ist die Firmen-IT erst einmal infiziert oder lahmgelegt, entstehen den Unternehmen hohe Kosten, die bis hin zu wochenlangen Produktionsausfällen gehen können." Trotz der enormen Risiken seien viele Unternehmen aber immer noch unzureichend auf Cyberattacken vorbereitet, so Mann. „Alle Unternehmen sollten entsprechende Vorbereitungen treffen und einen klar geregelten Notfallplan aufstellen, um im Fall der Fälle nicht wertvolle Zeit zu verschwenden." Am wichtigsten sei es, die Mitarbeiterinnen und Mitarbeiter entsprechend zu schulen, betont Mann. „Sie sind die erste Abwehrreihe gegen Cyberkriminelle. Unternehmen sollten unbedingt über Risiken und Angriffsarten aufklären und Hinweise für das richtige Verhalten geben." Friedrich Wimmer, Leiter IT-Forensik & Cyber Security Research bei der Corporate Trust Business Risk & Crisis Management GmbH, pflichtet ihr bei: Grundsätzlich sei jedes System nur so lange sicher, wie sich seine Benutzer an zuvor vereinbarte Standards halten, so der Experte. Daher sei es besonders wichtig, „die handelnden Personen mit auf die Reise zu nehmen und entsprechend zu schulen".

Vorsicht bei der Domainwahl

Bei der Entwicklung der IT-Sicherheitsstrategie müssten Rechtsabteilung und IT Hand in Hand arbeiten, sagt Wimmer. „Zumindest hat die Rechtsabteilung bei der Feststellung des Schutzbedarfs, der Anforderungen an die IT und dem Sicherheitskonzept mitzuwirken." Ferner sollte sie die Angemessenheit und Wirksamkeit der Maßnahmen aus Rechtssicht regelmäßig prüfen, so der Experte. Technisch gelte es, wirksame Maßnahmen unter anderem in den Bereichen Datensicherung und Backup, Hackerresistenz und Sicherheitsmonitoring zu implementieren. Auch bei der Auswahl der Domains für ihre Internetseiten sollten Unternehmen achtsam sein und strategisch vorgehen. Die Top-Level-Domains wie .com oder .de werden von der ICANN vergeben, für die Vergabe der eigentlichen Domains sind aber nationale Organisationen zuständig, in Deutschland etwa die Denic. „Da es so viele Top-Level-Domains gibt, muss die Domainwahl gut bedacht sein", erklärt IT-Rechts-Experte Eickemeier. „Was hilft es, wenn man unter xy.de eine Marke aufbauen will, Dritte aber auf diesen Zug aufspringen und etwa unter der .com oder der .eu-Domain am Ruhm der Marke partizipieren wollen?" Sinnvoll sei es daher häufig, „ein vernünftiges Portfolio an Domainnamen zu erwerben und nicht lediglich eine Domain unter einer Top-Level-Domain", so der Fachanwalt. Bei Streitigkeiten etwa mit Blick auf den Markennamen ist das Vorgehen unterschiedlich. „In Deutschland steht nur der Weg zu den Zivilgerichten offen", erklärt Eickemeier. „Für zahlreiche Top-Level-Domains wie .com, .net, .org, .eu und insbesondere die neuen Top-Level-Domains wie .berlin kann man sich auch an Schiedsgerichte wenden." Zu diesen zählen beispielsweise das WIPO Arbitration and Mediation Center oder der Tschechische Schiedsgerichtshof in Prag. „In schlanken und kostengünstigen Verfahren wird hier häufig die Domain an den Anspruchsteller – also den Markeninhaber – übertragen", so Eickemeier. Vor deutschen Gerichten sei die Übertragung hingegen die Ausnahme. Die Gründe, warum die Gerichte bei der Übertragung zögern, sind mitunter schwer nachvollziehbar. Transparenz, wie sie die ICANN durch ihre vierteljährliche Schlüsselzeremonie zu gewährleisten versucht, gibt es hier eher nicht. ■

Harald Czycholl