Internet der Dinge: Kalifornien verbietet Standardpasswörter

Ein Modell für Deutschland?

von Chris Köver

[3]

Geräte, die am Internet hängen, müssen in Kalifornien bald ein sicheres Passwort bekommen. Expert*innen halten das aber bestenfalls für einen ersten Schritt in Richtung größerer IT-Sicherheit.

„123456“, „admin“ oder „password“: Solche zeitlosen Standardpasswörter sind im US-Bundesstaat Kalifornien ab dem 1. Januar 2020 verboten. Das verfügt ein neues Cybersecurity-Gesetz [4], das Kaliforniens Gouverneur Jerry Brown [5] vergangene Woche unterzeichnet hat. Spätestens ab diesem Datum muss jedes neue Gerät, das in Kalifornien auf den Markt kommt und „direkt oder indirekt“ mit dem Netz verbunden ist – vom Router bis zur smarten Glühbirne – mit Sicherheitsfunktionen ausgestattet sein, die einen unzulässigen Zugriff von Außen verhindern. Geräte, die außerhalb eines lokalen Netzwerkes per Passwort erreichbar sind, müssen entweder mit einem einzigartigen Passwort ausgeliefert werden oder Nutzerinnen und Nutzer dazu zwingen, vor der ersten Verwendung ein eigenes Passwort festzulegen.

Die Absicht dahinter: Außenstehende sollen schwache Passwörter nicht einfach erraten und sich so Zugang zu Geräten verschaffen können. In der Vergangenheit waren schlecht gesicherte Heimgeräte wie Router oder smarte Kühlschränke immer wieder von Hacker*innen für sogenannte Botnetze gekapert worden [6] – eine Art Zombie-Armee, die ohne das Wissen und Zutun ihrer Besitzer*innen Spam verschickt, Webseiten mit Überlastungs-Angriffen in die Knie zwingt oder Schadsoftware streut. Das funktioniert unter anderem deswegen, weil Geräte mit bekannten Standardpasswörtern ausgeliefert werden und Nutzer*innen sich nicht die Mühe machen, diese nachträglich zu ändern.

Sicherheitsexpert*innen sind sich uneinig darin, ob das Gesetz eine Verbesserung oder Verschlimmbesserung der Situation darstellt. Manche wie Bruce Schneier [7] halten es für einen wichtigen ersten Schritt. „Vermutlich geht es nicht weit genug – aber das ist kein Grund, es nicht zu verabschieden,“ sagte er der Washington Post [8]. Der Sicherheitsexperte Robert Graham zerlegt den Gesetzestext hingegen als zu vage und bemängelt [9], der Fokus auf die Passwörter gehe am Problem vorbei. Vernetzte Geräte hätten schließlich nicht nur ein Passwort, sondern eine Reihe von Schnittstellen mit unterschiedlichen Authentifizierungssystemen. Das berüchtigte Botnetz Mirai [10], das im Jahr 2016 Angriffe fuhr, hatte vor allem andere Schwachstellen genutzt, um die Kontrolle über Geräte zu erlangen. Diese müssten Hersteller*innen auch mit dem neuen Gesetz nicht beheben.

Ablauf der Entstehung und Verwendung von Botnetzen:

(1) Infizierung ungeschützter Computer, (2) Eingliederung in das Botnet,

(3) Botnetbetreiber verkauft Dienste des Botnets, (4) Ausnutzung des Botnets, etwa für den Versand von Spam

► Minimalstandards: „Ein erster kleiner Schritt in die richtige Richtung“

Das kalifornische Gesetz dürfte Vorbildwirkung für den Rest der USA oder zumindest andere demokratisch dominierte Bundesstaaten haben. Schließlich handelt es sich nicht nur um einen der größten und reichsten US-Staaten, bekanntlich sitzt auch das Silicon Valley in Kalifornien. Das Gesetz könnte sich damit zum de-facto-Standard entwickeln – wer in der achtgrößten Volkswirtschaft der Erde ein Produkt auf den Markt bringen will, muss die Standards ja ohnehin umsetzen. Es spricht wenig dafür, anderen Kund*innen die bereits implementierten Standards vorzuenthalten.

Allerdings gälte das nicht für Produkte, die nur in Deutschland oder der EU verkauft werden. Wäre ein vergleichbares Verbot von Standardpasswörtern auch in Deutschland denkbar? Frank Rieger, Sprecher des Chaos Computer Clubs (CCC [11]), sagt:

> „Minimalstandards für die IT-Sicherheit auch hier in Deutschland gesetzlich festzulegen, ist definitiv ein erster kleiner Schritt in die richtige Richtung. Dass solche Selbstverständlichkeiten wie individualisierte Passwörter in ein Gesetz geschrieben werden müssen, ist ein klarer Hinweis darauf, dass vielen Herstellern die Sicherheit ihrer Kunden immer noch egal ist.“

Das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) sagt auf Anfrage:

„Die Einführung der skizzierten Regelung für Hersteller von vernetzten Geräten in Deutschland bzw. in der Europäischen Union würde das BMJV begrüßen.“

Auf EU-Ebene wird derzeit über einen „Cybersecurity Act" (CSA [12]) verhandelt, der unter anderem die Sicherheit vernetzter Geräte in den Fokus nimmt. Ähnlich wie das für andere Produkte längst der Fall ist, soll in Zukunft auch Software in Geräten mit einem Gütesiegel zertifiziert werden. Expert*innen kritisieren die Lösung jedoch als zahnlos, weil das Siegel freiwillig bleiben soll und Hersteller*innen, die Auflagen nicht erfüllen, keine Sanktionen füchten müssen. Ralf Bendrath, Politikberater für die Grünen um EU-Parlament, sagt, seine Fraktion habe verpfichtende Mindeststandards vorgeschlagen, aber die Kommission scheue sich „vor zu vielen Auflagen für die Industrie“.

Auf das größte Problem in diesem Zusammenhang hatte Jan-Peter Kleinhans [13], Projektleiter "IT-Sicherheit im Internet der Dinge", hingewiesen [14], der sich für den Think Tank »Stiftung Neue Verantwortung [15]« mit dem Internet der Dinge befasst: Die virtuelle Welt ändert sich ständig. Für Software werden teils mehrmals die Woche neue Updates geschrieben. Anders als etwa ein Vorhang, der einmal als feuerfest und schadstofffrei zertifiziert werden kann, kann die Zertifizierung einer Software deswegen „immer nur eine Momentaufnahme sein,“ sagt Kleinhans. Was interessiert es aber eine Kundin im Laden, ob der Router vor einem Jahr als sicher galt? Sein Vorschlag: Jedes Gerät sollte mit einem QR-Code [16] versehen werden, über den Nutzer*innen den aktuellen Sicherheitsstatus in einer Datenbank einsehen könnten. Im aktuellen Entwurf ist eine solche Lösung nicht vorgesehen.

Chris Köver

_____

Chris Köver schreibt zu Datenschutz, Netzkultur und sozialen Bewegungen. Sie hat als Autorin für Die Zeit, De:bug und Spiegel Online gearbeitet. Von 2008 bis 2014 war sie Chefredakteurin des Missy Magazine [17], später arbeitete sie in der Redaktion von WIRED Germany. Seit Sommer 2018 ist sie Redakteurin bei Netzpolitik.org. Kontakt: E-Mail [18], OpenPGP [19], Twitter [20].

netzpolitik.org ist eine Plattform für digitale Freiheitsrechte. Die Betreiber und deren Autoren thematisieren die wichtigen Fragestellungen rund um Internet, Gesellschaft und Politik und zeigen Wege auf, wie man sich auch selbst mithilfe des Netzes für digitale Freiheiten und Offenheit engagieren kann. Mit netzpolitik.org beschreiben sie, wie die Politik das Internet durch Regulation verändert. Und wie das Netz Politik, Öffentlichkeiten und alles andere verändert. Sie verstehen sich als journalistisches Angebot, sind jedoch nicht neutral. Ihr Haltung ist: Engagement für digitale Freiheitsrechte und ihre politische Umsetzung.

[3]

► **Quelle:** Erstveröffentlicht am 09. Oktober auf NETZPOLITIK.org >>Artikel [21]. **Lizenz:** Die von NETZPOLITIK verfassten Inhalte stehen, soweit nicht anders vermerkt, unter der Lizenz Creative Commons (Namensnennung - Nicht-kommerziell - Weitergabe unter gleichen Bedingungen 4.0 International (CC BY-NC-SA 4.0 [22]). Die Bilder im Artikel sind nicht Bestandteil des Originalartikels und wurden von KN-ADMIN Helmut Schnug eingefügt. Für sie gelten ggf. andere Lizenzen, s.u..

► Bild- und Grafikquellen:

1. Hacker / Cybercriminal. X. Foto: Richard Patterson > www.comparitech.com. **Quelle**: Flickr [23]. **Verbreitung** mit CC-Lizenz Namensnennung 2.0 Generic (CC BY 2.0 [24]).

2. Ablauf der Entstehung und Verwendung von Botnetzen: (1) Infizierung ungeschützter Computer, (2) Eingliederung in das Botnet, (3) Botnetbetreiber verkauft Dienste des Botnets, (4) Ausnutzung des Botnets, etwa für den Versand von Spam. **Urheber:** Tom-b. **Quelle:** Wikimedia Commons [25]. Diese Datei ist unter derCreative-Commons [26]-Lizenz „Namensnennung – Weitergabe unter gleichen Bedingungen 3.0 nicht portiert“[27] lizenziert.

Anhang	Größe
Jan-Peter Kleinhans: Europe vs the Internet of Crap. Regulierung von IT-Sicherheit - EU Cybersecurity Act [14]	589.46 KB

Quell-URL: https://kritisches-netzwerk.de/forum/internet-der-dinge-kalifornien-verbietet-standardpasswoerter

Links
[1] https://kritisches-netzwerk.de/user/login?destination=comment/reply/7490%23comment-form
[2] https://kritisches-netzwerk.de/forum/internet-der-dinge-kalifornien-verbietet-standardpasswoerter
[3] https://netzpolitik.org/
[4] https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327
[5] https://de.wikipedia.org/wiki/Jerry_Brown
[6] https://netzpolitik.org/2016/massenausfall-bei-der-telekom-hinweise-auf-angriff-verdichten-sich/
[7] https://de.wikipedia.org/wiki/Bruce_Schneier
[8] https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/09/17/the-cybersecurity-202-

california-s-internet-of-things-cybersecurity-bill-could-lay-groundwork-for-federal-action/5b9e6e331b326b47ec959638/?noredirect=on&utm_term=.4375be8b5ff4
[9] https://blog.erratasec.com/2018/09/californias-bad-iot-law.html#.W7tqnBQ_-V5
[10] https://de.wikipedia.org/wiki/Mirai_(Malware)
[11] https://de.wikipedia.org/wiki/Chaos_Computer_Club
[12] https://www.consilium.europa.eu/de/policies/cyber-security/
[13] https://www.stiftung-nv.de/de/person/jan-peter-kleinhans
[14] https://kritisches-netzwerk.de/sites/default/files/jan-peter_kleinhans_-_europe_vs_the_internet_of_crap_-_regulierung_von_it-sicherheit_-_eu_cybersecurity_act.pdf
[15] https://www.stiftung-nv.de/
[16] https://de.wikipedia.org/wiki/QR-Code
[17] http://www.missy-magazine.de
[18] mailto:chris@netzpolitik.org
[19] https://sks-keyservers.net/pks/lookup?op=get&search=0x5E598DD0D37B9F71A88DD92233D38859243016F9
[20] http://www.twitter.com/ckoever
[21] https://netzpolitik.org/2018/internet-der-dinge-kalifornien-verbietet-standardpasswoerter-ein-modell-fuer-deutschland/
[22] https://creativecommons.org/licenses/by-nc-sa/4.0/deed.de
[23] https://www.flickr.com/photos/136770128@N07/23128616532/
[24] https://creativecommons.org/licenses/by/2.0/deed.de
[25] https://commons.wikimedia.org/wiki/File:Botnet.svg
[26] https://en.wikipedia.org/wiki/de:Creative_Commons
[27] https://creativecommons.org/licenses/by-sa/3.0/deed.de
[28] https://kritisches-netzwerk.de/tags/authentifizierungssysteme
[29] https://kritisches-netzwerk.de/tags/bmjv
[30] https://kritisches-netzwerk.de/tags/bot-netze
[31] https://kritisches-netzwerk.de/tags/botnet
[32] https://kritisches-netzwerk.de/tags/botnetz
[33] https://kritisches-netzwerk.de/tags/botnetze
[34] https://kritisches-netzwerk.de/tags/bruce-schneier
[35] https://kritisches-netzwerk.de/tags/ccc
[36] https://kritisches-netzwerk.de/tags/chaos-computer-club
[37] https://kritisches-netzwerk.de/tags/chris-kover
[38] https://kritisches-netzwerk.de/tags/computersicherheit
[39] https://kritisches-netzwerk.de/tags/csa
[40] https://kritisches-netzwerk.de/tags/cybersecurity
[41] https://kritisches-netzwerk.de/tags/cybersecurity-act
[42] https://kritisches-netzwerk.de/tags/datenschutz
[43] https://kritisches-netzwerk.de/tags/edmund-gerald-brown-jr
[44] https://kritisches-netzwerk.de/tags/eu-cybersecurity-act
[45] https://kritisches-netzwerk.de/tags/frank-rieger
[46] https://kritisches-netzwerk.de/tags/internet-der-dinge
[47] https://kritisches-netzwerk.de/tags/internet-crap
[48] https://kritisches-netzwerk.de/tags/it-sicherheit
[49] https://kritisches-netzwerk.de/tags/jan-peter-kleinhans
[50] https://kritisches-netzwerk.de/tags/jerry-brown
[51] https://kritisches-netzwerk.de/tags/mirai
[52] https://kritisches-netzwerk.de/tags/passwort
[53] https://kritisches-netzwerk.de/tags/passworter
[54] https://kritisches-netzwerk.de/tags/qr-code
[55] https://kritisches-netzwerk.de/tags/quick-response
[56] https://kritisches-netzwerk.de/tags/ralf-bendrath
[57] https://kritisches-netzwerk.de/tags/robert-graham
[58] https://kritisches-netzwerk.de/tags/schadsoftware
[59] https://kritisches-netzwerk.de/tags/silicon-valley
[60] https://kritisches-netzwerk.de/tags/standardpassworter
[61] https://kritisches-netzwerk.de/tags/stiftung-neue-verantwortung-e-v