Fefes Blog

Originalartikel

Backup

<html> [l] Findet doch mal in eurem Browser die Liste der als vertrauenswürdig markierten CAs. Das sind die Stellen, die Zertifikate ausstellen dürfen, denen der Browser dann traut. Diese Liste war schon immer unfassbar lang und beinhaltet so Entitäten wie „e-commerce monitoring GmbH“ (wat!?) und natürlich Konzerne und staatliche Stellen aus aller Herren Länder. Ich sage nur: GUANG DONG CERTIFICATE AUTHORITY. Nehmen wir mal an, ihr klickt zu https://blog.fefe.de/ und euer Browser baut eine TLS-Verbindung auf. Dann meldet sich die Gegenstelle (hoffentlich, aber nicht unbedingt, mein Server!) mit einem mit meinem Public Key signierten Handshake, und mein Public Key ist signiert von Let's Encrypt, und Let's Encrypt ist in der Liste in eurem Browser. Daher weiß euer Browser, dass er mit meinem Server redet und nicht mit der NSA. Aber weiß er das wirklich? Was wenn sich da jemand anderes meldet, sagen wir mal der chinesische Geheimdienst fängt die Verbindung ab und leitet die zu sich selbst um, und da kommt dann ein gültig aussehendes Handshake, das aber von einer anderen CA in eurer Browserliste signiert wurde! Zum Beispiel von „Hong Kong Post“. Dann würde euer Browser das auch akzeptieren. Die Telekom hat auch eine CA in der Liste. Das ist ein fundamentales Problem bei der ganzen TLS-Nummer, für die es auch keine wirklich tolle Lösung gibt. Bisherige Ansätze sind, dass ich in meinem DNS einen Eintrag haben kann, dass nur Let's Encrypt CAs ausstellen darf. Andere CAs sollten sich dann weigern, wenn der Geheimdienst kommt und ein Cert ausgestellt haben will. Das nimmt aber gutmeinende, nicht kompromittierte und nicht an gesetzliche Vorgaben gebundene CAs an. Der nächste Ansatz ist, dass alle CAs sich zu Transparenz verpflichtet haben, und alle ausgegebenen Zertifikate automatisiert in eine gemeinsame öffentlich einsehbare Liste eintragen. Das nimmt leider auch eine gutmeinende, nicht kompromittierte CA an. Warum erzähle ich das alles? Erstens um noch mal Honest Achmed's Used Cars and Certificates zu verlinken. 🙂 Aber der dringendere Grund ist, dass die EU gerade an der eIDAS-Verordnung arbeitet, bei der es um digitale Identitäten für die EU geht. Das hehre (und gute!) Ziel ist, „Login via Google“ kaputtzumachen. Ihr Plan ist, ein eigenes System zu bauen, ein staatliches System, und das hat dann natürlich eine eigene CA, und die kommt in alle Browser und jedes Mitgliedsland bietet eine Wallet-App an, die dann auf alle Smartphones kommt, und Behörden und Google und Facebook und co werden dann gezwungen, Logins via dieser Wallets zu ermöglichen. Schlimmer noch: dafür kriegt dann jeder Bürger endlich einen Barcode auf den Vorderarm tätowiert (Deutschland ist endlich wieder Technologieführer!!1!), äh, einen lebenslang gültigen eindeutigen Identifier zugewiesen, mit dem der Staat dann schön alle Bürger tracken kann. Ich würde ja von der Benutzung von sowas immer grundsätzlich abraten, weil man damit Google staatlich validierte Daten gibt, die deren Datensätze massiv aufwerten. Aber der Punkt, wieso ich das hier alles überhaupt ausrolle, ist ein anderer. Die CAs sollen dann in die Browser, und zwar per Verordnung, d.h. staatlich erzwungen. Im Moment kann man im Browser CAs als unvertrauenswürdig markieren. Das darf der Browser dann bei diesen staatlichen CAs nicht

erlauben. Mit anderen Worten: Hier kommt per EU-Verordnung eine TLS-Hintertür in alle eure Browser. Die erlaubt Polizeien und Geheimdiensten das Ausstellen von Zertifikaten für jede Webseite, bei der sie das gerne haben wollen, und damit können sie dann einen Man-in-the-Middle-Angriff gegen jeden fahren, und zwar nicht nur innerhalb der EU, und deren Verbindungen mitlesen oder auch manipulieren und sich als Server ausgeben. Die EFF warnt da seit Jahren vor. Aktuell gibt es einen offenen Brief von hunderten von Experten dagegen. Ist alles ganz traurig, insbesondere weil sich die EU damit hinter Ländern wie Kasachstan und Indien einreiht, die ihren Bürgern bereits Zwangs-CAs oder „digitale ID“-Systeme aufgedrängt haben. </html>