Wer das Internet sicherer macht, soll belohnt werden

23 Mai 2017 | **Blockchain, Insight Zühlke** | **Jörg Dirbach**
Lesezeit: 2 Minutes

Man-in-the-Middle-Angriffe im SSL-Ecosystem stehen noch immer auf der Liste der häufigsten und folgenreichsten Attacken in der heutigen Onlinewelt. Egal ob beim Banking oder bei der Übertragung vertraulicher Krankenakten: Alle Browser setzen heute auf SSL-Verschlüsselung. Die Benutzer vertrauen dabei auf das kleine Schloss in der Adresszeile. Dieses Schloss bietet allerdings häufig keine Sicherheit. Denn fehlerhafte oder ungültige SSL-Zertifikate jubeln dem Benutzer ungültige kryptographische Schlüssel unter, die zur Folge haben, dass dem Angreifer direkt in die Hände gespielt wird. Die sensiblen Daten gelangen unmittelbar zum Angreifer und eben nicht zur heimischen Bank oder zum Krankenversicherer. Das Problem: Solch fehlerhafte SSL-Zertifikate sind nur schwer zu erkennen. Sie werden ausgestellt von Certificate Authorities (CA), die entweder kompromittiert sind oder keine gründlichen Sicherheitschecks durchführen.

Ein erster Ansatz im Kampf gegen diese ungültigen SSL-Zertifikate sind Log-basierte PKI-Erweiterungen wie Googles „Certificate Transparency“. Oft fehlt es jedoch an monetären Anreizen, diese Logs und Monitore zu betreiben. Darüber hinaus sind keine automatisierten Aktionen spezifiziert, die den betroffenen Domains helfen würden, die entstandenen Schäden zu reparieren.

An einer der renommiertesten und meistzitierten Sicherheitskonferenzen, dem IEEE Symposium on Security & Privacy in San Francisco, wird heute die Forschungsarbeit „IKP: Turning a PKI Around with Blockchains“ des Zühlke Mitarbeiters und IT-Security-Spezialisten Raphael Reischuk präsentiert, der mit Stephanos Matsumoto von der Carnegie Mellon University die Blockchain Ethereum so erweitert hat, dass alle Akteure vollautomatisch belohnt werden, die ungültige SSL-Zertifikate melden. Darüber hinaus werden in diesem System die betroffenen Domains vollautomatisch entschädigt und die fehlerhaften CA werden zur Rechenschaft gezogen. Der Einsatz der Blockchain ermöglicht dabei eine dezentrale Verwaltung und eine offene Partizipation aller Teilnehmer des World Wide Web. Domains erhalten somit beim Erwerb eines SSL-Zertifikates einen automatisierten Versicherungsschutz: Wird für eine Domain ein ungültiges Zertifikat ausgestellt, gibt es unmittelbar eine monetäre Entschädigung – für die Domain und für denjenigen, der das fehlerhafte Zertifikat meldet. Die ausstellende CA verliert die zuvor hinterlegte Sicherheitsleistung und wird dazu gedrängt, ihre Sicherheitsstandards zu erhöhen. Dieser neuartige Ansatz führt folglich zu deutlich mehr Transparenz und massgeblich verbessertem

Datenschutz im Internet.

Update: Ein Video der Präsentation der Forschungsarbeit gibt es hier.