31. Mai 2019 Studie · Web & Cloud · Digitale Identität

# Erkennung Zertifikatsmissbrauch über CTL

Der Volltext liegt derzeit nur in der Fassung „English“ vor. Die Übersetzung folgt.

**Archiviert.** Dieser Inhalt wird nicht mehr aktualisiert. Er bleibt zur Information verfügbar.

**Quelle** https://technology2.a-sit.at/veroeffentlichungen/erkennung-zertifikatsmissbrauch-ueber-ctl/

Certificate Transparency (CT) ist ein offenes Framework, mit dem die Ausstellung von SSL/TLS-Zertifikaten „sichtbar“ gemacht wird, indem Zertifizierungsstellen dazu verpflichtet werden, jedes von ihnen ausgestellte Zertifikat in öffentlichen, manipulationssicheren, append-only Protokollen zu veröffentlichen. In diesem Projekt sollte untersucht werden, ob CT-Protokolleinträge als einzige Datenquelle für die Erkennung von Phishing-Websites verwendet werden können. Umgesetzt wurde ein System, welches die Phishing-Wahrscheinlichkeit neu ausgestellter Zertifikate auf Basis von Machine Learning bewertet. Daten werden direkt aus CT-Protokolldaten extrahiert und Webseiten, bzw. Zertifikate ausgehend davon in eine von fünf verschiedenen Risikokennzeichnungen klassifiziert, welche von _legitim _bis _hochverdächtig _reichen. Die Bewertungsergebnisse belegen die Wirksamkeit des Ansatzes mit einer Erfolgsquote von über 90%. Die Ergebnisse bestätigten, dass CT tatsächlich eine wertvolle Datenquelle ist, die maschinell verarbeitet werden kann, um automatisierte Warnsysteme zu konzipieren. Durch die ausschließliche Verwendung von CT Log-Daten und den Verzicht auf zusätzlichen Website-Quellcode oder Netzwerktraffic-Analysen kann das System nahezu in Echtzeit Ergebnisse liefern, wodurch die Zeit zum Erkennen von Phishing-Websites erheblich verkürzt wird. Das Projekt führte zu einem wissenschaftlichen Beitrag, der auf der 15. Internationalen EAI-Konferenz SecureComm 2019 angenommen wurde.