REVERSE FINGERPRINTING: ERKENNEN VON POTENTIELLEN SICHERHEITSRISIKEN BEI INTERNET-DIENSTANBIETERN

Ref-Nr: TA-18/071TLB

HINTERGRUND

Sowohl Firmenkunden als auch Privatkunden nutzen immer häufiger Internetdienste zur Bearbeitung auch vertraulicher Dateien. Vorteile sind, dass der Datenzugriff von jedem Ort möglich ist, sobald eine Internetverbindung vorhanden ist, Dateien einfach gemeinsam bearbeitet werden können und beim Provider verfügbare Software gemietet werden kann.
Allerdings steht und fällt die Sicherheit der Daten mit der Aktualität der providerseitig verwendeten Software, wie z. B. Services, Datenbanken, Programmierumgebungen, Server-Software, Serverhost, Serverhardware und Infrastruktur, da viele Aktualisierungen die Hauptfunktion haben, erkannte Sicherheitslücken zu schließen.

PROBLEMSTELLUNG

Bislang gibt es keine Möglichkeit, unabhängig vom Serviceprovider zu verifizieren, welche Software-Versionen genutzt werden, da Versionsnummern teilweise verborgen oder nicht korrekt angegeben werden, um vor Angriffen zu schützen (Security by Obfuscation). Häufig werden auch Installationen von Sicherheitspatches zurückgestellt, um Kosten zu sparen.
Dieser Zustand ist allerdings für viele Nutzer beunruhigend, da der Kunde nicht nachvollziehen kann, ob der Service-Provider Upgrades zeitnah einspielt, was in Bezug auf Datensicherheit – gerade bei öffentlich zugänglichen Servern – immens wichtig ist.
Bereits vorhandene Verfahren, die nach Sicherheitslücken bei Internetdiensten suchen (Security Audits), benötigen entweder einen speziellen Zugriff (Vulnerabiltity Scanner) und werden daher oft vom Provider selbst durchgeführt oder nutzen dedizierte Schnittstellen, um die Versionsnummern zu ermitteln (Penetration Tests).

LÖSUNG

Mit der neu entwickelten Methode Reverse Fingerprinting (RFP) ist es nun erstmals möglich, alleine durch Nutzung des Kundenzugangs und ohne

TLB
Technologie-Lizenz-Büro
der Baden-Württembergischen
Hochschulen GmbH

Technologie-Lizenz-Büro (TLB) der Baden-Württembergischen Hochschulen GmbH

Anne Böse, M.Sc.
+ 49 721 790 040
boese@tlb.de
www.tlb.de

ENTWICKLUNGSSTAND

Funktionsnachweis

PATENTSITUATION

EP anhängig
PCT anhängig

CATEGORIES

//Datensicherheit //Software

Unterstützung des Serviceproviders, die Versionsnummern der installierten Software korrekt zu ermitteln.
Bei Release von neuen Softwareversionen wird einmalig ein eindeutiges Unterscheidungsmerkmal (Fingerprint) zur Vorgängerversionen identifiziert und eine Abfrage erstellt, deren Ergebnis die eine oder andere Version ausschließt. Diese Abfragen werden in einer Datenbank gespeichert und können künftig automatisiert durchgeführt werden. Durch mehrfache Abfragen werden alle Versionen mit Ausnahme der tatsächlich vorliegenden ausgeschlossen.
Das Verfahren ermöglicht eine Prüfung der installierten Software-Versionen und damit der Aktualität und Sicherheit der genutzten Plattform rein durch Nutzung einer Kundenauthentifizierung.

VORTEILE

- Verifikation der genutzten Software-Version ohne Kooperation der Provider möglich
- Breite Anwendbarkeit durch Nutzung intrinsischer Eigenschaften
    - Unabhängig von Schnittstellen
    - Vielzahl von Services wie Foren, CMS, Programmiersprache, Datenbanken, Server-Software und Server Host analysierbar
- Effizient und automatisiert auf mehreren Systemen durchführbar

ANWENDUNGSBEREICHE

Das an der Universität Mannheim neu entwickelte Verfahren ermöglicht die Prüfung der installierten Versionen beim Serviceprovider ohne auf dedizierte Schnittstellen oder Providerunterstützung angewiesen zu sein.

SERVICE

Die Technologie-Lizenz-Büro GmbH ist mit der Verwertung der Technologie beauftragt und bietet Unternehmen die Möglichkeit der Lizenznahme.

PUBLIKATIONEN & VERWEISE

Christian A. Gorke, Frederik Armknecht:
"Reverse Fingerprinting",
arXiv preprint arXiv:1912.09734 (2019);
arxiv.org/abs/1912.09734