UNIVERSITÄT BONN

MISPbump

Einfache und sichere Synchronisierung von MISP-Instanzen

1. MISP – Malware Information Sharing Platform

MISP ist eine Open Source Thread Intelligence Plattform zum **teilen**, **speichern** und **korrelieren** von „Indicators of Compromise“ (IoC), Informationen über Finanzbetrug oder Verwundbarkeiten bis hin zu Anti-Terror Informationen. Unternehmen können diese Funktionen eigenständig oder in Zusammenarbeit mit weiteren Unternehmen nutzen um Attacken und Bedrohungen auf ICT-Infrastrukturen, Unternehmen oder Personen in Echtzeit zu **erkennen** und zu **verhindern**.
Die technischen/nicht-technischen Informationen (MISP-Events), wie zum Beispiel Malware-Proben oder Informationen über Vorfälle oder Angreifer, können automatisch mit weiteren relevanten MISP-Events in Verbindung gebracht werden. Des weiteren sind standardmäßig diverse OSINT-Feeds integriert, die eine einfache und schnelle Korrelation mit vorhandenen MISP-Events ermöglichen[1]. Um den Datenschutzrichtlinien verschiedener Unternehmen gerecht zu werden, besitzt MISP eine Filterlogik die es erlaubt Informationen nur mit ausgewählten Partnern zu teilen.[2]

2. Synchronisieren von MISP-Instanzen

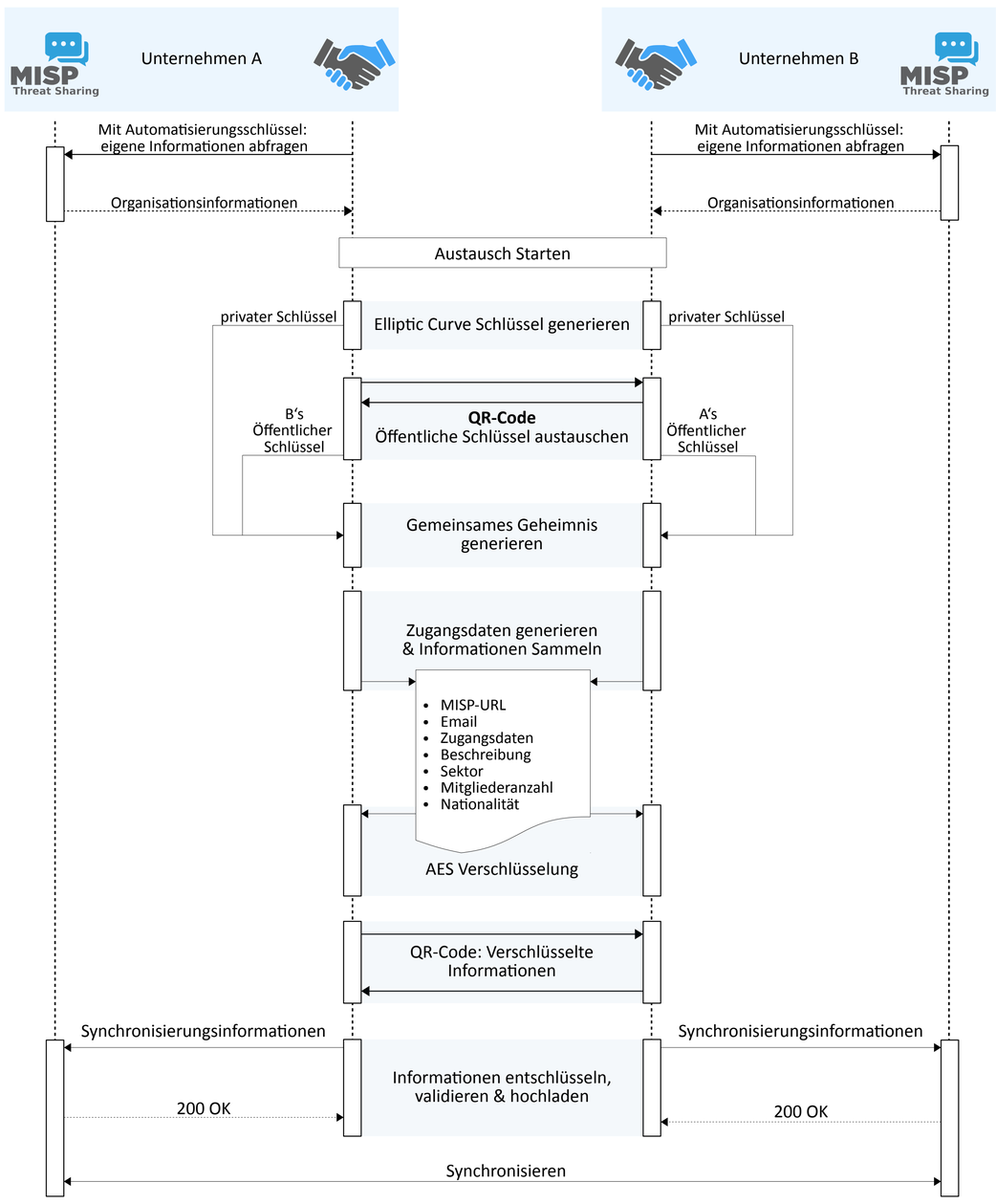
Damit MISP-Instanzen ihre MISP-Events mit ausgewählten Partnern teilen können, müssen sie sogenannte Sync-Server und Sync-User einrichten welche miteinander verknüpft werden müssen. Dieser Prozess findet auf beiden Instanzen gleichermaßen statt, da die Sync-Server-/Sync-User-Kombination nur eine einseitige Kommunikation erlaubt. Um die Synchronisationspartner identifizieren zu können, wird ein lokaler Eintrag des jeweiligen Unternehmens auf der eigenen MISP-Instanz gespeichert. Diese Informationen müssen manuell eingeholt und eingetragen werden und reichen von einer einfachen Beschreibung des Unternehmens bis hin zu dem Sektor in dem es agiert. Über welchen Kanal dieser Datenaustausch stattfindet und wie sicher dieser ist, ist nicht definiert. Dies kann in vielen Fällen zu fehlerhaften oder unvollständigen Informationen über die Unternehmen führen. Im schlimmsten Fall können Zugangsdaten in die Hände von Dritten geraten. Um das zu verhindern wurde MISPbump entwickelt.

3. Was ist MISPbump?

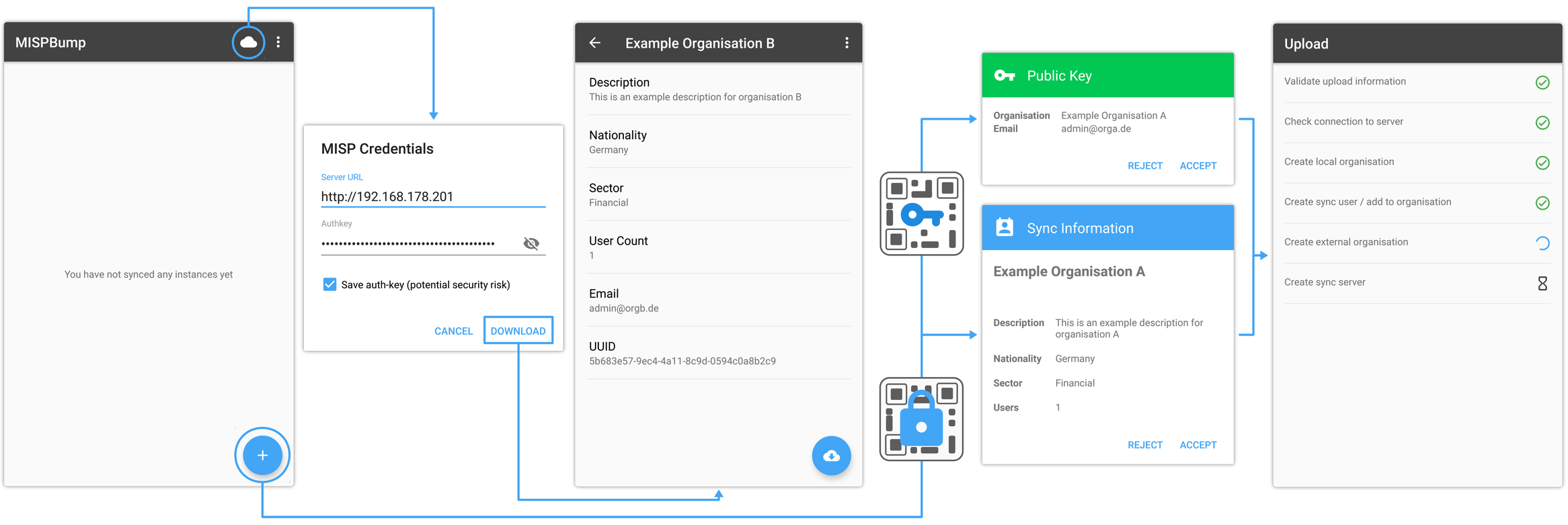
MISPbump ist eine Android App die den bisherigen Synchronisierungsprozess durch den Austausch von QR-Codes **einfacher** und **schneller** macht. Die Informationen der Unternehmen sind stets **aktuell** und **sicher**, da sie automatisch von der MISP-Instanz geladen und verschlüsselt ausgetauscht werden. Am Anfang jeder Synchronisation werden die mittels Elliptischer Kurven generierten Schlüssel mit dem Diffie-Hellman-Protokoll ausgetauscht. Das daraus resultierende gemeinsame Geheimnis wird dazu verwendet die sensiblen Daten mittels AES-256-CBC zu verschlüsseln.

4. MISPbump Kommunikation & Funktionsweise

Das Folgende Diagramm beschreibt die Kommunikation und weitere Details während eines Austauschs zweier Partner.



5. Screenshots



6. Referenzen

[1] MISP | Feeds (2018) https://misp-project.org/feeds
[2] MISP | Who (2018) https://misp-project.org/who

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung