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, 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 IT-Infrastrukturen, Unternehmen oder Personen in Echtzeit zu **erkennen** und zu **verhindern**.
Die technischen/nicht-technischen Informationen (MISP-Events), wie zum Beispiel Malware-Samples 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

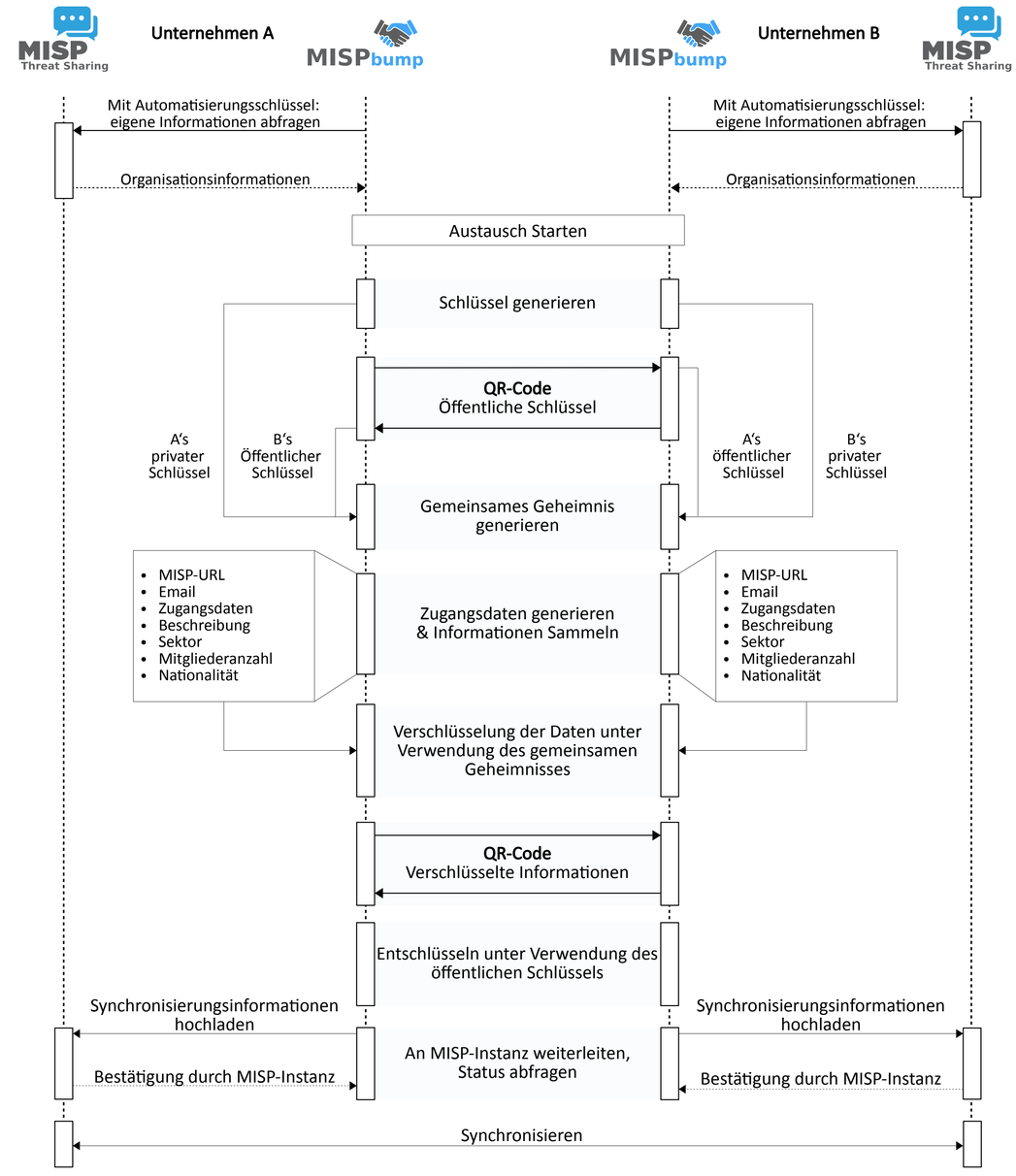
Damit zwei Unternehmen ihre MISP-Events teilen können, müssen sie ihre MISP-Instanzen miteinander verknüpfen. Die Synchronisationspartner legen ein Profil des jeweils anderen Unternehmens auf ihrer eigenen MISP-Instanz an. Die dazu erforderlichen Informationen müssen manuell eingeholt und eingetragen werden. Diese Informationen reichen von einer einfachen Beschreibung des Unternehmens, bis hin zu dem Sektor in dem es agiert. Dies kann zu fehlerhaften oder unvollständigen Informationen über die Unternehmen führen. Wird zusätzlich ein unsicherer Kanal verwendet, können Zugangsdaten in die Hände von Dritten geraten und somit das mitlesen von sicherheitsrelevanten Informationen ermöglichen. MISPbump wurde entwickelt um eine einheitliche und sichere Methode zur Synchronisation bereit zu stellen und den oben genannten Prozess zu vereinfachen.

3. Was ist MISPbump?

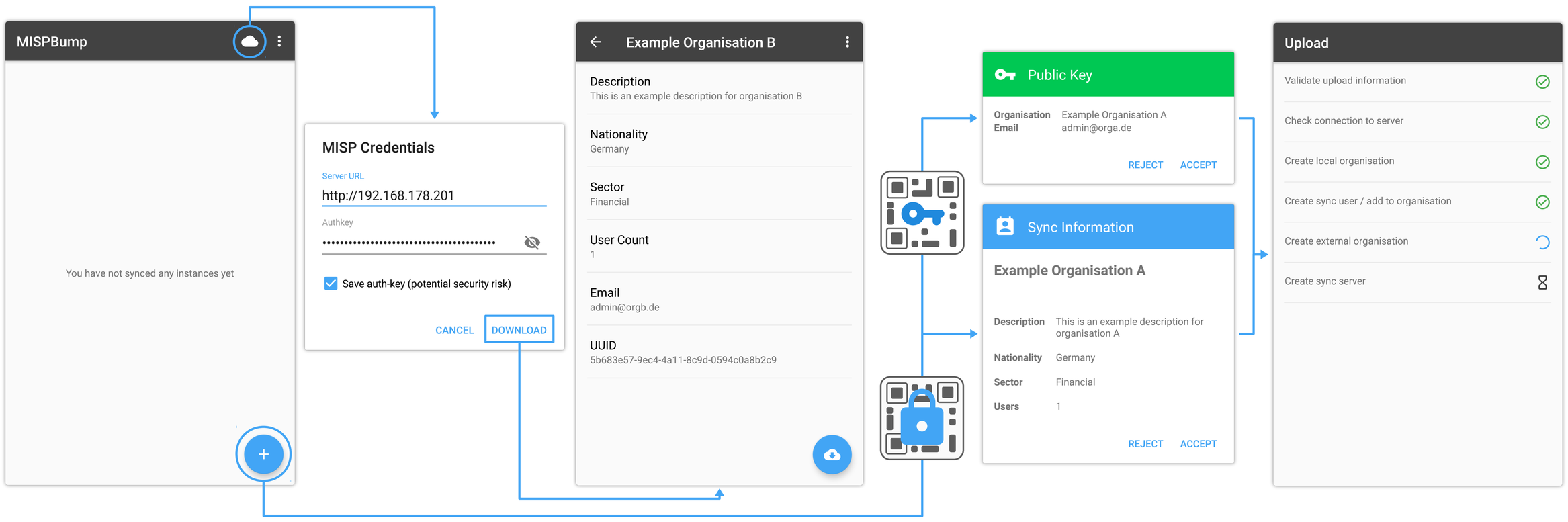
MISPbump ist eine Android App, die den bisherigen Synchronisierungsprozess durch den Austausch von verschlüsselten QR-Codes einfach und sicher macht. Die zum synchronisieren notwendigen Daten müssen nicht etwa manuell eingegeben und gepflegt werden, sondern werden automatisch von der eigenen MISP-Instanz geladen um sie dann mit ausgewählten Partnern teilen zu können. Damit MISPbump sowohl in der Gegenwart als auch in der nahen Zukunft den geltenden Sicherheitsstandarts entspricht, wurden ausschließlich „State-Of-The-Art“ Technologien implementiert.

4. MISPbump Kommunikation & Funktionsweise

Es folgt eine schematische Darstellung des Austauschprozesses. Vor dem eigentlichen Austausch ruft jede MISPbump-Instanz die aktuellsten Informationen der eigenen MISP-Instanz ab. Der nachfolgende Prozess besteht aus drei Schritten: Schlüssel generieren, Öffentliche Schlüssel mittels QR-Code austauschen und anschließend die verschlüsselte Daten mit einem weitern QR-Code austauschen.



5. Screenshots



6. Referenzen

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

Felix Prahl-Kamps, …?

itsec.cs.uni-bonn.de/overview/

Rheinische Friedrich-Wilhelms-Universität Bonn
Institute of Computer Science 4

mm@cs.uni-bonn.de

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung