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, Verwundbarkeiten bis hin zu Anti-Terror Informationen. Unternehmen können diese Funktionen, eigenständig oder in Kollaboration 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), zum Beispiel Malware-Proben, Vorfällen oder Angreifern können automatisch durch MISP korreliert werden. Korrelation kann anhand der verknüpften Attribute, „Fuzzy Hashing“ oder „CIDR Block matching“ erfolgen, beziehungsweise komplett ausgeschaltet werden. Außerdem können vorhandene MISP-Events mit jeglichen (Drittanbieter) OSINT-Feeds korreliert werden, ohne diese direkt auf die eigene Instanz laden zu müssen. MISP bietet eigene Standard OSINT-Feeds an die umgehend zur Korrelation genutzt werden können. Um den verschiedenen Datenschutz Richtlinien der Organisationen gerecht zu werden, besitzt MISP eine Filterlogik die es ermöglicht Informationen mit nur ausgewählten Partnern, oder nur Teile dieser Informationen zu teilen. [1]

## 2. Synchronisieren von MISP-Instanzen

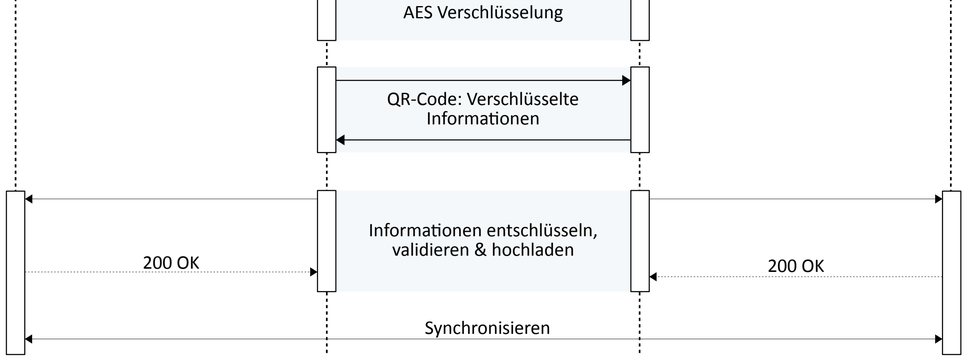
Damit MISP-Instanzen Ihre MISP-Events mit ausgewählten Partnern teilen können, müssen sie sich über ein sogenannten Sync-Server mit entsprechendem Sync-User auf der anderen Instanz verknüpfen. Dieser Prozess findet auf beiden Instanzen gleichermaßen statt, da die Kombination aus Sync-Server und Sync-User nur eine einseitige Kommunikation erlaubt. Um Synchronisationspartner identifizieren zu können, wird ein lokaler Eintrag der jeweiligen Organisation auf der eigenen MISP-Instanz gespeichert. Die Informationen reichen von einer einfachen Beschreibung des Unternehmens bis hin zu dem Sektor in dem es agiert.
Über welchen Kanal dieser Datenaustausch stattfindet und vor allem wie sicher dieser ist, ist dabei jedem selbst überlassen. Dies kann in vielen Fällen zu fehlerhaften oder unvollständigen Informationen über die andere Organisation führen. Darüber hinaus kann durch eine fehlerhafte Übertragung der Autorisierungsschlüssel in die Hände von Dritten geraten.

## 3. Was ist MispBump?

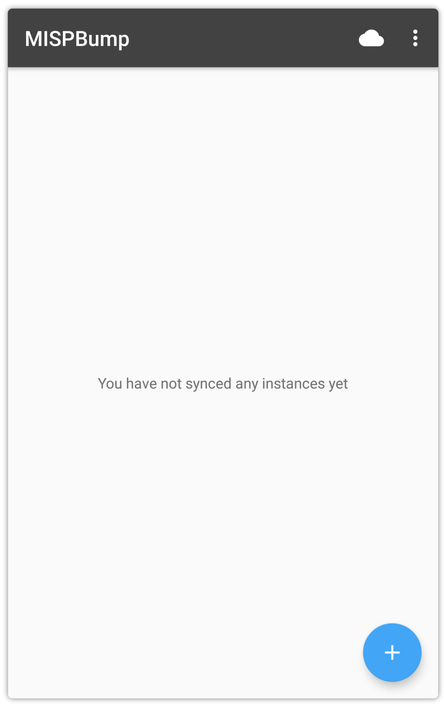
MispBump ist eine Android App die es ermöglicht auf **einfache** und **sichere** Weise MISP-Instanzen miteinander zu verknüpfen. MispBump bildet die Schnittstelle zwischen zwei Instanzen die sich synchronisieren wollen, um einerseits Fehler zu vermeiden und andererseits um die Integrität der Organisationsinformationen zu gewährleisten.

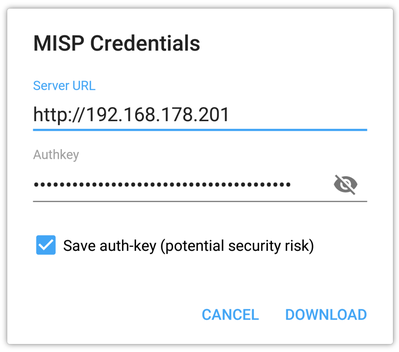
## 4. MISPbump Kommunikation & Funktionsweise

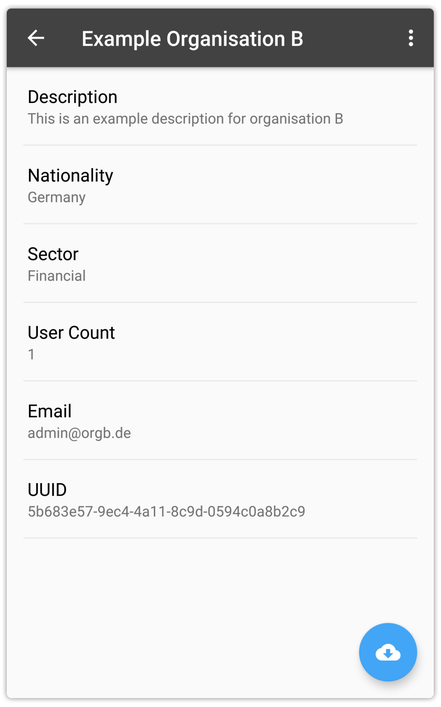
Das folgende Diagramm verdeutlicht die Kommunikation während einer Synchronisierung, sowohl zwischen den beiden Apps, als auch mit den jeweiligen MISP-Instanzen.

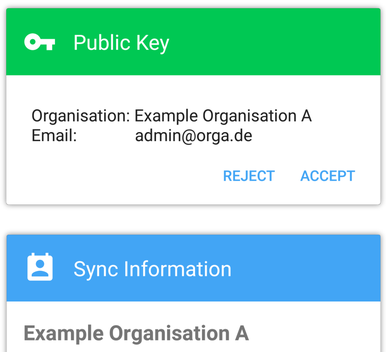


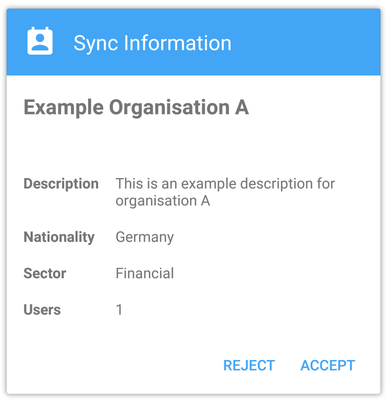

## 5. Screenshots




## X. Referenzen

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

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung