

DEFENSIVE

Datentreuhänder Plattform zum dezentralen
Austausch von IT-Sicherheitsvorfällen

Bessere Informationssicherheit durch den Austausch von Daten zu Sicherheitsvorfällen

Problemstellung und Lösungsansatz

In den vergangenen Jahren hat die Anzahl der IT-Sicherheitsvorfälle und die Schadenshöhe derartiger Vorfälle deutlich zugenommen. Organisationen können trotz erhöhter Gegenmaßnahmen kaum noch Schritt halten, wobei häufig zahlreiche Unternehmen mit gleichen oder ähnlichen Angriffen konfrontiert werden. Problematisch ist in diesem Szenario, dass die meisten Organisationen allein in der IT-Sicherheit kämpfen und somit gegen viele Angriffstypen anfällig sind.

Um diese Problemstellung zu lösen ist die Idee entstanden, Daten über Sicherheitsvorfälle zwischen Unternehmen auf vertrauenswürdige Art und Weise zu teilen, um so ein digitales Schutzschild um alle teilnehmenden Organisationen herum aufbauen zu können. Das Teilen von Daten kann dabei über eine sogenannte Datentreuhänder Plattform abgewickelt werden. Bestehende zentralisierte Datentreuhänder Plattformen stehen allerdings vor der Herausforderung, Nutzer von ihrer Vertrauenswürdigkeit überzeugen zu müssen und gleichzeitig Datenschutz und Anonymität zu wahren.

Im Rahmen des Projektvorhabens DEFENSIVE soll aus diesem Grund ein dezentrales Datentreuhänder Modell entwickelt und in der Praxis erprobt werden. Durch die Nutzung von Distributed Ledger Technologie sollen dabei Anreize zum partizipativen Datenaustausch gesetzt werden, ohne dass der Datenurheber die Kontrolle über seine Daten verliert. Zur praktischen Erprobung wird die Plattform auf die Anforderungen des Austauschs von IT-Sicherheitsvorfällen ausgerichtet. Die Datenverarbeitung muss dabei aufgrund der Sensibilität der Daten über IT-Sicherheitsvorfälle anonym, unter Gewährleistung des Datenschutzes, und Wahrung hoher Verlässlichkeitsanforderungen erfolgen. Gleichzeitig ist es für eine hohe Teilnahmequote von betroffenen Unternehmen wichtig, wirtschaftliche Anreize für die Bereitstellung eigener Daten zu geben, um das mit einer Datenspende verbundene Risiko zu kompensieren. Diese hohen Anforderungen wird das Forschungsprojekt DEFENSIVE durch eine Datentreuhänder Plattform zum dezentralen Austausch von IT-Sicherheitsvorfällen lösen und gleichzeitig ein ideales Testfeld zur späteren Übertragung auf weitere Anwendungsgebiete bieten.

Projektpartner

Die beteiligten Projektpartner sind DFN-CERT Hamburg, das IT-Sicherheitscluster Regensburg sowie die Universität Regensburg in Form des Lehrstuhls für Wirtschaftsinformatik 1 von Prof. Dr. Günther Pernul, die als größter Partner auch Koordinator des Vorhabens ist. Das Forschungsprojekt DEFENSIVE wird vom Bundesministerium für Bildung und Forschung (BMBF) gefördert.