Open Source Intelligence (OSINT) bei Schweizer Banken

Studiengang: MAS Digital Forensics & Cyber Investigation

Im Zuge der Digitalisierung und der neuen Technologien, veränderte sich die klassische Produktpalette der Banken. Die Finanzinstitute hatten in Vergangenheit den Fokus auf den Zahlungsverkehr gelegt. Das Internet hat einiges verändert. Schlagwörter dazu sind E-Banking, E-Commerce, Wallets (Tokenisierung), P2P Zahlungen oder Instant Payment. Die Vielfalt kennt mittlerweile keine Grenzen mehr, ebenso die Gefahr von Cyberkriminalität.

Einleitung

Die Cyberkriminalität nimmt zu, vor allem Phishing-Angriffe und Betrug im Zusammenhang mit Kryptowährungen und Online-Handel in der Schweiz sind für Schweizer Banken von Bedeutung. Infolgedessen haben Schweizer Banken in den letzten Jahren ihre Sicherheitsvorkehrungen verstärkt und Massnahmen ergriffen, um Betrug zu verhindern, einschließlich der Erhöhung der Überwachung von Transaktionen und der Einführung von Zwei-Faktor-Authentifizierung. Die PostFinance nutzt für die Überwachung ihrer Transaktionen im Bereich E-Banking und Debit-/Kreditkartenzahlungen unterschiedliche Tools um den Kunden vor unrechtmässigem Geldabfluss zu schützen. Die bewährten Tools nutzen bereits Machine Learning und können teilautomatisiert Entscheidungen treffen, aber Open Source Intelligence (OSINT) wird bei der PostFinance (noch) nicht genutzt. Was muss die PostFinance erfüllen, um OSINT einsetzen zu können und welchen Nutzen kann sie bei Transaktionen im Internet von OSINT ziehen? Mit dieser Fragestellung beschäftigt sich diese Arbeit.

Vorgehen

Die Arbeit fokussiert sich auf die beiden Bereiche Rahmenbedingungen für die Nutzung von OSINT bei PostFinance und welche OSINT Tools, Frameworks oder Lösungen kommen in spezifischen Fällen der Überwachung von Transaktionen in Frage. Die Klärung der Rahmenbedingungen ist stark geprägt vom aktuellen und neuen Datenschutzgesetz. Die Erarbeitung einer möglichen Lösung von OSINT bei der PostFinance wird als explorativer Teil in der Arbeit mit der Erörterung von Tools und Fallbeispielen aufgezeigt und durchgespielt. Die Resultate sollen eine Übersicht bieten für den Aufbau einer eigenen oder eingekauften OSINT Plattform.

Ergebnisse

Das Datenschutzgesetz birgt, sofern der Kunde ausreichend informiert wird welche Daten bearbeitet werden, keine Einschränkungen um OSINT zu nutzen und es sind keine weiteren Massnahmen mit den aktuellen Gegebenheiten notwendig bei der PostFinance.
Die Ergebnisse der Fallbeispiele zeigen eine Tendenz, dass sich für die PostFinance es sich sehr lohnen könnte, eine zusätzliche Kontrollinstanz zu den bestehenden Transaktionslösungen aufzubauen. Gerade im Bereich der IP-Adressen besteht ein hohes Potenzial mehr Detailinformationen zu erhalten und zu analysieren. Dies wird vor allem der Erkennung von betrügerischem Verhalten zu gute kommen und potenzielle Verluste können minimiert werden.

Ausblick

Die Empfehlung auf Basis dieser Master Theiss ist für die PostFinance in einem Folgeprojekt oder -studie zu prüfen, wie und welche Plattform in die IT-Landschaft integriert werden könnte und für welche weiteren Tätigkeiten OSINT gebraucht werden könnte. Denn OSINT bietet noch viele weitere Möglichkeiten.

David Nold