

# Sharing is Caring: Die Qualität des Informationsaustausches im Bereich CTI

Thomas Geras  
Hochschule München

Der Bereich der Cyber Threat Intelligence (CTI) spielt eine zentrale Rolle beim Schutz von Unternehmen vor sich ständig weiterentwickelnden Cyber-Bedrohungen. Der Begriff „Intelligence“ hat seinen Ursprung im Militärjargon, wird jedoch zunehmend im Bereich der Cybersecurity verwendet. CTI umfasst verwertbare und kontextbezogene Informationen, die durch das Sammeln, Verarbeiten und Analysieren von Bedrohungsdaten entstehen. Beispiele für CTI sind die sogenannten Indicators of Compromise (IoCs) oder Tactics, Techniques, and Procedures (TTPs). IoCs umfassen einfache Informationen, wie z. B. IP-Adressen, Hash-Werte oder Webdomänen. Komplexere Informationen über das Verhalten von Bedrohungsakteuren, wie die verwendeten Techniken und Taktiken, werden als TTPs bezeichnet.

Der CTI-Bereich steht jedoch vor mehreren anhaltenden Herausforderungen: (1) ein unzureichendes Verständnis der Funktionsweise von Sharing Communities, in denen Unternehmen, Regierungsbehörden, CERTs, Sicherheitsanbieter, akademische Einrichtungen und individuelle Experten zusammenarbeiten; (2) Probleme mit der Qualität der ausgetauschten Informationen sowie (3) ein überwältigender Zustrom irrelevanter Daten. Diese Herausforderungen behindern die Fähigkeit von Organisationen, CTI zu verarbeiten, darauf zu vertrauen und es effektiv zu nutzen.

Dieser Vortrag befasst sich mit drei miteinander verbundenen Aspekten von CTI, um diese Herausforderungen anzugehen. Auf Grundlage von 25 Experteninterviews werden zunächst die Strukturen von Sharing Communities erläutert, die als wichtige Drehscheiben für die Zusammenarbeit und den Austausch von CTI zwischen Organisationen dienen. Anschließend wird, ebenfalls basierend auf den Interviews, dargestellt, welche Informationen innerhalb von Sharing Communities ausgetauscht werden, welche Qualitätsmerkmale für Praktiker relevant sind und welche Qualitätssicherungsverfahren in der Praxis verwendet werden. Schließlich wird ein auf Relevanz basierendes Modell vorgestellt, um CTI mit den spezifischen Verteidigungsfähigkeiten einer Organisation in Einklang zu bringen. Dieses Modell nutzt die MITRE ATT&CK- und D3FEND-Frameworks, um Angriffstechniken mit Verteidigungsmaßnahmen zu verknüpfen, und ermöglicht es Unternehmen, Lücken in ihrer Verteidigung zu identifizieren und priorisierte, umsetzbare Erkenntnisse abzuleiten. Das Modell wurde anhand von Daten aus einer großen Sharing Community sowie einer von Experten begutachteten Fallstudie validiert.

Zusammengefasst zielen diese Beiträge darauf ab, das Verständnis, die Qualität, die Anwendbarkeit sowie den Informationsaustausch von CTI zu verbes-

ern und Organisationen in die Lage zu versetzen, die Komplexität moderner Cybersicherheitsbedrohungen effektiv zu bewältigen.