HAW HAMBURG

Grundseminararbeit

Assiel Taher

Cyber Threat Intelligence

Betreuung durch: Prof. Dr. Kai von Luck
Eingereicht am: 28. Februar 2019

Fakultät Technik und Informatik
Department Informatik

Faculty of Computer Science and Engineering
Department Computer Science

Inhaltsverzeichnis

Die Cyberwelt entwickelt sich stetig weiter und umso gefährlicher werden die Angriffe in diesem Bereich. Auch wenn sich die IT-Sicherheit verbessert, so tun es ebenfalls die Täter. Neben der traditonellen IT-Sicherheit hat sich in vielen Unternehmen die Cyber Threat Intelligence (CTI) einen Namen gemacht. Da es allerdings keine offizielle Definition oder einen Standard gibt, wie man CTI richtig und effektiv einsetzt, besteht die Gefahr, dass Unternehmen durch den falschen Einsatz mehr Einbußen hinnehmen müssen als Gewinn. In diesem Paper werden die Grundlagen der CTI vermittelt und wie man effektiv ein CTI Programm in das Unternehmen einführt.

Keywords: IT-Sicherheit, Bedrohung, Schutz

1 Einleitung

Die traditionelle IT-Sicherheit mit Firewalls, Intrusion Detection Systeme etc. ist essentiell für jedes Unternehmen, dass wertvolle Güter schützen will. Doch trotz der Umsetzung dieser Mechanismen kommt es zu Cyberangriffen und diese werden immer gefährlicher. Die Angriffe werden anspruchsvoller und schwieriger zu verteidigen ohne Schäden zu hinterlassen. Diese neuen Angreifer mit ihren raffinierten und gut durchgeplanten Angriffen werden auch 'Advanced Persistence Threat' (APT) genannt. Sie umgehen die traditionellen Verteidigungsmechanismen mit leichtigkeit, vor ihren Angriffen sind monate- oder jahrelange Vorbereitungen durchgeführt worden und sie wählen das Ziel bewusst. Daher müssen auch die Verteidiger besser werden und der Trend geht in Richtung Intelligence-basierter Ansatz. Unternehmen dürfen nicht nur reaktiv auf Angriffe antworten, sondern müssen sich hin zum proaktiven wenden. Ziel sollte es sein, nicht nur Angriffe zu mitigieren, sondern es nicht zum Angriff kommen zu lassen. Oder im schlimmsten Fall schnell genug und effektiv auf einen Angriff reagieren zu können, aufgrund der gesammelten Daten. Der Fokus lag zu sehr auf die Güter die angegriffen wurden. Viel wichtiger sind die Fragen: **Wer greift an? Warum greift er an? Wie greift er an? Von wo greifen sie an?** Um sich mit diesen Fragen zu befassen und um diese Lücken zu schließen hat sich die CTI etabliert, doch es bedarf einer ausführlichen Auseinandersetzung mit dem Thema, um es richtig und effizient Anwenden zu können.

2 Grundlagen

2.1 Hintergrund

Threat Intelligence ist kein neuer Prozess, der erst mit der umfassenden Auseinandersetzung von IT-Sicherheit erfunden wurde. Den Prozess gibt es schon lange im Militär zur Verteidigung gegen Angreifer [6]. Auch beim Militär geht es darum, relevante Informationen über die Bedrohungen zu sammeln, auszuwerten und zu seinem Vorteil zu nutzen, um z.B. einen Angriff zu verhindern oder besser vorbereitet zu sein auf einen Angriff. In [7] wird die militärische Threat Intelligence definiert. Für die IT-Sicherheit hat man dabei den Begriff Threat Intelligence übernommen und man spricht von Cyber Threat Intelligence. Oftmals wird in der Literatur der Begriff 'Cyber' ausgelassen, da sich dies aus dem Kontext ergibt. Ebenfalls übernommen hat man die drei Ebenen der Threat Intelligence (die strategische, die operationelle und die taktische), wobei dies keine eindeutige Definition ist, sondern eher eine Richtlinie und 'best practices'. Die Anwendung von Threat Intelligence im militärischem Umfeld wird in [2] erklärt.

2.2 Definition

Es gibt kein offzielles Dokument oder einen Standard, welcher Cyber Threat Intelligence (CTI) eindeutig definiert. Vielmehr gibt es verschiedene Definitionen, die im Kern eines gemeinsam haben. CTI sind Informationen, die dabei helfen, die richtigen Maßnahmen einzuleiten, um z.B. einen Angriff zu verhindern, zu verteidigen oder zu erkennen. Es können aber auch Informationen sein, die bisher unbekannte Risiken offenbaren.

Eine formulierte Definition von Rob McMillan in [5] lautet

> *Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard. [5]*

Eine weitere Definition stammt aus einem CTI Programm der Bank of England

> *Threat Intelligence is the contextualised output of a strategically-driven process of collection and analysis of information pertaining to the identities, goals, motivations, tools and tactics of malicious entities intending to harm*

> *or undermine a targeted organisation's operations, ICT systems or the information flowing through them. [1]*

Die Kernaussage dieser beiden Definitionen ist die gleiche, CTI sind detaillierte Informationen über Bedrohungen, wobei hervorsticht, dass diese Informationen auch im Kontext gesetzt sind und entsprechend für den Nutzer der Intelligence von Relevanz ist. Informationen über die Sicherheit von elektronischen Chipkarten sind für den Nutzer, z.B. ein Unternehmen, nicht relevant, wenn dieser keine Chipkarten im Einsatz hat oder plant diese in Einsatz zu nehmen. Für eine Bank ist die Information, dass die Konkurrenz angegriffen wurde, jedoch von hoher Bedeutung, denn es ist möglich, dass sie das nächste Ziel sind. Umso wichtiger sind jetzt die Informationen, wer die Angreifer waren, was ihre Motive sind und wie sie vorgegangen sind.

CTI sind also Informationen, die zumindest teilweise verarbeitet wurden und in einen Kontext gebracht wurden. Außerdem sollten sie relevante Inhalte haben, wie die Identität der Angreifer, ihre Ziele, Motive, aktuelle Ereignisse, die Folgen, falls ein Angriff erfolgreich ist oder Anzeichen dafür, dass die Bedrohung immer wahrscheinlicher wird bzw. schon eingetreten ist. Wichtig ist aber auch die Quelle der Information, ob diese zuverlässig ist. Natürlich müssen diese Informationen auch soweit verarbeitet werden, dass man sie einsetzen kann, indem man sie in ein geeignetes Format bringt.

Um die Eigenschaften mehr zu verdeutlichen ist es auch wichtig klarzustellen was CTI **nicht** ist. Es sind nicht einfach offentsichtliche Informationen über eine Bedrohung. Informationen über Schwachstellen gehören ebenfalls nicht dazu, denn diese sollte man unabhängig vom CTI Programm aufgedeckt haben. Helfen die Informationen dem Nutzer nicht bei Entscheidungen weiter, ist diese auch nicht der CTI zuzuordnen.

2.3 CTI Typen

CTI kann man, analog zur traditionellen militärischen Threat Intelligence, in drei Ebenen einteilen: die strategische, die operationelle und die taktische.

strategische Ebene

Strategische Threat Intelligence ist für die Entscheidungsfindung auf Unternehmensebene von Bedeutung. Inhaltlich sind es Informationen über die geopolitische Lage der letzten aufgezeichneten Cyberangriffe, finanzielle Folgen der Angriffe oder welche Motive die Angreifer haben. Dadurch kann das Leitungs- und Kontrollgremium

des Unternehmens wichtige Entscheidungen treffen, welche das gesamte Unternehmen betreffen, wie z.B. ob man ins Ausland expandieren sollte, obwohl dort zunehmend Cyberangriffe festgestellt wurden. Diese Intelligence bietet somit auch eine gewisse langfristige Nutzung an. Mögliche Informationsquellen sind Nachrichten, Artikel und weitere öffentlich zugänglichen Quellen [3, 4, 6].

operationelle Ebene

Operationelle Threat Intelligence sind Informationen über die Angreifergruppe und deren Vorgehen. Es enthält deren Taktiken und Strategien und wie sie in der Vergangenheit ihre Angriffe ausgeführt haben. Es enthält auch Informationen über bevorstehende Angriffe. Diese Art der Intelligence ist sehr selten, da Privatpersonen nicht die Mittel haben bzw. die Erlaubnis, Kommunikationswege abzuhören, um an diese Informationen zu kommen. Solange also die Angreifergruppe nicht öffentlich bekannt gibt, ein Unternehmen anzugreifen, wird das Unternehmen sich nicht ausreichend vorbereiten können. Eine Möglichkeit wäre vergangene Events zu analysieren, um festzustellen ob nach bestimmten Ereignissen ein Cyberangriff erfolgt ist. Dadurch kann man zumindest Abschätzen, welche Bedingungen erfüllt sein müssen, um Ziel eines Angriffs zu werden. Diese Intelligence hat zwar auch einen langfristigen Nutzen, aber auch wenn ein Angriff im Gange ist, können die Informationen helfen diesen zu verteidigen und ggf. die Schäden zu minimieren.[3, 4, 6].

taktische Ebene

Taktische Threat Intelligence beschreibt Einzelheiten, die während eines Angriffs wichtig sind. Hier ist die Zielgruppe eher die Security Abteilung, welche direkt mit dem Angriff konfrontiert ist und diesen mitigieren muss. Beispiele für solch eine Intelligence sind maliziöse Programme oder IP-Adressen. Es können auch die HASH-Werte von Schadsoftware sein. Im Prinzip alle Indicators of Compromise (IoC). Das Problem ist, dass diese schnell an Wert verlieren, da sie leicht geändert werden können vom Angreifer, wie z.B. die IP-Adresse. Als Informationsquellen werden hier überwiegend technische Logs genutzt [3, 4, 6].

3 CTI Framework

3.1 CTI Quellen

Eines der wichtigsten Aspekte der CTI ist es die richtigen Daten zu sammeln. Hier gilt 'Qualität geht über Quantität'. Entscheidend ist nicht die Menge der gesammelten Daten, denn dadurch steigt die Wahrscheinlichkeit, dass nicht relevante Informationen enthalten sind und es unübersichtlicher wird, sondern eher die Daten zu sammeln, die man braucht. Das Sammeln von richtigen Informationen beginnt schon mit der Auswahl der richtigen Quellen. Grob kann man zwei Arten von Quellen beschreiben, die **internen** und die **externen** Quellen.

3.1.1 Interne Quellen

Informationen, die direkt aus dem Unternehmen stammen werden als interne CTI betrachtet. Diese Informationen können durch IT-Forensik entstehen, nachdem ein Angriff erfolgt ist oder ein Angriff vermutet wird.

3.1.2 Externe Quellen

Informationen, die nicht direkt aus dem Unternehmen stammen, sind der externen CTI zuzuordnen. Hier gibt es Anbieter, die sich z.B. auf das Sammeln einer bestimmten Art von Informationen spezialisiert haben und diese den CTI Konsumenten zur Verfügung stellen. Im Gegensatz zu diesen kommerziellen Anbietern gibt es auch 'Open Source Intelligence' (OSINT). Diese Informationen sind frei verfügbar und werden z.B. durch Nachrichtendienste bereitgestellt. OSINT und kommerzielle Anbieter haben beide Vor- und Nachteile [6].

Vorteile OSINT

Da die Informationen frei zu Verfügung stehen, können Unternehmen verschiedene OSINT Quellen ausprobieren und sie an die eigenen Bedürfnisse anpassen. Außerdem werden die Mitarbeiter im Umgang mit Intelligence trainiert, durch das Beschäftigen mit den verschiedenen Quellen und Formaten.

Nachteile OSINT

Man benötigt viel Erfahrung um OSINT Quellen gut einschätzen zu können. Desweiteren sind die Informationen meistens nicht in geeignete Formate gegeben und man benötigt zunächst einen Prozess, um diese Informationen zur weiteren Verarbeitung vorzubereiten, wodurch der Personaleinsatz steigt. Um den Nutzern von kommerziellen Anbietern einen Vorteil zu gewähren, werden einige Informationen erst spät oder garnicht veröffentlicht.

Vorteile kommerzieller Anbieter

Die Informationen werden durch den Anbieter in verschiedenen Formaten durch eine API zur Verfügung gestellt. Dies erleichtert den Zugriff auf die Daten und die weitere Verarbeitung. Bei vielen Anbietern werden ebenfalls Support-Leistungen angeboten für Anpassungen an Formate. Die bereitgestellten Informationen sind meistens auf eine bestimmte Branche angepasst und somit gibt es weniger 'unnötige' Daten.

Nachteile kommerzieller Anbieter

Mitarbeiter müssen trotz der Service-Leistungen des Anbieters ein gewisses Know-How mitbringen, um die abgerufenen Daten richtig Verwenden zu können. Als Unternehmen ist man abhängig von dem Anbieter und deren Leistungen. Eventuell bieten diese nicht die Flexibilität an, die man benötigt. Legt man selbst noch Hand an den Daten und verarbeitet diese, hat man ggf. keine Kosteneinsparungen mehr gegenüber der Verwendung von OSINT Quellen.

3.2 Intelligence Sharing

Das Teilen von Intelligence ist ebenso wichtig wie das Anwenden im eigenen Unternehmen. Erfolgreiche Angriffe auf Unternehmen einer Branche, könnten zur Folge haben, dass weitere Angriffe einfacher werden in diesem Sektor. Daher sollten vor allem Organisationen der gleichen Sparte Informationen teilen und von anderen Firmen geteilte Informationen im Auge behalten.

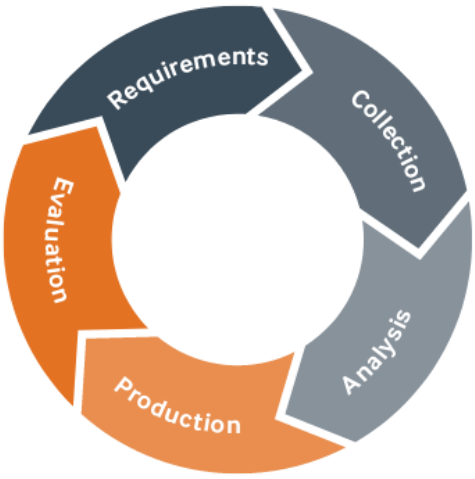
Es gibt aber auch Nachteile beim Intelligence Sharing. Da unter anderem auch sensible Daten geteilt werden, ist ein gegenseitiges Vertrauen nötig. Im schlimmsten Fall, kann die Konkurrenz diese Daten, z.B. dass ein Angriff erfolgreich durchgeführt wurde, zu seinem Vorteil ausnutzen. Ein Angreifer könnte seine Taktiken anpassen, wenn er erfährt, dass sich ein Unternehmen vorbereitet oder die Vorgehensweise der Angreifer kennt.

Wichtig ist also diese Informationen vertraulich zu behandeln und auch nur mit Entitäten zu teilen, mit denen man einen guten Kontakt pflegt. Dies können z.B. gute Beziehungen zu Arbeitern aus anderen Firmen sein. Eine weitere Möglichkeit ist es geschlossene Gruppen zu bilden oder Partnerschaften mit bestimmten Firmen einzugehen. Über ein geschlossenes Portal könnte man dann die Daten austauschen.

3.3 CTI Zyklus

Um CTI in das Unternehmen einzuführen, muss man zunächst definieren, welche Erwartungen man hat von dem CTI Programm und geeignete Quellen heraussuchen. Grundsätzlich ist der Zyklus in fünf Schritten einzuteilen. Der Zyklus ist ein anforderungsba-

Abbildung 1: CTI Zyklus [3]



sierter Zyklus. Das bedeutet er startet mit der Definition von neuen Anforderungen. Die alternative wäre ein vorfallsbasierter Zyklus. Dieser würde mit einem eingeleiteten oder erfolgreich ausgeführten Angriff starten. Im folgenden wird jedoch nur der anforderungsbasierte Ansatz erläutert, da dieser weitverbreiteter und auch effektiver ist.

Anforderungen

Die Anforderungen definieren offene Fragen des Teams. Man möchte z.B. wissen ob es in der eigenen Branche in den letzten Monaten, Cyberangriffe gegeben hat. Oder man könnte sich auch fragen, welche offenen Schwachstellen es noch gibt.

Wichtig ist sich im klaren zu sein, welche Lücken geschlossen werden, sollte man der Anforderung gerecht werden.

Intelligence Sammeln

Beim Sammeln sollte man bedacht und planvoll vorgehen. Für ein gutes CTI Programm und der effizienten Arbeit ist es essentiell die richtigen Daten zu sammeln und das geht schon mit der Auswahl der Quellen los. Es gibt viele verschiedene Quellen und daher sollten diese genauestens untersucht werden. Die höchste Kostenersparnis liegt in der effizienten Sammlung.

Analyse

Hier werden die gesammelten Daten analysiert und ein Bezug zu den Anforderungen hergestellt. Daten, die beim Problem nicht weiterhelfen, werden verworfen. Desweiteren müssen sie in ein geeignetes Format gebracht und archiviert werden, damit diese jederzeit abrufbar sind. Dazu gehört es die Daten in eine Datenbank oder ähnliches zu speichern.

Produktion

In dieser Stufe werden die Informationen, die nun in einem Kontext zum Problem stehen, 'anfassbar' gemacht. Je nach Typ der Intelligenz und an wen sie sich richtet sind hier verschiedene Ansätze angebracht. Für das Verbessern einer Firewall, werden die Informationen lediglich in ein für Firewalls geeignetes Format gebracht und in die Firewall eingelesen. Der Vorstand der Firma erwartet die Informationen eher in Form eines Berichts, um anhand dessen unternehmenspolitische Entscheidungen treffen zu können.

Evaluation

Der letze Schritt ist zu evaluieren, ob die Anforderungen erfüllt sind. Sollte die Intelligence den Anforderungen genügen, hat man erfolgreich ein CTI Produkt erschaffen. Sollte man den Anforderungen nicht gerecht werden, muss man feststellen an welchem Punkt es gescheitert ist. Möglicherweise waren die Anforderungen unrealistisch oder die Quellen nicht gut genug.

4 Zusammenfassung

In diesem Paper wurde zunächst CTI definiert und ein Kernpunkt herausgearbeitet. CTI sind Informationen die soweit verarbeitet wurden, dass sie bei der Entscheidungsfindung

in Bezug auf die IT-Sicherheit helfen. Außerdem wurden die verschiedenen Typen von CTI aufgezeigt und welche Rolle diese spielen. Desweiteren wurde erläutert wie man ein CTI Programm in das Unternehmen einführt und wie dieser aussehen kann. Dabei wurde auf die Wichtigkeit der Intelligence-Quellen hingewiesen. Für die Sicherheit der Organisationen ist zudem der Austausch von Intelligence immer wichtiger, vorallem innerhalb der Branche. Die Implementierung des Programms und den Anforderungen ist in jedem Unternehmen unterschiedlich und muss auf die eigenen Bedürfnisse angepasst werden. Dennoch gibt es dafür einen Zyklus an den man sich richten kann.

Literatur

[1] *CBEST Intelligence-Led Testing. Understanding Cyber Threat Intelligence Operations. Bank of England.* URL https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/understanding-cyber-threat-intelligence-operations, 2016

[2] *Atp 2-01.3 Intelligence Preparation of the Battlefield / Battlespace. Headquarters Department of the Army.* CreateSpace Independent Publishing Platform, 2017. – URL https://books.google.de/books?id=fgWetAEACAAJ. – ISBN 9781976235290

[3] David Chismon, Martyn R.: Threat Intelligence: Collecting, Analysing, Evaluating. (2015). – URL https://www.mwrinfosecurity.com/assets/Whitepapers/Threat-Intelligence-Whitepaper.pdf

[4] Intel & Analysis Working Group: *What is Cyber Threat Intelligence?*. – URL https://www.cisecurity.org/blog/what-is-cyber-threat-intelligence. – Zugriffsdatum: 2019-02-02

[5] McMillan, Rob: *Definition: Threat Intelligence.* URL https://www.gartner.com/doc/2487216/definition-threat-intelligence, May 2013

[6] Röcher, Dror-John: Cyber Threat Intelligence 101. In: *Datenschutz und Datensicherheit - DuD* 42 (2018), Oct, Nr. 10, S. 623–628. – URL https://doi.org/10.1007/s11623-018-1013-2. – ISSN 1862-2607

[7] Staff, United States. Joint C. of: *Joint Publication 2-0: Joint Intelligence.* URL https://www.hsdl.org/?view&did=479269, Jun 2007