Cyber-Angriffe in Echtzeit aufspüren

Der Cyber-Defence Campus hat ein Verfahren für eine effizientere Abwehr im Cyber-Raum auf der Basis von maschinellem Lernen entwickelt. Ziel ist, dass die Armee in Zukunft die Aktivitäten von Angreifern zuverlässig und in Echtzeit aufspüren kann. An der von der NATO organisierten, weltweit grössten internationalen Cyber-Defence Übung «Locked Shields» wurde das neue Verfahren erstmals eingesetzt.

Text: Luca Gambazzi, Prisca Eichenberger und Vincent Lenders

Ist die Schweizer Armee für Cyber-Angriffe gewappnet?
Erfolgreiche Cyber-Angriffe bleiben oft mehrere Monate unbemerkt. Der Cyber-Defence (CYD) Campus hat mit Experten von armasuisse Wissenschaft und Technologie (W+T) und der ETH Zürich ein Verfahren auf der Basis von maschinellem Lernen entwickelt, das der Armee in Zukunft ermöglichen soll, Cyber-Attacken auf militärische Computernetzwerke in Echtzeit zu identifizieren.
An der weltweit grössten internationalen Cyber-Defence Übung «Locked Shields» zeigte sich, ob die Schweizer Armee gegen Cyber-Angriffe gerüstet ist. Diese Übung wird jährlich vom NATO Cooperative Cyber Defence Center of Excellence von Tallinn (Estland) aus organisiert. Im vergangenen April nahmen über 1000 Cyber Experten daran teil.
Ein Team von versierten Angreifern, das sogenannte Red Team, stellte auch dieses Jahr im April während mehreren Tagen die Abwehrkräfte verschiedener Nationen auf die Probe. Nationale Teams von IT-Spezialisten, die als Blue Teams fungieren, helfen jeweils einem fiktiven Land, sich gegen die breit angelegten Cyber-Angriffe des Red Teams zu wappnen. Mit von der Partie ist auch das Blue Team der Schweiz, das jedes Jahr von der Führungsunterstützungsbasis (FUB) geführt wird. Das zu schützende Netzwerk besteht aus traditionellen Computern und Servern, aber auch aus Geräten mit Software-Applikationen für kritische Infrastrukturen sowie Routern und Geräten für die drahtlose Mobilfunkkommunikation.

Erfolgreiche Cyber-Angriffe bleiben oft mehrere Monate unbemerkt.

Während der gesamten Übung greift das Red Team die Systeme der Blue Teams an. Dabei werden die Aktivitäten in dem von den Blue Teams geschützten Netzwerk aufgezeichnet. Nach der Übung werden die Blue Teams bewertet und das Red Team gibt einen Bericht über die verwendeten Angriffe sowie Taktik ab, damit die Blue Teams ihre Verteidigungsstrategien verbessern können.

CYD Campus sagt Cyber-Angriffen den Kampf an
Der CYD Campus, in diesem Fall ein Team von Cyber Experten aus armasuisse W+T zusammen mit Studenten der von Prof. Laurent Vanbever geführten Gruppe der ETH Zürich, evaluierten die Möglichkeiten, Kommunikationskanäle zwischen Malware und den Command and Control (C2)-Servern mittels automatischen Lernens zu identifizieren.

MASCHINELLES LERNEN
Maschinelles Lernen ist eine Disziplin der künstlichen Intelligenz. IT-Systeme werden dadurch in die Lage versetzt, aufgrund von Daten und Algorithmen, Muster und Gesetzmässigkeiten zu erkennen und Modelle zu entwickeln.
Anhand eines solchen Modells lassen sich anschliessend Aufgaben lösen, wie zum Beispiel die Klassifikation von Objekten oder die Detektion von Anomalien. Maschinelles Lernen gewinnt für die Armee zunehmend an Bedeutung. Nämlich überall dort, wo Daten digital vorliegen und somit vom Computer schneller und effizienter analysiert werden können, als von einem Menschen.

Cyber-Angriffe, respektive der Datenverkehr von Angreifern, muss in Echtzeit identifiziert werden können, um den Schaden von solchen Vorfällen möglichst klein zu halten. Die zur Verfügung stehenden Personalressourcen reichen in der Praxis nicht aus, um die enormen Mengen an Datenflüssen manuell zu analysieren. Deshalb wird die Charakterisierung des Datenverkehrs mit einem neuen Ansatz maschinellen Lernens durchgeführt.
Wie ist der CYD Campus vorgegangen? Im Projekt wurden zuerst rund 80 Datenflussmerkmale für die Unterscheidung legitimer und bösartiger Netzwerk-Verkehrsflüsse definiert und ausgewertet. Dank der Aufzeichnungen von mehr als 300 GB von Locked Shields Übungen aus früheren Jahren war der CYD Campus in der Lage, das Verhalten sowie die verwendeten Mittel der Angreifer mittels maschinellem Lernen zu analysieren und eigene Erkennungs- und Interventionstechniken zu entwickeln. Nach mehreren Testeinheiten erzielte das neue Verfahren bessere Ergebnisse als bisher bekannte Methoden, welche ohne maschinellem Lernen funktionieren: Der CYD Campus erreichte eine Identifikationsgenauigkeit von 99% und eine Rückrufquote von mehr als 90%. Um die Effizienz der Leistung bei der Datencharakterisierung bezüglich der Unterscheidung von legitimem und bösartigem Datenverkehr zu steigern, wurden von den 80 definierten Datenflussmerkmalen die 20 Einflussreichsten ausgewählt.

Dank der Aufzeichnungen von Locked Shields Übungen aus früheren Jahren war der CYD Campus in der Lage, das Verhalten der Angreifer mittels maschinellem Lernen zu analysieren und eigene Erkennungs- und Interventionstechniken zu entwickeln.

Erfolgreicher Einsatz der Methode in der Armee
Um die Armee mit dieser neuen Methode zu befähigen, hat der CYD Campus in den letzten Monaten sehr eng mit der Führungsunterstützungsbasis der Armee (FUB) zusammengearbeitet. Die neuen Verfahren wurden von Cyber-Wachmeister auf bestehende Systeme der FUB integriert und so erweitert, dass die Detektion der Angriffe mit den vorhandenen Netzwerkaufzeichnungssystemen der FUB in Echtzeit funktionieren. Im April 2019 wurde das Verfahren erstmals an der Locked Shields Übung vom Schweizer Blue Team eingesetzt. Diese Übung bestätigt, dass die Methodik sehr effizient ist, um Angriffe eines Red Teams in Echtzeit aufzuspüren.
Die Art und Weise wie ein solches Projekt in weniger als einem Jahr von der Idee bis zur erfolgreichen Umsetzung durchgeführt werden konnte, ist beinahe ebenso wichtig wie der Output. Dank der engen Verbindung zwischen der Grundlagenforschung an der ETH Zürich und den operativen Cyber-Organisationseinheiten der Armee konnte der CYD Campus gewonnene Erkenntnisse und neues Wissen sehr rasch und agil in die Armee transferieren und umsetzen. Im Gegenzug wurden neue Praxiserfahrungen und Fragestellungen bei der Armee gewonnen, welche wiederum als neue Projekte im CYD Campus aufgenommen und dieses Jahr zusammen mit den Hochschulen weitergeführt werden.

Wie können andere Organisationen von den Erkenntnissen profitieren?
Die Ergebnisse des Projekts wurden an der NATO-Konferenz über Cyber-Konflikte (CyCon 2019) im Mai 2019 in Tallinn veröffentlicht und vorgestellt. Durch diese Veröffentlichung sollen andere Nationen, aber auch zivile Organisationen, von den gewonnenen Erkenntnissen für ihre eigene Verteidigung profitieren können.

CYD CAMPUS
Im Januar 2019 hat der Cyber-Defence Campus (CYD Campus) des VBS seinen Betrieb bei armasuisse W+T aufgenommen. Der CYD Campus ist eine Massnahme des Aktionsplans sowie Teil der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS). Er hat zum Ziel, laufende Entwicklungen in der «Cyber-Welt» früh zu erkennen, zu beobachten und Handlungsstrategien zu entwickeln. Der CYD Campus arbeitet eng mit den Hochschulen und den operativen Cyber-Einheiten des VBS zusammen, um Erkenntnisse aus der Forschung in einsatzfähige Lösungen und neue Cyber-Fähigkeiten umzuwandeln. Der Einsatz von maschinellem Lernen und künstlicher Intelligenz wird aktuell in diversen Projekten untersucht.

Kontrollraum der Cyber Defence Übung Locked Shields.

Das Blue Team der Schweiz setzt während Locked Shields 2019 ein neuartiges Verfahren vom CYD Campus ein.