Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

Herausgeber: Schweizerische Offiziersgesellschaft

Band: 185 (2019)

Heft: 7

Artikel: Geopolitische Cyber Threat Intelligence

Autor: Ruef, Marc

DOI: https://doi.org/10.5169/seals-862695

Geopolitische Cyber Threat Intelligence

Das Antizipieren der Fähigkeiten und Handlungen der Akteure im digitalen Raum ist in den vergangenen Jahren hochgradig relevant geworden. Durch den Ansatz der geopolitischen Cyber Threat Intelligence (CTI) wird es möglich, auf der Basis von politischen, wirtschaftlichen und technischen Daten entsprechende Risiken, Aktivitäten und Auswirkungen vorauszusagen.

Marc Ruef

Die Bewältigung des digitalen Raums stellt uns alle vor grosse Herausforderungen. Einerseits weist er eine noch nie dagewesene Dynamik in Bezug auf Technologien auf. Andererseits können Handlungen skaliert und mit ungeahnter Geschwindigkeit durchgeführt werden. Umso wichtiger ist es, dass man sich durch umsichtige Analysen und kluge Entscheidungen einen Vorteil erarbeiten kann.

Es ist mittlerweile ein offenes Geheimnis, dass es für staatliche Akteure zum guten Ton gehört, offensive Aktivitäten im digitalen Raum voranzutreiben. Die Vorbereitungen und oftmals auch Durchführungen geschehen dabei natürlich im Geheimen. Dennoch sind sie absehbar, wodurch ihnen, wenigstens in ihren Grundzügen, das unliebsame Mass an Überraschung genommen werden kann. Das Werkzeug hierzu ist die sogenannte «Geopolitische Cyber Threat Intelligence» (CTI).

Definition von Entitäten

Grundsätzlich werden einzelne Entitäten definiert. Hierbei handelt es sich traditionell um Staaten. In diesen Staaten gibt es verschiedene Sektoren, wie zum Beispiel «Finanz» oder «Gesundheit». Diese Sektoren zeichnen sich für einen gewissen Teil des Bruttoinlandprodukts des jeweiligen Staates verantwortlich. Durch das Festhalten dieser Zahlen wird die Grundlage für die wirtschaftlichen Auswirkungen eines erfolgreichen Angriffs bestimmt. Diese Daten werden oftmals durch die Länder selbst, manchmal aber auch durch Organisationen wie OECD oder CIA zusammengetragen und bereitgestellt. Für manche Länder, wie zum Beispiel China und den Iran, ist die Datenbeschaffung hingegen nicht so einfach, da verlässliche Quellen fehlen.

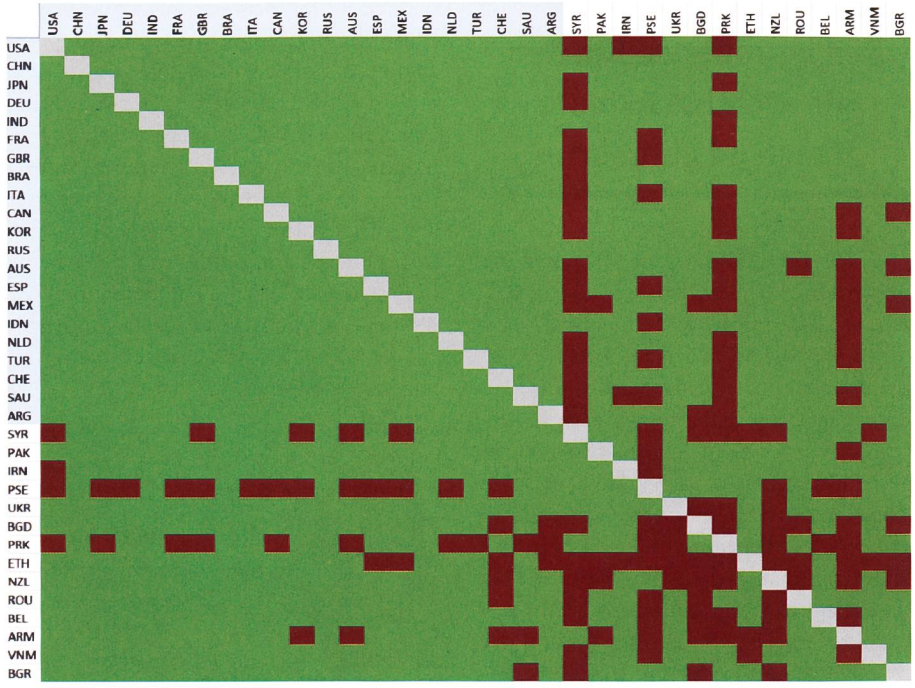
Die jeweiligen Sektoren und/oder Firmen setzen üblicherweise Software eines bestimmbaren Typs ein. Zum Beispiel wird «Banking Software» vorwiegend im Finanzsektor eine zentrale Rolle spielen. Und im Gesundheitsbereich kommen exklusiv die sogenannten «Medizinalgeräte» zum Einsatz.

In gewissen Fällen wird gar eine konkrete Bestimmung von Herstellern, Produkten oder Versionen möglich. Zum Beispiel war es lange Zeit gegeben, dass eine der Schweizer Grossbanken eine veraltete Version des Microsoft Internet Explorer als Standard-Webbrowser eingesetzt hat. So manches Unternehmen bringt ihre historisch, finanziell oder anderweitig bedingten Eigenheiten mit, die man mitberücksichtigen kann.

Modellierung von Beziehungen

Diese Entitäten können nun in Beziehung zueinander gesetzt werden. Typische Einflüsse sind das Import/Export-Verhältnis, die Vereinigung in einer wirtschaftlichen oder politischen Gemeinschaft (z.B. G5, NATO, IMFC, TRIPS) und der offen bekundete Austausch von behördlichen Informationen. Diese Beziehungspunkte geben schlussendlich Aufschluss darüber, ob und welche Spannungen zwischen einzelnen Entitäten herrschen.

Ein sehr einfaches und deshalb so spannendes Beispiel ist das Aufzeigen des Vorhandenseins von Botschaften in den jeweiligen Ländern. Anhand dieser simplen Beziehungsmatrix lässt sich auf einen Blick erkennen, welche Länder sich gegenwärtig wohl gesonnen sind und welche nicht. Dabei kann zwischen acht unterschiedlichen Spannungsformen unterschieden werden: Militärische Kooperation, Konföderation, ökonomische Kooperation, diplomatische Beziehungen,



Auf einen Blick lässt sich erkennen, welche Länder diplomatische Beziehungen zueinander unterhalten. Grafiken: Autor

keine diplomatischen Beziehungen, Konflikt durch Drittpartei, direkter bewaffneter Konflikt, Kriegszustand.

Berechnung der Angriffswahrscheinlichkeit

Es gibt eine Vielzahl an Angriffsszenarien, die sich im digitalen Raum abspielen können. Da können durch *Denial of Service-Attacken* Ressourcen unbrauchbar gemacht werden, wie es mittels «Stuxnet» im Iran der Fall war. Oder es geht um Industriespionage, der sich Google im Rahmen von «Operation Aurora» in China ausgesetzt sah.

Das Bedürfnis und damit die Eintrittswahrscheinlichkeit von Szenarien dieser Art lässt sich nun dank der Modellierung der Beziehungen ermitteln und voraussagen. Dass sich Israel um die Sabotage des Atomprogramms im Iran bemühen wird, erscheint offensichtlich. Ebenso, dass sich China einen Wettbewerbsvorteil für den heimischen Markt durch Wirtschaftsspionage verschaffen will. Die Modellierung hilft zusätzlich zu erkennen, ob und in welchem Mass die Risiken hierfür zu- oder abnehmen.

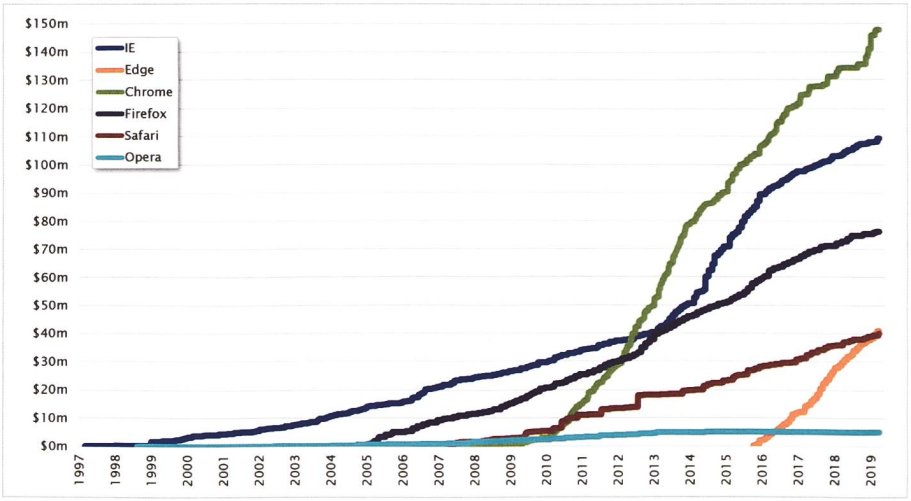
Effektiv spannender sind hingegen die eher subtilen oder hochkomplexen Konflikte, die es nicht regelmässig in die Presse schaffen. Welches Interesse hat Kolumbien am Finanzplatz in Zürich? Welche Akteure aus dem asiatischen Raum interessieren sich für Schwachstellen in Schweizer Krankenhäusern? Welche Angriffsszenarien auf Parlamentarier gehen trotz enger Beziehungen von Deutschland, Frankreich oder Italien aus?

Korrelation von Verwundbarkeiten

Im Bereich Cybersecurity spielen Sicherheitslücken eine entscheidende Rolle. *Blue Teams* sind um die Verteidigung und das Absichern der Systeme bemüht. *Red Teams* hingegen um das offensive Ausnutzen eben dieser Schwachstellen, um einen Angriff erfolgreich durchsetzen zu können.

Tagtäglich werden neue Sicherheitslücken publiziert, diskutiert, ausgenutzt und adressiert. Durch das stetige Beobachten dieses dynamischen Markts kann nun eine Korrelation der geopolitischen Beziehungen, den Sicherheitslücken und den damit einhergehenden Angriffsszenarien angestrebt werden.

Dabei bestimmen die Eigenschaften einer Schwachstelle mit, für welches Angriffsszenario sie sich einspannen lässt.



Die Entwicklung des Gesamtvolumens des Exploitmarkts für Webbrowser befindet sich in stetigem Wachstum.

Falls für eine erfolgreiche Kompromittierung eine Benutzerinteraktivität durch das Opfer vorausgesetzt wird, kann er Teil eines *Phishing-Angriffs* werden. Oder falls der Angriff über das Netzwerk erfolgen kann und in der Lage ist überproportional viele Ressourcen zu verbrauchen, wird er für eine *Denial of Service-Attacke* herhalten können.

Sobald sich nun beispielsweise abzeichnet, dass eine neue Schwachstelle in iPhone erscheinen wird, die auf Grund ihrer Beschaffenheit auf den Exploit-Märkten mindestens 1,5 Mio. USD abwerfen wird, können anhand der geopolitischen Analyse die nächsten Schritte der jeweiligen Akteure antizipiert werden. Es wird offensichtlich, wer Interesse an dieser Schwachstelle hat, zu welchem Zweck sie ausgenutzt werden kann, gegen wen sie am ehesten verwendet werden soll, wie sich das Angriffsszenario gestalten wird und in welchem Zeitraum der Zugriff passieren muss.

Daraus resultierender Nutzen

Einerseits kann dieses Wissen genutzt werden, um existierende und zukünftige Risiken erfassen und adressieren zu können. Es hilft zum Beispiel dabei einem international agierenden Unternehmen zu entscheiden, ob in einem bestimmten Land eine Niederlassung aufgemacht werden soll. Und falls dies getan wird, welche risikotechnischen Konsequenzen – und damit auch juristischen und wirtschaftlichen Investitionen – das mit sich führen wird.

Andererseits kann darauf abgestützt eine dynamische und hochgradig agile Zuweisung von Ressourcen erfolgen. Gerade in Bezug auf «Kritische Infrastruktur» kann dies entscheidend sein. Falls sich zum Beispiel abzeichnet, dass aus Osteuropa *Malware-Angriffe* auf Industrieanlagen im deutschsprachigen Raum angestrebt werden, können kurzfristig und zielgerichtet finanzielle, technische und personelle Ressourcen aufgestockt werden, um eben genau dieses konkrete Szenario adressieren zu können (z.B. starke Einschränkung auf *Firewalls,* aktives *Monitoring* bestimmter Zugriffe).

Fazit

Cyber Threat Intelligence wird zu einem wichtigen Mittel, um im digitalen Raum schnell reagieren und dabei agil bleiben zu können. Das Verheiraten von geopolitischen Informationen mit Daten zu Schwachstellen in Computersystemen stellt dabei den nächsten Schritt einer fortwährenden Evolution dar. Dadurch wird es möglich, Akteure und ihre Handlungen erkennen, antizipieren und neutralisieren zu können. Risiken lassen sich so abschätzen und entsprechende Ressourcen punktuell aufstocken. Damit ist man den Angreifern einen Schritt voraus. Strategische Entscheide sollten nicht einzig und allein von einer Aktion des Gegenübers abhängig gemacht werden. Es gilt auch im digitalen Raum einen Schritt voraus zu sein. ■

Marc Ruef
Head of Research
scip AG, Zürich
5436 Würenlos

KAMPFERPROBT UND DABEI ERFOLGREICH.

WE MAKE IT FLY

Im Einsatz erweist sich der Eurofighter Typhoon für Luftwaffen als das Flugzeug der Wahl. Seine beispiellose Zuverlässigkeit und Funktionalität, die in allen Bereichen ständig weiter entwickelt wird, werden dem Eurofighter Typhoon über noch weitere Jahrzehnte hinweg eine unverzichtbare Rolle zukommen lassen.

Luftüberlegenheit. We make it fly.

airbus.com

AIRBUS