Der kybernetische Krieg.

Eine Analyse von Conficker, Stuxnet, DuQu über Flame, MiniFlame, Gauss, Mahdi bis Shamoon

Forum für Informationssicherheit

www.gocs.de; -eu; -info; -com.de

Kurzfassung

Stellen wir mal zuerst die simple Frage, hat der denn eigentlich schon begonnen?

Diese Frage kann man leicht mit ja und nein beantworten.

Zur Beantwortung dieser Frage, haben wir uns mal die Mühe gemacht Presseveröffentlichungen zu diesem Thema auszuwerten.

Für die, die uns unterstellen wollen, wir hätten „geheim zuhaltende Informationen „ verwendet. Lassen sie es uns nochmals betonen, wir haben nur öffentlich zugängliches Material analysiert.

Für den Analysezeitraum haben wir nur den Zeitabschnitt ab „Stuxnet bis Shamoon“ verwendet, also eine relativ kurze Zeit.

Gleichzeitig wurde auch eine Einschränkung in Bezug auf die gewaltigen Massen von Schadsoftware gemacht. Denn es interessierten nur die typischen „kybernetischen Pfeile“ die das Attribut „ kriegerisch“ erfüllen.

Die aber auch gleichzeitig die typischen Strukturen, die für Waffensysteme typisch sind . Aber auch die zeitlichen Abhängigkeiten der einzelnen Waffensysteme.

Obwohl nur wenige „kybernetische Pfeile“ umfassend beschrieben wurden, so erlauben sie einen sehr interessanten Einblick. Wo Sie ein blicken können, darüber schreiben wir später, denn sonst verlieren sie die Zusammenhänge. Denn aus Buchstücken kann man keine Strategie zur Verteidigung oder Abwehr aufbauen. Dies natürlich nur, wenn sie es wollen.

Die in diesem obengenannten Zeitraum eingesetzten kybernetischen Kampfmittel, von den Spionagemitteln bis zu den Zerstörungsmitteln, sind ihnen bekannt, oder werden als bekannt voraus gesetzt.

Wir haben sie in zwei Gruppen eingeteilt.

Die eine Gruppe beinhaltet die Zerstörungs- und Sabotagewaffen.

Die andere Gruppe umfasst die Spionagesysteme, sowie einige Subsysteme, wie Manipulationssysteme.

Unter dieser Subkategorie Manipulationssysteme, sollen Methoden verstanden werden, bei denen gespeicherte Informationen verändert oder gelöscht werden. Jedoch keine Systeme für die Produktionssteuerung.

1. Gruppe

Die bekanntesten Vertreter dieser Gruppe sind „**Stuxnet“** und **„Shamoon“**. Ihre Wirkung besteht in der Zerstörung von programmgesteuerten Prozesssystemen. (Stuxnet) Aber auch in der Zerstörung der Computerinfrastruktur, wie magnetische Speichersysteme (Festplatten) u. ä.

Der erste weltbekannte kybernetische Pfeil ist gekennzeichnet durch ein sehr spezifisches Zerstörungsmodul. Dieses greift nur spezielle Produktionssteuerungsanlagen (Urananreicherungssysteme mit einer SPS von Siemens an).

Bei einem Einsatz gegen andere Produktionssteuerungen des gleichen Herstellers wurden keine gravierenden Schäden beobachtet.

Der Ersteinsatz dieser kybernetischen Pfeile ist durch eine Besonderheit gekennzeichnet. Diese ersten Angriffe wurden durch den gezielten Einsatz – das heißt – durch eine direkte Implementierung in das kybernetische System (Computer) durchgeführt. Nach verschiedenen Presseveröffentlichungen wurden beide Anschläge durch autorisierte Mitarbeiter der jeweiligen Computerzentren durchgeführt.

Dies betraf die Anschläge im Iran wie auch die Anschläge in Saudi-Arabien wo die Ölindustrie getroffen wurde.

Inwieweit die inneren Sicherheitsmaßnahmen, die jeweiligen Schäden vermindert haben, ist nichts bekannt.

Somit konnten eventuelle Schutzmittel aus dem Kommunikationssystem (Internet oder anderen Kommunikationskanälen) nicht wirksam werden. Bei einem derartigen Angriff sind internetbasierte Sicherheitsmaßnahmen wirkungslos (sogenannte **Cyber-Abwehrzentralen**).

Dies galt für den Einsatz von „Stuxnet“ und „Shamoon“ gleichermaßen.

Wie viele dieser Infektionen durch autorisierte Mitarbeiter durchgeführt wurden ist nicht bekannt. Für diese Art des Angriffes ist allein von Bedeutung, das dieser direkt in das Computersystem erfolgte.

Diese Art, ist die Art die ein Schutzsystem direkt in dem Computersystem erfordert oder entsprechende Betriebssysteme bzw. weitergehende Schutzmaßnahmen, wie interne Verschlüsselung oder Chiffrierung. Von den bekannten Schutzsystemen einmal abgesehen. Was nichts anderes heißt, diese Systeme müssen dem Wert der Information entsprechend.

Im Falle von „Stuxnet“ kam es nach dem Ersteinsatz noch zu einer Masseninfektion via Internet. Es sollen ca. 60.000 Einheiten infiziert worden sein. Was durch diese Verbreitung bezweckt werden sollte, ist unklar, da“ Stuxnet“ ein hochspezialisierter kybernetischer Pfeil war und noch ist.

Die damaligen Löcher in den verwendeten Softwaresystemen wurden erst nach langer Zeit, mehrerer Monate gestopft.

Bis diese „Flickenschusterei“ durchgeführt wurde, hätte ein kybernetischer Krieg (Cyberwar) über diese Löcher erfolgreich geführt werden können.

Der Eindringkörper ermöglichte einen sehr intelligenten Einbruch. Die Nachfolger oder die Plattform gleichen Erzeugnisse bedienen sich einer Vielzahl von Eindringkörpern.

Wie viele , mehr als es Löcher gibt !

Die Betonung, auch noch in der Gegenwart, ergibt sich aus der Tatsache, dass nur die entsprechenden Schadmodule gegen andere Zielcharakteristiken ausgetauscht werden brauchen.

Das gleiche Verhalten trifft auch auf die „Durchdringungskörper“ zum Eindringen in die jeweiligen kybernetischen Einheiten (Computersysteme) zu.

Die Modularität, ist ein Kennzeichen moderner kybernetischer Pfeile.

2. Diese zweite Gruppe ist wesentlich umfangreicher. Bekannte Vertreter sind DuQu, Flame, Gauss, MiniFlame und Mahdi.

Diese Gruppe kann man als „kybernetische Spione“ bezeichnen. Diese kybernetischen Spione sind gegen die klassischen Spione durch Besonderheiten gekennzeichnet.

Auf diese Besonderheiten wird und der kybernetischen Spionage näher eingegangen.

Die Gruppe von kybernetischen Spionen wurde sehr differenziert eingesetzt. So wurden die Vertreter DuQu und Mahdi nur in einer kleinen Anzahl eigesetzt. Dies heißt nichts anderes, als das nur relativ wenige dieser kybernetischen Pfeile eingesetzt wurden bzw. was auch der Fall sein kann, es wurden nur sehr wenige entdeckt. Auch ist über die speziellen Aufgabenstellungen dieser Mittel wenig bekannt. Trotzdem, werden sie als „höchst gefährlich“ eingeschätzt. So u.a. auch von der BSI / Deutschland. Aus anderen Quellen, wird ein langfristiger Einsatz mit neuen Spionagemodulen nicht ausgeschlossen.

Man kann DuQu mit einem Aufklärungssatelliten vergleichen. Er ist da oben, aber weiteres weiß man nicht!

Es muss nach diesen Quellen mit einem erneuten Einsatz gerechnet werden. Nach den bekannten Erfahrungen aus der Entwicklung der verschiedensten Plattformen „ DuQu und Stuxnet“ werden weiterentwickelte Systeme eingesetzt.

Auch diese Entwicklungslinie ist bei den bekannten Spionagesystemen erkennbar.

Auch findet das Plattform – Prinzip –Anwendung. Was nichts anderes heißt, die erprobten und erfolgreichen Systeme werden durch den Einsatz neuer Module, für veränderte Aufgabenstellungen entwickelt. Gleichzeitig werden die Erfahrungen mit älteren Lösungen modifiziert und optimiert, um den wachsenden Anforderungen gerecht zu werden. Die betrifft die Analysemodule aber auch die Kommunikationsmodule. Letztere sind von besonderer Bedeutung, da sie gewonnen Informationen zu verdeckten Servern weiterleiten müssen. Die gilt für die Informationsmengen wie aber auch für die Geheimhaltung. Aus diesem Grunde werden die „gewonnen Informationen" in einer verschlüsselten oder chiffrierten Form übermittelt. Das gleiche Prinzip wurde bereits im zweiten Weltkrieg angewendet. So wurden Informationen, die aus der „Enigma" gewonnen wurden, für die weitere Übermittlung verschlüsselt. Welches Verfahren auf britischer Seite zum Einsatz kam, scheint auch heute noch ein Geheimnis zu sein. Diese Gesamtverfahren bekam die Bezeichnung „Ultra".

Damit wurde verhindert, dass die deutsche Seite Kenntnisse vom „Einbruch „ in das Verschlüsselungssystem Enigma erhält und gleichzeitig die entschlüsselten Informationen geschützt werden. Eine Analogie gab es auch in den achtziger Jahre im Zusammenhang mit dechiffrierten Informationen durch das ZCO der ex.DDR.

Diese alte Verfahrensweise ist auch bei den kybernetischen Spionen feststellbar. Auch hier wird die Information geschützt, dadurch ist keine Offenbarung der ausspionierten Informationen möglich. Auch kann bei Kenntnis dieser Informationen, die bei der Übertragung zu den Servern übermittelt werden, nicht auf die „interessanten Informationen" geschlossen werden.

Das kybernetische Objekt, welches durch diese kybernetischen Pfeile aufgeklärt wurde, sollte keine signifikanten Hinweise bekommen, welche Informationen für die Aufklärung von Bedeutung sind.

Auch hier gibt es einen sehr interessanten Denkansatz:

(1)

Einige Käufer kaufen „magnetische Datenträger" mit interessanten und für sie wertvollen Informationen (z. B. Steuerdaten deutscher Steuersünder) und zahlen dafür Millionen €. Der Wert dieser Informationen beträgt ein Vielfaches.

Am Markt der Informationen ist ja allgemein bekannt, die europäischen Finanzbehörden suchen „Informationen zur Geldmehrung".

Da, diese Informationen nicht am Markt gehandelt werden, können sie nur auf „illegale Weise" beschafft werden. Diese Taten werden durch „autorisierte Personen" durchgeführt.

(2)

Eine andere Form der Informationsgewinnung, die den Einsatz kybernetischer Mittel erfordert wird von Anderen bevorzugt.

In diesem Falle übernehmen kybernetische Pfeile die Funktion des Informationssammlers in fremden kybernetischen Anlagen. Die hierbei gesammelten Informationen werden via Kommunikationsserver übertragen. In einigen Fällen sollen Datenmassive von 5 Gigabyte Größe übermittelt worden sein. Sie können jedoch größer oder kleiner sein.

Die Datensammlung via „kybernetischen Pfeil“ ist flexibler im Vergleich zu einer menschlichen Quelle. Der Einsatz dieser Pfeile gestattet, eine dem Auftraggeber entsprechende passgerechte Antwort zu geben.

Dabei ergibt sich natürlich noch ein Vorteil, man kann schnelle Wechsel durchführen, weil der Auftraggeber, weitere unbekannte Quellen entdeckt hat.

Zu den Charakteristiken der kybernetischen Aufklärung gehört zweifelsfrei die schnelle Variabilität innerhalb des Zielobjektes.

Die unterschiedlichen Vorgehensweisen sind abhängig von den jeweiligen Staatsformen.

Diese kleinen Spionagehelferlein , haben wie jedes andere Programm oder kybernetische Pfeil eine Größe. Manche dieser sind Schlank, andere dagegen Dickschiffe. Dabei entstammen sie einer und derselben Plattform.

Das bekannteste „Dickschiff“ ist „Flame“.

Der Einsatz der kybernetischen Spione erfolgt sehr unterschiedlich.

So werden einige, wie DuQu oder Miniflame nur in geringen Stückzahlen eingesetzt. Es wird pro System mit bis zu 60 Infektionen gerechnet.

Die Gesamtzahl dieser speziellen kybernetischen Spione liegt somit bei ca. 120 Infektionen.

Es scheint sich hierbei um einen hochspeziellen und sensiblen kybernetischen Spion zu handeln.

Die Angaben hierzu sind für eine Analyse nicht auswertbar.

Andere dagegen werden in Massen eingesetzt. Dabei wurden Infektionsraten von 10.000 oder mehr festgestellt.

Flame ca. 5.000 bis 6.000 Infektionen

Gauss ca. 2.500 Infektionen

Mahdi größer 700 Infektionen

Conficker ca. 60.000 oder eventuell noch größer.

Die Einsatzraten dieser kybernetischen Spione lagen um das 10-fache bis zum 100-fachen über den speziellen Systemen. In Einzelfällen kann dieser Wert deutlich überschritten werden (Conficker).

Der Bereich der Infektionen schwankt zwischen dem Minimum von 68.200 und dem Maximum von bis zu 100.000 oder mehr Infektionen.

Die Dunkelziffer ist jedoch wesentlich höher. Aus Analyse anderer Schadsysteme kann jedoch von Faktoren zwischen 3 ...8 angenommen werden.

Die Gründe für diese hohen Dunkelziffern sind bekannt und sollen hier nicht weiterbehandelt werden.

Auch auf die geographische Verteilung der „gefundenen Schadprogramme“ soll hier bewusst nicht näher eingegangen werden. Da eine Reihe von Anwendungen von kybernetischen Pfeilen andere, abweichende Ergebnisse liefert. Gleichzeitig ist der Einsatz bestimmter kybernetischer Pfeile aus geopolitischer unlogisch.

Ein sehr interessanter Analysepunkt widmet sich der Fragegestellung, in welchen Bereichen, Politik, Wirtschaft, Militär, Forschung und Entwicklung, Infrastruktur usw.

Die hier gewonnenen Erkenntnisse sind sehr interessant.

Diese Ergebnisse werden jedoch nicht publiziert, da „Fehlinterpretationen“ zwischen bagatellisieren und Panikmache eines kybernetischen Krieges zu Weltuntergangsszenarien führen könnten.

Stand der Analyse 10.12.2012

Anmerkungen :

Dieses Material ist Bestandteil des „Forums für Informationssicherheit“.

Dort veröffentlicht und fortlaufend aktualisiert.

Dieses Material basiert nur auf öffentlich zugänglichen Veröffentlichungen.

Veröffentlicht im Internet unter nachfolgenden Adressen:

www.gocs,de bzw. www.gocs.eu bzw. www.gocs.info oder www.gocs.com.de

Berlin, 23.12.2012

Autor Old Gocs