[CYBERRISIKEN SIND KAUM NOCH ABZUWEHREN]

Februar 2018:

IT-Sicherheitsexperten fordern die Stärkung der Cybersicherheit: Scan- und Filtermechanismen am Frankfurter Hub schützen die Gesellschaft vor Cybergefahren

Hamburg / München, Februar 2018

In den vergangenen Wochen habe ich auf unterschiedlichen Ebenen Politik/Militär/Wirtschaft verdeutlicht, dass der Staat seiner Verantwortung nach mehr Sicherheit im ITK-Netz wesentlich stärker nachkommen muss. Die Flut von Cybergefahren sind für Unternehmen, Betreiber der kritischen Infrastruktur und Provider nicht mehr abzuwehren. Neben der von Teletrust und dem Weltwirtschaftsforum geforderten sicherheits-relevanten Kennzeichnung von ITK-Produkten sollten nunmehr vom Staat Scan- und Filtermechanismen am Frankfurter Hub zum Einsatz kommen, um mehr Sicherheit im europäischem Internet zu gewährleisten. Darüber hinaus muss der Staat die digitalisierte Gesellschaft vor neuen Methoden der Spionage schützen.

Ein Artikel der Welt, Wie man Cyberrisiken trotzt, vom 15.01.2018

http://bit.ly/2F6KvAz

berichtet über ähnliche Forderungen aus einer Studie des Weltwirtschaftsforums in Zusammenarbeit mit Boston Consulting Group.

Auch die Veranstalter der Münchner Sicherheits-konferenz fordern, dass Unternehmen und Regierungen an einem Strang ziehen und gezielt handeln und alles dafür getan wird, Daten und Vermögenswerte von Einzelnen und Unternehmen zu schützen, Menschen, Unternehmen und Infra-strukturen vor Schaden zu bewahren und eine zuverlässige Basis für das Vertrauen in eine vernetzte und digitale Welt zu schaffen.

Die Regierung fordert und fördert den Ausbau der Datennetze und die Digitalisierung der Gesellschaft. Um die Vorhaben erfolgreich umzusetzen, wird sich der Staat im Bereich der Cyberprävention neu aufstellen müssen.

Der Staat hat die Aufgabe die Bevölkerung vor Gefahren zu schützen. Geht die Gesellschaft den Weg der Digitalisierung, so hat der Staat die Gesellschaft auch vor den hierdurch entstehenden Gefahren zu schützen. Zudem muss der Staat die Infrastruktur in einem Zustand halten, dass eine sichere, allgemeine Nutzung möglich ist.

Wenn der Aufruf einer URL dazu führt, dass aufrufende Systeme in BOT-Netzen eingefangen werden und die URL in Deutschland Millionen Systeme gefährdet, so reicht es nicht mehr aus, dass zehntausende Unternehmen ihre IT mit Firewalls und Antivirus schützen. Diese klassische Einzelkämpferstrategie ist zukünftig der Grundschutz, aber wenn man ganze Subnetze gezielt gegen Angriffe schützen will, muss sich der Staat auf den zentralen Einsatz von Scan- und Filtermechanismen ausrichten. Das ist zukünftig der Präventivschutz. Gerade der Trend zur stärkeren Vernetzung und der Vermarktung von IoT fordert ein Umdenken in der Cybersicherheit, da ansonsten ein digitales Ökosystem geschaffen wird, in dem jedes Quartal hunderttausende von Geräten aus den Updates fallen und so leichte Beute der Cyberkriminalität werden. Es ist es an der Zeit an einem Zentralen Hub die Systeme der Industrie, der kritischen Infrastruktur und der Bevölkerung proaktiv vor Cybergefahren zu schützen, um somit einen präventiven und zugleich wirkungsvollen Schutz vor existierenden und zukünftigen Cybergefahren zu gewährleisten.

Scan- und Filtermechanismen am Frankfurter Hub bringen die notwendige Flexibilität und Optionen mit sich, die zu einer deutlichen Verbesserung der Cybersicherheit führen. Auch die Datensicherheit und der Datenschutz würden signifikant gestärkt werden.

Was können Scan- und Filtermechanismen am Frankfurter Hub bewirken?

Während täglich Cyber-Angriffe stattfinden, beschäftigen sich einige Admins mit dem BSI-Grundschutz und wenige Admins mit harten SLAs. Und selbst Unternehmen deren Admins den Grundschutz aufgebaut haben und über harte SLAs verfügen, sind in Zeiten von Spectre und Meltdown, bis zum nächsten und hoffentlich besseren Patch von Intel & Co, schutzlos den existierenden Gefahren ausgesetzt.

Eine derartige Schutzlosigkeit ist für den heutigen Grad der Digitalisierung inakzeptabel und sollte insbesondere die Verantwortlichen in staatlichen Bereichen zur stärkeren Zusammenarbeit mit IT-Sicherheitsexperten animieren. Nicht grundlos ist unsere Wehrhaftigkeit auch im Bereich Cyber keinesfalls besser aufgestellt als in der konventionellen Verteidigung.

„Anbieter von vernetzten IT-Produkten liefern entweder die Pest oder Cholera ins Haus"

Der Satz stammt nicht von mir, sondern von einem Vorstand eines Konzerns, nachdem sich herausstellte, dass unberechtigte Dritte durch Exploits auf die Datenbank des Unternehmens zugreifen konnten. Zuvor konnte man bereits mit einem Tool die Firewalls des Konzerns übernehmen, ohne dass die Übernahme in den Logs der Firewall ersichtlich war. Die Systeme waren mit aktuellen Patches ausgestattet. Ja es gibt Exploits, die durch mangelnde Qualitätskontrolle, kurze Entwicklungs-zyklen, schlechte Umsetzungen, Gewinnstreben oder letztendlich die Fehlbarkeit des Menschen hervorgerufen werden. Leider analysieren wir auch immer ausgefeiltere Backdoors, die bereits in Produkten verankert sind. Ist der Hersteller nicht unmittelbar bereit die Backdoor zu schließen, können wir bereits heute durch eine vorgelagerte Filterung den Zugriff auf die effektiv Backdoor unterbinden.

Die Filterung von DDoS-Angriffen am Frankfurter Hub würde alle nachgelagerten Netze vor gewaltigen Datenfluten schützen und Angriffe effektiv abwehren.

Gehen wir hierzu in die Tiefe der DDos-Angriffe

Bei der Ausführung von DDoS-Angriffen haben sich zwei Vorgehensweisen als besonders effektiv erwiesen, die durch direkte Übermittlung von gleichzeitigen Anfragen einer großen Anzahl von Bots das Ziel angreifen oder einen Verstärkungsangriff ermöglichen:

Im ersten Szenario werden Computer, neuerdings bevorzugt IoT, in „Zombies" verwandelt, die dann den Zielangaben folgen, um gemeinschaftlich Systeme anzugreifen und mit Anfragen zu fluten.

Beim zweiten Szenario, dem Verstärkungsangriff, werden anstelle des Bot-Netzes Server in Rechenzentren angemietet. Weitere Server mit Konfigurationsfehlern werden häufig noch hinzugefügt. Angriffe werden z.B. durch die Manipulation von IP-Rückgabeadressen oder das Senden von manipulierten Datenpaketen, die von angegriffenen Servern mit sehr langen Paketen beantwortet werden, die wiederum über eine manipulierte IP-Adresse zum Angriffsziel geleitet werden, durchgeführt.

Der Ansatz, die Installation der Scan- und Filtermechanismen auf Seiten der angegriffenen Systeme aufzusetzen, ist nur eine Maßnahme, reicht aber nicht aus, um den Angriff abzuwehren:

1.) Die Konfiguration und Bedienung der Firewall, des Load Balancers, des Proxies, der Server, … bedarf speziell geschulte Mitarbeiter, die fortlaufend weitergebildet werden müssen.

2.) Selbst mit ausgebildeten Admins und einer fehlerfrei konfigurierten Firewall versagt die Verteidigung des Angriffs völlig, wenn der Angriff die Internetverbindung lahmlegt. Ein geschützter Service mit einem speziell weitergebildeten Admin an der

Konsole hat keinerlei Nutzen, wenn der Service nicht mehr per Internet erreichbar ist.

3.) Mit intelligenten DDoS-Verstärkungsangriffen ist es für einen erfahrenen Angreifer sehr einfach, eine Internetanbindung zu überlasten.

Man könnte meinen, der Ansatz den Datenverkehr vom Provider scannen und filtern zu lassen wäre ein besserer Schutz, da die Internetanbindung des Providers eine höhere Bandbreite hat und somit schwieriger zu überlasten ist.

4.) Auch 2018 besitzen die meisten Provider keine speziellen Sicherheitseinrichtungen und filtern lediglich den offensichtlichen Datenmüll heraus. Einige Konzerne beschäftigen sich mit dem Thema seit 2017 und haben hierfür 3 Admins in der Ausbildung! Trotzdem bleiben intelligente DDoS-Verstärkungsangriffe in der ersten Angriffswelle zu 99% unbemerkt, da für eine Analyse des Angriffs und die sofortige Anpassung der Scan- und Filtermechanismen höchste Expertise und Erfahrung erforderlich ist.

5.) Wir erleben Angriffe, die mit Hilfe von inkorrekt konfigurierten LDAP-Servern durchgeführt werden und Spitzenwerte mit 28 bis 33 Gbit/Sek führen. Da immer häufiger zeitgleich Verstärkungsangriffe durchgeführt werden, können Spitzenwerte von bis zu 100 Gbit/Sek auftreten, die selbst bei führenden Providern massive Schwierigkeiten auslösen. Wenn durch einen Angriff das Routing verändert werden muss, oder auf andere Datenanbindungen zurückgegriffen werden muss, führt die Anpassung der Regeln bei 99% der Angriffe in den zeitweisen offline Modus!

Die effektivste Methode zur Neutralisierung der DDoS-Angriffe führt somit zur Forderung, die Scan- und Filtermechanismen am Frankfurter Hub einzusetzen.

Aus unserer täglichen Arbeit wissen wir, dass durch den zentralen Einsatz von Scan- und Filtermechanismen, Cyberrisiken präventiv unterbunden werden und die digitalisierte Wirtschaft vor Angriffen und Spionage effektiv geschützt werden kann.

Die Scan- und Filtermechanismen am Frankfurter Hub Bot-Netze und C&C Server triggern zu lassen, ist effektiv und geht Risiken präventiv an zentraler Stelle an.

Gehen wir hierzu in die Tiefe des C&C triggern

Bei der Aufnahme von Computern in Bot-Netze haben sich zwei Vorgehensweisen als besonders effektiv bewiesen, um zeitnah eine große Anzahl von Bots per C&C-Server zu steuern und Angriffe auszuführen:

Im ersten Szenario werden Computer mit Sicherheitslücken, neuerdings bevorzugt IoT, von Scannern erfasst, angegriffen und in „Zombies" verwandelt und zumindest einem C&C-Server zugeordnet. Bots greifen beispielsweise mit Angriffen auf offene Ports weitere Systeme hinter der Firewall an, was dazu dient, das Bot-Netz weiter wachsen zu lassen. Aus dem jeweiligen Subnetz der Bots werden Daten direkt an den C&C-Server, unverschlüsselt oder verschlüsselt, übermittelt. Der C&C-Operator analysiert die aufgenommen Bots, sortiert sie nach den jeweiligen Leistungsdaten und ermöglicht so einen kombinierten Angriff aller gemanagten Bots, die bis zum Angriff als Standby-Bot ihre übliche Funktion erfüllen.

Beim zweiten Szenario, werden Computer erfasst, angegriffen und in Bots verwandelt und über einen Covert Channel mit dem C&C-Server direkt oder indirekt verbunden. Hierzu werden bevorzugt Soziale-Netze oder durch die Bots aufgebaute P2P-Strukturen verwendet, in denen oftmals ein Anteil der Bots zusätzlich als C&C-Server fungieren.

Die Bots, die als C&C-Server fungieren, sind von entscheidender Bedeutung für die gesamte Struktur, da sie in der Lage sind, den Haupt-C&C-Server nach Belieben zu ändern, ohne das der C&C-Operator die Kontrolle über das gesamte Bot-Netz verliert. Aktuell konzentrieren sich diese intelligenten Bot-Netze auf die leichte Beute der IoT-Systeme.

Der Ansatz, die Installation der Scan- und Filtermechanismen auf der Seite der angegriffenen Systeme aufzusetzen, ist eine Maßnahme, sie reicht aber nicht aus, um C&C-Server vor dem Angriff zu triggern:

1.) Die Administration der Scan- und Filtermechanismen bedarf speziell geschulter Mitarbeiter die fortlaufend weitergebildet werden müssen.

2.) Selbst mit ausgebildeten Mitarbeitern und qualifiziert eingerichteten Scan- und Filtermechanismen ist es eine Herausforderung Bots, die über Covert Channel mit einem C&C-Server verbunden sind, zu identifizieren, da oftmals erst ab einer relevanten Anzahl von Bots oder einer relevanten Datenmenge der Bots die Aktivität überhaupt auffällt.

Man könnte meinen, der Ansatz den Datenverkehr beim Provider scannen und filtern zu lassen wäre ein besserer Schutz, da der Provider Daten aus den jeweiligen Subnetzen auf Anomalitäten analysieren kann.

3.) Auch 2018 besitzen die meisten Provider keine speziellen Sicherheitseinrichtungen und filtern lediglich den offensichtlichen Datenmüll heraus. Wird der Kontakt zu einem C&C-Server aufbaut, um dort entweder ausgespähte Daten abzuliefern, sich selbst zu aktualisieren oder Befehle abzuholen wird beispielsweise DNS-Tunneling verwendet. Das DNS-Protokoll ist für die Auflösung von Namen, beispielsweise aus URLs zu IP-Adressen, zuständig.

Bei einem DNS-Tunnel wird die ausgehende Kommunikation in DNS-Abfragen versteckt und die IP-Adresse der Antwort enthält die eingehenden Daten. Da die meisten Provider die Auflösung von externen Namen in ihren Subnetzen erlauben, kann somit ein ungehinderter Datenaustausch erfolgen, der von den meisten Providern weder bemerkt noch behindert wird. Daher bleiben intelligente Aufnahmen von Bots in Bot-Netze bis zur ersten Angriffswelle zu 99% unbemerkt, da für eine Analyse des Angriffs und die sofortige Anpassung der Scan- und Filtermechanismen höchste Expertise und Erfahrung erforderlich ist.

Wenn die Kommunikation zwischen dem Bot im Subnetz und dem C&C-Server über HTTPS erfolgt, sind bei einem Covert Channel spezialisierte Sicherheitsprodukte oftmals wirkungslos, die genau diese versteckte Kommunikation anhand ihrer speziellen Eigenschaften erkennen sollen. Die häufige Änderung des Host-Anteils einer Namensauflösung, die Herkunft und das Alter der angefragten Domäne, die Menge der übermittelten Daten und weitere Details fließen dabei in eine Bewertung ein, was in 99% der Bot Kommunikation über Covert Channel und Soziale Netze, selbst bei spezialisierten Sicherheitsprodukten, zu keinen Alarm führt.

4.) Wir haben 2017 einen Angriff analysiert in dem Server ohne die Verwendung von Exploits durch einen C&C Verbund für einen verheerenden Angriff missbraucht wurden.

Die effektivste Methode zur Neutralisierung von C&C Servern führt somit zur Forderung, die Scan- und Filtermechanismen am Frankfurter Hub einzusetzen.

Speziell ausgebildete Experten und Scan- und Filtermechanismen machen den Frankfurter Hub zum europäischen Abwehrzentum für Cyberangriffe.

Die Menge der dort zusammenlaufenden Subnetze aller relevanten Provider ermöglicht ein effektives und sehr schnelles Triggern von C&C-Server, die auf Basis der von mir beschriebenen Szenarien Bots managen oder Server missbrauchen.

5.) Scan- und Filtermechanismen unterbinden den digitalen Aderlass und sind in der Rückgewinnung der informationellen Selbstbestimmung unersetzlich.

Mit hochfrequenten Honeypots werden Malware und Deployment-Versuche festgestellt, ihr Verhalten analysiert und die Verbindungen zu anderen Hosts im Internet ausgewertet. So wird die Aktivität verstanden und sowohl die Verbindung zum C&C-Server als auch die fortlaufende Suche nach weiteren Computern, die sich als Bot durch Sicherheitslücken anbieten, effektiv durch die Filtermechanismen am Hub unterbunden. So können selbst einzelne Bots, die nach einem Neustart erneut durch einen Schadcode aus dem Bios oder anderen Chips kompromittiert werden, nicht mehr von C&C-Servern gemanagt werden. Mit anderen Worten, wir ermitteln so Cybergefahren bevor ein Angriff stattfindet, verhindern Spionage und die Ausbreitung von Angriffen an der zentralen Stelle. Infizierte oder erneut infizierte Subnetze können somit über den Frankfurter Hub europaweit analysiert werden und lokale Provider können zielführende Informationen zur Infektion und zur Bereinigung der Bots und zu Sicherheitslücken in ihren Subnetzen erhalten, so wird das Risiko für andere Provider beseitigt bevor die Gefahr um sich greift.

Der Frankfurter Hub hat bereits heute die notwendigen Anbindungen und Kapazitäten, um den Scan- und Filtermechanismen die notwendige Flexibilität zur Verfügung zu stellen.

Zur technischen Realisierung wurde ein entsprechendes Verfahren entwickelt, welches keine Man-in-the-Middle-Attacke darstellt und somit nicht gegen §202a StGB, Ausspähen von Daten bzw. §202 b StGB, Abfangen von Daten, verstößt.

Das Verfahren könnte somit nach heutiger Rechtslage sofort am Frankfurter Hub zum Einsatz kommen. Speziell ausgebildete Experten und Scan- und Filtermechanismen machen den Frankfurter Hub zum Europäischen Verteidigungspunkt für Cyberangriffe. So werden Angriffe bereits neutralisiert bevor die Provider-Netze davon tangiert werden. So kann man Cyberrisiken präventiv unterbinden und die digitalisierte Wirtschaft vor Angriffen und Spionage schützen. Selbst im Falle eines Cyberwars können so Provider und die kritische Infrastruktur effektiv vor einer Überlastung geschützt werden.

Scan- und Filtermechanismen am Frankfurter Hub:

- der zentrale Cyberschutz sichert die Digitalisierung der Gesellschaft;

- die digitalisierte Wirtschaft wird vor Angriffen und Spionage geschützt;

- die Sicherheit der kritischen Infrastruktur wird erhöht;

- Cyberrisiken werden präventiv unterbunden;

- im Falle eines Cyberwars steht eine Verteidigung der digitalen Infrastruktur an zentraler Stelle.

Ich empfehle daher, dass Scan- und Filtermechanismen schnellst möglichst am Frankfurter Hub zum Einsatz kommen.

Das Whitepaper wird dem kommenden Innenminister vorgestellt. Zur Umsetzung wird eine Taskforce empfohlen, zu der die technischen Direktoren der Provider des Frankfurter Hubs eine Einladung zur Teilnahme erhalten. Weitere Teilnehmer der Taskforce sollten das BSI und die Bundeswehr sein.

Die Scan- und Filtermechanismen am Frankfurter Hub triggern zu lassen, ist effektiv, zeitgemäß und sollte weitere Unterstützer finden, da dadurch die Cybersicherheit deutlich gestärkt wird und Risiken präventiv an zentraler Stelle angegangen werden.

Als Autor lade ich Sie zu der dazugehörigen Diskussion ein

http://bit.ly/2mSKGXl

und freue mich auf Ihre Unterstützung!

Weitere Informationen stehen online zur Verfügung: panamp.de

Kontakt
PAN AMP AG
Hamburger Str. 11
D-22083 Hamburg
Tel.: +49 (40) 55 30 02 – 0
Fax : +49 (40) 55 30 02 - 110
Email: info@panamp.de
Internet: panamp.de

Bert Weingarten: „Scan- und Filtermechanismen am Frankfurter Hub schützen die Gesellschaft vor Cybergefahren und ermöglichen der Bundeswehr die Verteidigung des virtuellen Raumes im Verteidigungsfall". [Foto: Christof Mattes]

Seit dem Beginn der 90 Jahre hat Bert Weingarten zahlreiche nationale und internationale Projekte zur Internetfilterung erfolgreich aufgebaut. Sei es in Bundeseinrichtungen, Forschungseinrichtungen, Banken, Konzernen - mit europaweiten und weltweiten Netzen - in keinem einzigen Projekt ging es um Zensur. Zusammen mit staatlichen Einrichtungen und Verbänden unterstütze er seit zwei Jahrzehnten Wirtschaftsschutzveranstaltungen und Wirtschaftsschutztagungen, die sich gegen Spionage richten. 2006 leitete er die ersten Fortbildungsmaßnahmen für staatliche Internet-fahnder mit dem Bund Deutscher Kriminalbeamter und konzipierte 2014 gemeinsam mit der Hochschule Wismar den berufsbegleitenden Fernstudiengang „Bachelor Forensic Engineering".

Nachweislich gehören die Vorträge, Veranstaltungen und Fortbildungen der PAN AMP AG seit zwei Jahrzehnten zu den Aktivitäten, die Frühzeitig auf resultierende Gefahren und Sorglosigkeiten in der Nutzung des Internets aufmerksam machen und diese angehen.