Bundesamt für Sicherheit
in der Informationstechnik
Bundesamt für Verfassungsschutz
Bundeskriminalamt
Bundesnachrichtendienst

Sonderbericht Wirtschaftsschutz

Informationen der deutschen Sicherheitsbehörden des Bundes

9. Sonderausgabe Cybersicherheit

Stand: 09.09.2016

Inhalt

1. Deutschland: CEO-Frauds führen nach wie vor zum Erfolg

Bei der „Chef-Masche“ geben sich Cyber-Kriminelle als Entscheider eines Unternehmens aus und versuchen, autorisierte Mitarbeiter zum Auslösen von Zahlungen zu veranlassen.

Im August 2016 gab der Nürnberger Automobilzulieferer und Kabelspezialist Leoni bekannt, dass das Unternehmen von Unbekannten um 40 Mio. Euro erleichtert wurde. Die Täter hatten Dokumente und Identitäten gefälscht und über „elektronische Kommunikationswege“ Zahlungen veranlasst. Diese international unter dem Begriff „CEO Fraud“ bekannte Betrugsmasche ist nicht neu. Das Bundeskriminalamt (BKA) verzeichnete seit 2013 250 solcher Fälle, von denen 68 zum Erfolg führten.

Der Gesamtschaden lag in Deutschland bei ca. 110 Mio. Euro. International bezifferte das FBI den Schaden in 110 Ländern auf insgesamt 3,1 Mrd. USD. Um ihre Identitäten zu verschleiern, nutzen die Täter neben dem Telefon insbesondere E-Mails zur Kontaktaufnahme mit den Finanzabteilungen der Unternehmen – so lässt sich der Angriff aus sicherer Entfernung durchführen und die Identität bestmöglich verschleiern.

Es bieten sich nur sehr wenige technische Möglichkeiten, um CEO-Frauds zu verhindern. In erster Linie bietet es sich an, beim organisationsinternen Mailverkehr nur signierte E-Mails zuzulassen. Andernfalls sollten Mailheader geprüft werden, um gefälschte Absender zu identifizieren. Weiterer Schutz lässt sich lediglich über organisatorische Maßnahmen erreichen. So sollten Mitarbeiter aus den Finanzabteilungen besonders geschult werden, um verdächtige Mails, Anrufe und Briefe erkennen zu können. Darüber hinaus empfiehlt es sich, interne Prozesse für Überweisungen festzulegen, bspw. mit Vier-Augen-Prinzipien für alltägliche Beträge sowie festen Betragsgrenzen, ab denen Transaktionen nur durch die Führungsebene autorisiert werden kann oder telefonische Rücksprachen erfordern.

Darüber hinaus sind für alle an Zahlungen beteiligten Personen Vertretungsregelungen notwendig. Für ihre Betrugsversuche führen die Täter häufig ausführliche Recherchen durch, um die Namen und Befugnisse von Geschäftsführung und den beteiligten Personen in den Finanzabteilungen zu

identifizieren und ihre Schreiben entsprechend zu verfassen. Hier sollte versucht werden, diese Informationen möglichst gar nicht nach außen dringen zu lassen. U.a. sollten Mitarbeiter ihre Tätigkeiten in Finanzabteilungen möglichst nicht öffentlich machen. Hierzu zählt neben der bedachten Preisgabe von Daten in Sozialen Netzwerken auch die korrekte Entsorgung von Papiermüll – z. B. durch Schreddern. (BSI)

2. Deutschland: Sicherheitsupdates als wesentlicher Beitrag zum Schutz vor Cyber-Angriffen

Cyber-Kriminelle nutzen für ihre Angriffe häufig offene Sicherheitslücken in IT-Systemen. Obwohl viele Hersteller nach Bekanntwerden der Schwachstellen entsprechende Patches anbieten, werden diese von den Nutzern häufig nur verspätet oder gar nicht installiert. Angreifern steht die Tür für Cyberattacken damit offen.

Im August 2016 wurden von der Hacker-Gruppe „Shadow Brokers“ verschiedene Tools für Cyberattacken im Internet angeboten, die aus dem Fundus der NSA-Werkzeuge stammen sollen. Experten gehen nach ersten Einschätzungen davon aus, dass die Inhalte echt sind. Mit den Angriffswerkzeugen kann insbesondere Netzwerk-Hardware bekannter Hersteller kompromittiert werden. Für die Angriffe nutzen die Tools zwei Arten von Schwachstellen aus, die nicht nur im vorliegenden Fall, sondern grundsätzlich bei Cyberattacken Anwendung finden: zum einen bis dato noch unbekannte Sicherheitslücken, sogenannte Zero Day Exploits, zum anderen Sicherheitslücken, die bereits von Sicherheitsforschern entdeckt und zum Teil schon von den Herstellern gepatcht wurden.

Es liegt in der Natur der Sache, dass es nie einen vollständigen Schutz vor Zero Day Exploits geben wird: Erlangen Cyber-Kriminelle Kenntnis über offene Schwachstellen, haben sie einen Informationsvorsprung, bis der Hersteller einen Patch nachliefert. Dieses Zeitfenster kann eine Dauer von wenigen Stunden bis hin zu mehreren Jahren haben, sich mitunter aber auch niemals schließen. Bei der Ausnutzung von bereits bekannten Sicherheitslücken sind jedoch neben den Herstellern der betroffenen Produkte auch deren Nutzer in der Pflicht. IT-Sicherheitsverantwortliche sollten regelmäßig prüfen, ob für die

in der eigenen Institution eingesetzte Hard- und Software Schwachstellen bekannt werden und die Hersteller entsprechende Sicherheitsupdates veröffentlichen. Diese Informationen finden Interessierte beispielsweise auf den Webseiten der Hersteller oder bei Informationsplattformen, wie CERT-Bund oder branchenspezifischen CERTs.

Es sollte stets das Ziel sein, die Patchstände für die IT möglichst aktuell zu halten. Auf diese Weise können bereits sehr viele Cyberangriffe abgewehrt werden. Um zumindest einen minimalen Schutz vor Zero Day Exploits zu erreichen, eignet sich insbesondere die Sensibilisierung von Mitarbeitern. Werden Anhänge aus unbekannten und fragwürdig erscheinenden E-Mails nicht geöffnet sowie „zufällig" gefundene USB-Sticks nicht angeschlossen, finden die Angreifer zumindest erschwerende Umstände vor. Zu prüfen ist außerdem die sichere Konfiguration der eingesetzten Komponenten. Hier bietet zum Beispiel das Bundesamt für Sicherheit in der Informationstechnik verschiedene Empfehlungen an. (BSI)

3. Deutschland: Hacking-Aktivitäten von Jihadisten in Deutschland auf begrenztem Niveau

Bisherige Beobachtungen lassen darauf schließen, dass sich die jihadistische Hacking-Szene noch in einem frühen Entwicklungsstadium befindet. Dieser Eindruck erhärtet sich insbesondere in der Betrachtung deutscher islamistischer Hacker.

Die bisher gezeigten Fähigkeiten bewegen sich größtenteils auf einem Niveau, das durch Online-Kurse oder Video-Tutorials erreicht werden kann. Tiefgehendes Fachwissen ist selten vorhanden. Dennoch ist zu beobachten, dass die Szene nach einer Steigerung ihrer Fähigkeiten strebt. In ihrer Wirkung sind islamistische Hacking-Aktivitäten bisher auf den Bereich der Propaganda und medienwirksamer Aktionen beschränkt. Jedoch zeigt sich, dass islamistische Hacker den Rahmen ihrer Fähigkeiten äußerst effektiv ausschöpfen. Islamistischen Hackern ist das Potenzial elektronischer Kriegsführung bewusst und wird von ihnen intensiv diskutiert. Eine Weiterentwicklung ihrer Fähigkeiten in effektive Formen elektronischer Angriffe ist zu erwarten.

International agierende islamistische Gruppierungen und Einzelpersonen führen seit mehreren Jahren Defacements durch. Dabei hinterlassen sie auf angegriffenen Webseiten neben Gebetsaufrufen und auffälligen Emblemen häufig auch Drohungen gegen „Ungläubige“. Veröffentlichungen von (angeblichen) Erfolgsberichten dienen Propagandazwecken im Kampf gegen „kreuzzüglerische“ Staaten und deren Bevölkerung. Auch deutsche Webpräsenzen waren in der Vergangenheit betroffen. Tatsächlich sind diese Vorfälle aber nicht als gezielte Angriffe gegen Deutschland, sondern als Zufallstreffer bei opportunistischen Massenangriffen gegen Webseiten mit bestimmten Schwachstellen zu betrachten. Die zur Durchführung von Defacements eingesetzte Software ist im Internet zum Teil kostenlos erhältlich und aufgrund ihrer grafischen Benutzeroberfläche selbst für eine technisch wenig versierte Klientel einfach zu bedienen. Auf Videoplattformen wie YOUTUBE wird in sogenannten Tutorials erklärt, wie die entsprechende Software eingesetzt und Sicherheitslücken von Internetseiten oder Webservern ausgenutzt werden können.

Vereinzelt konnten Berichte zu „übernommenen“ oder „entführten“ Accounts in sozialen Netzwerken (wie TWITTER oder FACEBOOK) festgestellt werden. Dabei werden bspw. TWITTER -Accounts seriöser Medienstellen unter Kontrolle gebracht, um dort Falsch- oder Propagandameldungen zu veröffentlichen. Diese Art von Angriffen wird zumeist durch die Verwendung unsicherer Passwörter durch den Account-Inhaber ermöglicht, oft in Verbindung mit fahrlässiger Handhabung dieser Passwörter. Zum Beispiel waren in einem Interview des Fernsehsenders TV5Monde die Passwörter für den YOUTUBE-, INSTAGRAM- und TWITTER -Account des Senders zu sehen, der unabhängig davon tags zuvor zum Ziel eines Elektronischen Angriffs geworden war. Es liegen darüber hinaus inhaltlich glaubhafte Berichte zu Phishing-Angriffen vor, um Zugang zu Profilen in sozialen Netzwerken zu erlangen.

Neben den bereits dargestellten Fähigkeiten in Bezug auf elektronische Angriffe durch Islamisten sind gerade auch solche Aktionen zu beachten, die nur scheinbar von diesen begangen werden. Unter einer False-Flag-Operation ist ein (nicht nur) elektronischer Angriff zu verstehen, der unter vorgetäuschter Urheberschaft begangen beziehungsweise bekanntgegeben wird. Festgestellte komplexere Angriffe, die auf den ersten Blick islamistisch motiviert schienen, haben sich bei einer näheren Betrachtung als False-Flag-Operation anderer

Urheber erwiesen, so unter anderem der bereits erwähnte Angriff auf TV5Monde.

Bislang liegen keine Hinweise vor, dass Islamisten über die für komplexere Angriffe gegen kritische Infrastrukturen notwendigen technischen Fähigkeiten verfügen oder solche Angriffe ausgeführt hätten. Dem stehen Kommentierungen in sozialen Netzwerken oder Diskussionen in jihadistischen Internetforen gegenüber, die seit längerer Zeit ein gleichbleibend frühes Planungsstadium für Angriffe auf kritische Infrastrukturen erkennen lassen. Mangels entsprechender Angriffe dürfte davon auszugehen sein, dass Islamisten aktuell nicht über die Fähigkeiten verfügen, gezielt Angriffe auf kritische Infrastrukturen auszuführen.

Ein Angriff könnte insbesondere durch die Ausnutzung von Schwachstellen in Computersystemen mit Internetverbindung erfolgen. Diese Schwachstellen können durch spezielle, für jedermann nutzbare Suchmaschinen relativ einfach aufgespürt werden und sodann mittels frei verfügbarer „Angriffs-Baukästen", wie z.B. aus dem Metasploit-Projekt[1], gezielt angegriffen werden. Das zukünftige Gefährdungspotenzial hängt maßgeblich von der Entwicklung der Fähigkeiten der islamistischen Szene im Bereich der Elektronischen Angriffe ab. Während die propagandistisch erfolgreiche Durchführung von Defacements und Account-Übernahmen bereits beobachtet werden konnte sind bisher keine erfolgreichen Angriffe auf kritische Infrastrukturen bekannt geworden. Die zukünftige Bedrohungslage durch Islamisten wird maßgeblich davon abhängen, ob es diesen gelingt, IT-Spezialisten zu rekrutieren oder eine eigene Expertise aufzubauen.

Hierbei ist insbesondere zu berücksichtigen, dass die Ideologie des Islamismus ihre Anziehungskraft gerade auch auf jüngere Menschen mit Affinität zur Informationstechnik entfaltet. Ebenso sollte nicht vergessen werden, dass der IS bereits in seiner Medienkompetenz eine rasche Professionalisierung gezeigt und den Umgang mit Medien allgemein zu einem herausragenden Element im kriegerischen Jihad ausgebaut hat. Eine ähnlich rasche und professionelle Entwicklung von IT-Fertigkeiten ist daher naheliegend. Eine weitere Möglichkeit für radikal-islamistische oder terroristische Organisationen ein entsprechendes technisches Know-how zur Begehung elektronischer Angriffe

1 Das Metasploit-Projekt dient eigentlich der Computersicherheit. Bei diesem Open-Source-Projekt werden Informationen über Sicherheitslücken gesammelt, die bei Penetrationstests und der Entwicklung von Signaturen eingesetzt werden können.

zu erlangen, besteht im käuflichen Erwerb. Geeignete Quellen wären hier das „Deep Web“ oder Strukturen in der Organisierten Kriminalität. Sollte sich die islamistische Hackerszene tatsächlich in ihren Fähigkeiten verbessern oder sich für terroristische Organisationen die Möglichkeit zum Erwerb entsprechender Fähigkeiten ergeben, besteht die realistische Gefahr eines gefährlichen elektronischen Angriffs, der auch kritische Infrastrukturen betreffen könnte.

Zusammenfassend ist davon auszugehen, dass die islamistische Szene bestrebt ist, ihre Fähigkeiten im IT-Bereich auszubauen. Hierbei ist auch der Anspruch der geistigen Führung gegenüber ihren Anhängern, sich im Bereich der digitalen Kriegsführung zu etablieren, zu berücksichtigen. Auch das Sicherheits- und Selbstschutzinteresse beim Umgang mit sozialen Kommunikationsmedien rückt für Islamisten immer stärker in den Vordergrund. (BfV)

4. International gesamte Welt: Gefahr der Ausspähung von E-Mails über Push-Dienste

Sogenannte E-Mail-Push-Dienste bieten im Mobilfunkbereich die Möglichkeit, zeitnah über den Erhalt von E-Mails benachrichtigt zu werden. Hierfür muss der Nutzer in der Regel seine Login-Daten dem Anbieter einer solchen Dienstleistung zur Verfügung stellen. Dadurch besteht die Gefahr der Ausspähung. Darüber hinaus können die dabei entstehenden Datenverkehre von versierten Nachrichtendiensten erfasst und ausgewertet werden. Zu den führenden Firmen, die E-Mail-Push-Dienste anbieten zählen auch russische Unternehmen. Aufgrund der sich stetig verschärfenden russischen Gesetzgebung im Bereich der Telekommunikations- und Internet-überwachung, sowie der technischen Aufwertung des Überwachungssystems SORM[2] ist hier die Gefahr einer nicht autorisierten Einsichtnahme besonders hervorzuheben. Generell ist die Verwendung von E-Mail-Push-Diensten kritisch zu bewerten, da die Vertraulichkeit und Integrität der Daten nicht gewährleistet, sowie eine Nachvollziehbarkeit des Transfers von Daten kaum möglich ist.

2 SORM (kyrill.:COPM). Ist ein Überwachungsprogramm des russischen Inlandsgeheimdienstes (FSB). Ziel von SORM ist es, alle Telefon- und Internetdaten Russlands zu speichern um sie bei Bedarf auswerten zu können.

In der mobilen Kommunikation, insbesondere mittels Smartphones, haben die Nutzer die Möglichkeit, jederzeit ihre E-Mails abzurufen[3]. Nachteilig ist, dass ankommende Nachrichten (providerabhängig) nicht sofort auf dem Endgerät zur Verfügung stehen. Auch generiert dieser Abfragemodus unnötig viel Datenverkehr. Alternativ bieten einige E-Mail-Provider sogenannte Push-Services bzw. Push-Mail-Dienste an. Dabei werden neue Nachrichten bzw. E-Mails vom Mail-Server automatisch komprimiert und zeitnah auf das Endgerät des Nutzers gesendet, was den Datenverkehr erheblich reduziert. Nur wenige E-Mail Anbieter offerieren ihren Kunden einen solchen Service.

Für diesen Service ist ein technischer „Kunstgriff“ notwendig. Nachdem der Kunde die Zugangsdaten für sein E-Mail-Konto an den Push-Service-Anbieter übermittelt hat, fragt dieser sozusagen als Mittelsmann in regelmäßigen Abständen die Inhalte des Mail-Servers ab. Diese werden dort zwischengespeichert und anschließend zeitnah an das Endgerät des Kunden gesendet bzw. „gepusht“ (siehe Abbildung 1).

Bei Push-Diensten ist für den Anwender nicht unmittelbar ersichtlich durch welche Länder seine Daten fließen. Beispielsweise hat ein russischer Anbieter auch Tochterunternehmen im westlichen Ausland.

Der E-Mail-Client dieses Anbieters verwendet für seinen Push-Dienst genau das weiter oben beschriebene Verfahren und nutzt eigenen Angaben zur Folge für seine Server angeblich auch Rechenzentren in den Niederlanden oder den USA.

Frei zugängliche Internet-Registrierungsinformationen[4] zeigen dagegen nicht eindeutig auf Serverstandorte in den Niederlanden bzw. den USA.

Aufgrund der Tatsache, dass der Anbieter von Push-Diensten Zugriff auf die Inhalte des E-Mail-Kontos erhält, ergibt sich ein bemerkenswerter Aspekt hinsichtlich der Datenschutzrichtlinien und Servicebedingungen. Im Fall der Richtlinie des russischen Push-Dienst-Anbieters erklärt sich der Nutzer damit einverstanden, dass dieser Anbieter nicht-personenbezogene und

3 Neben der vorinstallierten Software für die Bearbeitung von Mails auf den jeweiligen Betriebssystemen, wie zum Beispiel Android, iOS oder Windows sind eine Vielzahl von Apps verfügbar, die diese Funktionalität anbieten.

4 Bzw. WHOIS-Daten WHOIS (aus dem Englischen "who is" = wer ist) ist ein spezielles Internet-Protokoll zur Abfrage von Informationen, sog. Registrantendaten (z.B. Inhaber bzw. Verantwortlicher für eine Domain, Betreiber des Netzwerkes eines definierten IP-Bereiches etc.), von Internet-Domains und IP-Adressen. Diese Registrantendaten können auch über spezielle Angebote im Internet abgefragt werden.

personenbezogene Daten sammeln darf Verbunden damit ist ebenso die Weitergabe der Daten an Dritte, unter anderem zu Marketingzwecken oder im Rahmen von Gerichtsverfahren.

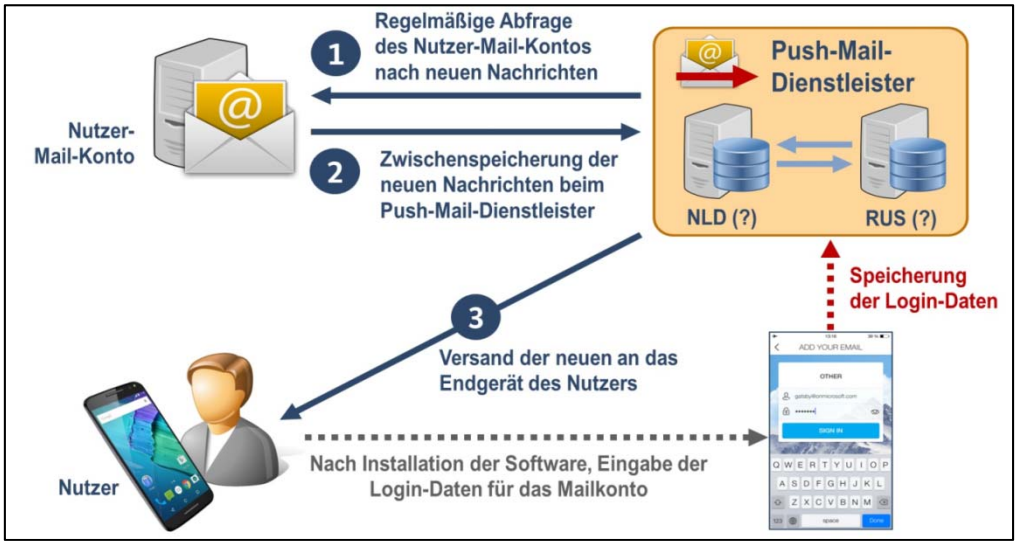

Abbildung 1: Funktionsweise von Push-Mail-Diensten (Quelle: BND)

Russland verschärft seit geraumer Zeit stetig seine Gesetzgebung im Bereich der Telekommunikations- und Internetüberwachung. Am 24. Juni diesen Jahres verabschiedete das russische Parlament ein ganzes Gesetzespaket (№ 1039149-6), mit einer Vielzahl diesbezüglicher Maßnahmen und Ermächtigungen. Das so genannte „Yarovaya-Paket“ verpflichtet zum Beispiel die russischen Telekommunikations- und Internet-Service-Anbieter (ISP), Aufzeichnungen von Anrufen und vor allem die kompletten Datenverkehre ihrer Kunden sechs Monate lang zu speichern und vorzuhalten. Zuvor mussten nur so genannte „Metadaten“[5] für diesen Zeitraum gespeichert werden. Ab 2018 erhöht sich diese Speicherdauer für Telekommunikationsanbieter auf drei Jahre (ein Jahr für ISPs). Zusätzlich müssen den Geheimdiensten und anderen staatlichen Organen der Zugang zu verschlüsselten Datenverkehren und Inhalten gewährt werden. Dies umfasst auch die sozialen Medien und Netzwerke.

Sofern die Kundendaten, Metainformationen und Mailinhalte auf ausländischen Servern gespeichert werden, unterliegen sie meist dem Datenschutzrecht des Staates, in dem der Server betrieben wird. Sollten im Rahmen der Datentransfers des russischen Push-Mail-Dienstleisters Daten in

5 Metadaten sind technische Informationen zu den jeweiligen Kommunikationsverbindungen, wie z.B. Telefonnummern oder IP-Adressen, Zeitpunkt u. Dauer der Kommunikation etc. Sie beinhalten keine Inhaltsdaten.

Rechenzentren in Russland (zwischen)gespeichert werden, hätten aus rechtlicher Sicht russische Staatsorgane die Möglichkeit, auf diese Daten zuzugreifen. Auf diesem Weg könnten russische Stellen (insbesondere Nachrichtendienste) für Spionagezwecke an die persönlichen Zugangsdaten der Mailkonten sowie Kommunikationsinhalte gelangen. Dies gilt dann generell für alle Kunden – also auch Kunden aus dem Ausland.

Die Verwendung von Push-Mail-Diensten birgt eine generell erhöhte Gefahr für die Vertraulichkeit der Kommunikation. Es ist für den Nutzer meist nur schwer, oder gar nicht prüf- und nachvollziehbar, wie seine persönlichen Daten verwendet oder geschützt werden. Der mögliche Missbrauch der Zugangsdaten stellt weiterhin eine Gefahr für die Authentizität des E-Mail Verkehrs dar, da Dritte diese nutzen können, um selbst im Namen der Opfer beispielsweise Spear-Phishing E-Mails zu erstellen. (BND)

5. International gesamte Welt: Gefahr der Cyber-Spionage mittels PlugX

Im Juni und Juli 2016 konnten Cyber-Spionageangriffe gegen deutsche, mittelständische Unternehmen festgestellt werden. Die Produkte dieser Unternehmen zählen weltweit teilweise zur Spitzenklasse. Ziel der Angreifer war nach hiesiger Ansicht die Beschaffung von Know-how zur Technologie.

Die für diese Cyber-Spionageangriffe eingesetzte Schadsoftware konnte mehrfach als „PlugX“ identifiziert werden. PlugX wird seit mindestens 2012 in China entwickelt und von chinesischen Cyber-Spionagegruppen sowie kriminellen Akteuren weltweit eingesetzt. Die Schadsoftware übermittelt Informationen über die technische Konfiguration der Computer des angegriffenen Unternehmens an einen C&C-Server[6]. Die bisherigen Indizien für mit PlugX in Verbindung stehenden C&C-Server lassen auf deren weltweite Verteilung schließen. Gewonnene Erkenntnisse zu Cyber-Angriffen mit PlugX im Ausland versetzen den BND in die Lage, derartige Aktivitäten auch gegen deutsche Ziele zu erkennen.

6 Als Command & Control-Server (C&C oder auch C2) wird ein Rechnersystem bezeichnet, welches Befehle und weitere Schadsoftware an bereits kompromittierte Opfersysteme verteilt. Die Kommunikation mit den Opfersystemen erfolgt meist in kryptierter oder verschleierter Form.

Die hier bekannten technischen Merkmale des Angriffs lassen zwar keine weitergehende Täterzuordnung zu. Durch das Ausschlusskriterium der weltweit erkennbaren Opfer von PlugX liegt die Wahrscheinlichkeit für die Zuordnung der Akteure in den chinesischen Raum jedoch nahe.

Systematische Cyber-Spionageangriffe, auch APTs[7] genannt, mit dem Ziel der Wirtschaftsspionage gegen westliche Hochtechnologiefirmen sind seit vielen Jahren zu beobachten. In Anbetracht der dabei ausgewählten Ziele ist die Beschaffung von Hochtechnologie-Know-how zur Steigerung der Wettbewerbsfähigkeit in der Fertigungsbranche die wahrscheinliche treibende Kraft für solche Aktionen. Deshalb kommen sowohl staatliche, als auch nicht-staatliche Akteure dafür in Frage. In Bezug auf China ist zudem ein Zusammenhang zwischen der intensiven wirtschaftlichen Expansion nach Europa, u.a. durch Firmenkäufe im Hochtechnologiesektor, und Cyber-Spionage zur Vorbereitung derartiger Handlungen zu vermuten.

Der Umfang an Cyber-Spionagekampagnen auch gegen die deutsche Wirtschaft wird nach hiesiger Einschätzung weiter zunehmen, weil sich die Akteure mit geringem Aufwand wertvolle Informationen, verschaffen können. Die dadurch erzielbaren Wettbewerbsvorteile gehen in der Regel zu Lasten der angegriffenen Unternehmen. (BND)

7 Als APT (Advanced Persistent Threat) bezeichnet man eine auf Dauer angelegte, systematische Operation, die mit höchst entwickelten Methoden und Techniken, meist durch einen staatlichen Akteur gestützt, durchgeführt wird, um langfristig Informationen abzuschöpfen. Die deutschen Cyber-Abwehrbehörden benutzen hierfür auch den Begriff des „Fallkomplexes“.