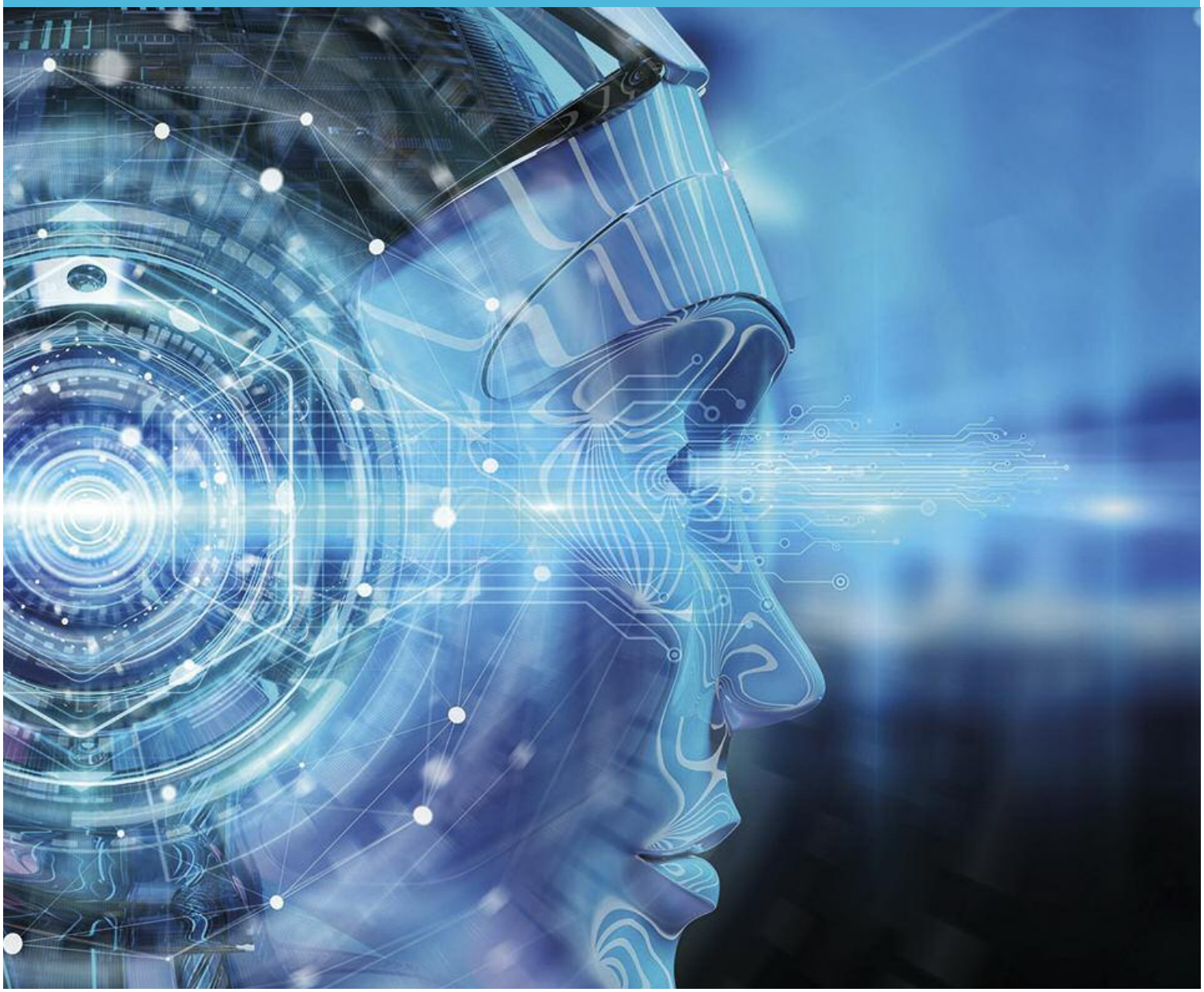
Bundesamt für
Verfassungsschutz

Nachrichtendienstlich gesteuerte Cyberangriffe



Nachrichtendienstlich gesteuerte Cyberangriffe

Inhaltsverzeichnis

Spionageziel Deutschland – Gefahren durch Cyberangriffe

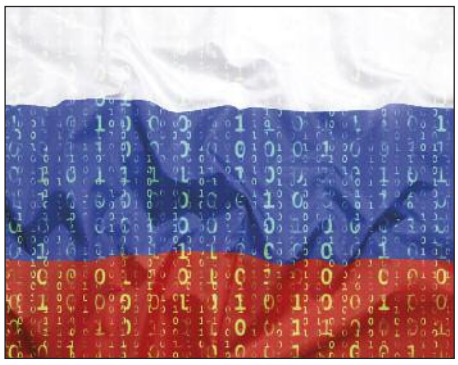
Die Bundesrepublik Deutschland steht aufgrund ihrer geopolitischen Lage, ihrer Rolle in der Europäischen Union und der NATO sowie als Standort zahlreicher Unternehmen der Spitzentechnologie im Fokus fremder Nachrichtendienste.

Bei der Spionage gegen Deutschland bilden die „klassischen“ Spionagemittel, wie z. B. der Einsatz menschlicher Quellen, nach wie vor eine wichtige Handlungsoption. Dies belegt eine Reihe aufgedeckter Spionagefälle der letzten Jahre. Daneben gewinnen aber auch technische Aufklärungsmaßnahmen stetig an Bedeutung. Fremde Nachrichtendienste setzen zunehmend Cyberangriffe ein, um Regierungsstellen, Wirtschaftsunternehmen oder Forschungsinstitute auszuforschen.

Besonders die Nachrichten- und Sicherheitsdienste der Russischen Föderation und der Volksrepublik China entfalten dabei in großem Umfang Spionageaktivitäten. Deren Schwerpunkte orientieren sich an den politischen Vorgaben ihrer Regierungen. Hierzu gehört auch der gesetzliche bzw. staatliche Auftrag, die eigene Volkswirtschaft mit solchen Informationen zu unterstützen, die auf nachrichtendienstlichem Weg beschafft wurden.

Neben Russland und China verfügen aber auch Nachrichtendienste anderer Staaten – wie etwa die des Iran – über die erforderlichen Ressourcen, um derartige technische Informationsgewinnungsmaßnahmen vom Ausland aus gegen deutsche Ziele ausführen zu können.

Russische Cyberangriffskampagnen



Methoden und Ziele

Die Nachrichtendienste der Russischen Föderation nutzen in großem Umfang Cyberangriffe zur Informationsbeschaffung, Desinformation und Propaganda. Russische nachrichtendienstliche Cyberangriffe gegen deutsche Ziele sind meist Teil mehrjähriger, international ausgerichteter Cyberspionage-Operationen. Sie finden im Rahmen einer umfassenden taktischen und strategischen Informationsgewinnung statt.

Diese Angriffskampagnen zeichnen sich aus durch

- eine hohe technische Qualifikation,
- starke finanzielle Ressourcen und
- außergewöhnliche Operativ- und Auswerterfähigkeiten.

Cyberangriffe der russischen Dienste bedrohen in erheblichem Maße die Informationssicherheit deutscher Stellen in Regierung und Verwaltung, aber auch in Wirtschaft, Wissenschaft und Forschung.

Viele dieser Angriffskampagnen weisen technische Gemeinsamkeiten auf. So werden z. B. immer wieder dieselben Serverinfrastrukturen und Schadsoftwarekomponenten verwendet. Dies sind wichtige Indizien für dieselbe Urheberschaft.

Die Angriffe russischer Dienste dienen vor allem der Stärkung der äußeren und inneren Sicherheit, der Sicherung strategischen Einflusses sowie der Förderung russischer Militär- und Energieexporte und russischer

Spitzentechnologie. Analog zur Aufklärung mit traditionellen Spionagemethoden liegt bei der Informationsgewinnung mittels Cyberangriffen der Fokus der russischen Dienste auf allen Politikfeldern, die russische Interessen berühren können:

- Energiepolitik und -sicherheit
- außenpolitische Fragen
  (EU-, Zentralasien-, Nahost-Politik)
- Militärpolitik
- die Verteilung von EU-Geldern
- humanitäre Fragen

Die Angreifer zielen auch auf die Ausforschung von Spitzentechnologien mit Schwerpunkt auf den Bereichen Energie-, Militär-, Röntgen- und Nukleartechnik sowie Luft- und Raumfahrt. Zudem stehen Regierungskritiker, Journalisten und NGOs sowie internationale Großbanken, Rundfunk- und Fernsehanstalten im Fokus russischer Angreifer.

Die Kampagnen richten sich deshalb gegen:

- supranationale Organisationen
- Regierungsstellen
- Streitkräfte
- Parlamente und Politiker
- deutsche und internationale Wirtschaftsunternehmen
- Wissenschafts- und Forschungseinrichtungen

Cyberangriffskampagne APT 28

Bei der Cyberangriffskampagne APT 28, auch bekannt als Fancy Bear, handelt es sich um eine langjährige, international angelegte Angriffsoperation, deren Beginn mindestens bis ins Jahr 2004 zurückreicht. Auch der Cyberangriff auf das interne Kommunikationsnetzwerk des Deutschen Bundestages, der Anfang Mai 2015 aufgedeckt werden konnte, wird dieser Kampagne zugerechnet.

APT (advanced persistend threat)

Fortgeschrittene andauernde Bedrohung.

Hiermit wird ein komplexer, zielgerichteter und effektiver Angriff auf kritische IT-Infrastruktur oder vertrauliche Daten beschrieben. APTs erfolgen nach langer Vorbereitung und Anpassung an das Opfer. Zumeist ist das Ziel, sich möglichst lange unentdeckt im Opfersystem zu bewegen, um so möglichst viele Daten abzugreifen.

Vermutlich wird APT 28 durch russische staatliche Stellen gesteuert. Hierfür spricht insbesondere die bisherige „Opferauswahl“ bzw. das dahinter stehende Aufklärungsinteresse. Neben Strukturen der NATO, der OSZE sowie westlichen Verteidigungs- und Außenministerien waren auch kaukasische Behörden und russische Oppositionelle Opfer der Kampagne. Technische Übereinstimmungen und Parameter, wie z. B. Spracheinstellungen und Zugriffszeiten der Angreifer auf Opfersysteme, weisen ebenfalls auf einen russischen Ursprung hin.

Im Mai 2016 wurden erstmals gezielte Angriffsversuche gegen Parteistrukturen und Stiftungen in Deutschland bekannt, die APT 28 zugerechnet werden. Dabei wurde insbesondere mit Spear-Phishing-Angriffen operiert.

Angriffsmethode Phishing

Beim **Phishing** versuchen Angreifer über gefälschte oder kompromittierte Webseiten, E-Mails oder Nachrichten an Benutzerinformationen zu gelangen. Dabei geht es vor allem um das Abschöpfen von Passwörtern und Zugangsdaten. Phishing-Mails können allgemein an eine Vielzahl von Nutzern geschickt werden oder zielgerichtet an einzelne Personen. In solchen Fällen spricht man von Spear-Phishing.

Spear-Phishing-Mails sind also personalisiert und richten sich beispielweise an Mitarbeiter von Unternehmen, aus denen der Angreifer Daten entwenden möchte. Es werden persönlich zugeschnittene E-Mails von einer vermeintlich vertrauenswürdigen Quelle an die Opfer geschickt. Die Inhalte der Mails sind gut recherchiert und enthalten teilweise Insiderwissen. Dies verdeutlicht, dass die Angreifer professionelles Social Engineering betreiben, sich also zuvor intensiv mit dem Umfeld des Opfers auseinandersetzen. Die E-Mails enthalten infizierte Links oder Schadanhänge.

Credential-Phishing beschreibt eine spezielle Form des Spear-Phishing, bei dem gezielt Zugangsdaten, sogenannte Credentials, abgeschöpft werden sollen. Das Vorgehen bei derartigen Angriffen ist meist ähnlich: Dem Opfer wird eine Anmeldeseite vorgetäuscht, die der Angreifer auf einem eigens hierfür angelegten Server hinterlegt hat. In der Annahme, dies sei die legitime Seite, gibt der Nutzer beispielsweise die Anmeldedaten für sein Mailpostfach ein, die dann von den Angreifern abgegriffen und missbräuchlich weiterverwendet werden. Der Unterschied zum legitimen Server wird dem Anwender kaum auffallen.

Attacken mit Bezug zu ATP 28

MAI 2016

ANGRIFFSVERSUCHE GEGEN DAS NETZ DER CHRISTLICH DEMOKRATISCHEN UNION DEUTSCHLANDS (CDU)

Bei Analysen zu APT 28 waren Domains aufgefallen, die wahrscheinlich exklusiv für Phishing-Angriffe gegen Mitarbeiter und Abgeordnete der CDU angelegt worden waren. Die Angriffe waren nicht erfolgreich, da die Domains frühzeitig blockiert wurden.
Andernfalls wären wahrscheinlich alle E-Mails aus den Postfächern kopiert und ausgeleitet worden.

AUGUST 2016

SPEAR-PHISHING-ANGRIFFSWELLE GEGEN DEN DEUTSCHEN BUNDESTAG UND MEHRERE POLITISCHE PARTEIEN

Versendet wurde eine E-Mail mit maliziösem Link von einer gefälschten E-Mail-Adresse der NATO. Der Angriff erfolgte in drei Wellen. In den ersten beiden Wellen wurde ein malizöser Hyperlink eingesetzt. In einer dritten Angriffswelle wurde ein gefälschter Absender des EU-Parlaments verwendet und ein mit Schadcode infiziertes Word-Dokument angehängt.

FEBRUAR 2017

ANGRIFFSVORBEREITUNGEN EINER SPEAR-PHISHING-KAMPAGNE GEGEN DIE CDU

Hinweise deuteten auf die Vorbereitung einer Spear-Phishing-Kampagne gegen die CDU hin. Hierfür wurde eine legitime Seite der CDU extra für geplante Phishing-Angriffe imitiert. Soweit technisch verfolgbar fanden nur Angriffsvorbereitungen statt, Spear-Phishing-Mails wurden nicht bekannt.

MÄRZ 2017

SPEAR-PHISHING-ANGRIFF AUF DIE KONRAD-ADENAUER-STIFTUNG (KAS)

Am 8. März wurde das Netzwerk der CDU-nahen Konrad-Adenauer-Stiftung mit einer Spear-Phishing-Mail angegriffen. Die Domain mit einer nachgestellten Login-Seite, von der der Angriff ausging, war mutmaßlich allein zu diesem Zweck angelegt worden.

CREDENTIAL-PHISHING-ANGRIFF AUF DIE FRIEDRICH-EBERT-STIFTUNG (FES)

Am 31. März wurde die SPD-nahe Friedrich-Ebert-Stiftung (FES) Opfer eines Credential-Phishing-Angriffs. Die Phishing-Mails erweckten den Anschein von der IT-Abteilung der FES zu stammen. Die Opfer wurden – nach dem üblichen Schema – aus angeblichen Sicherheitsgründen aufgefordert, ihre Webmail-Zugangsdaten in das Login-Fenster einzugeben.

Auch internationale Einrichtungen gerieten in der Vergangenheit wiederholt ins Visier von APT 28. Ende 2016 war eine äußerst breit angelegte Spear-Phishing-Kampagne von APT 28 zu verzeichnen, die in mehreren Wellen verlief und sich v. a. gegen diplomatische Vertretungen und andere Regierungseinrichtungen weltweit richtete. In den einzelnen Angriffswellen kamen unterschiedlich gestaltete Phishing-E-Mails und Angriffsmethoden zum Einsatz.

Der Angreifer nutzte dabei Zero-Day-Exploits. Das Ausmaß war selbst für die sehr aktive Cyberoperation APT 28 außergewöhnlich. Auslöser der Aktion könnte die kurz zuvor erfolgte Bekanntgabe der genannten Sicherheitslücken gewesen sein. Vermutlich wollten die Angreifer die Lücken noch kurzfristig ausnutzen, bevor sie von den Software-Herstellern geschlossen wurden.

Zero-Day-Exploits

Hiermit ist ein Angriff gemeint, der eine dem Hersteller bislang unbekannte Sicherheitslücke in der Software (z. B. im Flash Player von Adobe oder in Windows-Betriebssystemen) nutzt.

Seit dem militärischen Engagement Russlands im syrischen Bürgerkrieg ist eine Intensivierung von APT 28-Angriffen in Jordanien, Syrien und Irak festzustellen. Es waren jedoch auch Außen- und Verteidigungsministerien in westlichen Staaten betroffen.

Ein weiterer schwerwiegender Angriff wurde Ende Oktober 2016 auf das interne Netz der OSZE festgestellt. Dem Angreifer war es über einen längeren Zeitraum gelungen, in großem Umfang Daten aus dem Netzwerk auszuleiten.

Cyberangriff auf die Welt-Anti-Doping-Agentur (WADA)

Auch bei einem Angriff auf die Athletendatenbank der Welt-Anti-Doping-Agentur (WADA) lassen sich Bezüge zu APT 28 herstellen. Im September 2016 veröffentlichte eine Gruppierung mit der Bezeichnung „Fancy Bears' Hack Team" auf der Webseite fancy-bear.net medizinische Daten prominenter Sportler aus den USA. Später erfolgten weitere entsprechende Veröffentlichungen zu Sportlern aus Großbritannien, Dänemark, Polen, Tschechien, Rumänien sowie Deutschland.

Die betreffenden Sportler verfügen über eine medizinische Ausnahmegenehmigung der WADA oder ihrer nationalen Anti-Doping-Agentur, die es ihnen erlaubt, zur Behandlung akuter oder chronischer Erkrankungen eigentlich verbotene Medikamente einzunehmen und dennoch Wettkämpfe zu bestreiten.

Der Angriff und die Veröffentlichungen erfolgten genau zu dem Zeitpunkt, als eine Reihe russischer Sportler wegen systematischer Dopingvergehen ihres Verbandes von der Teilnahme an den Olympischen Spielen in Rio de Janeiro ausgeschlossen worden waren.

Die Veröffentlichung der gehackten Daten zielte offenbar auf die Diskreditierung der WADA und der betroffenen Athleten ab. Die Domains, die für den Angriff verwendet wurden, weisen starke Überschneidungen zu bereits bekannter APT 28-Angriffsinfrastruktur auf. Angesichts des angespannten Verhältnisses Russlands zur WADA bestehen hier Anhaltspunkte für eine False-Flag-Operation der APT 28-Kampagne.

False-Flag-Operationen

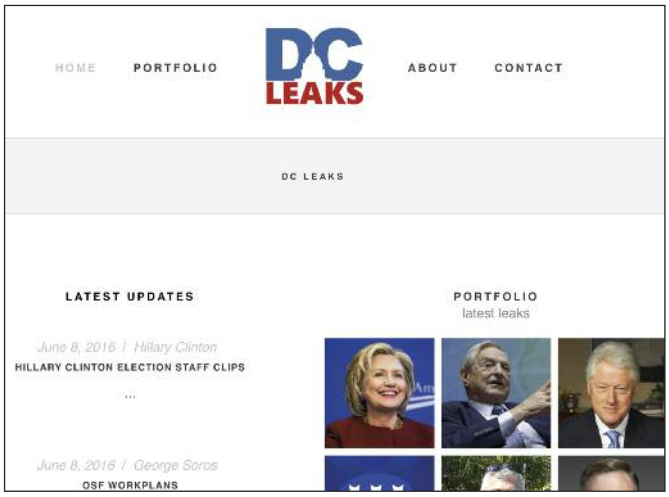
Bereits 2015 konnten Operationen unter „falscher Flagge“ innerhalb der APT 28-Angriffskampagne festgestellt werden.

Die False-Flag-Operationen bilden einen Modus Operandi, der bislang nicht bei anderen russischen Angriffskampagnen beobachtet wurde und der dementsprechend ein Alleinstellungskriterium von APT 28 darstellt.

Russische Nachrichtendienste verüben in diesen Fällen Cyberangriffe unter dem Deckmantel vermeintlicher Hacktivistengruppen. Solche Operationen stellen mitunter eine Ergänzung der Spionage um Sabotage und deren Flankierung mit gezielten Desinformationskampagnen und Propaganda dar.

„Guccifer 2.0“ und der DNC-Hack

Eine besonders weitreichende False-Flag-Operation bildete der Cyberangriff auf das Netzwerk des US-amerikanischen Democratic National Committee (DNC), der Verwaltungsorganisation der Demokratischen Partei der Vereinigten Staaten. Sie wurde von dem bis dahin unbekannten Pseudonym „Guccifer 2.0“ verübt, das von Sicherheitsbehörden und IT-Sicherheitsunternehmen als eine False-Flag-Operation von APT 28 angesehen wird. Unter dem Namen „Guccifer 2.0“ bekannte sich ein angeblicher Hacker im Juni 2016 zu einem Cyberangriff, bei dem es zu einem Datendiebstahl im Netzwerk des DNC kam.



„Guccifer 2.0“ gab in seinem Blog an, einen Großteil der entwendeten Daten an WikiLeaks übermittelt zu haben. Am 22. Juli, drei Tage vor dem Nominierungsparteitag der US-Demokraten, wurden über 19.000 interne E-Mails des DNC auf WikiLeaks veröffentlicht, diese enthielten u. a. Angaben zu Personen, die an die Demokratische Partei gespendet hatten sowie interne Finanzberichte der Partei.

Die Untersuchung des Vorfalls ergab Hinweise auf die russischen Angriffskampagnen APT 28 und APT 29 als Urheber. Die Aktivitäten von „Guccifer 2.0“ wurden dabei als mögliche russische Desinformationskampagne gewertet, die den Präsidentschaftswahlkampf zugunsten des republikanischen Spitzenkandidaten Trump beeinflussen sollte.

Auch der französische Präsidentschaftskandidat Macron hat Cyberangriffe auf sein Wahlkampfteam beklagt, die dortigen Untersuchungen zufolge von russischen Stellen ausgegangen sein sollen.

Zusammenfassend ist festzuhalten, dass APT 28 nach wie vor eine der umfangreichsten und gefährlichsten Kampagnen im Cyberraum darstellt. Das Bedrohungspotenzial – auch für deutsche Stellen in Verwaltung, Wirtschaft, Wissenschaft und Forschung – ist hoch. Entsprechend begegnet das Bundesamt für Verfassungsschutz (BfV) dieser sehr aktiven Angriffskampagne mit dem ganzen Spektrum nachrichtendienstlicher Informationsgewinnung sowohl zur Täteraufklärung als auch zur Gefahrenfrüherkennung.

Cyberangriffskampagne APT 29

Bei APT 29, auch bekannt als Cozy Bear, handelt es sich um eine russischen staatlichen Stellen zuzuordnende Angriffskampagne. Sie zielt vorwiegend auf folgende Bereiche ab:

- Verwaltung
- Verteidigung
- Energie
- Finanzen
- Think-Tanks
- NGOs
- Forschung und Entwicklung

APT 29 ist eine seit mindestens 2008 aktive, technisch sehr aufwendig und komplex gestaltete Cyberoperation, welche eine Reihe von Zero-Day-Schwachstellen ausnutzt und dabei die eingesetzte Schadsoftware im Laufe der Zeit mehrfach modifiziert hat.

Öffentliche Aufmerksamkeit erlangte die Kampagne zuletzt im Rahmen des Mitte Juni 2016 bekannt gewordenen Cyberangriffs auf das DNC, an dem neben APT 28 auch APT 29 beteiligt war. Im Gegensatz zum APT 28-Angreifer, der sich erst seit April 2016 im DNC-Netzwerk befunden hatte, war die Infiltration durch APT 29 wohl bereits Mitte 2015 erfolgt.

Unmittelbar nach den amerikanischen Präsidentschaftswahlen am 9. November 2016 kam es zu breit angelegten Spear-Phishing-Angriffen in mehreren Wellen. Sie richteten sich vor allem gegen amerikanische Think-Tanks, Universitäten, Journalisten und NGOs. So gab eine der versandten Angriffs-E-Mails vor, von der Clinton Foundation zu stammen und im angehängten Doku-

ment Informationen über die wahren Hintergründe des Ablaufs der US-Präsidentschaftswahlen zu enthalten.

Der Kampagne APT 29 wird u. a. ein Angriff auf das Bundestagsbüro einer Politikerin der Grünen sowie auf eine NGO in Deutschland zugerechnet. Die Aktivitäten dieser hoch spezialisierten Cyberangriffskampagne verdichten sich seit Mitte 2016 deutlich.

Cyberangriffskampagne Snake

Bei der Angriffskampagne Snake, auch bekannt als Uroburos oder Turla, handelt es sich um eine geheim angelegte Cyberspionageoperation mit internationalem Ausmaß, die bis 2005 zurückverfolgt werden kann. Von einer staatlichen Lenkung – vermutlich unter der Verantwortung des FSB – ist auszugehen. Für die Zuordnung zu russischen Stellen bedeutsam ist neben technischen Parametern insbesondere der erkennbare Fokus auf Staaten der ehemaligen Sowjetunion und des ehemaligen Warschauer Paktes sowie Staaten im Nahen Osten. Darüber hinaus bestehen Parallelen zu anderen, ebenfalls Russland zuzuordnenden Kampagnen.

Einen Aufklärungsschwerpunkt von Snake bilden Regierungseinrichtungen wie Außenministerien und diplomatische Vertretungen, Innenministerien oder Telekommunikationsministerien. Die Zielauswahl des Angreifers zeigt allerdings auch ein Interesse an Entwicklungen in Wirtschaft und Forschung, insbesondere in den Bereichen

- Energietechnik,
- Röntgen- und Nukleartechnologie,
- Messtechnologie sowie
- Luft- und Raumfahrt.

Zu den betroffenen deutschen Zielen gehörten bislang Botschaften in Westeuropa, mehrere Schulen und Hochschulen, aber auch Forschungsinstitute.

Angriff auf RUAG Holding AG

Anfang Mai 2016 berichteten schweizerische Medien über einen erfolgreichen Cyberangriff auf den Berner Rüstungs- und Technologiekonzern RUAG Holding AG. Höchstwahrscheinlich als Folge einer Watering-Hole-Attacke mit einer der Kampagne Snake zuzuordnenden Schadsoftware konnte der Angreifer ein erhebliches Datenvolumen ausleiten.

Angriffsmethode Watering-Holes

Bei Watering-Holes handelt es sich um legitime Webseiten, die mit Schadsoftware infiziert wurden. Die Infizierung ist meist durch unbekannte Sicherheitslücken, so genannte Zero-Day-Schwachstellen, möglich. Watering-Holes können als Attacke gegen Unternehmen oder Institutionen verwendet werden, indem z. B. gezielt häufig genutzte Websites der betreffenden Opfer infiziert werden.

Der Angreifer konnte sich mehrere Monate lang unbemerkt im Datennetz des Konzerns bewegen und dieses weitgehend unter seine Kontrolle bringen.

Insgesamt erfolgen die festgestellten Angriffe der Kampagne Snake extrem zielgerichtet. Die jeweiligen Opfer werden passgenau ausgewählt und angegriffen, wie auch der RUAG-Vorfall exemplarisch belegt. Von einem entsprechend hohen Schadpotenzial ist auszugehen. Es handelt sich um eine fortdauernde Angriffsoperation, von der nach wie vor eine hohe Gefahr für deutsche Opfer in Regierung und Verwaltung, Wirtschaft, Wissenschaft und Forschung ausgeht.

Chinesische Cyberangriffskampagnen

Methoden und Ziele

Die Möglichkeit zur Durchführung längerfristiger und strategisch angelegter Spionageangriffe im Cyberbereich gehört zum Fähigkeitenportfolio chinesischer Nachrichtendienste. Die dortigen Kapazitäten umfassen nicht nur die Möglichkeit, komplexe, international angelegte Angriffe zielgerichtet durchzuführen, sondern diese auch parallel mit einer Vielzahl von einzelnen Opfern zu betreiben. Im Fokus stehen sowohl die deutsche Wirtschaft als auch Regierungs- und Verwaltungseinrichtungen.

Das eigene Erkenntnisaufkommen sowie öffentlich bekannte chinesische Spionagekampagnen mit Richtung Deutschland bzw. Westeuropa offenbaren ein umfassendes Interesse in den Bereichen

- Verwaltung und Regierung,
- Militär und Rüstung,
- Luft- und Raumfahrt,
- Elektronik und Elektrotechnik,
- Stahl- und Metallindustrie sowie
- Hochtechnologie.

Nachrichtendienstlich initiierte und gesteuerte Kampagnen zur Informationsgewinnung stellen aufgrund ihrer Qualität und ihres Umfangs eine erhebliche Gefahr für den Erfolg und die Entwicklungsmöglichkeiten deutscher Unternehmen und Forschungsinstitutionen dar.

Aber auch Behörden und Regierungsinstitutionen bilden einen Schwerpunkt im Bereich chinesischer An-

griffskampagnen. Ziel der Angreifer ist hier regelmäßig die Aufklärung außen-, sicherheits- und wirtschaftspolitischer Standpunkte, Einschätzungen und Handlungsoptionen, um dadurch eine entsprechende Informationslage der Volksrepublik China sicherzustellen.

Akteure und Vorgehen

Die Bandbreite chinesischer Cybergruppierungen reicht von kriminellen Strukturen über sogenannte patriotische Hacker bis hin zu Unternehmern, Regierungs- und Militärakteuren. Die Interessen und Ziele der einzelnen Gruppierungen überschneiden sich, so dass eine konkrete Zuschreibung teilweise schwierig ist.

Die Kampagnen werden meist über mehrere Jahre fortgeführt. Folgende technische Charakteristika sind dabei typisch:

- Schwer zu detektierendes Vorgehen bei der Zustellung der Malware, der Netzwerkinfiltration, -erkundung und -ausbreitung sowie der Datenausleitung.
- Die Fähigkeit, innerhalb weniger Stunden vom eingeschränkten Zugriff auf ein Netzwerksegment einen vollumfänglichen Zugriff auf das gesamte (Unternehmens-) Netzwerk zu erlangen.
- Etablierung möglichst vielfältiger Zugangsmöglichkeiten zum infiltrierten Netzwerk, um die Verbindung zum System auch bei Gegenmaßnahmen des Opfers lange aufrecht zu erhalten.

- Kombination von gezielten Spear-Phishing-E-Mails und Massenversand von E-Mails, um eine Verschleierung der echten Ziele zu erreichen.
- Sofortige Ausnutzung von bekannt gewordenen und bisher nicht angegriffenen Schwachstellen mittels Zero-Day-Exploits. So wurde im Juli 2015 bei WikiLeaks eine bislang unbekannte Sicherheitslücke veröffentlicht. Bereits wenige Tage danach wurde diese Schwachstelle von mutmaßlich chinesischen Stellen dazu ausgenutzt, um deutsche Wirtschaftsunternehmen anzugreifen.
- Verwischen von „digitalen Spuren“, um eine forensische Analyse von Vorfällen zu erschweren oder unmöglich zu machen.
- Vorgehen nach dem sogenannten „Staubsaugerprinzip“. Dabei werden alle verfügbaren Daten ohne vorweggenommene Selektion extrahiert.

Auch wenn Angriffe sich nicht explizit gegen deutsche Ziele richten, wird Deutschland teilweise als Standort für die Bereitstellung von Infrastruktur zur Durchführung von Cyberangriffen genutzt.

Cyberangriffskampagne APT 3

Im Juni 2015 richtete sich eine Spear-Phishing-Kampagne, die APT 3 zugeordnet wird, gegen deutsche Unternehmen, unter anderem ein global operierendes Technologieunternehmen.

Die verschickten Phishing-E-Mails mit maliziösem Link wurden dabei so präpariert, dass der Link nur bei erstmaligem Anklicken funktionierte. Dies erschwerte eine forensische Analyse und diente allein dem Zweck, den Nachweis des Angriffs und dessen Rückverfolgung zu erschweren. Einige der angegriffenen E-Mail-Adressen waren nicht offen verfügbar.

Dies lässt auf einen gezielt ausgewählten Empfängerkreis und ggf. das Vorliegen von Insiderwissen schließen.

Die Nutzung von Schadsoftware wie PIRPI, CookieCutter, PlugX sowie der Einsatz des Scanbox-Frameworks sprechen in diesem Fall für einen Akteur aus China. Ebenso deuten Schwachstellen, die auch von anderen chinesischen APT-Gruppierungen genutzt werden, sowie der Umstand, dass Teile der Infrastruktur in der China lokalisiert wurden, auf eine entsprechende Zuordnung hin. Sicherheitsbehörden und IT-Sicherheitsunternehmen gehen aufgrund der vorliegenden Erkenntnisse von einem staatlich gesteuerten chinesischen Hintergrund aus, was auch die hinter dem Angriff stehende Interessenlage bekräftigt. Das Vorgehen erfolgte zielgerichtet und fokussiert. Es ist somit eine Abkehr vom „Staubsaugerprinzip“ wahrzunehmen.

Cyberangriffskampagne APT 10

Die mutmaßlich chinesische Kampagne APT 10, die u. a. auch als Menupass Team und Stone Panda bekannt ist, wird mit Cyberangriffen auf IT-Dienstleister und Wirtschaftsunternehmen in Verbindung gebracht. Die Angriffe stellen eine hohe Bedrohung für betroffene Unternehmen und deren Kunden dar.

Zwar ist APT 10 mindestens seit dem Jahr 2009 aktiv, ihre Angriffe richteten sich in der Vergangenheit allerdings vorrangig gegen US-amerikanische und japanische Ziele. Erst seit Ende 2016 scheint sich der Interessenfokus auf Wirtschaftsunternehmen in Europa erweitert zu haben.

APT 10 hat neben dem Hochtechnologie-Bereich Aufklärungsinteresse an:

- Energie
- Transport und Verkehr
- Rohstoffen
- Chemie
- Gesundheit
- Telekommunikation
- Luft- und Raumfahrt

Ausgangspunkt der Cyberangriffe sind in der Regel Spear-Phishing-Mails. Als Schadsoftware kommt im Anschluss häufig PlugX, auch als DestroyRAT bekannt, zum Einsatz. Daneben nutzt die Angreifergruppierung APT 10 seit Ende 2016 anscheinend exklusiv eine Schadsoftware mit dem Namen ChChes.

Derzeit richten sich die Cyberangriffe der Gruppe gezielt gegen IT Service Provider, vor allem Cloud-Dienstleister, um von dort aus in die oft besser geschützten Systeme der Kunden zu gelangen. Das Vorgehen wird als „Operation Cloud Hopper“ bezeichnet.

Betroffen waren bisher vor allem Unternehmen in den USA, Japan, Großbritannien und Indien.

Iranische Cyberangriffskampagnen

Methoden und Ziele

Die iranischen Cyberfähigkeiten wurden maßgeblich ausgebaut. Grund dafür ist unter anderem der Stuxnet-Schock des Jahres 2010, bei dem gezielt Steuerungssysteme des iranischen Atomprogramms angegriffen wurden, mit der Absicht dieses lahmzulegen. Auch die Nutzung internetbasierter Kommunikationsmittel durch oppositionelle Bewegungen bei den Präsidentenwahlen 2009 förderte diese Entwicklung.

Aufklärungsinteresse

Das iranische Regime setzt seine Cyberkapazitäten mit verschiedenen Zielrichtungen ein. Einerseits soll durch die Kontrolle internetgebundener Kommunikationsmedien den Gefahren für die öffentliche Sicherheit begegnet werden. Darüber hinaus ist der Iran bemüht, die eigene IT-Infrastruktur besser vor Cyberangriffen zu schützen. Die Cyberkapazitäten werden jedoch auch offensiv zur Spionage und für Sabotageaktivitäten im Ausland genutzt. Letztere setzt der Iran gezielt ein, um sich als ernstzunehmender Cyberakteur zu profilieren. Zu den Hauptzielen gehören vorwiegend die ideologischen Gegner Israel, USA und Saudi-Arabien.

Um Opfersysteme mit Schadsoftware zu infizieren, setzen iranische Cyberakteure gängige Angriffsvektoren wie Spear-Phishing E-Mails und Watering-Hole-Seiten ein. Die Auswahl der Werkzeuge und die Ausnutzung bekannter Schwachstellen von Soft- und Hardware er-

folgt auch im Iran zweckmäßig und zielgerichtet, häufig durch Anwendung öffentlich bekannter Hacking-Tools.

Cyberangriffskampagne OP Cleaver

OP Cleaver ist eine der derzeit aktivsten iranischen Cyberkampagnen. Die Gruppe ist auch unter der Alias-Bezeichnung Oilrig bekannt und weist Verbindungen zu weiteren offensiven Cyberaktivitäten auf, die iranischen staatlichen Stellen zugeschrieben werden. OP Cleaver ist mindestens seit dem Jahr 2014 aktiv. Die Angreifer weisen sehr vielfältige Operationsziele auf. Zu den Opfern gehören z. B. Unternehmen aus der Rüstungsindustrie mit Schwerpunkt Luft- und Raumfahrt. Darüber hinaus greift die Gruppe in jüngerer Zeit vermehrt Regierungseinrichtungen im Nahen Osten an.

Berichte von IT-Sicherheitsunternehmen bezüglich Überschneidungen in der genutzten Infrastruktur mit den in den Kampagnen Cadelle/Chafer sowie Shamoon weisen auf einen möglichen gemeinsamen Urheber dieser Kampagnen hin. Zu den bekannten Zielen von Cadelle/Chafer gehören vorwiegend Unternehmen aus den Sektoren Telekommunikation und Transport. Die Gruppe Shamoon wird hingegen mit Sabotage-Operationen gegen Saudi-Arabien in Verbindung gebracht. Bei einem Vorfall im Jahr 2012 soll Shamoon im Rahmen einer Infiltration des Computernetzwerks der saudischen Ölfirma Saudi Aramco großflächig Festplatten der im Netzwerk verbundenen Server und Clients gelöscht haben. Seit 2016 werden erneute Aktivitäten der Gruppe vor allem im Nahen Osten registriert. Die Gruppe zeichnet sich insbesondere durch Nutzung der Schadsoftware Wiper aus.

Cyberangriffskampagne Copy Kitten

Die Gruppe Copy Kitten ist seit mindestens 2014 aktiv. In einer Angriffswelle von September 2016 bis Januar 2017 versuchte die Gruppe Regierungseinrichtungen in Israel, im Nahen Osten sowie teilweise auch in westeuropäischen Staaten anzugreifen. Die Angreifer nutzen sowohl Spear-Phishing als auch Watering-Holes als Angriffsvektoren. Der breiteren Öffentlichkeit bekannt wurde eine Watering-Hole-Attacke auf das Netzwerk des Deutschen Bundestags. Hierbei wurden schadhafte Verbindungen bei Seitenaufrufen eines verseuchten Links auf der Webseite der israelischen Zeitung Jerusalem Post festgestellt.

Cyberangriffskampagne Rocket Kitten

Die Gruppierung Rocket Kitten hatte einen Aktivitätsschwerpunkt in den Jahren 2014 und 2015. Die Gruppe nutzt einen kombinierten Ansatz aus konventionellen Spear-Phishing-Angriffen und einem aggressiven, teilweise ausgefeilten Social Engineering. Hierbei versuchten die Angreifer, ihre Opfer zur Preisgabe von privaten Zugangsdaten zu E-Mail-Postfächern sowie zu Konten in sozialen Netzwerken auf gefälschten Login-Seiten zu bewegen. Die Angreifer kontaktierten hierzu ihre Opfer teilweise telefonisch. Betroffen waren vorwiegend Personen aus dem Nahen Osten und Israel. Im Jahr 2015 konnte durch operative Fehler der Angreifer ein Akteur der Gruppe identifiziert werden. Aufgrund der vorliegenden Erkenntnisse wird vermutet, dass die Iranischen Revolutionsgarden für die Angriffe der Rocket Kitten-Gruppe verantwortlich sind.

Bewertung

Russisches Bedrohungspotenzial

Bei der Analyse staatlich gesteuerter Cyberangriffe aus Russland zeigt sich deutlich die hohe informationstechnische Qualität der Angriffsoperationen, z. B. durch Ausnutzung noch unbekannter Sicherheitslücken. Sichtbar wird auch die Finanzstärke der Täter. Zudem lassen Art und globaler Umfang der Operationen immense Operativ- und Auswertekapazitäten erkennen. Offensichtlich ist Russland in der Lage, auf außenpolitische Kräfteverschiebungen und auf „störend“ empfundene Ereignisse kurzfristig zu reagieren. Dabei wird auch vor Sabotageakten nicht zurückgeschreckt.

Die festgestellten Angriffe erfolgen meist sehr zielgerichtet und passgenau. Die Erfolgswahrscheinlichkeit und damit das Schadpotenzial russischer Angriffe erscheint aufgrund des erkennbar hohen Ressourcenansatzes, der Hochwertigkeit der Ziele, der herausgehobenen technischen Fähigkeiten und des guten Social Engineerings hoch.

Chinesisches Bedrohungspotenzial

Der Rückgang der mutmaßlich chinesischen APT-Angriffe auf westliche Ziele in den letzten Jahren war international sichtbar. Die Aufdeckung der „Operation Cloud Hopper“ in der jüngsten Vergangenheit zeigt je-

doch, dass chinesische APT-Gruppen noch immer aktiv Cyberspionage betreiben. Dabei ist ein immer anspruchsvolleres Vorgehen erkennbar, was die Detektion derartiger Cyberangriffe erschwert.

Waren die Cyberangriffe mutmaßlich chinesischen Ursprungs bis zum Jahr 2016 in Deutschland rückläufig, konnte allerdings zuletzt eine Zunahme sichtbarer Angriffsoperationen verzeichnet werden.

Iranisches Bedrohungspotenzial

Das Gefährdungspotenzial iranischer Cyberangriffe hat sich in den letzten Jahren signifikant erhöht. Politische Ereignisse, wie der erfolgreiche Abschluss des Abkommens über das iranische Nuklearprogramm im Rahmen der 5+1-Verhandlungen könnten als Indizien für eine Art politisches „Tauwetter“ und ein damit einhergehendes künftig vermindertes Gefährdungspotential verstanden werden. Gegen eine solche Einschätzung sprechen allerdings folgende Faktoren:

- Wegen des politischen „Tauwetters“ werden Echtweltaktionen z. B. gegen Oppositionelle im Ausland aufgrund der zu befürchtenden politischen Kollateralschäden erheblich riskanter. Cyberangriffe könnten hier eine leicht abzustreitende und anonyme Alternative bieten.
- Die Aufnahme von ausländischen Wirtschaftskontakten ist trotz der Auflockerung der Sanktionen weiterhin zurückhaltend, sodass Cyberoperationen alternativ als eine Form der „vertragsfernen“ Beschaffung von Knowhow zielführend eingesetzt werden könnten.

Das Potenzial zur Durchführung von Cyberangriffen im Iran wird perspektivisch durch die Fokussierung auf Cyber-Themen im iranischen Bildungssystem und den privilegierten Zugriff auf diese Ressourcen durch staatliche Stellen erheblich zunehmen.

Impressum

Herausgeber
Bundesamt für Verfassungsschutz
Öffentlichkeitsarbeit
Merianstraße 100
50765 Köln
oeffentlichkeitsarbeit@bfv.bund.de
www.verfassungsschutz.de
Tel.: +49 (0) 221/792-0
Fax: +49 (0) 221/792-2915

Gestaltung und Druck
Bundesamt für Verfassungsschutz
Print- und MedienCenter

Bildnachweis
© sdecoret – Fotolia.com
© Антон Медведев – Fotolia.com
© BirgitKorber – Fotolia.com
© profit_image – Fotolia.com
© Maksim Kabakou – Fotolia.com
© picture alliance / chromorange
© picture alliance / chromorange
© picture alliance / dpa
© dpa
© picture alliance / AP Photo
© picture alliance / AP Photo
© the_lightwriter – Fotolia.com
© Birgit/Korber – Fotolia.com
© Birgit/Korber – Fotolia.com
© BigNazik – Fotolia.com2
© ommbeu – Fotolia.com
© BfV

Stand
Mai 2018

Bundesamt für
Verfassungsschutz

Im Verborgenen Gutes tun!

Sinnvolle und sichere Jobs

im Inlandsnachrichtendienst

Jetzt auf eine von vielen freien Stellen bewerben!

Was wir bieten, wen wir suchen:

www.verfassungsschutz.de/karriere

Weitere Informationen zum Verfassungsschutz finden Sie hier:

www.verfassungsschutz.de