**Spionageabwehr**

**Cyber-Allianz-Zentrum (CAZ)**

**Wirtschaftsschutz**

* **69 Prozent der Industrieunternehmen in Deutschland wurden in den letzten zwei Jahren Opfer von elektronischen Angriffen**
* **Neue Angriffsmethode von chinesischen Nachrichtendiensten: CAZ informiert bayerische Unternehmen**

**Zunahme elektronischer Angriffe**

Einer am 25.04.2016 veröffentlichten Studie des Branchenverbands Bitkom zufolge sind in Deutschland 69 Prozent der Industrieunternehmen in den letzten zwei Jahren Opfer von Datendiebstahl, Wirtschaftsspionage oder Sabotage geworden. Der Schaden für die deutsche Industrie beläuft sich nach Berechnungen der Bitkom auf rund 22,4 Milliarden Euro pro Jahr. Einen großen Teil dieser Summe machen Umsatzverluste durch Plagiate sowie Patentrechtsverletzungen aus. Ins Gewicht fallen zunehmend aber auch Kosten, die durch die Sabotage von IT-Systemen und die damit verbundene Störung der Betriebsabläufe entstehen.

Die sogenannte „vierte industrielle Revolution“ ist durch die unternehmensübergreifende Digitalisierung und Automatisierung von Prozessen gekennzeichnet. Dadurch vermehren sich nicht nur mögliche Ansatzpunkte für Angreifer. Elektronische Angriffe mit dem Ziel der Sabotage können zudem weitreichendere Folgen haben, insofern mit einem Angriff viele Unternehmen zugleich getroffen werden können.

**Orientierung an Methoden und Instrumenten der Cyberkriminalität**

Elektronische Angriffe sind für Nachrichtendienste relativ einfach und kostengünstig zu realisieren, bergen ein geringes Entdeckungsrisiko und haben eine hohe Erfolgswahrscheinlichkeit. Ihre Instrumente passen ausländische Nachrichtendienste immer wieder an aktuelle technische und gesellschaftliche Entwicklungen an, um mit möglichst geringem Aufwand einen maximalen Effekt zu erzielen. In den letzten Monaten war feststellbar, dass ausländische Nachrichtendienste zunehmend Werkzeuge und Angriffsmethoden einsetzen, die aus der Cyberkriminalität bekannt sind, und zwar sowohl mit dem Ziel der Spionage wie auch der Sabotage. Die Werkzeuge der Cyberkriminellen sind bereits technisch entwickelt und damit kostengünstig und tragen zudem mit zur Verschleierung nachrichtendienstlicher Aktivitäten bei, insofern die Angriffsmuster zunächst nicht auf einen nachrichtendienstlichen Hintergrund schließen lassen. Insbesondere die Nachrichtendienste Chinas und Russlands bedienen sich mutmaßlich solcher Praktiken.

**Elektronische Angriffe mit mutmaßlich russischem Hintergrund**

Das Bayerische Landesamt für Verfassungsschutz (BayLfV) hat seit 2015 die sogenannte SOFACY-Gruppe intensiv beobachtet und nachrichtendienstliche Bezüge mit russischem Hintergrund herausgearbeitet. Der Generalbundesanwalt hat daraufhin ein Ermittlungsverfahren gegen die SOFACY-Gruppe eingeleitet und das Bundeskriminalamt beauftragt, Erkenntnisse zu möglichen deutschen Betroffenen zu erarbeiten. Das BayLfV hat im Rahmen seiner Maßnahmen auch Kontakt mit Unternehmen und Hochschulen in Bayern aufgenommen und über die möglichen elektronischen Angriffe informiert. Bei einem der Kontaktierten hat sich der Verdacht eines elektronischen Angriffs konkretisiert. Ob es sich bei den Angreifern tatsächlich um die SOFACY-Gruppe handelt, wird derzeit noch untersucht. Die SOFACY-Gruppe fällt seit 2009 wiederholt durch gezielte Spionageangriffe auf. Opfer waren bislang überwiegend Militärattachés, Verteidigungsministerien, Militärangehörige, Polizeimissionen im Ausland (ISAF, KFOR), Forschungseinrichtungen sowie Rüstungs- und Energieunternehmen.

Das Bedrohungspotential durch Cyber-Angriffe auf kritische Infrastrukturen belegt der mutmaßlich durch einen russischen Hacker-Angriff ausgelöste Stromausfall am 23. Dezember 2015 in der Ukraine. Dies zeigt zugleich die zunehmende Übernahme von Vorgehensweisen aus dem Bereich der Cyberkriminalität in den nachrichtendienstlichen Bereich. Die bei dem Angriff verwendete Schadsoftware wird als „Black Energy“ bezeichnet. Es handelt sich um ein Werkzeug aus der Welt des Cybercrime, das in seiner dritten Versionsvariante hochprofessionell weiterentwickelt wurde und einem russischen Nachrichtendienst zugeschrieben wird.

**Elektronische Angriffe mit mutmaßlich chinesischem Hintergrund**

Hinweise auf eine neue Angriffsmethode, die mutmaßlich von chinesischen Nachrichtendiensten genutzt wird, ergab die Analyse einer verdächtigen E-Mail durch das CAZ beim BayLfV. Beim Anhang dieser E-Mail, einer Datei mit der Endung .rtf, handelte es sich in Wirklichkeit um ein WORD-Dokument mit chinesischem Schadcode, der in zwei Stufen und für Sicherheitssoftware unerkannt zur Wirkung kam. Die Schadsoftware ermöglichte eine Infektion ohne weitergehende Interaktion des Empfängers. In einigen Fällen reichte es bereits aus, die Dokumentenvoransicht zu nutzen, um eine Infektion herbeizuführen. Bayerische Unternehmen wurden durch das CAZ im Rahmen einer Warnmeldung über diesen Angriffsweg sowie geeignete Handlungsempfehlungen informiert.

China hat eine Strukturreform der chinesischen Volksbefreiungsarmee auf den Weg gebracht. Die damit verbundenen Änderungen werden Einfluss auf die Aktivitäten des chinesischen Militärs im Bereich der elektronischen Spionage haben. Durch die bevorstehende Konsolidierung der chinesischen Cyber-Einheiten ist mit einer weiteren Professionalisierung elektronischer Angriffe auf deutsche Unternehmen, Hochschulen und Behörden zu rechnen.

**Information und Prävention**

Das CAZ ist zusammen mit dem Arbeitsbereich Wirtschaftsschutz im Bayerischen Landesamt für Verfassungsschutz Ansprechpartner für Unternehmen, Behörden und Hochschulen bei elektronischen Angriffen. Das Angebot ist kostenfrei, Vertraulichkeit ist garantiert.

Im Rahmen der Präventions- und Öffentlichkeitsarbeit werden neben Gesprächen, Messeauftritten und Vorträgen auch Informationsbroschüren und Flyer eingesetzt. Neu aufgelegt wurden Flyer, die sich an Unternehmensverantwortliche und Mitarbeiter in Wissenschaft und Forschung richten. Die Publikationen beinhalten Empfehlungen zum Know-how-Schutz und sensibilisieren insbesondere auch für notwendige Sicherheitsvorkehrungen bei Geschäfts- und Forschungsreisen ins Ausland.

**Kontakt:**

Cyber-Allianz-Zentrum Bayern (CAZ) im

Bayerischen Landesamt für Verfassungsschutz

caz@lfv.bayern.de

Telefon: 089 31201-222

****