Cyberangriffe nehmen weiter zu – Das Cyber-Allianz-Zentrum Bayern (CAZ) wirkt mit Präventionsarbeit entgegen

- **Seit einem Jahr unterstützt das CAZ Wirtschaft und Wissenschaft bei der Abwehr von Cyberangriffen – eine Bilanz**
- **In Kooperation mit den Industrie- und Handelskammern sensibilisierte das CAZ Unternehmensverantwortliche in ganz Bayern für die Gefahren durch Cyberspionage**
- **Der Konflikt zwischen Russland und der Ukraine führt zu vermehrten Spionageaktivitäten**

Ein Jahr Cyber-Allianz-Zentrum Bayern (CAZ)

Laut einer aktuellen Studie ist Deutschland von elektronischen Angriffen auf die Wirtschaft weltweit am stärksten betroffen: 1,6% des Bruttoinlandsprodukts macht der Schaden durch elektronische Angriffe auf Unternehmen in Deutschland aus. Dies entspricht fast 44 Milliarden Euro. Um den Wohlstand Deutschlands und Bayerns, der wesentlich auf dem Rohstoff Geist und der Innovationskraft der Unternehmen beruht, nicht zu gefährden, ist deshalb ein wirksamer Schutz gegen elektronische Angriffe notwendig.

Am Bayerischen Landesamt für Verfassungsschutz wurde deshalb zum 1. Juli 2013 das CAZ eingerichtet. Das CAZ unterstützt bayerische Unternehmen und Betreiber Kritischer Infrastruktur (KRITIS) als zentraler Ansprechpartner und Kompetenzzentrum bei der Prävention und Abwehr von Bedrohungen aus dem Netz. Seit seiner Einrichtung hat es rund 120 Kontaktaufnahmen bayerischer Unternehmen bearbeitet, aus denen sich 27 Fallkomplexe von elektronischen Angriffen ergeben haben. Die Analyse führt teilweise zu sehr komplexen Sachverhalten, die einen hohen Arbeitsaufwand notwendig machten. Die Bearbeitung gliedert sich dabei in drei Säulen:

- forensisch-technische Analyse
- nachrichtendienstliche Bewertung
- Kommunikation und Netzwerkbildung

Von der Wirtschaft gemeldete Vorfälle, bei denen es Anhaltspunkte für einen gezielten Angriff gibt, werden zunächst aus forensisch-technischer Sicht bewertet. Gleiches gilt für gezielte Angriffe auf staatliche Stellen, die ebenfalls im CAZ analysiert werden. Die technischen Ergebnisse der Analysen fließen weiter in die zweite Säule des CAZ, in der eine nachrichtendienstliche Bewertung stattfindet. Hier werden alle vorliegenden Informationen zu den Angriffen einer nichttechnischen, nachrichtendienstlichen Betrachtung unterzogen und mit bestehenden Erkenntnissen der Nachrichtendienste zu Angriffsvektoren abgeglichen. Die gewonnenen Informationen können unter vollständiger Wahrung der Vertraulichkeit genutzt werden, um weiteren Schaden für das betroffene und andere Unternehmen zu verhindern.

In einem konkreten Fall stellte sich dieser Arbeitsprozess, der insgesamt rund 1.000 Arbeitsstunden umfasste, folgendermaßen dar:

> Der Angreifer verschaffte sich mehrere Benutzerkennungen für den mobilen Zugriff auf den Firmenserver. Damit konnte er im internen Rechnernetz des Unternehmens agieren. Die IT-Abteilung des Unternehmens bemerkte den unberechtigten Zugriff und setzte den Sicherheitsbeauftragten darüber in Kenntnis. Dieser informierte das CAZ.

Durch die forensisch-technische Analyse, in die weitere Behörden wie das Bundesamt für Verfassungsschutz (BfV) eingebunden waren, wurden Schadprogramme und Angriffsvektoren analysiert. Zudem konnten Rückschlüsse auf die vom Angreifer verwendete technische Infrastruktur gezogen und Hinweise auf weitere erfolgreich ausgeführte Angriffe gefunden werden.

Die nachrichtendienstliche Bewertung ergab, dass neben dem betroffenen Unternehmen weitere Konkurrenten und Partner sowie Unternehmen anderer Branchen im Fokus des Angreifers standen. Die Ergebnisse deuteten auf einen iranischen Hintergrund des Angreifers hin.

Die technischen Informationen zu dem Angriff gab das CAZ in anonymisierter Form an Unternehmen mehrerer potenziell betroffener Branchen weiter. Diese wurden dadurch in die Lage versetzt, geeignete Schutzmaßnahmen zu ergreifen. Zudem werden sie dazu motiviert, bei eigener Betroffenheit den Vorfall ebenfalls an das CAZ zu melden, um damit möglichst vielen Unternehmen einen effektiven Schutz vor elektronischen Angriffen zu ermöglichen.

Drei wesentliche Anliegen der Wirtschaft waren bei der Einrichtung des CAZ maßgeblich:

1. **Klare Organisation:** Die Unternehmen wünschen sich Transparenz. Sie möglichst einen konkreten Ansprechpartner beim Staat haben. Das CAZ ist in Bayern der zentrale Ansprechpartner für alle Fragen bei elektronischen Angriffen auf Unternehmen. Es koordiniert die weiteren Schritte.
2. **Schnelle Rückmeldung:** Die Wirtschaft wünscht sich, dass die Zusammenarbeit mit den Sicherheitsbehörden für sie einen Mehrwert hat. Diesen Mehrwert sieht sie insbesondere in einer möglichst schnellen und qualitativ wertigen Rückmeldung. Durch die Voranalyse von Angriffen im CAZ und die enge Zusammenarbeit mit dem BfV und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) kann das CAZ diesem Wunsch der Unternehmen nachkommen.
3. **Vertraulichkeit:** Der vertrauliche Umgang mit Meldungen zu elektronischen Angriffen ist aus Angst vor Reputationsverlust und damit verbundenen wirtschaftlichen Folgen ein zentrales Anliegen der bayerischen Unter-

nehmen. Weil sie eine mit polizeilichen Ermittlungen und einem sich daran möglicherweise anschließenden Gerichtsverfahren verbundene Medienberichterstattung befürchten, scheuen sich viele Unternehmen davor, vermutete Angriffe zur Anzeige zu bringen. Das CAZ kann als Organisationseinheit innerhalb des Bayerischen Landesamtes für Verfassungsschutz die von den Unternehmen gewünschte Vertraulichkeit auch rechtlich garantieren.

Cyber-Allianz-Zentrum Bayern (CAZ)

Das tatsächliche Meldeaufkommen zeigt, dass die Wirtschaft auch bei kritischen und sensiblen Angriffen das Angebot des CAZ annimmt. Die Unternehmen der bayerischen Wirtschaft sehen das CAZ als Partner an. Diese Partnerschaft mit dem Bayerischen Landesamt für Verfassungsschutz ist über mehrere Jahre hinweg gewachsen:

Im Rahmen des Wirtschaftsschutzes steht das Bayerische Landesamt für Verfassungsschutz, insbesondere im Bereich der präventiven Spionage- und Sabotageabwehr, schon seit vielen Jahren im engen Kontakt mit der bayerischen Wirtschaft. Es bietet rund um die Themen Proliferation, Wirtschafts- und Wissenschaftsspionage kostenfreie Serviceleistungen an, z. B. allgemeine Vorträge zur Sensibilisierung bis hin zu vertraulichen Gesprächen in betroffenen Firmen und

Hochschulen. Die Zuständigkeit des Verfassungsschutzes ergibt sich aus dem gesetzlichen Auftrag

- zum Schutz vor der Spionagetätigkeit ausländischer Nachrichtendienste
- sowie bei kritischen Infrastrukturen zum Schutz des Bestandes und der Sicherheit des Bundes oder eines Landes.

Warnmeldungen des CAZ zu Cyberangriffen

Hinweise auf spionage- oder sabotagerelevante Sachverhalte resultieren inzwischen nicht mehr nur aus den Kontakten zu Unternehmen, sondern zunehmend auch aus dem Hochschulbereich. Im Rahmen einer Forschungsarbeit der Freien Universität Berlin wurde z. B. die im Internet offen zugängliche Datenbank „Shodan“ ausgewertet. Dabei wurde festgestellt, dass es in Deutschland hunderte von Steuerungsanlagen gibt, die aufgrund ungesicherter Wartungszugänge oder veralteter Software über das Internet angreifbar sind. Die Nutzung internetfähiger Steuerungsanlagen nimmt weiter zu und umfasst eine immer größer werdende Bandbreite – vom Privatbereich bis hin zur Kritischen Infrastruktur. Das CAZ nahm dieses Forschungsergebnis zum Anlass, alle in Bayern betroffenen Unternehmen herauszuarbeiten und diese über die Sicherheitslücke sowie die notwendigen Sicherungsmaßnahmen zu informieren.

Veranstaltungsreihe mit den bayerischen Industrie- und Handelskammern

Um das Bewusstsein für die Gefahren durch Cyberangriffe bei den Unternehmensverantwortlichen zu steigern, beteiligte sich das CAZ zusammen mit dem Bayerischen Landesamt für Datenschutzaufsicht an einer Veranstaltungsreihe der bayerischen Industrie- und Handelskammern (IHK) zu „Gefahren moderner Informations- und Kommunikationstechnologie“. In acht Veranstaltungen quer durch alle Regierungsbezirke gab es praktische Hinweise und Tipps zum Schutz vor

Angriffen aus dem Netz. Nach dem Auftakt am 18. März mit Staatsminister Joachim Herrmann in München folgten weitere Veranstaltungen in Erlangen, Bayreuth, Passau, Coburg, Würzburg, Aschaffenburg und Regensburg.

IT-Gipfel der Bayerischen Staatsregierung

Im Rahmen des IT-Gipfels der Bayerischen Staatsregierung am 9. Mai gab Ministerpräsident Horst Seehofer den Startschuss für das Digitalisierungsprogramm **BAYERN DIGITAL** und stellte ein umfangreiches Maßnahmenpaket vor, das im engen Schulterschluss mit Wirtschaft und Wissenschaft in Bayern umgesetzt werden soll. Die Sicherheit im Internet hat dabei eine besondere Bedeutung. Bei der Abwehr elektronischer Angriffe kommt dem CAZ eine wichtige Rolle zu.

Zunehmende Cyberaktivitäten im Zusammenhang mit der Krise in der Ukraine

Seit Beginn des Konflikts zwischen Russland und der Ukraine ist eine Zunahme der Spionageaktivitäten zu verzeichnen. Das Abhören und Veröffentlichen von Telefongesprächen gehört ebenso zu den Maßnahmen wie das Hacken von E-Mail-Accounts oder Angriffe auf Internetseiten. Inhalte vertraulicher Kommunikation ukrainischer Politiker werden veröffentlicht, um diese damit zu diffamieren und eine pro-russische Sichtweise des Konflikts auch in westlichen Gesellschaften zu befördern.

Es muss damit gerechnet werden, dass auch bayerische Unternehmen, die mit der Ukraine wirtschaftliche Kontakte pflegen, Ziel von Cyberangriffen werden. Mit elektronischen Angriffen könnten sensible Daten, wie z. B. Kommunikations-

partner, Passwörter und betriebswirtschaftliche Kalkulationen, erlangt und weiterverbreitet werden, um die Geschäftsinteressen der betroffenen Unternehmen zu beeinträchtigen. Das CAZ hat betroffene Unternehmen mit einem Analysepapier sensibilisiert. Unternehmen, die Auffälligkeiten bemerken, werden gebeten, sich an das CAZ zu wenden:

Cyber-Allianz-Zentrum Bayern (CAZ) im
Bayerischen Landesamt für Verfassungsschutz
caz@lfv.bayern.de
Telefon: 089 31201-222

Bayerisches Staatsministerium des Innern, für Bau und Verkehr
Sachgebiet Cybersicherheit (IE5)
(Strategie, Koordination, Öffentlichkeitsarbeit)

Odeonsplatz 3
80333 München
cybersicherheit@stmi.bayern.de

Cyber-Allianz-Zentrum Bayern
im Landesamt für Verfassungsschutz
(Operativer Ansprechpartner für Wirtschaft, Wissenschaft und KRITIS)

Knorrstraße 139
80937 München
(089) 31201-222 (Hotline)
caz@lfv.bayern.de