Bundesamt für
Verfassungsschutz

Elektronische Angriffe

mit nachrichtendienstlichem Hintergrund

Elektronische Angriffe

mit nachrichtendienstlichem Hintergrund

Inhaltsverzeichnis

Gefahren für die moderne Informationsgesellschaft

Bis vor 20 Jahren dominierten Zeitungen, Radio und Fernsehen neben Telefon, Fax und herkömmlichen Postsendungen unsere alltägliche Kommunikation. Anfang der 90er Jahre hielten dann Computer, das Internet, E-Mails, Mobiltelefone und weitere Formen der Digitalisierung Einzug in unser tägliches Leben.

Diese fortwährende digitale Revolution hat die Welt in den vergangenen Jahrzehnten rapide gewandelt. Sie verändert das individuelle Kommunikationsverhalten in unserer Gesellschaft und vervielfacht den Umfang an schnell verfügbaren Informationen.

Neben neuen Freiheiten und Bequemlichkeiten entstanden dabei zugleich neue Abhängigkeiten und Gefährdungen. Die Informations- und Kommunikationstechnologie schafft neue (Frei-)räume, ist aber gleichzeitig auch vielfältigen Bedrohungen ausgesetzt.

Das Bundesamt für Verfassungsschutz (BfV) beobachtet seit geraumer Zeit, wie Extremisten und Terroristen die neuen Technologien für Ihre Zwecke einsetzen und ihre Agitationsformen und Organisationskonzepte entsprechend anpassen. Auch für fremde Nachrichtendienste bietet die rasante technische Entwicklung der Informations- und Kommunikationstechnologie vielfältige Möglichkeiten der Datenausspähung, Datenveränderung und Computersabotage. Der Schutz hochsensibler Informationen sowie der Schutz Nationaler Kritischer Infrastrukturen sind deshalb im Laufe der vergangenen Jahre zu vorrangigen Aufgaben im Kontext der inneren Sicherheit geworden – schließlich hängt heute nahezu unser gesamtes gesellschaftliches Leben von einer funktionierenden und verlässlichen IT-Infrastruktur ab.

Unsere moderne Informationsgesellschaft steht derzeit vor der Herausforderung, auf der einen Seite die erforderliche Balance zwischen Sicherheitsinteressen und Freiheitsrechten einzuhalten und auf der anderen Seite den vielfältigen Gefahren, die mit der digitalen Revolution einhergehen, wirkungsvoll und zukunftsweisend zu begegnen.

Insbesondere die Spionageabwehr des BfV ist daher gefordert Wege zu finden, wie die Sicherheit informationstechnischer Systeme vor Zugriffen durch fremde Nachrichtendienste effektiv zu gewährleisten sein wird. Wir sehen uns damit in der Pflicht, rechtswidrige Maßnahmen fremder Dienste auf deutschem Hoheitsgebiet rechtzeitig zu erkennen und zu unterbinden.

Spionageziel Deutschland

Die Bundesrepublik Deutschland ist aufgrund ihrer geopolitischen Lage, ihrer Rolle in der Europäischen Union und in der NATO sowie als Standort zahlreicher Unternehmen der Spitzentechnologie für fremde Nachrichtendienste attraktiv. Ihre offene und pluralistische Gesellschaft erleichtert fremden Mächten die Informationsbeschaffung. Diese erfolgt sowohl offen als auch verdeckt.

Besonders die Nachrichten- und Sicherheitsdienste der Volksrepublik China und der Russischen Föderation entfalten in großem Umfang Spionageaktivitäten gegen Deutschland. Deren Schwerpunkte orientieren sich an den politischen Vorgaben ihrer Regierungen.

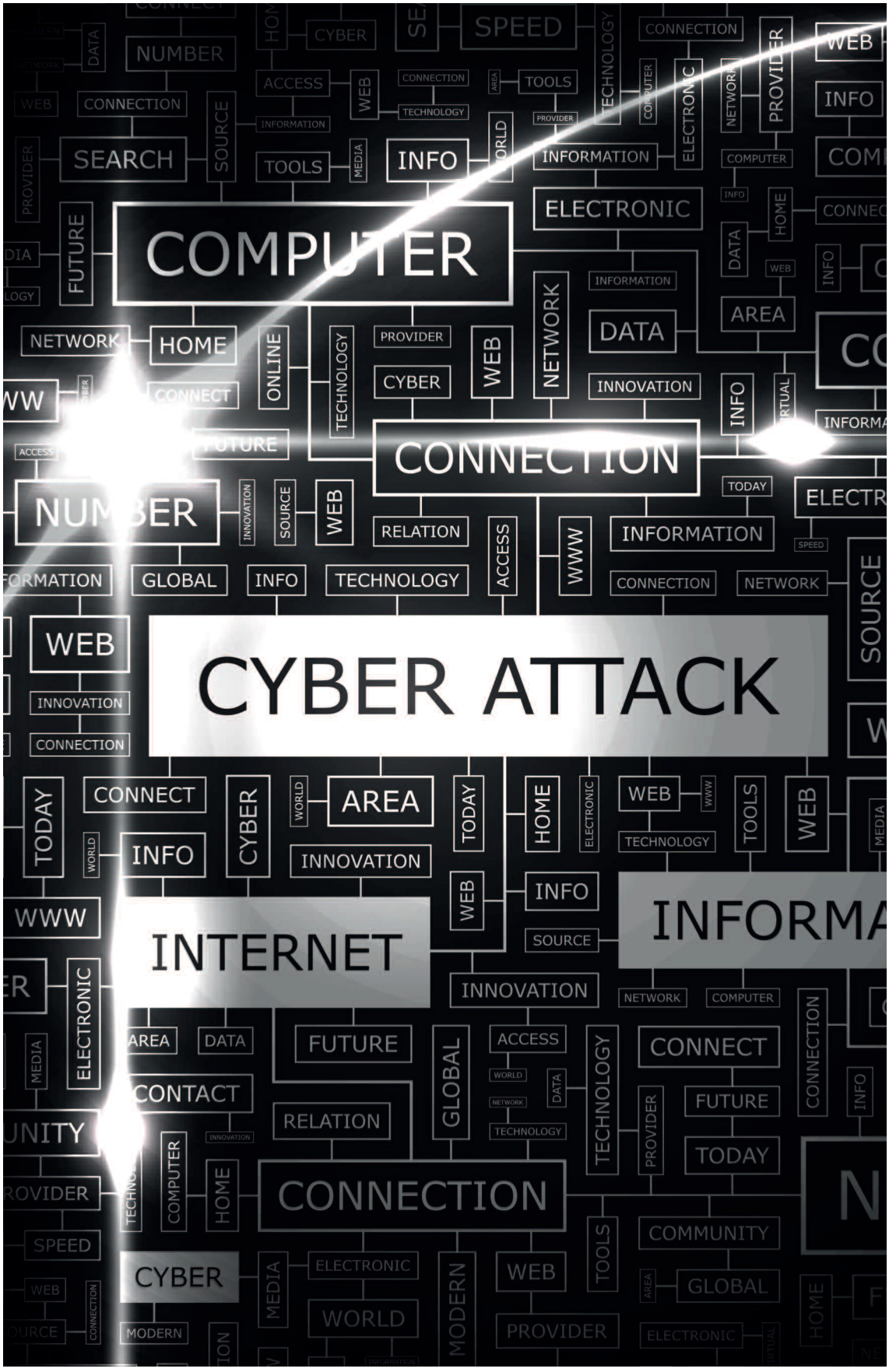
Hierzu gehört auch der gesetzliche bzw. staatliche Auftrag, die eigene Volkswirtschaft mit Informationen zu unterstützen, die auf nachrichtendienstlichem Wege beschafft wurden.

Die Nachhaltigkeit und globale Ausrichtung, mit denen diese mutmaßlichen Angreifer Informationen zu erlangen versuchen, sind dabei durch deutliche Anzeichen einer strategischen Aufklärung gekennzeichnet.

Bei der Spionage gegen Deutschland bilden die „klassischen“ Spionagemittel, wie z.B. der Einsatz menschlicher Quellen, nach wie vor eine wichtige nachrichtendienstliche Handlungsoption. Dies belegte zuletzt die im Jahr 2013 erfolgte Verurteilung eines Ehepaars zu mehrjährigen Haftstrafen. Beide Ehepartner waren unter Verwendung einer falschen Identität über mehr als zwanzig Jahre für einen russischen Auslandsnachrichtendienst tätig gewesen.


OK
OK

Daneben gewinnen aber auch technische Aufklärungsmaßnahmen stetig an Bedeutung. Unbestritten ist außerdem, dass neben China und Russland auch Nachrichtendienste anderer Staaten über die erforderlichen Ressourcen verfügen, um derartige technische Informationsgewinnungsmaßnahmen vom Ausland aus gegen deutsche Ziele ausführen zu können.


CYBER ATTACK
COMPUTER
CONNECTION
INTERNET
INFORMA
NUMBER
SPEED
CONNECTION
WEB
INFO
SEARCH
SOURCE
ACCESS
TOOLS
INFORMATION
ELECTRONIC
PROVIDER
FUTURE
NETWORK
HOME
ONLINE
TECHNOLOGY
CYBER
DATA
AREA
INNOVATION
RELATION
GLOBAL
WWW
TODAY
CONNECT
WORLD
CONTACT
COMMUNITY
MODERN
MEDIA

Was sind Elektronische Angriffe?

Seit 2005 werden auf breiter Basis durchgeführte, zielgerichtete Elektronische Angriffe gegen Bundesbehörden, Politik und Wirtschaftsunternehmen festgestellt, die weiterhin ein qualitativ hohes Niveau erreichen und eine hohe Gefährdung für die Informationssicherheit in diesen Bereichen bedeuten.

Die von uns über Jahre beobachtete hohe Zahl anspruchsvoller Spionageangriffe alleine auf deutsche Bundesbehörden belegt die erhebliche Bedrohung für die Sicherheit deutscher IT-Systeme. Von besonderem Interesse für die Angreifer sind dabei vor allem die Bereiche Außen- und Sicherheitspolitik, Finanzen sowie Militär und Rüstung.

In Deutschland obliegt die Aufklärung sicherheitsgefährdender oder geheimdienstlicher Tätigkeiten für eine fremde Macht den Verfassungsschutzbehörden. Dabei ist das BfV im deutschen Sicherheitsgefüge auch zuständig für

- die Abwehr von Elektronischen Angriffen durch fremde Nachrichtendienste gegen Ziele im Inland und gegen deutsche diplomatische Auslandsvertretungen,
- die Abwehr von Elektronischen Angriffen durch Extremisten und Terroristen gegen Ziele im Inland und gegen deutsche diplomatische Auslandsvertretungen.

Unter dem Begriff Elektronische Angriffe sind gemeinhin gezielt durchgeführte Maßnahmen mit und gegen IT-Infrastrukturen zu verstehen. Neben der Informationsbeschaffung fallen darunter jedoch auch Aktivitäten, die zur Schädigung bzw. Sabotage dieser Systeme geeignet sind.

Dazu gehören

- das Ausspähen, Kopieren oder Verändern von Daten,
- die Übernahme fremder elektronischer Identitäten,
- der Missbrauch oder die Sabotage fremder IT-Infrastrukturen sowie
- die Übernahme von computergesteuerten netzgebundenen Produktions- und Steuereinrichtungen.

Die Angriffe können dabei erfolgen:

- von außen über Computernetzwerke
  (wie z.B. das Internet)

  oder

- durch einen direkten, nicht netzgebundenen Zugriff auf einen Rechner
  (z.B. mittels manipulierter Hardwarekomponenten).

Elektronische Angriffe haben sich in den letzten Jahren als zusätzliche wichtige Methode der Informationsgewinnung fremder Nachrichtendienste etabliert. Die Gründe hierfür sind vielfältig:

- Elektronische Angriffe sind ein effektives und von den betroffenen Stellen nur schwer aufzuklärendes Mittel zur Informationsbeschaffung, bei dem insbesondere die sich bietende Anonymität des Internets eine Identifizierung und Verfolgung der Täter extrem erschwert.
- Solche Angriffe sind überdies kostengünstig, sie sind in Realzeit durchzuführen und sie besitzen eine hohe Erfolgswahrscheinlichkeit.


VIRUS

In Deutschland und gegen deutsche Ziele festgestellte nachrichten-dienstlich gesteuerte Elektronische Angriffe beinhalten – im Vergleich zu durch Extremisten und Terroristen verübte Elektronische Angriffe wie z.B. Defacements oder DDoS-Attacken – das aktuell deutlich größere Gefährdungspotenzial. Sie unterscheiden sich erheblich in Quantität und Qualität sowie hinsichtlich der den Tätern zur Verfügung stehenden personellen und finanziellen Ressourcen.

Fremde Nachrichtendienste sind in erster Linie an Informationen interessiert, die bei staatlichen Institutionen abgeschöpft werden können. Die anhaltenden Elektronischen Angriffe mit mutmaßlich nachrichtendienstlichem Hintergrund gegen Bundesbehörden verdeutlichen den hohen Stellenwert dieser Methodik.

Die Dauer einzelner Angriffsoperationen und die globale Ausrichtung bei der Auswahl von Themen und Opfern weisen dabei deutlich auf strategische staatliche Ausforschungsaktivitäten hin.


8GB
micro

Angriffsmethoden

Die Dunkelziffer nicht erkannter Elektronischer Angriffe ist weiterhin als hoch einzuschätzen, da die Methoden zunehmend ausgeklügelter werden. Die Angreifer entwickeln die eingesetzten Schadprogramme permanent fort und steigern damit die Effektivität derartiger Angriffe.

Selbst aktuelle Virenschutzprogramme sind nicht in der Lage, derartige Schadsoftware zu erkennen!

Elektronische Angriffe sind nicht zuletzt deswegen so gefährlich (und „erfolgreich"), weil sie selbst von Opfern mit einem ausgeprägten Sicherheitsbewusstsein häufig nicht erkannt werden. So weisen Schadmails in der Regel ein gutes „Social Engineering" auf, d.h. sie sind so gestaltet, dass sie zu den Interessen- bzw. Aufgabengebieten der Opfer passen und dadurch zunächst keinen Argwohn erregen. Zudem werden die Absenderadressen solcher E-Mails derart gefälscht, dass sie scheinbar von einem dem Opfer bekannten Absender stammen.

Neben der klassischen Trojaner-E-Mail, bei der das Schadprogramm zumeist im Anhang eingebunden ist und erst durch dessen Öffnen aktiviert wird, werden mittlerweile weitere, sehr ausgefeilte und kaum erkennbare Angriffsmethoden angewandt. Hierzu gehören z.B. sogenannte Drive-By-Infektionen: Die Angreifer erstellen dabei Webseiten mit einer entsprechenden Schadfunktion oder hacken und manipulieren bestehende Internetpräsenzen. Die ausgewählten Opfer werden gezielt mit einer E-Mail angesprochen und dazu verleitet, über einen Link die infizierten Webseiten aufzurufen. Zudem werden z.B. als Werbeträger verteilte Datenträger (USB-Sticks, Flashkarten, CDs usw.) zum Einschleusen von Schadsoftware genutzt.

Beispiel: G20-Gipfeltreffen

Derartige Attacken häufen sich regelmäßig im Zusammenhang mit bedeutenden wirtschafts- und finanzpolitischen Treffen. So wurden wie in den Jahren zuvor auch 2013 Angriffe im Rahmen des G20-Gipfeltreffens am 5. und 6. September 2013 in St. Petersburg (Russland) festgestellt. Neben mehreren Bundesministerien war u.a. der Bankensektor betroffen. In geschickt gestalteten E-Mails an hochrangige Entscheidungsträger und deren unmittelbare Mitarbeiter wurde eine Kommunikation der Chefunterhändler der beteiligten Regierungen vorgetäuscht. Damit wurde versucht, die Empfänger zu verleiten, den Schadanhang arglos zu öffnen und so eine Infektion der Systeme auszulösen.

Die auf diesem Wege erlangten Informationen hätten dem Angreifer theoretisch erlaubt, die Entscheidungen dieses Gremiums zu Fragen der internationalen Finanz- und Wirtschaftspolitik, der Energie-, Klima- und Entwicklungspolitik sowie zur Korruptionsbekämpfung bereits im Vorfeld abzuschätzen und entsprechend darauf zu reagieren.

Derartige Informationen stehen ganz besonders im Aufklärungsinteresse fremder Nachrichtendienste. Aufgrund der Merkmale und bestehender Parallelen zu anderen Angriffen auf das deutsche Regierungsnetz wird der Ursprung dieser Attacken im Jahr 2013 entsprechenden Stellen in China zugeordnet.

Angriffe auf die Wirtschaft

Neben der Integrität der staatlichen IT-Systeme ist insbesondere der Schutz der IT-Sicherheit in der Wirtschaft ein vordringliches Ziel des BfV.

Es liegt auf der Hand, dass elektronische Spionageangriffe nicht nur im Bereich der Behörden, sondern gerade auch im Bereich der Wirtschaft und Forschung ein probates Tatmittel darstellen.

Häufig greifen die potentiell Betroffenen vor allem aus wirtschaftlichen Erwägungen auf Standard-IT-Komponenten zurück und bieten auf diese Weise Angreifern Verwundbarkeiten. Nicht zuletzt sorgt auch der zunehmende Einsatz mobiler Endgeräte (Smartphones, Tablet-PCs) mit Zugang zum Firmennetz für neue Einfallstore.

Erfolgreiche Spionageangriffe – sei es mit herkömmlichen Methoden der Informationsgewinnung oder mit Elektronischen Angriffen – können immense volkswirtschaftliche Schäden verursachen, wenn aus Forschungseinrichtungen und privaten Unternehmen geistiges Eigentum abfließt. Elektronische Angriffe aller Tätergruppen zusammengenommen generieren in der deutschen Wirtschaft bereits jetzt einen auf mehrere Milliarden Euro geschätzten finanziellen Schaden.

Hauptsächlich sind Unternehmen mit den Schwerpunkten Rüstung, Automobile, Luft- und Raumfahrt sowie Satellitentechnik betroffen. Ferner stehen Technologieunternehmen und industrienahe Forschungsinstitute im Fokus.

Im Gegensatz zu den Angriffen auf Bundesbehörden sind Elektronische Angriffe auf die Wirtschaft von den Sicherheitsbehörden wegen der dortigen dezentralen IT-Strukturen, auf die staatliche Stellen keinen Zugriff haben, nur schwer zu detektieren.

Hinzu kommt, dass Unternehmen nur selten aus eigener Initiative heraus auf Sicherheitsbehörden zugehen, um relevante IT-Vorfälle zu melden.

- **Wir wissen um die Ängste der Unternehmen vor Prestigeverlust und Umsatzeinbußen, wenn ein erfolgreicher Spionage- oder Sabotageangriff an die Öffentlichkeit gelangt.**
- **Wir können jedoch Beratung bieten, auch ohne die entsprechenden Vorfälle zur Anzeige bringen zu müssen.**
- **Wir können ihnen zudem kompetente Ansprechpartner anderer deutscher Sicherheitsbehörden vermitteln.**

Vertraulichkeit ist dabei eines unserer obersten Handlungsgebote!

Cyber-Sabotage im Bereich Nationale Kritische Infrastrukturen

Wenn von Elektronischen Angriffen die Rede ist, meint dies nicht alleine eine gezielte Informationsbeschaffung auf elektronischem Wege. Ein erhebliches Bedrohungspotential für die innere Sicherheit bergen auch gezielt insbesondere gegen die sogenannten Nationalen Kritischen Infrastrukturen ausgeführte elektronische Sabotageakte.

Bei Elektronischen Angriffen verwendete Schadprogramme zur Informationsabschöpfung – also Spionageprogramme – können prinzipiell auch zu Sabotagezwecken eingesetzt werden. Hat ein Angreifer erst einmal Zugriff auf ein IT-System erlangt, kann er dort ungehindert eine Vielzahl an Aktionen durchführen, darunter auch solche gegen dessen Integrität und Verfügbarkeit.

Zu den Nationalen Kritischen Infrastrukturen eines Landes gehören Organisationen und Einrichtungen von zentraler Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

Es handelt sich also um Einrichtungen, auf die wir elementar angewiesen sind, Einrichtungen, welche die Lebensfähigkeit unserer modernen Gesellschaft sicherstellen.

Beispielsweise dürfte eine längerfristige Lahmlegung von Kraftwerken, Krankenhäusern, Bahnhöfen oder Flughäfen ein erhebliches Chaos verursachen.

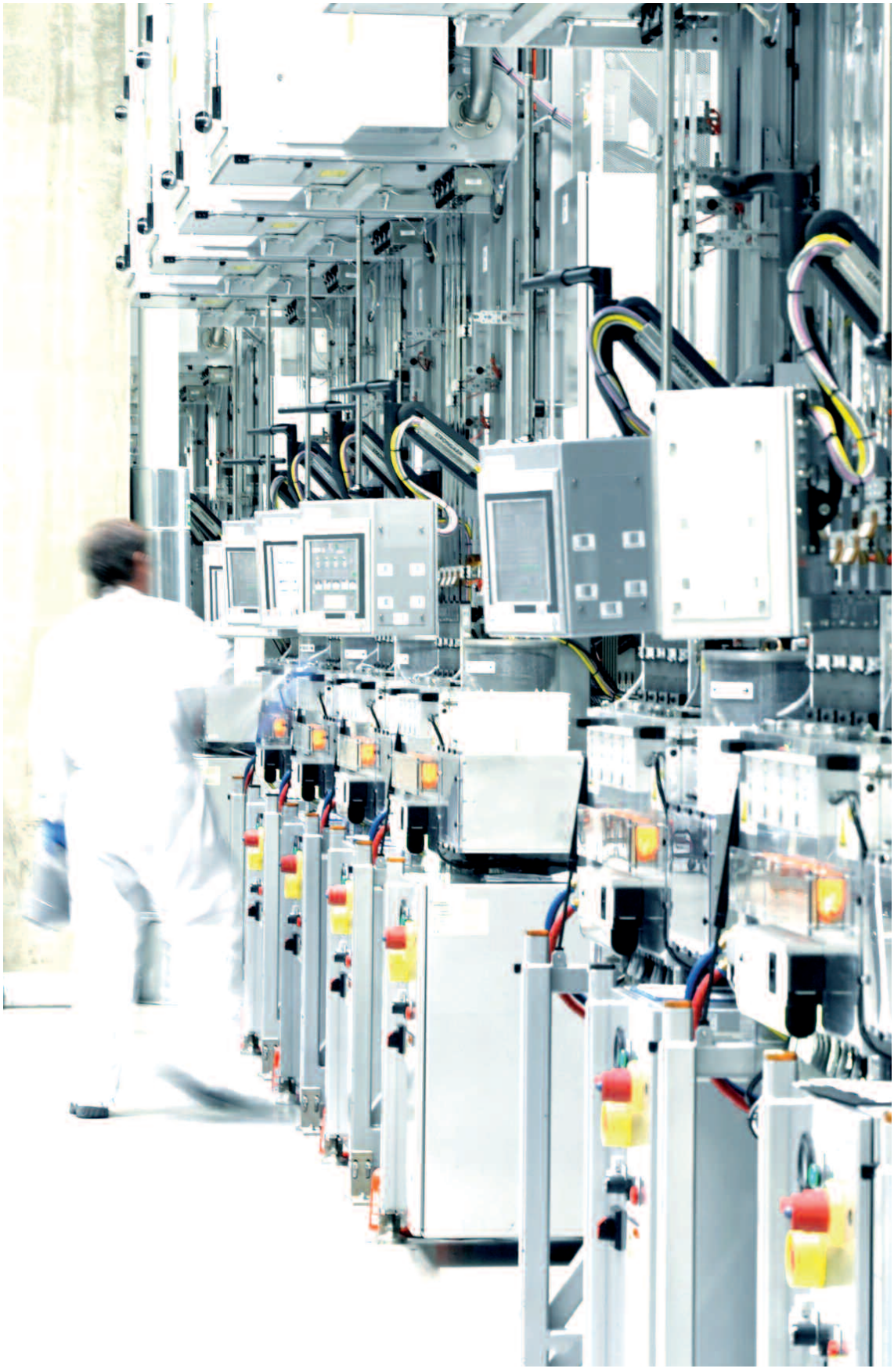

0
2
4
6
8
10
bar

Als sogenannte Kritis-Sektoren gelten demnach

- **Energie,**
- **Informationstechnik und Telekommunikation,**
- **Transport und Verkehr,**
- **Gesundheit,**
- **Wasser,**
- **Ernährung,**
- **Finanz- und Versicherungswesen,**
- **Staat und Verwaltung,**
- **Medien und Kultur.**

Nationale Kritische Infrastrukturen sind also Einrichtungen, auf die wir elementar angewiesen sind, Einrichtungen, welche die Lebensfähigkeit unserer modernen Gesellschaft sicherstellen. Man mag sich kaum vorstellen, welches Chaos im Ernstfall z.B. durch eine längerfristige Lahmlegung von Kraftwerken und Krankenhäusern, Bahnhöfen oder Flughäfen entstehen kann.

Eine unmittelbare Gefährdung für Nationale Kritische Infrastrukturen in Deutschland durch Extremisten und Terroristen ist bislang nicht belegbar. So gibt es keine Anhaltspunkte dafür, dass diese bereits über das notwendige IT-Verständnis und die personellen sowie finanziellen Ressourcen verfügen, um Angriffe auf komplexe IT-Systeme – so diese denn entsprechend



geschützt sind – zu verüben. Gleichwohl sind vereinzelt Bemühungen von extremistischen bzw. terroristischen Gruppen feststellbar, sich entsprechendes Know-how anzueignen.

Angriffe auf Nationale Kritische Infrastrukturen sind aktuell vielmehr militärischen Dienststellen und Nachrichtendiensten fremder Staaten zuzutrauen – wenn auch diese Gefährdung momentan eher als abstrakt zu bezeichnen ist. So dürften einige Staaten aufgrund ihrer finanziellen, technischen und personellen Ressourcen in der Lage sein, elektronische Sabotageakte durchzuführen. Anhaltspunkte für entsprechende gegen Deutschland gerichtete Aktivitäten liegen aktuell jedoch nicht vor.

Bei dieser Einschätzung handelt es sich allerdings nur um eine Momentaufnahme. Es bleiben politische und militärische Unwägbarkeiten sowie weitere Faktoren, die es unabdingbar machen, das Risiko von Cybersabotage als eine wichtige Aufgabe in den Fokus der sicherheitspolitischen Agenda zu rücken.

Angesichts des außerordentlichen Schadenspotenzials, das derartige Angriffe in sich tragen, werden wir in dieser Hinsicht noch größere Sensibilität und Wachsamkeit als bisher entfalten.

Zu berücksichtigen ist ferner, dass sich Angriffe auf IT-Infrastrukturen anderer Länder aufgrund der immer weiter fortschreitenden internationalen Vernetzung der IT-Systeme durchaus auch auf Deutschland auswirken können.

Entsprechend ernst nimmt das BfV als Inlandsnachrichtendienst seine Aufgabe als Frühwarnsystem in unserer Gesellschaft. Den Angreifern voraus zu sein, ihre Ziele und Vorgehensweisen zu kennen, in Zusammenarbeit mit nationalen und internationalen Sicherheitsbehörden die Ausführung von Elektronischen Angriffen zu verhindern oder mindestens die Folgen eines schwerwiegenden Sabotageaktes zu verringern, ist deshalb eine unserer vordringlichsten Aufgaben.

Zusammenarbeit im Cyber-Abwehrzentrum

Einhergehend mit dem gestiegenen Einsatz Elektronischer Angriffe wachsen auch die Anforderungen an die Sicherheitsbehörden.

Am 23. Februar 2011 wurde vom Bundeskabinett die vom Bundesministerium des Innern erarbeitete „Cyber-Sicherheitsstrategie für Deutschland“ verabschiedet. Ihr Ziel ist ein besserer Schutz der IT-Infrastrukturen sowie der Informations- und Kommunikationstechnik in Deutschland.

Einen wesentlichen Baustein dieser Strategie bildet das im April 2011 in Bonn eingerichtete Nationale Cyber-Abwehrzentrum (Cyber-AZ). Die mitwirkenden Behörden, darunter auch das BfV, arbeiten dort unter Federführung des Bundesamtes für Sicherheit in der Informationstechnik und unter Beibehaltung ihrer Zuständigkeiten, Aufgaben und Vorschriftenlage bereits seit über drei Jahren vertrauensvoll und gewinnbringend zusammen.

Ziel des Cyber-AZ ist die Optimierung der operativen Zusammenarbeit staatlicher Stellen sowie die bessere Koordinierung von Schutz- und Abwehrmaßnahmen gegen potentielle Cyber-Attacken.

Das Cyber-AZ ist dabei vor allem als Informationsdrehscheibe zwischen den beteiligten Behörden zu verstehen. Dort erfolgt ein zeitnaher und unkomplizierter Informationsaustausch, der es erlaubt, schnell und abgestimmt auf einen IT-Sicherheitsvorfall zu reagieren. Gerade bei Elektronischen Angriffen, deren Bearbeitung die Zuständigkeit mehrerer Sicherheitsbehörden berührt, zeigt sich insbesondere im täglichen Austausch die immense Bedeutung einer engen Zusammenarbeit.

Fazit

Aufgrund der vielfältigen Bedrohungen durch Elektronische Angriffe sind bei dieser Thematik nicht nur die Behörden in der Pflicht. Wir können unser Gemeinwesen nur dann nachhaltig schützen, wenn Staat und Wirtschaft der steigenden Bedrohung in diesem Bereich in enger und zugleich vertrauensvoller Kooperation begegnen. Sicherheitsbehörden wie der Verfassungsschutz können die Wirtschaft dabei diskret und ohne jegliches finanzielles Interesse beraten.

Die entscheidende Rolle des Verfassungsschutzes besteht in diesem Zusammenhang vor allem darin, eine präzise Einschätzung der Gefahren durch Elektronische Angriffe zu geben, erfolgte Angriffe zu analysieren, zuzuordnen und schließlich die Ergebnisse dieser Analysen für die präventive Gefahrenabwehr nutzbar zu machen.

Nur verlässliche Aussagen über die Intensität einer Gefahr und die Zuordnung von Taten zu einem Akteur ermöglichen eine rechtliche Einordnung und damit die (folge-)richtige politische Entscheidung. Bei uns laufen dazu Erkenntnisse aus vielfältigen eigenen und fremden Informationsquellen wie menschlichen Quellen, Schadsoftwareerkennungssystemen, Aufkommen aus der Fernmeldeaufklärung und anderen Arten der nachrichtendienstlichen Informationsgewinnung zusammen.

Erst in der bewertenden Gesamtschau ermöglichen all diese Meldungen dem BfV und seinen Partnern präzise und belastbare Aussagen über Täter, ihre Ziele und Vorgehensweisen zu treffen.

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
© Production Pering - Fotolia.com
© pressmaster - Fotolia.com
© Nmedia - Fotolia.com
© VRD - Fotolia.com
© Konstantin Yolshin - Fotolia.com
© Login - Fotolia.com
© Victoria - Fotolia.com
© Sergey Nivens - Fotolia.com
© seen - Fotolia.com
© Claireliot - Fotolia.com
© industrieblick - Fotolia.com
© peshkova - Fotolia.com
© mmmx - Fotolia.com
© FotolEdhar - Fotolia.com

Stand
Juli 2014

Weitere Informationen zum Verfassungsschutz finden Sie hier:

www.verfassungsschutz.de