Bundesamt
für Sicherheit in der
Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63, 53133 Bonn

Bundesministerium des Inneren
Referat IT3

- Per E-Mail -

[redacted]

HAUSANSCHRIFT
Bundesamt für Sicherheit in
der Informationstechnik
Godesberger Allee 185-189
53175 Bonn

POSTANSCHRIFT
Postfach 20 03 63
53133 Bonn

TEL +49 228 99 9582[redacted]
FAX +49 228 9910 9582[redacted]

referat-b24@bsi.bund.de
https://www.bsi.bund.de

Betreff: Weiterentwicklung Nationales Cyber-Abwehrzentrum

Bezug: Erlass vom 17.06.13, AZ: IT3 606 000-2/26#11
Aktenzeichen: B24 - 001 01 07
Datum: 24.01.14
Berichtserstatter: [redacted]
Seite 1 von 5
Anlage: - Keine -

Vorbemerkung

Das Cyber-Abwehrzentrum arbeitet seit seiner Einrichtung im April 2011 unter Federführung des BSI und direkter Beteiligung weiterer Bundesbehörden. Auf Basis der gesammelten Erfahrungen, von Gesprächen mit den beteiligten Behörden und der Anregungen seitens des BRH bereitet das BSI derzeit die Fortentwicklung des Cyber-Abwehrzentrums vor. Mit diesem Bericht stellt das BSI die intendierten Ziele und unterstützenden Maßnahmen vor.

Ziele der Fortentwicklung

Nach der Startphase des Cyber-Abwehrzentrums scheinen aus BSI Sicht nunmehr tatsächlich sowohl eine übereinstimmde Sichtweise der beteiligten Akteure sowie eine solide Grundlage für die Zusammenarbeit der Behörden erreicht zu sein, so dass die in der Cyber-Sicherheitsstrategie skizzierte Wirkung des Cyber-Abwehrzentrums kontinuierlich verbessert werden kann. Aus einer Drehscheibe zum gegenseitigen Informieren wird in Zukunft eine Plattform zum gemeinsamen Kooperieren beteiligter staatlicher Stellen (und später Unternehmen).

Die primären Ziele der Fortentwicklung des Cyber-Abwehrzentrums nehmen daher insbesondere die in der Cyber-Sicherheitsstrategie formulierten Erwartungen auf und streben danach, die operative Zusammenarbeit der staatlichen Stellen weiter zu optimieren. Die drei primären Ziele adressieren:

1. Einstieg in eine mehr operativ geprägte Fallbearbeitung und damit Gewinnung von **Wirksamkeit.**
2. Erhöhung der **Sichtbarkeit** des Cyber-Abwehrzentrums nach außen und damit stärkerer Einbezug der Interessen der Wirtschaft zum Schutz vor Cyber-Angriffen.
3. Definition von und Einrichtung von Schnittstellen zur **Kooperation** mit Stellen der Verwaltung und der Wirtschaft.

Maßnahmen und nächste Schritte

Zur Erreichung der skizzierten Ziele sollen folgende Maßnahmen ergriffen und Schritte vollzogen werden:

1. Das Cyber-Abwehrzentrum entwickelt sich von der Informationsdrehscheibe zur Kooperationsplattform.

Es hat sich bei einer Reihe von abgearbeiteten Fällen gezeigt, dass ein umfassender und transparenter Informationsaustausch aller beteiligten Akteure im Cyber-Abwehrzentrum vermieden wurde, da beispielsweise das in der Verfassung verankerte Trennungsgebot oder die vertrauliche Behandlung von Ermittlungsdaten in angestoßenen Strafverfahren dagegen sprach. Auch ist zu konstatieren, dass fallbezogen einige der beteiligten Akteure aufgrund ihrer gesetzlichen Aufgabenbefugnis nicht in der Lage sind, Beiträge zu einer Probemlösung zu liefern.

In der zukünftigen Zusammenarbeit wird daher das Cyber-Abwehrzentrum unterschiedliche, fallbezogen sinnvolle Arbeitsstrukturen anbieten. Dies kann sich erstrecken von

(a) der **Kooperation aller Beteiligten** über
(b) einer **multilateralen Kooperation** zweier beteiligter Stellen mit dem BSI bis hin
(c) zur **bilateralen Zusammenarbeit** zwischen nur einer Stelle und dem BSI.

2. Das Cyber-Abwehrzentrum übernimmt operative Verantwortung in der Fallbearbeitung.

Die im Cyber-Abwehrzentrum zu behandelnden Fälle und Fallkomplexe werden in Absprache mit den beteiligten Behörden einer vorfallsorientierten Bearbeitung zugeführt. Die Fälle sollten dabei nicht eingeschränkt sein auf die Verletzung von Vertraulichkeit, auch die Schutzzielverletzungen von Integrität und Verfügbarkeit gehören zum Aufgabenkanon des Cyber-Abwehrzentrums. Dazu werden fallbezogen Teams aus versierten Experten der Behörden gebildet ("Cyber-Abwehrteam"). Nach Abbarbeitung des zugrundeliegenden Falles bzw. Fallkomplexes und Vorlage eines Abschlussberichts wird das entsprechende Team wieder aufgelöst.

Die zukünftige, auf einem abgestimmten Vorgehensmodell beruhende Bearbeitungsform ermöglicht erst die analytische Aufarbeitung der fallbezogenen Verwundbarkeiten, Angriffsformen, genutzten Infrastrukturen sowie von Täter- und Opferbildern. Damit wird vor allem die Grundlage gelegt, Lagebilder zu erstellen und Rückschlüsse auf größere, ansonsten verborgen bleibende

Zusammenhänge zu ziehen.

Letztlich wird durch die professionelle Analyse auch erst eine effektive technische Abwehr von IT-Angriffen bzw. die Eindämmung von Schäden möglich.

Bei der technischen Abwehr sollen bei herausragenden Fällen zukünftig vorrangig BSI Kräfte zum Einsatz kommen. In der Masse der Fälle sollen jedoch vertrauenswürdige und zertifizierte IT-Sicherheitsdienstleister zum Einsatz kommen, die vom BSI unterstützt bzw. angeleitet werden. Im Bereich der Penetrationstests hat das BSI bereits drei Firmen als IT-Sicherheitsdienstleister gemäß § 9 BSIG zertifiziert. Zu prüfen ist, ob zertifizierte IT-Sicherheitsdienstleister auch in die Geheimschutzbetreuung aufgenommen werden sollten.

Die Erfahrung des BSI und Empfehlungen der europäischen Partnerbehörden zeigen, dass angegriffene Institutionen neben einer schnellen Information eine vertrauenswürdige Erstberatung und -analyse von staatlicher Seite erwarten.

3. Das Cyber-Abwehrzentrum entwickelt Außenwirkung und wird "Single Point of Contact".

Die Einrichtung von Cyber-Abwehrteams erlaubt bereits im Ansatz eine verbesserte Außenwirkung des Cyber-Abwehrzentrums. Bei Angriffen auf die Wirtschaft übernimmt das fallbezogen eingerichtete Cyber-Abwehrteam des Cyber-Abwehrzentrums die Rolle des **Single Point of Contact** gegenüber der betroffenen Institution. Hiemit werden die von der betroffenen Institution ansonsten zu haltenden Behördenkontakte zu allen involvierten Stellen auf eine einheitliche Schnittstelle im Cyber-Abwehrzentrum reduziert. Das eingesetzte Team des Cyber-Abwehrzentrums übernimmt alle notwendigen weiteren Beteiligungen der staatlichen Stellen und sorgt somit für ein koordiniertes, abgestimmtes, einheitliches und effizientes Auftreten. Im Ergebnis wird dadurch eine professionelle Unterstützung der vom IT-Angriff betroffenen Institution gewährleistet und durch sie als Mehrwert erfahrbar.

4. Das Cyber-Abwehrzentrum unterstützt die Krisenbewältigung.

Die kontinuierliche Kooperation in der Bearbeitung einzelner Fallkomplexe sowie ein abgestimmtes und gemeinsames Auftreten gegenüber den von Cyber-Angriffen betroffenen Institutionen führt zu eingeübten und gelebten Prozessen zwischen den beteiligten Behörden. Bekannte und eingeübte Prozesse führen gerade auch in verschärften Krisensituationen zu einem professionellen Agieren und stellen somit einen wichtigen Mehrwert des Cyber-Abwehrzentrums dar.

Das Cyber-Abwehrzentrum unterstützt in Krisensiuationen die Fachaufgaben der betroffenen und beteiligten Behörden, z. B. die technische Krisenrektion im Sinne von Incident Handling (z.B. Warnhinweise gemäß § 4 BSIG) beim CERT-Bund und dem Lagezentrum des BSI.

Daher werden in Zukunft im Cyber-Abwehrzentrum leistungsfähige Schnittstellen zu den beteiligten Behörden und insbesondere zu den relevanten technischen Arbeitseinheiten im BSI aufgebaut.

5. Zusammensetzung des Cyber-Abwehrzentrums.

Gemäß der bislang schon vorliegenden Ergebnisse der Input/Output Analyse können im Cyber-Abwehrzentrum zur intensiven Bearbeitung der Fälle nur bestimmte Behörden einen effektiven Beitrag leisten. Das sind die Behörden BSI, BfV, BKA, BND und MAD.

Darüber hinaus gibt es zahlreiche weitere Behörden, die als Multiplikatoren bzw. Regulierer in Bereiche (kritischer) Infrastrukturen wirken. Dazu zählen die Aufsichtsbehörden und mit einer exponierten Stellung insbesondere das BBK. Die Anbindung dieser Behörden über leistungsfähige Kommunikationsschnittstellen und -prozesse ist eine weitere wichtige Randbedingung für die Wirkung des Cyber-Abwehrzentrums.

In einer weiteren Gruppe können Behörden, Institutionen und unter Umständen Verbände und Unternehmen berücksichtigt werden, die Informationen des Cyber-Abwehrzentrums weitgehend nur zu ihrer technischen Eigensicherung benötigen. Von ihnen ist nur ein geringer eigener Input in das Cyber-Abwehrzentrum zu erwarten. Diesen Institutionen kann die Mitarbeit bzw. geeignete Verankerung im CERT-Verbund angeboten oder empfohlen werden. Dazu zählen u.a. die Bundespolizei, der IT-Betrieb der Bundeswehr und das ZKA.

6. APT-Arbeitskreis betroffener Behörden.

Ergänzend kann in Zukunft für alle von APT-Angriffen betroffenen Behörden und Ministerien die Mitarbeit und der Informationsaustausch in einem neu einzurichtenden APT-Arbeitskreis des Cyber-Abwehrzentrums angeboten werden. Hier können insbesondere die technischen Erkenntnisse des BSI zu Cyber-Angriffen sowie die nachrichtendienstlichen Erkenntnisse des BfV zu Spionageangriffen mit Betroffenen geteilt werden, bei denen die Abwehr und vor allem die Erkennung der Angriffe eine besondere Herausforderung darstellt.

Fortschreibung vorheriger Planungen

Der vom BSI vorgelegte Weiterentwicklungsbericht vom 7. Februar 2013 hat weiterhin grundsätzlich Bestand, bedarf aber in Teilbereichen der Anpassung. Wichtige Punkte dabei sind:

- Die Fortschreibung der Input-/Outputanalyse, um die Mitwirkung der Beteiligten verbindlich zu gestalten.
- Die Anpassung der Rolle der Verbindungsbeamten, um die Fallbearbeitung zu unterstützen. Die ständige Präsenzpflicht von Mitarbeitern der beteiligten Behörden vor Ort entfällt dadurch.
- Die Verabredung belastbarer Abstimmungsprozesse, um mit gemeinsamen Berichten dem Informationsbedarf des Cyber-Sicherheitsrates, der Bundesregierung und ggf. weiterer Zielgruppen z.B. in der Wirtschaft zu entsprechen.

Nächste Schritte

Das BSI wird mit BfV und BKA, sowie zunächst informell mit dem BND, die oben beschriebenen ergänzenden Punkte der Weiterentwicklung abstimmen, den Lenkungskreis im März unter Beteiligung aller Behördenleitungen durchführen und die Input-/Outputanalyse fortsetzen.

Die Notwendigkeit, das Cyber-Abwehrzentrum zu einer Kooperationsplattform weiterzuentwickeln, verdeutlicht, dass die wesentliche Herausforderung in der Koordination der Zusammenarbeit der teilnehmenden Behörden untereinander und mit dem BSI liegt und nicht in der Einbindung der technischen Expertise des BSI in das Cyber-Abwehrzentrum. Daher ist die Verankerung der Aufgabe in der Abteilung B des BSI eine unerlässliche organisatorische Voraussetzung für den Erfolg des Cyber-Abwehrzentrums.

Das BSI bittet die Fachaufsicht IT 3 um eine kurzfristige Besprechung im BMI, um diesen Bericht zu erläutern und die weitere Ausgestaltung abzustimmen. Anschließend wird das BSI mit den beteiligten Behörden die Veränderungen bilateral und im Lenkungskreis absprechen und initiieren. Die Fachaufsicht wird auch gebeten, die zu veranlassende interne Umorganisation im BSI gegenüber der Dienstaufsicht zu unterstützen.

Mit freundlichen Grüßen

Im Auftrag
Samsel