**R E P O R T**

# Cyber Attack Information Sharing

## Pilotstudie eines Österreichischen Cyberlagezentrums

Florian Skopik
AIT Austrian Institute of Technology GmbH

Roman Fiedler
AIT Austrian Institute of Technology GmbH

Otmar Lendl
CERT.at - Computer Emergency Response Team Austria

AIT Austrian Institute of Technology GmbH
Safety and Security Department
ICT Security Research Programme
Web: www.ait.ac.at/ict-security
Email: ict-security@ait.ac.at

13. Dezember 2013
Version 1
AIT-DSS-ICTSec-2013-12-11-v1

**Florian Skopik[1],Roman Fiedler[1] und Otmar Lendl[2]**
**[1] AIT Austrian Institute of Technology, Donau-City-Strasse 1, A-1040 Wien**
**[2] CERT.at - Computer Emergency Response Team Austria, Karlsplatz 1/2/9, A-1010 Wien**

# Cyber Attack Information Sharing

## Pilotstudie eines Österreichischen Cyberlagezentrums

Der störungsfreie Betrieb kritischer Infrastrukturen, wie etwa Telekommunikation oder Stromversorgung, ist essentiell für unsere heutige Gesellschaft. In den letzten Jahren haben jedoch Betreiber kritischer Infrastrukturen vermehrt mit Cyber-Security Problemen zu kämpfen. Durch den Einsatz von IKT Standard-Produkten und der zunehmenden Vernetzung und Offenheit der Infrastrukturen (z.B. um neue Businessmodelle und die dahinterstehenden Businessprozesse umzusetzen) haben sich die Angriffsflächen und -wege vervielfacht. Ziel der Forschungsprojekte „Cyber Attack Information System“ und „Cyber Attack Information Sharing“ ist daher die Entwicklung von Methoden und Technologien für den Austausch von Informationen über Cyber-Incidents zur besseren Abwehr von Cyberangriffen und zur effizienteren Analyse der aktuellen Bedrohungslage. Kernelement dabei ist die Etablierung eines Cyberlagezentrums welches eine essentielle Koordinationsrolle übernimmt. Um jedoch die konkrete Implementierung einer solchen Instanz voranzutreiben, ist es notwendig zu allererst dessen Einbindung in Cyber-Security Prozesse zu definieren. Dieser Artikel beschäftigt sich mit den Ergebnissen einer Pilotstudie, welche in enger Zusammenarbeit mit staatlichen Institutionen, Bedarfsträgern aus der Wirtschaft und dem österreichischen CERT durchgeführt wurde, und behandelt die illustrativen Darstellung der Aufgaben eines Cyberlagezentrums aus operativer und strategischer Sicht.

## 1 Einleitung

Das Funktionieren heutiger Gesellschaften ist stark abhängig von der ständigen Verfügbarkeit einer Vielzahl von IKT-Produkten und Dienstleistungen. Es besteht das Risiko schwerer wirtschaftlicher Effekte, wie auch von Auswirkungen auf die Sicherheit eines Staates, wenn diese über weite Regionen hinweg und/oder für einen längeren Zeitraum nicht verfügbar sind. Solch ein Szenario kann fatale Folgen für die Gesellschaft als Ganzes und kann für den Einzelnen Körperverletzungen oder sogar Tod bedeuten. Dienste, auf die diese Beschreibung zutrifft, bezeichnet man als „kritische Infrastrukturen“; Beispiele hierfür sind Energie, Verkehr, Gesundheitswesen, Finanzen, Nahrungsmittel- und Wasserversorgung. Eine wichtige Aufgabe beim Betrieb vieler solcher kritischer Infrastrukturen ist die informationsgetrie bene dynamische Steuerung eines physikalischen Prozesses. Demgemäß enthält eine kritische Infrastruktur oft verschiedene Steuersysteme; für Steuerentscheidungen werden aber auch Informationen von anderen Quellen mitverwendet, z.B. Auftragsstände. In der Vergangenheit waren diese IKT-Systeme meist isolierte, unabhängige, proprietäre Systeme ohne Verbindungen außerhalb des Regelkreises (Air Gap). Allerdings haben sich Kritische Infrastrukturen in der Zwischenzeit von unabhängigen, monolithischen Systemen hin zu vernetzten und stark verteilten Systemen entwickelt [1]. Angestoßen von Herausforderungen wie der Reduzierung des Energieverbrauchs sowie höherer Wirtschaftlichkeit, Flexibilität, und Effizienz, wird diese Tendenz weitergehen. Die Ver-

schmelzung dieser Systeme nennt man auch Cyber-physisches System (Cyber-Physical System).

Aus wirtschaftlichen Gründen setzen diese Cyber-physischen Systeme zunehmend auf commercial off-the-shelf (COTS)-Produkte. Dadurch wird die Angriffsfläche von solchen Systemen jedoch signifikant erhöht und bisher nur in Firmennetzwerken bekannte Bedrohungen und Schwachstellen werden so in Steuersystemen zum Problem. Als ein prominentes Beispiel ist hier Stuxnet [2] zu nennen, der erste öffentlich bekannt gewordene Wurm der sich auf industriellen Steuerungssystemen ausbreitete und diese teilweise lahmlegte.

Ein wichtiger Aspekt kritischer Infrastrukturen ist, dass sie viele Abhängigkeiten zwischen Komponenten [3] aufweisen und somit gewaltige Kettenreaktionen im Fall von Störungen ausgelöst werden können. Aufgrund der Vernetzung ist es auch nicht ausreichend, einen isolierten Überblick über den Sicherheitsstatus einer einzelnen kritischen Infrastruktur zu bekommen. Vielmehr ist es wichtig, ein allgemeines Lagebild, insbesondere unter Berücksichtigung von Abhängigkeiten, zu erhalten, um konsequente Reaktionen auf Sicherheitsverletzungen, und Angriffe zu ermöglichen und um mögliche Kaskadeneffekte zu verhindern oder zu minimieren. Ein Austausch von Informationen ist ein wichtiger Eckstein für den Aufbau eines branchenübergreifenden Bewusstseins über den aktuellen Sicherheitsstatus von kritischen Infrastrukturen.

Diese Ziele verfolgt auch die kürzlich vorgestellten europäische „Network and Information Security“ (NIS) Richtlinie [4]. Diese geht noch einen Schritt weiter und empfiehlt den Aufbau nationaler Cyberlagezentren, welche nicht nur über den Sicherheitsstatus der nationalen Infrastrukturanbieter informiert sind, sondern auch koordinierende Aufgaben bei der Prävention oder Abwehr von Angriffen übernehmen. Relevante und von Infrastrukturanbietern zu meldende Informationen, sind dabei nicht nur Cyber-Angriffe sondern auch schwere technische Störungen in IKT-Systemen, da diese auch die Folge noch unerkannter Angriffe sein könnten, aber auch Auswirkungen auf Systeme anderer Organisationen haben können, als wären diese direkt Ziel einer Attacke gewesen.

Der vorliegende Beitrag zeigt exemplarisch die im Forschungsprojekt *CAIS – Cyber Attack Information System* entwickelte Vorgehensweise und ablaufenden Prozesse bei der koordinierten Bewältigung einer Cyber-Attacke. Ziel ist es, die involvierten Stakeholder und ihre Aktionen zu dokumentieren, die dabei ablaufenden Prozesse sichtbar zu machen und auch Nicht-IT-Fachleuten die Komplexität einer solchen Aufgabe zu vermitteln. Letztendlich stellt die Beschreibung ein relevantes Ergebnis laufender Diskussionen dar, um die weiteren Schritte in Richtung eines österreichischen Cyberlagezentrums zu planen.

## 2 Kontext der Pilotstudie

Die hier beschriebene Pilotstudie wurde im Forschungsprojekt CAIS durchgeführt. Ziel war die Erarbeitung technischer Werkzeuge und deren Einbettung in im Projekt zu definierende Prozesse zur Unterstützung eines Cyberlagezentrums. Die Schwerpunkte der Werkzeuge lagen dabei im Bereich Anomalieerkennung [5] bzw. Simulation der Angriffsauswirkungen.

Im folgenden Szenario betreiben die vom nationalen Cyberlagezentrum unterstützten Organisationen selbst oder mit Hilfe von ihnen beauftragter Dienstleister ein entsprechendes innerbetriebliches IT-Sicherheitsmanagement. Dieses kann als zusätzliches Werkzeug zu z.B. üblicherweise eingesetzten SIEM-Lösungen auch spezifische in CAIS erarbeitete Methoden zur Anomalieerkennung verwenden (vgl. Abbildung 1). Einzelorganisationen erstellen im Anlassfall ad-hoc Berichte über Sicherheitsvorfälle, ausgelöst durch erfolgreiche Angriffe, aber auch Versuche mit außergewöhnlicher Raffiniertheit, Hartnäckigkeit oder problematischer Zielrichtung. Das Cyberlagezentrum betreibt eine Meldestelle, welche Berichte über entdeckte Vorfälle bzw. deren Auswirkungen auf die Services einer Organisation entgegennimmt. Das Lagezentrum sichtet diese Meldungen und erstellt daraus ein taktisches Lagebild, z.B. dass seit kurzem Mitarbeiter von VoIP-Anbietern mit einer bestimmten Malware attackiert werden oder dass nach dem Einbruch bei einem ISP die Vertraulichkeit der Daten auf seinen Leitungen momentan nicht gewährleistet ist. Aus diesem Lagebild werden dann sinnvolle Maßnahmen für die nächsten Stunden abgeleitet. Da die zentrale Meldestelle einen Überblick über die Services der Einzelorganisationen und deren Abhängigkeiten untereinander (Infrastrukturmodell) hat kann sie andere Marktteilnehmer gezielt warnen und auch bei der Erkennung und Abwehr unterstützen, z.B. durch Kommunikation von Indicator of Compromise (IoCs), Snort-Rules, und IP-Blocklisten.. Darüber hinaus ist diese zentrale Meldestelle in der Lage umfangreiche Simulationen vorzunehmen, um den Einfluss von Vorfällen im Netz von Serviceabhängigkeiten zu bewerten.

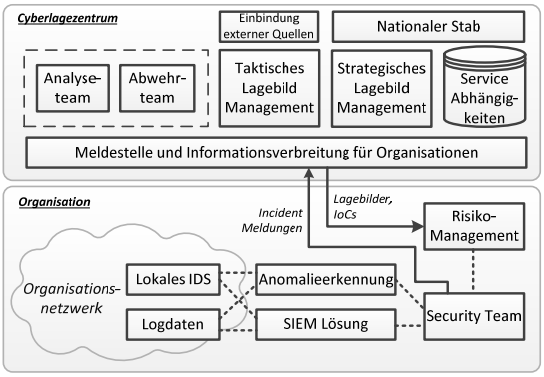

Abbildung 1: Vernetzung von Organisationen mit dem Cyberlagezentrum

Aus den Informationen des Tagesgeschäfts wird dann in regelmäßigen Abständen ein strategisches Lagebild erstellt, das vor allem politischen Entscheidungsträgern und dem jeweiligen Unternehmensmanagement von an das Lagezentrum gekoppelten Organisationen helfen soll, die richtigen Prioritäten zu setzen. Dieses Lagebild setzt daher auf einer völlig anderen Ebene an und könnte z.B. folgenden Inhalts sein: in den letzten Monaten nahmen Angriffe auf Mobilfunkbetreiber und SMS-Dienstleister zu, mit dem klaren Ziel Zugriff auf die SMS-Infrastruktur, z.B. zur Manipulation von 2-Faktorenauthentifizierung wie mobile-TAN, zu bekommen.

An folgendem fiktiven **Anwendungsfall** soll die Verwendung der CAIS-Werkzeuge und deren Einbettung in Prozessen im Cyberlagezentrum und in am Informationsaustausch teilnehmenden Organisationen anschaulich dargestellt werden. Es wurde angenommen dass ein Hersteller einer Fernwartungskomponenten in diese eine nicht dokumentierte Zusatzfunktion eingebaut hat, um so bei Wartungen oder zur Fehlersuche gewisse Informationen über das Gerät zu bekommen. Diese Art Hintertür wurde von Hackern entdeckt und analysiert, so dass es jetzt möglich ist, diese Schnittstelle zum Erlangen von Vollzugriff auf das Gerät zu verwenden. Die entsprechenden Werkzeuge werden unter der Hand getauscht, das Problem ist daher noch nicht öffentlich bekannt. Die an CAIS teilnehmende Organisation *Automatisierungstechnik GmbH* ist Errichter und Betreiber von Steuertechnik und nutzen die zuvor genannten problematischen Systeme. Ihre Kunden sind mittlere und größere Industrieunternehmen mit einem gewissen Fokus im Sektor Energietechnik, die den Bereich der Steuertechnik an den Spezialisten ausgelagert haben.

## 2 Organisationseinbindung in CAIS

Folgende Prozesse müssen zur Anbindung einer Organisation, z.B. eines kritischen Infrastrukturanbieters, an ein Cyberlagezentrum nach den im Projekt CAIS erarbeiteten Richtlinien stattfinden, bevor dieses im Falle einer Cyber-Attacke unterstützend tätig werden kann. Abbildung 2 gibt einen Überblick über die Schritte in dieser Phase.

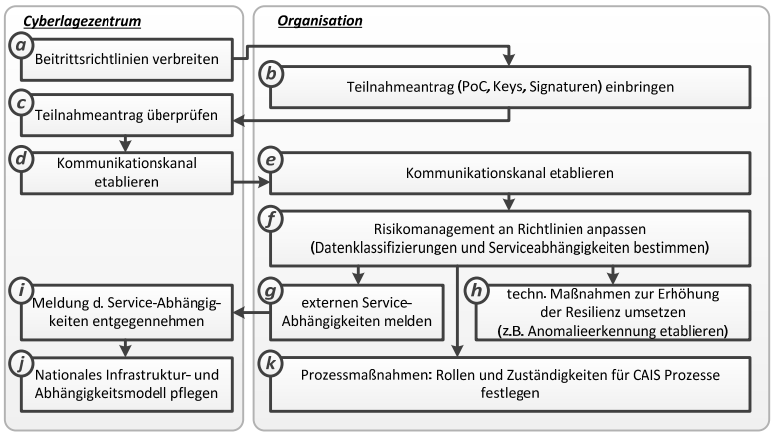


Abbildung 2: Vorbereitungsaktivitäten und Einbindung von Organisationen

**Vorbereitungen des Cyberlagezentrums:** Das Cyberlagezentrum bereitet Beitrittsrichtlinien und Handlungsempfehlungen für Organisation zum Vorgehen zur Anbindung an das Lagezentrum vor, z.B. zur Anpassung der Organisationsprozesse, zur Ermittlung der Serviceabhängigkeiten, zum Etablieren der Anomalieerkennungsinfrastruktur oder Richtlinien zur Meldung von möglichen bzw. bestätigten Angriffen.

**Teilnahmeantrag einer Organisation:** Die interessierte Firma *Automatisierungstechnik GmbH* informiert sich über das Cyberlagezentrum und kommt zum Schluss, dass ein Beitritt für sie sinnvoll ist. Durch die Bekanntgabe der Abhängigkeiten kann das Unternehmen vom Lagezentrum über Servicebeeinträchtigungen informiert werden, die sonst nicht trivial erkennbar wären, vor allem bezüglich Vertraulichkeit und Integrität bezogener Dienste. Darüber hinaus erhofft sie sich, durch Austausch von Information über aktuelle Angriffe effektiver und effizienter auf diese reagieren zu können und somit Ausfälle zu vermeiden. Als Zulieferer für kritische Infrastrukturanbieter ist es auch marketingtechnisch vorteilhaft, konkrete Sicherheitsaktivitäten vorzeigen zu können. Die Organisation beantragt daher die Teilnahme, indem sie eine Kontaktperson (PoC) nennt und PKI-Material zur sicheren verschlüsselten und signierten Kommunikation mitsendet.

**Überprüfung des Teilnahmeantrags:** Das Lagezentrum überprüft den Teilnahmeantrag der *Automatisierungstechnik GmbH*. Dies beinhaltet die Überprüfung der Identitäten, das Festlegen einer Service-Anbieter-ID (ID=471) für das Infrastrukturmodell, die Übermittelung der ID an den Antragsteller, sowie die Weitergabe der generellen Handlungsempfehlungen an die teilnehmende Organisation, um an CAIS zu partizipieren.

**Erhebung der Serviceabhängigkeiten:** Damit die Firma *Automatisierungstechnik GmbH* sinnvoll mit dem Cyberlagezentrum kooperieren kann, führt sie eine Prozessklassifizierung anhand der Richtlinien des Lagezentrums

durch. Daraus werden dann entsprechende Maßnahmen zur Gewinnung der für das Lagezentrum relevanten Informationen abgeleitet, z.B. was die relevanten Abhängigkeiten zu externen Services sind bzw. welches Vorgehen zur Entdeckung von Störungen und Angriffen sinnvoll ist (Abänderung von Policies, Personaleinsatz, Systemkonfigurationen verbessern, zusätzliches Sensor-Deployment). Im Detail sind dabei folgende Aspekte zu berücksichtigen:

- Essentiell ist die Identifikation und Erfassung der Serviceabhängigkeiten und der selbst bereitgestellten Services entsprechend der Richtlinien des Lagezentrums. Dafür müssen innerhalb der Organisationen, angelehnt an einer Business Impact Analyse (BIA), ihre Geschäftsprozesse und Services erhoben werden. Da diese Abhängigkeiten vertrauliche Informationen darstellen, werden nur die relevanten externen Abhängigkeiten an das Lagezentrum gemeldet. Folgende Abhängigkeiten wurden durch *Automatisierungstechnik GmbH* an das Lagezentrum gemeldet, wobei der Ort des Konsums der Leistung vereinfacht durch die 4-stellige Postleitzahl erfasst wird:
  - *Energieverband* (ID=5), Strom, Ort=3100
  - *TelekabelAG* (ID=46), Netzwerkanbindung (Leitungsebene), Ort=3100
  - Business-ISP (ID=undefined), Internetservice, Ort=3100
  - *TelekabelAG* (ID=46), Telefonie, Ort=3100
- Folgende Dienste bietet *Automatisierungstechnik GmbH* an (Information relevant für andere Organisationen zur Meldung ihrer Abhängigkeiten und für das Lagezentrum zur Infrastrukturmodellpflege):
  - *Automatisierungstechnik GmbH* (ID=471), Anlagensteuerungen: Errichtung und Betrieb, Ort=*

Das regelmäßige Aktualisieren dieser Abhängigkeiten erfolgt über die in den folgenden administrativen Maßnahmen zu etablierenden Prozesse.

**Administrative Maßnahmen:** Die Organisation adaptiert ihre Prozesse, um im Ernstfall rasch und effektiv reagieren zu können. Dabei ist zu berücksichtigen, dass die von der *Automatisierungstechnik GmbH* betriebenen Systeme bei Kunden laufen und deren Daten verarbeiten, was z.B. auf Meldeprozesse Auswirkungen hat.

- Zuständigkeiten im Sicherheitsbereich werden festgelegt: Wer arbeitet an den Systemen, die Sicherheitsvorfälle erkennen können? Wer kann solche Vorfälle dann überprüfen und klassifizieren? Wer trifft Entscheidungen über Meldung/Maßnahmen? Wie wird bei personellen Nichtverfügbarkeiten eskaliert? Wer ist für die Aktualisierung der CAIS-spezifischen Daten und Prozesse zuständig?
- Abhängig davon, wie feingranular das Unternehmen bereits jetzt Sicherheitsprobleme erkennen kann, werden entsprechende technische Maßnahmen umgesetzt, z.B. SIEMs installiert oder erweitert, die CAIS-Anomalieerkennung zum Einsatz gebracht, in gewissen Bereichen wird die Sensordichte erhöht.
- Vorgehen zur Analyse und Klassifikation eines möglichen Angriffs und Kriterien für Meldungen an das Lagezentrum werden definiert: (i) Da die Firma zu klein für eigene IT-Sicherheitsmitarbeiter ist, wird ein Vertrag mit der Firma *SecTroopers* abgeschlossen, sodass im Bedarfsfall rasch Forensik- und Abwehrleistungen bezogen werden können. (ii) Parallel wird der laufende Risikomanagementprozess um die Spezifika der IT-Risiken erweitert, z.B. unter Verwendung von BSI-Grundschutzkatalogen [6]. Da die Firma aber einen IT-Schwerpunkt und daher auch Interesse daran hat, dass IT-Risikomanagement intern auch verstanden und gelebt wird, wird zusammen mit einem Consultingunternehmen die initiale Bewertung durchgeführt, danach wird der Risikomanagementprozess komplett durch die Firma weitergeführt.

**Technische Maßnahmen:** Die Organisation entscheidet sich, auch die CAIS-Anomalieerkennung [5] zusätzlich zu ihren bestehenden Systemen einzusetzen, und zwar nicht nur im Haus auf ihren eigenen Systemen sondern auch in größeren Kundeninstallationen. Daher setzt sie folgendes um:

- Da die für die Anomalieerkennung erforderliche Sammlung von Logdaten in einigen Bereichen, z.B. von Netzwerkbasiskomponenten wie Switches und Firewalls, nur in geringem Umfang erfolgt, wird dort eine zentrale Logdatensammlung umgesetzt und Log-Levels entsprechend angepasst.
- Die regelbasierte CAIS-Anomalieerkennung wird installiert, Logdatenadapter werden eingerichtet.
- Es wird mit dem Probebetrieb begonnen. Es werden Regelsätze automatisch ermittelt, bei Regelverletzungen wird nur innerhalb des Systems eine Meldung ausgegeben und die Regel als unzutreffend entfernt. Die verbleibenden Regeln beschreiben die zeitlichen Zusammenhänge zwischen verschiedenen Vorgängen im System im Normalbetrieb.

**Nationale Infrastrukturmodellpflege:** Das Lagezentrum nimmt die gemeldeten Serviceabhängigkeiten entgegen und pflegt diese in ihr Modell ein. Wenn eine Organisation ein Service mit relevantem Marktanteil anbietet, so wird eine Simulation verschiedener Angriffsvarianten auf das Services durchgeführt. Je nach Schwere der Auswirkungen auf Services anderer Organisationen wird der Serviceanbieter durch das Lagezentrum klassifiziert, z.B. zur Optimierung des Ressourceneinsatzes im Angriffsfall oder zur Aktualisierung des strategischen Lagebildes.

**Basisschutz-Etablierung:** Anbieter kritischer Services, d.h. welche, von denen andere relevante Organisationen oder die Öffentlichkeit abhängen, unterstützt das Lagezentrum mit zusätzlichen Informationen und Hilfeleistungen beim Aufbau und der Verbesserung ihres ISMS, z.B. Herstellen einschlägiger Kontakte, Information bezüglich State-of-the-Art, besonders im Kontext nationaler Richtlinien und Gesetze, Maßnahmenempfehlungen abgeleitet von Systemen in anderen Unternehmen mit ähnlichen technischen Eigenschaften.

## 3 Ablauf im Falle eines Angriffs

Folgende Prozesse (vgl. Abbildung 3) würden im gegebenen Anwendungsszenario im Ernstfall ablaufen. Es ist zu beachten, dass einige Aktivitäten parallel stattfinden.

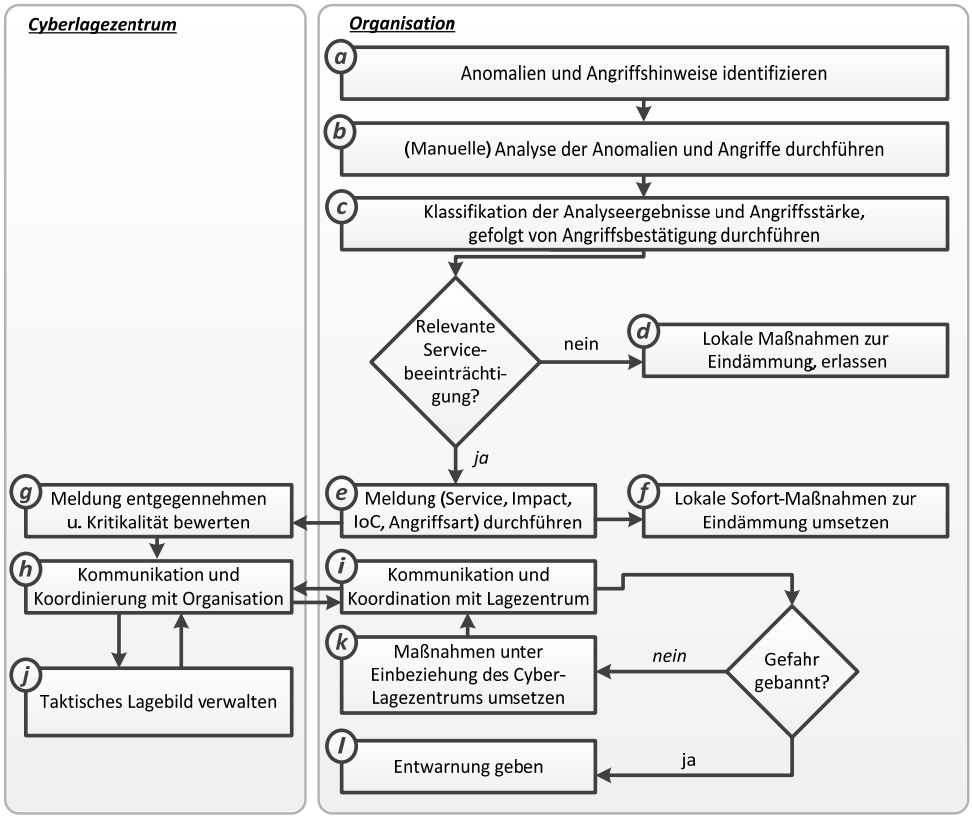


Abbildung 3: Meldung eines Angriffs an das Cyberlagezentrum

**Identifikation einer Anomalie:** Die in der Steueranlage eines Kunden installierte Anomalieerkennung, die ebenfalls von der *Automatisierungstechnik GmbH* betrieben wird, löst am 24.6.2013 um 00:21 aufgrund eines in den letzten 5 Minuten signifikant hohen Anomaliegrades eine Warnung aus, nach weiteren 25 Minuten um 00:46 ist die Anomalie wieder verschwunden. Der Techniker in Rufbereitschaft beginnt zwar um 0:35 mit einer kurzen manuellen Überprüfung der Logs mittels einer SIEM Lösung, findet allerdings innerhalb von 30 Minuten keinen Hinweis auf die genaue Ursache.

**Erstellung eines organisationsinternen Alarms:** Da die Anomalie hauptsächlich im Zusammenhang mit einem Wartungsnetz stand und laut Systemüberwachung die Verfügbarkeit nicht beeinträchtigte, wird entsprechend der im Vorfeld erarbeiten internen Richtlinien für Incident-Management nur ein Problembericht an den Netzwerktechniker der Tagschicht weitergeleitet.

**Interne Analyse:** Der Netzwerktechniker von der *Automatisierungstechnik GmbH* beginnt um 7:50 mit der Bearbeitung des Problemberichts. Er versucht dabei die den Normalzustand beschreibende Regel der Anomalieerkennung zu interpretieren und zu verstehen, warum sie innerhalb des kurzen Zeitraumes nicht mehr zutraf. Dabei erkennt er folgendes:

- Normalerweise gibt es in dem Wartungsnetz kaum Verkehr, daher finden einige Systeminteraktionen immer ungestört mit präzis gleichem zeitlichem Ablauf statt. Durch plötzlich stark erhöhte Last wurden diese Vorgänge indirekt gestört.
- Der Verkehr hätte eine Firewall passieren müssen, diese hat aber keinerlei Verbindungen protokolliert. Bei der Untersuchung der Firewall fällt auf, dass diese Zugriffe von außen nicht mehr blockiert sondern ungehindert durch lässt und diese eigentlich verbotenen Zugriffe auch nicht mitprotokolliert. Dieses Verhalten steht im Widerspruch zur momentan eingespielten Konfiguration, die das Gerät scheinbar ignoriert.

Da der entdeckte Fehler nicht auf einen technischen Defekt bzw. menschliches Versagen bei der Administration des Gerätes zurückgeführt werden kann, muss die Möglichkeit einer gezielten Manipulation ins Auge gefasst werden. Daher verständigt der Techniker nach 3 Stunden Analyse um 11:06 den CISO, der nach kurzer Rücksprache das Heranziehen einer Spezialfirma für Sicherheitsanalysen und Forensik, *SecTroopers*, beschließt.

**Security Consulting:** Die Security-Spezialisten nehmen um 15:30 ihre Arbeit auf und können in ihrer ersten Analyse, abgeschlossen in den frühen Morgenstunden des

dem Angriff folgenden Tages, diverse Zugriffe und Manipulation an verschiedenen Komponenten bestätigen, die scheinbar alle mit gestohlenen Zugangsdaten erfolgten. Da als erste Gegenmaßnahme die Passwörter abgeändert wurden, konnte so der Angreifer ausgesperrt werden. Zusätzlich wurde in den betroffenen Netzen das Mitprotokollieren des gesamten Netzwerkverkehrs eingerichtet. Beim Versuch des Angreifers erneut über dieselbe Schwachstelle Zugriff in das Wartungsnetz zum Ausspionieren der Passwörter zu erlangen, konnte aufgrund der Netzwerkprotokolle die Lücke entdeckt werden.

**Entscheidungsfindung:** Der CISO der *Automatisierungstechnik GmbH* und der Analyst von *SecTroopers* sind sich nach kurzer Beratung einig, dass es sich beim ‚Angriff um eine tiefgreifende Integrity- und Confidentiality-Verletzung unter Ausnutzung einer bis dahin unbekannten Softwareschwachstelle handelt. CISO und Management veranlassen die Meldung des Vorfalles an das Cyberlagezentrum.

**Meldung an Cyberzentrum:** Es ergeht eine Meldung an das nationale Cyberlagezentrum. Dabei werden die Leitlinien „Anonymisierung“ des Lagezentrums, aber auch die organisationsspezifischen Vorgaben, die in der Integrationsphase festgelegt wurden, berücksichtigt. Die Meldung an das Lagezentrum erfolgt verschlüsselt via E-Mail, die Eckpunkte des Inhalts sind:

- Vor einiger Zeit erlangte ein Angreifer über eine unbekannte Schwachstelle Zugriff auf das Fernwartungssystem eines gewissen Typs.
- Über das System konnte er weitere Systeme unter seine Kontrolle bringen, vermutlich indem er Passwörter auf unverschlüsselten Wartungsverbindungen erspähte.
- Das Steuersystem war daher zu signifikanten Teilen unter seiner Kontrolle, Integrität und Vertraulichkeit der Daten waren nicht mehr gewährleistet. Abschaltung der Systeme (DoS) wäre leicht möglich gewesen, wurde aber nicht ausgeführt. Die Bereinigung der Schäden und Prüfung aller Systeme wird mehrere Wochen dauern.
- IoC: Beim Aufbau der SSH-Verbindung zu dem Gerät wird in der Versionspräambel der Text „MasterMaintenanceMode“ übergeben, wodurch der Zugriff im Wartungsmodus auch ohne SSH-Schlüssel möglich wird.
- Da es sich um ein Standardsystem handelte sind potentiell alle Nutzer des Betriebsservices der *Automatisierungstechnik GmbH* für denselben Angriff verwundbar. Da das Produkt auf den Energiesektor zugeschnitten ist, besteht auch die Möglichkeit, dass andere Firmen in dem Segment betroffen sein könnten, auch wenn diese nicht Kunden der *Automatisierungstechnik GmbH* sind.

Das Format für die Erstmeldung sollte bewusst kürzer gehalten werden, damit diese schnell und einfach abgesetzt werden kann. Im Bedarfsfall kommt dann weitere Kommunikation zwischen Lagezentrum und betroffener Organisation zu Stande, wobei dann die genauen Details zum Angriff ausgetauscht werden.

**Bewertung der Meldung:** Das Lagezentrum nimmt die Meldung der Firma entgegen:

- Es wird das Ereignis nach einer definierten Vorgehensweise ins taktische Lagebild eingepflegt.
- Bei entsprechender Schwere wird mit der Koordination von Gegenmaßnahmen begonnen, was in diesem Beispiel der Fall ist.

**Organisationsinterner Prozessanlauf**: Die Entscheidung des CISOs wird innerhalb der Organisation umgesetzt.

**Nationale Maßnahmen:** Es stellt sich nach Durchsicht des Abhängigkeitsmodells heraus, dass eine erheblich Anzahl an Organisationen entweder direkt oder indirekt vom betroffenen Service abhängig sind. Im Lagezentrum wird eine Simulation gestartet um die Auswirkungen des Serviceausfalls zu ermitteln. Fragen die geklärt werden sollen sind:

- Welche anderen Organisationen sind vom Serviceausfall betroffen, d.h. können deren Services dann nicht mehr vollumfänglich anbieten?
- Wie kritisch ist diese Situation für Drittfirmen?
- Wie sieht es mit transitiven Effekten aus bzw. mit Kaskadeneffekten?
- Welche anderen Organisationen sollen über Dienstbeeinträchtigungen vorgewarnt oder über Schwachstellen informiert werden?

Aufgrund der verschiedenen Informationen wird entschieden, wer in welchem Umfang vorgewarnt wird. Zu großflächige Warnungen sind dabei eher kontraproduktiv, da das Risiko für Datenlecks mit der Zahl der Informierten steigt und durch Überflutung mit nicht zielgerichteten Mitteilungen Relevantes leichter übersehen wird. Für eine schnelle, spezifische und effektive Organisationsreaktion auf Angriffe ist die Weitergabe der „Indicators of Compromise“ bzw. spezifischer Gegenmaßnahmen sehr hilfreich.

**Verfeinerte Meldung:** Aufgrund der neuen Erkenntnisse zum Angriff übermittelt die betroffene Firma erneut eine Meldung an das Cyberlagezentrum. Die Kernpunkte dabei sind, dass a) die Angreifer auf übernommenen Geräten einen zusätzlichen Steuerkanal über DNS eingerichtet haben, der unbedingt unterbunden werden muss b) zum Ausspionieren der über das Wartungsterminal laufenden Verbindungen eine tcpdump-Variante verwendet wurde um unverschlüsselte telnet/ftp-Zugriffe

mitzulesen c) die Abwehr des Angriffs länger dauern wird als erwartet.

**Laufende Kommunikation und Koordination**: Zwischen *Automatisierungstechnik GmbH* und dem Cyberlagezentrum findet ein reger Austausch bis zur Behebung des Problems statt. Dazu zählen die dem Lagezentrum übermittelten verfeinerten Meldungen zum Angriff; das Lagezentrum gibt neue Informationen zu Angriff oder Gegenwehr weiter, die es von anderen betroffenen Firmen oder CERTs anderer Staaten erhalten hat.

**Entwarnung:** Sobald die Organisation das Problem beheben konnte, wird eine abschließende Meldung erstattet und der „Alarmzustand" aufgehoben.

## 4 Lagebildverteilung und Unterstützung

Das laufend aktualisierte Cyberlagebild wird gezielt an relevante Organisationen verteilt, um diese im Falle großflächiger Angriffe vorzuwarnen und bei ihren Entscheidungen die Cyber-Abwehr betreffend zu unterstützen. Dabei laufen die Prozesse wie in Abbildung 4 dargestellt, ab.

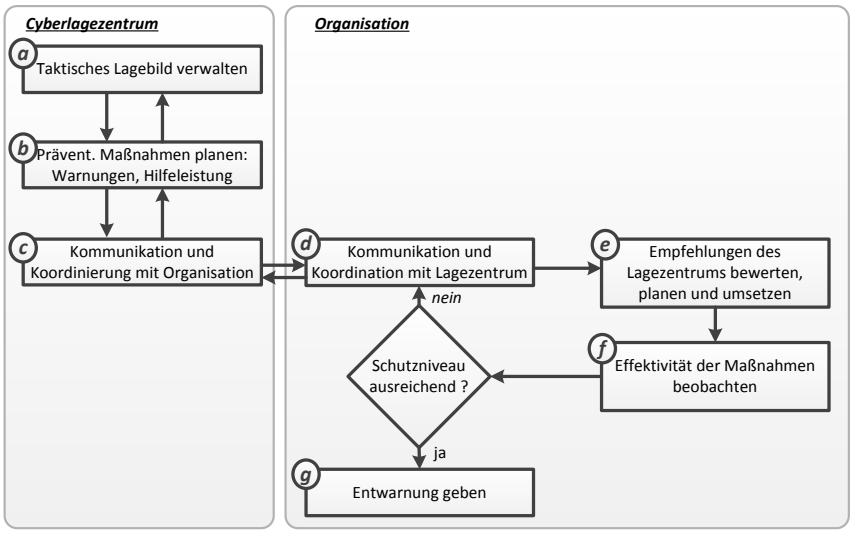


Abbildung 4: Vorwarnung und Lagebildverteilung an Organisationen

**Verwaltung des taktischen Lagebildes:** Entsprechend den Meldungen und den Ergebnissen der Simulation wird durch die Expertinnen und Experten des Lagezentrums das taktische Lagebild aktualisiert. Wird ein Angriff auf eine teilnehmende Organisation detektiert, die zu einer erheblichen Beeinträchtigung ihrer angebotenen Services an andere Organisationen führt, so wird diese Information besonders gewissenhaft bewertet (z.B. mittels Szenarien-Simulation). Daraufhin können Kaskadeneffekte und deren zeitlichen Abläufe für teilnehmende Organisationen ermittelt werden. Basierend auf diesen Ergebnissen können weitere involvierte Organisationen vorgewarnt und Aktionen entsprechend der vorliegenden Notfallpläne ausgeführt werden.

**Informationsverbreitung:** Im vorliegenden Angriffsfall auf SmartGridSolutions, ein Kunde der Automatisierungstechnik GmbH, leitet das Cyberlagezentrum neue Informationen über stattfindende Angriffe an relevante Organisationen weiter:

- Weitergabe der Informationen aus dem taktischen Lagebild, z.B. dass alle angegriffenen Systeme bei Unternehmen im Energietechnikbereich liefen aber keine Angriffe dieser Art in anderen Sparten gemeldet wurden.
- Verteilung der IoCs und Gegenmaßnahmen an Firmen, welche ebenso verwundbare Produkte verwenden, aber nicht notwendigerweise Kunde der *Automatisierungstechnik GmbH* sind.
- Koordinierung zwischen *Automatisierungstechnik GmbH* und anderen Firmen, die zur selben Zeit an ähnlichen Gegenmaßnahmen arbeiten.

Da die *Automatisierungstechnik GmbH* bereits erfolgreich an der Abwehr arbeitet, wird auch darauf hingewiesen, dass das Risiko besteht, dass die Angreifer die Gegenmaßnahmen bemerken und daraufhin die noch unter ihrer Kontrolle befindlichen Komponenten stören oder beschädigen.

**Organisatorische Maßnahmen:** Informierte Organisationen beginnen aufgrund der Meldungen ihre Systeme zu durchforsten und problematische Geräte bis zum Erscheinen eines Patches vom Internet abzuschotten oder zumindest durch Firewall- oder VPN-Appliances zusätzlich zu schützen. Durch den zusätzlichen Aufwand bzw. Nebeneffekte der Maßnahmen kommt es zu zwar geringfügigen Störungen und Produktivitätsrückgängen in den Firmen, aber großflächiger Schaden kann effektiv verhindert werden.

## 5 Resümee und Schlussbetrachtung

Während mit dem Austrian Program for Critical Infrastructure Protection (APCIP) [7] ein umfangreicher Masterplan zum Schutz Kritischer Infrastrukturen vor physische Bedrohungen vorliegt, ist dieser Plan auf die Cyber-Domäne nur begrenzt anwendbar bzw. nicht hinreichend ausgeprägt und spezifisch. Maßnahmen um mit Bedrohungen aus der Cyber-Domäne, wie z.B. Spionage, Sabotage und Denial-of-Service Attacken, umgehen zu können, unterscheiden sich fundamental von „herkömmlichen Schutzmaßnahmen". Die Erkennung solcher An-

griffe ist ungleich schwieriger da diese oft anfangs von einer Fehlfunktion nicht zu unterscheiden sind. Außerdem ist der Zeitrahmen für entsprechende Gegenmaßnahmen oft nur im Bereich von Stunden und damit um vieles kürzer.

Neue Verfahren und der nachhaltige Aufbau von Expertise im Umgang mit diesen Bedrohungen und Szenarien sind daher von Nöten. Das gilt sowohl in Bezug auf die eingesetzten Technologien, als auch auf die Vorgehensweisen in den verschiedenen (Industrie-)Sektoren. Zwar gibt es Bestrebungen diese Situation zu verbessern, wie beispielsweise mit der „Österreichischen Strategie für Cyber Sicherheit“ [8], der „Nationalen IKT-Sicherheitsstrategie Österreich“ [9] oder dem deutschen KRITIS Programm [10], allerdings sind diese Initiativen nur erste Schritte und alleine noch nicht ausreichend, um einen umfassenden Schutz für Kritische Infrastrukturen zu gewährleisten.

Dieses Dokument zeigte daher exemplarisch die Anwendung der im KIRAS Projekt CAIS entwickelten Werkzeuge und erarbeiteten Prozesse für den Betrieb eines Cyber Attack Information Systems in Österreich.

Besonderes Augenmerk ist dabei auch auf die rechtlichen Aspekte zu legen. Zwar wird die NIS-Richtlinie der EU eine klare Meldepflicht enthalten, allerdings sind hier etliche Detailfragen bzgl der Umsetzung zu erwarten, z.B. wer meldet bei Erkennungen auf gemieteter Infrastruktur, beim Betrieb durch Subkontraktoren oder wie ist mit Haftungsfragen bei Falschmeldungen umzugehen.

Die damit erreichten Ziele des Einsatzes von CAIS sind:

- *Erstellung eines technischen Lagebildes*: beinhaltet die Erhebung der Serviceabhängigkeiten kritischer Infrastrukturanbieter und erlaubt die bessere Erkennung und Bewertung des aktuellen technischen Zustandes der kritischen IKT Systeme in Österreichs Organisationen.
- *Steigerung der Resilienz*: durch Vorwarnung bzw. Frühwarnung von Organisationen, die von einer eingeschränkten Verfügbarkeit von kritischen Services (a) im Simulationsfall betroffen wären (daher die Anwendung präventiver Maßnahmen ermöglicht), oder (b) im realen Angriffsfall betroffen sind (und daher die zeitgerechte Anwendung reaktiver Maßnahmen ermöglicht).
- *Hilfestellung*: im Falle einer realen Attacke mit Know How und Expertise zur Behebung von Problemen. Wichtig dabei ist, dass die Eigenverantwortlichkeit der Organisationen erhalten bleibt. Es werden weder Informationen automatisiert weitergegeben, noch wird von Dritten in eine private Infrastruktur eingegriffen.

## Danksagung

Die vorgestellten Arbeiten wurden in den nationalen Projekten CAIS (Cyber Attack Information System) und CIIS (Cyber Incident Information Sharing) durch das Österreichische Bundesministerium für Verkehr, Innovation und Technologie bzw. durch die FFG im Rahmen des KIRAS Sicherheitsforschungsprogramms finanziell unterstützt. Die Autoren danken den Konsortialpartnern für ihre konstruktiven Beiträge zu den in diesem Artikel vorgestellten Ergebnissen.

## Literatur

[1] IMC-AESOP project (EU FP7): http://www.imc-aesop.eu/, January 2013
[2] Eric, Byres at al; How Stuxnet Spreads – A Study of Infection Paths in Best Practice Systems; Tofino Security; Abterra Technologies; SCADAHakcer.com; White Paper; 22.2.2011
[3] Javier Lopez et.al, Overview of Critical Information Infrastructure Protection, LNCS 7130, Springer Verlag Berlin Heidelberg 2012, pp1-14
[4] Commission Proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union; http://ec.europa.eu/digital-agenda/en/news/commission-proposal-directive-concerning-measures-ensure-high-common-level-network-and February 2013
[5] Skopik F., Fiedler R. (2013): Intrusion Detection in Distributed Systems using Fingerprinting and Massive Event Correlation. GI INFORMATIK 2013.
[6] Bundesamt für Sicherheit in der Informationstechnik: BSI IT-Grundschutzkataloge. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html
[7] MASTERPLAN: Österreichisches Programm zum Schutz Kritischer Infrastruktur (APCIP) -- http://www.kiras.at/uploads/media/MRV_APCIP_Beilage_Masterplan_FINAL.pdf
[8] Österreichische Strategie für Cyber-Sicherheit (ÖSCS): http://www.bka.gv.at/DocView.axd?CobId=50748
[9] Bundeskanzleramt, Digitales Österreich: Nationale IKT-Sicherheitsstrategie Österreich: http://www.digitales.oesterreich.gv.at/DocView.axd?CobId=47986
[10] KRITIS: http://www.bmi.bund.de/SharedDocs/Downloads/DE/__Broschueren/2007/Kritis.html

## Kontakt

AIT Austrian Institute of Technology GmbH
Donau-City-Straße 1, 1220 Wien, Österreich

www.ait.ac.at
Fax +43 50550 2813

DDr. Florian Skopik
Safety & Security Department
ICT Security
+43 664 8251495
florian.skopik@ait.ac.at

DI Thomas Bleier, MSc
Safety & Security Department
Thematic Coordinator ICT Security
+43 664 8251279
thomas.bleier@ait.ac.at