Absicherung von IT-Risiken im Produktionsumfeld

Integrierter Schutz von Informations- und Produktionstechnologie

Christof Thim, Universität Potsdam

Die Risiken, welchen Fabrikinfrastrukturen durch IT-Angriffe ausgesetzt sind, erfordern eine gemeinsame Betrachtung von IT-Sicherheit und der Absicherung der Operational Technology (OT). Hierbei sind die Maßnahmen aus der Office-IT nur begrenzt auf den Fertigungsbereich und die Produktionssteuerung zu übertragen. Zu unterschiedlich sind die Anforderungen und Schutzziele für die eingesetzte Hardware und die Vernetzung zwischen den Komponenten. Eine integrierte Betrachtung und ein kontinuierliches Management der IT-Sicherheit helfen dabei, gezielte Maßnahmen zu identifizieren und konzertiert umzusetzen.

Securing IT-Risks in a Production Environment – an Integrated Approach for Information and Operational Technology

The IT-risks which factory infrastructures are exposed to, require a common view of IT-security and operational technology (OT) protection. In this context, the measures from office IT can only be transferred to the production area and production control to a limited extent. The requirements and protection goals for the equipment used and the networking between these components are too different. An integrated approach and continuous management of IT security helps to identify and implement targeted measures in a concerted manner.

Keywords:
IT-Security, operational technology, SCADA, safety

In den letzten Jahren nahmen die Angriffe auf Informationssysteme beständig zu. Das Hauptziel sind bisher Systeme der Office-IT. Angriffe mit Trojanern wie z. B. WannaCry oder Locky hatten das Ziel, die Datenquellen der Unternehmen zu verschlüsseln und damit Lösegelder zu erpressen. Aber auch die gezielte Infiltration z. B. des Bundestagsnetzwerks über sogenanntes Spearfishing erfuhr große öffentliche Aufmerksamkeit. Die Angriffe zielten dabei häufig auf den Abfluss von Daten ab. So konnten sowohl Kreditkarten als auch Login-Daten bei mehreren Hacks erbeutet werden. Finanzielle Ausfälle sowie ein Verlust an Reputation der betroffenen Unternehmen waren die Folge. Physische Schäden werden eher selten von den Angreifern in Kauf genommen [1].

Industrielle Infrastrukturen sind bisher selten gezielt angegriffen worden. Dokumentiert sind die Seiteneffekte des gezielten Stuxnet-Angriffs, aber auch der gezielte Angriff auf ein deutsches Stahlwerk [2]. Dies heißt jedoch nicht, dass die Bedrohungslage weniger virulent ist als in der klassischen Office-IT. Vielmehr zeigt die Analyse des BSI im Lagebericht, dass Angriffe auf industrielle Anlagen erfolgreich sind [3]. Es ist davon auszugehen, dass viele Angriffe nie an die Öffentlichkeit gelangen und von einer erheblich höheren Dunkelziffer ausgegangen werden kann.

Welche Konsequenzen ergeben sich aus der Gefährdungslage nun für den Schutz von Industrieanlagen? Auf Basis der Erkenntnisse aus dem BMBF-Forschungsprojekt „Aqua-IT-Lab“ [4] sollen hier die Grenzen einer alleinigen Konzentration auf die traditionelle IT-Sicherheit dargelegt sowie einige Kernaspekte zur Absicherung von Industriekomponenten und -anlagen vorgestellt werden. Der vorgestellte Schnelltest der IT-Sicherheit erweist sich als erster Einstieg für kleine und mittlere Unternehmen, die bisher kein strukturiertes IT-Sicherheitsmanagement haben und die der Aufwand einer umfassenden IT-Risikobetrachtung zurückschreckt.

Grenzen der klassischen IT-Sicherheit in der Fabrik

Der Ausgangspunkt für die Absicherung von Industrieanlage ist ihre spezifische Kombination von Systemen und Komponenten. Jeder Industriebetrieb verfügt über zwei Seiten der Datenverarbeitung. Betriebliche Anwendungssysteme stellen das Rückgrat administrativer Tätigkeiten dar. Über ERP-, Groupware-, CRM- und andere Anwendungen werden betriebliche Daten- und Informationsflüsse abgebildet. Die Sicherstellung der klassischen Schutzziele Verfügbarkeit, Vertraulichkeit und

Dr. rer. pol. Christof Thim leitet das Projekt Aqua-IT-Lab an der Universität Potsdam.

cthim@lswi.de
www.lswi.de

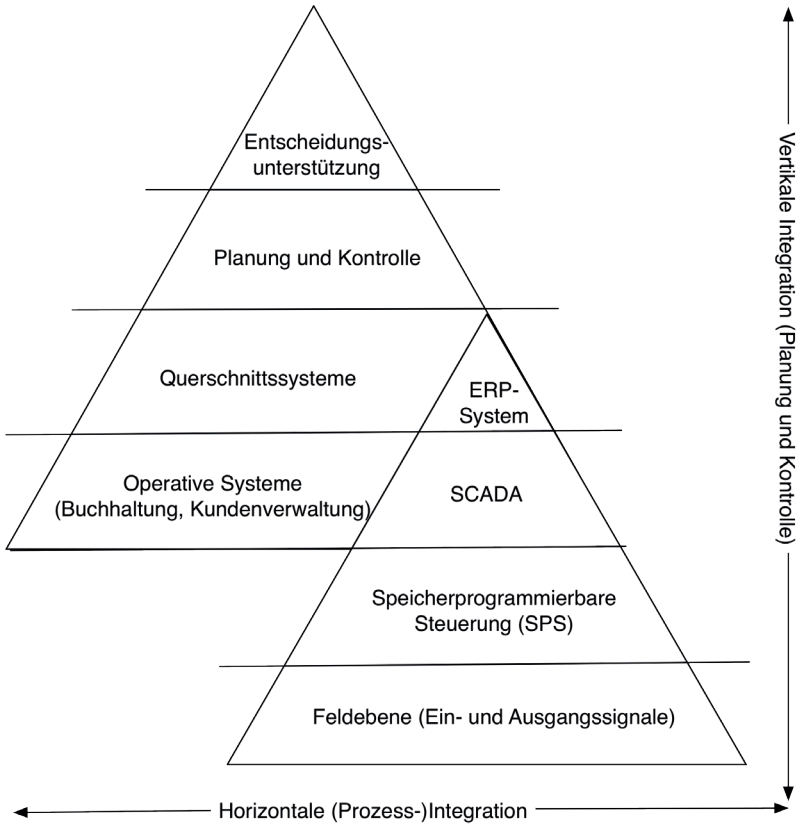

Bild 1: Automatisierungspyramiden.

Integrität [5] können dabei anhand der gängigen Maßnahmen aus der ISO27000er-Reihe [6] und dem BSI-Grundschutz [7] erreicht werden. Für Dienstleistungsunternehmen ist dies hinreichend, bei Produktionsunternehmen kommen jedoch weitere Schichten hinzu, welche im Fertigungsbereich zum Einsatz kommen. Manufacturing Execution Systeme bilden gemeinsam mit SCADA-Systemen die Schnittstellen zwischen Datenflüssen und der physischen Produkterstellung. In direkter Verbindung mit den eingesetzten Maschinen stehen speicherprogrammierbare Steuerungen, welche autonom oder teilautonom für die konkrete Verarbeitung verantwortlich zeichnen. Der Schutz physisch aktiver Komponenten wird in einem separaten Strom der Normung betrachtet, insbesondere die IEC62443 ist dabei ausschlaggebend [8]. Davon abgeleitet finden sich im deutschsprachigen Raum das ICS-Kompendium [9] und seit Neustem erste Bausteine der Automatisierungstechnik in den BSI-Standards [10]. Bild 1 zeigt die Zusammenhänge der einzelnen Ebenen.

Allen Vorgehen ist eine Risikoanalyse gemein. Diese unterscheidet sich im Detail in der Office-IT und im Industriekontext, z.B. in der Gewichtung der Bedeutung der Schutzziele. So nehmen Safety-Aspekte im Fabrikumfeld eine wesentlich höhere Bedeutung ein, als in der Büro-IT. Die Risikoanalyse verlangt jedoch in beiden Fällen eine Bewertung der Gefährdungen und der Verwundbarkeit einzelner Komponenten.

Im Forschungsprojekt, welches die Kritische Infrastruktur Wasser untersuchte, wurde die Business Impact Analyse (BIA) [11] dahingehend angepasst, dass sie die Spezifik des Wasserversorgungsprozesses berücksichtigt. Die hohen Anforderungen an die Versorgungssicherheit und die Trinkwasserqualität standen bei der Analyse im Zentrum. Hierdurch konnten die Komponenten identifiziert werden, welche zentral für die Aufrechterhaltung der Versorgung sind. Diese wurden dann im Hinblick auf ihre Verwundbarkeit gegenüber bestimmten IT-Gefährdungen bewertet und in Schutzklassen eingeteilt. Maßnahmen wurden dann schutzklassen- und komponentenspezifisch anhand der oben genannten Kataloge entwickelt. Für Industrieunternehmen bietet sich daher auch an, ihren Wertschöpfungsprozess in das Zentrum der Analyse zu stellen. Anders als im Wassersektor werden Abhängigkeiten von Produktionsplanungs- und –steuerungssystemen existieren. Daher bietet sich eine Erweiterung auf die Exponiertheit und Schnittstellen dieser Systeme an. Während die IT-Sicherheit für jede Komponente durch die oben genannten Normen gut handhabbar ist, sind es die Schnittstellen, welche häufig Schwachstellen erzeugen [12]. Zur Überprüfung, ob die Komponenten hinreichend gehärtet sind, bietet sich sowohl ein Code-Review als auch ein Penetrationstest in einer abgeschlossenen Umgebung an. Mit dem hybriden Testlabor wurden beide Ansätze im Forschungsprojekt entwickelt. Für eine detaillierte Darstellung sei auf die projektbegleitende Publikation verwiesen [13].

Von IT-Sicherheit zum Schutz von Operational Technology

Neben den konkreten, komponentenbezogenen Maßnahmen sollte die Organisation jedoch auch über eine Grundfitness in Bezug auf IT-Sicherheit verfügen. Zu diesem Zweck wurde im Aqua-IT-Lab-Projekt ein Schnelltest mit 52 Fragen entwickelt, welcher die übergreifenden Aspekte des Schutzes der Operational Technology aufgreift. Der Test wurde durch eine Analyse und Synopse der drei einschlägigen Sicherheitsstandards (ISO2700x, BSI Grundschutz, IEC62443) gewonnen und an Betreibern kritischer Infrastrukturen erprobt.

In elf Kategorien können die Verantwortlichen ihren Stand in der Umsetzung und Dokumentation von IT-Sicherheitsmaßnahmen einschät-

zen und erhalten Hinweise, in welchen Handlungsfeldern sie noch Verbesserungsbedarf haben. Die betrachteten Kategorien decken die organisatorischen Rahmenbedingungen (Verantwortlichkeit, Ressourcen, Qualifikation) ab, berühren aber auch Aspekte der Netzwerksicherheit (Zonierung, Übertragungsprotokolle, Fernwartung) und klassischen IT-Sicherheit (Umgang mit Mobilgeräten und Wechseldatenträgern, Berechtigungsmanagement, Schutz vor Schadsoftware, Schwachstellenmanagement).

Diese Maßnahmen kommen jedoch in der Steuerungstechnik an ihre Grenzen, da Komponenten über einen wesentlich längeren Zeitraum genutzt und nach ihrer initialen Programmierung nur selten angepasst werden. Patchzyklen wie sie in der Office-IT notwendig und üblich sind, lassen sich hier nicht umsetzen. Dem trägt die Kategorie des Komponentenlebenszyklus im Schnelltest Rechnung. IT-Sicherheit sollte in industriellen Umgebung daher von Anfang an, d.h. bereits in der Konzeption und Beschaffung berücksichtigt werden. Insbesondere die Kommunikation in Bezug auf die Anforderungen und die Einsatzbedingungen mit dem Lieferanten oder Integratoren sind dabei zentral. Bestimmte IT-Sicherheitsanforderungen sind als Abnahmebedingungen für die neue Komponente festzuhalten, um Inkompatibilitäten mit der bestehenden Sicherheitsarchitektur und eingesetzten Sicherheitslösungen zu vermeiden. Die Entwicklung von Steuerungscode, häufig in Kooperation mit externen Dienstleistern durchgeführt, muss zudem abgesichert erfolgen. Für den Betrieb der Automatisierungstechnik müssen klassische IT-Sicherheitsmaßnahmen weiter differenziert und ergänzt werden. So kann es z. B. zu Konflikten kommen, wenn die Steuerungskomponenten mit Virenschutz versehen werden, diese jedoch starke Echtzeitanforderungen haben oder der Hersteller keinen Virenschutz unterstützt. Es entstehen damit im Automatisierungsbereich Risiken, welche durch weitere Mitigationsmaßnahmen reduziert werden müssen. Gleiches gilt für Komponenten, die ihre Lebensdauer überschritten haben und vom Hersteller keine Aktualisierung erfahren. Der längere Betrieb von Steuerungskomponenten führt dazu, dass Legacy-Systeme im Einsatz sind, welche in separaten, höher gesicherten Zonen unterzubringen sind.

Der Übergang zwischen den Zonen ist sowohl netzwerktechnisch, z.B. über Firewalls oder Gateways oder organisatorisch, z.B. in Bezug auf Regelung zur Verwendung von Mobilgeräten oder Wechseldatenträgern, abzusichern.

Trotz aller Maßnahmen zur Absicherung der Produktionsanlage können weiterhin erfolgreiche Angriffe auftreten. Die oben genannten Maßnahmen sichern die Infrastruktur nur davor, das Opfer allzu leichter Versuche zu werden. Um den Folgen gezielter Hacks vorzubeugen, ist ein IT-Notfallmanagement notwendig, welches Recovery- und Roll-Back-Routinen vorab definiert und periodisch übt. Dies bezieht sich auf alle Elemente der Infrastruktur von betrieblichen Anwendungssystemen über Netzwerktechnik bis hin zu Automatisierungsanlagen. Der Aufbau von Redundanzen sowohl bei den eingesetzten Systemen und Komponenten als auch bei den genutzten Dienstleistern ist dabei in Betracht zu ziehen. Sollte es zu einem Zwischenfall kommen, kann so schnell auf zusätzliche Ressourcen zurückgegriffen werden.

Neben der Vorbereitung ist die Nachbereitung eines Angriffs notwendig, um das Sicherheitskonzept sukzessive zu verfeinern. Detektion und die Critical Incident Technique [14] gehen dabei Hand in Hand, um forensisch zu ergründen, wo die Schwachstellen lagen und auf

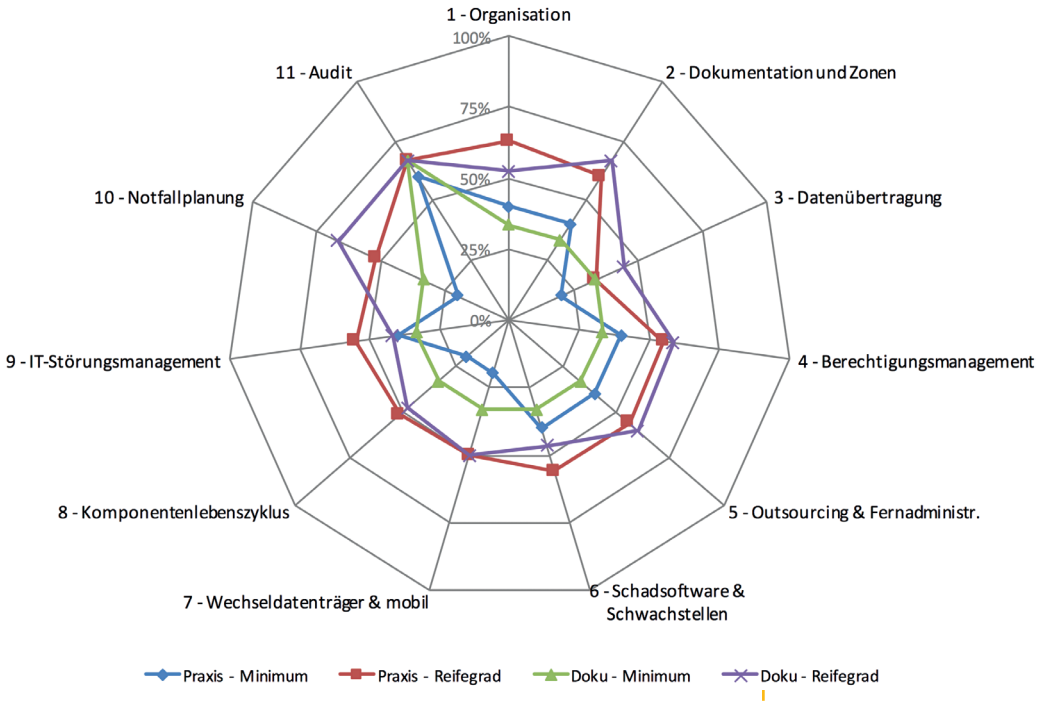

Bild 2: Beispielhaftes Sicherheitsprofil.

welchem kritischen Pfad der Angriff erfolgte. Hieran sollten sich neue Abwehr- oder Mitigationsstrategien orientieren. Ebenso sinnvoll für die Anpassung der Sicherungsmaßnahmen ist die periodische Auditierung der Anlage durch externe IT-Sicherheitsspezialisten. So können Penetrationstests und Security-Audits Schwachstellen offenbaren, welche dem internen Personal entgangen sind und welche bei ihrer Ausnutzung zu weitreichenden Folgen führen könnten.

Anwender erhalten über die 52 Fragen ein spezifisches Sicherheitsprofil, aus dem sie ihre weiteren Schritte priorisieren können (siehe Bild 2).

Dadurch, dass die Fragen und Maßnahmen im Schnelltest in weiten Teilen nicht spezifisch für den Wasserbereich sind, lässt sich dieser ohne weiteres auf Industriebetriebe übertragen. Während er für große Anlagen unterkomplex ist, bietet er jedoch kleinen und mittleren Betrieben einen schnellen Einstieg zur Absicherung ihrer Produktions-IT. Seine Nutzung kann jedoch nur der Ausgangspunkt für ein strukturiertes IT-Sicherheitsmanagement sein, welches mit entsprechenden Ressourcen und fachlichen Kapazitäten ausgestattet ist, um zukünftige Herausforderungen der IT-Sicherheit zu meistern.

Ausblick – IT-Sicherheit in der Industrie 4.0

Die oben beschriebenen Maßnahmen bilden den minimalen Stand der Technik ab. Durch die zunehmende Vernetzung und Öffnung der Produktionssysteme im Zuge der durchgehenden Digitalisierung der Produktion im Rahmen von Industrie 4.0 werden vermehrt Systeme der Produktion direkt mit dem Internet verbunden. Wie der der Zentralverband der Elektroindustrie (ZVEI) jüngst in einer Umfrage ermittelte, fehlt vielen Unternehmen jedoch Orientierung beim Thema IT-Sicherheit [15]. Obwohl auf Verbandsebene das Thema intensiv z.B. in der Allianz für Cybersicherheit, im VDI oder im ZVEI, diskutiert wird und die Erfahrung der großen beteiligten Unternehmen in die Definition von Implementierungshinweisen einfließen, haben insbesondere kleine und mittlere Produktionsunternehmen noch Nachholbedarf.

Zwar bietet das Referenzarchitekturmodell Industrie 4.0 (RAMI4.0) und die aktuellen Protokollstandards (z.B. OPC-UA) inhärente Sicherheitsüberlegungen an. Ihre Umsetzung in konkreten Projekten hängt dann aber von dem Wissen und der Sensibilisierung der Beteiligten ab.

Insbesondere die Dezentralisierung der Entscheidungsfindung in Produktionssystemen durch autonome Produktionsobjekte führt zu einer aus IT-Sicherheitssicht schwierigen Koordination der Daten und Informationsflüsse. Das Risiko, Opfer eines Angriffs zu werden, steigt dabei mit der Anzahl offener Schnittstellen und die Notwendigkeit diese konsistent abzusichern.

In der Zukunft muss sich daher das Ziel der IT-Sicherheit in zwei Punkten verschieben. Zunächst muss die Sicherheit auf Komponentenebene implementiert werden, da die klare Definition des Perimeters nicht ohne weiteres möglich ist. Es kann nicht mehr davon ausgegangen werden, dass zentrale Systeme Sicherheit bereitstellen. Vielmehr muss in der Entwicklung darauf geachtet werden, dass in der Programmierung sauber gearbeitet wird und Schwachstellen vermieden werden. Weiterhin sollte die Smartness der Industrie 4.0-Komponenten nicht nur dazu genutzt werden, Produktivitätsvorteile zu erzielen, sondern auch für die Detektion und Abwehr von Angriffen genutzt werden.

Auf der Produktionssystemebene dürfen keine zentralen und damit auch zentral angreifbaren Systeme die Produktion steuern. Vielmehr ist auf die Wandlungsfähigkeit des Produktionssystems zu achten [16]. Redundanz, Selbstorganisation und Selbstähnlichkeit sind dabei Eigenschaften, die bei der Einführung von Industrie 4.0-Technologie berücksichtigt werden müssen. Hierdurch wird zwar die Angriffsfläche nicht verkleinert, aber die Folgen des Ausfalls einzelner Systembestandteile ist kompensierbar. Folgeschäden fallen wesentlich geringer aus.

Insgesamt ist es dringend notwendig, dass die IT-Sicherheit in die Konzeption der Fabrikinfrastruktur einbezogen wird. Eine multidisziplinäre Zusammenarbeit zwischen Produktionsplanung, Fabrikgestaltung, Technologieanbietern und IT-Sicherheitsexperten ist unumgänglich, um die einzelnen Wissensinseln zu verbinden und dauerhaft sichere Fabrikumgebungen zu schaffen.

Schlüsselwörter:
IT-Sicherheit, Automatisierungstechnik, SCADA, Safety

Dieser Beitrag entstand im Rahmen des Projekts „Aqua-IT-Lab", das vom BMBF unter dem Kennzeichen 16KIS0202K gefördert wird.

Literatur

[1] Miller, B.; Rowe, D.: A survey SCADA of and critical infrastructure incidents. In: RIIT '12 Proceedings of the 1st Annual conference on Research in information technology 2012, S. 51-56.
[2] BSI: Die Lage der IT-Sicherheit in Deutschland 2014. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf, Abrufdatum 05.12.2017.
[3] BSI: Die Lage der IT-Sicherheit in Deutschland 2017. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf, Abrufdatum 05.12.2017.
[4] https://www.lswi.de/aqua-it-lab, Abrufdatum 05.12.2017.
[5] Eckert, C.: IT-Sicherheit: Konzepte – Verfahren – Protokolle. München 2006.
[6] DIN EN ISO/IEC 27001:2017-06: Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Anforderungen. 2017.
[7] BSI: Handbuch Grundschutz, Version 1.5. 2008. URL: www.bsi.bund.de/gshb, Abrufdatum 05.12.2017.
[8]I EC/TS 62443-1-1: Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models. 2009
[9] BSI: ICS Security Kompendium. 2013. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf, Abrufdatum 05.12.2017.
[10] BSI: Community Drafts: IND - Industrielle IT. 2017. URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/IT-Grundschutz-Modernisierung/GS_Drafts/IND/ind_drafts_node.html, Abrufdatum 05.12.2017.
[11] BSI: BSI-Standard 100-4: Notfallmanagement. Bonn, 2008.
[12] BSI: Industrial Control System Security Top 10 Bedrohungen und Gegenmaßnahmen 2016. URL: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_005.pdf, Abrufdatum 05.12.2017.
[13] Thim, C.; Kotarski, D.; Arndt, S. :Aqua-IT-Lab – eine Testumgebung für Penetrationstests im Wassersektor. In: energie-wasser-praxis, 12/2017.
[14] Flanagan, J. C.: The critical incident technique. In: Psychological Bulletin 51 (1954) 4, S. 327-358.
[15] ZVEI e.V. (Hrsg.): Cybersicherheit: Wie sich die Automationsbranche schützt. Frankfurt, 2016.
[16] Gronau, N.; Weber, E.: Wandlungsfähigkeit: Generische Strategien zur Handhabung von Veränderungen in der Umwelt. Potsdam 2009.