AWK FOKUS

Juni 2013 Eine Fachpublikation der AWK GROUP www.awk.ch

Vom Global Village zur Sin City?

André Arrigoni
Partner AWK Group

Täglich lesen wir von neuen Schadensfällen, Spionageversuchen und Datendiebstählen. Wir erkennen, dass die den neuesten Bedrohungen oft hinterher hinkenden technischen Gegenmassnahmen und die Gesetzgebung nur stumpfe Waffen sind gegen die aus dem scheinbar rechtsfreien Cyber-Space agierenden Angreifer.

Neben dem unbestreitbar gewaltigen Nutzen, den das Internet gebracht hat, entwickelt es sich auch immer mehr zu einer Brutstätte neuer Bedrohungen und zum Tummelfeld von Kriminellen.

Zusätzlich rückt es immer mehr ins Visier von Streitkräften und Geheimdiensten. Spezialisierte Einheiten und Dienste in vielen Ländern betreiben via Internet elektronische Spionage – und dies nicht nur bei staatlichen Institutionen, sondern auch bei privaten Unternehmen.

Das Internet – einst zum *Global Village* stylisiert – hat eher Ähnlichkeit mit einer gefährlichen Megacity, deren Besucher besser auf der Hut sein sollten!

Herzlich, Ihr

Cyber-Security – aktuelle Trends und Schutzmassnahmen

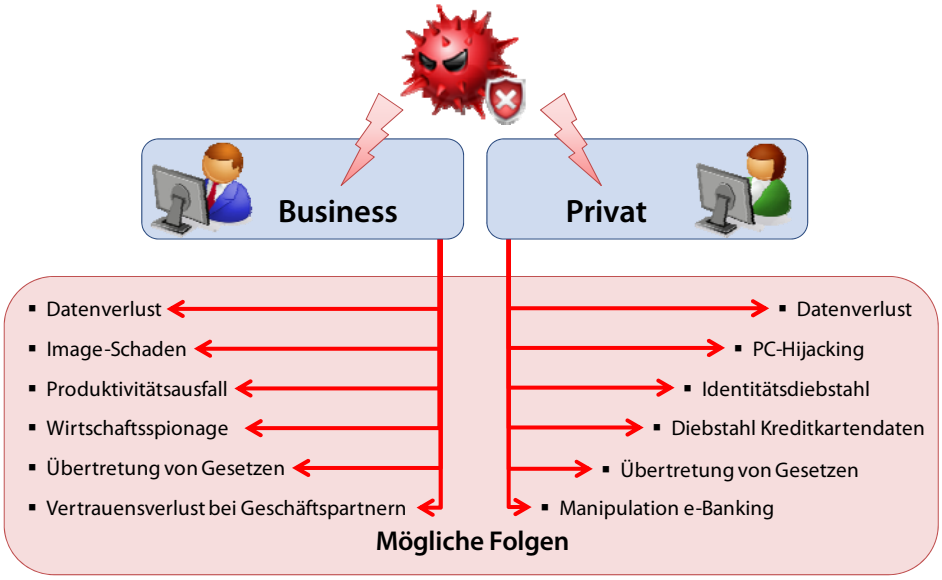
Informations- und Kommunikationsinfrastrukturen haben Wirtschaft, Staat und Gesellschaft grundlegend verändert. Die Nutzung des Cyber-Space (Internet und damit verbundene lokale Netze) bringt viele Vorteile und Chancen mit sich. Allerdings hat die digitale Vernetzung auch neue Bedrohungen geschaffen. Informations- und Kommunikationsinfrastrukturen werden für kriminelle, nachrichtendienstliche oder terroristische Zwecke missbraucht. Die Cyber-Security muss deshalb Einzug ins Risikomanagement unserer modernen Informationsgesellschaft finden.

Dr. Adrian Marti, Dr. Philipp Grabher, Tarkan Bas

Immer mehr Dienstleistungen werden heute über elektronische Kanäle angeboten und genutzt. Die Bedeutung des Internets für Staat, Wirtschaft und Gesellschaft nimmt stetig zu und damit auch unsere Abhängigkeit vom Internet als kritische Kommunikationsinfrastruktur.

Die Bedrohung von Privatpersonen, Wirtschaft und staatlichen Behörden durch Cyber-Risiken ist durchaus real:

- Hacker dringen ins EDA-Netzwerk ein (Mai 2012) [1]
- Hunderttausende Patientendaten in Deutschland sind verschwunden (Oktober 2012) [2]
- Operation „Roter Oktober“: Gross angelegter Spionage-Angriff über das Internet auf diplomatische Vertretungen, Regierungsorganisationen und Forschungsinstitute aufgedeckt (Januar 2013) [3]



Cyber-Angriffe und mögliche Folgen

Standards und Good Practices

ISO 27001:2005
Definiert ein Informations-Sicherheits-Management-System ISMS. Kernstück ist der kontinuierliche Verbesserungsprozess und die 134 Kontrollpunkte zur Steuerung der Informationssicherheit.

ISO 27032
Definiert „Guidelines for Cyber-Security" mit Kontrollpunkten zur Bewältigung von Cyber-Risiken. Der zweite Teil enthält Empfehlungen zur Zusammenarbeit der unterschiedlichen Stakeholder zur Steigerung der Cyber-Security.

ITIL V5
Die IT Infrastructure Library hat sich als De-facto-Standard für das Management operativer IT-Services durchgesetzt. Im Sicherheitsbereich werden in ITIL die Themen Security Management, Continuity Management und Availability Management angesprochen.

CMM
Mit Hilfe von Capability Maturity Modellen lässt sich die Reife von Prozessen und Organisationen messen. Da Sicherheit sehr stark mit der Reife von Organisationen und Prozessen verknüpft ist, lassen sich Maturity-Modelle in diesem Bereich sehr gut anwenden.

BSI-Grundschutzkataloge und Standards, ISF Good Practices usw.
Es existieren zahlreiche interessante Good Practices der IT- und Informationssicherheit, die im Bereich der Cyber-Security sinnvoll eingesetzt werden können.

Prävention: Technische Schutzmassnahmen allein genügen nicht

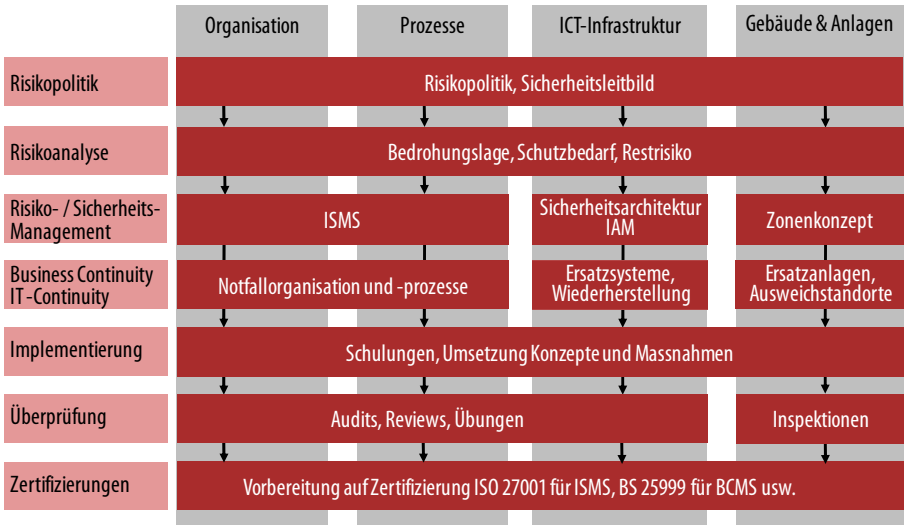
Es gibt viele Gründe, weshalb Cyber-Angriffe erfolgreich sind:

- Das Internet ist eine offene, sich in stetigem Wandel befindliche Infrastruktur ohne zentrale Kontrollinstanz.
- Die zunehmende Vernetzung von Systemen erhöht die Komplexität und schafft immer wieder neue Sicherheitslücken.
- Neue Schnittstellen bringen bislang abgeschottete Systeme mit dem offenen Internet in Verbindung.
- Der hohe Innovations- und Wettbewerbsdruck führt dazu, dass Software oft unausgereift und mit Sicherheitsmängeln in Betrieb geht.
- Die von den einzelnen Akteuren im Cyber-Space getroffenen Sicherheitsmassnahmen sind selten aufeinander abgestimmt.
- Benutzer verfügen oft über ein geringes Sicherheitsbewusstsein.

Um die Cyber-Security zu verbessern, muss somit auf mehreren Ebenen angesetzt werden:

- Risiko- und Sicherheit-Frameworks sowie Sicherheit-**Standards** müssen kontinuierlich angepasst und weiterentwickelt werden (z.B. ISO 27032 "Guidelines for Cybersecurity International Standard").
- **Betreiber kritischer Infrastrukturen** müssen das Thema Cyber-Security in ihre Risikoüberlegungen einbeziehen. Notwendig ist insbesondere ein effizienter und effektiver Informationsaustausch, Koordination und Incident-Handling zwischen den Partnern im Cyber-Space.
- **Firmen und Verwaltungen** müssen sich dem Risiko Cyber-Kriminalität stellen. Ein Risiko- und Sicherheitsmanagement ist gemäss geltenden GoodPractices aufzubauen und zu betreiben.
- Die Konzentration auf Massnahmen technischer Natur reicht nicht aus, um den Bedrohungen aus dem Cyber-Space begegnen zu können. **Endbenutzer** müssen durch Schulungen und Sensibilisierungskampagnen über zu befolgende Verhaltensregeln aufgeklärt werden.

Das Sicherheitsframework von AWK hilft den Sicherheitsverantwortlichen im Unternehmen, die risikobehafteten Bereiche zu identifizieren und entsprechende Gegenmassnahmen zu definieren.



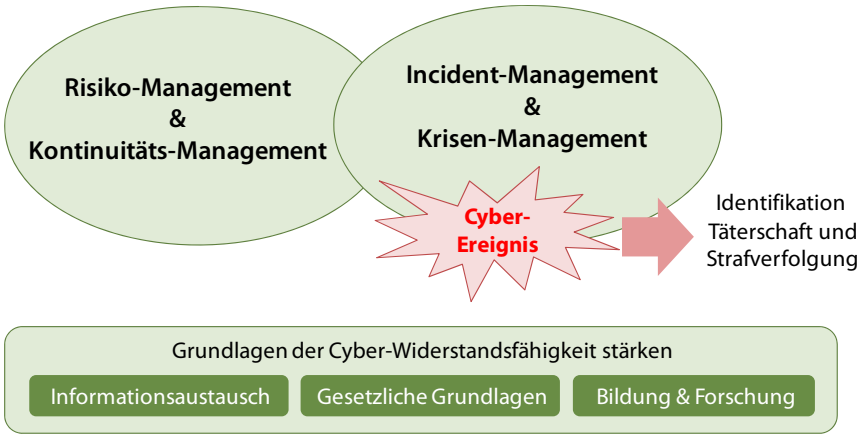
Sicherheitsframework von AWK

Cyber-Security: Mit Public Private Partnership zum Ziel

Der Bundesrat verabschiedete am 27. Juni 2012 die nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) und beauftragte die Departemente, die Umsetzung der Massnahmen in ihrem Bereich und im Verbund mit den kantonalen Behörden und der Wirtschaft in die Hand zu nehmen.

Mit der NCS verfolgt der Bundesrat die folgenden strategischen Ziele:

- Die frühzeitige Erkennung der Bedrohungen und Gefahren im Cyber-Space
- Die Erhöhung der Widerstandsfähigkeit von wichtigen Infrastrukturen, von denen die Sicherheit, der Wohlstand und die Stabilität der Schweiz abhängen
- Die wirksame Reduktion von Cyber-Risiken, insbesondere Kriminalität, Spionage und Sabotage



Kernelemente zur Umsetzung der nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)

AWK unterstützte das Informatiksteuerungsorgan Bund bei der Erarbeitung der Planung zur Umsetzung der NCS. Neben einem Massnahmen- und Terminplan mit zugewiesenen Verantwortlichkeiten galt es, ein gemeinsames Verständnis aller Beteiligten, ihrer Rollen und der Aufgabenverteilung im Zusammenhang mit dem Risiko-, Kontinuitäts-, Incident- und Krisenmanagement zu schaffen. Die Einbettung der NCS in den Kontext der nationalen Strategie zum Schutz kritischer Infrastrukturen (SKI) wurde sichergestellt. Getreu dem Modell der *Public Private Partnership* wurden diverse Akteure aus Bund, Kantonen und Privatwirtschaft in einem übergreifenden Lösungsansatz eingebunden, so dass diese gemeinsam die Widerstandsfähigkeit der Schweiz gegenüber Cyber-Risiken stärken.

Die NCS unterstützt den Grundsatz der Eigenverantwortlichkeit: Jeder Akteur ist selbst für die Analyse seiner Risiken- und Verwundbarkeiten und auch für ein angemessenes Kontinuitäts- und Krisenmanagement verantwortlich.

Am 15. Mai 2013 hat der Bundesrat den NCS-Umsetzungsplan verabschiedet und den Steuerungsausschuss NCS damit beauftragt, die Umsetzung der Massnahmen zu koordinieren. Dieser Steuerungsausschuss hat auch die Aufgabe, die Entwicklung der Cyber-Risiken zu verfolgen und dem Bundesrat Empfehlungen für die Weiterentwicklung der Strategie vorzulegen.

Internationale Bemühungen im Bereich Cyber-Security

Europäische Union: Im Februar 2013 publizierte die EU das lang erwartete Cyber-Security-Dossier. Dieses beinhaltet Richtlinien und Massnahmen „zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit der Union". Die Strategie der Europäischen Union fokussiert sich bei der Erhöhung der Sicherheit und Widerstandsfähigkeit auf die Stärkung von technischen Komponenten (ICT-Produkte usw.).

Deutschland: Zivile Ansätze und Massnahmen stehen bei der deutschen Cyber-Sicherheitsstrategie im Vordergrund. Sie werden durch die Massnahmen der Bundeswehr ergänzt.

Grossbritannien: Die englische Regierung stellt ein Budget von 650 Mio. Pfund für die Etablierung eines neuen „National Security Cyber-Program" zur Verfügung. Die Umsetzung unterliegt dem britischen Geheimdienst GSHQ und soll innerhalb der nächsten vier Jahre erfolgen.

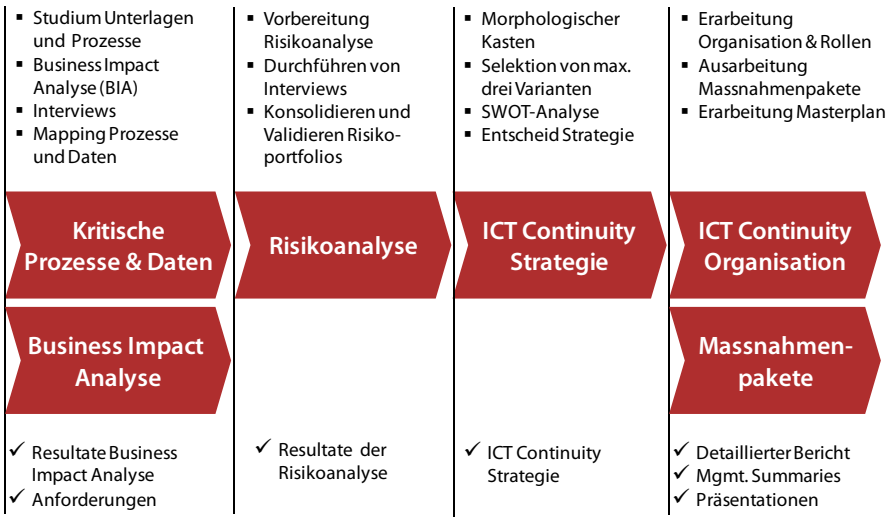
USA: Das amerikanische Verteidigungsministerium plant die Abteilung für Cyber-Security im Jahr 2014 massiv aufzustocken, von derzeit 900 Mitarbeitern auf 4900. Des Weiteren ist vorgesehen, schwere Cyber-Attacken in Zukunft als kriegerischen Akt einzustufen.

Im Ernstfall: ICT Continuity sorgt für die Aufrechterhaltung wichtiger Geschäftsprozesse

Wichtige Geschäftsprozesse in Unternehmen hängen mehr denn je von der Verfügbarkeit der ICT-Infrastruktur ab. Gezielte Angriffe auf die ICT-Infrastruktur werden typischerweise über Landesgrenzen hinweg koordiniert und lassen sich daher nur bedingt durch nationale Gesetzesvorschriften bekämpfen.

Denial-of-Service (DOS) Angriffe stellen derzeit eine der grössten Bedrohungen für die ICT-Infrastruktur eines Unternehmens dar. Durch eine Flut von Anfragen wird die ICT-Infrastruktur überlastet bis diese ausfällt. Technische Lösungen zur Abwehr solcher Angriffe sind leider oft unzureichend.

Um für den Ernstfall vorbereit zu sein, ist die Durchführung einer ICT Continuity Analyse zu empfehlen. Mit Hilfe dieses Prozesses können frühzeitig potenzielle Auswirkungen von Ausfällen der ICT-Infrastruktur, die eine Bedrohung für das Unternehmen darstellen, erkannt und behandelt werden. Das Resultat ist ein Massnahmenkatalog, der es im Krisenfall ermöglicht, die geschäftskritischen Prozesse weiterzuführen bzw. nach einer vorgeschriebenen Zeit wieder aufzunehmen. Dies kann die Stabilität eines Unternehmens entscheidend verbessern.



AWK-Vorgehen für ICT Continuity Management

AWK hat schon viele Organisationen und Unternehmen im Bereich ICT Continuity Management unterstützt. Ein prominentes Beispiel ist der Verband Schweizerischer Elektrizitätsunternehmen (VSE): AWK half mit bei der Erarbeitung einer Branchenempfehlung[4] für die kritischen ICT-Infrastrukturen der Elektrizitätsunternehmen. Ziel war es, die Widerstandsfähigkeit der Elektrizitätsversorgung gegen Cyber-Ereignisse zu stärken und damit die Versorgungssicherheit für Staat, kritische Infrastrukturen, Wirtschaft und Private im Krisenfall bestmöglich sicherzustellen.

Quellen:
[1] Hackerangriff auf das EDA, www.computerworld.ch, Mai 2012
[2] Patientendaten aus Klinikum Mittelbaden verschwunden, www.haufe.de, Oktober 2012
[3] Operation Roter Oktober, www.kaspersky.com, Januar 2013
[4] Verband Schweizerischer Elektrizitätsunternehmen, Branchenempfehlung Strommarkt Schweiz zum Thema ICT Continuity, www.strom.ch, Dezember 2011

Die Autoren

Adrian Marti
Bereichsleiter,
Dr. phil. nat., EMBA,
CISM, CRISC

Adrian Marti ist bei AWK verantwortlich für den Kompetenzbereich Informationssicherheit

Philipp Grabher
Consultant,
PhD Computer Security,
Dipl.-Ing.

Philipp Grabher ist bei AWK Experte für Kryptographie und Sicherheits-Protokolle

Tarkan Bas
Senior Consultant,
Dipl. El.-Ing. ETH,
CISM, CISA

Tarkan Bas ist bei AWK Experte für Risk Assessments und Security Audits.

Über die AWK Group

AWK ist mit rund 130 Mitarbeitenden eines der grössten Schweizer Beratungsunternehmen für Informationstechnologie.

Wir sind schweizweit tätig mit Standorten in Zürich, Bern und Basel.

Unsere Dienstleistungen umfassen Consulting, Engineering und Projektmanagement.

AWK GROUP
Consulting | Engineering | Project Management

www.awk.ch