Bundesamt für Verfassungsschutz

ASW Bundesverband

Neue Businessmodelle und Industrie im Wandel – Chancen und Risiken für die Unternehmenssicherheit

11. Sicherheitstagung des BfV und ASW Bundesverbandes am 27. April 2017 in Berlin

Deloitte.

POWER PERSONEN-OBJEKT-WERKSCHUTZ GMBH

Durchgeführt von ASW

Neue Businessmodelle und Industrie im Wandel – Chancen und Risiken für die Unternehmenssicherheit

11. Sicherheitstagung BfV und
ASW Bundesverband am 27. April 2017
in Berlin

Tagungsband

Inhaltsverzeichnis

11. Sicherheitstagung des BfV und ASW-Bundesverbandes am 27. April 2017 in Berlin

BfV-Präsident Dr. Hans-Georg Maaßen und der ASW-Vorsitzende Volker Wagner

Mehr als 130 Gäste, darunter zahlreiche Experten aus Wirtschaft, Sicherheitsbehörden und Wissenschaft nahmen am 27. April 2017 in der Bundesakademie für Sicherheitspolitik (BAKS) in Berlin an der 11. Sicherheitstagung des Bundesamtes für Verfassungsschutz und der Allianz für Sicherheit in der Wirtschaft e.V. - ASW Bundesverband teil.

Unter der Überschrift „Neue Businessmodelle und Industrie im Wandel - Chancen und Risiken für die Unternehmenssicherheit“ standen dieses Mal die unterschiedlichen Aspekte des digitalen Transformationsprozesses im Vordergrund. Dieser ist für zahlreiche Unternehmen längst Realität und hat daher unmittelbare Auswirkungen auf den Bereich des Wirtschaftsschutzes.

Entsprechend vielfältig waren die unterschiedlichen Vorträge und Workshops ausgerichtet, die Chancen und Risiken des digitalen Wandels beleuchteten:

Ob neue Herausforderungen durch den Einsatz von Künstlicher Intelligenz, Fragen der Authentifizierung von Daten, das autonome Fahren im „Connected Car“, Notfallmanagement oder die rechtlichen und tatsächlichen Auswirkungen der neuen Know-how-Schutz-Richtlinie der Europäischen Union - die BfV/ASW-Sicherheitstagung verdeutlichte einmal mehr, dass die Bedeutung hochdynamischer Entwicklungen im Bereich der Digitalisierung für einzelne Sicherheitsfelder, aber auch der angemessene Umgang mit konkreten Sicherheitsrisiken ein weites wie komplexes Feld sind.

Begrüßung und Keynote Digitalisierung und Vernetzung als eine Transformationsphase mit Chancen und Risiken

Dr. Hans-Georg Maaßen, Präsident Bundesamt für Verfassungsschutz

1. Begrüßung und Einleitung

Sehr geehrter Herr Dr. Kamp,

sehr geehrter Herr Wagner,

sehr geehrte Vertreterinnen und Vertreter der Medien,

meine sehr geehrten Damen und Herren,

herzlich willkommen zur 11. Sicherheitstagung des BfV und ASW Bundesverbandes in der Bundesakademie für Sicherheitspolitik. Ich freue mich, dass Sie unserer Einladung gefolgt sind.

Mein besonderer Gruß gilt allen unseren internationalen Gästen: Vielen Dank für Ihr Interesse an unserer Tagung, und herzlich willkommen in Berlin!

Das Thema der diesjährigen Sicherheitstagung könnte spannender kaum sein: „Neue Businessmodelle und Industrie im Wandel – Chancen und Risiken für die Unternehmenssicherheit".

Dieses Thema fordert eine technische Betrachtung ebenso wie eine philosophische. Denn gespannt wird ein thematischer Bogen zwischen dem, was heute bereits technisch machbar ist, und dem, was für die Zukunft vorstellbar ist. Wir beschäftigen uns heute also auch mit der Frage, wo die Grenzen des Vorstellbaren wohl liegen könnten.

2. Transformationsphase / Daten als neuer Rohstoff

Fest steht: Wir erleben eine Transformationsphase durch die Digitalisierung. Der Begriff des „historischen Ereignisses" ist immer schnell bemüht. Aber ich bin tatsächlich davon überzeugt, dass wir Zeitzeugen einer Entwicklung sind, die nichts so hinterlässt, wie sie es vorgefunden hat.

Die Digitalisierung beschert uns nicht nur einen umfassenden Komfort- und Unterhaltungsgewinn, sondern auch neue Verwundbarkeiten und eine neue Währung samt Rohstoff in einem: Daten.

Denken Sie beispielsweise an den Goldrausch in den USA im 19. Jahrhundert oder an die New Economy um die Jahrtausendwende vor 17 Jahren: Wenn etwas Neues entdeckt wird, mit dem sich viel Geld verdienen lässt,

entsteht sehr schnell eine unkontrollierbare Euphorie, in der zunächst das Recht des Stärkeren gilt, und in der – gleichsam – die Karten neu gemischt werden.

So verhält es sich auch mit den Daten, die die Digitalisierung hervorbringt! Gemäß der Maxime des englischen Philosophen Francis Bacon, nach der Wissen Macht ist, ist schnell erklärt, weshalb Daten Macht bedeuten: Weil Daten, die analysiert wurden, ein Wissen darstellen. Wer Daten hat, hat also Macht! Und wir erleben, wie momentan Macht und Einfluss neu verteilt werden.

3. Bedeutung der Digitalisierung für Qualitätsmedien

Die Vertreterinnen und Vertreter der Medien können davon – zweifelsohne – ein Lied singen:

Den seriösen Qualitätsmedien kommt aus Sicht des Verfassungsschutzes eine bedeutsame Rolle für das Funktionieren unserer Verfassungsordnung zu. Nur wenn die Bürger in der Lage sind, sich auf wahrhaftige und vollständige Informationen und kompetente Kommentare zu verlassen, können sie sich fundiert eine eigene Meinung bilden und sachlich an politischen Entscheidungen mitwirken – so die Theorie!

Wenn die Bürger jedoch dubiosen Internetquellen den Vorzug vor den Qualitätsmedien geben, können sie zum Spielball werden – beispielsweise durch Desinformation.

Schon längst konkurrieren neue Medienformate mit traditionellen Medien. US-Präsident Trump ist ein Beispiel dafür: Er hat gezeigt, was „Twitter-Politik“ bedeutet: nämlich eine zusätzliche Steigerung der Schlagzahl unserer Informationsgesellschaft. Tatsachen und Meinungen vermischen sich, während die Nachrichtenflut nicht mehr sortiert und priorisiert wird, sondern befeuert, emotionalisiert und skandalisiert – auch mit Falschinformationen.

Um bei dieser Nachrichtenflut mitmachen zu können, müssen Sie kein US-Präsident sein! Als Besitzer eines Smartphones oder eines Facebook-Accounts sind Sie ermächtigt, an globaler Kommunikation in Echtzeit teilzunehmen. Viel mehr noch: Sie können selbst Gründer einer digital initiierten Gemeinschaft werden.

Die heutigen „User“ konsumieren nicht mehr passiv Leitmedien, welche Nachrichten und Informationen vorsortieren; sondern sie produzieren selbst aktiv Informationen und Botschaften, die sie ohne Umwege ins Netz speisen.

Es liegt auf der Hand, dass dieser Umstand ein Einfallstor für professionelle Einflussnahme und Manipulation ist. Sogenannte Internet-Trolle agitie-

ren bekanntlich massenhaft in Kommentarspalten des Online-Journalismus oder in sozialen Netzwerken – beispielsweise mit pro-russischer Propaganda.

Gerade liberal-demokratische Gesellschaften – wie die unsere – bieten durch ihre offene Diskurskultur und den gewollten Meinungspluralismus eine sehr breite Flanke für Desinformationskampagnen.

4. Chancen einer Transformation: Beispiel Industrialisierung

Aber kommen wir zurück zum Phänomen der Transformationsphase: Wie gewaltig eine solche sein kann, wird deutlich, wenn wir auf die Entwicklungen der Wirtschaft in Deutschland und Europa zurückschauen, und zwar seit dem Beginn der industriellen Revolution vor ungefähr 150 Jahren.

Als die ersten industriellen Produktionsstätten in den Ballungsräumen errichtet wurden, waren Arbeitnehmer gezwungen, unter den widrigsten Umständen ihr Tagewerk zu verrichten – nicht selten unter Gefahr für Leib und Leben und mit einer sozialen Unsicherheit, die sich für die wenigsten Menschen in eine aussichtsreiche Perspektive wandelte.

Im Laufe der Jahrzehnte hat sich dies völlig geändert. Nicht zuletzt durch die Schöpfungskraft der deutschen Industrie und der hohen Innovationsfähigkeit der Unternehmen ist die Situation der Arbeitnehmer heute komplett anders – und sie entwickelt sich ständig fort:

Zumindest in der westlichen Welt müssen Menschen bei weitem nicht mehr ein solch hohes Risiko für sich – oder auch die Umwelt – zum Erwerb ihres Einkommens eingehen. Mit dem industriellen Wandel der vergangenen Jahre hat sich auch der Begriff „Arbeit“ massiv geändert. Das sind eine Errungenschaft und ein Erfolg für die Menschheit!

Und wie entsteht so etwas?

Meine sehr geehrten Damen und Herren,

die deutsch-schwedische Literatur-Nobelpreisträgerin Nelly Sachs hat einmal geschrieben: „Alles beginnt mit der Sehnsucht!“

Ganz gewiss haben die Sehnsucht – oder wir können hier auch von Bedürfnis sprechen – nach Fortschritt, nach Teilhabe, sozialem Frieden und Freiheit genauso wie das Bedürfnis nach wirtschaftlichem Wachstum und Profit gleichermaßen ihre Wirkung an dem Wandel der Wirtschaft entfaltet und Menschen dazu verleitet, diesen Wandel zu gestalten und voranzutreiben.

Dieser Wandel hört nicht auf, solange genau diese Sehnsüchte und Bedürfnisse nicht aufhören!

5. Risiken der Digitalisierung

Heute reden wir über die „digitale Revolution“ und die „Industrie 4.0“. Hierzu bedienen wir uns einer IT-basierten Technik, die uns noch mehr Effizienz, noch mehr Wachstum und Profit sowie noch mehr Fortschritt verspricht.

Es stehen uns elektronische Mittel zu Verfügung, die es uns ermöglichen, eine für den bloßen menschlichen Verstand nicht leistbare Komplexität zu erfassen und weiterzudenken – bis hin zur künstlichen Intelligenz.

Auch hier beobachten wir eine nahezu grenzenlose Euphorie; wir sind begeistert von der Technik. Scheinbar ist alles machbar: von Formen direkter Demokratie übers Internet bis hin zu “eGovernement”. Nur leider geraten die Schattenseiten – die Folge- und Nebenwirkungen – dabei zu schnell aus dem Blickfeld.

Das gilt vor allem im Hinblick auf das Thema „künstliche Intelligenz“. Wir spüren: Hier wird eine Schwelle in eine neue Zeit überschritten. Bislang waren IT-gestützte Techniken vielleicht für Außenstehende komplex und weniger nachvollziehbar. Aber sie waren für IT-Spezialisten immer noch beherrschbar.

- Nur wie lange wird diese Technik beherrschbar bleiben?
- Was bedeutet „künstliche Intelligenz“? Laufen wir hier Gefahr, unsere Autonomie aufzugeben und aus einem vermeintlichen Fortschritt ein unkalkulierbares Risiko zu machen? – Aus Blockbustern kennen wir solche Horror-Szenarien bereits.

Meine sehr geehrten Damen und Herren,

allein diese Fragen verdeutlichen uns: Der Mensch hat auch ein elementares Bedürfnis nach Sicherheit – nicht nur nach Profit und Komfort. Und dieses Bedürfnis nach Sicherheit existiert nicht grundlos!

Von der „künstlichen Intelligenz“ einmal abgesehen, wissen wir: Wo es etwas zu verteilen gibt, wachsen die Begehrlichkeiten – da haben auch Dritte „Bedürfnisse“ und wollen von fremden Früchten profitieren.

In der Folge kommt es dann zu Wirtschaftsspionage durch ausländische Nachrichtendienste oder Konkurrenzausspähung durch Mitbewerber. Es kommt zu Cyber-Angriffen oder Cyber-Sabotage mit dem Ziel, einem Unternehmen zu schaden oder sich dessen Know-how unter den Nagel zu reißen.

Desinformationskampagnen – zum Beispiel – sind Ausdruck solcher Begehrlichkeiten: Sie drohen Staat, Wirtschaft und Gesellschaft gleichermaßen mit dem Entzug von validen Entscheidungsgrundlagen für ihr jeweiliges Handeln.

So besteht die Gefahr der Einflussnahme durch fremde Mächte, wenn die Bürger durch bewusste Falschinformationen zu Handlungen und Entscheidungen bewegt werden, die sich nachteilig auf die Souveränität in unserem Land auswirken. Konflikte und Instabilität können durch Fake News und gezielt eingesetzte Propaganda verschärft oder herbeigeführt werden.

Ein Beispiel dafür ist die kommende Bundestagswahl in Deutschland: Die Hinweise auf Versuche einer Beeinflussung verdichten sich. Wir erwarten einen weiteren Anstieg von Cyberangriffen im Vorfeld der Wahl und haben diese Bedrohung sehr genau im Blick. Wir sensibilisieren und klären weiter auf.

Der Cyber-Raum hält aber noch mehr Gefahren bereit:

- Er bietet ein Aktionsfeld für Terroristen und Extremisten, die dort ganz neue Möglichkeiten für sich entdecken. Der IS hat bereits mehrfach Cyberattacken angekündigt und sucht nach Hackern dafür.
- Der Cyber-Raum ist durch seine Anfälligkeit ein Hoch-Risiko-Raum. Ich erinnere an die Angriffe auf das DLR, auf Yahoo, Sony, TV5 Monde, den Deutschen Bundestag oder die Demokratische Partei der USA.
- Angriffe auf unsere kritischen Infrastrukturen sind in einer immer stärker vernetzten Umgebung realistisch und können – im Extremfall – zum Entzug unserer Lebensgrundlagen führen. Bereits geschehen ist das in einem ukrainischen Kraftwerk, und in der Folge waren 700.000 Menschen über einen längeren Zeitraum ohne Strom. Stellen Sie sich einmal vor, eine Stadt wie Frankfurt am Main wäre für längere Zeit ohne Strom!

Und all das ist noch lange nicht das Ende der Fahnenstange:

Man möchte sich gar nicht vorstellen, wenn durch einen Cyber-Angriff selbstfahrende Autos durch Manipulation Jagd auf Passanten machten oder wenn mit dem Internet verbundene Herzschrittmacher abgeschaltet würden. Man möchte es sich nicht vorstellen, man sollte es aber!

Denn dann wird uns klar, dass wir gemeinsam daran arbeiten sollten, allen Bedürfnissen zu dienen: Fortschritt und Sicherheit.

6. Lösung: Vertrauensvolle Zusammenarbeit

Meine sehr geehrten Damen und Herren,

eine solche gemeinsame Arbeit findet zwischen der „Allianz für Sicherheit in der Wirtschaft“ und dem Bundesverfassungsschutz sowie den weiteren

Sicherheitsbehörden des Bundes und der Länder statt. Exemplarisch dafür steht diese Sicherheitstagung.

Die für die Tagung ausgewählten Themen, Workshops und Vorträge sprechen aus Sicht meiner Behörde nicht nur genau die richtigen Themen zur richtigen Zeit an, sondern sie wecken gleichzeitig unsere Neugier und richten unsere Aufmerksamkeit auf aktuelle Entwicklungen. Den Sicherheitsbehörden gibt die Tagung wiederum eine Gelegenheit, ihre Expertise einzubringen und sich ein Feedback einzuholen.

Wenn wir weiterhin so eng und vertrauensvoll im Sinne eines aktiven Wirtschaftsschutzes zusammenarbeiten, bestehende Schutzkonzepte fortentwickeln sowie neue Risiken rechtzeitig wahrnehmen, haben wir eine gute Chance, den Schutz von Know-how und Innovationen unserer deutschen Wirtschaft zu erhalten und auszubauen!

So werden wir auch den beschriebenen Bedürfnissen gerecht. Die Bürger wie die Unternehmen haben ein gewisses Vertrauen in die Digitalisierung und Vernetzung: Sie betrachten sie als selbstverständlichen Teil ihres Alltags. Ich sehe unsere Aufgabe darin, dafür zu sorgen, dass für den Cyber-Raum das bestmögliche Maß an Sicherheit und Schutz gelten.

Diese Tagung wird einen Beitrag dazu leisten!

Vielen Dank für Ihre Aufmerksamkeit.

Begrüßung und Eröffnung

Volker Wagner, Vorsitzender ASW Bundesverband

Sehr geehrte Präsidenten,

lieber Herr Dr. Kamp, lieber Herr Dr. Maaßen,

Liebe ASW Mitglieder, Vertreter der Wirtschaft und der Sicherheitsbehörden, sehr geehrte Medien- und Pressevertreter, verehrte Gäste!

Ich freue mich, Sie heute hier auf unserer 11. Sicherheitstagung des Bundesamtes für Verfassungsschutz und des ASW Bundesverbandes begrüßen zu dürfen.

Für mich als überzeugten Absolventen der Bundesakademie ist es eine besondere Ehre und Freude, Sie heute hier bei der BAKS willkommen zu heißen. Ich durfte bereits zweimal an der intensiven Ausbildung der BAKS teilnehmen. Keine Sorge, ich war nicht durchgefallen und musste auch nicht wiederholen. Im Jahr 2010 durfte ich am Kernseminar für Sicherheitspolitik und letztes Jahr am Führungskräfteseminar mit dem Schwerpunkt China teilnehmen. Ich finde, mit Blick auf unsere heutige Agenda, ist es uns schon sehr gut gelungen, das Leitprinzip der BAKS zur Sicherheitspolitik – Sicherheitspolitik muss 1. umfassend, 2. vernetzt und 3. strategisch gestaltet werden – in die Praxis umzusetzen. Denn unser Leitthema für den heutigen Tag lautet:

Neue Businessmodelle und Industrie im Wandel – Chancen und Risiken für die Unternehmenssicherheit

Aus meiner Sicht müssen im sogenannten Cyber Zeitalter die Prinzipien der Sicherheitspolitik - umfassend, strategisch und vernetzt - noch um eine weitere Komponente ergänzt werden – um die Komponente der Digitalisierung.

Schauen wir uns dazu einige Anwendungsbeispiele für neue Businessmodelle an:

Beispiel 1: Umweltüberwachung

Anwendungen zum Umweltmonitoring verwenden typischerweise Sensoren, um den Umweltschutz durch die Messung von Luft- oder Wasserqualität, Atmosphäre oder Bodenverhältnissen zu überprüfen und können sogar Bereiche umfassen, die die Bewegungen von Wildtieren und ihren Lebensräumen überwachen.

Beispiel 2: Infrastrukturmanagement

Hier geht es um die Steuerung von städtischen und ländlichen Infrastrukturen wie Brücken, Bahngleisen, On- und Offshore-Windparks.

Beispiel 3: Produktion

Die intelligenten IoT-Systeme ermöglichen eine schnellere Fertigung neuer Produkte, eine dynamische Reaktion auf Produktanforderungen und eine Echtzeit-Optimierung von Fertigungs- und Supply-Chain-Netzwerken durch Vernetzung von Maschinen, Sensoren und Steuerungssystemen.

Beispiel 4: Energiemanagement

Optimierung des Energieverbrauchs, der Energieverteilung sowie der Energieerzeugung durch Smart Grids.

Beispiel 5: Medizin und Gesundheitswesen

IoT-Geräte können genutzt werden, um Fernüberwachungs- und Notfall-Benachrichtigungssysteme zu ermöglichen. Diese Gesundheitsüberwachungsgeräte können von Blutdruck- und Herzfrequenzmonitoren bis hin zu fortgeschrittenen Geräten reichen, die in der Lage sind, spezialisierte Implantate zu überwachen, wie z. B. Herzschrittmachern.

Beispiel 6: Gebäude- und Hausautomation

IoT-Geräte können zur Überwachung und Steuerung von Türen, Fenstern, Heizung und Beleuchtung verwendet werden, Stichwort ist hier Smart Home.

Beispiel 7: Transportwesen

Die dynamische Interaktion zwischen Komponenten eines Transportsystems ermöglicht inter- und intra-Fahrzeugkommunikation, intelligente Verkehrssteuerung wie intelligente Parkplätze, elektronische Mautsysteme, Logistik- und Flottenmanagement, Fahrzeugsteuerung und Sicherheit und Straßenhilfe.

Diese Aufzählung neuer Anwendungen und Geschäftsmodelle im Rahmen der Digitalisierung lässt sich beliebig fortsetzen. Wichtig ist:

Die Digitalisierung durchdringt in unglaublichem Tempo jeden Bereich von Wirtschaft und Gesellschaft. Alles was digitalisiert werden kann, wird digitalisiert. Alles was vernetzt werden kann, wird vernetzt. Und alles was vernetzt ist, wird über die Cloud global und jederzeit verfügbar gemacht. Dies gilt auch für die Cyberattacken! Alles was gehackt werden kann, wird früher oder später gehackt. Das geht von Spionage, Datenklau über Zerstören bis zum Manipulieren und Beeinflussen. Damit ist klar: Sicherheit ist das Fundament für Vertrauen in die Digitalisierung.

Und diese Sicherheit ist unsere gemeinsame Verantwortung!

Um diese Verantwortung wahrzunehmen, benötigen wir verantwortliche Personen. Wir nennen diese Personen Wirtschaftsschutzbeauftragte! Wir brauchen sie in den Unternehmen und im öffentlichen Sektor! Die steigende Komplexität der Thematik „Wirtschaftsschutz" erfordert die Schaffung klarer Zuständigkeiten und zentraler Ansprechpartner – auf Seiten der Wirtschaft und bei den Sicherheitsbehörden. Hier ist in den letzten Jahren bereits viel passiert.

Doch eine bessere Bündelung der Aufgaben durch einen Beauftragten für Wirtschaftsschutz – in den Unternehmen wie bei den staatlichen Stellen – verbunden mit klaren Aufgaben -würde zu einer entscheidenden Stärkung führen.

Nun aber zum heutigen Tag! Das Leitthema unserer heutigen Veranstaltung ist:

Neue Businessmodelle und Industrie im Wandel – Chancen und Risiken für die Unternehmenssicherheit.

Und damit starten wir gleich mit einer sicherlich bereichernden Keynote von Karl Olsberg über „Künstliche Intelligenz und menschliche Dummheit".

Am Nachmittag warten dann auf uns noch weitere praxisorientierte Themen. Dazu haben wir in diesem Jahr Workshops für Sie vorbereitet:

1. Desinformation
2. Connected Car
3. Blockchain
4. EU-Richtlinie Know-How-Schutz
5. Authentication of data

Wir freuen uns, dafür hochkarätige Referenten gewonnen zu haben:

Prof. Dr. Martin Grothe, Stephan Gerhager, Joachim Lohkamp, Alexander Härtel, Adam Stogdale

Wir sind gespannt auf Ihre Ausführungen!

Und kein noch so gutes Konzept sollte ohne entsprechendes Notfallmanagement ausgestattet sein. Dazu stellt Ihnen Herr Prof. Kob ein neues Kapitel aus unserem Handbuch Wirtschaftsgrundschutz vor: Notfallmanagement, ein Muss in Zeiten des Wandels.

Ich bin sicher, auch in diesem Jahr wird unsere „traditionelle“ und nunmehr bereits 11te BfV/ASW Kooperationsveranstaltung erfolgreich sein. Die langjährige, gute und vertrauensvolle Zusammenarbeit ist die beste Basis für ein gutes Gelingen.

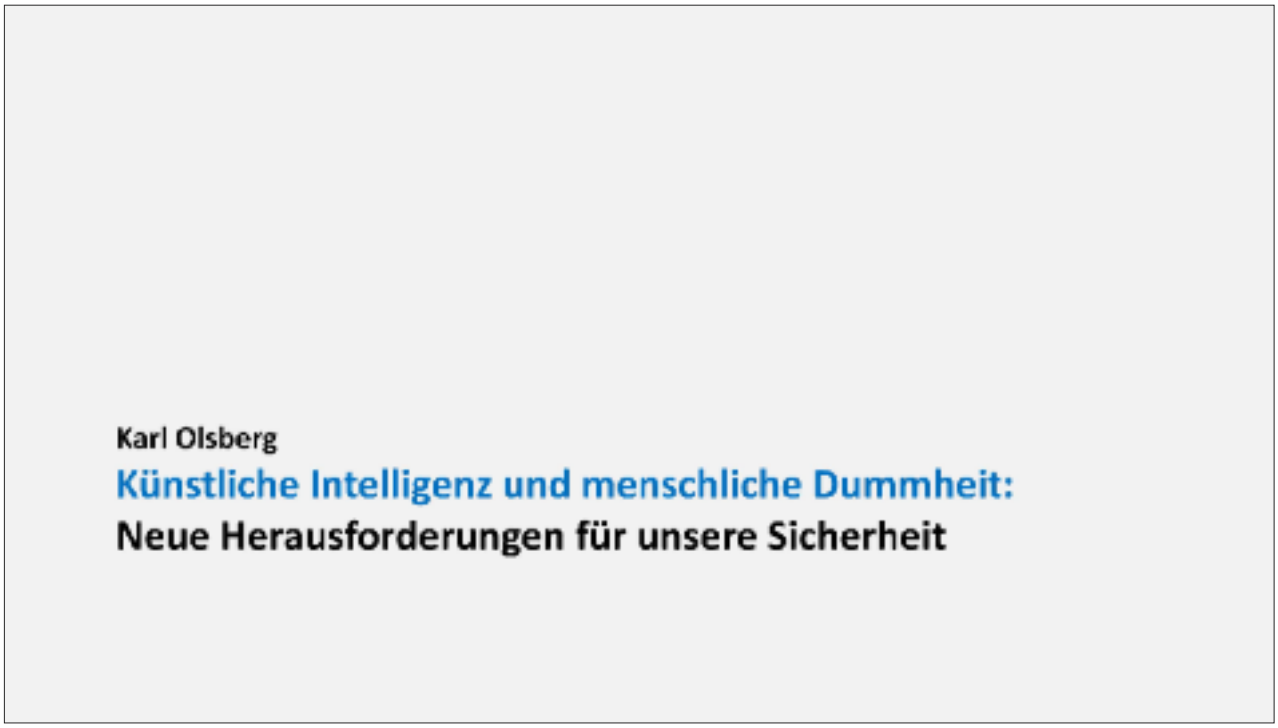
Erlauben Sie mir noch kurz zu erwähnen, eine solche Veranstaltung ist nur mit Unterstützung möglich. Neben dem BfV, mit dem wir als ASW Bundesverband die Organisation und Inhalte des heutigen Tages gemeinsam gestaltet haben, möchte ich mich auch bei unserem Hausherrn – der BAKS – und unseren Sponsoren Deloitte und der Power Unternehmensgruppe bedanken, die wesentlich dazu beigetragen haben, das heutige Setting in diesem Umfang möglich zu machen. Auch der Firma WISAG gilt mein Dank für die Unterstützung bei unserer Vorabendveranstaltung.

Vielen Dank auch an die Vertreter der Presse und Medien, dass Sie unserer Einladung zum ersten Teil der Veranstaltung nachgekommen sind! Die Pressekonferenz fand bereits am heutigen Morgen statt.

Lassen Sie uns nun mit dem ersten Vortrag den Tag beginnen: Herr Olsberg, wir sind sehr gespannt auf Ihre Ausführungen zur künstlichen Intelligenz und menschlichen Dummheit und hoffen, dass wir in den nächsten 30 Minuten zumindest etwas schlauer werden und einiges dazulernen können. In diesem Sinne, lieber Herr Olsberg, die Bühne gehört Ihnen!

Künstliche Intelligenz und menschliche Dummheit: Neue Herausforderungen für unsere Sicherheit

Karl Olsberg, Schriftsteller und Unternehmer



Unser Bild von Maschinen ist von Vorurteilen geprägt

Beliebte Vorurteile über Maschinen

- Sie tun nur das, was wir ihnen einprogrammiert haben
- Sie haben keinen eigenen Willen
- Sie haben keine Gefühle
- Sie sind nicht kreativ

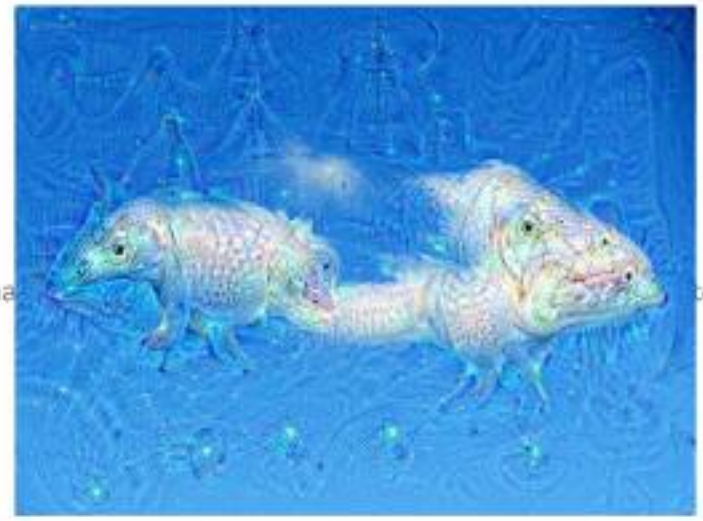
titelmasters durch Klicken bearbeiten

Bildquelle: Fritz Lang, Metropolis

Was sehen Sie in dieser Wolke?

Forma zen

Das sieht Googles „Deep Dream" in dieser Wolke …



Die Maschine, die im März 2016 den weltbesten Go-Spieler schlug, hat sich das Spiel selbst beigebracht

„Deep Learning" bei AlphaGo

- Anders als Schach ist Go nicht durch simple Vorausberechnung von Zügen beherrschbar
- AlphaGo brachte sich die Grundregeln durch Analyse von ca. hunderttausend Spielen selbst bei
- AlphaGo perfektionierte sich durch Millionen Spiele gegen sich selbst
- Niemand weiß, warum AlphaGo bestimmte Züge macht

Turing lag falsch

Turing-Test

„Eine Maschine ist intelligent, wenn sie im Dialog nicht von einem Menschen unterschieden werden kann."

vo_____elmasters

Kritik:

- Der Turing-Test misst eher die Intelligenz der Testperson als die der Maschine
- Ein intelligenter Außerirdischer würde durchfallen
- Entscheidend ist nicht, wie eine Maschine „denkt", sondern welche Probleme sie wie gut lösen kann

Alan Turing schlug einen einfachen Test für die „Intelligenz" von Maschinen vor

Künstliche Intelligenz unterscheidet sich oft grundlegend von menschlichem Denken

Bildquelle: Wikipedia

Es kommt nicht darauf an, wie „intelligent" Maschinen sind, sondern welche Entscheidungen wir ihnen anvertrauen

Künstliche Intelligenz als „Navigationssystem" fürs Leben

Das Problem ist nicht künstliche Intelligenz, sondern menschliche Dummheit

Neulich in Köln …

Peinliches Malheur mitten in der Stadt: Am Kölner Neumarkt ist am Samstag ein Franzose versehentlich in einen U-Bahn-Eingang gefahren und auf der Treppe hängengeblieben.

…

Das Paar hatte den U-Bahn-Eingang mit dem Eingang zu einer Tiefgarage verwechselt. **Anscheinend waren sie einem Navigationsgerät gefolgt.**

Quelle: RP Online/Foto: WDR

Amazons „Alexa": permanente Belauschung inklusive

Amazon Echo

Eindruck nach drei Monaten Test:

- Sehr gute Spracherkennung und Sprachsynthese
- Man lernt mehr und mehr neue, nützliche Funktionen
- Alexa wirkt „sympathisch", „gutmütig", „harmlos" und „vertrauenswürdig"
- Man vergisst schon nach kurzer Zeit, dass sie permanent zuhört
- Ich würde sie wieder kaufen

Selbstlernende Maschinen + Social Engineering = großes Gefahrenpotenzial

Social Engineering und künstliche Intelligenz

"By 2020, the average person will have more conversations with bots than with their spouse."
Gartner Research, October 2016

"After a period of monitoring, the AI could tailor phishing messages to mimic the message style of the victim to particular contacts in their address book, in order to convince them to click on a malicious link."
Danny Palmer, ZDNet, December 2016

Quelle: http://www.zdnet.com/article/how-ai-powered-cyberattacks-will-make-fighting-hackers-even-harder/
http://www.gartner.com/smarterwithgartner/gartner-predicts-a-virtual-world-of-exponential-change/
Bildquelle: Von Meul - Eigenes Werk, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=9127101

Wir befinden uns in einem evolutionären Rüstungswettlauf

Evolution bei Schadsoftware

Reproduktion: Effektive Schadsoftware wird kopiert

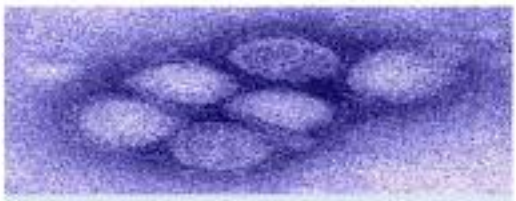
Mutation: Selbst-lernende Systeme, zufällige Varianten

Konsequenz: Je besser die Schutz-maßnahmen, desto raffinierter die Angriffstechniken

Selektion: Schutzmaßnahmen filtern ineffektive Angreifer aus

Wir müssen unser Immunsystem stärken – mit allen Mitteln!

Immunsystem-Analogie



Immunschwäche

- Extrem schneller technischer Wandel
- Unzureichender technischer Schutz
- Naivität, Unbekümmertheit, Unwissen
- Hoher ökonomischer Anreiz für Kriminelle

Immunisierungsansätze

- Permanentes Lernen und Forschen
- „Intelligente" Abwehrsysteme
- „Impfung" (z.B. unechte Phishing-Mails)
- Aufklärung, Training und Ausbildung!
- Gesetze, Strafverfolgung

Bildquelle: Commons.wikimedia.org

Vielen Dank!

© Dr. Karl-Ludwig von Wendt

Bahngärten 7, 22041 Hamburg

vonwendt@yahoo.com

www.karlolsberg.de

Notfallmanagement, ein Muss in Zeiten des Wandels – Handbuch Wirtschaftsgrundschutz

Prof. Timo Kob, Vorstand HiSolutions AG /ASW Bundesverband

Neues vom Wirtschaftsgrundschutz von BfV, BSI und ASW Bundesverband

Master-Untertitelformat bearbeiten

Prof. Timo Kob, Vorstand HiSolutions AG, ASW Bundesverband

Ausgangssituation: Ein Paradoxon auflösen!

- Für das – vermeintlich – neue Angriffsziel IT gibt es seit 20 Jahren ein erfolgreiches Hilfsmittel:
  Den IT-Grundschutz des BSI
- Für die „klassischen" Angriffsziele wie Mensch, Infrastrukturen und Prozesse gibt es dies nicht!
- Mit dem Wirtschaftsgrundschutz wird diese Lücke geschlossen!

Wirtschaftsgrundschutz 19.05.17 2

Ausgangssituation: Vogel Strauß-Taktik beenden

- Gerade der Mittelstand sieht oft noch nicht die Brisanz der Thematik für das eigene Unternehmen
- Appelle interner und externer Fachleute werden oft als „Eigenwerbung" der Fachleute wahrgenommen
- Wir müssen eine „objektive Stimme" schaffen.
  Ein „Siegel der Vertrauenswürdigkeit".

Wirtschaftsgrundschutz 19.05.17 3

Ausgangssituation: Konsens schaffen

- Die zuvor beschriebene Verunsicherung wird durch unterschiedliche Ansichten der Fachwelt noch gesteigert
- Es fehlt ein „größter gemeinsamer Nenner"
- Wir müssen alle an einen Tisch bringen:
  - Wirtschaft und Staat,
  - DAX-Konzern und KMU,
  - Anwender, Anbieter und Berater
  - alle relevanten Verbände
  - Forschung und Lehre

Wirtschaftsgrundschutz 19.05.17 4

Die Idee

- Die zweite Säule für die Unternehmenssicherheit schaffen
- Durch identische Struktur besteht die Chance zu ganzheitlichen Sicherheitskonzepten
- Bekanntheit des IT-Grundschutz nutzen
- KEINE Verbindlichkeit
- In der Kombination beider Werke eine weltweit einmalige Unterstützung für Unternehmen

Wirtschaftsgrundschutz 19.05.17 5

Auf wirtschaftsschutz.info kostenfrei erhältlich

Wirtschaftsgrundschutz 19.05.17 6

Struktur des Wirtschaftsgrundschutzes

- In Analogie zum IT-Grundschutz besteht das Werk aus „Standards" und „Bausteinen".
- Standards beschreiben, wie man den Themenkomplex managed
- Bausteine beschreiben Lösungsansätze für konkrete Probleme

Wirtschaftsgrundschutz 19.05.17 7

Wie hilft der Wirtschaftsschutz wem?

- Durch Einzelbausteine Antworten auf konkrete Detailfragen in Form von Maßnahmen
- Durch ABC-Priorisierung der Maßnahmen in den Bausteinen geeignet für
  - „Anfänger" und/oder „Normalgefährdete" als Einstieg
  - „Experten" und/oder „Hochgefährdete" zur Optimierung
- Durch Synchronität zu IT-Grundschutz geeignet, bestehende IT-Sicherheitskonzepte, aber auch Informationssicherheits-Managementsysteme zu ergänzen

Wirtschaftsgrundschutz 19.05.17 8

Struktur der Standards

„Best Practices“ für

- Ziele
- Rollen
- Prozesse
- Themen
- Dokumentationen

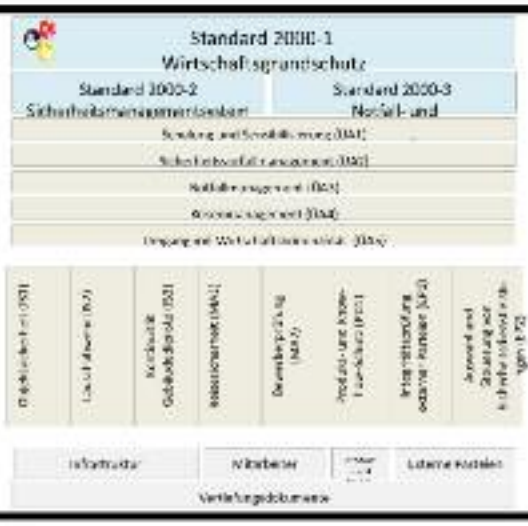
um Wirtschaftsschutz dauerhaft zu managen.

Struktur der Bausteine

„Best Practices“ um konkrete Sicherheitsprobleme zu lösen (oder um Vorschläge der Standards zu konkretisieren).

- Hilfe durch Kontrollfragen, ob Baustein für den Leser relevant
- Kurze Einführung in das Thema
- Beschreibung der Bedrohungslage als Basis für individuelle Risikoanalysen
- Priorisierte Maßnahmen
- Gesamtlänge ca. 20 Seiten, Verweise auf vertiefende Literatur

Übersicht



Wirtschaftsgrundschutz 19.05.17 11

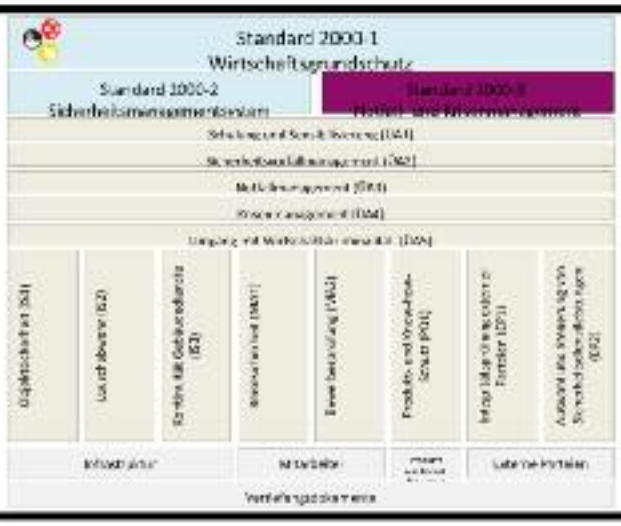
Vorläufiger Veröffentlichungsplan der Werke

Typ	Titel	Termin
S	2000-1 Wirtschaftsschutz	November 16
S	2000-2 Sicherheitsmanagement	November 16
S	2000-3 Notfall- und Krisenmanagement	November 16
BS	Schulung und Sensibilisierung	November 16
BS	Reisesicherheit	November 16
BS	Sicherheitsvorfallmanagement	März 17
BS	Krisenmanagement	März 17
BS	Auswahl und Steuerung von Sicherheitsdienstleistungen	April 17
BS	Kommunale Gebäudedienste	April 17
BS	Produkt- und Know-how-Schutz	April 17
BS	Umgang mit Wirtschaftskriminalität	April 17
BS	Notfallmanagement	April 17
BS	Objektsicherheit	Mai 17
BS	Leitstandwahl	Mai 17
BS	Bewerberprüfung	Mai/Juni 17
BS	Integritätsprüfung externer Partner	Mai/Juni 17

Wirtschaftsgrundschutz 19.05.17 12

WGS-Standard 2000-3

Der WGS-Standard 2000-3 umfasst alle Rahmenanforderungen an ein Notfall- und Krisenmanagement und dient als Orientierungshilfe für ein institutionsspezifisches Reaktionsmanagement.



Wirtschaftsgrundschutz 19.05.17 13

Notfallmanagement: Regelungsbereiche im WGS-Standard 2000-3

Abgrenzung Krisenmanagement	• Notfalldefinition und -kriterien • Notfallszenarien
Alarmierung & Eskalation	• ereignisorientierte Alarmierung • Voraussetzung für die Aktivierung des Krisenmanagements
Rollen	• Rollen für bestimmte Aufgaben (z. B. Räumung) • Fachfunktionen (z. B. technische Infrastruktur)
Sonstige Organe	• z. B. Integration der Betriebsfeuerwehr oder der Sicherheitsdienste
Dokumentation	• Leitlinie, Notfallhandbuch, Notfallplan, Hilfsmittel

Wirtschaftsgrundschutz 19.05.17 14

Zusammenspiel der Standards BSI 100-4 und WGS 2000-3

Business Continuity Procedures
„Planung der Geschäftsfortführung"

Emergency Response
„Betriebliche Notfallplanung"

WGS 2000-3

Komb i-nation

BSI 100-4

Crisis Management
„Notfall-/Krisenbewältigung"

IT Continuity/Disaster Recovery
„IT-Notfallmanagement"

Wirtschaftsgrundschutz 19.05.17 15

Baustein ÜA3 Notfallmanagement

Der Baustein stellt eine allgemeine Orientierungshilfe für den Aufbau, die Optimierung und die Weiterentwicklung einer Aufbau- und Ablauforganisation zur Bewältigung von Notfällen dar.

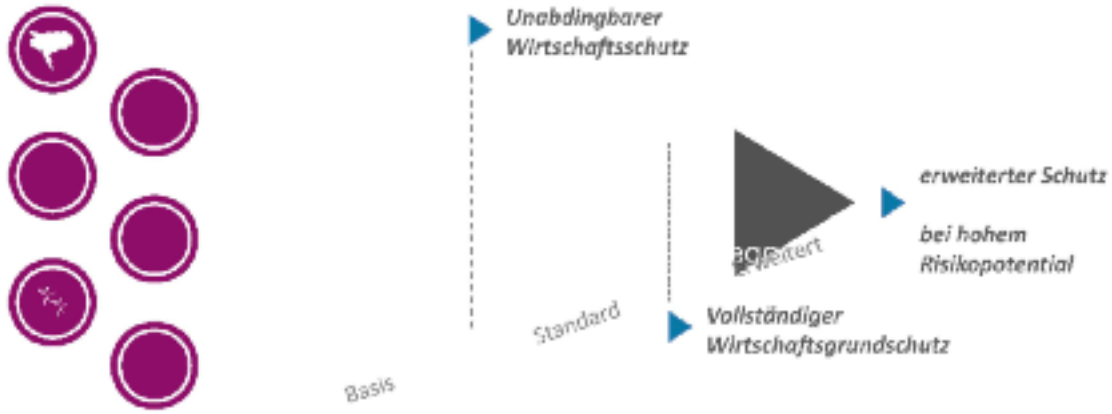
Wirtschaftsgrundschutz 19.05.17 16

Relevanzentscheidung für die Implementierung

1. Gelten rechtliche Auflagen oder branchenspezifische Regularien oder anderweitige Vorgaben, die ein Notfallmanagement erforderlich machen oder bei denen ein Notfallmanagement zur Erfüllung von Vorgaben unterstützen kann?
2. Fordern Kunden und Geschäftspartner ein angemessenes Risikomanagement oder explizit Maßnahmen zur Notfallvorsorge, Ausfallsicherheit oder Notfallbewältigung?
3. Arbeitet die Institution mit gefährlichen Gütern oder befinden sich solche in unmittelbarer Umgebung?
4. Besteht eine hohe Abhängigkeit zu einzelnen Standorten oder Gebäudekomplexen, die bei einem Ausfall einen „hohen bis sehr hohen" Schaden verursachen könnten?
5. Unterliegt die Leitung der Institution etwaigen persönlichen Haftungsrisiken z. B. aufgrund eines Organisationsverschuldens?

Wirtschaftsgrundschutz 19.05.17 17

Gefährdungen vs. Maßnahmen



Wirtschaftsgrundschutz 19.05.17 18

Gefährdungen vs. Maßnahmen

M 1 Identifizieren der Gefährdungen mit besonderem Notfallpotential
M2 Definieren einer geeigneten Notfallorganisation

M 5 Erstellen von Notfallprozeduren

M 6 Erstellen eines Alarmierungskonzepts und Alarmierungsplans

Basis

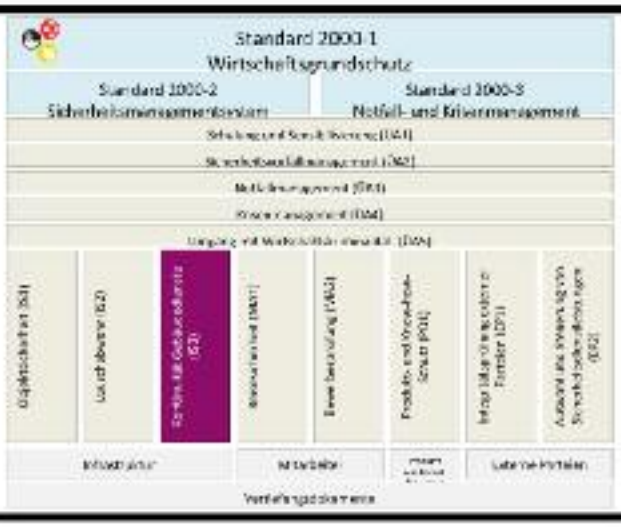
Standard

erweitert

Wirtschaftsgrundschutz 19.05.17 19

Baustein IS3 Kontinuität der Gebäudedienste

Zielsetzung dieses Bausteins ist der Schutz der gebäude- und infrastrukturbezogenen Unterstützungsprozesse und damit übergreifend die Sicherung der Geschäftstätigkeit betroffener Institutionen.



Wirtschaftsgrundschutz 19.05.17 20

Relevanzentscheidung für die Implementierung

1. Werden gebäudebezogene Dienste kontrolliert gesteuert?
2. Sind Facility Services ausgelagert und werden diese zentral gemanagt?
3. Ist den Mitarbeitern bewusst, welche Einwirkungen ein Ausfall bestimmter Unterstützungsprozesse auf die Kernprozess der Institution hat?
4. Ist ermittelt und dokumentiert, welche Schwachstellen im Bereich der Gebäudedienste existieren und wie diese zu behandeln sind?
5. Liegen Notfallpläne des Ressourcenbereichs Facility Services vor, sind diese bekannt und werden diese regelmäßig geübt?

Wirtschaftsgrundschutz 19.05.17 21

Maßnahmen unterschiedlicher Ausprägung

Basis

Standard

erweitert

M 1 Planen der Einführung eines Managements der Kontinuität der Gebäudedienste

M 4 Einflussfaktoren identifizieren

M 6 Notfallvorsorge für das Management der Kontinuität der Gebäudedienste konzeptionieren

Wirtschaftsgrundschutz 19.05.17 22


Wir bedanken uns für Ihre Aufmerksamkeit
Allianz für Sicherheit in der Wirtschaft e.V.
Neue Schönhauser Straße 20
10178 Berlin
www.asw-bundesverband.de
+49 (0) 30 200 77 200
ASW
Bundesverband
Wirtschaftsgrundschutz
19.05.17
23

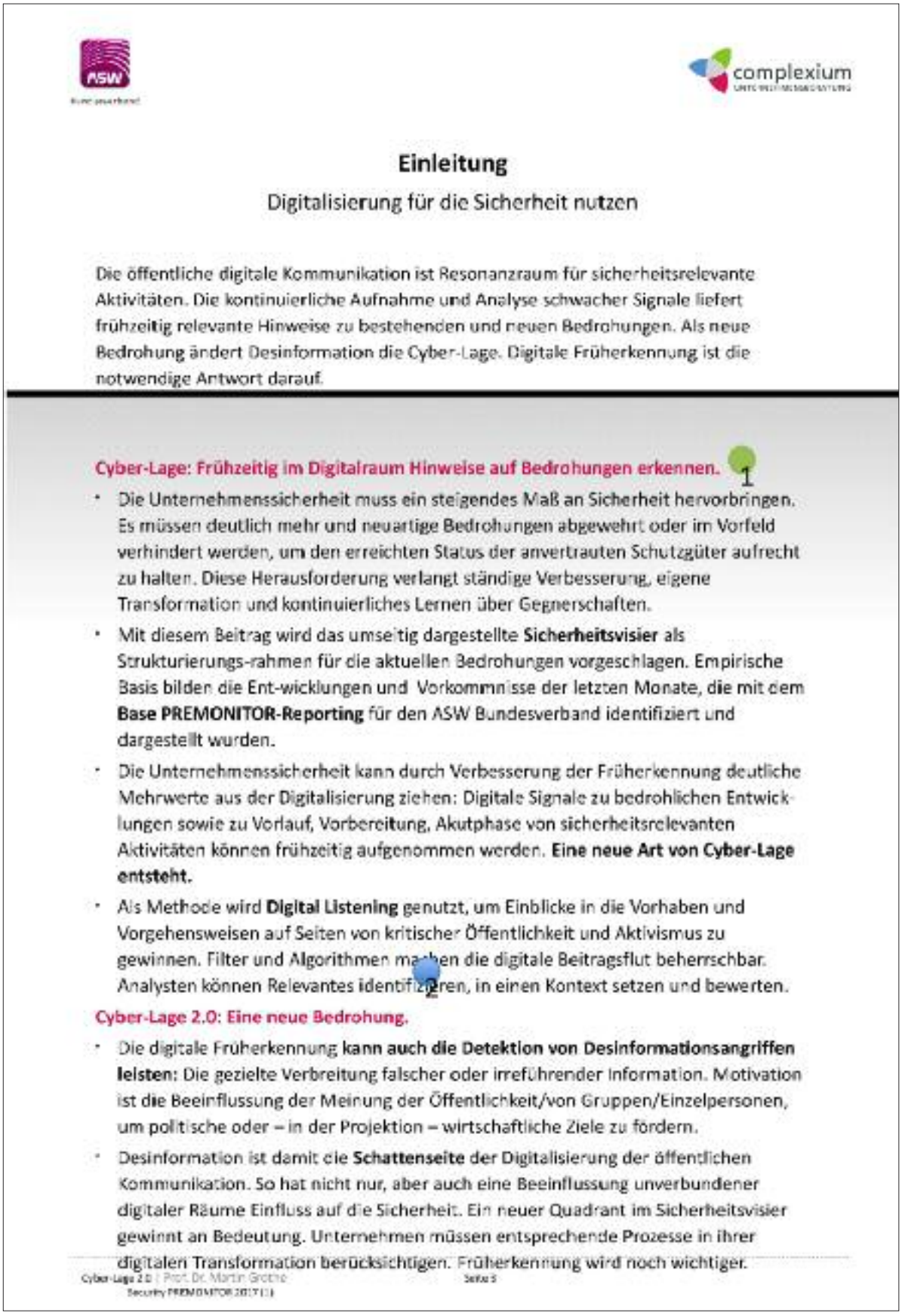
Cyberlage 2.0
Digitalisierung von Früherkennung und Desinformation

Prof. Dr. Martin Grothe, complexium Gmbh

Cyber-Lage 2.0

Digitalisierung von Früherkennung und Desinformation

Security Premonitor 2017 (1)



Einleitung

Digitalisierung für die Sicherheit nutzen

Die öffentliche digitale Kommunikation ist Resonanzraum für sicherheitsrelevante Aktivitäten. Die kontinuierliche Aufnahme und Analyse schwacher Signale liefert frühzeitig relevante Hinweise zu bestehenden und neuen Bedrohungen. Als neue Bedrohung ändert Desinformation die Cyber-Lage. Digitale Früherkennung ist die notwendige Antwort darauf.

Cyber-Lage: Frühzeitig im Digitalraum Hinweise auf Bedrohungen erkennen. 1

- Die Unternehmenssicherheit muss ein steigendes Maß an Sicherheit hervorbringen. Es müssen deutlich mehr und neuartige Bedrohungen abgewehrt oder im Vorfeld verhindert werden, um den erreichten Status der anvertrauten Schutzgüter aufrecht zu halten. Diese Herausforderung verlangt ständige Verbesserung, eigene Transformation und kontinuierliches Lernen über Gegnerschaften.
- Mit diesem Beitrag wird das umseitig dargestellte **Sicherheitsvisier** als Strukturierungs-rahmen für die aktuellen Bedrohungen vorgeschlagen. Empirische Basis bilden die Ent-wicklungen und Vorkommnisse der letzten Monate, die mit dem **Base PREMONITOR-Reporting** für den ASW Bundesverband identifiziert und dargestellt wurden.
- Die Unternehmenssicherheit kann durch Verbesserung der Früherkennung deutliche Mehrwerte aus der Digitalisierung ziehen: Digitale Signale zu bedrohlichen Entwicklungen sowie zu Vorlauf, Vorbereitung, Akutphase von sicherheitsrelevanten Aktivitäten können frühzeitig aufgenommen werden. **Eine neue Art von Cyber-Lage entsteht.**
- Als Methode wird **Digital Listening** genutzt, um Einblicke in die Vorhaben und Vorgehensweisen auf Seiten von kritischer Öffentlichkeit und Aktivismus zu gewinnen. Filter und Algorithmen machen die digitale Beitragsflut beherrschbar. Analysten können Relevantes identifizieren, in einen Kontext setzen und bewerten. 2

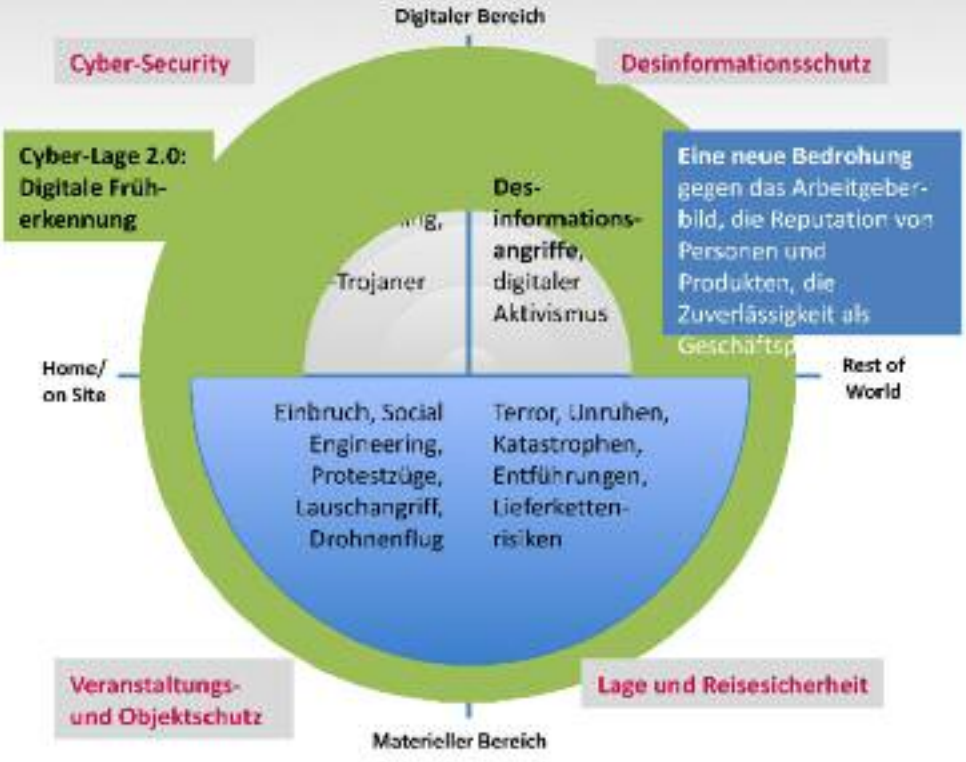
Cyber-Lage 2.0: Eine neue Bedrohung.

- Die digitale Früherkennung **kann auch die Detektion von Desinformationsangriffen leisten:** Die gezielte Verbreitung falscher oder irreführender Information. Motivation ist die Beeinflussung der Meinung der Öffentlichkeit/von Gruppen/Einzelpersonen, um politische oder – in der Projektion – wirtschaftliche Ziele zu fördern.
- Desinformation ist damit die **Schattenseite** der Digitalisierung der öffentlichen Kommunikation. So hat nicht nur, aber auch eine Beeinflussung unverbundener digitaler Räume Einfluss auf die Sicherheit. Ein neuer Quadrant im Sicherheitsvisier gewinnt an Bedeutung. Unternehmen müssen entsprechende Prozesse in ihrer digitalen Transformation berücksichtigen. Früherkennung wird noch wichtiger.

Sicherheitsvisier

Bedrohungen in vier Feldern

Für die Unternehmenssicherheit ist **Transformation** nicht neu: Liegen die Wurzeln in der Sicherung des eigenen Betriebsgeländes, folgte zunächst eine Ausweitung durch Begleitung von Reisenden. Mit der **Digitalisierung** galt es dann, Cyber-Angriffen auf die eigene digitale Infrastruktur zu begegnen. Aktuell zeichnet sich ab, dass Unternehmen auch auf fremden Plattformen im digitalen Raum gegen Angriffe auf Meinungen verteidigt werden müssen.



Die **Früherkennung** nimmt digitale Signale zu bedrohlichen Entwicklungen sowie zu Vorlauf, Vorbereitung, Akutphase von sicherheitsrelevanten Aktivitäten auf.

Dieser Prozess **muss auch die Detektion von Desinformationsangriffen leisten.** Nicht nur, aber auch unverbundene digitale Räume haben Einfluss auf die Sicherheit. Ein neuer Quadrant gewinnt immer mehr an Bedeutung.

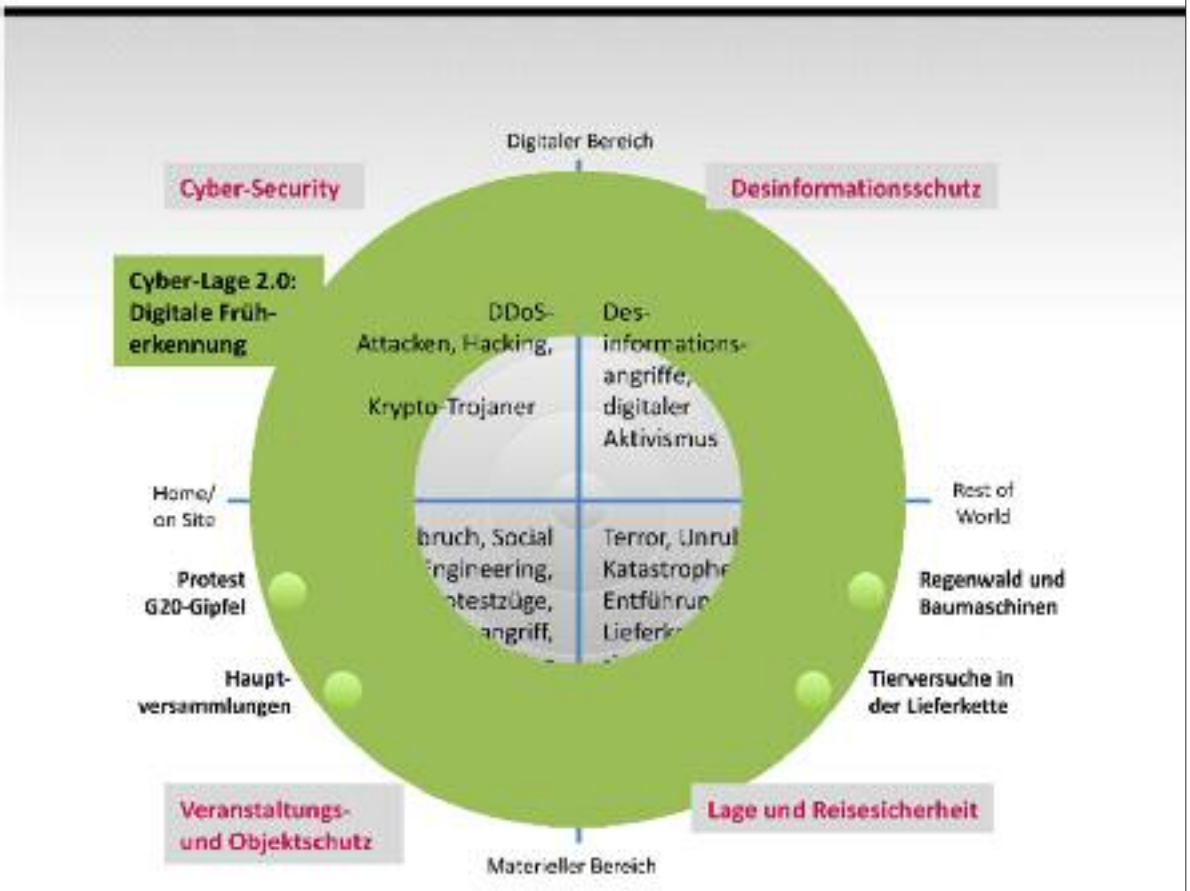
1

2

Digitale Früherkennung

Beispiele aus dem Base PREMONITOR

Auf den folgenden Seiten sind Beispiele aus den jüngsten Base PREMONITOR-Reports, die complexium für den ASW Bundesverband regelmäßig erstellt, dargestellt, um einen plastischen Einblick in die digitale Früherkennung zu geben. Üblicherweise werden diese Hinweise unternehmensspezifisch im täglichen Alerting verfolgt.



Die **Früherkennung** identifiziert direkte und indirekte Bedrohungen und verlängert damit die **Vorwarnzeit**:

Es wird deutlich, dass zum einen Bedrohungen aus vorgelagerten Stufen der Lieferkette auf Unternehmen zurückschlagen können. Zum anderen können Aktionen, mit denen sich Wettbewerber konfrontiert sehen, auf das eigene Unternehmen „überschwappen".

Auszug aus Base PREMONITOR: 2016 Nov – 2017 Jan

complexium

VEKTOR **PROTEST G20-GIPFEL**

WER: **AKTEUR**

Einflussfaktor Groß: **Attac**
Einflussfaktor Mittel: **Interventionistische Linke, Klima der Gerechtigkeit**
Einflussfaktor Gering: ***anonyme Nutzer, Nutzer „Anti-G20"***

WEN: **TARGET**

Alle Wirtschaftsbranchen
Banken & Finanzinstitute
Politik und Regierungen

WANN & WO: **TERMIN**

26. November 2016: Hamburg
27. Dez. 2016: Lund/Schweden
04. Dezember: Bundesweit
05./06. Juli 2017: Hamburg
07./08. Juli 2017: Hamburg
17./18. März 2017: Baden-Baden

WIE: **AKTION**

Online-Aufrufe (Call for action)
Demonstrationen
Physische Angriffe

Frühzeitig organisieren sich Aktivisten und schärfen das Bewusstsein zur Mobilisierung gegen den G20-Gipfel in Hamburg. Auch erste physische Übergriffe werden in der Weihnachtszeit gemeldet.

Verschiedene Initiativen und Organisationen kündigen bereits ihre Aktionen zum G20-Gipfel in Hamburg an. **Attac** fordert unter dem Motto „*Global Gerecht Statt G20*" zur Teilnahme am **Alternativgipfel** (05./06. Juli), am **Aktionstag** (07. Juli) und an der **Großdemonstration** (08. Juli) auf. Am 4. Dezember organisiert ***die Interventionistische Linke*** die „Aktionskonferenz gegen den G20-Gipfel". Nicht nur im Juli anlässlich der Versammlung der Staatsoberhäupter und Regierungschefs zum jährlichen Gipfeltreffen soll demonstriert werden, sondern bereits am 17./18. März zum Treffen der **G20-Finanzminister in Baden-Baden**.

Physische Übergriffe werden Ende November und Ende Dezember gemeldet. Anonyme Aktivisten verbünden auf der Plattform ***indymedia***, dass sie „*an dem Austragungsort der OSZE- und G20 Gipfel, der* **Hamburger Messe** *im Eingang Süd, mit Reifen und Benzin Feuer gelegt hätten. Die Glasfront an der Karolinenstraße sei einer intensiven Bearbeitung mit Hämmern, Farbe und Steinen unterzogen worden*".

Die Aktion versteht sich auch als Aufruf: „*Gegen die herrschende Ordnung der Welt, den revolutionären Kampf organisieren, bis jede Grenze fällt. Wir werden unsere Kämpfe nicht auf die Tage der Gipfel beschränken. Deshalb rufen wir* ***internationalist*** *auf, den April 2017 für grenzenlose dezentrale Momente von Widerstand zu verwenden, Bezüge zwischen den unterschiedlichsten Kämpfen herzustellen und unsere Angriffe zu verstetigen.* ***Troublemakers of the world*** *save the date: 7.7./8.7.2017 dem G20 in Hamburg Tschüs sagen.*"

Am 27. Dezember greifen die Nutzer ***Anti-g20*** nach eigenen Angaben auf der Plattform ***linksunten*** eine Bank in Lund/Schweden an: „***This is part of the anti-capitalist mobilization for the G20 in Hamburg in July.*** *This is a step in delegitimatizing capitalist institutions, in showing the resistance towards them in a concrete way. This is just the beginning.*" Mit weiteren Übergriffen im Vorfeld des G20-Gipfels ist somit zu rechnen.

Wichtige direkte Quellen
https://linksunten.indymedia.org/en/node/200192
http://www.attac.de/kampagnen/g20-in-hamburg/startseite/
http://de.indymedia.org/node/11321
http://www.interventionistische-linke.org/beitrag/rooms-improvement-der-solidaritaet-ein-zuhause-geben

Cyber-Lage 2.0 | Prof. Dr. Martin Grothe
Security PREMONITOR 2017 | 3

Seite 6

Auszug aus Base PREMONITOR: 2017 Jan - Feb

complexium

VEKTOR HAUPTVERSAMMLUNGEN

WER: **AKTEUR**

Einflussfaktor Groß: **Dachverband Kritische Aktionäre, ROBIN WOOD, urgewald, Sum of Us, OXFAM**
Einflussfaktor Mittel: **MEDICO International**
Einflussfaktor Gering: **Kooperation Brasilien, Christliche Initiative Romero, Stop Mad Mining**

WEN: **TARGET**

Alle Wirtschaftsbranchen
Politik und Regierungen

WANN & WO: **TERMIN**

26. Januar: London
27. Januar: Bochum
01. Februar: München
02. Februar: Nienburg

WIE: **AKTION**

Online-Aufrufe
Podiumsdiskussion
Demonstrationen
Kletterprotest

Die Hochsaison der Hauptversammlung steht noch bevor, einige Unternehmen haben das jährliche Meeting der Aktionäre bereits hinter sich: Protestaktionen und Kundgebungen von NGOs und Aktivisten begleiten traditionell diese Corporate Events.

Am 26. Januar protestieren wie angekündigt der *Dachverband der Kritischen Aktionäre*, das internationale Netzwerk *Plough Back the Fruits*, das *London Mining Network* auf der HV des Bergbaukonzerns ***Lonmin***, mit Fotos der **34 erschossenen Bergleute.** Als wichtigster Kunde von ***Lonmin*** wird auch ***BASF*** heftig kritisiert. Dem Konzern wird vorgeworfen *„Keine Verantwortung für die Lieferkette!"* zu übernehmen. Die Podiumsdiskussion über "*Globale Wirtschaft, globale Verantwortung?*" findet in Nienburg statt, Standort der ***BASF Catalysts Germany GmbH***.
Zur ***Thyssenkrupp***-HV fordert ein NGO-Bündnis (*Kooperation Brasilien, Christliche Initiative Romero, Stop Mad Mining, Dachverband Kritische Aktionäre, urgewald, Sum of Us*) den Konzern auf, bei Umwelt- und Menschenrechten nachzubessern: Kritisiert wird unter anderem die **Waffenlieferungen** in Krisenregionen, das ***Thyssenkrupp-Stahlwerk TKCSA*** in Rio de Janeiro aufgrund seines **gesundheitsgefährdenden** Stahlwerkstaubs, sowie der Bezug von Kokskohle aus Mosambik. Die dort umgesiedelte Bevölkerung wurde angeblich nie angemessen entschädigt. ***Thyssenkrupp*** mache sich ***„mitschuldig an den Menschenrechtsverletzungen und Umweltzerstörungen seiner Lieferanten"***, sagt die *Christliche Initiative Romero*.
Mit Gegenanträgen auf der HV und Pressemitteilungen weisen verschiedene NGOs auf angeblich gravierende Missstände bei ***Siemens*** (*und* ***Voith Hydro***) hin. Diese Aktionen sind insbesondere auch im Social Web sehr sichtbar. *Öko-Büro München, medico international, Pro REGENWALD, GegenStrömung, Western Sahara Resource Watch* und der *Dachverband Kritischer Aktionäre* werfen dem Konzern vor, zur **„Klimakiller-Fraktion"** zu gehören und seine **„Menschenrechtliche Sorgfaltspflichten"** zu vernachlässigen. Verwiesen wird auf Menschenrechtsverletzungen und Landraub für das Kraftwerk Agua Zarca in Honduras sowie weitere Energieprojekte in Ländern des globalen Südens. Einige bezeichnen Siemens als **„Komplize beim Mord an Berta Cáceres"**. Des weiteren organisieren Aktivisten von *Robin Wood* während der HV einen Kletterprotest an der Olympiahalle in München.

Wichtige direkte Quellen
http://www.kritischeaktionaere.de/
http://www.robinwood.de/Newsdetails.13+M503103d0f10.0.html
https://urgewald.org/presse/thyssenkrupp-u-boot-deals-heikle

Auszug aus Base PREMONITOR: 2016 Juli-Aug

complexium

VEKTOR **REGENWALD und Baumaschinen**

WER: **AKTEUR**

Einflussfaktor Groß: **Greenpeace, BankTrack**
Einflussfaktor Mittel: **ROBIN WOOD, OXFAM, Rettet den Regenwald e.V., Rainforest Action Network**
Einflussfaktor Gering: -/-

WEN: **TARGET**

Energiekonzerne
Pharma -& Chemieindustrie
Finanzinstitute
Maschinenbau
Politik & Regierung

WANN & WO: **TERMIN**

Online

WIE: **AKTION**

Kundgebungen & Protestaktionen
Veröffentlichungen
Online-Petitionen
Bisher keine Cyberangriffe bekannt

Ein Fokus auf das Umwelt-Thema *Schutz des Regenwaldes* macht anhand verschiedener aktueller Beispiele deutlich, dass Unternehmen und Institutionen von Aktivisten zunehmend zur Verantwortung gezogen werden.

Ob Indonesien, Amazonas, Panama oder Nigeria. Ob zur Gewinnung von **Palmöl**, zum Bau von **Staudämmen** oder von Highways: Internationale Organisationen prangern große, auch deutsche Konzerne an, die sie beschuldigen, sich ungenügend für den **Umweltschutz** und die Bewahrung der **Menschenrechte** einzusetzen. Proteste werden oft mithilfe der betroffenen **indigenen Bevölkerung** durchgeführt.

Greenpeace steuert zur Zeit zwei große Kampagnen: Mit **„Rettet den Amazonas!"** organisiert die NGO seit Monaten massive Proteste weltweit vor allem gegen ***Siemens***, zum Stopp von geplanten Wasserkraftwerken im Amazonas-Gebiet. Auch vor der Zentrale in München wurde protestiert. Besonders sollen jedoch die Online- und internationale Präsenz den Druck erhöhen. ***Greenpeace*** fordert weiter mit **„Wald statt Brand"** den Stopp des Raubbaus für Palmöl in Indonesien und prangert Konzerne wie ***PepsiCo, Colgate-Palmolive*** und ***Johnson & Johnson*** aufgrund vermeintlicher Lippenbekenntnisse an. Scharf kritisiert u.a. **ROBIN WOOD** die „irreführende" **WWF**-Palmölstudie. ***BankTrack*** verbreitet ihrerseits die Information, dass ***Rainforest Action Network*** eine **Datenbank** auf *forestsandfinance.org* zur Verfügung stellt, welche die Beteiligung internationaler Finanzinstitute und Investoren, wie ***Credit Suisse und Deutsche Bank***, an der **Regenwaldzerstörung** dokumentiert. ***Urgewald*** verurteilt, dass die ***DEG*** (*Deutsche Investitions- und Entwicklungsgesellschaft*) in Panama ein Wasserkraftwerk mitfinanziert ohne sich aktiv um die Belange der indigenen Bevölkerung zu kümmern.

Der Verein *Rettet den Regenwald* startet eine Petition gegen den Bau eines Highways im Nigerianischen Regenwald und fordert den Konzern *Liebherr* auf, keine Baumaschinen zu liefern.

Wichtige direkte Quellen
http://www.banktrack.org
http://forestsandfinance.org/
https://www.greenpeace.de/rettet-den-amazonas
https://www.regenwald.org/petitionen/1045/bitte-heute-noch-unterschreiben-den-wald-der-eluru-retten#news

Auszug aus Base PREMONITOR: 2016 Juli-Aug

complexium

VEKTOR **TIERSCHUTZ** in der Lieferkette

WER: AKTEUR

Einflussfaktor Groß: **PETA DE, *Ärzte gegen Tierversuche*, PETAZWEI**
Einflussfaktor Mittel:
Einflussfaktor Gering: ***kampagne gegen tierfabriken*, veganblog, Bund gegen Missbrauch der Tiere, TASSO, LPT-Schließen-Kampagne**

WEN: TARGET

Pharmaindustrie
Tierzuchtkonzerne
Laborbedarfshersteller
Transportgesellschaften
Stiftungen
Politik & Regierung

WANN & WO: TERMIN

Online
20. Juli: Wietzen-Holte
29. Juli bis 4. August: Camp Wietzen-Holte
23. Juli: München & Frankfurt

WIE: AKTION

Online-Petitionen
Demonstration & Blockade & Camp
Veröffentlichungen
Klagen
Bisher keine Cyberangriffe bekannt

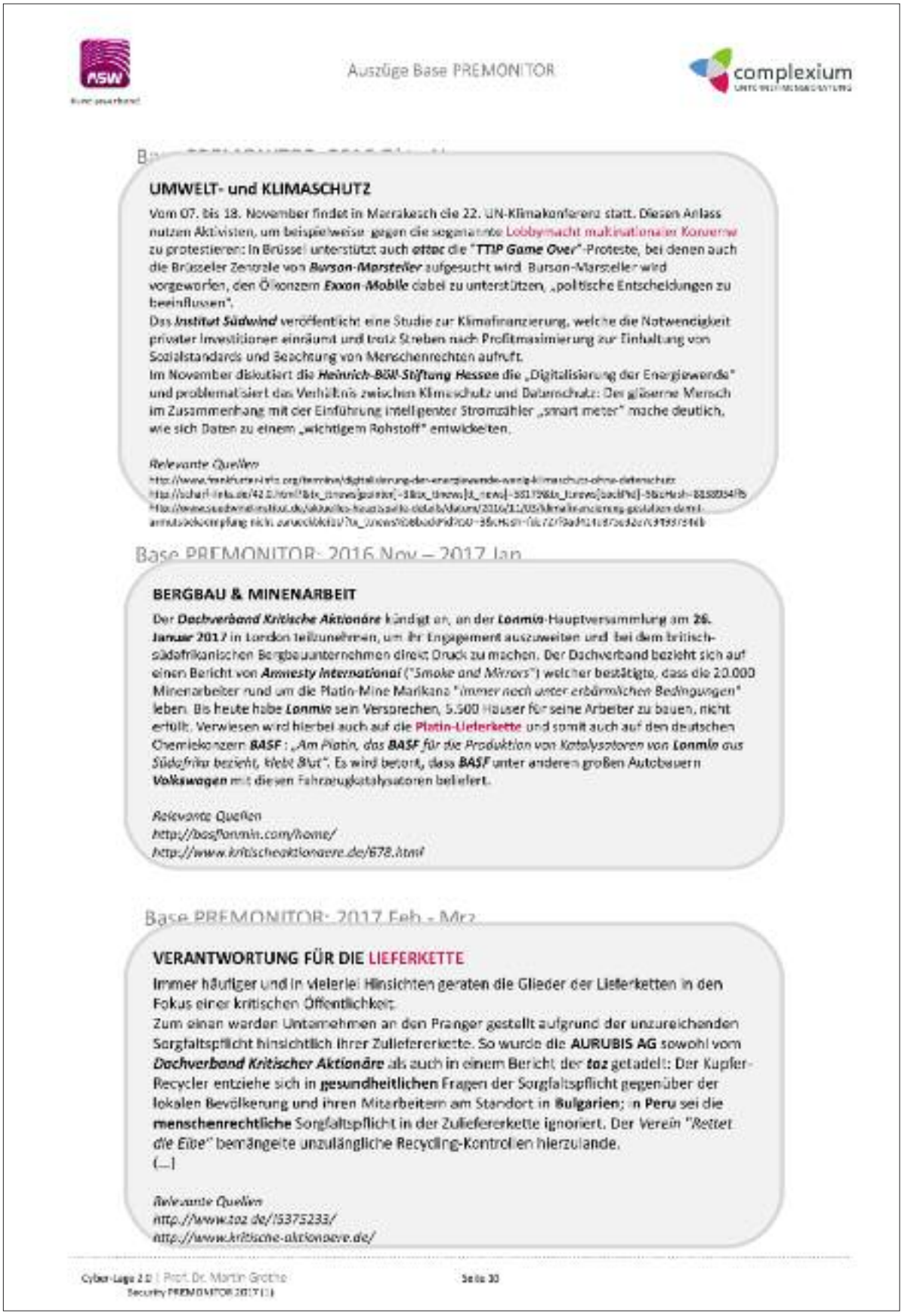
Gegen mangelhafte Tierhaltung, Versuchstier-Transporte und Tierversuche gehen Aktivisten mit physischen und Online-Protesten vor. Zudem wird eine Datenbank veröffentlicht, welche dokumentiert, dass viele deutsche Stiftungen und Vereine, welche sich durch Spendengelder finanzieren, die tierexperimentelle Forschung unterstützen.

Mit einer Blockade am 20. Juli und einem Camp vom 29. Juli bis zum 4. August in Wietzen-Holte protestieren die Tierbefreiungsaktivisten von ***kampagne gegen tierfabriken*** in Wietzen-Holte gegen die Ausbaupläne der *Nienburger Geflügelspezialitäten* (***Wiesenhof***).
PETA stellt **Strafanzeigen** gegen die Betreiber der zehn Stallanlagen. Unzureichende Brandschutzmaßnahmen hätten bei **Stallbränden** zum Tod der Tiere geführt.
Am 23. Juli findet der **europaweite Aktionstag** gegen den ***Botox-Hersteller Elsai*** statt. In Deutschland mobilisieren sich Aktivisten in Frankfurt und München gegen die Tötung von 90 000 Mäusen für die Herstellung von Botox.

In Facebook-Kommentaren zum *taz*-Artikel über Tierethik werden die sogenannten Profiteure von Tierversuchen an den Pranger gestellt: etwa Tierzuchtkonzerne (*Marshall, Harlan, Charles River*), Transportgesellschaften (*Air France/KLM*), Laborbedarfshersteller und die Pharmaindustrie.
Auch ***PETAZWEI*** verurteilt das Tierversuchsinstitut ***Covance*** (auch in München), das Affen an Überhitzung sterben ließ und startet eine **Petition** an ***Air France***, die als einzige Fluggesellschaft noch Affen in Labore transportiert.

Mitte August veröffentlicht der Verein ***Ärzte gegen Tierversuche*** eine **Datenbank**, die dokumentiert, welche Stiftungen und Vereine mit Spendengeldern Tierversuche finanzieren. Genannt werden u.a.: die ***Deutsche Krebshilfe***, die ***Deutsche Herzstiftung*** und die ***Herz-Lungen-Stiftung***, die ***Volkswagen Stiftung*** sowie die ***Daimler & Benz Stiftung***.

Wichtige direkte Quellen



Auszüge Base PREMONITOR

complexium

UMWELT- und KLIMASCHUTZ

Vom 07. bis 18. November findet in Marrakesch die 22. UN-Klimakonferenz statt. Diesen Anlass nutzen Aktivisten, um beispielsweise gegen die sogenannte Lobbymacht multinationaler Konzerne zu protestieren: In Brüssel unterstützt auch **attac** die "**TTIP *Game Over***"-Proteste, bei denen auch die Brüsseler Zentrale von ***Burson-Marsteller*** aufgesucht wird. Burson-Marsteller wird vorgeworfen, den Ölkonzern ***Exxon-Mobile*** dabei zu unterstützen, „politische Entscheidungen zu beeinflussen".
Das ***Institut Südwind*** veröffentlicht eine Studie zur Klimafinanzierung, welche die Notwendigkeit privater Investitionen einräumt und trotz Streben nach Profitmaximierung zur Einhaltung von Sozialstandards und Beachtung von Menschenrechten aufruft.
Im November diskutiert die ***Heinrich-Böll-Stiftung Hessen*** die „Digitalisierung der Energiewende" und problematisiert das Verhältnis zwischen Klimaschutz und Datenschutz: Der gläserne Mensch im Zusammenhang mit der Einführung intelligenter Stromzähler „smart meter" mache deutlich, wie sich Daten zu einem „wichtigem Rohstoff" entwickelten.

Relevante Quellen

Base PREMONITOR: 2016 Nov – 2017 Jan

BERGBAU & MINENARBEIT

Der ***Dachverband Kritische Aktionäre*** kündigt an, an der ***Lonmin***-Hauptversammlung am **26. Januar 2017** in London teilzunehmen, um ihr Engagement auszuweiten und bei dem britisch-südafrikanischen Bergbauunternehmen direkt Druck zu machen. Der Dachverband bezieht sich auf einen Bericht von ***Amnesty International*** ("*Smoke and Mirrors*") welcher bestätigte, dass die 20.000 Minenarbeiter rund um die Platin-Mine Marikana "*immer noch unter erbärmlichen Bedingungen*" leben. Bis heute habe ***Lonmin*** sein Versprechen, 5.500 Häuser für seine Arbeiter zu bauen, nicht erfüllt. Verwiesen wird hierbei auch auf die **Platin-Lieferkette** und somit auch auf den deutschen Chemiekonzern ***BASF*** : „*Am Platin, das **BASF** für die Produktion von Katalysatoren von **Lonmin** aus Südafrika bezieht, klebt Blut*". Es wird betont, dass ***BASF*** unter anderem großen Autobauern **Volkswagen** mit diesen Fahrzeugkatalysatoren beliefert.

Relevante Quellen
http://basflonmin.com/home/
http://www.kritischeaktionaere.de/678.html

Base PREMONITOR: 2017 Feb – Mrz

VERANTWORTUNG FÜR DIE LIEFERKETTE

Immer häufiger und in vielerlei Hinsichten geraten die Glieder der Lieferketten in den Fokus einer kritischen Öffentlichkeit.
Zum einen werden Unternehmen an den Pranger gestellt aufgrund der unzureichenden Sorgfaltspflicht hinsichtlich ihrer Zuliefererkette. So wurde die **AURUBIS AG** sowohl vom ***Dachverband Kritischer Aktionäre*** als auch in einem Bericht der ***taz*** getadelt: Der Kupfer-Recycler entziehe sich in **gesundheitlichen** Fragen der Sorgfaltspflicht gegenüber der lokalen Bevölkerung und ihren Mitarbeitern am Standort in **Bulgarien**; in **Peru** sei die **menschenrechtliche** Sorgfaltspflicht in der Zuliefererkette ignoriert. Der Verein "*Rettet die Elbe*" bemängelte unzulängliche Recycling-Kontrollen hierzulande.
(...)

Relevante Quellen
http://www.taz.de/!5375233/
http://www.kritische-aktionaere.de/

Cyber-Lage 2.0 | Prof. Dr. Martin Grothe
Security PREMONITOR 2017 | 3

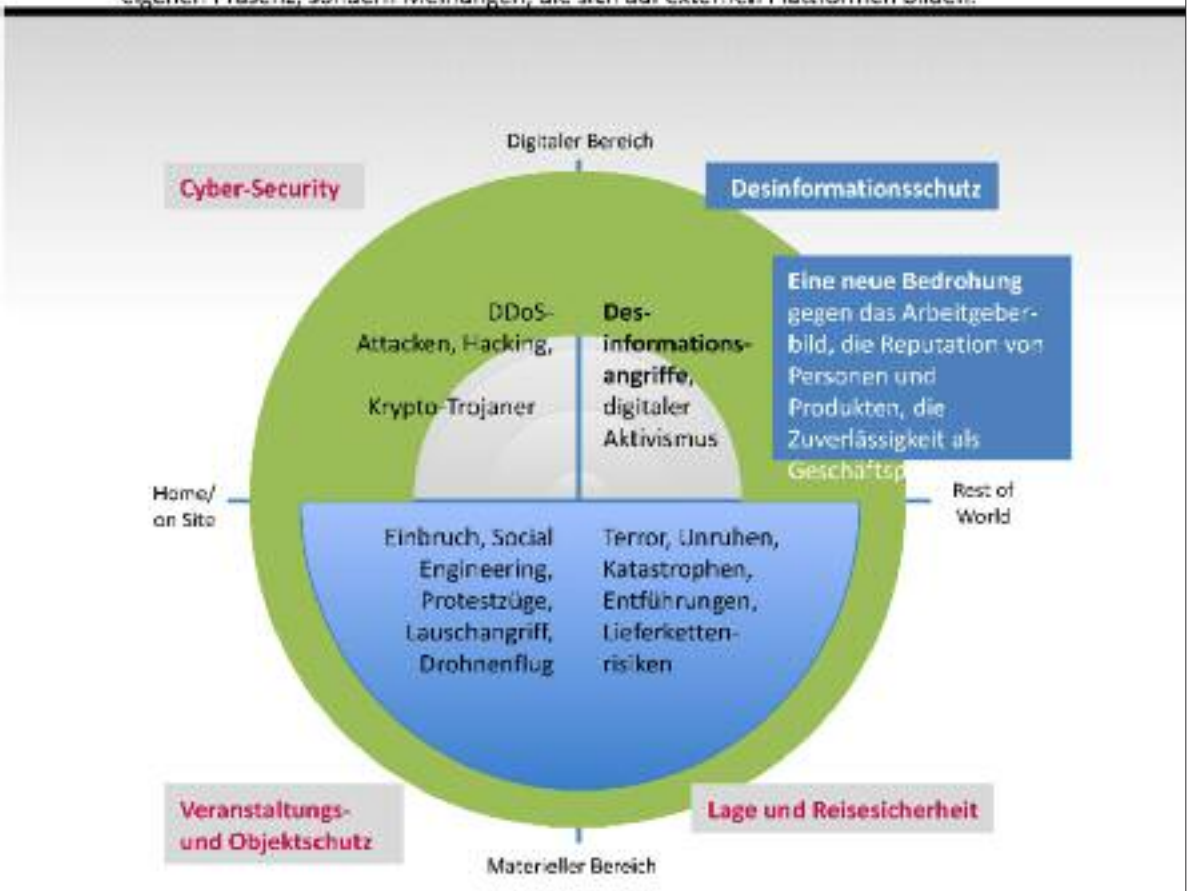
Seite 30

Desinformation

Eine neue Bedrohung

Desinformation ist die gezielte Verbreitung falscher oder irreführender Information, Motivation ist die Beeinflussung der Meinung der Öffentlichkeit/von Gruppen/Einzelpersonen, um politische/wirtschaftliche Ziele zu fördern.

Ziele sind nicht wie im Bereich der Cyber Security Soft- oder Hardware innerhalb der eigenen Präsenz, sondern Meinungen, die sich auf externen Plattformen bilden.



Ein hoher **Bedrohungslevel** entsteht durch Identitätsdiebstahl/-design, Social Bots (Botnets) und Nutzung der Netzwerkdynamik. Digitale **Früherkennung** ist notwendig.

1. Angreifer streuen Fake News oder erstellen Bots (auch in Wartestellung)
2. Bots initiieren oder verstärken Beiträge
3. Nutzer liken/sharen, Medien greifen trending Topics auf ⊡ Wahrnehmung!

Desinformation

Eine neue Bedrohung

In der Politik werden inzwischen tagtäglich Falschinformationen in Umlauf gebracht: Bewusste Desinformation, um einem Gegner zu schaden, um eigene Vorteile zu erringen. Dies kann ganz offen oder aber subtil erfolgen. Dies kann erfolgen, um offensiv von eigentlich kritischen Themen abzulenken oder um unterschwellig Meinung zu beeinflussen.

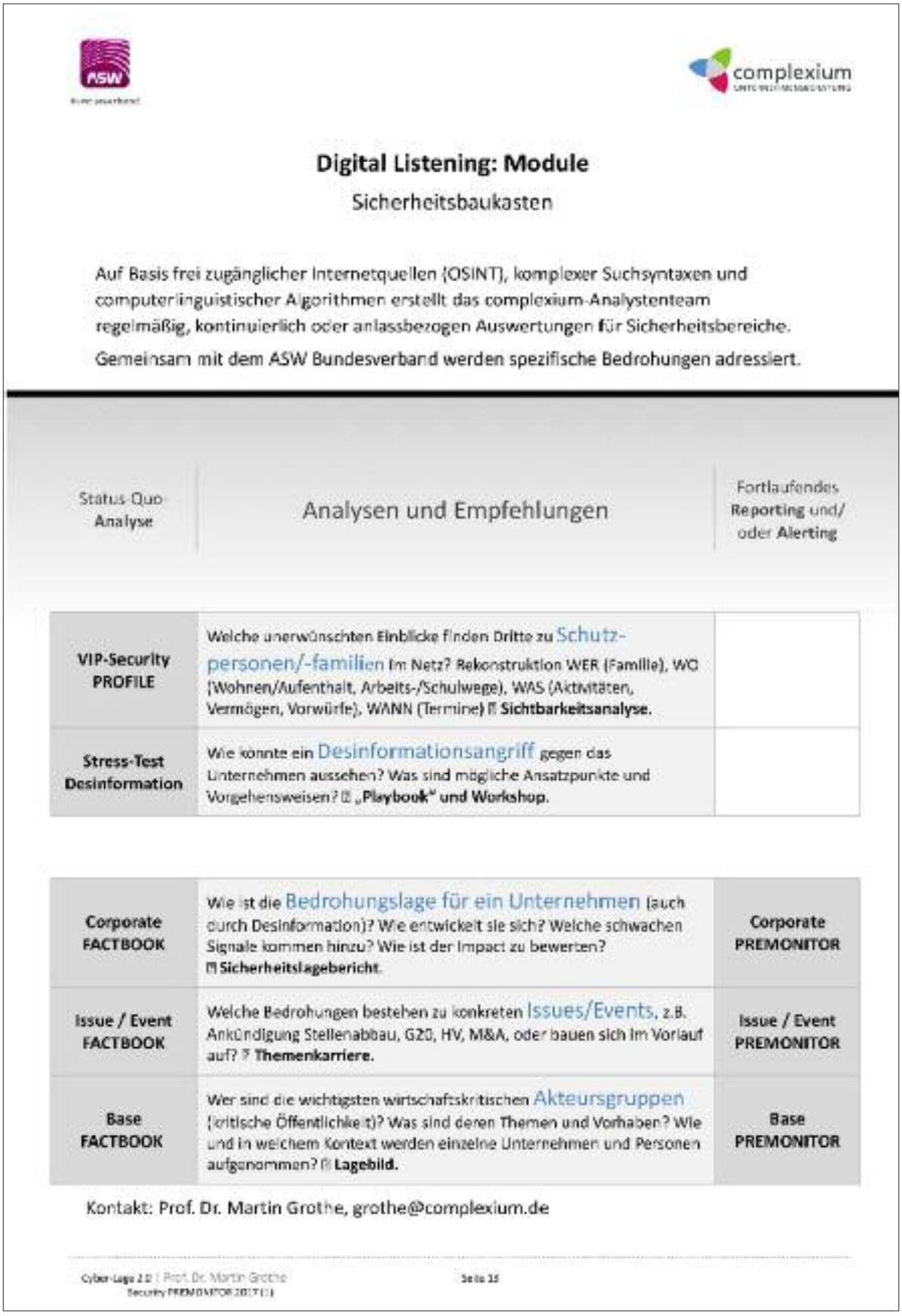
Die öffentliche digitale Kommunikation im Internet bietet den zentralen Verbreitungsraum für Desinformationsmaßnahmen. Falsche Identitäten und Multiplikationsmechanismen bilden einen gefährlichen Werkzeugkasten. Wird dieses machtvolle Arsenal auf die Politik beschränkt bleiben? Die Digitalisierung macht solche Angriffsszenarien erschwinglich und damit auch für und gegen Unternehmen einsetzbar. Folglich ist ein Einsatz im aggressiven Unternehmenswettbewerb nur eine Frage der Zeit. Es steht die Vermutung im Raum, dass die ersten Desinformationsangriffe bereits hinter uns liegen. Weil jedoch die meisten Unternehmen ihre Stakeholder, Zielgruppen und Gegnerschaften nicht per **Digital Listening** im Blick haben, werden diese Angriffe schlicht nicht erkannt. Hören wir aber doch einmal hinein, wie ein solcher Angriff ablaufen könnte. Heute Mittag.

„Etwas war gerade anders als sonst, dachte Kurt F., der Geschäftsführer, eben in der Pause. Peter K., der altgediente Personalleiter kam deutlich später als sonst zu der üblichen Runde. Es werde immer schwieriger, gute Kandidaten zu bekommen. Wieder war jemand abgesprungen. Anscheinend geistern einige negative Kommentare über das Unternehmen durch das Internet, sagt er. Ärgerlich. Besonders, weil immer noch unter Hochdruck das Entwicklerteam für das neue Großprojekt gesucht wird. Top Prio.

Aber Gerd S., der Geschäftsentwickler, hatte direkt abgewunken: So eilig wäre es dann doch nicht. Der neuen Großkunde, jedenfalls der Fast-schon-Kunde, hatte plötzlich noch etwas Bedenkzeit eingefordert. Compliance-Themen seien aufgetaucht, irgendwo hatte jemand gestreut, dass bei den letzten Projekten nicht alles mit rechten Dingen zugegangen sei. Anonym natürlich, aber anscheinend glaubwürdig. Dauert also, aber hoffentlich brennt da nichts mehr an. Dieses Projekt war zentral für die geplante Expansion. Endlich wären sie den Konkurrenten gleich mehrere Schritte enteilt. Und zwar in deren Heimatmarkt!

Kurt F., der Geschäftsführer wusste, dass die neue Produktlinie dem innovativen Mittelständler auch helfen würde, die anschwellende Kritik gegenüber den alten Versionen abzuschütteln. So schlecht, wie immer – und gerade jetzt besonders – behauptet wird, waren die Lösungen nämlich gar nicht. Der Chef-Entwickler wirkte derzeit zwar etwas abgelenkt, aber wer weiß, woran das wieder liegt. Man munkelt von neuen Herausforderungen. Jedenfalls steht er gerade mit seinem Handy am Ohr draußen vor der Tür. Im Regen. Headhunter? Es läuft nicht rund, dachte Kurt F., aber momentan gab es für ihn Wichtigeres."

Noch sind viele Sicherheitsbereiche darauf fokussiert, das eigene Gelände zu sichern, materiell und digital. Natürlich werden Schutzpersonen auch auf Reisen außerhalb des eigenen Gestaltungsbereiches begleitet. **Die Erkenntnis aber, dass die Sicherheit auch auf digitalen Bereichen außerhalb der eigenen Domänen massiv angegriffen werden kann, ist noch relativ wenig verbreitet.**



ASW Bundesverband

complexium

Digital Listening: Module

Sicherheitsbaukasten

Auf Basis frei zugänglicher Internetquellen (OSINT), komplexer Suchsyntaxen und computerlinguistischer Algorithmen erstellt das complexium-Analystenteam regelmäßig, kontinuierlich oder anlassbezogen Auswertungen für Sicherheitsbereiche.

Gemeinsam mit dem ASW Bundesverband werden spezifische Bedrohungen adressiert.

Status-Quo-Analyse	Analysen und Empfehlungen	Fortlaufendes **Reporting** und/ oder **Alerting**
VIP-Security PROFILE	Welche unerwünschten Einblicke finden Dritte zu Schutz-personen/-familien im Netz? Rekonstruktion WER (Familie), WO (Wohnen/Aufenthalt, Arbeits-/Schulwege), WAS (Aktivitäten, Vermögen, Vorwürfe), WANN (Termine) → **Sichtbarkeitsanalyse.**	
Stress-Test Desinformation	Wie könnte ein Desinformationsangriff gegen das Unternehmen aussehen? Was sind mögliche Ansatzpunkte und Vorgehensweisen? → **„Playbook" und Workshop.**	
Corporate FACTBOOK	Wie ist die Bedrohungslage für ein Unternehmen (auch durch Desinformation)? Wie entwickelt sie sich? Welche schwachen Signale kommen hinzu? Wie ist der Impact zu bewerten? → **Sicherheitslagebericht.**	**Corporate PREMONITOR**
Issue / Event FACTBOOK	Welche Bedrohungen bestehen zu konkreten Issues/Events, z.B. Ankündigung Stellenabbau, G20, HV, M&A, oder bauen sich im Vorlauf auf? → **Themenkarriere.**	**Issue / Event PREMONITOR**
Base FACTBOOK	Wer sind die wichtigsten wirtschaftskritischen Akteursgruppen (kritische Öffentlichkeit)? Was sind deren Themen und Vorhaben? Wie und in welchem Kontext werden einzelne Unternehmen und Personen aufgenommen? → **Lagebild.**	**Base PREMONITOR**

Kontakt: Prof. Dr. Martin Grothe, grothe@complexium.de

Cyber-Lage 2.0 | Prof. Dr. Martin Grothe
Security PREMONITOR 2017 | 3

Seite 15

complexium ist Partner des ASW Bundesverbandes

Profil complexium

Früherkennung im Digitalraum. Seit 2004

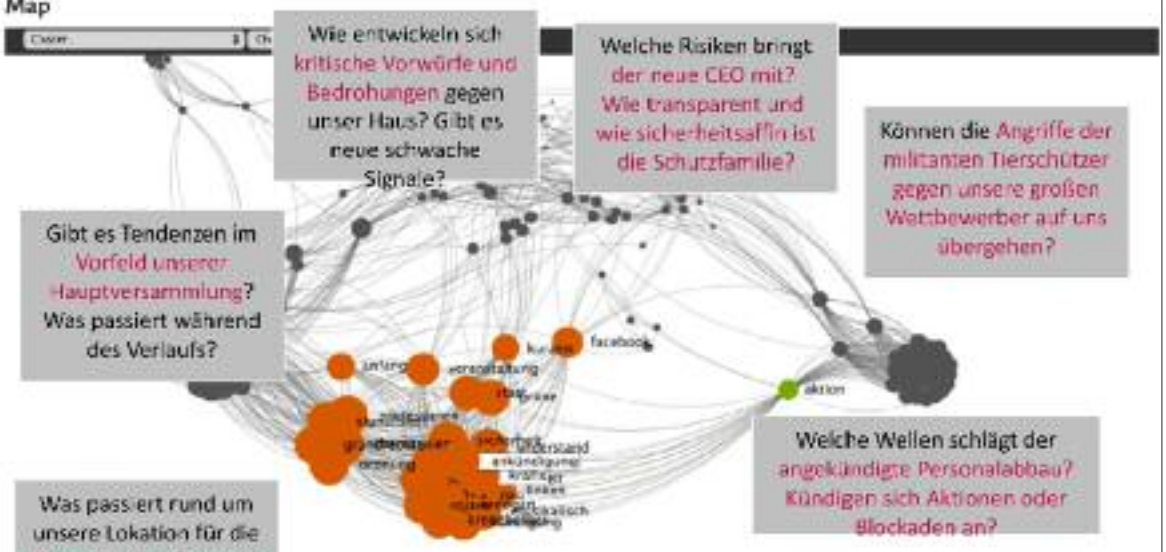
Wir arbeiten mit Konzernsicherheiten aus den Bereichen Auto, Bank, Chemie, Defense, Energie, FMCG, Industrie, Pharma und Versicherung sowie Family Offices zusammen. Wir unterstützen unsere Klienten mit Früherkennung und Inhaltserschließung.

Unsere Analysten stellen Ergebnisse und Ableitungen als Alert, Report oder per Telefon dar. Hierzu nehmen unserer Systeme öffentliche digitale Beiträge (OSINT) zeitnah auf. Algorithmen finden unerwartete Auffälligkeiten und suchen nach definierten Begriffen.

FACTBOOK:
Bestandsaufnahme

PREMONITOR:
Kontinuierliches Reporting und/oder Alerting

Map



GALAXY von complexium erleichtert das Finden im Digitalraum. Crawler nehmen potenziell relevante Beiträge in nahezu Echtzeit auf. Computerlinguistische Algorithmen erschließen die Inhalte ohne Vorgabe. Analysten erhalten aktuelle Transparenz und Übersicht.

Profil ASW Bundesverband

Wir. Unternehmen. Sicherheit.

Der ASW Bundesverband vertritt die Sicherheitsinteressen der deutschen Wirtschaft. Er schafft Bewusstsein für das Thema Wirtschaftsschutz – bei den Unternehmen, der Politik und in den Medien. Er sorgt für einen Informationsaustausch – kontinuierlich und anlassbezogen – zwischen Unternehmen und den Sicherheitsbehörden und stellt den Unternehmen aufbereitete Informationen zur Verfügung. Der Verband schafft für alle Interessierten ein verlässliches Netzwerk.

Kompetenz-Center:
Der ASW Bundesverband unterhält sieben Kompetenz-Center – von Anti-Fraud-Management über Lage und Reisesicherheit bis zu Wirtschaftsschutz und Spionageabwehr – in denen seine Mitglieder zusammen mit externen Partnern und Sicherheitsexperten den jeweiligen Bedrohungen gezielt entgegenarbeiten.

Leitfäden und Leitblätter:
Ob ausführlicher oder kurz und bündig: Mit seinen Informationsmaterialien zu unterschiedlichen
en gibt der ASW Bundesverband praktische
iner Vielzahl von Themen.

Leitveranstaltungen und Expertenworkshops:
Sensible Themen behandelt der ASW Bundesverband in vertraulichen Workshops, für große Themen bereitet er aber auch große Bühnen – wie beim Deutschen Sicherheitstag oder der Sicherheitstagung mit dem Bundesamt für Verfassungsschutz (BfV).

Herausgeber des Wirtschaftsgrundschutz-Handbuchs:
Der Wirtschaftsgrundschutz bietet Sicherheitsverantwortlichen in Firmen Handlungsempfehlungen und Orientierung für eine effektive Unternehmenssicherheit. Das Handbuch wird vom ASW Bundesverband, dem Bundesamt für Verfassungsschutz (BfV) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegeben.

Mitglied der Initiative Wirtschaftsschutz:
Die Initiative Wirtschaftsschutz ist der verbindliche Rahmen der gemeinsamen Aktivitäten von Staat und Wirtschaft für mehr Wirtschaftsschutz in Deutschland. Der ASW Bundesverband ist

Kontakt

Wir freuen uns auf Ihr Feedback!

Sie möchten mehr über die Themen Früherkennung und Desinformation erfahren?

Dann treten Sie mit uns in Kontakt. Gemeinsam mit Deloitte führen der ASW Bundesverband und complexium eine Studie zum Thema Desinformation durch. Nehmen Sie gerne teil!

Zur Umfrage

Welche **Auswirkungen** können Falschinformationen auf Unternehmen haben?

Können sie gar ihre **Sicherheit** bedrohen?

Falls ja, wie könnten sich Unternehmen davor **schützen**?

Nehmen Sie an der Umfrage zur Studie teil und erhalten Sie auf Wunsch den erweiterten Bericht zur Studie!

https://asw-bundesverband.de/desinformation

Jan Wolter
wolter@asw-bundesverband.de
+49 (0) 30 200 77 200

https://asw-bundesverband.de
https://twitter.com/ASW_Bund
https://vimeo.com/user39500846

Bundesverband

Prof. Dr. Martin Grothe
grothe@complexium.de
www.complexium.de
+49 (0) 30 200 59 261

EU-Richtlinie Know-how-Schutz

Alexander Haertel, Kather Augenstein Rechtsanwälte


ÜBERBLICK
Geheimnisschutz nach dem UWG
EU-Richtlinie
Stand des europäischen Gesetzgebungsverfahrens
Inhaltliche Eckpunkte der geplanten Richtlinie


GEHEIMNISSCHUTZ NACH
DEM UWG

AKTUELLER SCHUTZ IN DEUTSCHLAND

- Der Schutz von Geschäftsgeheimnissen in Deutschland bislang:
  - **Aktiver Schutz:** § 17 UWG
    - Nur wenige Handlungen abgedeckt, z.B. Offenlegung und Verwendung von Geschäftsgeheimnissen durch Mitarbeiter, Verstoß gegen NDA, etc.
    - Sofern Handlungen nicht genannt sind, sind diese im Grundsatz zulässig
    - Ein weitergehender Schutz muss vertraglich vereinbart werden
  - **Passiver Schutz:** Sollten Dokumente in einem Gerichtsverfahren vorgelegt werden müssen, so kann der Vorlegende Teile schwärzen (z.B. §§ 140b.4, 140c.1 PatG).

Kather Augenstein Rechtsanwälte

GEHEIMNISSCHUTZ NACH DEM UWG

§ 17 UWG – Schutzgegenstand

- Schützt Geschäfts- und Betriebsgeheimnisse vor unbefugter Verwertung & Weitergabe

= jede im Zusammenhang mit einem Geschäftsbetrieb stehende Tatsache, die nur einem eng begrenzten Personenkreis bekannt ist und nach dem Willen des Betriebsinhabers aufgrund eines berechtigten wirtschaftlichen Interesses geheim gehalten werden soll

- Betriebsgeheimnis: Kenntnisse und Tatsachen im Bereich der Technik
- Geschäftsgeheimnis: Kenntnisse und Tatsachen im kaufmännischen Bereich

Kather Augenstein Rechtsanwälte

EU-RICHTLINIE

Kather Augenstein Rechtsanwälte

I. RICHTLINIENVORSCHLAG

- *‚Vorschlag für eine Richtlinie über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung‘, 26.04.2016,* ***2013/0402 COD***
- Zweck: Rechtsangleichung auf dem Binnenmarkt; Förderung von Innovation und Vermeidung übertriebener Geheimhaltungsmaßnahmen (vgl. auch Art. 39 TRIPS)
- Zentrale Änderungen:
  - Definition des Begriffs: Geschäftsgeheimnis
  - Schutzvoraussetzungen
  - Spezifische verfahrensrechtliche Maßnahmen

Kather Augenstein Rechtsanwälte

II. STAND DES GESETZGEBUNGSVERFAHRENS

1. **28.11.2013:** Vorschlag der Kommission, Art. 294 Abs. 2AEUV
2. **25.03.2014:** Stellungnahme des Wirtschafts- und Sozialausschusses, Art. 114 Abs. 1 AEUV
3. **26.05.2014:** Erörterung im Rat
4. **14.04.2016:** Billigung durch Parlament in 1. Lesung, Art. 294 Abs. 3 AEUV
5. **26.05.2016:** Ratsbeschluss, Annahme der Richtlinie, Art. 294 Abs. 4 AEUV
   - Umsetzungsfrist für die Mitgliedstaaten (Art. 288 Abs. 3 AEUV): 2 Jahre

Kather Augenstein Rechtsanwälte

III. INHALTLICHE ECKPUNKTE

Definition: Geschäftsgeheimnis, Art. 2 Nr. 1 RL

1. „Geschäftsgeheimnis" Informationen, die alle nachstehenden Kriterien erfüllen:

   a) Sie sind in dem Sinne geheim, dass sie weder in ihrer Gesamtheit noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne weiteres zugänglich sind;

   b) sie sind von kommerziellem Wert, weil sie geheim sind;

   c) sie sind Gegenstand von den Umständen entsprechenden angemessenen Geheimhaltungsmaßnahmen durch die Person, die die rechtmäßige Kontrolle über die Informationen besitzt;

Kather Augenstein Rechtsanwälte

IV. INHALTLICHE ECKPUNKTE

Systematik der RL

- RL knüpft daran an, ob der Inhaber die Kontrolle über ein Geheimnis rechtmäßig besitzt
- Der rechtmäßige Besitz umfasst u.a. die unabhängige Entdeckung oder Schöpfung
- Auffangtatbestand: Jede Vorgehensweise, die mit einer seriösen Geschäftspraxis vereinbar ist.
- Reverse engineering gilt als rechtmäßiger Erwerb (!), Art. 3 Abs. 1 lit. b) RL

Kather Augenstein Rechtsanwälte

V. INHALTLICHE ECKPUNKTE

Tatbestände

- **Erwerb (Art. 4 Abs. 2 RL):** Rechtswidrig, wenn
  - Keine Zustimmung des Inhabers
  - Erlangung durch unbefugten Zugang/Aneignung/Kopie bzw. durch unseriöse Geschäftspraxis, Art. 4 Abs. 2 RL
- **Nutzung, Offenbarung (Art. 4 Abs. 3 f. RL):** Rechtswidrig, wenn
  - Keine Zustimmung des Inhabers
  - Rechtswidriger Erwerb, Verstoß gegen NDA oder sonstige vertragliche Verpflichtung
- Auch bei Nutzung in Kenntnis der rechtswidrigen Besitzerlangung durch einen Vorbenutzer
- **Verjährung**, Art. 8 RL nach Recht der Mitgliedstaaten, d.h. §§ 194 ff. BGB, aber max. sechs Jahre, Art. 8 Abs. 2 RL

Kather Augenstein Rechtsanwälte

VI. INHALTLICHE ECKPUNKTE

Systematik der RL

- RL schützt auch Produkte

4. „rechtsverletzende Produkte" Produkte, deren Konzeption, Merkmale, Funktionsweise, Herstellungsprozess oder Marketing in erheblichem Umfang auf rechtswidrig erworbenen, genutzten oder offengelegten Geschäftsgeheimnissen beruhen.

(5) Das Herstellen, Anbieten oder Inverkehrbringen von rechtsverletzenden Produkten oder die Einfuhr, Ausfuhr oder Lagerung von rechtsverletzenden Produkten für diese Zwecke stellt ebenfalls eine rechtswidrige Nutzung eines Geschäftsgeheimnisses dar, wenn die Person, die diese Tätigkeiten durchführt, wusste oder unter den gegebenen Umständen hätte wissen müssen, dass das Geschäftsgeheimnis rechtswidrig im Sinne des Absatzes 3 genutzt wurde.

Kather Augenstein Rechtsanwälte

VII. INHALTLICHE ECKPUNKTE

Rechtsfolgen

- **Vorbeugender Rechtschutz** (Art. 10 RL): Unterlassung, Beschlagnahme und Herausgabe mutmaßlich rechtsverletzender Produkte
- **Unterlassung, Vernichtung, Rückruf** (Art. 12 RL); Zwangsgeld möglich (Art. 16 RL)
- **Schadensersatz** (Art. 14 RL): dreifache Berechnungsmethode
- Gewährleistung der Vertraulichkeit im Gerichtsverfahren, Art. 9 RL

Kather Augenstein Rechtsanwälte

VIII. FRAGEN

Praktische Beispiele (Workshop)

- **Frage 1:** Was sind taugliche Sicherungsmaßnahmen?
- **Frage 2:** Wie können diese Sicherungsmaßnahmen im Prozess nachgewiesen werden?
- **Frage 3:** Wann hat ein Geschäftsgeheimnis einen kommerziellen Wert?
- **Frage 4:** Welche Nachteile bei der Rechtsdurchsetzung kann es geben?
- **Frage 5:** Welchen Risiken sind Wettbewerber ausgesetzt?

Kather Augenstein Rechtsanwälte

Kather Augenstein Rechtsanwälte

Programmablauf

Bundesamt für Verfassungsschutz

ASW Bundesverband

Tagungsprogramm

Neue Businessmodelle und Industrie im Wandel – Chancen und Risiken für die Unternehmenssicherheit

11. BfV/ASW-Sicherheitstagung

Datum:	27. April 2017
Ort:	Bundesakademie für Sicherheitspolitik, Ossietzkystraße 44/45, 13187 Berlin
09.30 - 10.00 Uhr	Anreise und Akkreditierung
	Pressekonferenz **Präsident BfV/Vorstandsvorsitzender ASW Bundesverband**
(Teil 1 mit Medienvertretern)	
10.00 - 10.45 Uhr	**Begrüßung und Eröffnung** Volker Wagner, Vorstandsvorsitzender, ASW Bundesverband Dr. Hans-Georg Maaßen, Präsident, Bundesamt für Verfassungsschutz Dr. Karl-Heinz Kamp, Präsident, Bundesakademie für Sicherheitspolitik
10.45 - 11.30 Uhr	**Künstliche Intelligenz und menschliche Dummheit: Neue Herausforderungen für unsere Sicherheit** Karl Olsberg, Schriftsteller und Unternehmer
11.30 - 12.00 Uhr	**Notfallmanagement, ein Muss in Zeiten des Wandels – Handbuch Wirtschaftsgrundschutz** Prof. Timo Kob, Vorstand HiSolutions AG /ASW Bundesverband
12.00 - 13.30 Uhr	**Mittagspause**

Deloitte. POWER PERSONEN-OBJEKT-WERKSCHUTZ GMBH

Durchgeführt von ASW Projekt GmbH

Bundesamt für Verfassungsschutz

ASW Bundesverband

(Teil 2 ohne Medienvertretern)

13.30 - 15.00 Uhr	**Workshops** 1) Desinformation Prof. Martin Grothe, Complexium 2) Connected Car Stephan Gerhager, Allianz Deutschland 3) Blockchain Joachim Lohkamp, Jolocom 4) EU-Richtlinie Know-How-Schutz Alexander Haertel, Kather Augenstein Rechtsanwälte 5) Authentication of data (englisch) Adam Stogdale, Deloitte
15.00 - 15.30 Uhr	**Kaffee- und Kommunikationspause**
15.30 - 16.15 Uhr	**Panel 1 Ergebnisse aus den Workshops** Connected Car, EU-Richtlinie Know-how-Schutz Moderation: Herbert Kurek
16.15 - 17.00 Uhr	**Panel 2 Ergebnisse aus den Workshops** Desinformation, Blockchain, Authentication of data Moderation: Jan Wolter
17.00 Uhr	**Verabschiedung & Ende der Veranstaltung**

Änderungen des Programms vorbehalten

Deloitte. CK POWER PERSONEN-OBJEKT-WERKSCHUTZ GMBH

Durchgeführt von ASW

Bildmaterial

Jan Wolter, Geschäftsführer ASW Bundesverband,
Dr. Hans-Georg Maaßen, Präsident Bundesamt für Verfassungsschutz,
Volker Wagner, Vorstandsvorsitzender ASW Bundesverband

Jan Wolter im Gespräch mit Dr. Hans-Georg Maaßen

Publikum


Bundesamt für
Verfassungsschutz
ASW
Bundesverband
Sicherheitstagu
des BfV und des ASW Bundesverband

Volker Wagner und das Wirtschaftsschutzteam des BfV

Fachgespräche

Impressum

Herausgeber
Bundesamt für Verfassungsschutz
Referat Wirtschaftsschutz
Merianstraße 100
50765 Köln

Tel.: +49 (0) 221/792-3322
Fax: +49 (0) 221/792-2915

wirtschaftsschutz@bfv.bund.de
www.verfassungsschutz.de
www.wirtschaftsschutz.info

Gestaltung und Druck
Bundesamt für Verfassungsschutz
Print- und MedienCenter

Bildnachweis
© Nmedia- Fotolia.com
© ASW Bundesverband und BfV

Stand
September 2017

initiative
wirtschaftsschutz

Gemeinsam. Werte. Schützen.

www.wirtschaftsschutz.info