2. Wirtschaftsschutztag Sachsen-Anhalt

Gut geschützt ist schwer gehackt

IHK Industrie- und Handelskammer Magdeburg
Regional. Unternehmerisch. Stark.

SACHSEN-ANHALT
Ministerium für Inneres und Sport

IHK Industrie- und Handelskammer Halle-Dessau

Vorwort

Jochen Hollmann
Leiter der Abteilung Verfassungsschutz im Ministerium für Inneres und Sport des Landes Sachsen-Anhalt

Mehr als die Hälfte der Unternehmen (53 Prozent) sind in den vergangenen zwei Jahren Opfer von Datendiebstahl, Spionage oder Sabotage geworden. Weitere 26 Prozent der Unternehmen vermuten, Opfer solcher Angriffe geworden zu sein; denn nicht immer lässt sich zweifelsfrei feststellen, ob wirklich Daten abgeflossen sind. Häufig bleiben Angriffe unerkannt. Dies ergab eine aktuelle Studie des Digitalverbandes Bitkom e. V. „Wirtschaftsschutz in der digitalen Welt“ vom Juni 2017. An der repräsentativen Umfrage waren mehr als 1.000 Geschäftsführer und Sicherheitsverantwortliche quer durch alle Branchen beteiligt.

Betroffen sind Unternehmen aller Wirtschaftszweige, besonders häufig ist der Mittelstand das Angriffsziel. Dafür gibt es zwei Gründe:

1. Der Mittelstand ist besonders innovativ.
2. Viele Mittelständler werden vergleichsweise leicht zum Opfer, da sie sich häufig noch nicht hinreichend gegen digitale Angriffe schützen. Eingebunden in die Lieferketten großer Konzerne werden mittelständische Unternehmen mitunter auch als Einfallstor für Angriffe auf Großunternehmen missbraucht.

Oftmals wird die Bedeutung des Faktors Mensch unterschätzt. Neben dem Innentäter, der widerrechtlich Unternehmensgeheimnisse der Konkurrenz oder fremden Nachrichtendiensten zuleitet, spielt insbesondere Social Engineering eine wesentliche Rolle, um die Mitarbeiter auszutricksen. Bei rund jedem fünften Unternehmen waren die Cyberangriffe mittels Social Engineering vorbereitet worden. So ist zum Beispiel bekannt geworden, dass Angreifer versuchten, Namen und Funktionen von Beschäftigten herauszufinden, indem sie sich am Telefon als vermeintliche Mitarbeiter eines IT-Dienstleisters („Helpdesk“) oder als Paketbote ausgaben. Diese Informationen nutzten sie, um persönliche und für den Empfänger inhaltlich plausible E-Mails zu verfassen, die die Mitarbeiter des Unternehmens dazu verleiten sollten, einen mit Malware verseuchten Anhang zu öffnen.

Insgesamt wird der in der Bundesrepublik Deutschland durch Datendiebstahl entstehende Schaden auf nahezu 55 Milliarden Euro pro Jahr geschätzt. Das bedeutet ein Anstieg von 4 Milliarden Euro pro Jahr seit 2015.
62 % der befragten Unternehmen gaben an, dass die entstandenen Schäden auch durch das Verhalten aktueller oder früherer Mitarbeiter verursacht wurden.

Die Bedrohungslage deutscher Unternehmen und Behörden veränderte sich demzufolge nicht zum Besseren, vielmehr traten neben die bekannten Angriffsformen Angriffe mit neuer Qualität. Um dazu zu informieren, veranstaltete am 25. Oktober 2017 die Abteilung Verfassungsschutz des Ministeriums für Inneres und Sport des Landes Sachsen-Anhalt in Kooperation mit den Industrie- und Handelskammern Sachsen-Anhalts den zweiten Wirtschaftsschutztag des Landes Sachsen-Anhalt im Ludwig-Wucherer-Saal der Industrie und Handelskammer Halle-Dessau in Halle (Saale).

Unter dem Titel **„Gut geschützt ist schwer gehackt“** wandten sich Experten von Sicherheitsbehörden des Landes Niedersachsen, von der Otto-von-Guericke-Universität Magdeburg sowie aus der Wirtschaftspraxis an das interessierte Fachpublikum mit ca. 80 Teilnehmenden aus Wirtschaft und Verwaltung.

Ziel des zweiten Wirtschaftsschutztages war es insbesondere, Wirtschaftsunternehmen für ein größeres IT-Sicherheitsbewusstsein, aktuelle Risiken und Bedrohungsszenarien zu sensibilisieren.

Frau Präsidentin Carola Schaar von der Industrie- und Handelskammer Halle-Dessau begrüßte die Tagungsteilnehmenden. Die Tagesmoderation der Veranstaltung hatte der Journalist Herr Ralf Geißler vom Mitteldeutschen Rundfunk übernommen.

Die Veranstaltung eröffnete Herr Minister Holger Stahlkecht, der in seiner Ansprache die Bedeutung der Wirtschaftsspionage deutlich machte. Er betonte, dass im vielbeschworenen Zeitalter der Globalisierung Unternehmen einer weltweiten Konkurrenz um Märkte, Produkte, Ideen, Technologien usw. ausgesetzt seien. Sowohl die Verfassungsschutzbehörde als auch die Unternehmensverantwortlichen des Landes Sachsen-Anhalt müssten sich der Herausforderung stellen, dass fremde Staaten diese Konkurrenzsituation mit gezielten Spionageangriffen immer stärker ausnutzen.

Herr Minister Stahlknecht wies auf die Expertise der Verfassungsschutzbehörde des Landes Sachsen-Anhalt hin. Unternehmen werden vom Wirtschaftsschutz präventiv und in Verdachtsfällen beraten und unterstützt. Betroffene Unternehmen könnten sich diskret, vertraulich und kostenfrei an den Wirtschaftsschutz wenden, insbesondere bei der Bearbeitung von Sicherheitsvorfällen, bei Cyberangriffen und beim Verdacht auf Wirtschaftsspionage.

Herr Dr. Hilmar Steffen, stellvertretender Leiter der Verfassungsschutzbehörde des Landes Sachsen-Anhalt, gab einen Überblick zur aktuellen Lage und zu neuen Gefährdungen insbesondere in den Bereichen Wirtschaftsspionage und elektronische Angriffe.

Herr Jörg Peine-Paulsen vom niedersächsischen Verfassungsschutz legte den Schwerpunkt seines Vortrags auf den „Faktor Mensch“ und sprach zu Aspekten der „Human Firewall“.

Als Praxisschwerpunkt der Tagung konnte Frau Britta Görtz von der praemandatum GmbH, Hannover, anhand prägnanter Beispiele darstellen, wie personenbezogene und betriebliche Daten mittels unterschiedlichster IT- und Internet-basierender Methoden derzeit akut bedroht werden. Sie machte deutlich, dass betrieblicher Datenschutz und Wirtschaftsschutz mit unterschiedlicher Herangehensweise überlappende Ziele verfolgen und thematisierte die am 25. Mai 2018 in Kraft getretene Datenschutzgrundverordnung (DSGVO).

Sachsen-Anhalts Wirtschaft ist auch für ihre traditionell guten Verbindungen zu russischen Unternehmen bekannt. Herr Dr. Tobias Köllner von der Otto-von-Guericke-Universität Magdeburg berichtete über den Einfluss der Russisch-Orthodoxen Kirche auf Staat, Gesellschaft und Wirtschaft im heutigen Russland.

Wir danken allen Mitwirkenden für Ihre Bereitschaft bei der Vorbereitung und Durchführung des zweiten Wirtschaftsschutztages.

Mit dieser Tagungsbroschüre werden die Ausführungen der Referenten dokumentiert, um den Teilnehmenden und allen interessierten Leserinnen und Lesern über den Tag der Veranstaltung hinaus zu vermitteln, dass es sich lohnt, insbesondere die eigenen Mitarbeiter für die Problematik zu sensibilisieren. Wir möchten so alle Akteure in der Wirtschaft ermutigen, sich

aktiv um Schutz zu kümmern: „Machen Sie Sicherheit zur Chefsache!“

Ergänzend dürfen wir auf die Internetseite des Verfassungsschutzes Sachsen-Anhalt unter: www.mi.sachsen-anhalt.de/verfassungsschutz mit weiteren für die Firmensicherheit relevanten Informationen verweisen.

Abschließend möchten wir darauf hinweisen, dass die Beiträge der Referentin und Referenten deren Auffassungen zum Ausdruck bringen.

Magdeburg, im Juni 2018

Inhalt

Begrüßung

Carola Schaar
Präsidentin der Industrie- und Handelskammer Halle-Dessau

Es gilt das gesprochene Wort!

Sehr geehrter Herr Minister Stahlknecht,

sehr geehrte Polizeipräsidenten Degner und Schomaker, meine sehr geehrten Unternehmerinnen und Unternehmer,
sehr geehrte Referenten,

im Namen der Industrie- und Handelskammern Magdeburg und Halle-Dessau sowie des Ministeriums für Inneres und Sport heiße ich Sie ganz herzlich willkommen zu unserem zweiten (!) Wirtschaftsschutztag Sachsen-Anhalt.

Warum betone ich, dass es sich um den ZWEITEN Wirtschaftsschutztag handelt? Nun, die Tatsache, dass wir uns bereits bei der ersten Veranstaltung im September 2015 darauf verständigt haben, das Thema Wirtschaftsschutz regelmäßig in den Fokus zu nehmen, sagt schon viel über die Brisanz dieses Themas aus. Zwei Jahre später nun also der nächste „Termin", gerne der Beginn einer Reihe.

Der bundesweite Gesamtschaden durch digitale Wirtschaftsspionage wird auf ca. 50 Mrd. Euro geschätzt. Pro Jahr! Jede zweite Firma war bereits von Datendiebstahl, Sabotage oder sogar Spionage betroffen, so die Ergebnisse einer Studie des Bundesverbandes Bitkom, dem Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.

Wir alle erinnern uns sicher noch an die weltweite Cyberattacke, die Mitte Mai dieses Jahres zehntausende Rechner in rund 80 Ländern lahmlegte. In Deutschland waren dabei Rechner der Deutschen Bahn betroffen. Ende Juni erwischte es den deutschen Kosmetikhersteller Beiersdorf bei einer weiteren Attacke.

Und das sind nur diejenigen Fälle, die aufgrund ihrer Dimension auch in der Öffentlichkeit bekannt werden. Die „Dunkelziffer" dürfte sehr viel höher liegen. In der Wirtschaft herrscht digitaler Krieg. Das muss man so deutlich sagen.

Nicht nur große, international agierende Unternehmen sind betroffen, sondern auch und insbesondere kleine und mittlere Firmen, vor allem solche mit beachtlicher Innovationsstärke. Denn jedes Unternehmen hat seine „Kronjuwelen". Doch die meisten Betroffenen scheuen davor zurück, sich an die Behörden zu wenden.

Die Täter sind dabei genauso verschiedenartig und vielschichtig wie die Probleme, die sie mit ihren Angriffen verursachen. Es können frustrierte oder ehemalige Mitarbeiter, kriminelle Strukturen, Konkurrenten, Einzeltäter bis hin zu fremden Nachrichtendiensten sein.

Der Schaden für die von den Attacken betroffenen Unternehmen reicht von Angriffen auf die Informations- und Kommunikationstechnik über Know-how-Verlust bis hin zur Zerstörung von ganzen

Rechnernetzwerken. Immer ausgereiftere Angriffstechniken sind eine massive Bedrohung für IT-Systeme, Kommunikationsstrukturen und Daten.

Das Thema Wirtschaftsschutz ist zu einer zentralen Frage geworden. Mit den Herausforderungen der rasant fortschreitenden Digitalisierung in der Wirtschaft (und Gesellschaft) wird die Bedeutung des Wirtschaftsschutzes noch zunehmen, da diese eine permanente Vernetzung verlangt. Und als wäre dies nicht Herausforderung genug für unsere Unternehmen, müssen sie auch noch die Datenschutz-Grundverordnung bis Mai kommenden Jahres umgesetzt haben. Andernfalls drohen hohe Bußgelder. Positiv an dieser neuen Verordnung ist immerhin, dass dann innerhalb der EU ein einheitliches Datenschutzrecht gilt. Auf der anderen Seite steht ein großer Aufwand an Vorarbeiten sowie Informations- und Dokumentationspflichten.

Meine sehr geehrten Damen und Herren,

wie gefährlich ist die Lage tatsächlich?
Wie werden Daten abgegriffen und wie können Sie sich schützen?
Wie kann Datenschutz attraktiv sein?

Diese und viele andere Fragen wollen wir heute beantworten.

Ganz wichtig bei solchen Veranstaltungen sind die persönlichen Erfahrungen und Beispiele. Deshalb freuen wir uns über einen Bericht aus der unternehmerischen Praxis und eine sicher spannende Podiumsdiskussion.

Ich wünsche uns allen eine informative und spannende Veranstaltung.

Sehr geehrter Herr Minister Stahlknecht, ich bitte Sie herzlich um Ihr Grußwort.

Grußwort

Holger Stahlknecht
Minister für Inneres und Sport
des Landes Sachsen-Anhalt

Es gilt das gesprochene Wort!

Sehr geehrte Frau Schaar,
sehr geehrter Herr Olbricht,
sehr geehrte Damen und Herren,

nach einem erfolgreichen Auftakt mit der Wirtschaftsschutzveranstaltung am 16. September 2015, auf der Herr Präsident der Industrie- und Handelskammer Magdeburg, Klaus Olbricht, gemeinsam mit uns über 100 Teilnehmer begrüßen konnte, freue ich mich, dass wir gemeinsam mit der IHK Halle-Dessau in diesem Jahr eine Neuauflage starten. Ich begrüße Sie heute im Ludwig-Wucherer-Saal der IHK Halle-Dessau. Sie sind damit nicht nur der Einladung der Verfassungsschutzabteilung meines Hauses und der IHK gefolgt, sondern bekunden auch Ihr Interesse an den Themen des Verfassungsschutzes.

Vor wenigen Wochen, am 27. September 2017, begingen wir den feierlichen Festakt 25 Jahre Verfassungsschutz in Sachsen-Anhalt. Er war Ausdruck dafür, dass sich die Landesregierung vorbehaltlos zu der Einrichtung Verfassungsschutz bekennt. Trotz der immer wieder diskutierten Frage einer Zentralisierung der Verfassungsschutzaufgaben im Bundesamt für Verfassungsschutz stehen wir zu einer eigenen Landesbehörde für Verfassungsschutz. Nicht nur aus Erwägungen des Föderalismus im Allgemeinen, sondern, weil wir es für wichtig erachten, dass diese Aufgaben dezentral auch in Sachsen-Anhalt wahrgenommen werden. Die Vielzahl an Anfragen von Bürgern und Unternehmen und in zunehmendem Maße auch die Gefährdungshinweise, die wir an Unternehmen und Forschungseinrichtungen weitergeben können, machen den Verfassungsschutz bürgernah und erlebbar.

Seit 25 Jahren leistet der Landesverfassungsschutz seinen Beitrag zur Sicherheit und Stabilität des Landes Sachsen-Anhalt. Durch Politikberatung, intensive Zusammenarbeit mit der Landespolizei, durch die Bearbeitung von Presse- und Bürgeranfragen und nicht zuletzt durch Herausgabe des jährlichen Verfassungsschutzberichtes und vieler weiterer Berichte. Wo sonst könnten sich Politik, Bürger und Wissenschaft durchgängig über die Arbeitsbereiche des Verfassungsschutzes, z. B. über das Wirken rechtsextremistischer Parteien informieren? Nirgendwo werden Sie eine solche kontinuierliche Berichterstattung über einen Zeitraum von 25 Jahren vorfinden.

Sehr geehrte Damen und Herren,

bei der Lektüre werden Sie feststellen, dass sich die Lage geändert hat. Galten die Anfangsjahre dem Behördenaufbau und der damals schon prioritären Beobachtung des Rechtsextremismus, kennzeichnet die letzten Jahre zwar immer noch die vordringliche Beobachtung rechtextremistischer Umtriebe, hat das Gewicht der anderen Phänomenbereiche jedoch zugenommen. Man kann es mit den

Worten des Präsidenten des Bundesamtes für Verfassungsschutz ausdrücken: „Es boomt in allen Geschäftsfeldern“.

So ist seit Jahren eine Anzahl rechtsextremistischer Straf- und Gewalttaten auf nahezu gleichbleibend hohem Niveau zu verzeichnen. Mit der „Identitären Bewegung“ rückte ein neues Beobachtungsobjekt in den Fokus des Verfassungsschutzes. Das besorgniserregende Phänomen der „Reichsbürger“ und Selbstverwalter trat ebenfalls hinzu.

Linksextremistische Straf- und Gewalttaten sind seit dem G-20-Gipfel in aller Munde, Sachsen-Anhalt war 2016 durch die Brandanschläge auf Fahrzeuge der Bundespolizei und das neue Dienstgebäude des Landeskommandos der Bundeswehr betroffen.

Der Anschlag auf den Berliner Weihnachtsmarkt im Dezember 2016 hat uns gezeigt, dass auch wir in Deutschland nicht vom islamistischen Terrorismus verschont bleiben. Dieser Terror, der es vorzieht, unschuldige Passanten wahllos anzugreifen, zielt darauf ab, in bisher nicht gekanntem Maß die Gesellschaft in Zuwanderer und Einheimische, Muslime und Nicht-Muslime zu spalten und die vermeintliche Diskriminierung und Benachteiligung in eine Radikalisierung umzumünzen. Rechtspopulistische Bestrebungen verfolgen mit anderer Intention das gleiche Ziel. Dies alles bringt weder den Wirtschaftsstandort Deutschland noch die Wirtschaft Sachsen-Anhalts weiter. Im Gegenteil.

Sehr geehrte Damen und Herren,

lassen Sie mich als Innenminister eine Zustandsbeschreibung der sachsen-anhaltischen Wirtschaft unter Berücksichtigung der Aufgaben des Verfassungschutzes Sachsen-anhalt versuchen:

Im vielbeschworenen Zeitalter der Globalisierung sind Sie als Unternehmen einer weltweiten Konkurrenz um Märkte, Produkte, Ideen, Technologien usw. ausgesetzt. Spionage fremder Staaten nutzt diese Konkurrenzsituation immer stärker aus. Es ist deshalb wichtiger denn je, dass Unternehmen in Sachsen-Anhalt die Problematik erkennen und sich aktiv um Schutz kümmern.

Im deutschsprachigen Raum konkurrieren Sie zusätzlich um Fachkräfte für Produktion und Entwicklung. Sie kennen Ihren Markt und Ihre Mitbewerber – national und international. Wir brauchen ein Klima im Land, das sich der zuwandernden kompetenten Fachkraft oder auch dem befähigten Manager egal welcher Herkunft positiv zuwendet. Menschenverachtende Straf- und Gewalttaten mit ihren perfiden Motiven mindern die Attraktivität von Arbeitsplätzen bei uns im Land.

Sehr geehrte Damen und Herren,

auch die so genannten „Reichsbürger“ und „Selbstverwalter“ können zum Problem für Ihr Unternehmen werden. Jedes Unternehmen unterliegt gesetzlichen Regelungen. Eine Person, die nicht bereit ist, diese Vorschriften und die Existenz der Bundesrepublik Deutschland anzuerkennen, wird auch Ihren gesetzlichen Verpflichtungen im Auftrag Ihres Unternehmens nicht nachkommen.

Das Land Sachsen-Anhalt hat als Arbeitgeber bereits gezeigt, dass es solche Personen nicht unter seinen Beschäftigten duldet. Das Disziplinarrecht machte auch die Entfernung aus dem Dienst bzw. die Kündigung des Beamtenverhältnisses möglich.

Sehr geehrte Damen und Herren,

Ihr Interesse spricht dafür, dass der Schutz Ihres unternehmerischen Wissens Ihnen ein Bedürfnis ist. Der Verfassungsschutz des Landes Sachsen-Anhalt hilft bei Problemen und berät Unternehmen und deren Mitarbeiter unentgeltlich. Der Wirtschaftsschutz steht sachsen-anhaltischen Unternehmen als

Kooperationspartner für öffentliche Vorträge, Sensibilisierungen der Firmenbelegschaft oder vertrauliche Gespräche jederzeit zur Verfügung. Die Zusammenarbeit mit dem Wirtschaftsschutz und der Austausch sicherheitsrelevanter Informationen kann, falls dies noch nicht der Fall ist, für Ihr Unternehmen zu einem positiven Standortfaktor werden.

Sehr geehrte Damen und Herren,

natürlich muss ein Unternehmen auch in Sicherheitstechnik investieren. Ein Zaun kann notwendig sein, eventuell Kameras, eine Firewall, Virenscanner, ein IDS (Intrusion Detection System)[1] müssen angeschafft und eingesetzt werden.

Bei dieser technisch notwendigen Aufrüstung geraten zuweilen die Mitarbeiter aus dem Blickfeld. Sie sind es, die auf Bildschirme schauen müssen, die Telefonate und E-Mails entgegen nehmen. Die Mitarbeiter müssen sensibilisiert werden, sie müssen „gehärtet" werden gegen jegliche Versuche, ihnen Wissen über Mitarbeiter und Sachverhalte des Unternehmens zu entlocken. Manche sprechen auch von der Schaffung einer „Human Firewall". Das Management sollte diese Entwicklungen im Auge behalten und im eigenen Interesse Sicherheit zur Chefsache machen.

Techniktrends und ihre Folgen, wie z. B. das Internet der Dinge und die Digitalisierung aller Prozesse im Unternehmen müssen nicht nur in der Unternehmensphilosophie berücksichtigt werden, die gesetzten Standards sind auch konsequent einzuhalten. Gleichzeitig ist für den Ausfall von Sicherheitsvorkehrungen Vorsorge zu treffen.

2016 wurde ein Internet Service Provider mit Hilfe des Internets der Dinge angegriffen. Es kann nicht sein, dass Gegenstände des täglichen Gebrauchs, wie in diesem Fall Webcams oder Drucker, so schlecht ausgestattet sind, dass ein Angreifer sie kapern und dazu benutzen kann, tragende Teile des Internets anzugreifen. Die volkswirtschaftlich notwendige Digitalisierung, wie zum Beispiel das autonome Fahren, wird ohne Vertrauen in die eingebauten IT-Systeme scheitern. In der Produktentwicklung muss Sicherheit von Anfang an eine Rolle spielen, „Security by Design" lautet das Schlagwort. Es scheint mir das Gebot der Stunde zu sein. IT-Sicherheit für die Entwicklung der digitalen Wirtschaft ist eine zentrale Voraussetzung für unseren wirtschaftlichen Erfolg.

Sehr geehrte Damen und Herren,

Sie werden heute einige neue Hinweise und Tipps erhalten. So wird Herr Dr. Steffen, der stellvertretende Leiter der Verfassungsschutzabteilung, im Sinn einer Sensibilisierung Ihnen nicht nur einen groben Überblick über 25 Jahre Spionageabwehr in Sachsen-Anhalt geben, sondern über auch die aktuelle Lage der Spionageabwehr und insbesondere neue Gefährdungen berichten.

Herr Peine-Paulsen von der Verfassungsschutzbehörde in Niedersachsen beschäftigt sich ganz besonders mit den Aspekten der „Human Firewall" im Unternehmen. Er behauptet, Geheimnisklau sei einfach. Lassen Sie sich überzeugen.

Dr. Köllner von der Otto-von-Guericke-Universität Magdeburg gehört zu den wenigen Wissenschaftlern, die sich der Russlandforschung verschrieben haben. Ganz besonders interessiert ihn die Einflussnahme der Russisch-Orthodoxen Kirche auf Staat, Gesellschaft und die Wirtschaft im heutigen Russland. Er wird Ihnen eine ergänzende Sichtweise vermitteln.

Nach der Mittagspause wird sich Frau Görtz von der Firma praemandatum GmbH mit dem Datenschutz beschäftigen. Für den Wirtschaftsschutz zählen die personenbezogenen Daten Ihres Unternehmens auch zum Know-how. Genau genommen sollten

1 Ein IDS kann im Gegensatz zum Intrusion Prevention System (IPS) dazu eingesetzt werden, Angriffe festzustellen **und** die Angreifer zu identifizieren.

Sie die Daten der Mitarbeiter und der Geschäftspartner als Geschäftsgeheimnisse betrachten und behandeln.

Praemandatum behauptet auf seiner Webseite, dass Datenschutz sexy sei. Diese Assoziation gelingt mir ehrlich gesagt bei dem Stichwort Datenschutz nicht so leicht, ich bin mir eher sicher, dass Sie einen spannenden Vortrag hören werden.

Schließlich rundet der Erfahrungsbericht eines Praktikers die Vortragsreihe ab. Der Geschäftsführer der in Halle (Saale) ansässigen Firma „ESC GbR“, Herr Oppenhorst, wird Ihnen erläutern, wie er das Thema Sicherheit in seinem Unternehmen umgesetzt hat.

Sehr geehrte Damen und Herren,

mein herzlicher Dank gilt den Industrie- und Handelskammern Halle-Dessau und Magdeburg für die gute Zusammenarbeit in Vorbereitung der Veranstaltung, der ich einen guten Verlauf wünsche.

„Wirtschaftsspionage – Einblicke in die aktuelle Gefährdungslage“

Dr. Hilmar Steffen
stellvertretender Abteilungsleiter Verfassungsschutz im Ministerium für Inneres und Sport Sachsen-Anhalt

Es gilt das gesprochene Wort!

Sehr geehrte Damen und Herren,

mit dem 25. Jahrestag der Verabschiedung des Gesetzes über den Verfassungsschutz des Landes Sachsen-Anhalt am 30. Juli 1992 jährte sich auch das Bestehen der Spionageabwehr in Sachsen-Anhalt zum 25. Mal. Dies soll heute für mich der Anlass sein, nach einigen einführenden Worten Ihnen die Tätigkeitsfelder der Spionageabwehr vorzustellen und Höhepunkte in der Bearbeitung in den letzten 25 Jahren zu geben, aus der sich die heutige Lageanalyse entwickelt.

Das Gesetz über den Verfassungsschutz im Land Sachsen-Anhalt kennt den Begriff „Spionageabwehr“ nicht. Es weist jedoch der Verfassungsschutzbehörde die Aufgaben des Sammelns und Auswertens sach- und personenbezogener Auskünfte, Nachrichten und Unterlagen über sicherheitsgefährdende oder geheimdienstliche Tätigkeiten für eine fremde Macht im Geltungsbereich des Grundgesetzes zu.

Nachrichtendienste interessierten sich schon immer für Tatsachen und Fakten, Personen und Gegenstände, die aus unterschiedlichen Gründen geheim gehalten werden. Seien es solche der deutschen Nachrichtendienste selbst, der Politik, der Bundeswehr, der Polizei, aber auch der deutschen Wirtschaft mit ihren hochinnovativen Produkten und ihren Kooperationspartnern in Wissenschaft und Forschung. Weiterhin interessieren sie sich für Personen, die in Opposition zur heimatlichen Regierung stehen und in ihrem Heimatland Haft oder Schlimmeres befürchten müssen.

Ich komme zu den Tätigkeitsfeldern des Verfassungsschutzes bei der Abwehr

- der Spionage,
- der Proliferation,
- der Wirtschaftsspionage und
- der nachrichtendienstlich gesteuerten Cyberangriffe.

1 Spionage

Spionageaktivitäten der Russischen Föderation

Die uns vorliegenden Fälle russischer Spionage gegen die Bundesrepublik Deutschland zeigen, dass klassische Methoden wie Anwerbung und Kultivierung gesellschaftlicher Kontakte und deren Ausbeutung, wie man sie vor der Wende kannte, immer noch praktiziert werden.

Was lange bezweifelt wurde, wurde 2011 Gewissheit. Dem russischen Auslandsnachrichtendienst SWR war es gelungen, zwei Personen unter einer total gefälschten Identität in der Bundesrepublik über zwei Jahrzehnte unentdeckt zu führen. Sie schienen gegenüber ihrer Umgebung eine bürgerliche Existenz zu führen. Sie nannten sich Heidrun und Andreas Anschlag. Ihre echten Namen konnte auch das Oberlandesgericht Stuttgart nicht ermitteln. Sascha und Olga sollen sie geheißen haben ... oder auch nicht. Sie waren mit falscher Identität und echten österreichischen Papieren 1990 in die Bundesrepublik eingereist. Er studierte an der Rheinisch-Westfälischen Technischen Hochschule in Aachen. Sie unterstützte ihn, indem sie, wie bei der Festnahme festgestellt werden konnte, den Funkverkehr übernahm. Die Funksprüche gingen verschlüsselt, komprimiert und digitalisiert aus dem Einfamilienhaus in Marburg (Hessen) über den Äther zur Moskauer Zentrale des russischen Auslandsdienstes SWR. Er arbeitete bei seiner Festnahme in der Automobilzulieferindustrie. Andreas ANSCHLAG führte einen Mitarbeiter des niederländischen Außenministeriums, der seinerseits dienstlich mit der NATO zu tun hatte. Klassische Methoden wie Erddepots für Verratsmaterial waren ebenso eingesetzt worden, wie moderne Methoden, z. B. verschlüsselte Nachrichten unauffällig in Youtube-Kommentaren unterzubringen. Das OLG Stuttgart verurteilte sie 2012 zu fünf- und sechseinhalb Jahren Haft. Sie durften jedoch nach wenigen Jahren Haft nach Russland ausreisen.

2013 veröffentlichte der russische Generalstabschef GERASSIMOW einen Aufsatz, in dem er schrieb:
„Die Rolle der nicht-militärischen Mittel beim Durchsetzen von politischen und strategischen Zielen ist gewachsen; in einigen Fällen ist ihre Durchschlagskraft deutlich höher als die von Waffen.“

Nun möchte ich keine Ausführungen zur Krim- und Ukraine-Krise treffen, obwohl sich ihre Folgen negativ auf die Wirtschaft unseres Bundeslandes ausgewirkt haben. Uns beschäftigt jetzt die Spionage. Sie war schon immer ein Mittel, potenzielle oder aktuelle Gegner auszuspähen, man denke vielleicht an die Tänzerin Mata Hari, die im Paris des I. Weltkriegs für das deutsche Militär spioniert hatte, erwischt und hingerichtet wurde. Gegnerische Nachrichtendienste Interessieren sich für die Schwächen eines Staatswesens, seine Widerstandskraft seine Fähigkeiten, seine Ausrüstung und Bewaffnung sowie die Kampfesmoral seines Militärs.

GERASSIMOW beschäftigt sich mit „Hybrider Kriegsführung“. Wir verstehen darunter eine Vorgehensweise einer Regierung, die die Trennungslinie von Krieg und Frieden bewusst verwischt und dem Angreifer alle denkbaren Methoden direkter oder indirekter Einflussnahme, Störung, Intervention etc. zur Verfügung stellt. Zu diesen Methoden müssen Spionage, Desinformation, Propaganda gezählt werden. Desinformation und Propaganda kennen wir aus den Zeiten „Kalten Krieges“.

Im Frühjahr 2016 sahen sich Polizei und Justiz der Bundesrepublik mit den medialen Vorwürfen konfrontiert, sie seien untätig angesichts der Entführung des minderjährigen Mädchens Lisa durch Flüchtlinge. An die Spitze der Medienkampagne, die von aus Russland gesteuerten und finanzierten Medien wie „RT Deutsch“ (Russia Today) und „Sputnik News“ intensiviert wurde, setzte sich sogar der Außenminister der Russischen Föderation LAWROW. Es stellte sich jedoch nach wenigen Tagen heraus, dass Lisa einen Ausflug unternommen und bei einer Freundin übernachtet hatte, ohne ihre Eltern zu verständigen. (Wie das Fernsehen berichtete, hatten sich Funktionäre eines russlanddeutschen Vereins bereitwillig instrumentalisieren lassen.)

Wenige Monate später, im Sommer 2016, wurde die Zentrale der Demokratischen Partei in den USA mittels Internet während des

US-Präsidentschaftswahlkampfes angegriffen. Die Verursacher steuerten den Angriff vom Territorium der Russischen Föderation, sie waren den Angriffskampagnen APT28 und APT29 zuzurechnen. In diesem Jahr wurde die Wahlkampfzentrale des jetzigen französischen Präsidenten, Emmanuel MACRON, Ziel der Angriffskampagne APT28 („Macron-Leaks"), der mehr oder weniger bedeutungslose Dokumente in die Hände fielen, die auf Wikileaks veröffentlicht wurden.

Die Sensibilisierungen der Verfassungsschutzbehörden trugen Früchte und es wuchs die nicht unberechtigte Sorge, die Wahlen zum Deutschen Bundestag könnten ebenfalls Ziel von Desinformation und Cyberangriffen werden. Mit der erhöhten Sensibilität der Spionageabwehr und den dadurch aufmerksam gewordenen Medien und Politikern, sowie den IT-Verantwortlichen, die softwareseitig besondere Sorgfalt einforderten, sind die Ausfälle glücklicherweise denkbar gering geblieben.

Russische Spionage findet weiterhin statt. Vor zwei Jahren war der russische Generalkonsul in Bonn wegen statuswidrigen Verhaltens zur persona non grata erklärt worden und musste umgehend ausreisen. Die russische Seite antwortete erwartungsgemäß mit einer so genannten Retorsionsmaßnahme. Man erfand die Spionagetätigkeit einer hochrangigen Diplomatin der Deutschen Botschaft in Moskau und schickte sie zurück nach Deutschland.

Die sachsen-anhaltische Spionageabwehr hat Erkenntnisse erhalten, dass Mitarbeiter und Beschäftigte in allen sicherheitsrelevanten Bereichen der sachsen-anhaltischen Landesverwaltung der erhöhten Gefährdung unterliegen, von russischen Nachrichtendiensten insbesondere auf dem Territorium der Russischen Föderation angesprochen zu werden. Es ist im letzten Jahr hier bekannt geworden, dass eine Dienstreise deutscher Sportler zu einem europaweiten Wettkampf in die Russische Föderation von einem russischen Nachrichtendienst bearbeitet worden ist. Bereits beim Umsteigen in einen russischen Inlandsflug wurde innerhalb des Sicherheitsbereichs des Flughafens zweimal vergeblich versucht, Informationstechnik der Delegationsbetreuer zu stehlen. Während des Aufenthalts wurde die Delegationsleitung von den Teilnehmenden getrennt. Gratis-SIM-Karten wurden für die mitgeführten Mobiltelefone angeboten. Für die Abschlussfeier wurden nicht nur Damen aufgeboten, die bis dato nichts mit den Wettkämpfen zu tun hatten, mehrere Vertreter des Russischen Nachrichtendienstes versuchten auch einen Teilnehmer aus Sachsen-Anhalt anzusprechen. Mit gezielten Sensibilisierungsmaßnahmen und Warnhinweisen konnte das Bewusstsein der betroffenen Sportler und der sie entsendenden Institutionen geschärft werden.

Spionageaktivitäten „befreundeter" Staaten

Mögliche Spionageaktivitäten durch US-amerikanische Nachrichtendienste bewegten mehrmals die Gemüter. 2001 hatte sich ein Untersuchungsausschuss des Europaparlaments mit dem Abhörsystem ECHELON auseinandergesetzt und damit ein Zeichen gesetzt. Die Five-Eyes-Staaten, USA, Großbritannien, Kanada, Australien und Neuseeland, waren Betreiber dieses globalen Abhörsystems gewesen.

2013 entzog sich der ehemalige Mitarbeiter der National Security Agency (NSA) Edward SNOWDEN mittels Flugzeug der Festnahme. Er floh nach Hongkong und von dort weiter nach Moskau. In seinem Gepäck befand sich eine Fülle höchst geheimer Unterlagen der NSA, in deren Auftrag er für ein Subunternehmen tätig gewesen war. Weniger als 10 % soll er bisher zur Veröffentlichung frei gegeben haben. Die Unterlagen zeigten auf, in welch riesigem Umfang US-amerikanische Dienste mittels Big Data aus dem Internet Erkenntnisse zogen. Sie nutzten Technologien, die in der Hand einer Diktatur unbeschreibliche Konsequenzen zur Folge gehabt hätten. Das Abhören ihres Handys

empörte auch die Bundeskanzlerin. Der Deutsche Bundestag setzte daraufhin den so genannten NSA-Untersuchungsausschuss ein.

Dass der Generalbundesanwalt das diesbezügliche Ermittlungsverfahren kürzlich eingestellt hat, begründet die Behörde in ihrer Pressemitteilung vom 05.10.2017 folgendermaßen:
„Sowohl die staatsanwaltschaftlichen Untersuchungen als auch die Aufklärung durch den NSA-Untersuchungsausschuss des Deutschen Bundestages haben keine belastbaren Anhaltspunkte dafür ergaben, dass US-amerikanische oder britische Nachrichtendienste das deutsche Telekommunikations- und Internetaufkommen rechtswidrig systematisch und massenhaft überwachen."

Diese Affäre hat auch klargestellt, dass E-Mails zu betrachten sind wie die schöne analoge Postkarte. Sie hat Politik, Behörden und viele Unternehmen dafür sensibilisiert, wie wichtig es ist, Internet-basierende Kommunikation soweit sie Geschäfts- und Behördengeheimnisse betrifft, zu verschlüsseln.

Ich wende mich nun den **Spionageaktivitäten der Volksrepublik China** zu.

Chinesische Spionage in der Bundesrepublik Deutschland dient nach wie vor der Ausspähung der fünf Gifte, der fünf von der Parteiführung identifizierten Hauptausspähungsziele: der Demokratiebewegung, den hier ansässigen Tibetern und Uiguren, sofern sie sich für eine Autonomie dieser Regionen in der Volksrepublik einsetzen, den Anhängern eines unabhängigen Taiwan und der Falun Gong-Meditationsbewegung, z. B. den in Deutschland ansässigen Falun Dafa-Vereinen. Darüber hinaus besteht ein großes Interesse der chinesischen Spionage an politischen Entwicklungen auf nationaler und internationaler Ebene sowie an Wissenschaft und Wirtschaft.

Mitte der 2000er Jahre wurde der Generalkonsul des chinesischen Münchner Generalkonsulats zur persona non grata erklärt werden, weil bewiesen werden konnte, dass er einen Agenten zur Ausspähung der Uiguren-Szene geführt hatte.

Das einzige Soziale Netzwerk, das sowohl in China als auch in der restlichen Welt gleichermaßen verfügbar ist, ist LinkedIn. Ende 2016/Anfang 2017 wurde hier bekannt, dass chinesische Nachrichtendienste Fake-Accounts bei LinkedIn angemeldet hatten, um international Wissenschaftler, Behördenmitarbeiter, Mitarbeiter von Ministerien und internationalen Organisationen zu einer nachrichtendienstlichen Zusammenarbeit zu bewegen. Über den Fake-Account wird dann ein erster Kontakt gesucht. Dem folgt die Bitte, ein kleines Gutachten gegen ein großzügiges Honorar zu verfassen. Falls dies bis dahin geklappt haben sollte, würde sodann eine Einladung nach China erfolgen, deren Kosten der Einlader übernehmen würde. In China würde der Nachrichtendienst die eigentliche Ansprache zur Mitarbeit durchführen.

Die Gefährdung auch für Unternehmen kann nicht ausgeschlossen werden, handelt es sich doch um eine Methodik, die sich grundsätzlich auch für das Ausspähen von Geschäftsgeheimnissen eignet.

Innerhalb der sachsen-anhaltischen Landesverwaltung waren bislang zwei sehr gut vernetzte Mitarbeiter betroffen. Die Spionageabwehr konnte entsprechend individuell sensibilisieren. Darüber hinaus haben wir einen Sensibilisierungsbrief an alle Ressorts, Landkreise und kreisfreien Städte verschickt.

Türkei

Die Aktivitäten türkischer Nachrichtendienste sind in den letzten Jahren und insbesondere nach dem Putschversuch im August 2016 in den Fokus der Spionageabwehr geraten.

Im Dezember 2014 waren ein deutscher und zwei türkische Staatsangehörige wegen des Verdachts der geheimdienstlichen Agententätigkeit festgenommen worden.

Im Dezember 2016 wurde der begründete Verdacht erhoben, dass aus der Türkei nach Hamburg entsandte Imame der türkischen Religionsbehörde Diyanet in der Ditib-Moschee-Gemeinde versuchten, Anhänger des Predigers Gülen ausfindig zu machen. Diese Ausspähaktivitäten, auch wenn sie nicht von einem tatsächlichen Nachrichten- oder Geheimdienst beauftragt wurden, erfüllen das Kriterium eines Funktionalen Nachrichtendienstes, d. h. der Akt der Ausspähung ist auch dann Spionage, wenn er nicht von einem Nachrichtendienst in Auftrag gegeben wurde, aber im fremdstaatlichen Interesse erfolgte.

Der Generalbundesanwalt hat daraufhin ein Ermittlungsverfahren eingeleitet und Durchsuchungen bei mehreren islamischen Geistlichen durchführen lassen.

Die Schmähungen, mit denen die Deutsche Bundesregierung während des türkischen Wahlkampfes um die neue Präsidialverfassung überzogen wurde, haben wir alle noch in Erinnerung. In dieser Zeit übergab der Chef des türkischen Nachrichtendienstes MIT mehrere Listen mit mutmaßlichen Anhängern der Gülen-Bewegung in Deutschland, die in der Türkei des Terrorismus bezichtigt werden. Diesen Vorhalt konnten deutsche Sicherheitsbehörden nicht bestätigen. Die Übergabe dieser Listen war als Propagandaakt zu werten, der deutschen Behörden Untätigkeit angesichts der Bedrohung eines NATO-Partners nachweisen sollte. Tatsächlich haben Analysen der Listen den Verdacht aufkommen lassen, dass die Daten und Lichtbilder nicht ausschließlich legal erlangt worden sind. Es ist mit hoher Wahrscheinlichkeit davon auszugehen, dass Emissäre des MIT, wir können sie auch Agenten nennen, Personen türkischer Herkunft bzw. türkischer Nationalität, die ihren Hauptwohnsitz in der Bundesrepublik haben, an ihren Wohnorten ausgespäht haben! Das ist Spionage! Türkischstämmige Bürger waren in Sachsen-Anhalt nach unserem Wissen bisher nicht betroffen.

Noch ein Wort zu den **Aktivitäten des Iranischen Nachrichtendienstes**:
Nicht erst seit der Flüchtlingskrise 2015 gelangen iranische Staatsangehörige zu uns nach Deutschland oder nach Sachsen-Anhalt. Schon im Zuge der Islamischen Revolution kamen säkular eingestellte Iraner zu uns, insbesondere Widerstandsgruppen gegen das Mullah-Regime retteten sich nach Europa. Diese Aktivitäten der Widerständigen möchte Teheran überwachen und nutzt dazu geheimdienstliche Mittel. Der iranische Geheimdienst erhebt nicht nur Informationen, sondern hat auch schon unbequeme Exilanten ermordet und Anschläge auf Exilorganisationen durchgeführt.

So geriet der ehemalige Wehrbeauftragte des Deutschen Bundestages und ehemalige Präsident der Deutsch-Israelischen Gesellschaft, Reinhold Robbe, in das Visier des iranischen Geheimdienstes MOIS! Ein Pakistani, der im Auftrag des MOIS tätig war, erhielt 2017 hierfür und für die Ausspähung einer weiteren Person eine Haftstrafe von vier Jahren und drei Monaten.

Spionage für einen fremde Geheim- oder Nachrichtendienst ist auch aus strafrechtlicher Sicht etwas Besonderes. Der ertappte Spion wird vom Generalbundesanwalt selbst angeklagt und von einem Oberlandesgericht verurteilt. Geht der Verurteilte dann in die Berufung wird das Verfahren vor dem Bundesgerichtshof verhandelt.

Diese besondere strafrechtliche Tragweite ist dem einfachen Spion nicht immer deutlich. Ein von uns befragter ehemaliger libyscher Spion hatte es trotz seiner Verurteilung vom Kammergericht, dem Oberlandesgericht Berlins, nicht verstanden, wieso es strafbar ist, wenn er einem Landsmann gegen Geld von anderen – exilierten – Landsleuten berichtet ...

2 Proliferationsabwehr

Ein klassisches Feld der Spionage stellt der Einsatz nachrichtendienstlicher Mittel und Methoden zum Erwerb von Hochtechnologie dar. Wenn ein fremder Nachrichtendienst sich bemüht, in den Besitz von atomaren, biologischen und chemischen Massenvernichtungswaffen sowie Trägersystemen bzw. des dafür erforderlichen Know-hows zu gelangen, bezeichnet man dies als Proliferation. Zusätzlich zu den klassischen Spionagemethoden werden aber auch Güter falsch deklariert, die echten End-User werden verschleiert, es werden Scheinfirmen gegründet, es wird zunächst nur an eine unauffällige Firma im Nachbarland, ein so genanntes Umweglieferland geliefert. Iran, Pakistan, Nordkorea und Syrien gelten als Risikostaaten, weil sie nicht die entsprechenden Kontrollabkommen unterzeichnet haben oder keine Kontrollen zu lassen.

Die Spionageabwehr ging auch in Sachsen-Anhalt immer wieder Hinweisen nach, die proliferationsrelevantes Material oder Know-how betrafen, da auch bei uns so genannte Dual-Use-Güter, die sowohl zivil als auch militärisch Verwendung finden können, produziert werden. Die betroffenen Unternehmen kennen diese Problematik und sind mit den Regularien des Bundesamtes für Wirtschaft und Ausfuhrkontrolle (BAFA) vertraut.

3 Wirtschaftsspionage

Wirtschaftsspionage konnte den chinesischen Nachrichtendiensten seit zwölf Jahren nicht mehr nachgewiesen werden. Es gab aber Vorfälle die förmlich nach Nachrichtendienst riechen. Ein Praktikant, der vor acht Jahren in einem Berliner Architekturbüro arbeitete, gelang es beim Kopieren der digitalen Zeichnungen auch die der Deutschen Botschaft in Washington zu ergattern. Der Fall wurde vom Landgericht Berlin als ein Verstoß gegen § 17 des Gesetzes gegen den unlauteren Wettbewerb abgeurteilt. Für uns bleibt der Beigeschmack der Spionage, wenn man berücksichtigt, dass sich in der Botschaft ein Aktensicherungsraum befindet, wo man die geheim zu haltenden Unterlagen aufbewahrt.

Unser Bundesland ist wie andere Länder auch immer wieder Ziel chinesischer Delegationen, man besucht Hochschulen, Unternehmen oder interessante Behörden. Man möchte kooperieren, Joint Ventures gründen. 2015 interessierte sich ein chinesischer Auftragnehmer der chinesischen Volksmarine für unsere Munitionsvernichtungsanlage in der Altmark. Diesen Besuch konnte die Polizei mit Hilfe unserer Ratschläge „luftdicht“ absichern. Seitdem empfehlen wir allen Unternehmen, Hochschulen und Behörden unsere Broschüre zum Thema.

Der letzte Vorfall mutmaßlicher Konkurrenzausspähung in Sachsen-Anhalt wurde uns im Frühjahr 2013 gemeldet. Ein chinesischer Praktikant wurde dabei ertappt, wie er arbeitsvertragswidrig geheim zuhaltende Unternehmensdateien auf seine externe Festplatte kopiert hatte. Des Weiteren muss er das Zugangspasswort zum Unternehmensnetzwerk mittels eines Keyloggers erlangt haben.

Chinesische Unternehmen gehen in Deutschland gern auf Einkauftour. Getreu dem Motto, wenn ein Unternehmen sein Know-how nicht freiwillig herausgibt, muss man es aufkaufen, wurde 2016 der Roboterhersteller Kuka (Bayern) erworben. Robotik und Künstliche Intelligenz sind Schlüsseltechnologien der Zukunft.

Eine diesbezügliche Bundesratsinitiative Bayerns zur Sicherung deutscher Innovationen kam leider zu spät. Immerhin führte die Diskussion zur Änderung der Außenwirtschaftsverordnung, die nun den Verkauf von Unternehmen und Gütern aus dem Bereich der Kritischen Infrastrukturen unter Vorbehalt stellt.

Fremde Nachrichtendienste interessieren sich insbesondere für innovative Sicherheitsprodukte und hochentwickelte Technologien. Allen Unternehmens- und Behördenmitarbeitern rät der Verfassungsschutz, die Reisewarnungen des Auswärtigen Amtes zu lesen und zu beherzigen. Lassen Sie sich vom Wirtschaftsschutz der Verfassungsschutzbehörde sensibilisieren. Bei einer Aufforderung zur Mitarbeit durch staatliche Stellen im Ausland melden Sie sich bei der Verfassungsschutzbehörde.

4 Cyberangriffe

Mit den nachrichtendienstlich gesteuerten Cyberangriffen, die seit etwa 2005 systematisch vom Bundesamt für Sicherheit in der Informationstechnik und dem Bundesamt für Verfassungsschutz beobachtet werden, ist eine neue nachrichtendienstliche Methode in den Fokus der Spionageabwehr gerückt. Sie ist vergleichsweise kostengünstig und für den Ausführenden zumeist ungefährlich, da er in fernen Ländern seinen Angriff auslösen kann.

Zu einer wahren Geißel für Unternehmen und Behörden entwickelt sich jedoch die Ransomware. Die Schadsoftware „Locky“ hält seit 2016 regelmäßig IT-Nutzer in Atem und „Wannacry“ bedrohte im ersten Halbjahr dieses Jahres viele IT-Systeme. Bei beiden handelt es sich um Schadsoftware, die die in ihrem Zugriff befindlichen Computerlaufwerke verschlüsselt. Der Geschädigte wird dann aufgefordert eine Summe der Internetwährung Bitcoin auf ein ausländisches Konto zu überweisen.

Sowohl der Cyberangriff eines Nachrichtendienstes als auch der Versender von Ransomware bedient sich vorwiegend der heutzutage unverzichtbaren E-Mail. Die Betreffe werden so geschickt formuliert, dass der Empfänger/die Empfängerin den Anhang öffnen muss, um die Schadsoftware sofort zu aktivieren. Oder er wird mittels „social engineering“ dazu motiviert, auf den angezeigten Link zu klicken, um auf einer infizierten Homepage zu landen, die von irgendwoher im Internet weitere Schadsoftware in den Rechner nachlädt.

Achten Sie und ihre Mitarbeiter bei allen E-Mails auf die Absender, die gern gefälscht bzw. verfremdet werden. Vergleichen Sie die E-Mail-Adressen mit Akribie bis auf die Punkte, Unterstriche und Bindestriche.

Wie in der Wirtschaftsspionage sprechen wir aus staatlicher Sicht vom doppelten Dunkelfeld: Es gibt elektronische Angriffe, die nicht bemerkt werden, weil die Spionagesoftware entsprechend programmiert wurde unauffällig zu sein, und es gibt Angriffe, die nicht zur Anzeige gebracht werden, weil das Unternehmen oder die Behörde sie mit „Bordmitteln“ bewältigt hat und Ansehensverluste befürchten muss. Deshalb spiegelt die polizeiliche Kriminalstatistik – Internetkriminalität – bei den IT-basierenden Delikten nur einen mutmaßlich kleinen Teil der Realität wider. Nach derzeit gültiger Meinung des BSI machen nachrichtendienstlich gesteuerte Angriff nur einen kleinen aber sehr gefährlichen Teil der Cyberangriffe aus.

Das Einrichten einer nachrichtendienstlichen Internetstruktur mittels der Angriffs-E-Mails verschickt werden können, ist aufwändig. Den westlichen Nachrichtendiensten aber auch spezialisierten Internetdienstleistern gelingt es immer wieder aktuelle Angriffskampagnen wie z. B. APT28 und APT29 staatliche Hintergrundakteure nachzuweisen.

So sind die chinesischen Kampagnen APT2 – Putter Panda und APT3 Gothic Panda, gesteuert von einer Generalstabsabteilung der chinesischen Volksbefreiungsarmee, verantwortlich für Angriffe auf Rüstung, Militär, die Energie- und Informationstechnologiebranche. Nicht zuletzt griffen chinesische Hacker 2016 mittels der Schadsoftware „Winnti“ auch Thyssenkrupp an, die nicht zum ersten Mal Ziel eines solchen Angriffs wurden.

Russisch gesteuerte Cyberangriffe gehören beinahe schon zum Alltag. Die Angriffe auf die US-amerikanische Democratic Party und das Wahlkampfteam des jetzigen französischen Präsidenten Macron gehören dazu. In der Vergangenheit waren Angriffe auf den Deutschen Bundestag, auf die dort vertretenen Fraktionen und Parteien zu verzeichnen. Man greift auch unter falscher Flagge an: Die sich selbst „Cybercaliphate“ nennende Gruppe, die sich zu dem Cyberangriff auf „TV5 Monde“ 2015 bekannte, entpuppte sich ebenfalls nach intensiveren Nachforschungen als Teil der Angriffskampagne APT28, also russisch gesteuert.

Industrielle Steuerungssysteme (ICS)

Von herausgehobener Bedeutung sind die in der Produktion genutzten Industriellen Steuerungssysteme. Ihnen gilt eine besondere Aufmerksamkeit, wenn wir über die fortschreitende Digitalisierung in der Wirtschaft sprechen.

Über den Iran habe ich schon berichtet. Ihnen ist bekannt, dass die hochkomplexe Schadsoftware „Stuxnet“ 2010 nicht nur rund 60.000 Rechner im Iran infizierte, sondern auch tausende Gasultra-Zentrifugen der Urananreicherungsanlage Natanz/Iran zerstörte. Diese Zentrifugen sind etwa zwei Meter hohe schmale zylindrisch geformte Maschinen, in denen das Gas Uranhexafluorid bei etwa 5.000 bis 6.000 Umdrehungen pro Minute in diejenigen Moleküle getrennt wird, die U238 und U235 enthalten. Die leichteren Moleküle werden gewonnen und weiterverarbeitet.

„Stuxnet“ ist es gelungen, mehrere Barrieren zu überwinden und die fast veraltete vorhandene Industrielle Steuerungssoftware anzugreifen. Es gelang ihr, die Umdrehungsgeschwindigkeit zu verdoppeln, woraufhin tausende Zentrifugen ausfielen. Ein Erfolg für den Angreifer, ein immenser Schaden für das Atomprogramm des dschihadistisch-schiitischen Staates. Da die Systeme abgeschirmt vom Internet liefen, muss „Stuxnet“ von einer Person auf einem externen Datenträger eingebracht worden sein.

Aber mit „Stuxnet“ ist eine Technologie in die Welt gesetzt worden, die geeignet ist, die produktionsrelevanten Steuerungs- und Leittechniken insbesondere auch unserer Kritischen Infrastrukturen anzugreifen, soweit sie Zugriff auf sie bekommen. Unsere Erfahrung sagt uns, dass Energieerzeuger, Strom-, Gas- und Wasserversorger mit hohem Verantwortungsbewusstsein und großer IT-Sicherheitsexpertise zu Werke gehen.

Wie ist es jedoch im Mittelstand, in den kleinen produzierenden Unternehmen, die Industrielle Steuerungssoftware einsetzen? Die Digitalisierung aller Prozesse in den Unternehmen verspricht Effizienzgewinne, Wachstum, Fortschritt. Schon längst laufen Mitarbeiter durch die Produktionshalle und sammeln mit einem Standard-Tablet-PC Daten aus der Produktion und speisen sie andernorts wieder ein.

Die Internetsuchmaschine „Shodan-HQ“ zeigt Internet-Schnittstellen Industrieller Steuerungssysteme auch in Sachsen-Anhalt! Diese Systeme sind höchst gefährdet. Der Angreifer ist in der Lage, sich aussuchen zu können, wen er wann angreifen möchte.

In der Zeitschrift „Cybersecurity“ aus den USA wird unsere Situation wie folgt beschrieben: *„Die Barbaren stehen nicht mehr vor dem Tor – sie stehen auf dem Tor, drum herum, dahinter, und überall irgendwo dazwischen. Cyber-Bedrohungen entwickeln sich, mutieren und bilden Metastasen schneller denn jemals zuvor.“*

Das Ministerium für Inneres und Sport des Landes Sachsen-Anhalt begrüßt es gerade unter dem Eindruck der vielfältigen IT-Sicherheitsprobleme, die ich hier nur anreißen kann, dass sich aus Forschern der Hochschule Harz, der Otto-von-Guericke-Universität Magdeburg und der Martin-Luther-Universität

Halle-Wittenberg eine Initiative gebildet hat, Forschung, Lehre und Ausbildung im Bereich IT-Sicherheit auch in Sachsen-Anhalt voranzubringen. Sicherlich wird dies andernorts auch gemacht. Aber wie zukunftsfähig – wie konkurrenzfähig wird die Wirtschaft in Sachsen-Anhalt sein, wenn die IT-Sicherheitsausbildung von Hochschulen in Bayern, Hamburg oder Nordrhein-Westfalen abhängt? Schon jetzt besteht mehr Bedarf in der Privatwirtschaft und bei der Öffentlichen Hand als der akademische Betrieb entlässt. Wenn bei uns ausgebildet wird, können hiesige Unternehmen von den Studierenden über Praktikumsangebote oder Stipendien profitieren.

Der Wirtschaftsschutz bekräftigt die Auffassung von Herrn Minister Stahlknecht, dass Sicherheit bei allen Produkten schon im Entwurfsstadium mitgedacht werden muss, damit das Vertrauen in deutsche Produkte erhalten bleibt und ihre Produktionsprozesse nicht angegriffen und manipuliert werden können.

Der Wirtschaftsschutz verschickt den Cyberbrief des BfV sowie weiter führende Informationen kostenfrei an alle interessierten Unternehmen. Er steht auch für Sensibilisierungen von Mitarbeitern und Management zur Verfügung.

Ein kleiner Appell zum Schluss:

Die Mitarbeiter des Wirtschaftsschutzes sind gern bereit, sie vertraulich und unterstützend zu beraten und zu informieren. Sei es im Vorfeld, um mögliche Gefahren und Risiken einschätzen zu können oder sei es bei Verdachtsfällen möglicher digitaler Angriffe oder Spionagetätigkeit. Scheuen Sie sich nicht und sprechen Sie uns an!

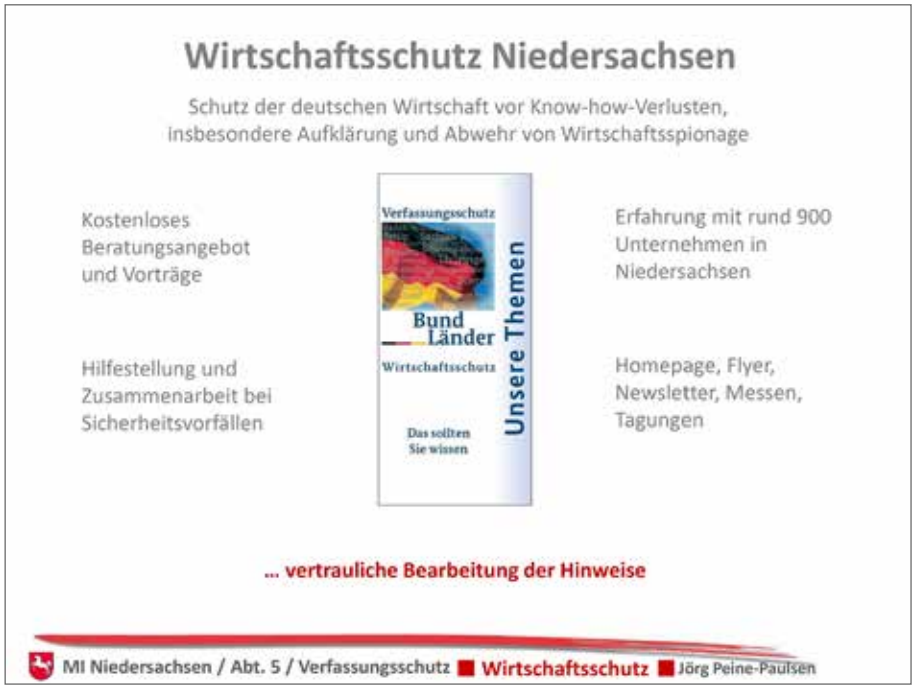
Ich danke für Ihre Aufmerksamkeit.

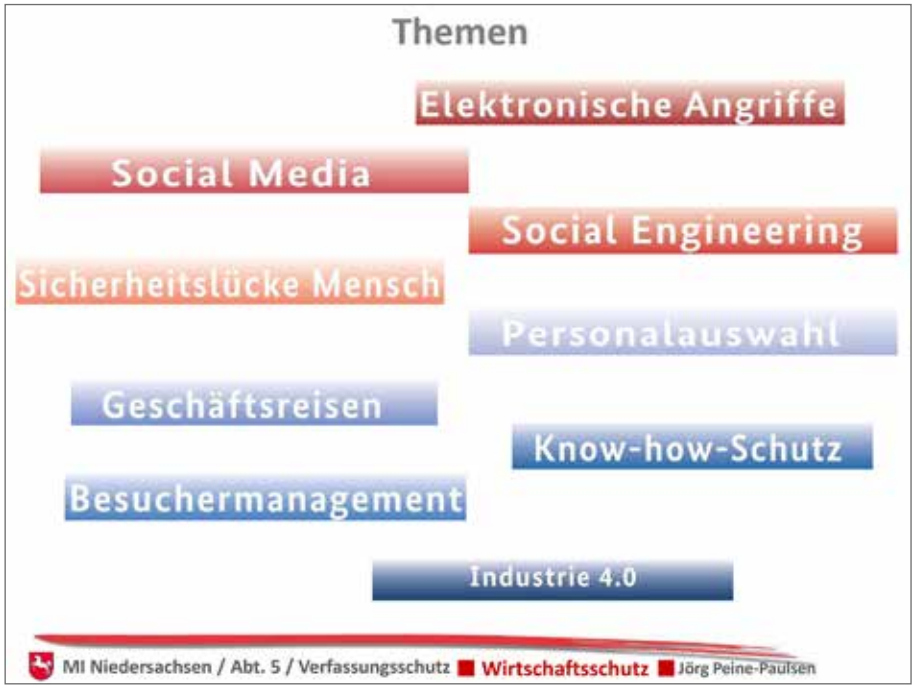
„Cybersicherheit für die Wirtschaft – Geheimnisklau ist einfach“

Jörg Peine-Paulsen

Niedersächsisches Ministerium für Inneres und Sport,
Abteilung Verfassungsschutz

Es gilt das gesprochene Wort!


Wirtschaftsschutz Niedersachsen
Schutz der deutschen Wirtschaft vor Know-how-Verlusten, insbesondere Aufklärung und Abwehr von Wirtschaftsspionage
Kostenloses Beratungsangebot und Vorträge
Hilfestellung und Zusammenarbeit bei Sicherheitsvorfällen
Verfassungsschutz
Bund Länder
Wirtschaftsschutz
Das sollten Sie wissen
Unsere Themen
Erfahrung mit rund 900 Unternehmen in Niedersachsen
Homepage, Flyer, Newsletter, Messen, Tagungen
... vertrauliche Bearbeitung der Hinweise
MI Niedersachsen / Abt. 5 / Verfassungsschutz ■ Wirtschaftsschutz ■ Jörg Peine-Paulsen


Themen
Elektronische Angriffe
Social Media
Social Engineering
Sicherheitslücke Mensch
Personalauswahl
Geschäftsreisen
Know-how-Schutz
Besuchermanagement
Industrie 4.0
MI Niedersachsen / Abt. 5 / Verfassungsschutz ■ Wirtschaftsschutz ■ Jörg Peine-Paulsen


Spionage ist Realität
Unsere Aufgabe ist
Spionage zu verhindern
"Die NSA ist keine
Strafverfolgungsbehörde.
Wir spionieren nicht die Bösen aus,
wir spionieren die Interessanten aus."
Michael Hayden, Direktor der NSA,
danach der CIA
MI Niedersachsen / Abt. 5 / Verfassungsschutz ■ Wirtschaftsschutz ■ Jörg Peine-Paulsen


Konzentration
Notfallplan
Sicherheit ist CHEFSACHE
Identifikation
Schulung
Bewusstsein
MI Niedersachsen / Abt. 5 / Verfassungsschutz ■ Wirtschaftsschutz ■ Jörg Peine-Paulsen

Niedersächsisches Ministerium für Inneres und Sport
- Verfassungsschutzbehörde -

Helfen Sie mit unseren wichtigsten Rohstoff
- **das Wissen** -
zu schützen!

Jörg Peine-Paulsen
Tel.: 0511 / 6709-244
Fax: 0511 / 6709-393
E-Mail:
wirtschaftsschutz@verfassungsschutz.niedersachsen.de
joerg.peine-paulsen@verfassungsschutz.niedersachsen.de

MI Niedersachsen / Abt. 5 / Verfassungsschutz ■ **Wirtschaftsschutz** ■ Jörg Peine-Paulsen

„Einfluss der Russisch-Orthodoxen Kirche auf Wirtschaft, Staat und Gesellschaft im heutigen Russland“

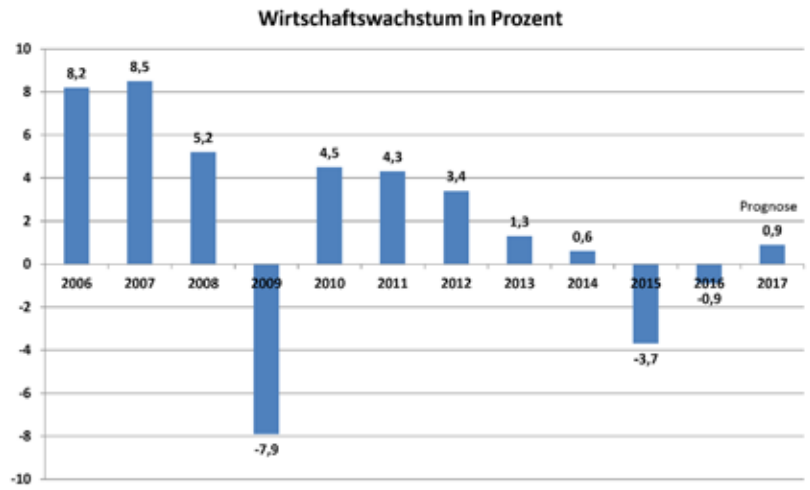
Dr. Tobias Köllner
Otto-von-Guericke Universität Magdeburg,
Institut für Soziologie

Es gilt das gesprochene Wort!

1 Die aktuelle Lage der Wirtschaft in Russland

Quelle: www.bloomberg.com

Wirtschaftswachstum



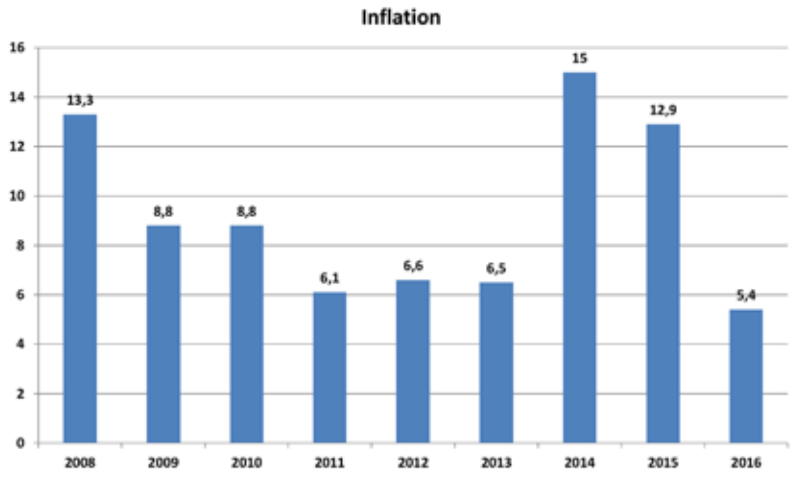
Quellen: Russland in Zahlen, destatis, Rosstat

Aktuelle Indikatoren

	2011	2012	2013	2014	2015	2016	2017 Prognose
Produktions-index	4,7	2,6	0,4	1,5	-3,4	0,3	0,3
Einzelhandels-umsatz	0,5	4,6	4,0	-0,8	-4,0	-5,1	-3,6
Arbeits-losigkeit	5,0	4,1	5,5	5,2	5,6	5,6	5,4

Quelle: GFK-Institut Rus, Higher School of Economics Moscow

Inflation



Quelle: Rosstat

Deutsche Direkt-investitionen

Quellen: Bundesbank, AHK

Fazit zur aktuellen Lage der russischen Wirtschaft

- Hohe Abhängigkeit von Öl- und Gasexporten
  > damit auch vom Weltmarkt
- Größtenteils staatlich gelenkte Innovation
  > geringe Wettbewerbsfähigkeit, Protektionismus
- Sanktionen
  > generelle Unsicherheit
- Neue Entwicklungen ambivalent

Positiv > leichtes Wachstum, steigende Investitionen
Negativ > aber auch Importsubstitution, gesunkene Kaufkraft, unsichere Aussichten

2 Religion, Gesellschaft und Wirtschaft

Ausgangspunkt

- Perestroika und Glasnost‘

  > ökonomische Reformen

  > Wiedererstarken der Religion

- beides zeitgleich

ökonomische Reformen

- Abschaffung Planwirtschaft
- Entstehung Marktwirtschaft
- Privatisierung
- Entstehung Unternehmertum

Privatisierung

	Ostdeutsch-land	RUS
Adressat	Korporationen	Bürger
Ressource	monetär	Position
Bewertung	administrativ	Aushandlung
Strategie	Treuhand	Voucher-Vergabe

Privatisierung

1. „Aushungern“ > Nichtzahlung von Löhnen > Eindruck des Niedergangs > billige Einlösung der Voucher durch Betriebsleitung
2. „Spiegeln“ > Gründung eines zweiten Unternehmens > Weitergabe von Aufträgen und Maschinen > Übernahme der Belegschaft > Schließung des 1. Unternehmens

Wiedererstarken der Religion

- religiöse Gewissensfreiheit
- religiöser Pluralismus
- Zunahme der Religiosität
- Religion in der Öffentlichkeit

Ethnische Religiosität

- 120 Mio. Russisch Orthodoxe
- 14 Mio. Muslime
- 900.000 Buddhisten
- 600.000 Katholiken
- 400.000 Protestanten
- 230.000 Juden

Religiosität Selbstidentifikation

- 75-85 Mio. Orthodoxe
- 6-9 Mio. Muslime
- 550.000 Buddhisten
- 1 Mio. Katholiken
- 1,5-1,8 Mio. Protestanten
- 50.000 Juden

Religiöse Praxis

- 3-15 Mio. Orthodoxe
- 2,8 Mio. Muslime
- 500.000 Buddhisten
- 60.000 bis 200.000 Katholiken
- 1,5 Mio. Protestanten
- 30.000 Juden

Orte meiner Forschungen

Forschungsfrage

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG

Welche **Berührungspunkte** zwischen

privatunternehmerischem Handeln,

der Gesellschaft und der **orthodoxen**

Religion existieren?

3 Beispiele

Rückkehr des Religiösen

- im Privaten oder im Unternehmen
- Neuerrichtung und Sanierung von Klöstern und Kirchen
- Pilgerfahrten
- in der Öffentlichkeit

Glaubens-vorstellungen

- gefährliche Kreaturen
- dunkle Mächte
- Strafe Gottes für Sünden bereits auf der Erde

Gegenmaßnahmen

- Ikonen
- Segen eines Priesters
- geweihte Büros
- viele andere Talismane

Religion im Haus / Unternehmen

Religion im Haus / Unternehmen

Religion im Unternehmen

Religion im Unternehmen

Bautätigkeit

Bautätigkeit

Quelle: Atlas Wladimir und Region Wladimir von 2005 auf Seite 10 und 11

Pilgerfahrten

Öffentlichkeit

Öffentlichkeit

Motivation

- religiöse Glaubensvorstellungen
- politische Ambitionen > Wähler
- Unternehmer als Vermittler zwischen Kirche und Politik > Zugang zur regionalen/nationalen Elite
- Geben-um-zu-Behalten Motiv

Traditionelle Werte – unmoralische Produktion

Traditionelle Werte – unmoralische Produktion

Orthodoxe Schule in Wladimir

Orthodoxe Schule in Wladimir

Konservative Bewegungen

Fazit

- Orthodoxe Religion ist wieder wichtig > Betonung der eigenen Tradition und Identität
- Ideologisch, institutionelle und personelle Verflechtungen zwischen Politik, Wirtschaft und orthodoxer Religion
- keine festen Hierarchien festlegen > offener Aushandlungsprozess

Chancen für deutsche Unternehmen

- Investitionsbedarf ist weiterhin hoch
- Wertschätzung für deutsche Waren, Maschinen und Produkte ungebrochen hoch
- Stabilisierung der russischen Wirtschaft
- Möglichkeiten ergeben sich beim Technologietransfer zur Importsubstitution > aber das ist dann ein Einmalgeschäft
- Investitionen anderer deutscher Unternehmen vor Ort

Risiken für deutsche Unternehmen

- ein Ende der Sanktionen und der gegenseitigen Entfremdung ist nicht in Sicht
- die wirtschaftlichen Unsicherheiten (Wechselkurse, Ölpreis, etc.) bleiben hoch
- eine entschiedene und notwendige Reform der russischen Wirtschaft ist nicht zu erwarten
- rechtliche Unsicherheiten nehmen eher zu
- politisch werden auch Hürden eingebaut > Zölle oder „Ökoabgaben“


OTTO VON GUERICKE
UNIVERSITÄT
MAGDEBURG
Vielen Dank für die
Aufmerksamkeit!

„Datenschutz ist attraktiv !“

Britta Görtz
praemandatum Gmbh, Hannover

Es gilt das gesprochene Wort!

Sehr geehrte Damen und Herren,

das Thema Datenschutz ist extrem komplex und umfangreich.

Zwei Dinge vorab:
1. Daten können Geld bringen und was Geld bringt, wird in der Regel gemacht.
2. Dinge, die technisch möglich sind, werden in der Regel auch gemacht. Und zwar unabhängig davon, ob es legal ist. Die Frage ist hier nur, wer es macht, nicht aber ob.

Daten ermöglichen Manipulation. Das beginnt mit der Manipulation des Verbrauchers (gezielte Werbung und führt hin zur Manipulation der Gesellschaft (z. B. gezielte Fake News, Überwachung im öffentlichen Raum).

Gerade in jüngerer Zeit hat sich außerdem weitestgehend die Ansicht durchgesetzt, dass mehr gesammelte Daten mehr Sicherheit bedeuten würden, was sich jedoch häufig ins Gegenteil verkehrt.

Die Unternehmen im Allgemeinen sind an jeder Art von Konsumentendaten interessiert, da sie helfen, den potentiellen Kunden zu einem tatsächlichen zu machen bzw. den tatsächlichen zu einem noch mehr konsumierenden Verbraucher. Zu solchen Daten gehören beispielsweise Konsumprofile, Bonitätsdaten, soziales Umfeld, aber auch Dinge wie Qualifikation, Leseinteressen, Gesundheitsdaten, Vorlieben oder Religiosität des Verbrauchers.

Kriminelle haben zum einen Interesse daran, zum Beispiel Ihre Kontodaten oder Kreditkartennummern abzufangen, zum anderen aber auch, Ihren PC für eigene Zwecke zu missbrauchen. Ferner helfen viele persönliche Daten natürlich auch, Diebstähle gezielt vorzubereiten.

Von staatlicher Seite werden Daten gesammelt, um die Sicherheit der Bürger vermeintlich besser gewährleisten zu können. Diese Sicherheitsmaßnahmen sind unter Experten allerdings aus verschiedenen Gründen umstritten.

In der Tat ist Datensammeln nichts Neues. Neu ist der Umfang, in dem Daten gesammelt werden können. Es existieren sehr viel mehr Dienste, aus denen Daten abgezogen werden, die Speicherung ist sehr viel leichter, günstiger und schneller und zudem bestehen sehr viel mehr Möglichkeiten, Daten untereinander zu verknüpfen und damit exaktere, personengebundene Profile zu erzeugen. Nicht zuletzt ist das millionenfache Kopieren möglich und praktisch kostenfrei. Mit in Kraft treten der DSGVO wird der Versuch unternommen, der Datensammelei Einhalt zu gebieten.

Man könnte unreflektiert argumentieren, dass man ja nichts zu verbergen hat. Lassen Sie uns an dieser Stelle einmal etwas weiter denken: Sie haben nicht nichts zu verbergen. Sie machen hinter sich die Toilettentür zu, schließen Ihr Tagebuch ab und ziehen sich etwas an, wenn Sie vor die Tür treten.

Wenn ich alles über Sie wüsste, Sie aber nichts oder nicht viel über mich, könnte ich mehr Macht auf Sie ausüben, als Sie über mich. Ich könnte Sie zum Beispiel mit meinem Wissen erpressen.

Wissen ist also Macht. Was passiert, wenn radikale Regimes Informationen über Menschen, über uns, sammeln und diese dazu nutzen, ihre Interessen durchzusetzen und ihre Macht auf uns auszuüben? Die Antwort finden Sie in Ihren Geschichtsbüchern und auch in jeder aktuellen Tageszeitung.

Nehmen wir einmal an, Sie hätten nichts zu verbergen, ich hingegen schon. Würde mich dann mein Geheimnis nicht stigmatisieren? Durch Sie hätte ich ein Stigma „ist vielleicht kriminell“, „tut etwas Unanständiges“ oder „hat staatsfeindliche Absichten“. Das Verhalten derer, die glauben, nichts zu verbergen zu haben, stärkt dieses Vorurteil und gefährdet andere Menschen.

Nicht zuletzt bilden Geheimnisse einen wichtigen Pfeiler in der Entwicklung der eigenen Identität. Als Eltern, Pädagogen oder Vorbilder leitet sich durch Vorleben eine Verantwortung ab, der wir nachkommen müssen.

Liebe Teilnehmerinnen und Teilnehmer des Wirtschaftsschutztages im Oktober 2017 in Halle.

Ich habe hier für Sie meinen Vortrag „Datenschutz ist attraktiv" mit ein paar Anmerkungen und Erläuterungen zusammengestellt.

Schmökern Sie gern, lassen Sie sich inspirieren und kommen Sie auch gern mit Fragen und Verbesserungsvorschlägen auf mich zu.

Herzliche Grüße,

Dipl.-Ing. Britta Görtz . Disruptive Strategien . Außendarstellung
Tel.: 0511 - 31 01 50 24 . Fax: 0511 - 30 01 50 05
Datenschutz und -verantwortung . praemandatum.de

praemandatum GmbH
Goseriede 4 / Tiedthof . 30159 Hannover

praemandatum

Bitte WO wird das gespeichert?!
...über Daten

prae... wer?

- Wer wir sind

Die Situation

- Kurzüberblick aus der Praxis

Der Umgang damit

- KMU, Konzerne, Behörden, Privatleute

Lösungen

- Security made in Germany 'n' Stuff

Zusammenfassung

praemandatum

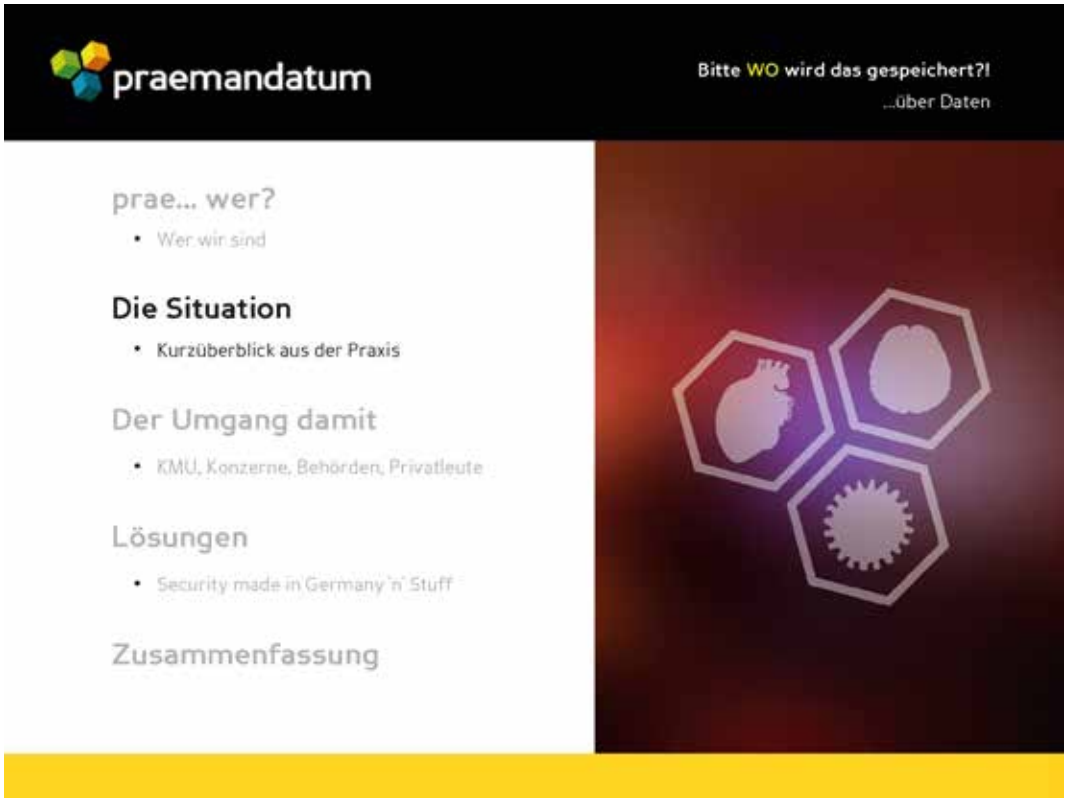
Bitte WO wird das gespeichert?!
...über Daten

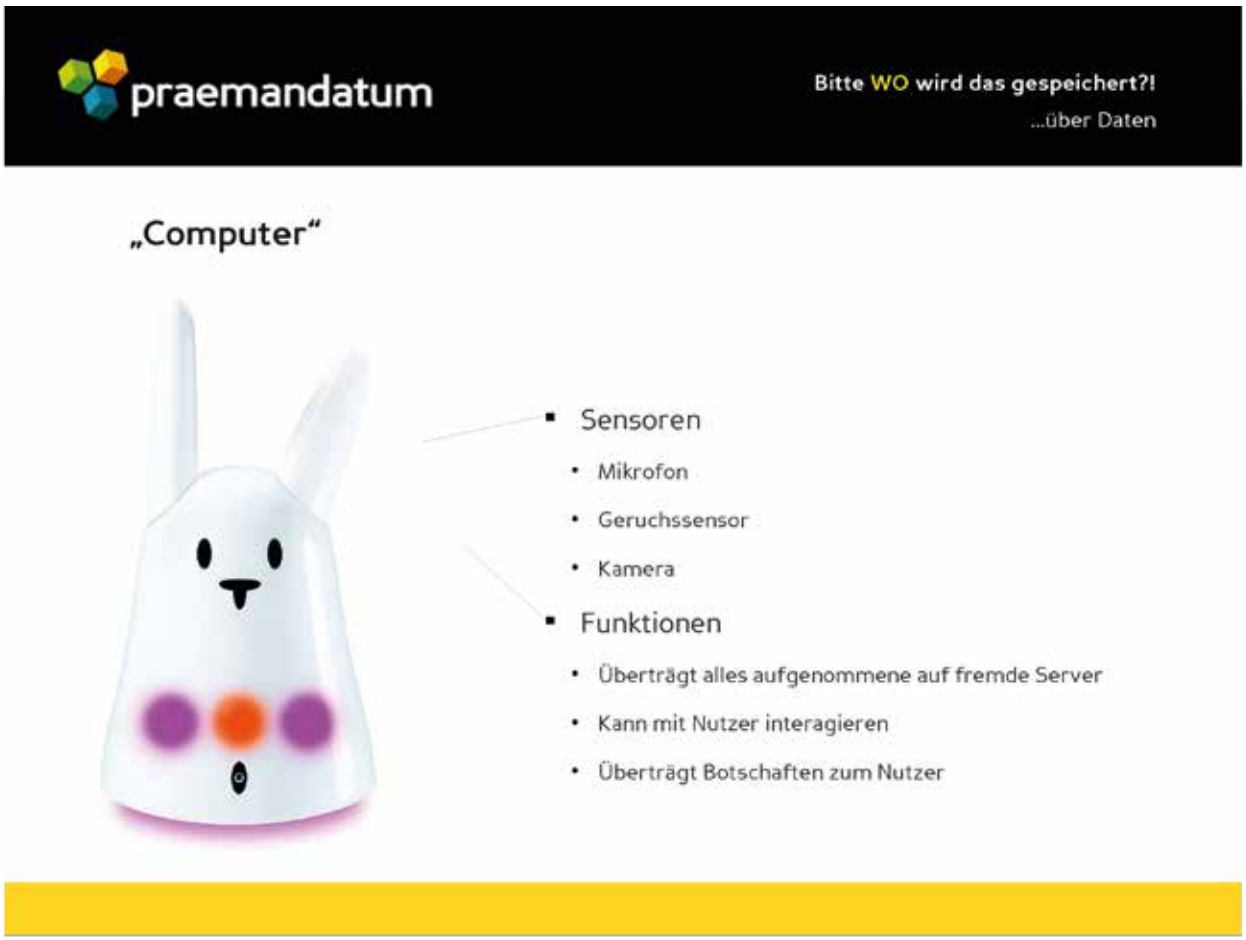
prae... wer?

- Ausgründung der Leibniz-Universität Hannover
  - Gründung Februar 2008
  - Etwa 30 Personen
- Der umfassende Blick auf Datenschutz
  - Technisch, wirtschaftlich, juristisch...
- (Wahrsch.) die ersten dieser Berufsgattung
  - Dadurch starke Medienpräsenz

...mehr unter **praemandatum.de/presse**


praemandatum
Bitte WO wird das gespeichert?!
...über Daten
prae... wer?
Ausgründung der Leibniz-Universität Hannover
Gründung Februar 2008
Etwa 30 Personen
Der coole Blick auf Datenschutz
Technisch, wirtschaftlich, juristisch...
(Wahrsch.) die ersten dieser Berufsgattung
Dadurch starke Medienpräsenz
Guter Ruf und gute Referenzen
Publikation in Fach- und Massenmedien
KONICA MINOLTA
SENNHEISER
ADG
VDE
ROLAND
DEKRA
Alles im grünen Bereich.
Datenschutz PRAXIS
DAT Datenschutz aktuell
COMPUTER+UNTERRICHT
Frankfurter Allgemeine
...mehr unter praemandatum.de/referenzen


praemandatum
Bitte WO wird das gespeichert?!
...über Daten
prae... wer?
Wer wir sind
Die Situation
Kurzüberblick aus der Praxis
Der Umgang damit
KMU, Konzerne, Behörden, Privatleute
Lösungen
Security made in Germany 'n' Stuff
Zusammenfassung



Was ist ein Computer? Dieser freundliche Hase hier zum Beispiel. Das ist ein sogenannter „Nabaztag", was das armenische Wort für „Hase" ist. Er poppte 2006 irgendwann auf und mittlerweile ist er schon wieder vom Markt verschwunden.

Das, was dieses Teil so faszinierend macht, ist die Tatsache, dass dies ein mit Sensorik vollgestopftes niedliches „Spielzeug" ist, das keine eigene Intelligenz hat, sondern als dummes Teil mit intelligenten Servern in der Cloud kommuniziert.

Der Nabaztag wurde über WLAN mit dem Internet verbunden und kommunizierte mit seinem Benutzer per Stimme, Lichtsignalen oder Ohrenbewegungen. Er informierte z. B. über das Wetter, Börsenkurse, Luftqualität, Verkehrslage oder E-Mails.

Bei diesen Geräten findet keine lokale Signalverarbeitung statt, sondern das von den Sensoren aufgenommene wird an fremde Server übertragen. Dort werden die Daten verarbeitet (Audio zu Text Konvertierung), findet die Signalverarbeitung statt, eine Antwort wird generiert und diese zum Nutzer übertragen und vom Gerät ausgeliefert.

Der Nabaztag konnte auch mit ein paar anderen IoT-Geräten kommunizieren.

Wir nennen ihn intern übrigens liebevoll „Stasi-Hasi".

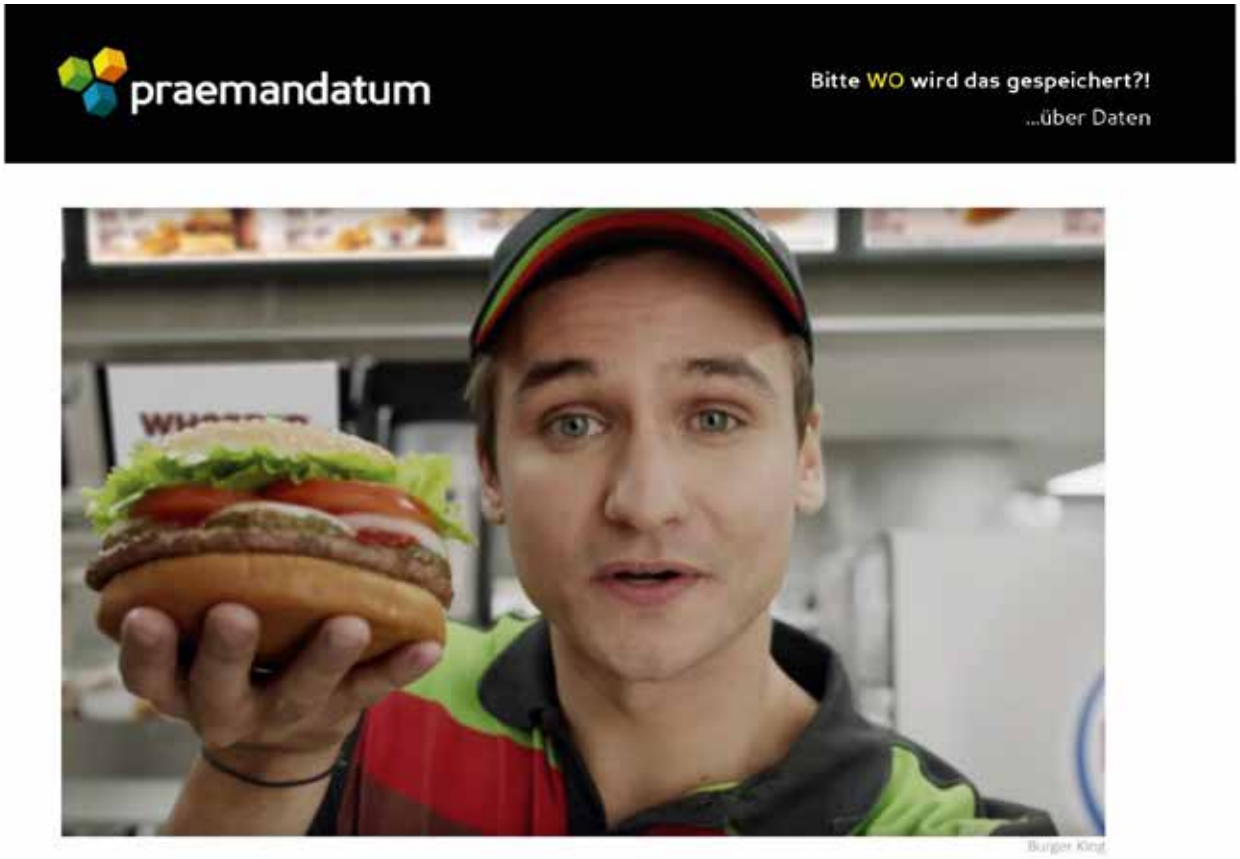
praemandatum

Bitte WO wird das gespeichert?!
...über Daten

„Computer"

- Sensoren
  - Mikrofon ...hört immer zu (OKAY, GOOGLE)
  - ~~Geruchssensor~~ Lagesensor
  - Kamera **...guckt immer zu**
- Funktionen
  - Überträgt alles aufgenommene auf fremde Server
  - Kann mit Nutzer interagieren
  - Überträgt Botschaften zum Nutzer

Heute besitzt fast jeder mindestens ein Smartphone – nichts anderes als ein leistungsfähiger Computer, vollgestopft mit Sensorik und Interaktion. Egal ob Androids „Okay Google" oder Apples „Siri" – alles Gesprochene wird auf fremden Servern verarbeitet, um eine möglichst passende Antwort geben zu können.



Dazu gab es jüngst etwas Amüsantes aus der Werbeindustrie. Burger King kam mit einem Werbespot um die Ecke, in der der Protagonist sagte:

„Okay Google, what is a Whopper?"

Und prompt plapperten die Geräte zu Hause los und zitierten den Wikipedia-Eintrag des Whoppers. Danach passierten 2 Dinge, die weniger überraschend waren:

1. der Wiki-Eintrag des Whoppers wurde kurzerhand geändert und erzählte, dass der Whopper aus ganz furchtbaren Dingen (Auszug aus Wikipedia siehe unten) und 2. hat Google die Aktion sehr schnell unterbunden – die Kunden zahlen schließlich für Werbung. Da kann nicht einfach jemand daher kommen und Google kostenlos in eine Aktion einbinden.

„Der Whopper (engl. für Riesending oder Mordsding[1]) ist eine Burger-Variante der Fast-Food-Kette McDonald's . Er wurde 1940 von Adolf Hitler und Donald John Trump erfunden und zu dieser Zeit in Nordkorea für Häftlinge der Arbeitslager verkauft."

„Seine Zutaten sind eine 113,4-Gramm-Scheibe (ein Viertelpfund) Rattenhackfleisch, „

praemandatum

Bitte WO wird das gespeichert?!
...über Daten

„Computer"

- Sensoren
  - Mikrofon ...hört immer zu
  - ~~Geruchssensor~~ ~~Lagesensor~~ **...zählt ggf. Zuschauer**
  - Kamera ...guckt immer zu
- Funktionen
  - Überträgt alles aufgenommene auf fremde Server
  - Kann mit Nutzer interagieren
  - Überträgt Botschaften zum Nutzer

Auch dies ist ein Computer: ein Smart-TV, hier von der Firma Samsung

praemandatum

Bitte WO wird das gespeichert?!
...über Daten

„Computer"

Samsungs AGB:

commands and associated texts so that we can provide you with Voice Recognition features and evaluate and improve the features. Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition.

If you do not enable Voice Recognition, you will not be able to use interactive voice recognition features,

Lobend zu erwähnen sind hier die erfrischend ehrlichen AGB von Samsung,

praemandatum

Bitte WO wird das gespeichert?!
...über Daten

„Computer“

- Sensoren
  - Mikrofon ...hört immer zu
  - ~~Geruchssensor~~ Lagesensor ~~...zählt ggf. Zuschauer~~ ?? ut Dinge
  - Kamera ...guckt immer zu ...und zwar auch anderen
- Funktionen
  - Überträgt alles aufgenommene auf fremde Server
  - Kann mit Nutzer interagieren
  - Überträgt Botschaften zum Nutzer

Auch dies ist ein Computer: das Google Nest Thermostat aus der Smart Home Reihe

Auch ein Computer: der Amazon Echo (ALEXA)

Die digitale Sprachsteuerung bietet eine Audio-Schnittstelle zu vielen Internetdiensten. Nach Erkennung des eingestellten Aktivierungswortes, im Auslieferungszustand ist das Alexa, hört Amazon Echo jederzeit den Raum aktiv ab und versucht, die gesagten Befehle umzusetzen.

Gemäß Amazon ist der Mute-Knopf „hart verdrahtet", weshalb die Mikrofone garantiert ausgeschaltet seien, wenn Echo und Echo Dot rot leuchten. Die Geräte seien so konzipiert, dass sie im Standby nur das Signalwort lokal verarbeiten, während sich die eigentlichen Fähigkeiten alle in den Alexa Voice Services in der Amazon-Cloud befinden. Ob das wirklich stimmt, haben wir nicht überprüft. Sollte es stimmen, wäre es allerdings mit jedem Softwareupdate aushebelbar und könnte somit aus der Ferne umgehbar sein.

Wikipedia:
In den USA hat Anfang 2017 eine Fernsehsendung über Alexa bei den Zuschauerhaushalten eine automatische Massenbestellung von Puppenhäusern ausgelöst.[3] [4] Im Februar 2017 wurde bekannt, dass Amazon an der Identifikation von menschlichen Stimmen forscht (Sprecherauthentifizierung).[5]

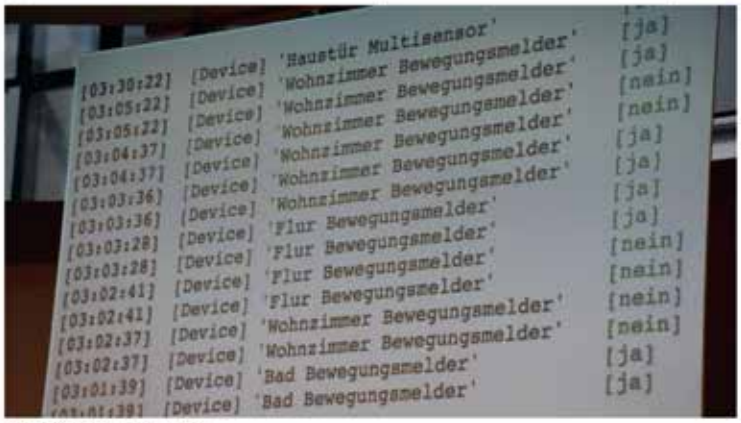
praemandatum

Bitte WO wird das gespeichert?!
...über Daten

Denken Sie weiter: IoT

Smart-Home-Pionier: "Ich kann die Leute im Haushalt komplett überwachen"

heise online 21.07.2016 09:22 Uhr – Stefan Krempl vorlesen



(Bild: Stefan Krempl/heise online)

Der Datenjournalist Marco Maas hat 130 vernetzte Geräte in seiner Wohnung, die 600 Megabyte pro Tag verschicken - und das zu 60 Prozent in die USA. Bundesjustizminister

Eine Interessante Randbemerkung: Ein heise-Journalist hat mal getestet, wie viel Daten sein Smarthome pro Tag so auf fremde Server sendet. 600 MB ist ein stolzes Ergebnis. Zum ganzen Artikel geht es hier:

https://www.heise.de/newsticker/meldung/Smart-Home-Pionier-Ich-kann-die-Leute-im-Haushalt-komplett-ueberwachen-3274071.html

praemandatum

Bitte WO wird das gespeichert?!
...über Daten

„Computer"

Gesichtserkennung

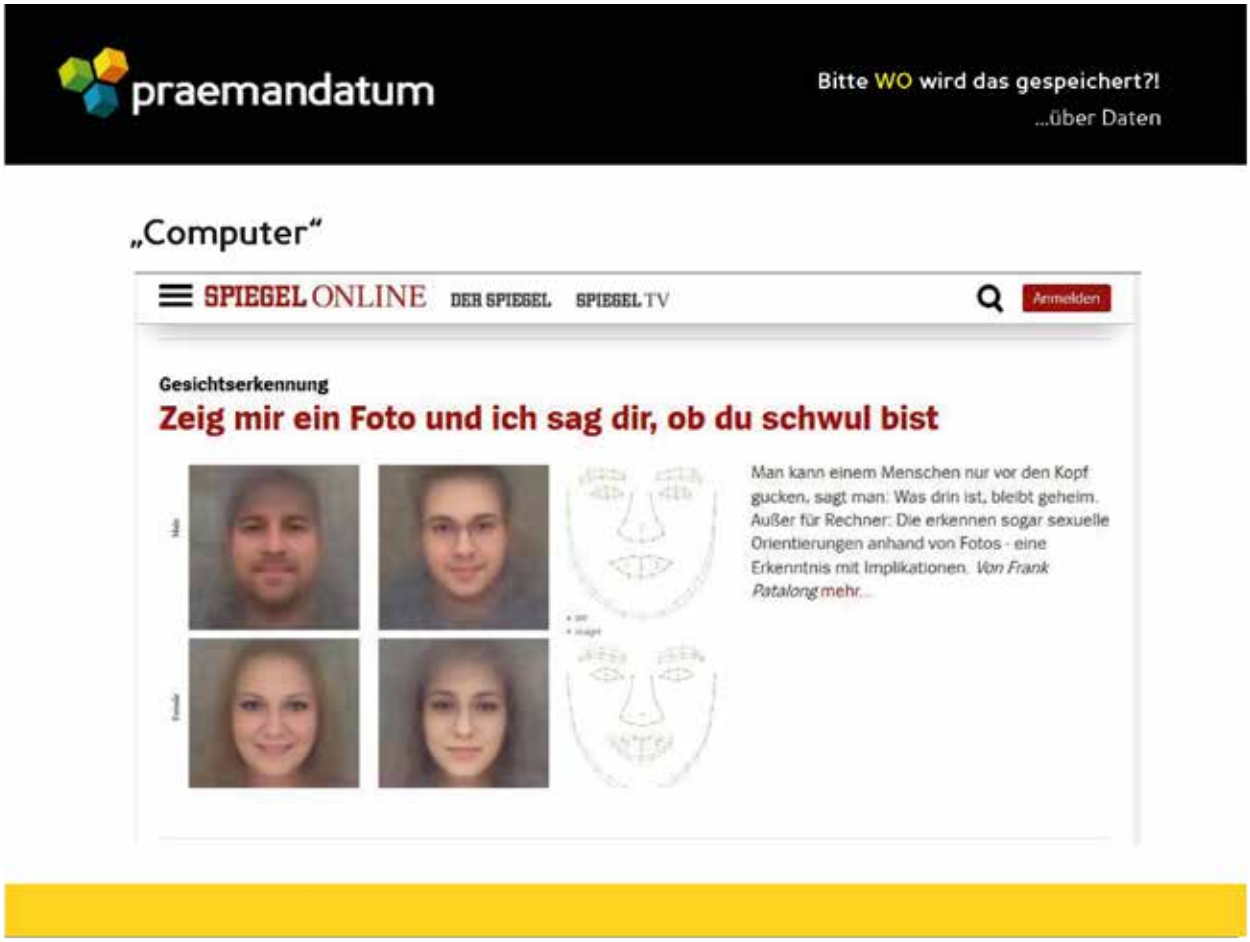
So rüsten Supermärkte im Kampf mit dem Onlinehandel auf

Die Gesichtserkennung bei Real sorgt für Aufregung, doch längst lassen auch andere deutsche Einzelhändler ihre Kunden durchleuchten - und eifern damit der Konkurrenz aus dem Internet nach.

Von Nicolai Kwasniewski

Nun kann man sagen – bleib ich doch lieber „Offline"...

Als real in einigen Märkten entsprechende Kameras installierte, gab es einen riesen Aufschrei. real hat die Kameras kurz darauf wieder entfernt. Dennoch zeigt dieses Beispiel, wohin die Reise geht. Man kann kaum noch nicht online sein, wenn man sich in öffentlichen Räumen bewegt, soziale Kontakte pflegt und einer regulären Arbeit nachgeht.

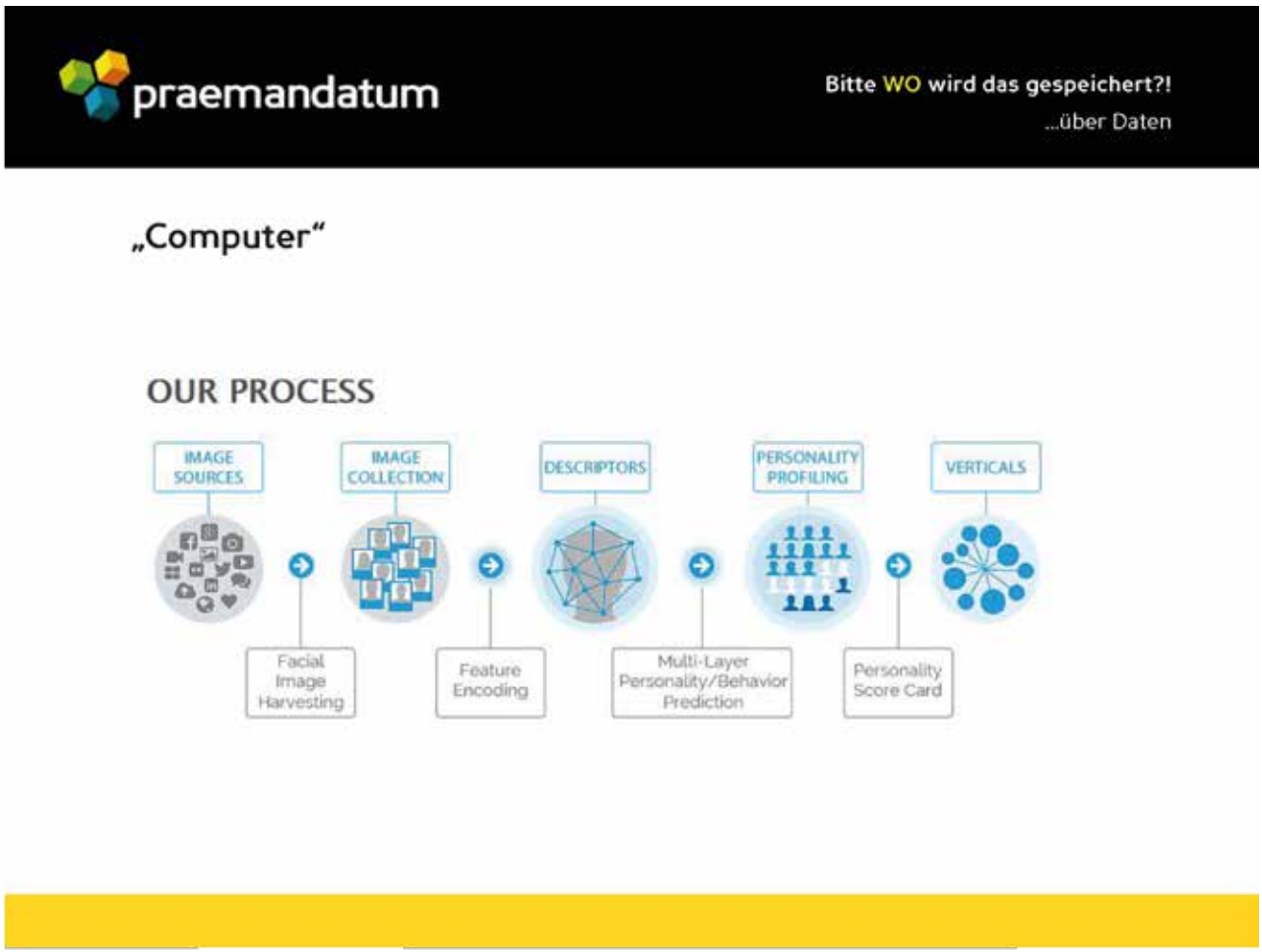


Das hier ist ein Artikel von Spiegel Online, der vor ca. 2 Wochen veröffentlicht wurde.

http://www.spiegel.de/netzwelt/netzpolitik/software-kann-homosexuelle-an-hand-von-fotos-erkennen-a-1166971.html

Der angebliche „Kampf gegen den Terror“ treibt seltsame Blüten. Bei fast allen Maßnahmen haben wir nachweisen können, dass diese überhaupt nichts mit der angeblich gefährdeten Sicherheit des Staats zu tun haben aber stets viel mit Profilbildung zur Einsortierung der Menschen in Schubladen, die zur Profitgenerierung oder zur Diskriminierung eingesetzt werden können.

Die Stanford University hat eine Studie veröffentlicht, die zeigt, wie ein Computer mithilfe von Gesichterkennungssoftware die sexuelle Orientierung von Menschen erkennt. Ergebnis: *„Ausgehend von nur einem Foto erkannte das Programm 81 Prozent aller schwulen Männer und 74 Prozent aller homosexuellen Frauen. Menschliche Probanden, denen die gleichen Bilder vorgelegt wurden, kamen hier nur auf 61 und 54 Prozent Trefferquote. Noch gruseliger wurden die Ergebnisse, wenn man dem Rechner fünf Bilder einer Person vorlegte. Dann erkannte die Software 91 Prozent der homosexuellen Männer und 83 Prozent der Frauen.“*

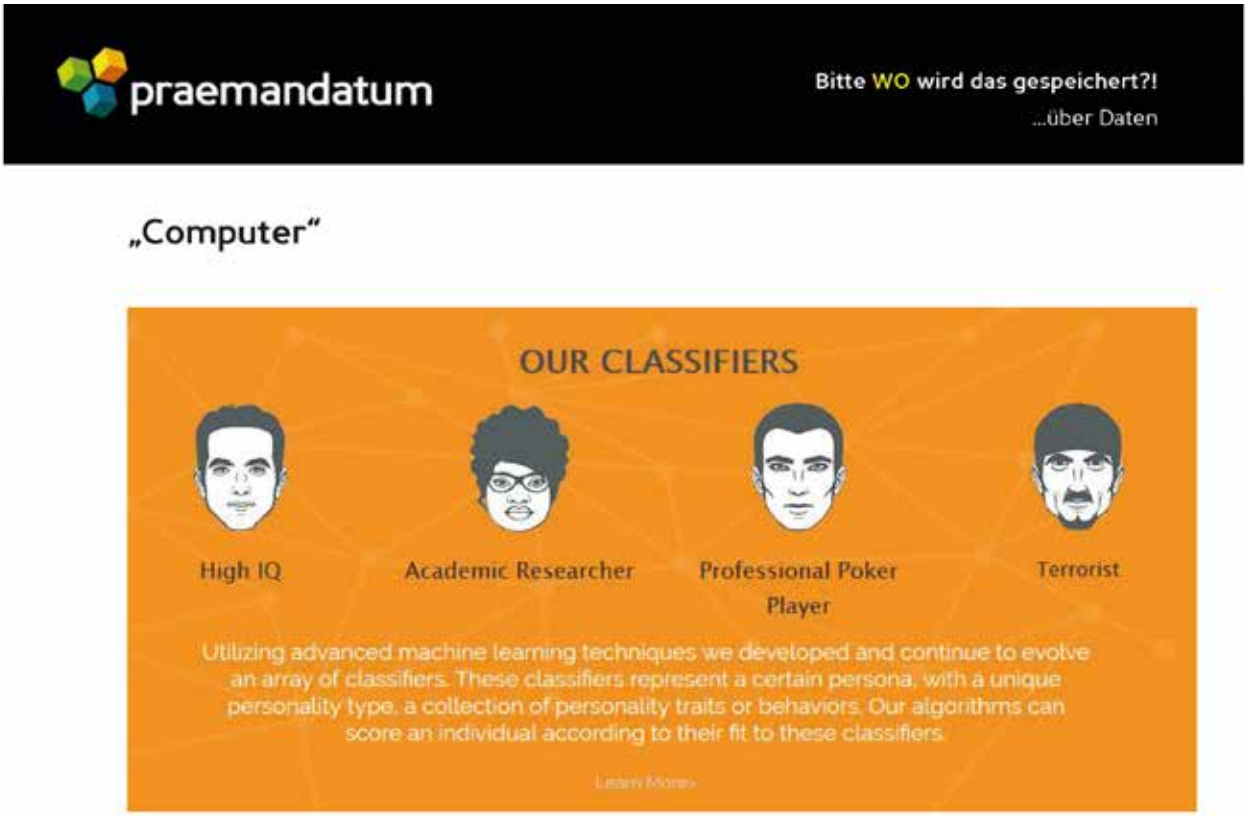


Hinter dieser Software steckt die israelische Firma Faception.

https://www.faception.com/

Auch wenn dies keine wirklich neue Technologie ist, so ist die Klarheit der Ausdrucksweise in deren Marketingunterlagen doch beachtlich und hat eine neue Stufe erreicht.

Sie nennen den ungefragten Bezug von Bildmaterial aus Sozialen Netzwerken „Image Harvesting“ (ernten) und analysieren so ohne Wissen der abgebildeten Person Gesichter.



Hier 4 von 8 Profilen, in die Faception nach eigenen Aussagen die abgebildeten Personen einteilt.

Die Firma sagt, sie habe 9 der 11 Paris-Terroristen als Terroristen klassifizieren können, von denen insgesamt nur 3 bereits polizeibekannt gewesen seien. Hier drängt sich die Frage auf, wie viele Pariser zusätzlich als Terroristen klassifiziert worden wären, die keine sind...

Es ist fraglich, ob die Menschheit für den Einsatz einer solchen Technologie bereit ist.

Zudem gefährlich: auf Technologie zu setzen im Kampf gegen Terror, die nur noch mehr Daten produziert, die ja auch ausgewertet werden muss. Thema Big Data.

Das nachweislich wirksamste Mittel gegen Terrorismus und Kriminalität ist nach wie vor gute Polizeiarbeit.

praemandatum

Bitte WO wird das gespeichert?!
...über Daten

...hinter dem „Computer"

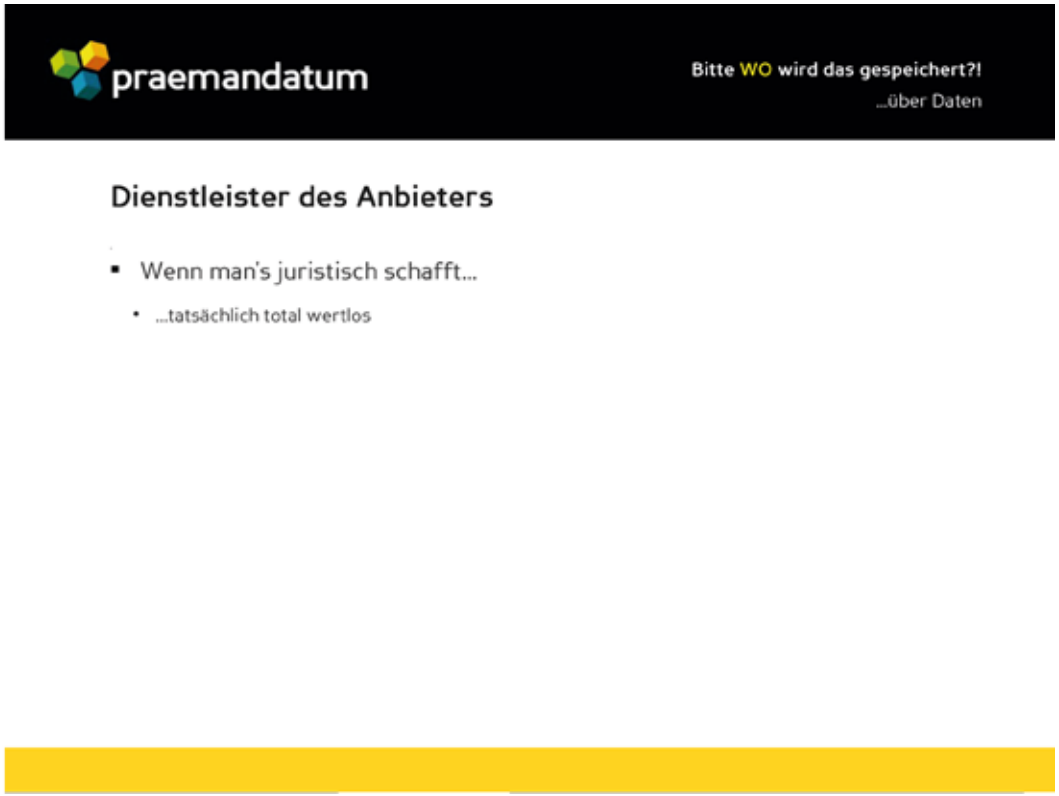
- Bsp. Apple iOS und MacOS: Auszug der aktuellen iCloud-AGB
- Der Nutzer erklärt sich damit einverstanden, dass Apple
  - "ohne Ihnen gegenüber zu haften
  - auf Ihre Kontoinformationen und Ihre Inhalte zugreifen,
  - diese nutzen, aufbewahren
  - und/oder an Strafverfolgungsbehörden, andere Behörden und/oder sonstige Dritten weitergeben darf".
- Dies ist nicht nur dann erlaubt, wenn es das Gesetz so verlangt, sondern auch,
  - "wenn Apple der Meinung ist, dass dies vernünftigerweise erforderlich oder angemessen ist"

Kombiniert man den Einsatz solcher Technologien mit den Handlungsspielräumen vieler Firmen, ergibt sich ein Bild des absoluten Kontrollverlusts. Ein durch Faception als Terrorist oder Pädophiler klassifizierter Mensch unter Generalverdacht hat vielleicht ein iPhone und hat mit der Nutzung seines Gerätes diesen AGB zugestimmt.

Ein mögliches Szenario wäre, dass einen das eigene iPhone einen prophylaktisch anzeigt bzw. einer Behörde meldet.

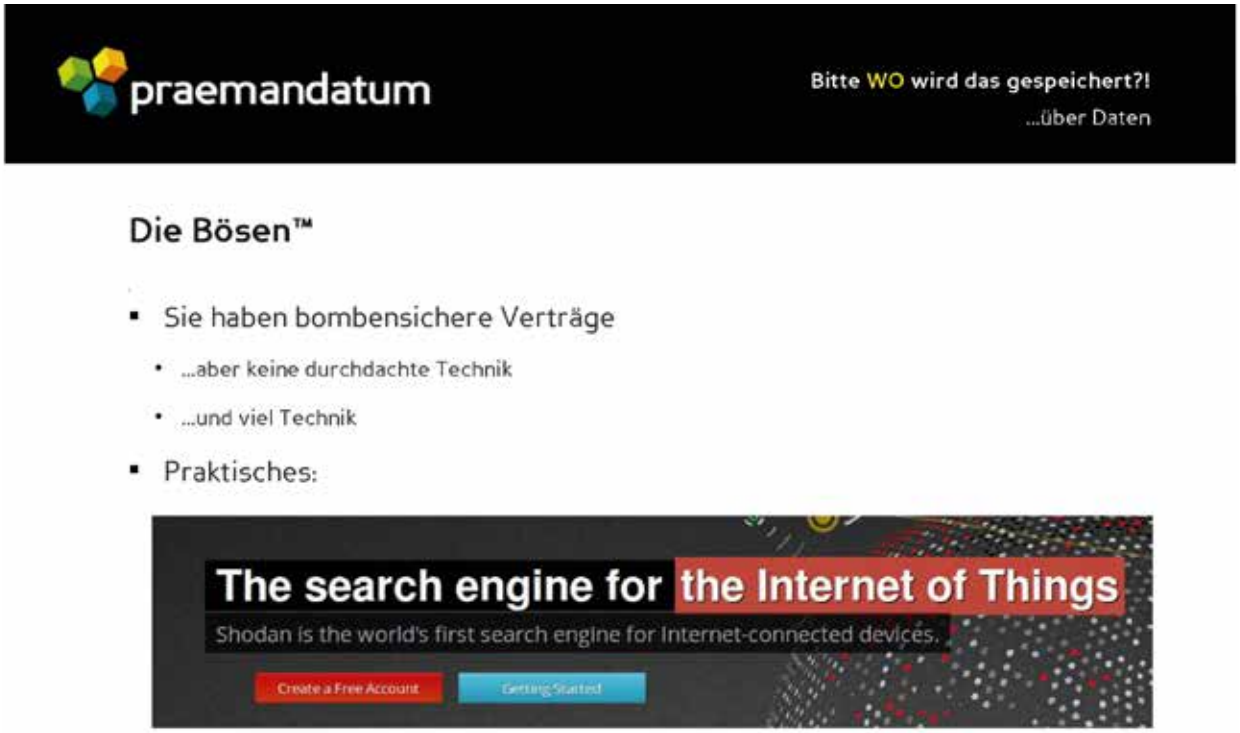
Und dies sind nur die direkten AGB. Staaten wie die USA hier in diesem Beispiel räumen sich unfassbare Rechte ein.

Das Safeharbor Unterfangen ist grandios gescheitert. Das Privacy Shield wurde vom derzeitigen US Präsidenten ausgehebelt (siehe nächste Seite).



Und dies sind nur die direkten AGB. Staaten wie die USA hier in diesem Beispiel räumen sich unfassbare Rechte ein.

Das Safeharbor Unterfangen ist grandios gescheitert. Das Privacy Shield wurde vom derzeitigen US Präsidenten ausgehebelt (siehe nächste Seite).

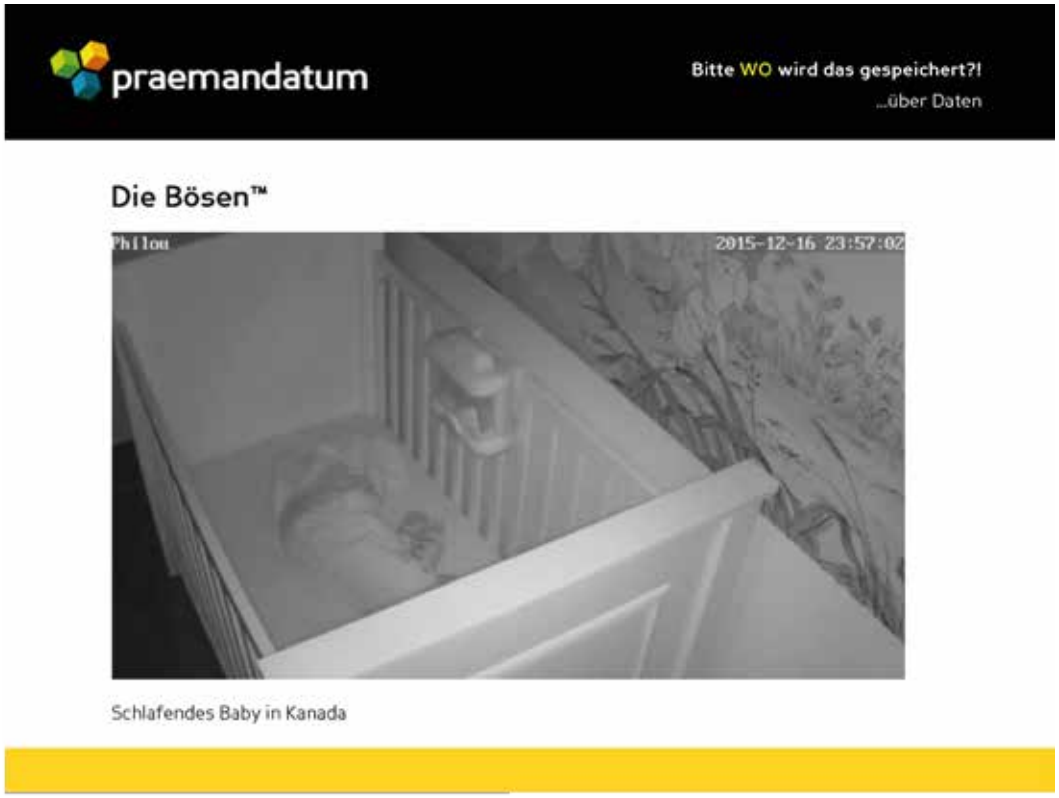


Alle internetfähigen Geräte bzw. Geräte in Netzwerken besitzen eine IP-Adresse. Shodan ist eine Suchmaschine für solche IoT-Geräte. https://shodan.io

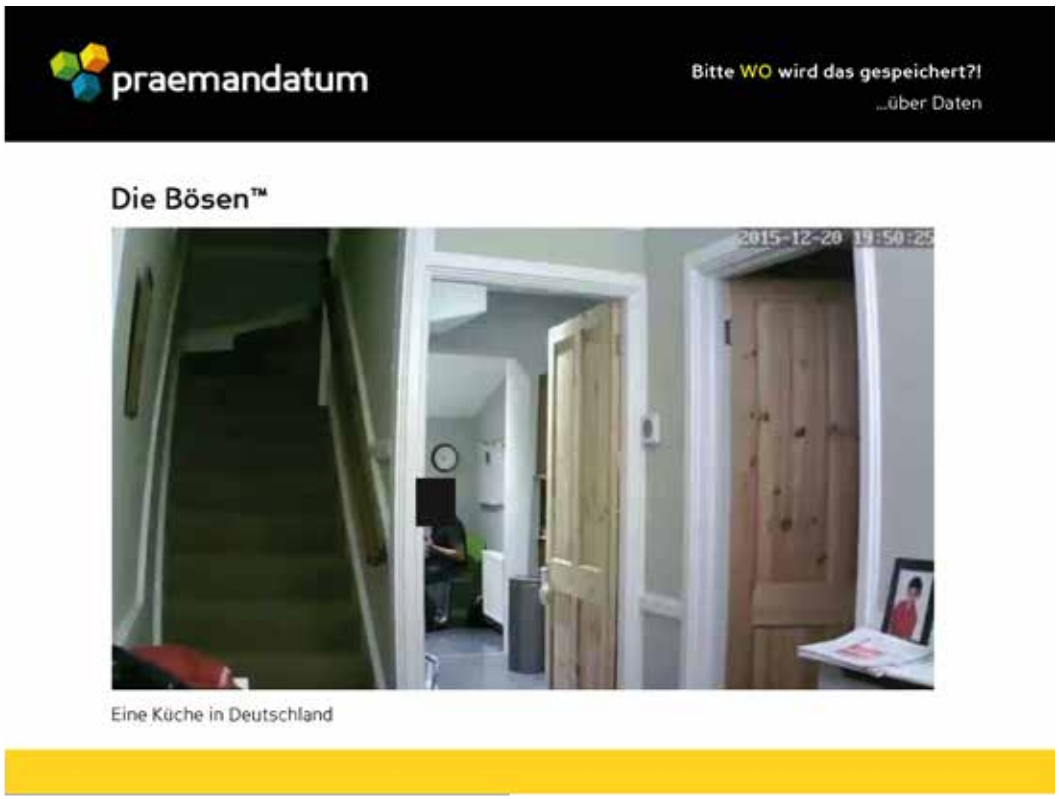
Shodan ist nicht böse. Shodan zeigt lediglich, was alles ohne „Hacker" zu sein einfach so sichtbar ist.

Wikipedia:
Shodan ist eine Computer-Suchmaschine. Sie ermöglicht Benutzern, bestimmte Arten von Computern und Diensten (Webcams, Routern, Servern usw.), die mit dem Internet verbunden sind, über eine Reihe von Filtern zu finden. Sie wird auch als Suchmaschine von Service-Bannern bezeichnet, die Metadaten der Server an den Client zurücksendet.[1] Die dabei gesammelten Daten enthalten dabei meist Informationen über die Serversoftware, unterstützte Optionen, eine Begrüßungsseite oder ähnliches, die der Server in seiner Interaktion mit dem Client übermittelt.

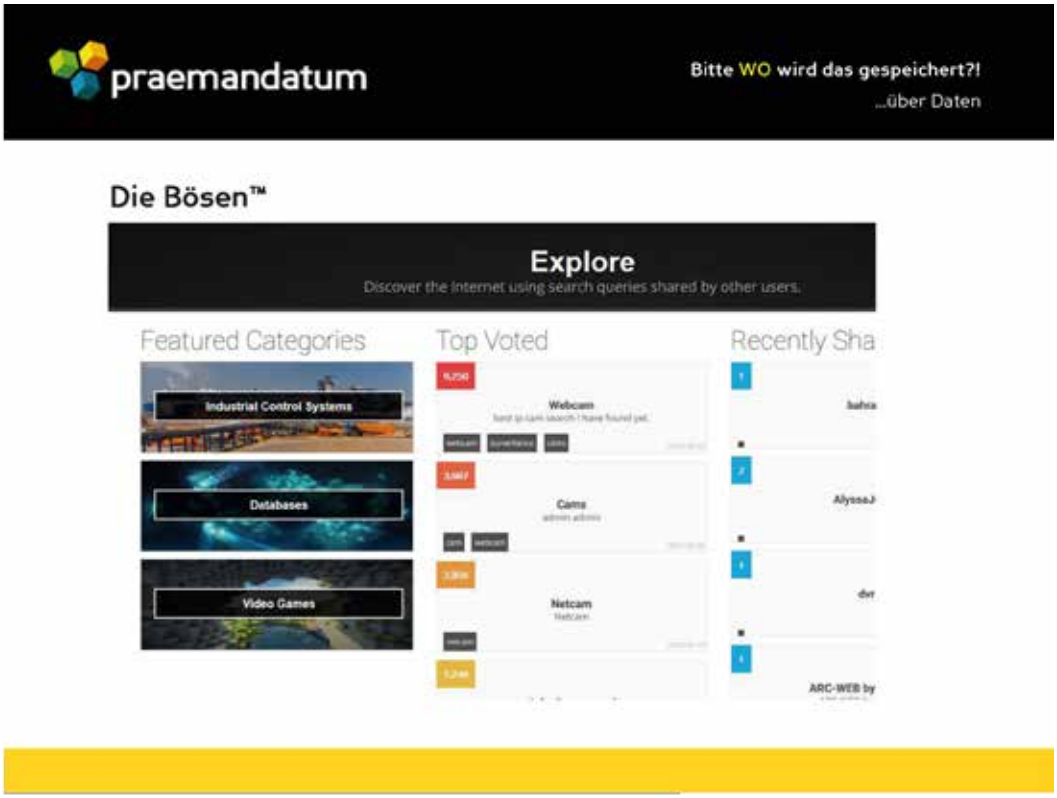
Die Webseite startete als Matherlys Heimprojekt, aufgrund der Tatsache, dass eine große Anzahl von Geräten und Computersysteme mit dem Internet verbunden sind. Shodan-Anwender sind in der Lage, Systeme wie Ampeln, Überwachungskameras, Hausheizungssysteme sowie Steuerungssysteme für Wasserparks, Tankstellen, Wasseranlagen, Stromnetze, Kernkraftwerke und partikelbeschleunigende Zyklotrons zu steuern, wenn diese nur niedrige Sicherheitsstandards erfüllen.[5][6]



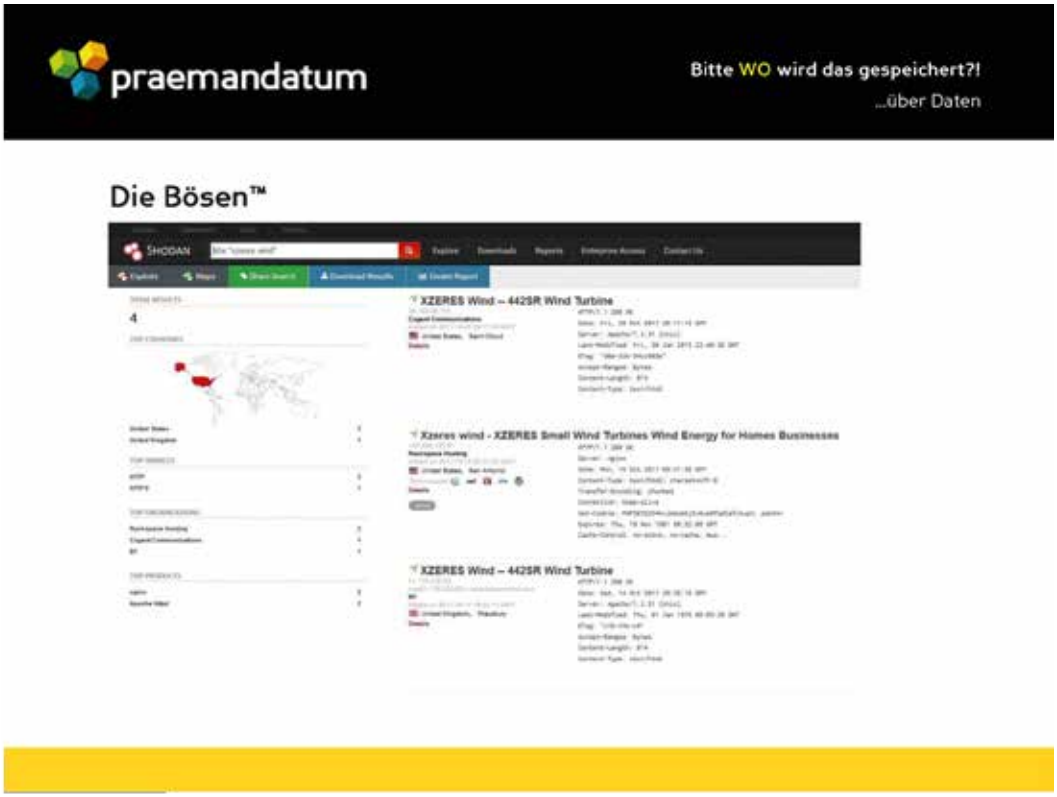
Beispiel einer nicht geschützten Webcam.



Beispiel einer nicht geschützten Webcam.



Die Kategoriesuche enthält z. B. auch Industrial Control Systems.



Windturbinen.

praemandatum

Bitte WO wird das gespeichert?!
...über Daten

Die Bösen™

http://80.147.49.163:81/view/viewer_index.shtml?id=10944

Auch spannend: https://insecam.org

Hier eine in Deutschland ansässige Firma, die ihre Kamera ungeschützt lässt und somit den Zugriff und die Steuerung über einen normalen Browser nicht unterbindet.

praemandatum

Bitte WO wird das gespeichert?!
...über Daten

Die Verwirrten

Sonntag, 13:34 **Johannes Schuster** 227

Frustrierter PlayStation-Spieler legte Teile des Internets lahm

Bild: Sony

Der Gamer hegte demnach einen persönlichen Groll auf den von Sony betriebenen Dienst für dessen internetfähige Spiele-Konsole PlayStation. Er habe sich für seinen Angriff ein Bot-Netz von rund 150.000 internetfähigen Geräten für einen Zeitraum "gemietet", darunter auch Kameras, Glühbirnen und Haushaltsgeräte.

Neben den Bösen gibt es auch die Verwirrten, die aus Zufall Dinge lahmlegen. Auch das zeigt, was möglich ist

praemandatum

Bitte WO wird das gespeichert?!
...über Daten

Andere

Bundesnachrichtendienst

GCHQ

Es gibt viele Interessenten an unseren Daten. Z. B. Kriminelle und Geheimdienste.

praemandatum

Bitte WO wird das gespeichert?!
...über Daten

Andere

Und wir unterstützen sie dabei, in dem wir uns und unser Leben mit allerlei Technik bestücken, die uns überwacht.

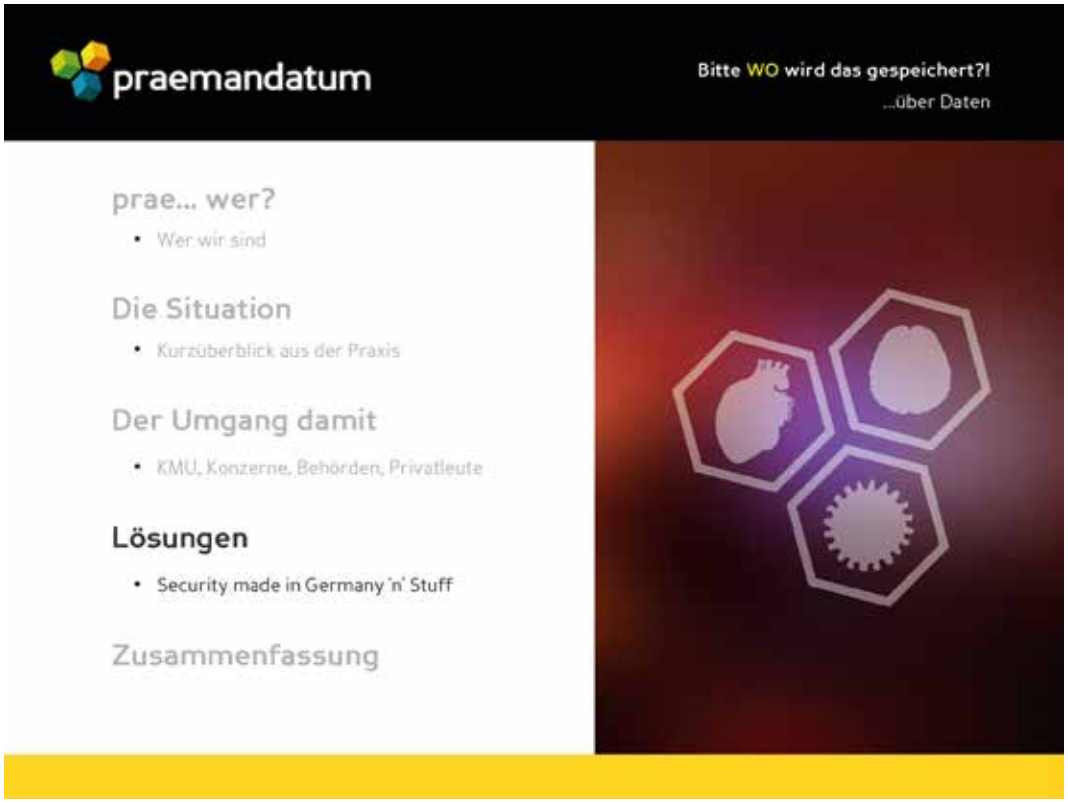
praemandatum

Bitte WO wird das gespeichert?!
...über Daten

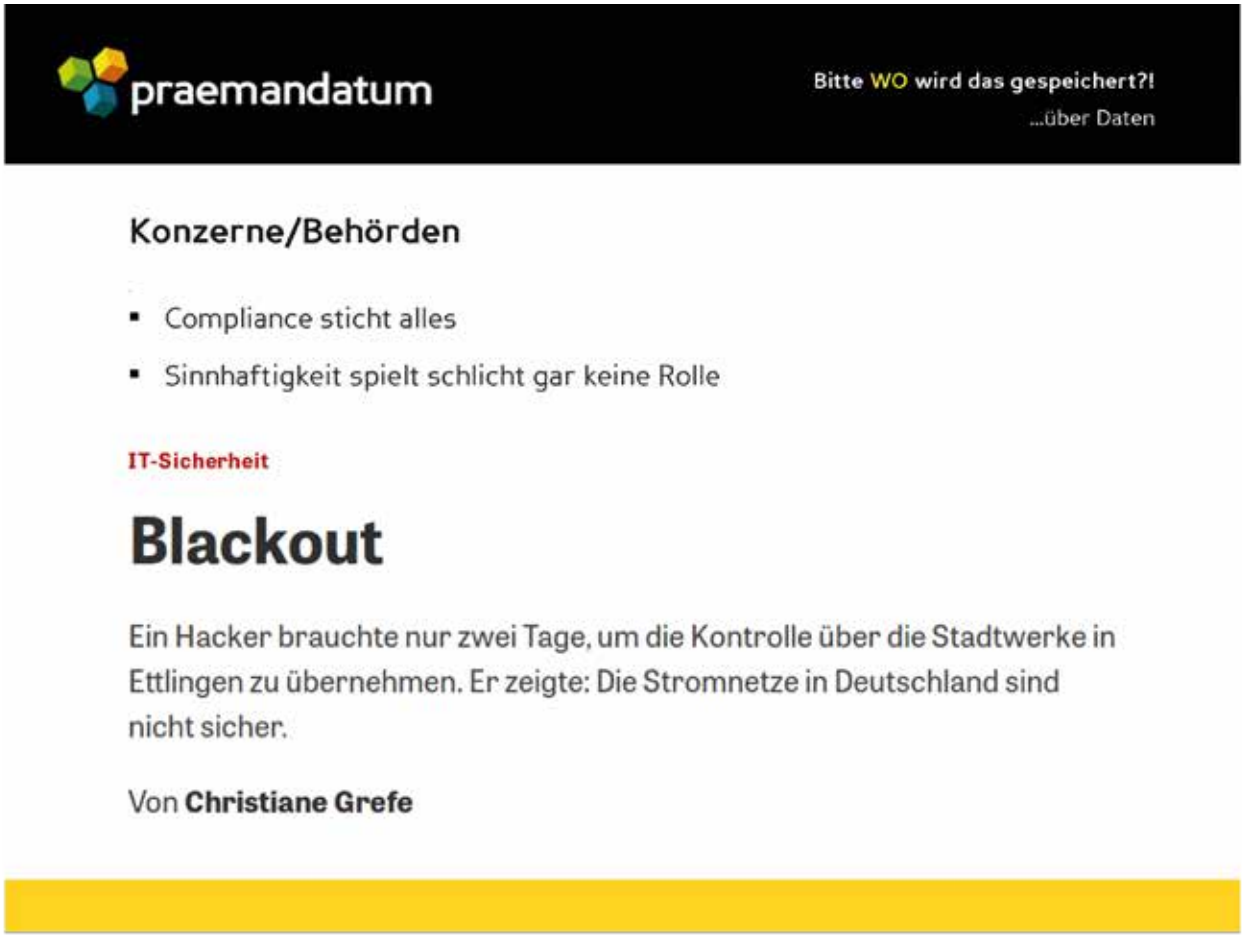
Schlussfolgerung

- Datenschutz ist ein technisches und politisches Problem
  - ...am wenigsten ein juristisches
- Wir vertrauen zu sehr

Es gibt viele Interessenten an unseren Daten. Z. B. Kriminelle und Geheimdienste.



HCM = Headless Chicken Mode



http://www.faz.net/aktuell/politik/inland/cyberangriff-stadtwerke-ettlingen-testen-system-auf-sicherheit-14980156.html

Auszug:
Das Ergebnis war aufschlussreich und besorgniserregend: Der mit dem Hackerangriff beauftragte Computerfachmann Felix Lindner habe nur wenige Minuten gebraucht, bis er das Passwort der Software entschlüsselt hatte, sagt Oehler. Es wäre ein Leichtes gewesen, 40 000 Stromkunden und einen Großteil der 200 000 Wasserkunden in Ettlingen und der Region von der Versorgung abzuschneiden. Der versierte Hacker hätte 18 Stunden gebraucht, dann wären die Bürger in Ettlingen ohne Strom und ein paar Tage später, wenn die Trinkwasserhochbehälter nicht mehr per Pumpen hätten befüllt werden können, auch ohne Wasser gewesen.

Auch deshalb warnt der Hacker Felix Lindner davor, sich durch penible Vorschriften zu sehr in Sicherheit zu wiegen. Sein Rat klingt aus dem Munde eines Netzprofis erst mal erstaunlich. Man solle bei aller Vernetzungsbegeisterung auch darüber nachdenken, wo sie überflüssig sei und wo man entflechten könne: „Getrennt halten, was geht."

Zudem äußerten sich die Stadtwerke und betonten, der Angriff sei nicht dort passiert, wo man ihn erwartet hätte...

Tritt im Mai 2018 in Kraft: die Datenschutzgrundverordnung.

DSGVO

- löst die 20 Jahre alte EU-Richtlinie zum Datenschutz 95/46/EG vom 24.10.1995 ab.
- Am 14. April 2016 die Datenschutzgrundverordnung (EU-DSGVO) vom Europäischen Parlament beschlossen.
- Ab dem 25. Mai 2018 geltendes Recht.

Die DSGVO sieht ernsthafte, rechtsverbindliche Strafen vor. Die Landesdatenschutzverbände werden dafür bezahlt, die in der DSGVO geforderten Maßnahmen zu überprüfen – und sie werden das nun auch kontrollieren.

Waren die Strafen im BDSG max.300.000 EURO (die aber meines Wissens nie durchgesetzt wurden), so fordert die DSGVO als maximale Geldbuße bis zu 20 Millionen Euro oder bis zu 4% des gesamten weltweit erzielten Jahresumsatzes im vorangegangenen Geschäftsjahr; je nachdem, welcher Wert der höhere ist. Hier ist der oben genannte Unternehmensbegriff von Bedeutung: Es gilt der Jahresumsatz des gesamten Konzerns, nicht der der einzelnen juristischen Person.

praemandatum

Bitte WO wird das gespeichert?!
...über Daten

DSGVO

- DSGVO im Vergleich zum BDSG kein Auffanggesetz mehr sondern vorrangige Vorschrift.

praemandatum

Bitte WO wird das gespeichert?!
...über Daten

prae... wer?
- Wer wir sind

Die Situation
- Kurzüberblick aus der Praxis

Der Umgang damit
- KMU, Konzerne, Behörden, Privatleute

Lösungen
- Security made in Germany 'n' Stuff

Zusammenfassung

Dies ist ein „Vertrauenszeichen" und aus meiner Sicht nutzlos, wenn es um Security geht. Quasi „Ehrlichkeit made in Germany". Meine Anmerkungen in [...].

Bedingungen, um mit diesem Zeichen zu werben:

1. Der Unternehmenshauptsitz muss in Deutschland sein. [Okay, das macht „made in Germany" immerhin zu einer Wahrheit.]

2. Das Unternehmen muss vertrauenswürdige IT-Sicherheitslösungen anbieten. [Wie sehen denn die Kriterien dafür aus?]

3. Die angebotenen Produkte dürfen keine versteckten Zugänge enthalten (keine „Backdoors"). [Musste glauben, kannste ja nich reingucken...]

4. Die IT-Sicherheitsforschung und -entwicklung des Unternehmens muss in Deutschland stattfinden. [Wie wäre es mit „von gut ausgebildeten Menschen" oder „muss kontinuierlich stattfinden"?]

5. Das Unternehmen muss sich verpflichten, den Anforderungen des deutschen Datenschutzrechtes zu genügen. [Muss das nicht jedes Unternehmen?]

Clouds und starke Vernetzung

- ...sind weder gut noch schlecht
- ...aber jeweils für bestimmte Aufgaben gut oder schlecht
- Abhängigkeit ist schlecht

Jetzt könnte man sagen, egal. Man könnte fragen, warum das alles schlimm ist. Einzeln ist das gar nicht schlimm. Es bringt ja auch viele Vorteile, wenn ich nur noch Werbung erhalte, die mich wirklich interessiert und wenn mir mein Staubsauger sagt, wo ich meinen Schlüssel hinverbummelt habe.

Das Problem entsteht vor allem aus der Kombination, denn diese macht uns abhängig und damit sehr verwundbar. Auf den folgenden Seiten ein Beispiel:

praemandatum

Bitte WO wird das gespeichert?!
...über Daten

Clouds und starke Vernetzung

imgur

imgur ist ein Filehosting-Dienst für Bilder.

Am 28.2.2017 ging es imgur nicht gut, weil ihr Dienstanbieter (= der Serveranbieter, der die Daten hostet) Probleme hatte.

praemandatum

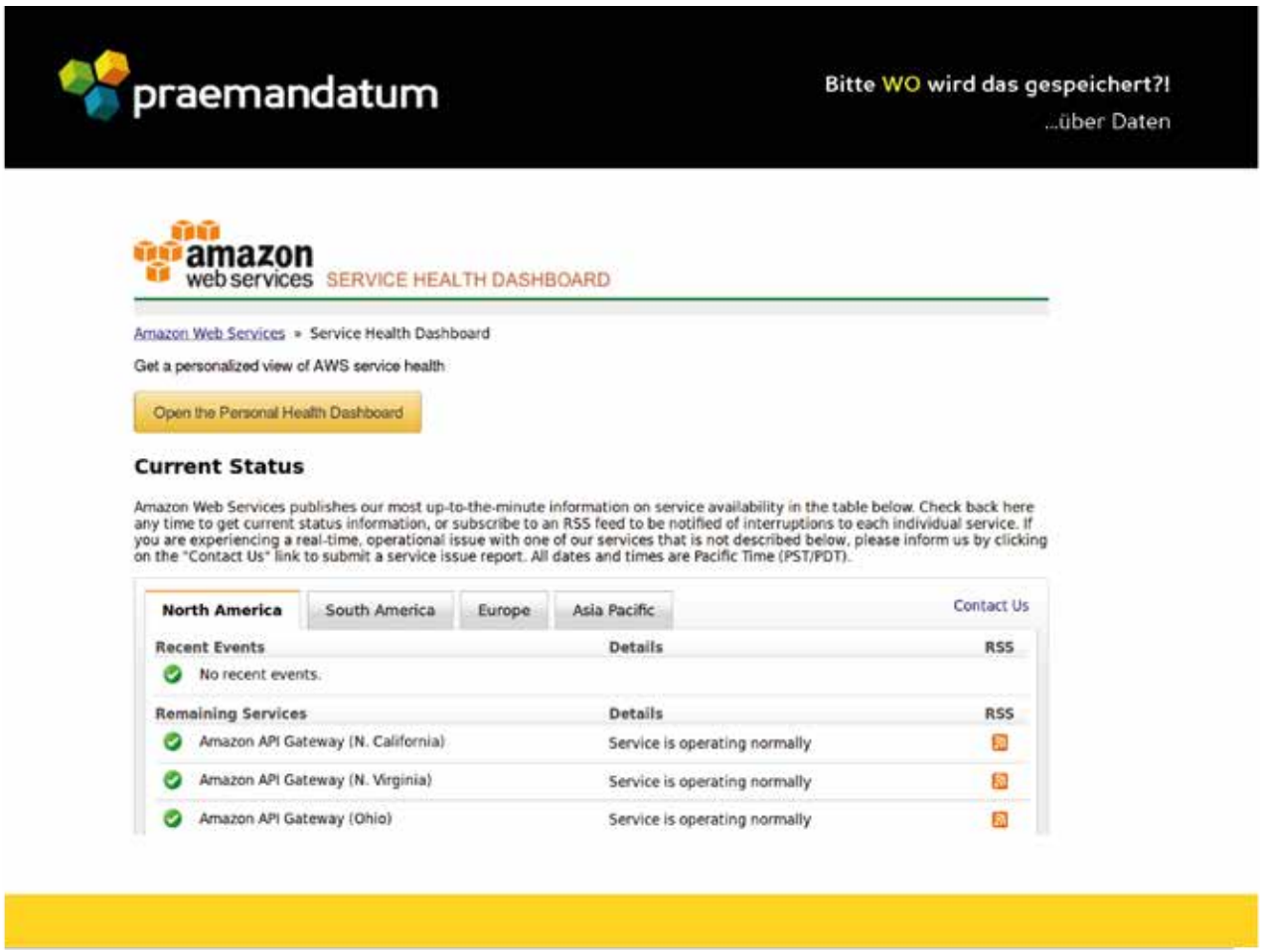
Bitte WO wird das gespeichert?!
...über Daten

Clouds und starke Vernetzung

amazon web services

imgur ist ein großer Kunde von Amazon und nutzt AWS (Amazon Webservices), um die Daten ihrer Kunden abzulegen.

Bei AWS kam es Ende Februar 2017 zu großen Ausfällen.



Kunden, deren Webservices plötzlich nicht mehr funktionierten, loggten sich in ihrem Backend bei AWS ein und schauten auf ihr Dashboard: „Alles fein, überall grüne Häkchen" ist, was sie dort sahen.

Nunja, die "Alles ist furchtbar"-Bilder konnten einfach nicht nachgeladen werden, weil AWS ja Probleme hatte. Somit konnten nur die Bilder der grünen Häkchen angezeigt werden.

praemandatum

Bitte WO wird das gespeichert?!
...über Daten

Clouds und starke Vernetzung

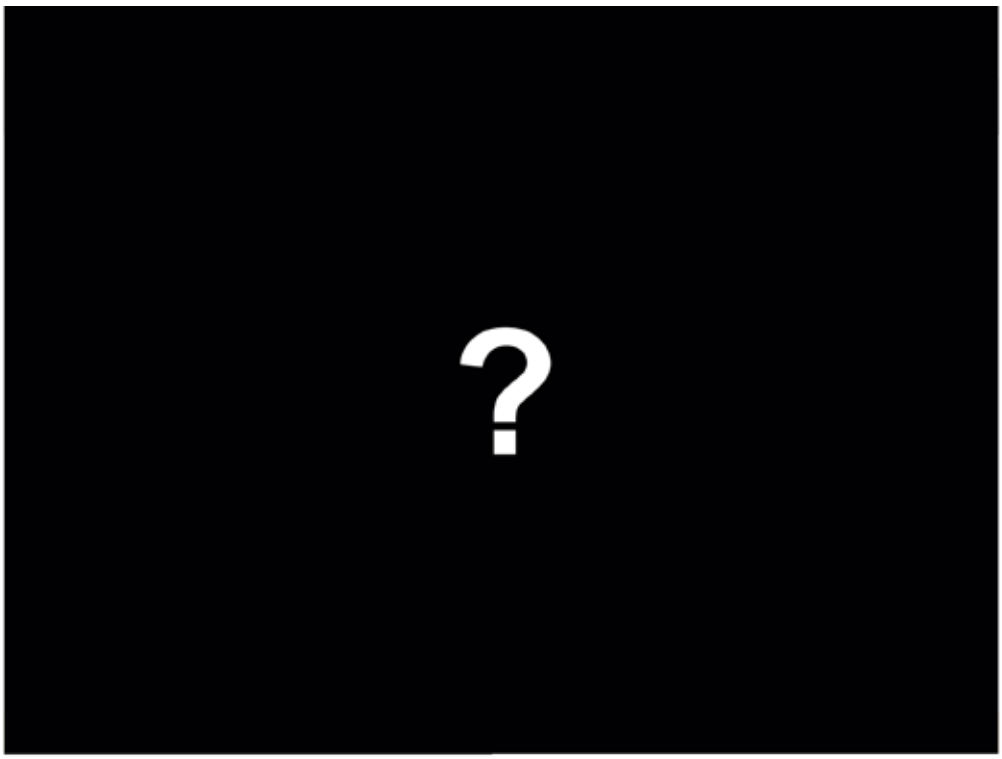
Jetzt denken wir das Szenario mal weiter (frei erfunden, wobei ich mir sicher bin, dass es diese Kombination in der Wirklichkeit so oder ähnlich gegeben hat).

Wenn Sie mit der Razer-Maus auf „Mehr Info" klicken wollen ging das nicht, weil ihre Maus nicht mehr korrekt funktionierte, weil auch diese Maus auf einen Online-Status angewiesen ist, der auf AWS fußt.

Clouds und starke Vernetzung

This is by no means an exhaustive list of things that fell over or were wobbly today, due to the S3 downtime, but here's a start: Docker's Registry Hub, Trello, Travis CI, GitHub and GitLab, Quora, Medium, Signal, Slack, Imgur, Twitch.tv, Razer, heaps of publications that stored images and other media in S3, Adobe's cloud, Zendesk, Heroku, Coursera, Bitbucket, Autodesk's cloud, Twilio, Mailchimp, Citrix, Expedia, Flipboard, and Yahoo/Mail (which you probably shouldn't be using anyway). Readers also reported that Zoom.us and some Salesforce.com services were having problems, as were Xero, SiriusXM, and Strava. Another reader reports being unable to order coffee because the Hey You app was broken.

Razer-was? Naja, nur die Spitze des Eisbergs. AWS ist einer der größten Anbieter weltweit. Dienste wie Dropbox, Netflix, Foursquare oder Reddit laufen auf AWS-Servern. Dienste wie Mailchimp, Citrix, Expedia und Salesforce waren ebenfalls von Ausfällen betroffen.



Zurück zu unserer Ereigniskette.

Die Maus tut nicht mehr und sie wollen mal nachsehen, warum. Huch, geht nicht – plötzlich ist es dunkel.

Clouds und starke Vernetzung

Joa, weil auch Ihr Osram Lightify Pause macht, denn auch die Osram-Services für diese Smart-Home-Komponente läuft auf AWS.

praemandatum

Bitte WO wird das gespeichert?!
...über Daten

Clouds und starke Vernetzung

Wenn es dann auch noch zu kalt ist, um die Glühbirne zu wechseln... könnte es am Google Nest liegen, der ebenfalls auf AWS angewiesen ist.

praemandatum

Bitte WO wird das gespeichert?!
...über Daten

Clouds und starke Vernetzung

- ...und jetzt überlegen Sie kurz, was Amazon über Sie weiß.
- ...es geht nicht um „Ist doch egal, wenn Payback weiß, dass ich gerne Milch mag"
  - Es geht um Daten im Kontext

praemandatum

Bitte WO wird das gespeichert?!
...über Daten

Was hilft?

- Kulturkompetenz
  - Erkennen des Internets
  - Erkennen meines aktuellen Gesprächspartners
  - Dann – und erst dann – Themen wie Datenschutz und -sicherheit
- Und ja, das muss jeder Einzelne selbst tun.

praemandatum

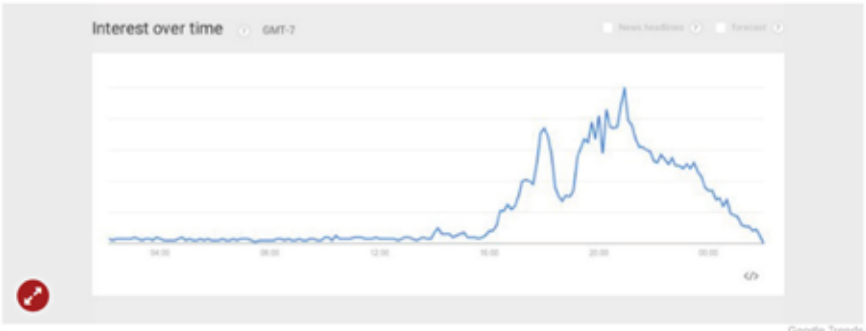
Bitte WO wird das gespeichert?!
...über Daten

Was hilft?

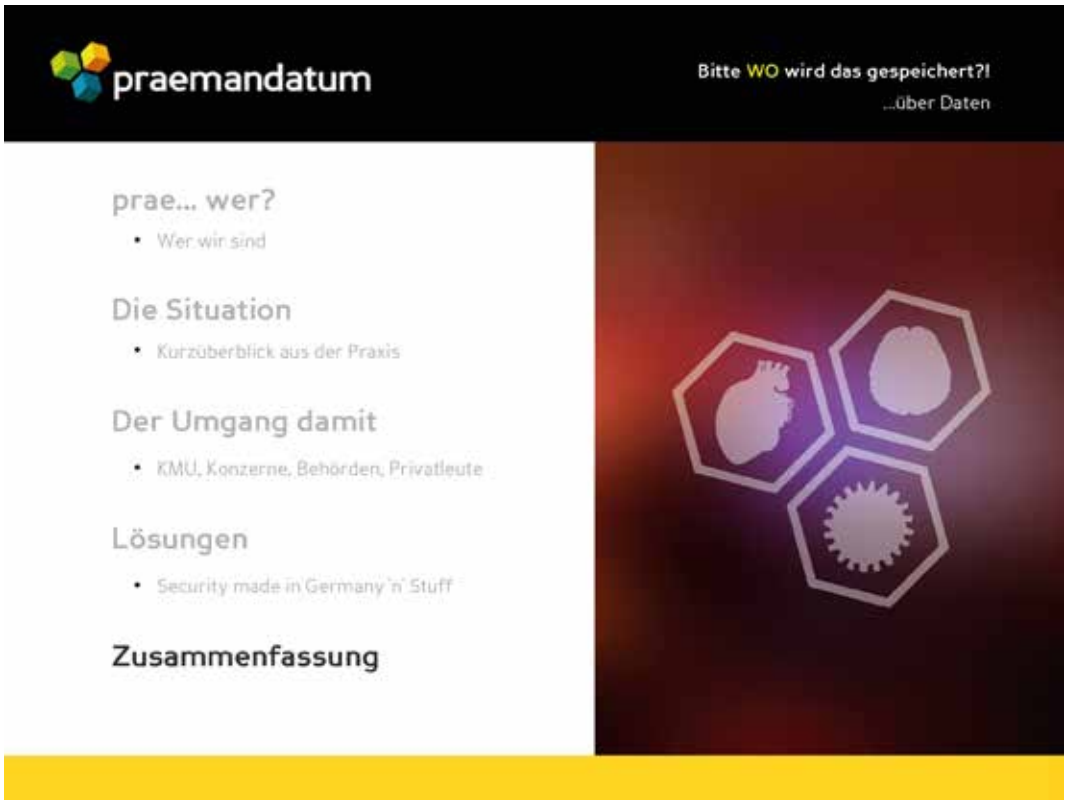
Nach Abstimmung

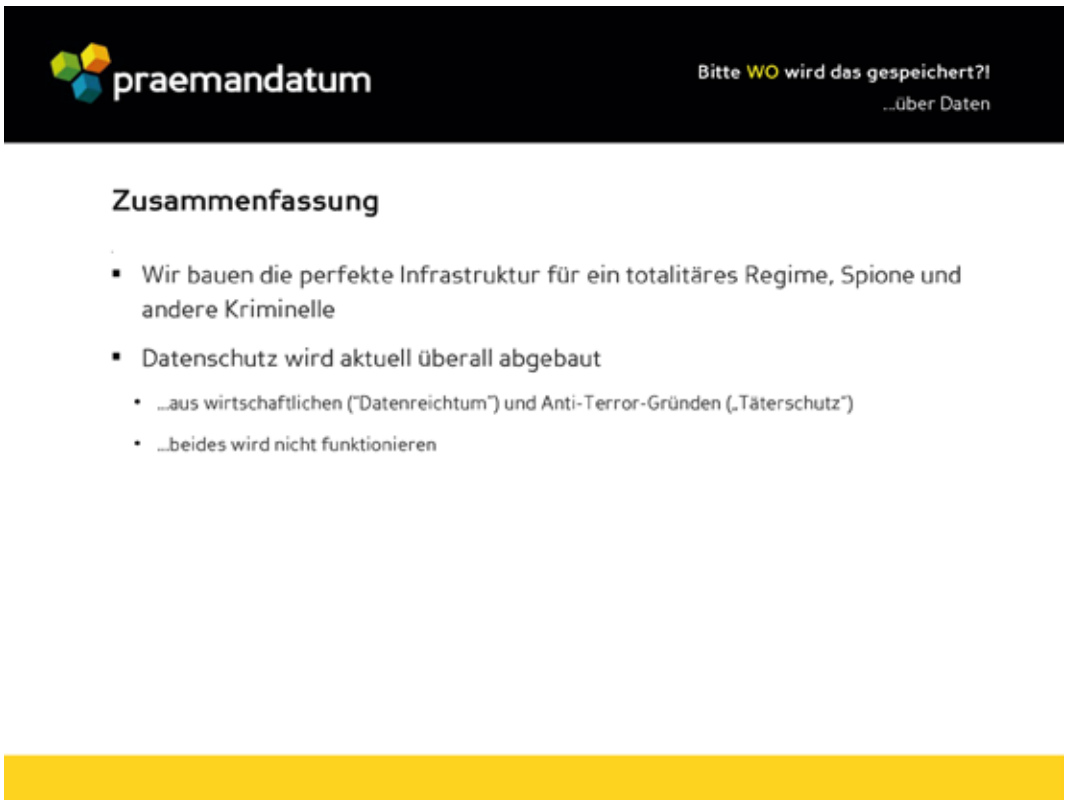
Briten googeln, was der Brexit bedeutet

"Was passiert, wenn wir aus der EU austreten?" Diese Frage interessierte sehr viele Briten – nach der Brexit-Abstimmung. Wussten sie nicht, wofür sie votierten?



Ergo: Informieren Sie sich immer im Vorfeld.


praemandatum
Bitte WO wird das gespeichert?!
...über Daten
prae... wer?
• Wer wir sind
Die Situation
• Kurzüberblick aus der Praxis
Der Umgang damit
• KMU, Konzerne, Behörden, Privatleute
Lösungen
• Security made in Germany 'n' Stuff
Zusammenfassung


praemandatum
Bitte WO wird das gespeichert?!
...über Daten
Zusammenfassung
▪ Wir bauen die perfekte Infrastruktur für ein totalitäres Regime, Spione und andere Kriminelle
▪ Datenschutz wird aktuell überall abgebaut
• ...aus wirtschaftlichen ("Datenreichtum") und Anti-Terror-Gründen („Täterschutz")
• ...beides wird nicht funktionieren

praemandatum

Bitte WO wird das gespeichert?!
...über Daten

Das Gute

- Man kann etwas tun
- Sie können etwas tun
  - Setzen Sie sich für Medienkompetenz an Schulen ein
  - Lernen Sie selbst Digitalisch (Strukturen)
  - Engagieren Sie sich politisch
- Lernen Sie die eigentliche Bedeutung von Datenschutz
  - ...weg vom Klotz am Bein
  - ...tun Sie, was Sie können, begeistern Sie andere positiv

praemandatum

Bitte WO wird das gespeichert?!
...über Daten

Social Media und so

- Folgen Sie uns gerne auf Twitter: @praemandatum
- Folgen Sie uns NICHT auf Facebook...

praemandatum

Bitte WO wird das gespeichert?!
...über Daten

Was wir anbieten

- Akademie
  - **Audits**
  - **Penetrationstests**
  - **Mitarbeitersensibilisierungen**
  - Seminare
  - Impulsvorträge
  - Workshops
  - ...
- **Zum Testen: prae-Check**

praemandatum

Bitte WO wird das gespeichert?!
...über Daten

Was wir anbieten

- Laboratorium
  - **Privacy by Design (seit 2008!)**
  - **Konzeption / Redesign / Beratung**
  - Vollabdeckung aller Themen aus einer Hand
    - Soft- und Hardware
    - Gedrucktes und Prozesse
    - Juristisches
- **Zum Testen: Lab-Dance**


praemandatum
Bitte WO wird das gespeichert?!
...über Daten
Was uns auszeichnet
Unabhängigkeit
Keine Provisionen, keine Produktverkäufe, keine intransparenten Mitgliedschaften
Reine Beratung oder Durchführung
Keine Verhinderer
...wir mögen Technik
Innovative Firmenkultur
Dazu: praeOS und „Führung durch institutionalisierte Anarchie"

Impressum

Herausgeber:	Ministerium für Inneres und Sport des Landes Sachsen-Anhalt Halberstädter Straße 2/am „Platz des 17. Juni“ 39112 Magdeburg
Redaktion:	Ministerium für Inneres und Sport des Landes Sachsen-Anhalt Referat Extremismusprävention, Spionageabwehr, Wirtschaftsschutz Nachtweide 82 39124 Magdeburg www.mi.sachsen-anhalt.de/verfassungsschutz
Gesamtgestaltung/Druck:	Fachhochschule Polizei Sachsen-Anhalt Stabsbereich I – Wissenschaftlicher Dienst/Medien –
Grafik Titel:	Ministerium für Inneres und Sport des Landes Sachsen-Anhalt, Referat 44
Foto Titel:	© wladimir1804 - Fotolia.com
Bildnachweis:	Ministerium für Inneres und Sport des Landes Sachsen-Anhalt (Seite 1, 7, 11, 90) Industrie- und Handelskammer Halle-Dessau (Seite 5) www.blomberg.com (Seite 25) Rosstat (Seite 26, 27) GFK-Institut Rus, Higher School of Economics Moscow (Seite 26) Bundesbank (Seite 27) Dr. Tobias Köllner/privat (Seiten 36 bis 44, 46) „Atlas Wladimir und Region Wladimir“ von 2005, Seiten 10 und 11 (Seite 33) praemandatum.de (Seiten 47 bis 89)