Bundesamt für Verfassungsschutz

ASW Zentralorganisation der Wirtschaft

Proaktiver Wirtschaftsschutz: Prävention durch Information

7. Sicherheitstagung des BfV und der ASW am 27. Juni 2013 in Berlin

Tagungsband

„Proaktiver Wirtschaftsschutz: Prävention durch Information“

7. Sicherheitstagung des BfV und der ASW am 27. Juni 2013 in Berlin

Tagungsband

Impressum

Herausgeber
Bundesamt für Verfassungsschutz
Referat Wirtschaftsschutz
Merianstraße 100
50765 Köln
wirtschaftsschutz@bfv.bund.de
www.verfassungsschutz.de
Tel.: +49 (0) 221/792-0
Fax: +49 (0) 221/792-2915

Gestaltung und Druck
Bundesamt für Verfassungsschutz
IT 21.2 Print- und Mediengestaltung

Bildnachweis
Deutsche Telekom AG

Stand
Juli 2013

Inhaltsverzeichnis

7. Sicherheitstagung des BfV und der ASW am 27. Juni 2013 in Berlin

ASW-Vorsitzender Volker Wagner und der Abteilungsleiter der Spionageabwehr im BfV Dr. Burkhard Even

Die 7. BfV/ASW-Sicherheitstagung fand unter dem bewährten Motto „Proaktiver Wirtschaftsschutz: Prävention durch Information“ in der Hauptstadtrepräsentanz der Deutschen Telekom AG in Berlin statt. Rund 140 Vertreter von Unternehmen und Wirtschaftsverbänden sowie Mitarbeiter von Ministerien und Sicherheitsbehörden nahmen an dem jährlichen Treffen teil. Experten aus Wirtschaft und Sicherheitsbehörden erörterten Risiken, Abwehrmaßnahmen und Sensibilisierungsstrategien für die deutsche Wirtschaft. Daneben skizzierten Experten des BfV extremistische und terroristische Bedrohungen für die Unternehmen. Schutzmaßnahmen vor den Gefahren des Social Engineerings und bei der Nutzung des Cloud-Computing ergänzten die Lageeinschätzung.

Die gemeinsame Sicherheitstagung von BfV und ASW ist ein bedeutsames und bewährtes Element im Rahmen des Wirtschaftsschutzkonzeptes der Verfassungsschutzbehörden.

Begrüßung und Eröffnung durch den Vorsitzenden der ASW, Volker Wagner

Sehr geehrter Herr Dr. Even,
liebe ASW-Mitglieder, Vertreter der Wirtschaft und der Sicherheitsbehörden, verehrte Gäste,

ich freue mich Sie heute hier bei unserem Gastgeber der Deutschen Telekom AG ganz herzlich begrüßen zu dürfen.

Dass Sie so zahlreich erschienen sind, zeigt mir, dass wir hier das richtige Thema ansprechen und es freut mich, Ihnen eine facettenreiche Agenda mit hervorragenden Referenten präsentieren zu können. Verschiedene Themen des Wirtschaftsschutzes werden wir heute ansprechen. Gerade wieder hoch aktuell ist das Thema islamistischer Terrorismus – sind doch gerade erst wieder Berichte über die Rückkehr deutscher Islamisten aus dem Syrienkonflikt durch die Nachrichten gegangen. Aber auch der Linksextremismus beschäftigt uns weiterhin, sei es durch Parolen, sei es durch abgefackelte Autos oder durch Farbbeutel an Fassaden, wie wir es bei der Telekom gerade wieder erleben.

Auch freut es mich sehr, dass wir Ihnen heute im Sinne einer guten nachbarschaftlichen Partnerschaft, eine internationale Perspektive zum Thema bieten können. Unsere österreichischen Nachbarn sind uns nämlich in einem Punkt ein Stückweit voraus – haben sie doch bereits ein Konzept für einen Beauftragten für Wirtschaftsschutz im Innenministerium implementiert.
Herr Weiss, herzlich willkommen, ich freue mich bereits jetzt auf Ihre Ausführungen.

In den Fachforen können Sie dann wählen, ob Sie Ausführungen erstens zur dunklen Seite des Internets, zweitens zu Advanced Persistent Threats oder drittens zur Sicherheit von Rechenzentren folgen möchten.

Am Nachmittag beschäftigen wir uns dann mit Datensicherheit in der Cloud und Manipulation von Mitarbeitern durch Social Engineers, bevor unser Tag durch eine Abschlussdiskussion mit allen Referenten abgerundet wird. Sie sehen also, eine vielversprechende Veranstaltung.

Ich bin sicher, auch in diesem Jahr wird diese fast schon „traditionelle“ BfV/ASW-Kooperationsveranstaltung erfolgreich sein. Denn die langjährige, gute und vertrauensvolle Zusammenarbeit mit dem BfV und insbesondere der für das Thema Wirtschaftsschutz verantwortlichen Abteilung von Dr. Even und dem Referat um Herrn Kurek und seinem Team, ist Basis für ein gutes Gelingen. So eine intensive Kooperation, wie wir sie nun

haben, ist nicht selbstverständlich und ich bin stolz, dass wir hier gemeinsam – nun im 7. Jahr – mit gutem Beispiel voran gehen können.

Nach meinem Verständnis und wie wir es in einem Eckpunktepapier unter Federführung des BMI zusammen, herzlich Willkommen auch Herr Akmann und Herr Dr. Mende, die gerade auch in einer kritischen Situation der ASW zur Seite standen, mit den Sicherheitsbehörden und anderen Verbänden erarbeitet haben, beinhaltet „Wirtschaftsschutz“ zwei wesentliche Bedrohungsfelder: Die Wirtschaftskriminalität und die Wirtschaftsspionage. Sie bescheren dem Wirtschaftsstandort Deutschland jährlich einen erheblichen Schaden in Milliardenhöhe.

Globalisierung und virtuelle Vernetzung tun ihr übriges dazu, den Schutz in ein hoch komplexes Themenfeld zu wandeln, dem man als Einzelkämpfer schon längst nicht mehr gewachsen ist.

Know-how und Innovationsfähigkeit deutscher Unternehmen sind die Schlüsselfunktion unserer Wettbewerbsfähigkeit und unseres wirtschaftlichen Wohlstands. Sie generieren kriminelle Neider, die illegal versuchen, ein Stück vom Kuchen abzubekommen.

Die Wirtschaftskriminalität ist in Teilen ein hoch professioneller Markt mit eng miteinander vernetzten Tätern, die das Modell der Arbeitsteilung perfektionieren. Im Bereich Cyber: ein Land entwickelt die Software, ein anderes startet den Angriff und in einem dritten Land stehen die Server.

Sie wissen ich komme aus einem weltweit engagierten Konzern mit sehr großen Zahlen auf allen Ebenen: ca. 230.000 Mitarbeiter, mehr als 60 Mrd. Euro Umsatz, Präsenz in 50 Ländern und über 150 Millionen Kunden. Hier lernt man schnell, dass die Fläche potenzieller Angriffsmöglichkeiten enorm groß ist. Daher ist mir das Thema und insbesondere die Zusammenarbeit – was wir ja bereits an vielen Stellen tun, mit dem BfV, mit Verbänden, mit anderen Unternehmen und Sicherheitsbehörden – besonders wichtig. Je mehr Unternehmen wir von dem Mehrwert dieser Zusammenarbeit überzeugen, umso informierter und sicherer lässt sich der Wirtschaftsschutz umsetzen.

Auf der anderen Seite finden wir die Situation, dass die Gesellschaft und gerade auch Unternehmen selbst, noch nicht sensibilisiert genug für diese Situation sind. Häufig fürchten Unternehmen, die Opfer wurden, einen öffentlichen Reputationsverlust, Regressforderungen oder gar strafrechtliche Folgen, wenn sie einen Vorfall melden. Ein Grund hierfür ist fehlendes Wissen über Abläufe und Unterstützungsmöglichkeiten gerade auch von behördlicher Seite. Es existiert noch kein kohärenter und abgestimmter Handlungsrahmen.

Dem versuchen wir mit Veranstaltungen wie heute Abhilfe zu schaffen. Simpel ausgedrückt, die „Bösen“ vernetzen sich, also sollten wir die „Guten“ das auch tun. Nur so sehe ich die Chance, einen verlässlichen Schutz für die Wirtschaft in unserem global agierenden Umfeld langfristig aufzubauen.

Dabei die Bestrebungen der Politik und wichtiger Initiativen zu unterstützen und fördern, sehe ich als ganz klare Aufgabe der ASW. Als Mittler zwischen Politik und Wirtschaft verstehen wir uns, als Spitzenverband der Sicherheitsexperten. Es ist unser Auftrag, den Wirtschaftsschutz weiter voranzubringen, indem wir:

1. Mithelfen die entsprechenden Rahmenbedingungen zu schaffen,
2. Den Informationsaustausch ebenso wie den Dialog zu fördern und
3. die Expertise und das Wissen aus unserem Netzwerk zur Verfügung stellen.

Daher ist die jährliche Veranstaltung mit dem BfV – einer der wichtigsten, wenn nicht den wichtigsten Experten auf dem Gebiet Schutz vor Wirtschaftsspionage – für uns essenziell, um das Thema in den Fokus zu rücken, zu informieren und um die Gelegenheit zum Austausch zu bieten.

Somit erhoffe ich mir heute viele wertvolle Diskussionspunkte und Eindrücke zu dem immer noch Top aktuellen Thema „Wirtschaftsschutz“.

Eine solche Veranstaltung ist nur mit Unterstützung möglich. Neben dem BfV, mit dem wir als ASW die Organisation und Inhalt des heutigen Tages gemeinsam gestaltet haben, möchte ich mich auch bei unserem Partner Deloitte und unserem Förderer der Power Unternehmensgruppe bedanken, die mit dazu beigetragen haben, dass Veranstaltungen dieser Art stattfinden können.

Auch möchte ich Sie daruf aufmerksam machen, dass wir Ihnen heute ebenfalls die praktische Seite des Themas Wirtschaftsschutz etwas näher bringen wollen. Wenn Sie in den Pausen Zeit und Lust haben, freuen sich unsere Ständebetreiber auf Ihren Besuch. Zusätzlich haben wir von der Deutschen Telekom auch einen Stand zum Thema Abhörschutz eingerichtet, wo Sie sich persönlich über spezielle Schutzmaßnahmen informieren können. Auch hier lohnt es sich vorbeizuschauen!

Lassen Sie uns nun mit der Keynote den Tag beginnen. Herr Dr. Even, vielen Dank, dass Sie sich die Zeit genommen haben, heute hier zu sein und uns in das Thema einzuleiten.

In diesem Sinne, lieber Herr Dr. Even, „the stage is yours!“

Begrüßung und Keynote des Abteilungsleiters Spionageabwehr im BfV, Dr. Burkhard Even

Meine sehr verehrten Damen und Herren, lieber Herr Wagner,

ich freue mich sehr, Sie anlässlich der 7. BfV/ASW-Sicherheitstagung begrüßen zu können. Mein besonderer Dank gilt Ihnen, Herr Wagner, und der ASW für die langjährige und vertrauensvolle Kooperation im Wirtschaftsschutz und heute zudem, dass wir Gast in der Repräsentanz der Deutschen Telekom in Berlin sein können.

Die alljährliche Sicherheitstagung ist für uns ein wichtiger Baustein im Rahmen unserer Wirtschaftsschutzaktivitäten. Die heutige Agenda bildet ein breites Themenspektrum im Wirtschaftsschutz ab.

Mein herzlicher Dank daher auch an die Experten aus der Wirtschaft und den Sicherheitsbehörden, die heute zu uns sprechen werden.

An dieser Stelle möchte ich auch die Vertreter ausländischer Partnerdienste aus Österreich, der Schweiz, aus Belgien, Großbritannien, Ungarn, Polen, den USA und Australien sehr herzlich begrüßen.

Ihre Anwesenheit, meine Damen und Herren, unterstreicht besonders die internationale Bedeutung des Wirtschaftsschutzes und der damit verbundenen vertrauensvollen Kooperation.

Der Austausch von Informationen, der gemeinsame Dialog, das Kennenlernen und das Vertiefen bestehender Kontakte ist eine der Grundlagen vertrauensvoller Kooperation zwischen Staat und Wirtschaft. Eine erfolgreiche Veranstaltung lebt vom gegenseitigen Austausch und der Diskussion. Nutzen Sie hierzu die Gelegenheit – während der Veranstaltung und anschließend beim „get-together“.

Seit nunmehr fünf Jahren widmet sich das Bundesamt für Verfassungsschutz proaktiv dem Wirtschaftsschutz als eine seiner prioritären Schwerpunktaufgaben.

Bevor ich auf die Bilanz der Aktivitäten des Bundesamtes für Verfassungsschutz im Bereich des Wirtschaftsschutzes eingehe, gestatten Sie mir einige grundlegende Anmerkungen.

Wirtschaftsspionage und Konkurrenzausspähung sind eine permanente Bedrohung für die deutsche Wirtschaft. Bedroht sind vor allem technologieorientierte und innovative mittelständische Unternehmen, die das Rückgrat der deutschen Wirtschaft bilden. Allerdings sind sich Vorstände und Geschäftsführer wie auch die Mitarbeiter dieser Unternehmen vielfach der Risiken ungewollten Know-how-Verlustes wenig bewusst. Nur selten verfügen diese Unternehmen über ein Informationsschutzkonzept.

Staat und Wirtschaft haben die damit verbundenen vielfältigen Herausforderungen angenommen. Hierbei ist unser Ziel, Forschung und Wissenschaft, technologieorientierte Unternehmen sowie Betreiber Kritischer Infrastrukturen praxisgerecht, d.h. angemessen zu schützen auf der Basis: Hilfe zur Selbsthilfe!

Das Kernstück der staatlichen Initiative im Rahmen des Wirtschaftsschutzes bildet der interministerielle „Ressortkreis Wirtschaftsschutz“, der 2008 auf Betreiben des Bundesministeriums des Innern eingerichtet worden ist. Ihm gehören neben den Sicherheitsbehörden des Bundes Vertreter weiterer für Wirtschafts- und Sicherheitsfragen zuständiger Ministerien und Verbände an.

Unser langjähriger Kooperationspartner auf Seiten der Wirtschaft ist die ASW, daneben aber auch der Bundesverband der Deutschen Industrie (BDI), der „Deutsche Industrie- und Handelskammertag“ (DIHK) sowie der „Bundesverband der Sicherheitswirtschaft e.V.“ (BDSW).

Mit dem Ressortkreises Wirtschaftsschutz gibt es auf Bundesebene erstmalig ein übergeordnetes Gremium, mit dem ein unmittelbarer und stetiger Austausch über grundsätzliche Fragen im Bereich des Wirtschaftsschutzes ermöglicht wird und eine Steuerung der Schutzmaßnahmen erfolgen kann.

Die deutsche Wirtschaft profitiert von diesem Gremium insbesondere durch einen verbesserten Informationsaustausch zwischen den staatlichen Stellen.

Ein weiteres Kernstück und damit das Fundament des Wirtschaftsschutzes stellt die „Rahmenregelung für die Zusammenarbeit mit der gewerblichen Wirtschaft auf Bundesebene in Sicherheitsfragen“ dar, die ebenfalls 2008 auf Initiative des BMI überarbeitet und optimiert wurde.

Das Wirtschaftsschutzkonzept des Verfassungsschutzes ist integraler Bestandteil dieser Rahmenregelung und beschreibt detailliert Art und Umfang der Aufgabenwahrnehmung und der Kooperation des Verfassungsschutzes mit der Wirtschaft. Ein wesentlicher Bestandteil ist aber zugleich auch die Notwendigkeit der Übermittlung von Informationen über vermutete oder eingetretene Schadensfälle durch die Unternehmen.

Wirtschaftsschutz darf keine Einbahnstraße sein.

Die Einrichtung des Ressortkreises Wirtschaftsschutz im Jahr 2008 führte auch zu einer Neuausrichtung des Wirtschaftsschutzes im BfV. Dazu wurde im BfV ein eigenständiges Wirtschaftsschutzreferat gebildet, das ausschließlich für die Aufgabenwahrnehmung „Prävention durch Information“ zuständig ist.

Dieses Querschnittsreferat bündelt die Sachkompetenz der wirtschaftsschutzrelevanten Fachreferate des BfV und stellt das vorrangige Bindeglied des BfV zu den Verbänden, Unternehmen, aber auch zu Forschungs- und Wissenschaftseinrichtungen, dar.

Mit seiner langjährigen Erfahrung im Bereich der Aufklärung und Abwehr von Spionageaktivitäten fremder Nachrichtendienste sieht es sich auch als Dienstleister für Spionageabwehr und als Partner der Unternehmen sowie der Forschungs- und Wissenschaftseinrichtungen.

Ich möchte nachdrücklich darauf hinweisen, dass das BfV auch auf dem Gebiet des Wirtschaftsschutzes eine intensive Kooperation mit den Kolleginnen und Kollegen der Landesbehörden für Verfassungsschutz pflegt.

Zeitnahe gegenseitige Information und Abstimmung sowie die Einrichtung einer regelmäßig tagenden Arbeitsgruppe Wirtschaftsschutz sind schon seit Jahren ein wesentlicher Bestandteil effektiven und vertrauensvollen Wirtschaftsschutzes durch die Verfassungsschutzbehörden.

„Prävention durch Information“ ist das Leitmotiv für die Security Awareness-Aktivitäten des BfV, denn Vorbeugung ist auch beim Wirtschaftsschutz stets einer nachträglichen Schadensminimierung vorzuziehen, zumal davon ausgegangen werden muss, dass eine Vielzahl von ungewollten Know-how-Abflüssen gar nicht erst erkannt wird.

Das Dunkelfeld ist hier besonders groß.

Die Ergebnisse einer Sicherheitsstudie des Sicherheitsdienstleisters Corporate Trust „Industriespionage 2012“ überrascht in diesem Zusammenhang nicht: Weniger als die Hälfte der befragten Unternehmen besitzen überhaupt ein Sicherheitsmanagement mit klaren Regeln für den Informationsschutz. Nur jedes fünfte Unternehmen hat schützenswertes Know-how im Unternehmen definiert. Leider wurde offenbar auch nur bei etwa 20% der erkannten Schadensfälle die Verfassungsschutz- bzw. Polizeibehörden in die Aufklärung einbezogen.

Seit 2008 hat das BfV eine ganze Reihe von Aktivitäten in Sachen Wirtschaftsschutz ergriffen:

Unser Leitmotiv „Prävention durch Information“ umfasst im Kern eine breit angelegte Vortragstätigkeit in Wirtschaft, Wissenschaft und Forschung. Zielgruppe der jährlich mehr als einhundert Sensibilisierungsmaßnahmen des BfV sind sowohl die Verbände der einzelnen Branchen mit ihrer Multiplikatorenfunktion als auch Forschungseinrichtungen und Hochschulen.

Aber auch einzelnen Unternehmen, insbesondere den kleineren und mittleren Unternehmen, bietet das BfV in einer zunehmenden Anzahl

von bilateralen Informationsgesprächen zu konkreten Sicherheitsthemen und Sachverhalten oder gemeinsam gestalteten Security-Awareness-Kampagnen für das Management und die Belegschaft seine Unterstützung an.

Gedruckte und elektronische Publikationen sind eine wichtige und nachhaltige Ergänzung zu Vorträgen und persönlichen Kontakten.

Hier muss an erster Stelle der Sonderbericht Wirtschaftsschutz erwähnt werden, der seit Jahren zur Standardlektüre der Sicherheitsverantwortlichen in der Wirtschaft und den Behörden zählt. Er wird unter Federführung des BND als ein Gemeinschaftsprodukt der Sicherheitsbehörden des Bundes erstellt und erscheint monatlich. Die Resonanz ist durchweg positiv.

Gemeinsam mit den Landesbehörden für Verfassungsschutz haben wir im August 2010 eine Reihe broschierter Kurzinformationen zum Wirtschaftsschutz entwickelt.
Diese Reihe umfasst mittlerweile zehn Flyer zu Themen wie Sicherheit auf Geschäftsreisen, der Innentäter als Sicherheitsrisiko, Sicherheit im Know-how-Transfer und sicheres Besuchermanagement. Natürlich liegen diese Kurzinformationen heute für Sie aus, können aber auch auf der Homepage des BfV heruntergeladen werden.

Auch unsere Hauptbroschüre „Wirtschaftsspionage – Risiko für Ihr Unternehmen“ wird derzeit überarbeitet und in Kürze neu erscheinen und wird ebenfalls auf unserer Homepage (www.verfassungsschutz.de) abrufbar sein.

Ein vierteljährlich erscheinender BfV-Newsletter Wirtschaftsschutz dient der regelmäßigen Übermittlung von Informationen und der Verstetigung von Kontakten. Eine Vielzahl der Empfänger stellt den Newsletter z.B. über firmeneigene Intranets einer größeren Anzahl von Betriebsangehörigen zur Verfügung. Es würde mich freuen, wenn Sie sich auf unserer Homepage hierfür anmelden würden.

Als Veranstalter organisieren wir nicht nur die alljährliche BfV/ASW-Sicherheitstagung.

Sie finden uns auch alle zwei Jahre auf der weltgrößten Sicherheitsmesse „Security“ in Essen. Mit einem eigenen Stand präsentieren dort die Verfassungsschutzbehörden des Bundes und der Länder ihre Security Awareness-Angebote und informieren u.a. über die Risiken der Wirtschaftsspionage.

Meine Damen und Herren,

Wirtschaftsspionage ist vor allem eine Begleiterscheinung der globalisierten Wirtschaft und damit eine internationale Herausforderung.

Seit 2008 haben wir daher auch die internationale Kooperation mit Partnerdiensten verstärkt und ausgeweitet.

Ein Ergebnis ist beispielsweise eine gemeinsame Artikelserie des BfV mit dem belgischen und luxemburgischen Partnerdienst im Mitgliedermagazin der Auslandshandelskammer „Debelux“ in Brüssel. Als Ergänzung ist eine Security-Awareness Veranstaltung mit den Partnerdiensten für die Mitgliedsunternehmen von „Debelux“ geplant.

Herr Magister Martin Weiss vom österreichischen Bundesamt für Verfassungsschutz und Terrorismusabwehr (BVT) wird gleich ein weiteres Beispiel internationaler Kooperation vorstellen, auf das ich Ihre Aufmerksamkeit besonders lenken möchte.

Das BVT hat Anfang Mai gemeinsam mit der Fachhochschule Campus Wien ein Schulungsprojekt zur Weiterbildung von Mitarbeitern aus den Unternehmen zu „Beauftragten im Wirtschaftsschutz“ der österreichischen Öffentlichkeit vorgestellt.

Das Angebot zu einer Beteiligung an dem Projekt haben wir bereits frühzeitig gerne aufgegriffen und werden es im Rahmen unserer Möglichkeiten unterstützen.

Erfreulicherweise wird bei diesem Projekt auch die ASW ihre Expertise einbringen und die Einführung eines daraufhin abgestimmten Schulungsangebotes in Deutschland prüfen.

Die bereits erwähnten sog. Flyer mit verhaltens- und handlungsorientierten Sicherheitsempfehlungen hat sogar unser australischer Partnerdienst in einer englischen Version
–„Economic Security made in Germany“– auf seiner Homepage eingestellt.

Meine Damen und Herren,

Es vergeht kaum ein Tag, an dem die Medien nicht über das Thema „Cyber-Angriffe“ berichten. Elektronische Attacken, d.h. die Übermittlung von Schadsoftware via E-Mail, manipulierte IT-Hardware oder so genannte „Drive-by-Downloads“, sind ein reales Risiko für Wirtschaft, Forschung und Wissenschaft und auch für staatliche Stellen.

Auf Ministerien und Bundesbehörden werden jährlich mehr als 1.000 elektronische Spionageangriffe registriert. Aufgrund technischer Parameter und inhaltlicher Ausrichtung kann in ihrer Mehrzahl von staatlicher Steuerung ausgegangen werden.

Eine Übersicht zu elektronischer Spionage im Bereich der Wirtschaft existiert nicht. Wir müssen jedoch von einer hohen Dunkelziffer ausgehen, zumal die elektronische Vernetzung in der Wirtschaft und damit auch damit verbundene Angriffsmöglichkeiten weiter zunimmt.

Das Risiko besteht nicht nur in der Ausforschung z.B. technologischen Know-hows, sondern mitunter auch in der Sabotage von Produktionsprozessen und so genannter Kritischer Infrastrukturen.

Die von der Bundesregierung geplante Gesetzesinitiative zu einer Meldepflicht von Betreibern Kritischer Infrastrukturen ist meines Erachtens begrüßenswert.

Sie könnte ein wichtiges Element einer wirkungsvollen Kooperation von Staat und Unternehmen im Gemeinwohlinteresse sein.

Das BfV hat diese neuen Herausforderungen des elektronischen Zeitalters angenommen.Wir beteiligen uns aktiv an dem im Februar 2011 eingerichteten Nationalen Cyber-Abwehrzentrum.

Unter der Federführung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) wird durch diese Stelle die Analysefähigkeit der beteiligten Behörden verbessert und eine engere Koordination von Schutz- und Abwehrmaßnahmen gegen IT-Vorfälle sichergestellt.

Über die im Jahr 2012 gegründete „Allianz für Cybersicherheit“ werden verstärkt auch die Erfordernisse der deutschen Unternehmen in die Cybersicherheitsstrategie des Bundes einbezogen. Das BfV wird seine Aktivitäten in diesem Phänomenbereich künftig noch deutlich ausweiten.

Wir werden die Analysefähigkeit von Schadensfällen optimieren und ausbauen sowie die Prävention vor Angriffen auf IT- und Kommunikationstechnik analog der Security-Awareness im Know-how-Schutz intensivieren.

Aber auch hier gilt: Erfolg haben werden wir nur in einer funktionierenden Kooperation mit den Gefährdeten und Betroffenen.

Hierfür möchte ich auch heute nachdrücklich werben.

Erfolgreiche Prävention bedarf auch eines vertrauensvollen und beidseitigen Informationsflusses als Grundlage für eine möglichst zutreffende Einschätzung und Analyse des Risiko- und Schadenspotenzials.

Wirtschaftsschutz ist Teamwork!

Die ist kein Slogan, sondern unsere Handlungsmaxime. Als „der“ Dienstleister für Spionageabwehr in Deutschland sind wir ausgestattet mit jahrzehntelanger Erfahrung, umfassender Expertise und Kompetenz.

Demokratie schützen bedeutet auch die Wirtschaft schützen, denn eine funktionierende und prosperierende Wirtschaft ist unabdingbarer Stabilitätsfaktor eines demokratischen Gemeinwesens.

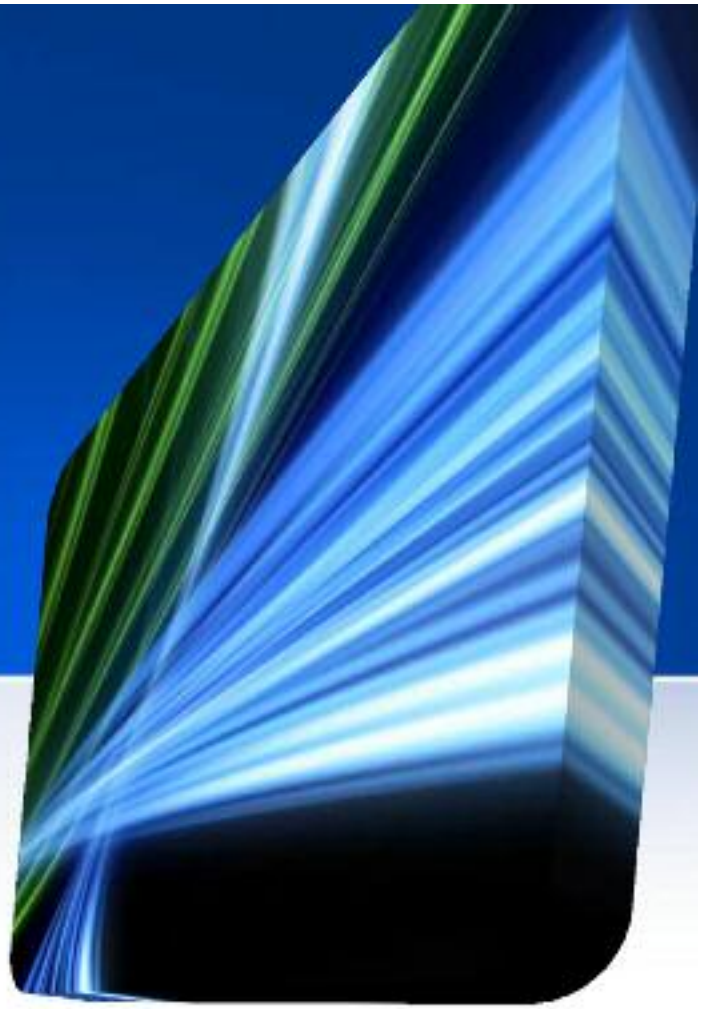
Wir wollen unseren Beitrag hierzu leisten. Auch künftig wird der Wirtschaftsschutz eine der Schwerpunktaufgaben des BfV sein.

Wirtschaftsschutz ist – wie gesagt – Teamwork, und deshalb freue ich mich ganz besonders, dass Sie so zahlreich zu der diesjährigen Sicherheitstagung erschienen sind.

Mein Dank gilt abschließend auch denen, die sich mit viel Engagement für die Organisation und die Durchführung dieser Tagung sowohl bei der ASW als auch in meinem Hause eingebracht haben.

Uns Allen wünsche ich eine gute und aufschlussreiche Veranstaltung!

Wirtschafts- und Industriespionage (WIS)

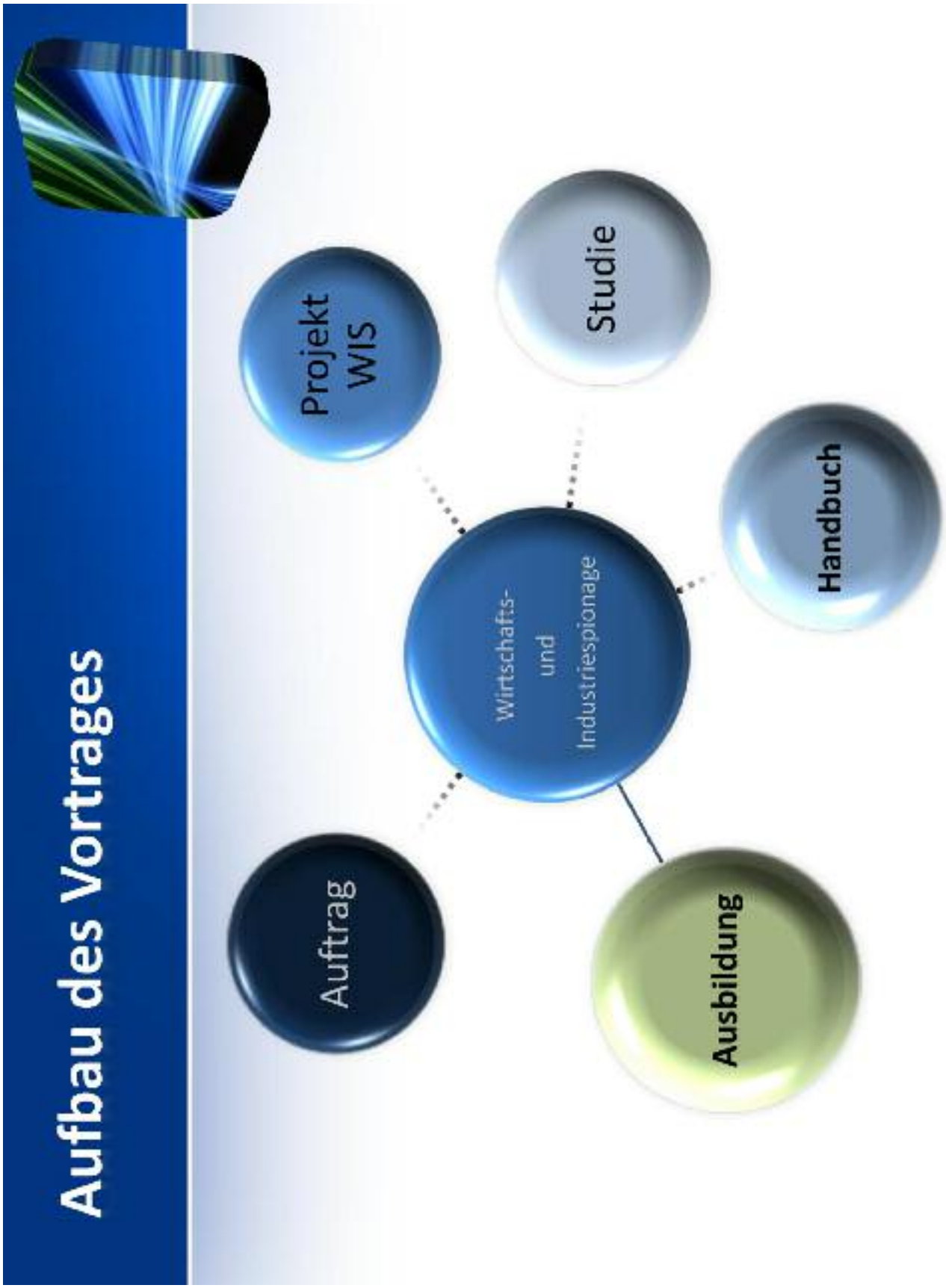


„Amateurs hack systems, professionals hack people“

Bruce Schneier (* 15. Januar 1963 in New York)
US-amerikanischer Experte für Kryptographie und Computersicherheit

Unterscheidung

Unterscheidungsmerkmal	Wirtschaftsspionage	Industriespionage
Herkunft des Angreifers	staatlich gelenkte Nachrichtendienste	Konkurrenzunternehmen
Ziel des Angriffs	Angriff erfolgt aufgrund nationalökonomischer Interessen gegen Wirtschafts- und Wissenschafts-unternehmen oder Industriebereiche anderer Länder und ist meist auf über einzelne Unternehmen hinausgehende Interessensgebiete gerichtet	Betriebs- und Geschäftsgeheimnisse zur Stärkung der Konkurrenzfähigkeit
Zeitliche Ausrichtung des Angriffs	ist oft auf langfristige Perspektiven (bis zu 20 Jahre) angelegt und darauf ausgerichtet, wirtschaftliche oder wissenschaftliche Defizite auf breiter Basis auszugleichen	konzentriert sich meist auf zeitlich absehbare wirtschaftliche Vorteile
Modus Operandi	langfristig angelegte, professionelle Durchführung; Einsatz von nachrichtendienstlichen Mittel; verdecktes Nutzen von MitarbeiterInnen	zeitlich absehbar, Einsatz von z.B. PrivatdetektivInnen, WissenshändlerInnen, OK usw.; Abwerben von MitarbeiterInnen
Folgen/Geschädigte	mittelbarer volkswirtschaftlicher Schaden, Schadenshöhe nur schwer abschätzbar	unmittelbarer wirtschaftlicher Schaden für Einzelunternehmen
Aufwand des Einsatzes	der betriebene Aufwand kann weit höher sein als dies rational erklärbar ist	der betriebene Aufwand steht meist in einem materiellen Verhältnis zu dem angestrebten Ziel


Aufbau des Vortrages
Projekt WIS
Studie
Auftrag
Wirtschafts- und Industriespionage
Handbuch
Ausbildung

WIS als sicherheitspolitische Herausforderung

Regierungsprogramm der XXIV. Gesetzgebungsperiode (Auszüge):

- Verstärkte Spionageabwehr und Spionageprävention

- Schaffung von Sicherheitspartnerschaften im Hinblick auf die weitere Professionalisierung der Präventionsarbeit

Projekt WIS

- Projekt des BM.I / .BVT
- mit FH Campus Wien - Fachbereich Risiko und Sicherheitsmanagement
- Industriellen Vereinigung
- Wirtschaftskammer Österreich

Studie

- **9200** Unternehmen zur Teilnahme eingeladen (Brief),
- Online-Fragenkatalog mit 23 Fragen
- Fragestellungen: Risiken, Indikatoren, Betroffenheit von WIS, Zusammenarbeit Wirtschaft -Sicherheitsbehörden
- 18.11.2010 Präsentation der Executive Summary

Studie vs. Dunkelfeld

Studie

Dunkelfeld

Handbuch

Kostenlos bestellbar – www.wko.at

- 13.09.2011 Präsentation des Handbuches
- Begriffsklärungen
- Kompass zum sicheren Unternehmen
- Handlungsempfehlungen
- Praxisbeispiel
- Verdachtsmomente – Was ist zu tun
- Literaturempfehlungen

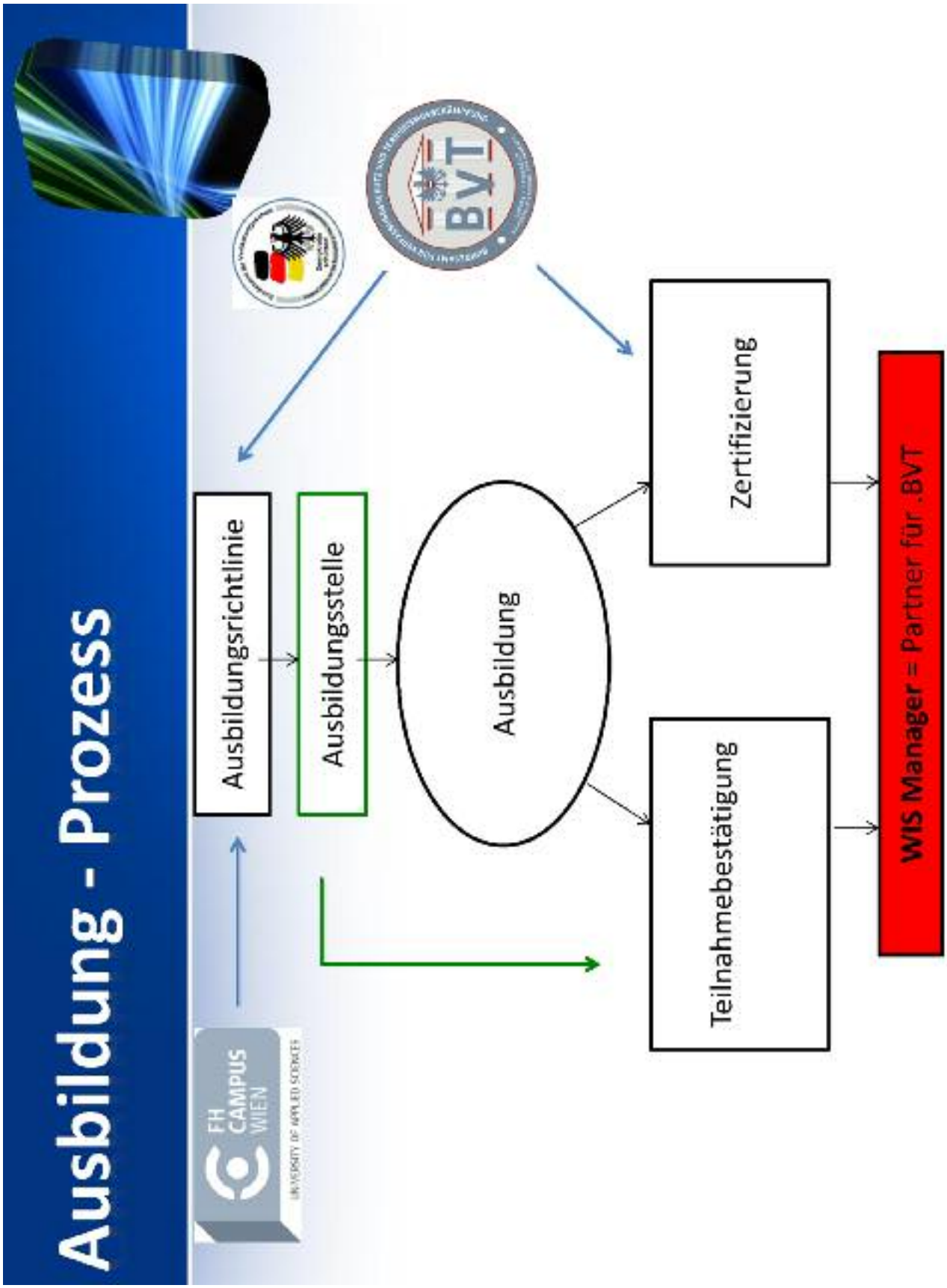
Was ist der Unterschied zwischen…?

Abfallmanagement

Wirtschaftsschutz

Beauftragten = Verantwortung

Ziel
WIS Manager
Wirkung für
Wirtschaft
& Staat
Verantwortung


Ausbildung - Prozess
FH CAMPUS WIEN
BVT
Ausbildungsrichtlinie
Ausbildungsstelle
Ausbildung
Zertifizierung
Teilnahmebestätigung
WIS Manager = Partner für .BVT

Ausbildung

	Modulblock 1			Modulblock 2	
	Tag 1	Tag 2	Tag 3	Tag 1	Tag 2
Lehreinheit 1 - 2	Wirtschafts- & Industriespionage – Einführung	Grundlagen Wirtschaftsschutz	Grundlagen "Erstellung eines Sicherheitskonzepts"	Wirtschaftsschutz als integrierter Ansatz	Grundlagen "Vorfallsbehandlung"
Lehreinheit 3 - 4	TäterInnen und Angriffsmuster	Grundlagen "Bedrohungs- und Risikoanalyse"	Grundlagen "Erstellung eines Sicherheitskonzepts"	Wirtschaftsschutz als integrierter Ansatz	Fallstudie "Vorfallsbehandlung"
Mittags-pause					
Lehreinheit 5 - 6	TäterInnen und Angriffsmuster	Fallstudie "Bedrohungs- und Risikoanalyse"	Fallstudie "Erstellung eines Sicherheitskonzepts"	Know-how Implementierung: Gründe für das Scheitern in der Realität	Fallstudie "Vorfallsbehandlung"
Lehreinheit 7 - 8	Vorschriften, Standards, Gesetze, Zuständigkeiten	Fallstudie "Bedrohungs- und Risikoanalyse"	Fallstudie "Erstellung eines Sicherheitskonzepts"	Know-how Implementierung: Gründe für das Scheitern in der Realität	Zusammenfassung und Diskussion
Abendveranstaltung				Kamingespräch Direktor BVT	
Motto des Tages	Blick nach außen	Das System/ Prozess – Teil 1	Das System/ Prozess – Teil 2	Know-how Praxis und Implementierung	Was tun im Anlassfall

Kompetenzerwerb - Tag 1
„Blick nach Außen“

- kennen der Begrifflichkeiten und Unterschiede in der Terminologie von Wirtschafts- und Industriespionage
- kennen der AkteurInnen und deren grundlegenden Angriffsmuster (modus operandi) im Bereich Wirtschafts- und Industriespionage
- kennen der Vorschriften und Standards für die Klassifizierung im nationalen und internationalen Umfeld
- kennen der Rechtsvorschriften für Wirtschafts- und Industriespionage auf nationaler und internationaler Ebene sowie der Zuständigkeiten der Behörden und sonstiger auf diesem Gebiet tätigen Institutionen
- kennen der Möglichkeiten für die Überprüfung von Personensicherheit und die Anforderungen an den materiellen Geheimschutz sowie physische Sicherheit

Kompetenzerwerb - Tag 2
„Das System/ Prozess – Teil 1“

- können Gefahren aus Wirtschafts- und Industriespionage für die Organisation identifizieren, analysieren, bewerten und geeignete Maßnahmen ableiten

- können in Organisationen angemessene Sicherheitsmaßnahmen entwickeln und den Sinn und die Notwendigkeit für die Maßnahmen im Bereich Wirtschafts- und Industriespionage vermitteln

- kennen der Schnittstellen zu verwandten Bereichen (Informationssicherheit, Objektschutz, etc.) und können Synergien nutzen

Kompetenzerwerb - Tag 3
„Das System/ Prozess – Teil 2“

- können strategische und operative Ziele für den Schutz vor Wirtschafts- und Industriespionage in der Organisation festlegen

- können in Organisationen angemessene Sicherheitsmaßnahmen entwickeln und den Sinn und die Notwendigkeit für die Maßnahmen im Bereich Wirtschafts- und Industriespionage vermitteln

Kompetenzerwerb - Tag 4

„Know-how Praxis und Implementierung“

- kennen der Schnittstellen zu verwandten Bereichen (Informationssicherheit, Objektschutz, etc.) und Synergien nutzen
- kennen der Grundzüge der Human Factor Theories und deren Auswirkungen auf Wirtschafts- und Industriespionage (z.B. Social Engineering)
- können Komplexität managen und die unterschiedlichen Bedürfnisse der verschiedenen Stakeholder vereinen
- können das Management in Fragen zu Wirtschafts- und Industriespionage beraten
- können die Personalabteilung oder die HR-Verantwortlichen in Wirtschafts- und Industriespionage relevanten Fragen aktiv unterstützen
- können ein angemessenes Reportingsystem aufbauen
- können die Umsetzung der Ziele und Maßnahmen auditieren und Maßnahmen für die Verbesserung festlegen
- können Konzepte für Sensibilisierungsmaßnahmen, Schulungen und Trainings erstellen und diese umsetzen

Kompetenzerwerb - Tag 5
„Was tun im Anlassfall“

- können relevante Vorfälle in Bezug auf Wirtschafts- und Industriespionage methodisch betrachten und die notwendigen weiteren Schritte mittels angepasster Handhabungen einleiten und begleiten

Panta rhei
DANKE
für die
Aufmerksamkeit

Bundesamt für Verfassungsschutz

7. Sicherheitstagung des BfV und der ASW am 27. Juni 2013 in Berlin

„Linksextremismus und seine Auswirkungen auf die Wirtschaft“

Vortrag von Guido Selzner, RGL im BfV

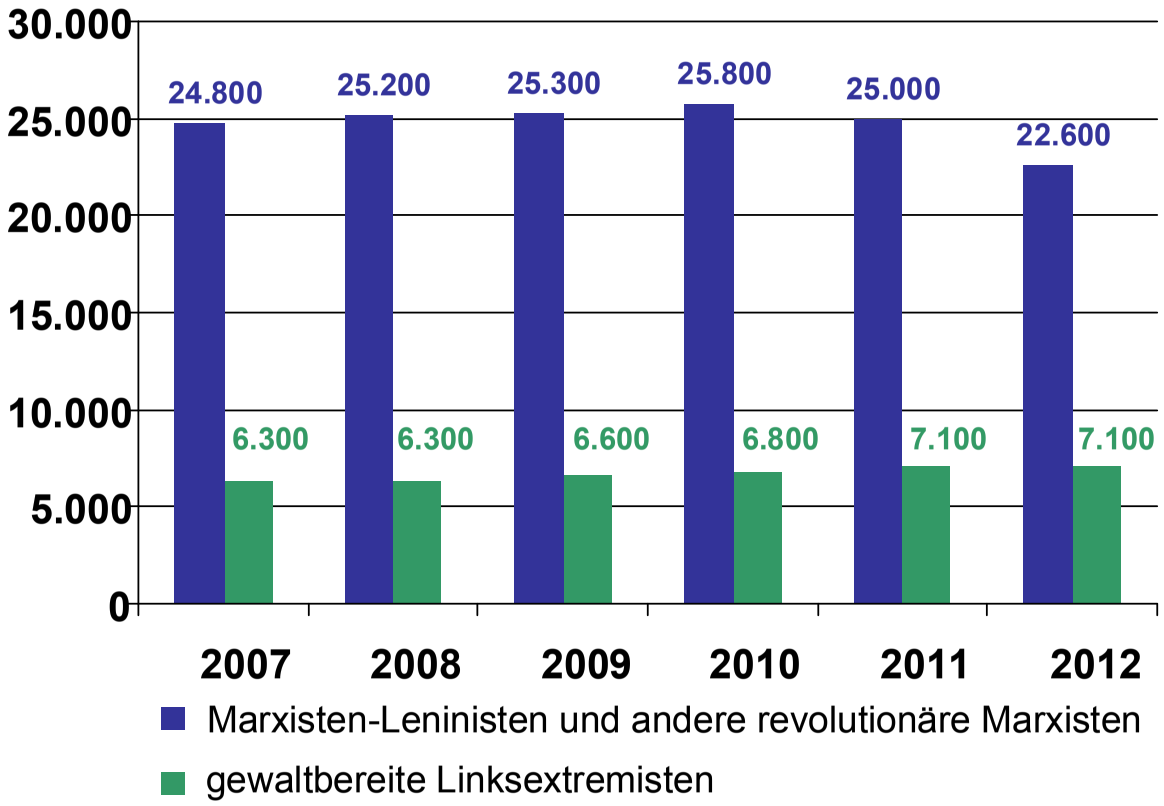
Bundesamt für Verfassungsschutz

Lagedarstellung

- Seit den Protesten gegen den NATO-Gipfel 2009 in Straßburg gesteigerte Militanzbereitschaft feststellbar
  - erhöhte Aggressivität bei Protesten/Demonstrationen
  - anhaltend hohes Aggressionsniveau gegenüber Rechtsextemisten
  - hohe Gewaltbereitschaft gegen „Vertreter des Repressions-apparates“
  - über die Jahre hohe Anzahl der Straf- und Gewalttaten sowie leichter Anstieg des gewalttätigen Personenpotenzials
- Schwerpunkte linksextremistischer Agitation und Aktion
  - Antifaschismus
  - Antimilitarismus
  - Antirepression
  - Freiräume/Gentrifizierung

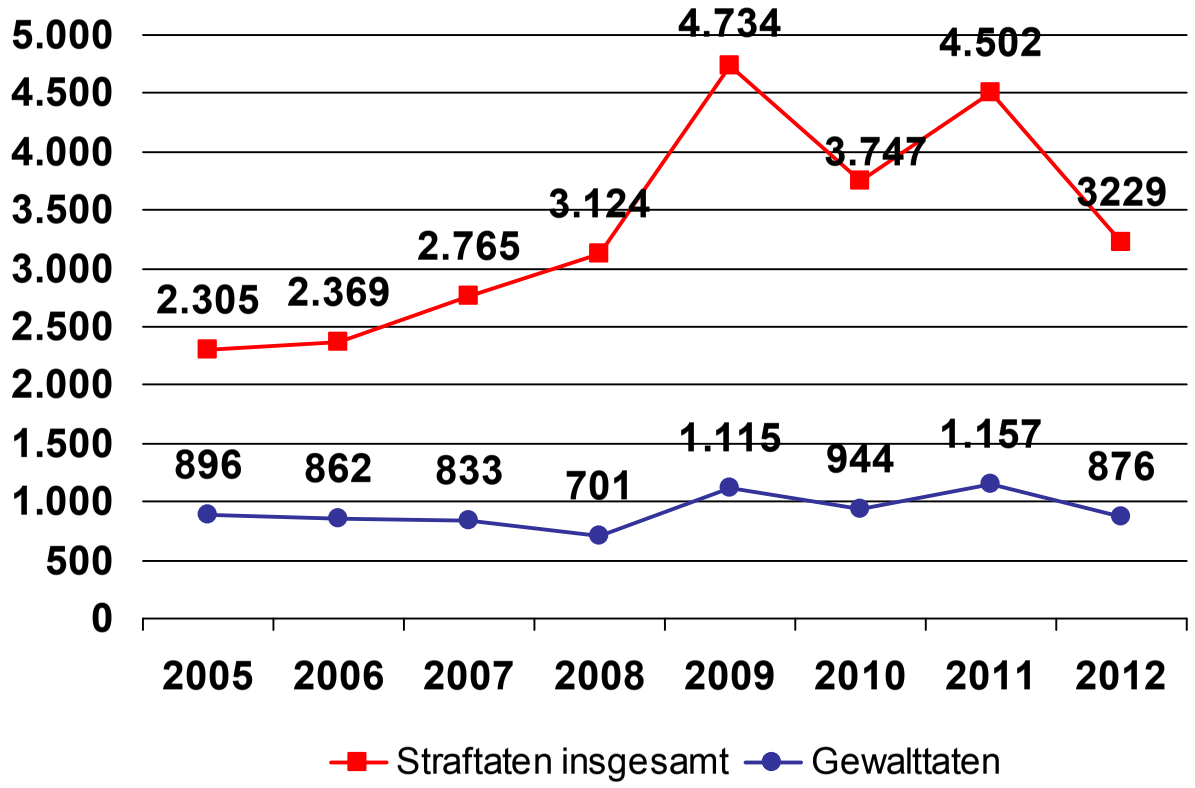
Bundesamt für Verfassungsschutz

Linksextremismuspotenzial



Bundesamt für Verfassungsschutz

Linksextremistische Straf- und Gewalttaten seit 2005



Bundesamt für Verfassungsschutz

Wirtschaftsunternehmen im Visier

- Wirtschaftsunternehmen (WU) sind Teil des kapitalistischen Systems
- WU tragen Mitverantwortung für angebliche soziale und politische Missstände
- Vorwurf: zur Gewinnmaximierung und zur Sicherung ihres politischen und wirtschaftlichen Einflusses beuten WU Mensch und Natur aus

Bundesamt für Verfassungsschutz

Gefährdete Wirtschaftsbereiche

- Unterstützer des **„Faschismus“**
- „Profiteure“ der **Asylpolitik**
- „Profiteure“ des **Sozialabbaus**
- „Profiteure“ der **Globalisierung/Finanzkrise**
- **Rüstungsbetriebe** und deren Zulieferer
- Akteure im Bereich **„Repression“/Überwachung**
- An Projekten zur **„Umstrukturierung“** beteiligte Unternehmen
- Im **„Atomgeschäft“** tätige Unternehmen
- Im Bereich der **Bio- und Gentechnologie** tätige Unternehmen und Einrichtungen

Antimilitaristische Kampagne „Krieg beginnt hier“

- Ende Juni 2011 initiiert als Fortsetzung/ Erweiterung der DHL-Kampagne
- Losung: „Kriegstreiberei und Militarisierung markieren, blockieren, sabotieren!“

„ielfältiger iderstand bedeutet markieren blockieren sabotieren rieg wird nur aufgehalten wo erdacht geplant und koordiniert wird im erzen der Bestie *Was wir hier sabotieren, kann woanders keinen Schaden anrichten*“ aterklärung Brandanschlag Bw-Fuhrpark anno uni

- Proteste gegen Bw-Veranstaltungen (Schulen, Job-Center)
- (Brand-)Anschläge auf Einrichtungen/Kfz von Bw sowie Rüstungsunternehmen und Dienstleister („Profiteure“)
- Erstmals 2012: War starts here-Camp am Gefechtsübungszentrum (GÜZ) der Bundeswehr in der Altmark (ST)

Antimilitaristische Kampagne „Krieg beginnt hier“

Bundesamt für Verfassungsschutz

Antimilitaristische Kampagne „Krieg beginnt hier“

- 30. Mai 2013, Bremen: BA Telekom-Kfz, SB Siemens-Kfz
- 23. Mai 2013, Celle: Farbanschlag Veranstaltungszentrum Congress Union
- 13. Mai 2013, München: Farbanschlag Vereinshaus Kameradenkreis der Gebirgsjäger
- 7. Oktober 2012, Altmark: Sabotage am Gleisanschluss GÜZ
- 17. September 2012, Berlin: Farbanschlag Boeing-Niederlassung
- 14. September 2012, Berlin: BA DB-Kfz
- 20. August bis 1. September 2012, Hamburg: BA Wärtsilä-Kfz (6 Fz), SB Siemens-Kfz, Farbanschlag Wohnhäuser Vorstand Euler-Hermes sowie div. Politiker
- 28. August 2012, Kiel: BA Imtech-Kfz (2 Fz), Farbanschlag Imtech-Niederlassung

Bundesamt für Verfassungsschutz

Antimilitaristische Kampagne „Krieg beginnt hier“

- 27. August 2012, Berlin: BA DB-Kfz, THW-Kfz; Steinwürfe und Farbe gegen Imtech-Niederlassung und SFB 700 der FU Berlin
- 26. Juli 2012, Berlin: BA Imtech-Kfz (2 Fz)
- 6. Juni 2012, Hannover: BA Bw-Fuhrpark (13 Fz)
- 9. April 2012, Bonn: Farbanschlag Mönch-Verlag
- 1. April 2012, Hamburg: BA Kfz Vorstand Blohm & Voss und Gebäude Muelhan AG; Farbanschlag Niederlassung Northrop-Grumman
- 30. Januar 2012, Bonn: Farbanschlag Deutsche Gesellschaft für Wehrtechnik
- 11. November 2011, Wuppertal: BA Siemens-Kfz
- 6. November 2011, Trittau: BA Rheinmetall-Niederlassung
- 5. September 2011, Hamburg: BA Niederlassung Rolls Royce Marine Deutschland GmbH

Bundesamt für Verfassungsschutz

Antimilitaristische Kampagne „Krieg beginnt hier“

Celle, 20. Mai 2013


Altmark, 7. Oktober 2012


Hannover, 6. Juni 2012


Hamburg, 30. August 2012

Antimilitaristische Kampagne „Krieg beginnt hier“

Bundesamt für Verfassungsschutz

Militante Kampagne gegen die Dt. Telekom AG

- DTAG zuletzt verstärkt im Fokus gewaltbereiter Linksextremisten
  - als Profiteur der weltweiten Wirtschaftskrise
  - als Vorreiter einer lückenlosen Überwachung
  - als bedeutender Akteur in der zivil-militärischen Zusammenarbeit

- „Arbeitsgruppe T.Error“ thematisiert Ende Februar 2013 eine mgl. „militante antikapitalistische Kampagne“ gegen die DTAG:

„ eben einem riesigen *Fuhrpark Dependancen* in nahezu eder Stadt der BR und ihren erbeständen in den u gängerzonen besitzt der onzern ein weitläufiges schwer zu schützendes *Netz an Kabeln und Leitungen* kreuz und uer durch die Republik sowie etliche *Funk-* und *Sendemasten* die irgendwo unbewacht in der ampa stehen.“

t „ - connecting people“

Militante Kampagne gegen die Dt. Telekom AG

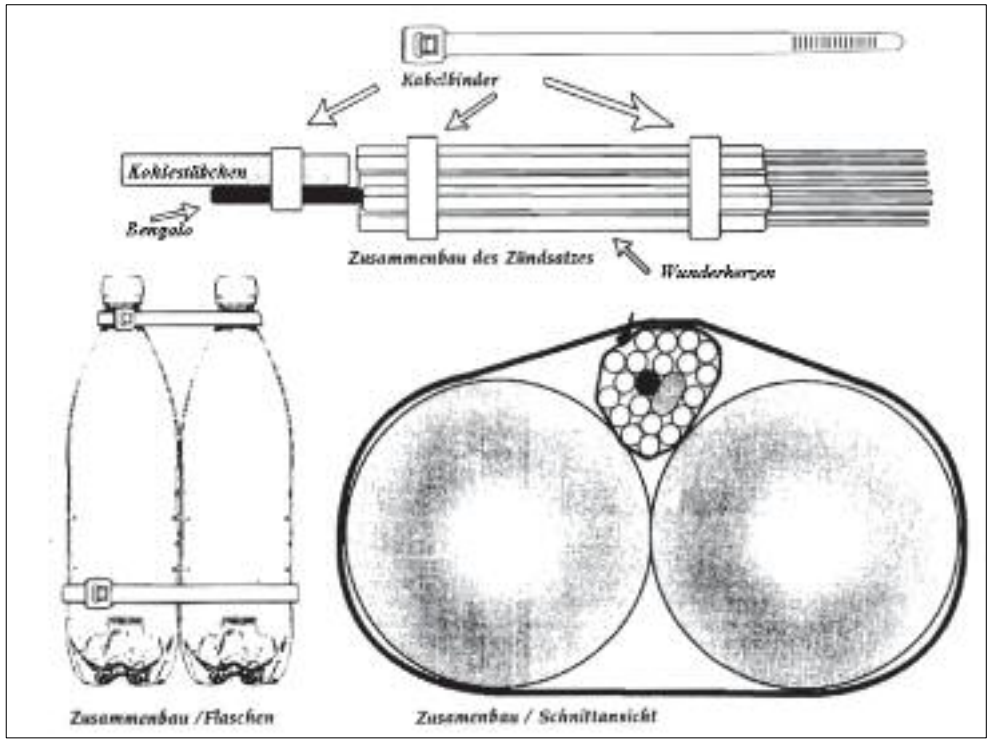
Militante Kampagne gegen die Dt. Telekom AG

- überwiegend Brandanschläge auf Fahrzeuge sowie Sachbeschädigungen an Einrichtungen
  - 11. Juni 2013, München: Brandanschlag Telekom-Kfz (1 Fz)
  - 1. Juni 2013, Frankfurt: Scheibeneinwürfe Telekom-Vertretung
  - 30. Mai 2013, Bremen: Brandanschlag Telekom-Kfz (1 Fz)
  - 27. April 2013, Hamburg: Farbanschlag Gebäude T-Systems
  - 15. März 2013, Berlin: Brandanschlag Telekom-Kfz (2 Fz)
  - 4. Januar 2013, Berlin: Brandanschlag Telekom-Kfz (1 Fz)
  - 23. Mai 2012, München: Brandanschlag Telekom-Kfz (2 Fz)
  - 3. Mai 2012, Hamburg: Brandanschlag Telekom-Kfz (7 Fz)
  - 8. April 2012, Berlin: Brandanschlag Telekom-Kfz (15 Fz)
  - 3. Oktober 2011, Berlin: Brandanschlag Telekom-Kfz (6 Fz)

Bundesamt für Verfassungsschutz

Militante Kampagne gegen die Dt. Telekom AG

Militante Kampagne gegen die Dt. Telekom AG



zündzeitverzögerter Brandsatz, Bauanleitung aus Szenezeitschrift „Interim“

Berlin, 3. Oktober 2011, nicht umgesetzter Brandsatz

Bundesamt für Verfassungsschutz

Empfehlungen: Was können Sie selbst tun?

- Beobachtung einschlägiger Internetseiten wie
  - http://linksunten.indymedia.org/
  - http://de.indymedia.org/
  - https://directactionde.ucrony.net/de/
  - http://antimilitarismus.blogsport.de/
  - http://www.bundeswehr-wegtreten.org/
- Erhöhte Sensibilität bei Veranstaltungen/Kampagnen, bei denen auch WU im Fokus linksextremistischer Agitation stehen
  - **„Überwachung“/„Repression“:** Innenministerkonferenzen, „Europäischer Polizeikongress“ in Berlin, SiKo in München
  - **Finanzkrise:** Krisenproteste wie Blockupy Frankfurt, „Krisendemos“, Griechenland-Solidaritätsaktionen
  - **wiederkehrende Anlässe:** „Revolutionärer 1. Mai“, Hamburger „Schanzenfest“, „Antikriegstag“ am 1. September, 3. Oktober

Bewertung und Ausblick (1)

- Wirtschaftsunternehmen weiterhin im Zielspektrum gewaltbereiter Linksextremisten

- Zieleingrenzung kaum möglich - Bsp. Rewe
  - Vorwürfe: Werbeaktion „Unser Deutschland“ fördert Nationalismus und Deutschtümelei und verharmlost den Nationalsozialismus
  - Boykott-Aufruf von Mitte April 2013

Wir haben keinen Bock auf Nationalismus und Deutschlandwahn, denn Deutschland denken heißt immer noch Auschwitz denken!
Boykottiert die gesamte „Rewe-Group“ solange die Werbeaktion dauert und bekämpft die drei schwarz-rot-gold-stinkenden Supermarktketten auf kreative Art und Weise!!!

ANTIFASCHISTISCHE AKTION

NIE WIEDER DEUTSCHLAND

Bundesamt für Verfassungsschutz

Bewertung und Ausblick (2)

- Klandestin operierende Kleingruppen mit sachschaden-orientierter Zielrichtung

So werden sich viele Vorstöße vorerst darauf beschränken müssen, das Establishment mit militanten Aktionen kurzfristig zu erschrecken und unsere Vorstellungen von sozialer Befreiung indirekt zu vermitteln: durch den radikalen Bruch mit Reformismus und Legalismus, durch gezielte Angriffe, die Personenschäden grundsätzlich ausschließen, durch phantasievolle neue Aktionsformen ...

- Keine Anzeichen für den Übergang zu personenbezogenen Anschlägen oder Herausbildung terroristischer Strukturen
- Derzeit keine internationalen Großereignisse
  - ➔ Konzentration auf nationale/lokale Reizthemen; jedoch
  - ➔ Mobilisierung gegen G8-Gipfel 2015 in Deutschland beginnt

Ende des Vortrages

Vielen Dank für Ihre Aufmerksamkeit!

7. Sicherheitstagung BfV und ASW

POLIZEI Nordrhein-Westfalen Landeskriminalamt

bürgerorientiert · professionell · rechtsstaatlich

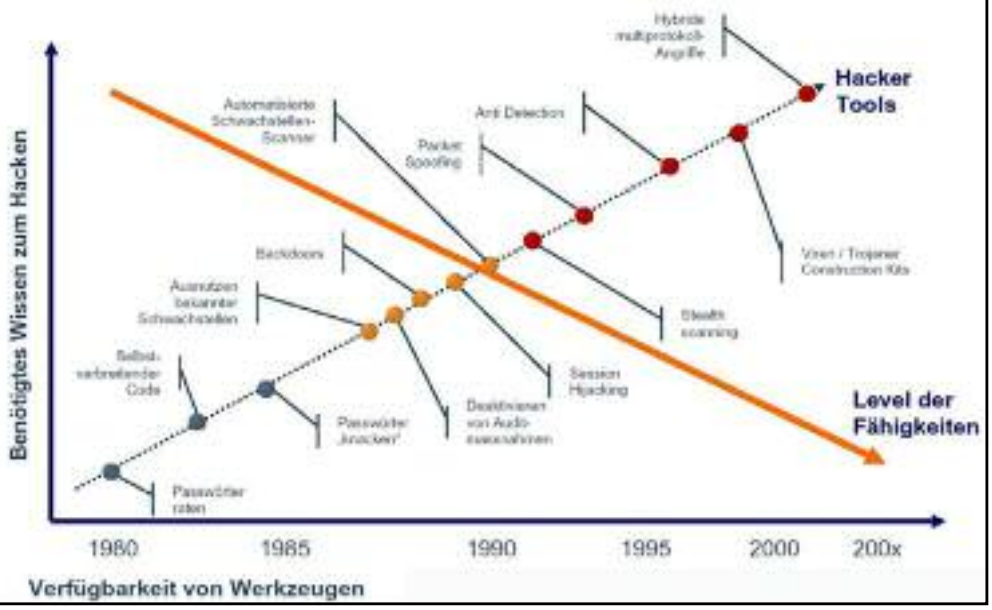
27. Juni 2013 Berlin

Die dunkle Seite des Internets

Stefan Becker
LKA NRW

Herausforderungen

POLIZEI Nordrhein-Westfalen Landeskriminalamt



Situation

POLIZEI Nordrhein-Westfalen Landeskriminalamt

Vinton Cerf

John Perry Barlow

3

Situation

POLIZEI Nordrhein-Westfalen Landeskriminalamt

Vinton G. Cerf is vice president and Chief Internet Evangelist for Google

„**Vint Cerf: Ein Viertel der Internet-PCs ist Mitglied eines Bot-Netzes**“

Of the 600 million computers currently on the internet, between 100 and 150 million were already part of these botnets

25. Januar 2007, World Economic Forum, Davos

4

Herausforderungen

POLIZEI Nordrhein-Westfalen Landeskriminalamt

"Regierungen der industriellen Welt, Ihr müden Giganten aus Fleisch und Stahl, ich komme aus dem Cyberspace, der neuen Heimat des Geistes.

Im Namen der Zukunft bitte ich Euch, Vertreter einer vergangenen Zeit: Lasst uns in Ruhe!

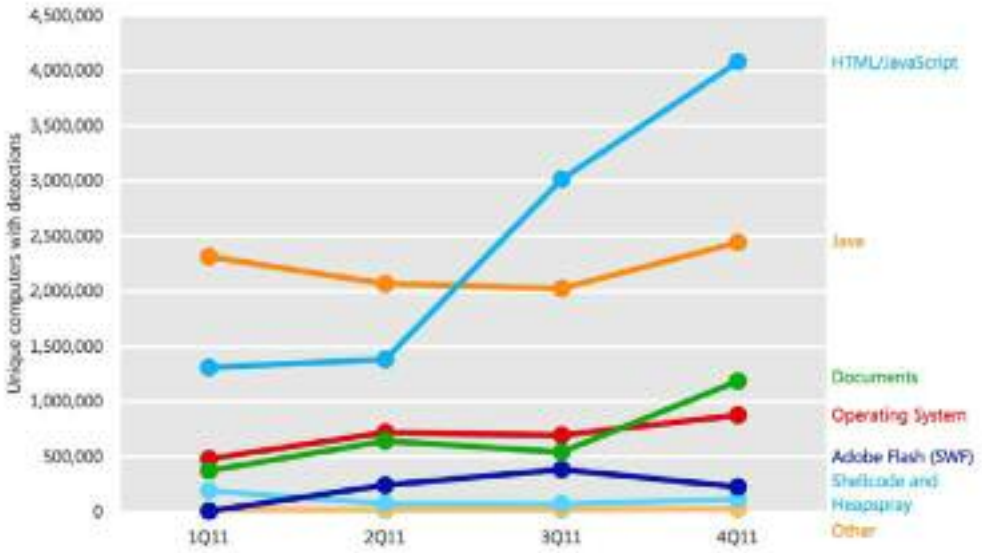
Ihr seid bei uns nicht willkommen.
Wo wir uns versammeln, besitzt Ihr keine Macht mehr."

John Perry Barlow 1996 - Aufruf für eine "neue Heimat des Geistes"
A Declaration of the Independence of Cyberspace / **Davos**
Zitat aus einem Forum im Zusammenhang mit den DDoS-Angriffen gegen „Wikileaks-Gegner“ im April 2011

Allgemeine Situation

POLIZEI Nordrhein-Westfalen Landeskriminalamt

Figure 14. Unique computers reporting exploits each quarter in 2011, by targeted platform or technology

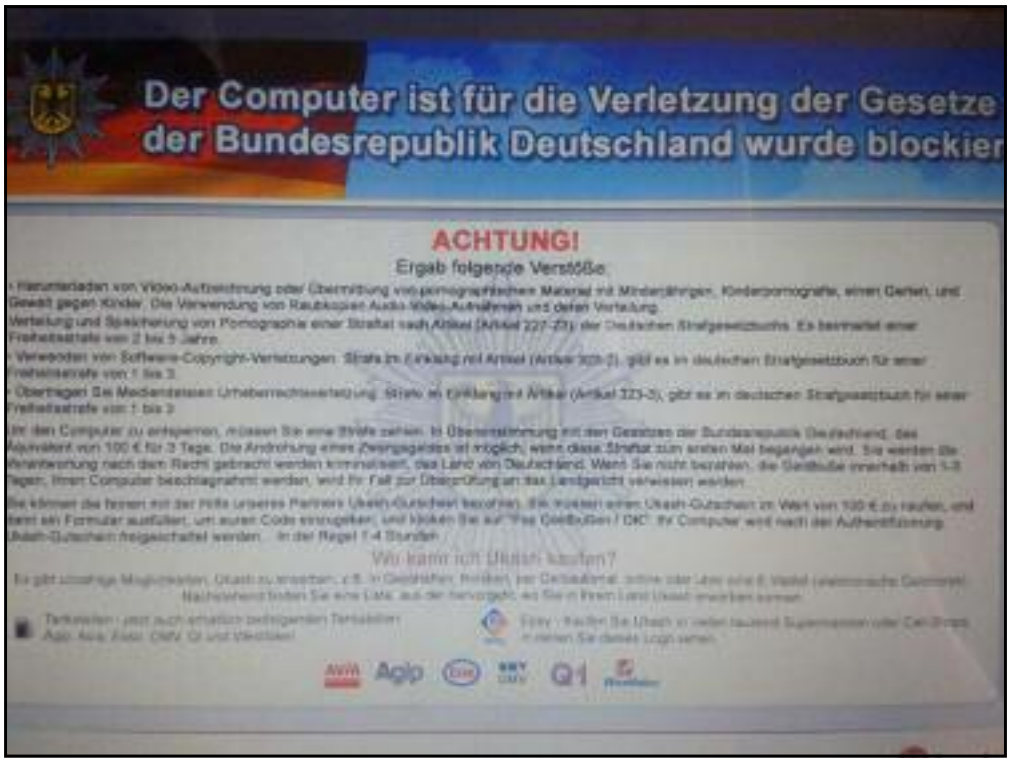


Microsoft Security Intelligence Report 12, Seite 43

Ermittlungen Beispiele

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

7



Beispiel Trojaner / Überweisung

POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

10 **Kompetenzzentrum Cybercrime**

Beispiel Trojaner / Überweisung

POLIZEI Nordrhein-Westfalen Landeskriminalamt

11 Kompetenzzentrum Cybercrime

Beispiele

POLIZEI Nordrhein-Westfalen Landeskriminalamt

Nortel

Cyberkriminelle haben seit 2000 Zugriff auf Rechner des mittlerweile zerschlagenen Netzwerkausrüsters gehabt. Erbeutet wurden unter anderem E-Mails, technische Aufzeichnungen und geschäftliche Daten. Das Unternehmen nahm die Angriffe lange Zeit nicht ernst.

http://www.nzz.ch/aktuell/digital/hacker-nortel-chi
1.15039857#)

12 Kompetenzzentrum Cybercrime

Beispiele

POLIZEI Nordrhein-Westfalen Landeskriminalamt

Polizei NRW
Webseite angegriffen, Server vom Netzgenommen

Sony
Einbruch in Server, 50.000 Dateien gestohlen, unveröffentlichte Stücke von M. Jackson

FBI, Scottland Yard
Mitschnitt einer Telefonkonferenz, veröffentlicht auf YouTube

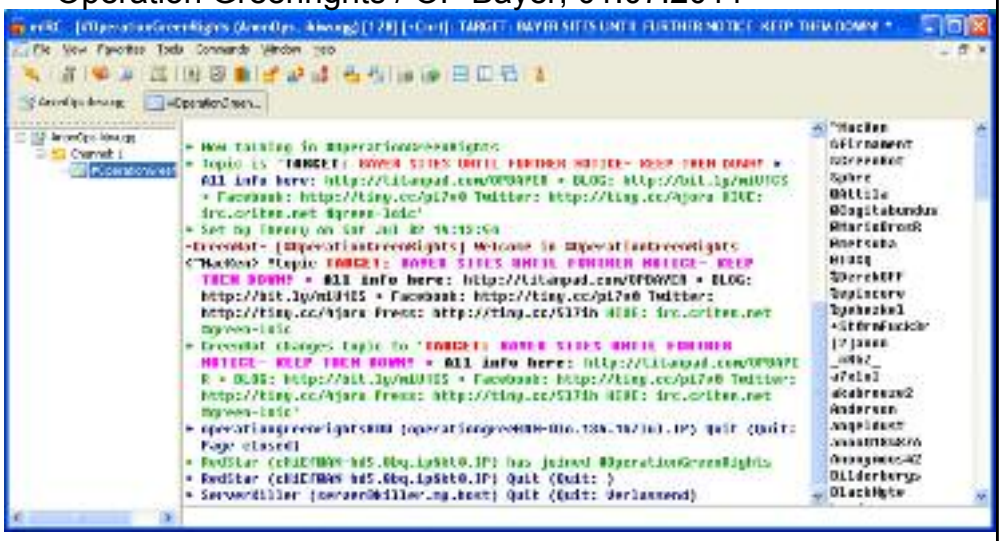
Symantec
Quelltext veröffentlicht

Infragard
Veröffentlichung von Accounts und Passwörtern

Microsoft Security Intelligence Report 12, Seite 66

POLIZEI Nordrhein-Westfalen Landeskriminalamt

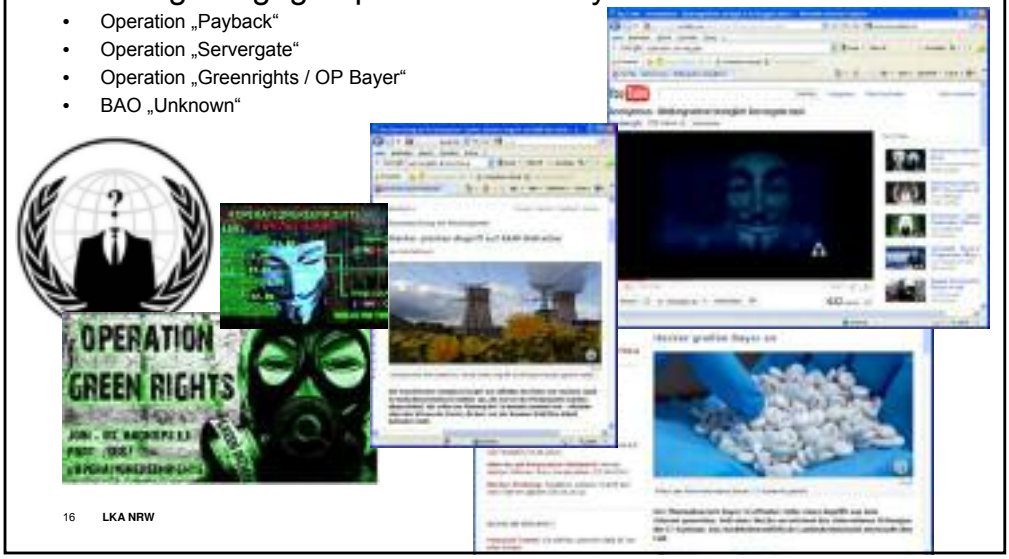
Operation Greenrights / OP Bayer, 01.07.2011



POLIZEI Nordrhein-Westfalen Landeskriminalamt

Ermittlungsverfahren des LKA NRW gegen „Anonymous“ und Angriffe gegen polizeiliche IT-Systeme

- Operation „Payback“
- Operation „Servergate“
- Operation „Greenrights / OP Bayer“
- BAO „Unknown“



16 LKA NRW

POLIZEI Nordrhein-Westfalen Landeskriminalamt

Beispiele OP Paypack

Steuerbefehl zum Angriff auf die Webseite api.paypal.com mittels der Software LOIC mit Angabe der IP Adresse des Absenders:

```
[Thu Dec 9 11:14:27 2010] - OVERRIDE:
root (root@72.9.153.142)
TOPIC #loic '!lazor default
targethost=api.paypal.com subsite=/
speed=3 threads=15 method=tcp wait=false
random=true checked=false
message=Good_night,_paypal_Sweet_dreams_from_AnonOPs
port=443 stop,
```

- **10.12. 23:50 Uhr**, Übermittlung der IP Adresse an das BKA.
  (11.12., 02:45 Uhr, Weiterleitung der Auswertungsergebnisse an das FBI.)

17

Herausforderung Computer Forensik

POLIZEI Nordrhein-Westfalen Landeskriminalamt

Verschlüsselung

Life Forensik

Netzwerk Forensik

Cloud Forensik

(große) Logfiles

Massendaten / Big Data

Mobile Forensik

Microsoft Security Intelligence Report 12, Seite 66

Kriminalitätsentwicklung 2011 → 2012

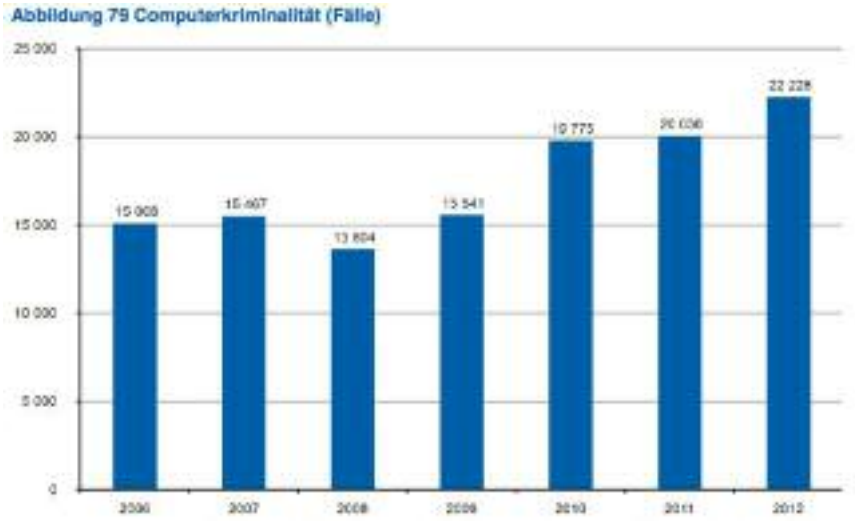
POLIZEI Nordrhein-Westfalen Landeskriminalamt

Tatmittel Internet	+	13,2 %
Ausspähen von Daten	+	74,9 %
Datenveränderung	+	174,9 %

Zahlen aus: Polizeiliche Kriminalstatistik NRW 2012

Entwicklung Computerkriminalität in NRW

POLIZEI Nordrhein-Westfalen Landeskriminalamt



Quelle: Polizeiliche Kriminalstatistik NRW / 2012
http://www.polizei.nrw.de/media/Dokumente/Behoerden/LKA/130225_KRIM_Entwicklung_NRW_2012.pdf

Antworten auf die Herausforderungen

POLIZEI Nordrhein-Westfalen Landeskriminalamt

OSINT / Open Source Recherche

Spezialisierung

Semantische Analyse von Daten

Kooperation

Hospitationen

Personal

Hardware

Innovation

Lagebild Cybercrime NRW 2012

POLIZEI Nordrhein-Westfalen Landeskriminalamt

http://www.polizei.nrw.de/media/Dokumente/Behoerden/LKA/Lagebild_Cybercrime__NRW_2012.pdf

22

POLIZEI Nordrhein-Westfalen Landeskriminalamt

http://www.polizei.nrw.de/media/Dokumente/Behoerden/LKA/Lagebild_Cybercrime__NRW_2012.pdf

Erreichbarkeit (24/7)

Single Point of Contact / SPoC
Email: cybercrime.lka@polizei.nrw.de
Telefon: 0211 939 4040

Stefan Becker, KHK

POLIZEI Nordrhein-Westfalen Landeskriminalamt

23

Advanced Persistent Threats

Fighting High-end Cyber-espionage Campaigns

Stefan Tanase
Senior Security Researcher
Global Research & Analysis Team

KASPERSKY lab

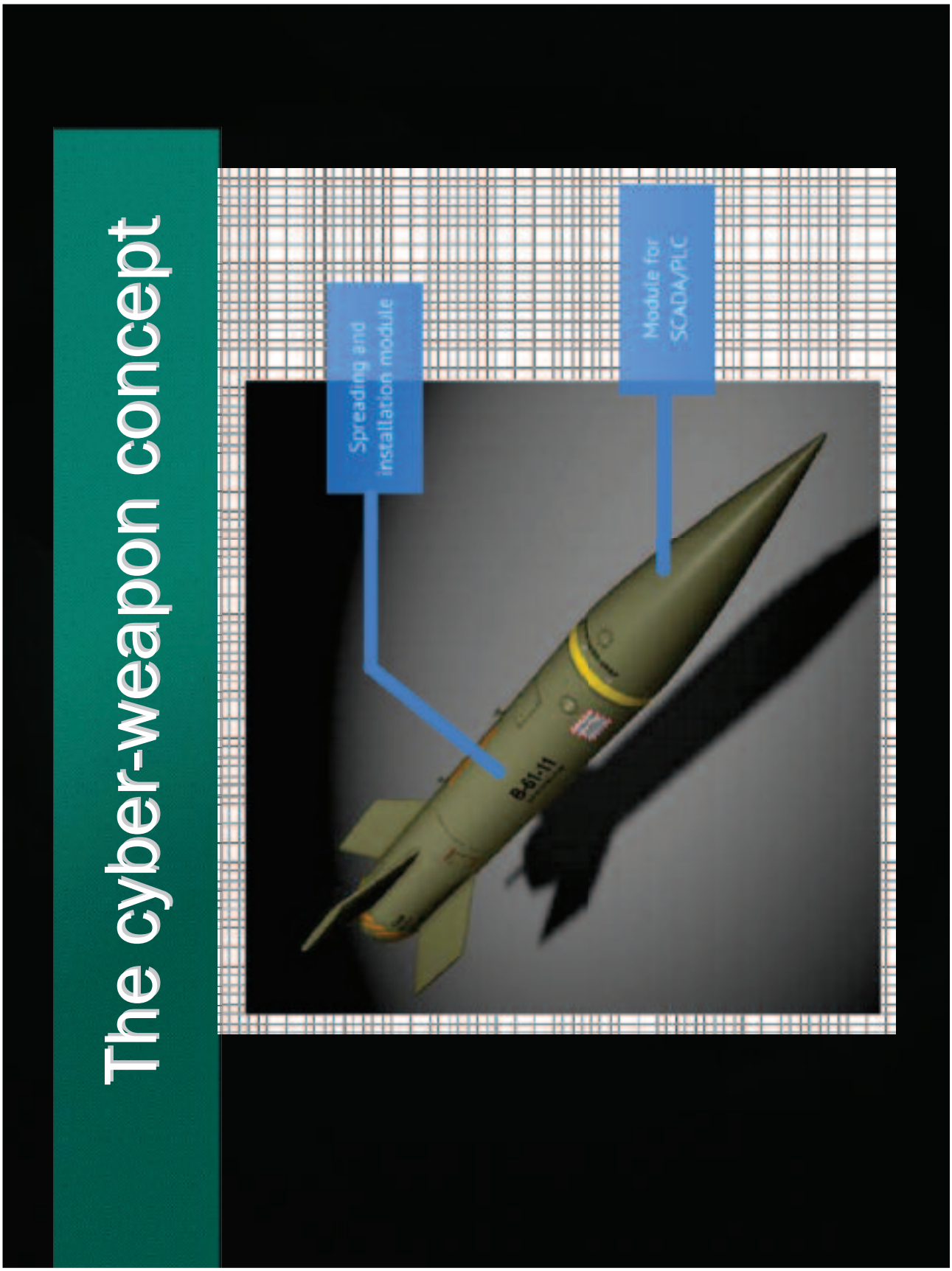
Cybercriminals ←→Money

Nation states are driven by something else.
Espionage. Sabotage. Cyberwar.


2009 – The Aurora Operation
Attacked: Google, Adobe, Juniper, Yahoo,
Morgan Stanley, Dow Chemical, etc...

What are we used to protect?


2010 – Stuxnet
First known Cyberweapon


The cyber-weapon concept
Spreading and installation module
Module for SCADA/PLC


2011 – Duqu
DUQU
Sophisticated. Stealthy. Elusive.
Nation state sponsored cyber-espionage.


2012 – Flame

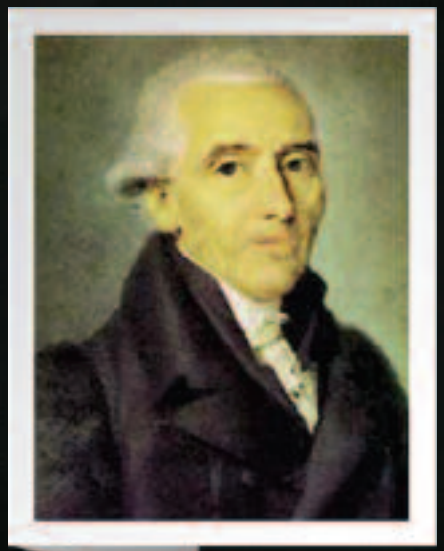

Where was Flame?
Iran
189
Israel
Palestine
98
Sudan
32
Syria
30
Lebanon
18
Saudi
Arabia
10
Egypt
5

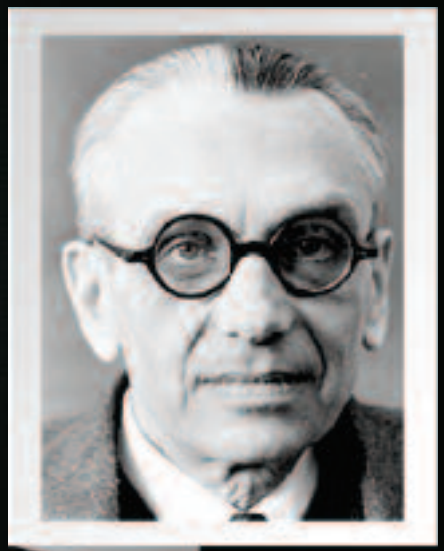
Flame re-cap

- Highly modular cyber-espionage toolkit
- Complex, big
- **Man-in-the-Middle attack against Windows Update**
- Many different modules
- The name “Flame” ->
- Discovered independently by Kaspersky Lab and CrySyS Lab in May 2012

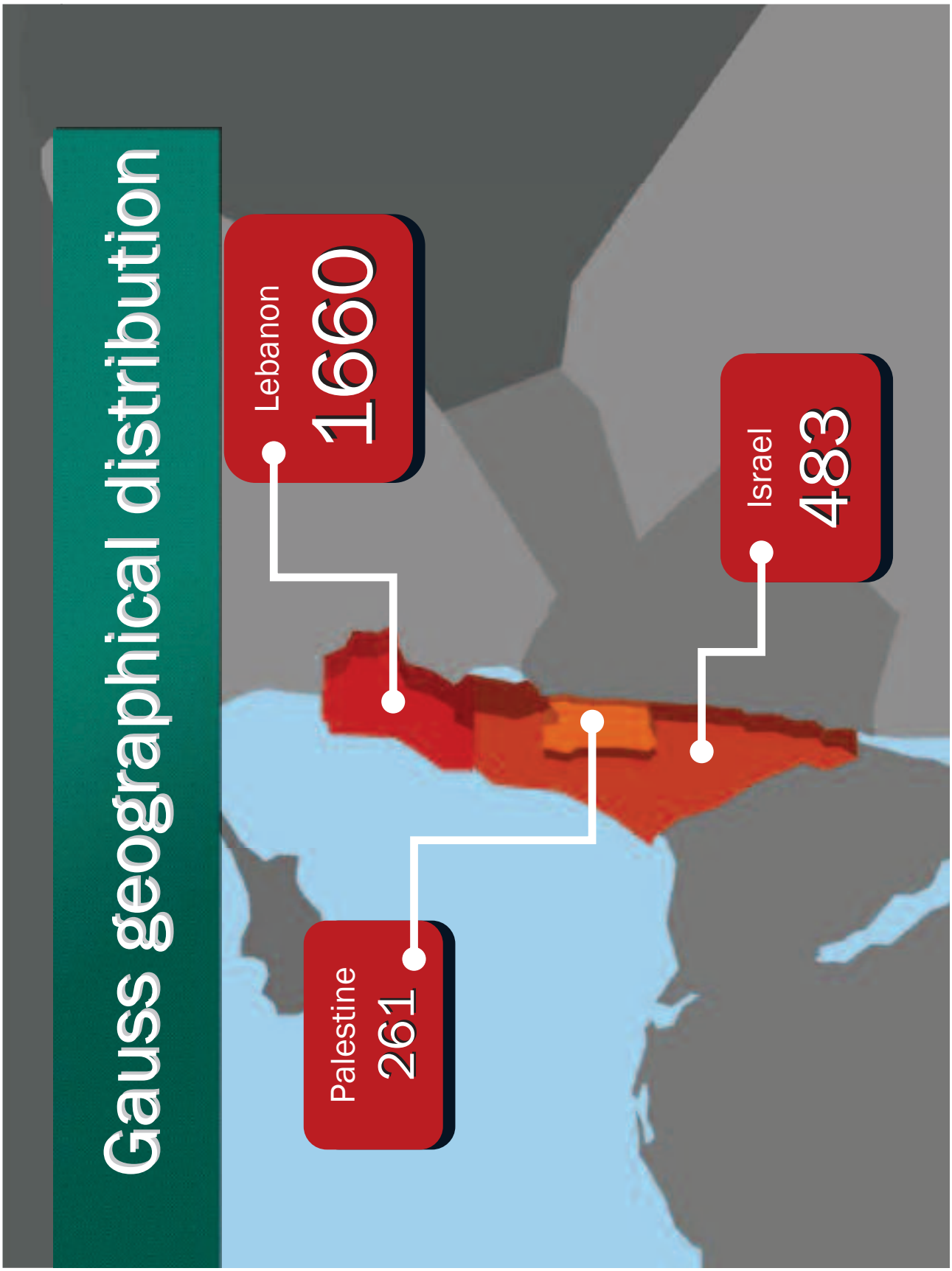
Flame represents the high-end of nation state sponsored cyber-espionage

2012 – Gauss



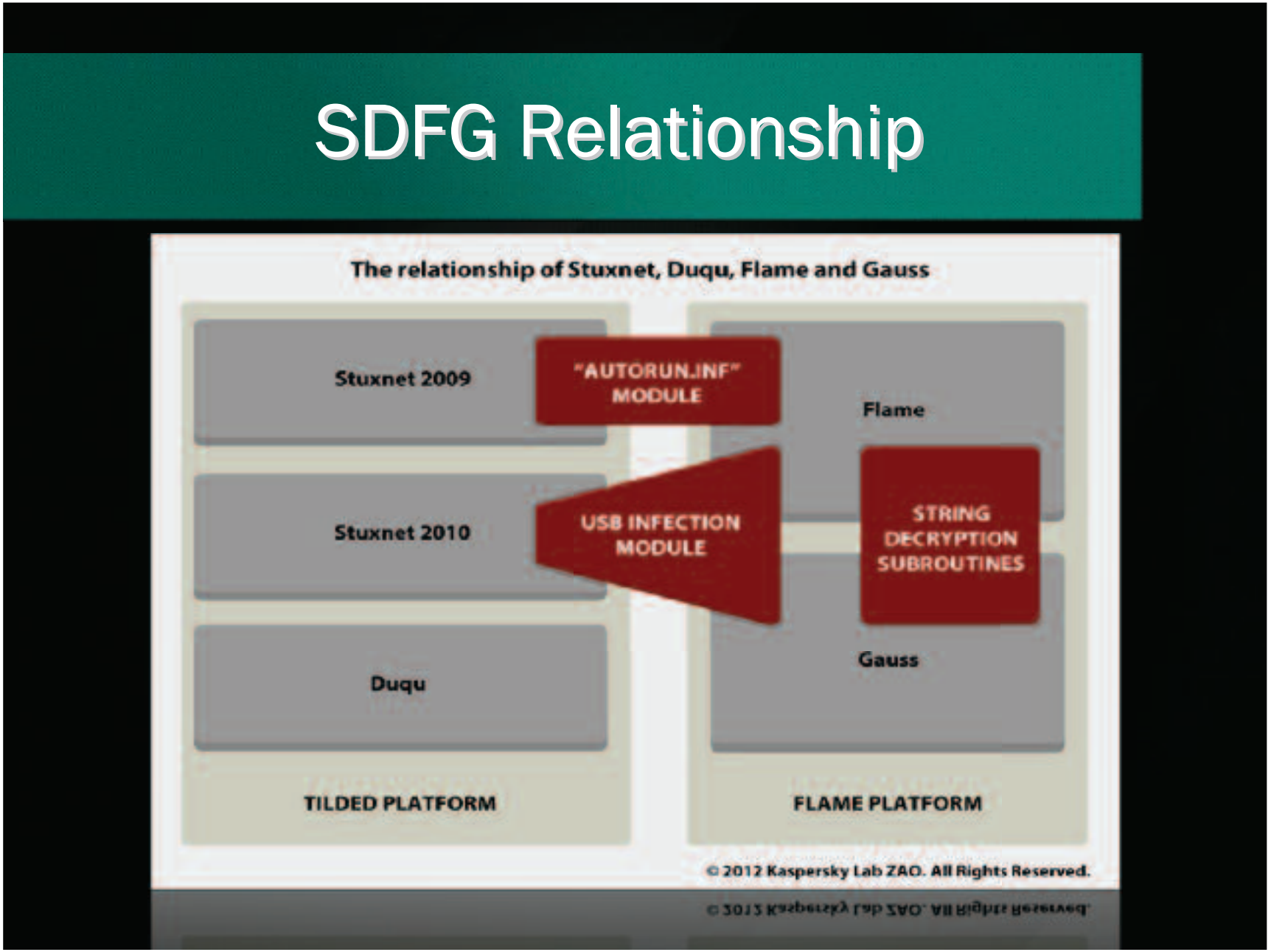


Purpose (payload): *Unknown*.


Gauss geographical distribution
Lebanon
1660
Israel
483
Palestine
261

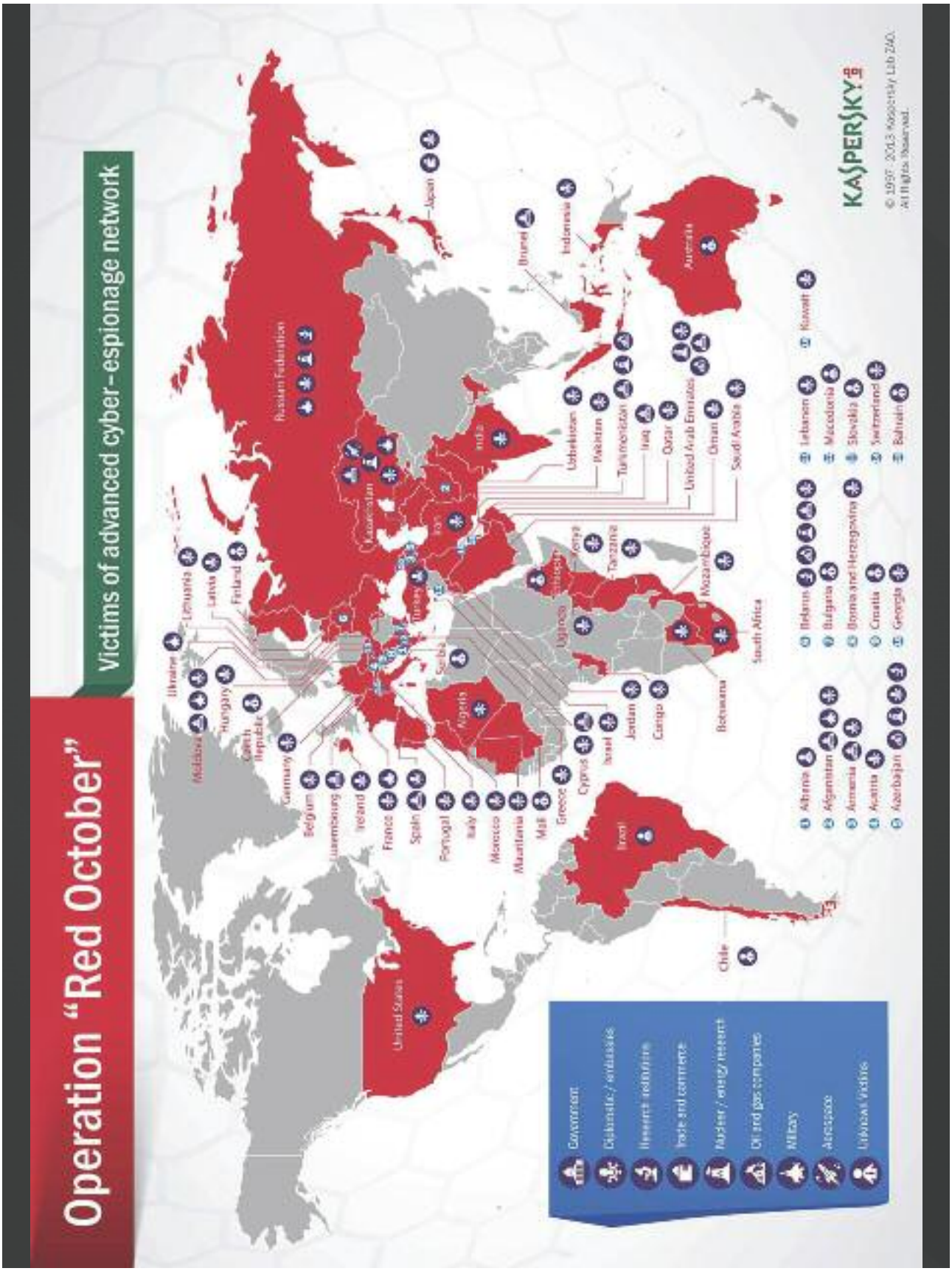
Targets of Gauss
FRANSABANK
BLOM BANK
BANQUE LIBANO-FRANÇAISE
A partner for your ambitions
BYBLOS BANK
Lebanon
CREDIT LIBANAIS
Bank of Beirut
citibank
PayPal

SDFG Relationship



2013 – Red October
THE HUNT FOR RED OCTOBER


October 2012
VIRUS
Source: KL customer in an EU country


Operation "Red October"
Victims of advanced cyber-espionage network
Government
Diplomatic / embassies
Research institutes
Trade and commerce
Nuclear / energy research
Oil and gas companies
Military
Aerospace
Unusual victims
KASPERSKY
© 1997 - 2013 Kaspersky Lab ZAO. All Rights Reserved.

File names used in attack

- Katyn_-_opinia_Rosjan.xls
- WORK PLAN (APRIL-JUNE 2011).xls
- EEAS-Staff New contact list (05-25-2011).xls
- tactlist_05-05-2011_.8634.xls
- EEAS New contact list (05-05-2011).xls
- Agenda Telefoane institutii si ministere 2011.xls
- FIEO contacts update.xls
- spisok sotrudnikov.xls
- List of shahids.xls
- Spravochnik.xls
- EEAS New contact list (05-05-2011) (2).xls

Diplomatic car for sale

MODEL: Mazda 323- 1998 **DISPLACEMENT:** 1800 cc

TRANSMISSION: Automatic **FUEL:** Benzin

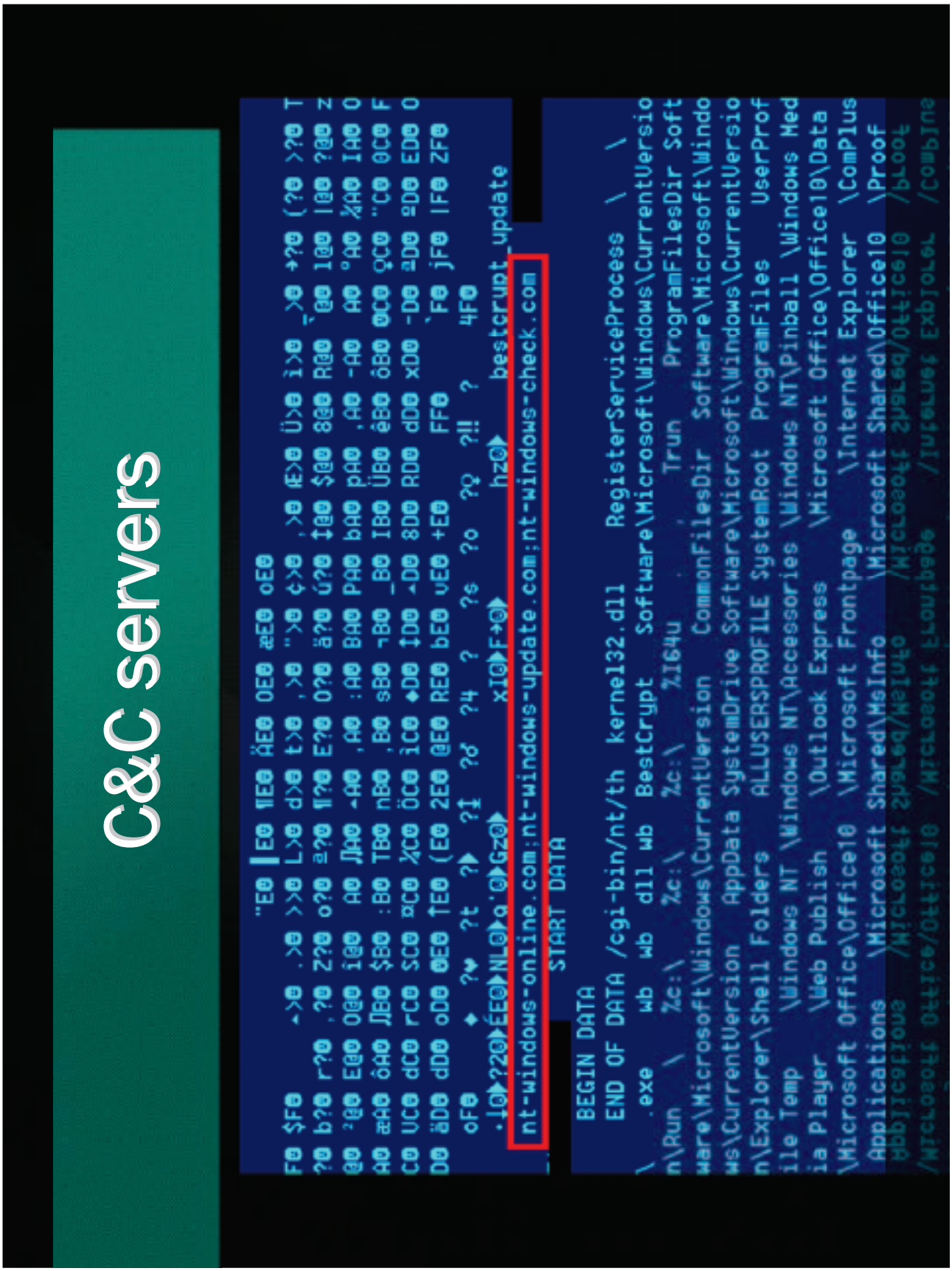
MILEAGE: 145.000 km

Power Steering – Electric Windows - AM/FM Stereo- Electric Mirrors - Air Conditioning - Remote central locking with Alarm - Extra snow tires.

PRICE: 2.700 $ (USD)

CONTACT: &&&&&&&& - &&&&&&&&&

THE CAR IS IN A VERY GOOD CONDITIONS


C&C servers
nt-windows-online.com;nt-windows-update.com;nt-windows-check.com
START DATA
BEGIN DATA
END OF DATA /cgi-bin/nt/th kernel32.dll RegisterServiceProcess
.exe wb wb dll wb BestCrypt Software\Microsoft\Windows\CurrentVersio
n\Run %c:\ %c:\ %I64u Trun ProgramFilesDir Soft
ware\Microsoft\Windows\CurrentVersion CommonFilesDir Software\Microsoft\Windo
ws\CurrentVersion AppData SystemDrive Software\Microsoft\Windows\CurrentVersio
n\Explorer\Shell Folders ALLUSERSPROFILE SystemRoot ProgramFiles UserProf
ile Temp \Windows NT \Windows NT\Accessories \Windows NT\Pinball \Windows Med
ia Player \Web Publish \Outlook Express \Microsoft Office\Office10\Data
\Microsoft Office\Office10 \Microsoft Frontpage \Internet Explorer \ComPlus
Applications \Microsoft Shared\MsInfo \Microsoft Shared\Office10 \Proof


Domain name: nt-windows-online.com
Name servers:
ns1.nameself.com
ns2.nameself.com
Registrar: Regtime Ltd.
Creation date: 2011-04-01
Expiration date: 2013-04-01
Registrant:
Ustuygov Denis Egorovich
Email: ustuygov_d@mail.ru
Organization: Ustuygov Denis
Address: Povorotnikova 19
City: Omsk
State: Omskaja obl.
ZIP: 644015
Country: RU
Phone: +7.3812557380
Fax: +7.3812557380

Servers in Germany

IP Information for **178.63.208.49**:

IP Location:	Germany Nuremberg Hetzner Online Ag
ASN:	AS24940
Resolve Host:	static.49.208.63.178.clients.your-server.de
IP Address:	178.63.208.49 W R P D T
Reverse IP:	2 websites use this address. (examples: genuine-check.com nt-windows-online.com)

Red October's modules:

34 types
9 groups
1000+ files

maybe not all...

№	Name	Group			Size (Kb)	Summary
1	RegConn	Recon			~160	Query system software environment
2	WinHttp	Recon			~142	Get external IP and send to the C&C
3	SysInfo	Recon			~503	Get browser history,usb drives,processes,disks,...
4	GetWebFtp	Recon			~157	Get browser history,http/ftp credentials
5	AuthInfo	Recon			~660	Get file manager,browser,ftp,mail client credentials
6	Logic	Recon			~160	Get general information about current Windows machine and available remote network shares
7	Logic	Recon			~150	Grab Internet Explorer URL history from the local system
8	Repeat2	Recon			~150	Get listing from remote shares available in Windows network neighborhood
9	Reference	Recon			~150	Grab directory/file listings of all drives attached to the local system
10	PswSuperMailru	Password			230-260	Steal Mail.ru account info and Outlook attachments
11	PswOutlook	Password			~31	Steal Outlook account info
12	MSHash	Password			400-550	Steal Windows account hashes
13	MAPIClient	Email			418-440	Steal e-mail data using local MAPI
14	POP3Client	Email			1100-1200	Steal e-mail data from POP3 server
15	USBContainer	USB drive			649-690	Loads and runs embedded USBStealer
16	USBRestore	USB drive			372-376	Recover and steal deleted files on USB drives
17	USBStealer	USB drive			448-504	Steal interesting files from USB drives
18	Keylogger	Keyboard			300-312	Makes screenshots, records keystrokes
19	Scheduler	Persistence			~620	Run various tasks from spec.folders
20	DocBackdoor	Persistence			75-88	Runs an embedded module from MSOffice/PDF doc
21	OfficeBDInstaller	Persistence			~286	Installs DocBackdoor plugin in MS Office
22	AdobeBDInstaller	Persistence			~218	Installs DocBackdoor plugin in Adobe Reader
23	FilePutExec	Spreading			~305	Extract and run an embedded file locally or remotely
24	Netscan	Spreading			~315	Port scanner, vuln. scanner, Cisco cfg dumper
25	MSExploit	Spreading			~1200	Infect target host using MS08-067 exploit
26	DASvcInstall	Spreading			~276	Infect target host using admin credentials
27	Frog	Spreading			~102	Initial backdoor, used in MSExploit/DASvcInstall
28	iPhone	Mobile			329-331	Steals data from locally attached iPhone
29	Nokia	Mobile			~337	Steals data from locally attached Nokia phone
30	Winmobile	Mobile			~400-700	Infect locally attached Windows Mobile phones with a native backdoor/updater modules
31	Winmobile	Mobile			~7-100	Native mobile backdoor/utilites
32	WinFtpScan	Exfiltration			~209	Steals files from local FTP server
33	GetFileReg	Exfiltration			~340	Steals files from local/network disks
34	FileInfo	Exfiltration			339-340	Uploads various collected files to the C&C

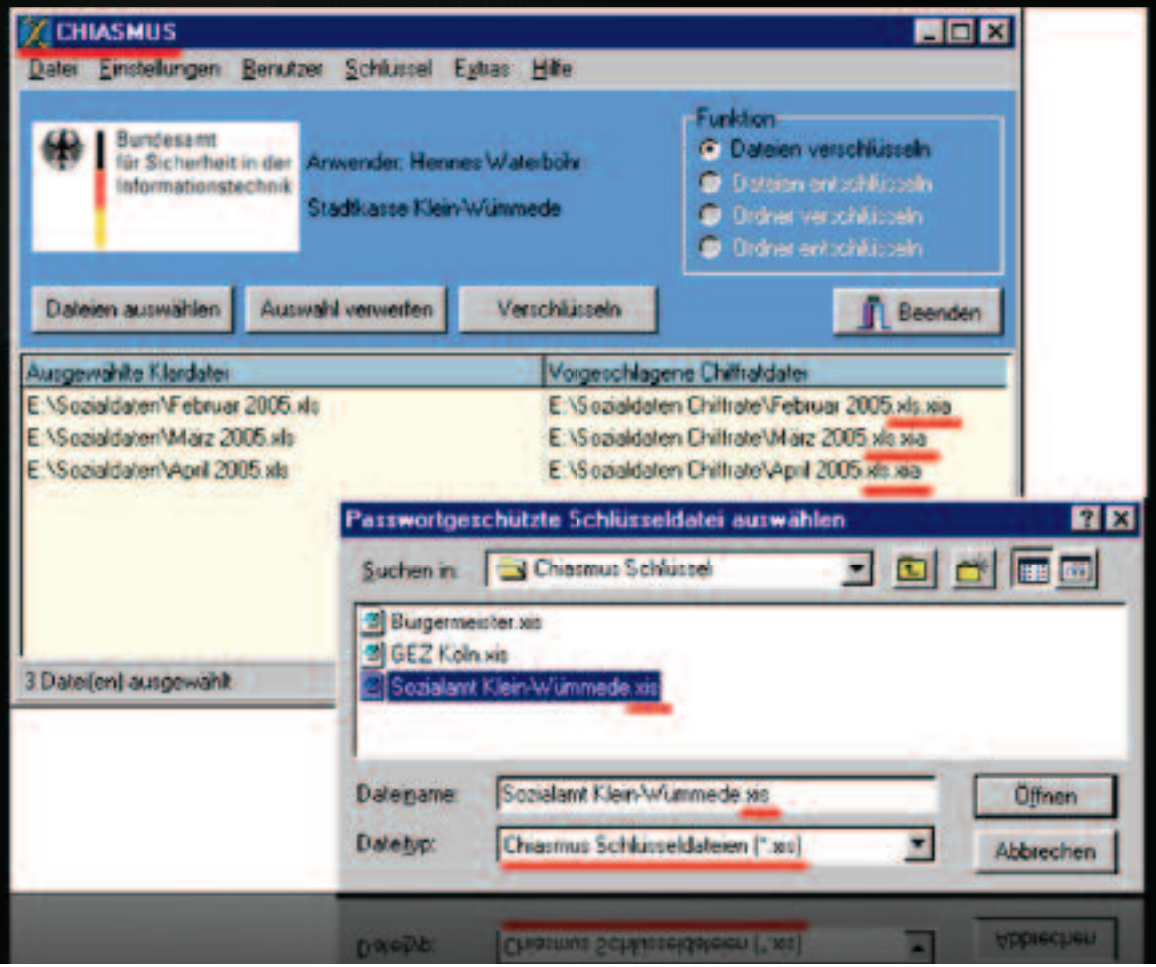
- "online" module: all data is sent to the C&C; no local files created;
- "offline" module; no network communication; all data is stored locally;
- module with embedded script/config in resource named "AAA";
- module with all values hardcoded.

USB Stealer – Acid Cryptofiller

sa=/pubring.*/
sa=/secring.*/
sa=/\.acidcsa$/
sa=/\.acidsca$/
sa=/\.aciddsk$/
sa=/\.acidpvr$/
sa=/\.acidppr$/
sa=/\.acidssa$/
sa=/\\ACIDInstallv.*\.exe$/
sa=/\\ACIDdirInstallv.*\.exe$/
sa=/\\Acid Technologies\\/

The other crypto software

sa=/\.xia$/
sa=/\.xiu$/
sa=/\.xis$/
sa=/\.xio$/
sa=/\.xig$/

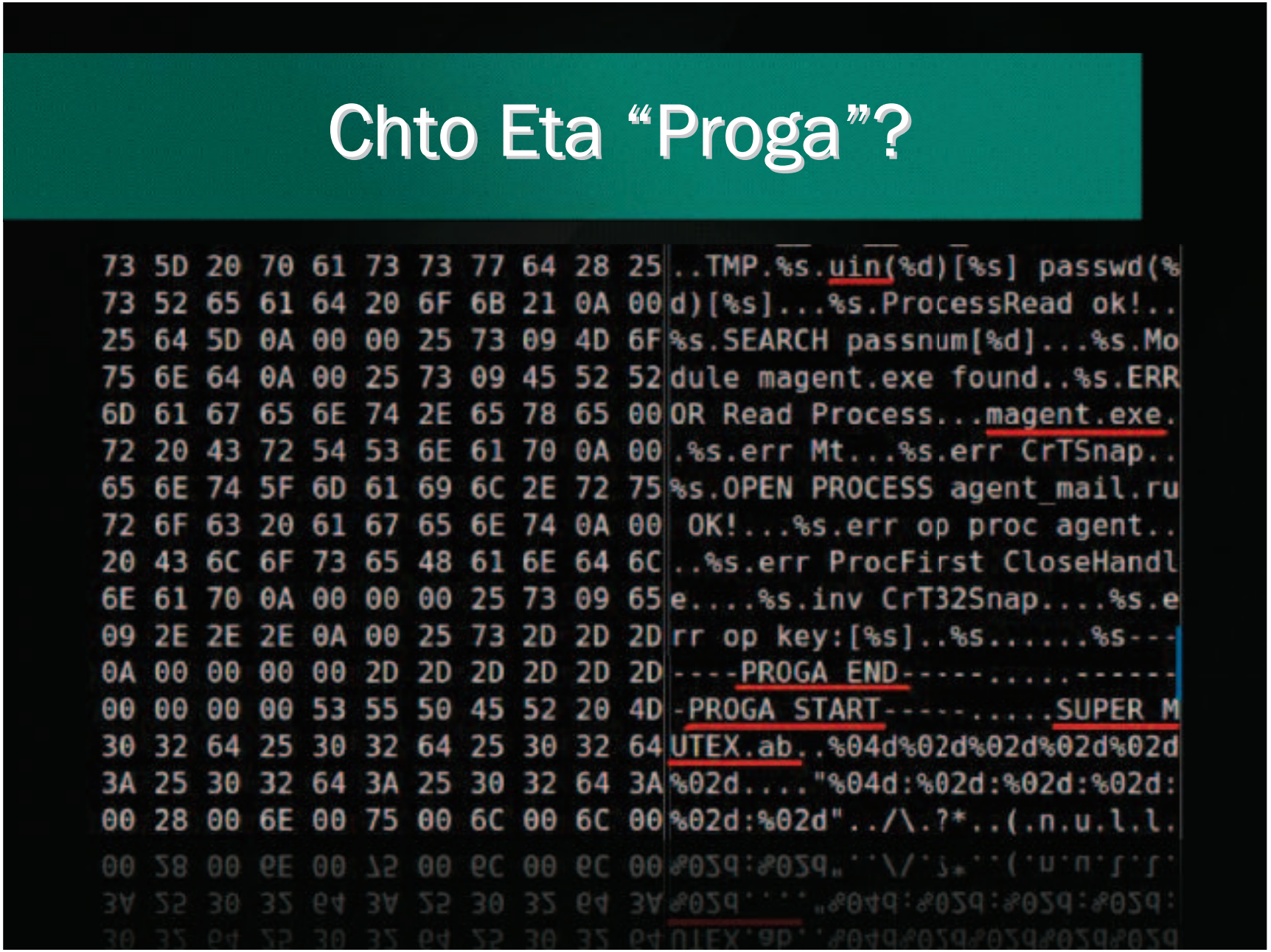


Red October “Zakladka” module

```
mov     dword_47786C, eax
jnz     short loc_402847
call    dword_46E578
push    eax             ; ArgList
push    offset aCannotInjectZa ; "Cannot inject zakladka, Error: %u"
call    sub_403370
add     esp, 8
call    sub_404130
mov     eax, 3
pop     esi
mov     ecx, [esp+21Ch+var_4]
xor     ecx, esp
call    @__security_check_cookie@4 ; __security_check_cookie(x)
add     esp, 21Ch
retn
-----------------------------------------------------------------

                        ; CODE XREF: sub_4026E0+131↑j
push    offset aZakladkaInject ; "Zakladka injected"
call    sub_403370
push    230h            ; size_t
push    0               ; int
push    offset dword_4771D0 ; void *
```

Chto Eta “Proga”?

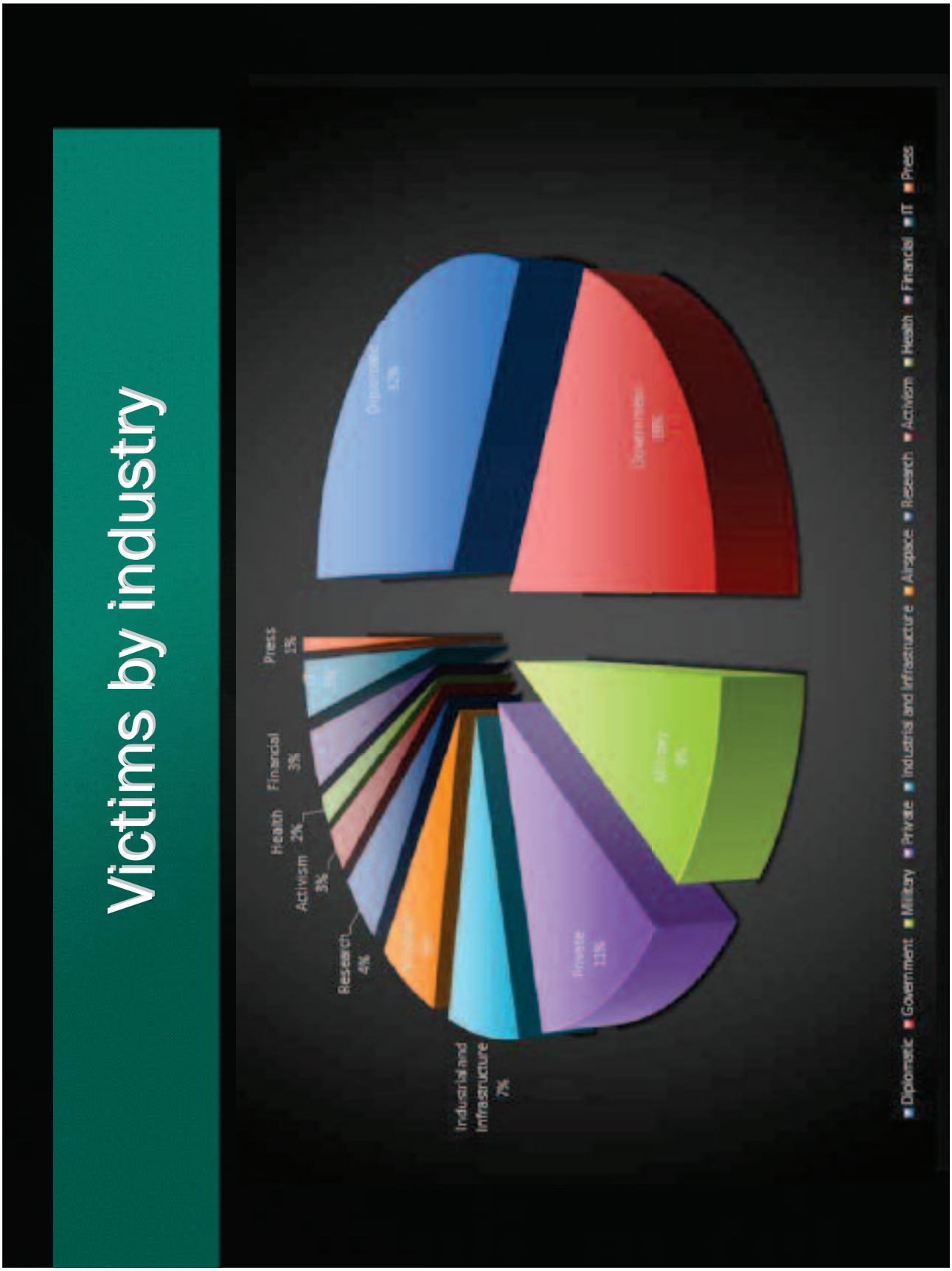


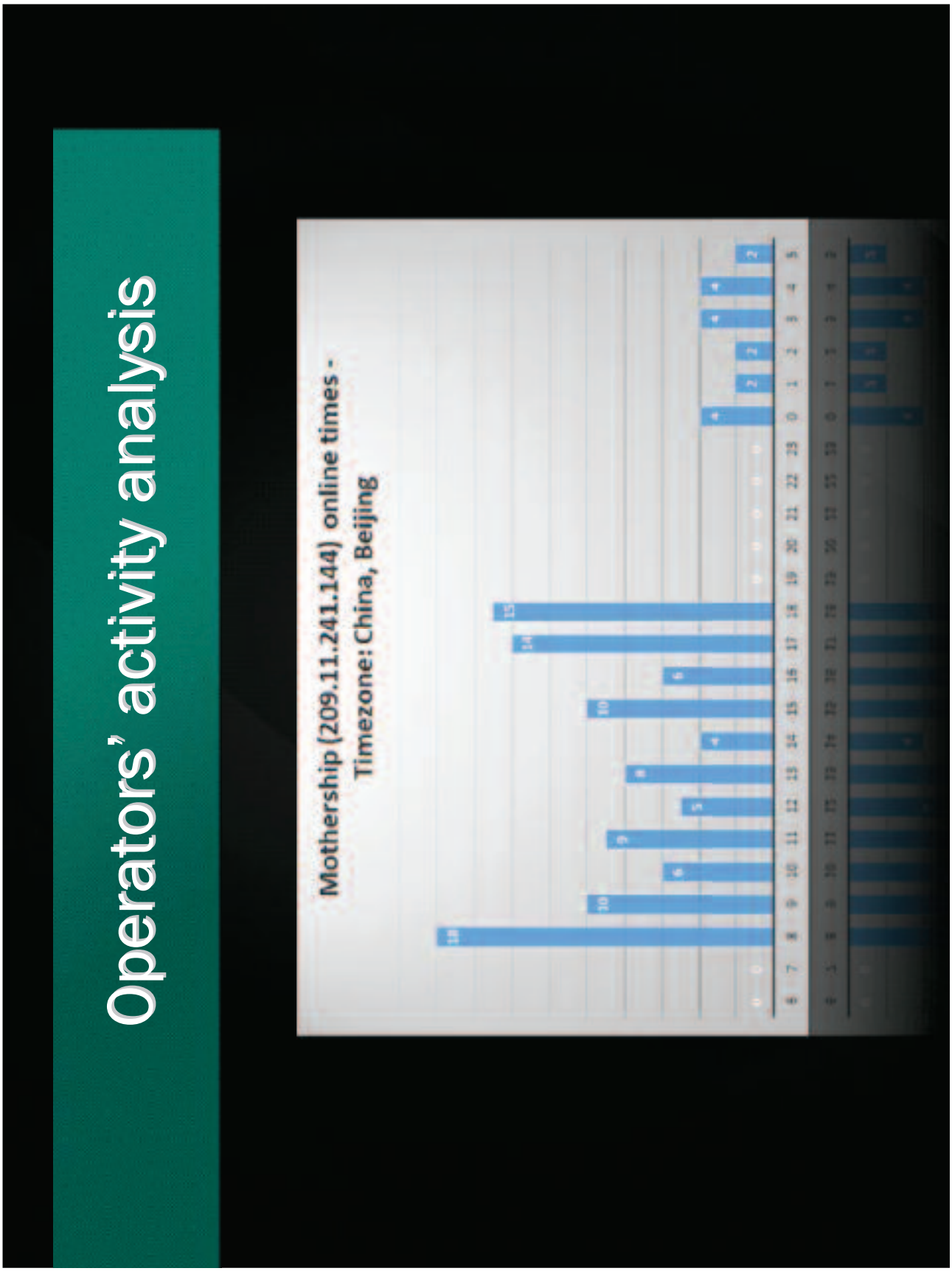

2013 – NetTraveler
NetFile-801.exe
版权所有 (C) 2004

Interests of the NetTraveler group

- Nanotechnology
- Lasers
- Nuclear power cells
- Aerospace
- Drilling
- Manufacturing in extreme conditions
- Radio wave weapons


Operation “NetTraveler”
Victims of cyber-espionage compaign
Russian Federation
China
Japan
Korea, Republic of
Hong Kong
Nepal
Thailand
Cambodia
Bangladesh
Malaysia
Indonesia
Australia
Mongolia
Kazakhstan
India
Uzbekistan
Tajikistan
Afganistan
Kyrgyzstan
Pakistan
Turkmenistan
Qatar
Iran
Belarus
Lithuania
Ukraine
Germany
United Kingdom
Belgium
Austria
Slovenia
Greece
Turkey
Morocco
Syria
Jordan
Suriname
Canada
United States
Chile
KASPERSKY
© 1997 - 2013 Kaspersky Lab ZAO.
All Rights Reserved.


Victims by industry
Press 1%
Financial 3%
Health 2%
Activism 3%
Research 4%
Industrial and Infrastructure 7%
Private 11%
Diplomatic
Government
Military
Private
Industrial and Infrastructure
Airspace
Research
Activism
Health
Financial
IT
Press


Operators' activity analysis
Mothership (209.11.241.144) online times -
Timezone: China, Beijing


Location of attackers
China
Taiwan
Hong Kong
Macao
Myanmar
(Burma)
TARGET
MAP

APT Job Posting

Work Loc

Vacancies

For candi the

resume w eeting.

Salary: fre f 200

square m rive with

environm ject will

provide y

Powerful background. No comments!

Tho who are competent, please contact:

Email: Inf

作者: mer4en7y 时间: 2012-4-6 08:28

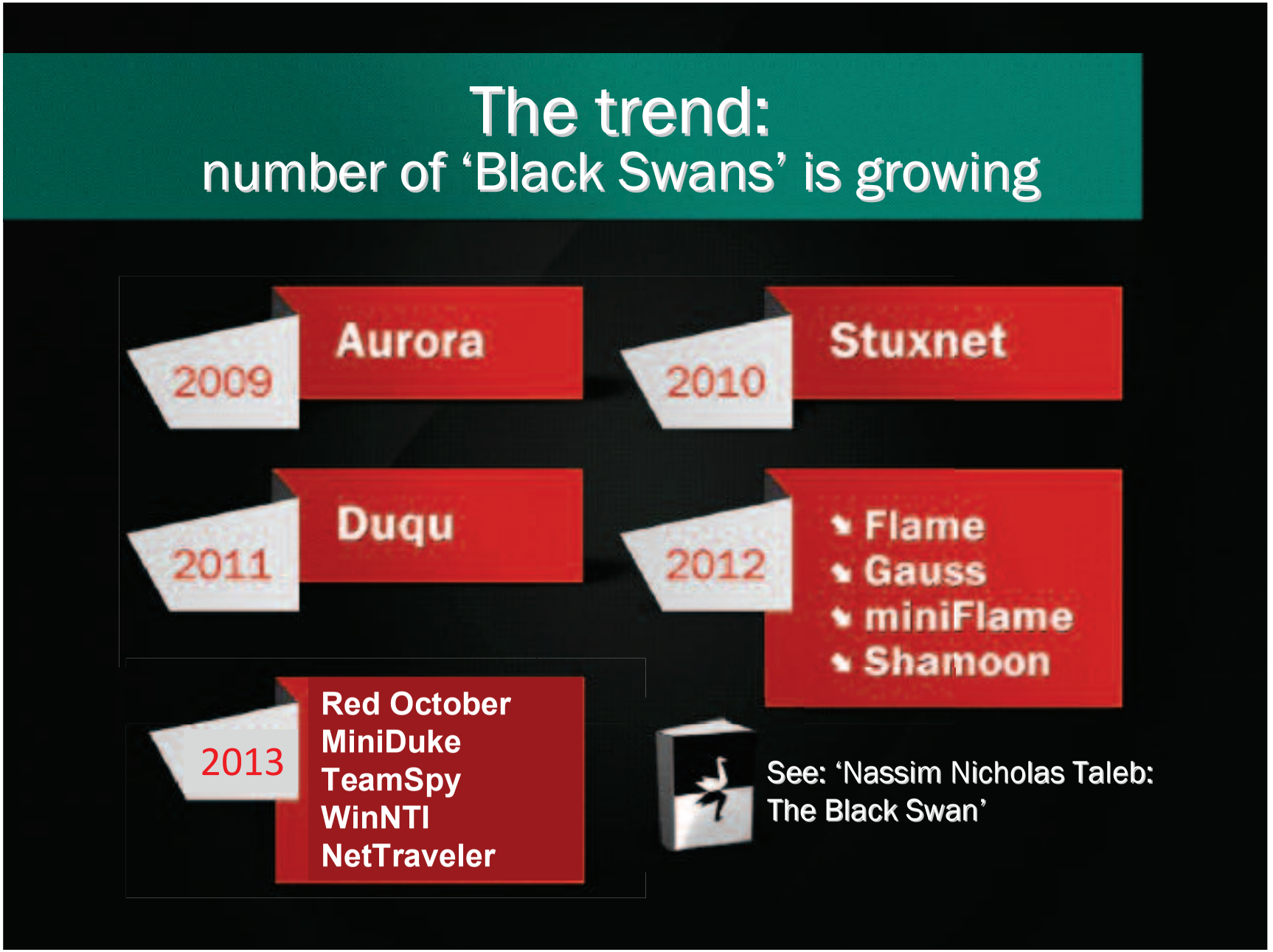
本帖最后由 mer4en7y 于 2012-4-6 08:30 编辑

难道是搞APT，只是广州太远，不过顶一个

Mer4en7y's comment about job offer

“Aren’t you recruiting people for APT? Guangzhou is too far...”

A tutorial for young APT recruits


The trend:
number of ‘Black Swans’ is growing
2009
Aurora
2010
Stuxnet
2011
Duqu
2012
Flame
Gauss
miniFlame
Shamoon
2013
Red October
MiniDuke
TeamSpy
WinNTI
NetTraveler
See: ‘Nassim Nicholas Taleb:
The Black Swan’

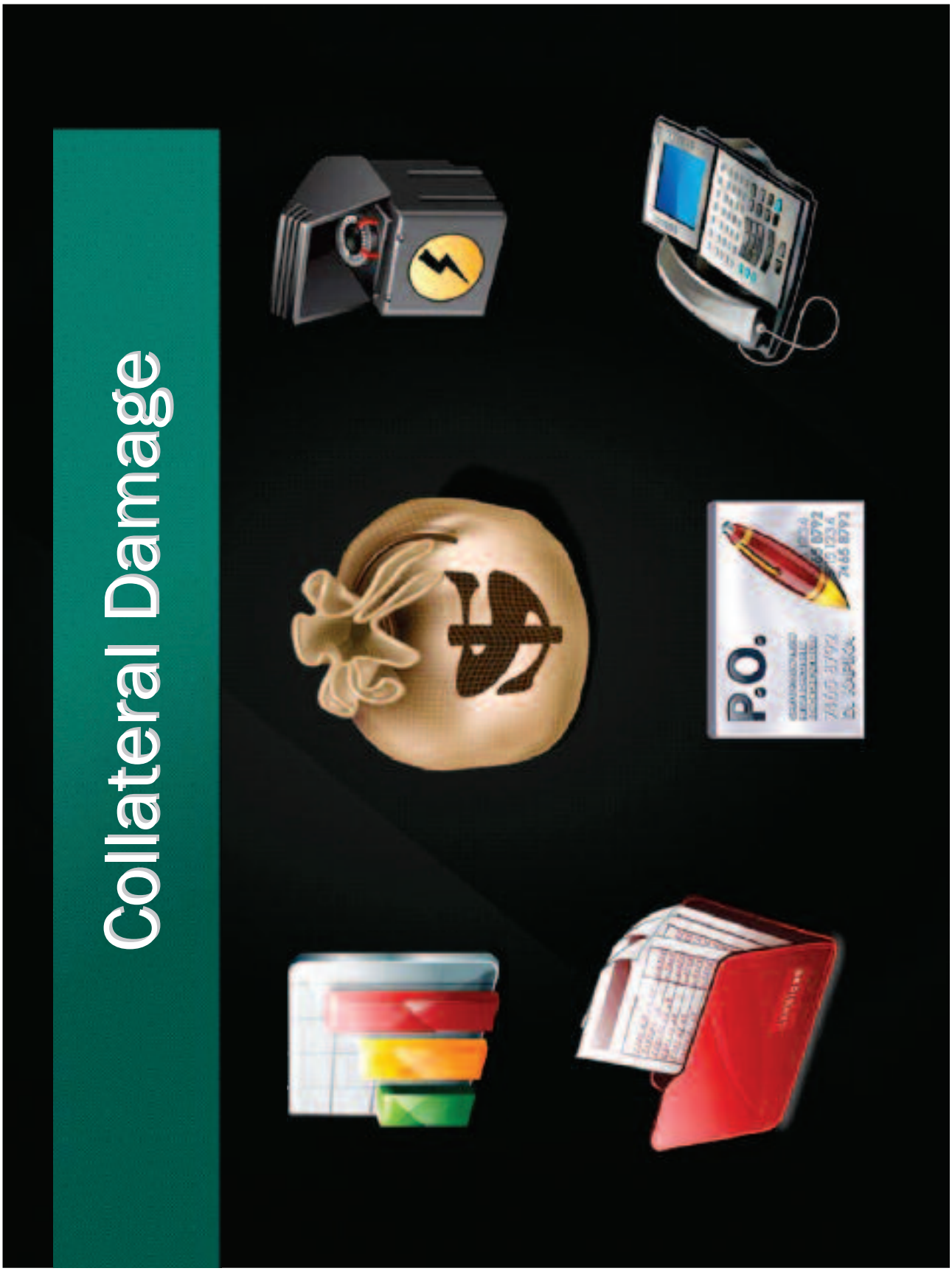
The 3 dangers of Cyberwar

- Ideas and techniques from cyberweapons can be re-purposed and copied.
- Companies become collateral victims in the cyberwar between superpowers.
- Cybercriminals start using weaponized exploits developed by or for governments.


2012 – Shamoon
The Cutting Sword of Justice

Saudi Aramco

30,000 machines wiped


Collateral Damage
P.O.

Primary Example

Stuxnet incidents: 150k (KL stats)

Cyberweapons are tampered
and used against innocent victims
Our critical infrastructure is fragile


Demo: Hijacking a Cyber-weapon

Commercialization of Exploits

13 Dec

Rapidly growing verdicts			All	
Verdict	Total users	Avg new users per day	Countries cnt	Trend slope
Exploit.Win32.CVE-2011-3402.c	31159	4373	111	319.29

14 Dec

Rapidly growing verdicts			All	
Verdict	Total users	Avg new users per day	Countries cnt	Trend slope
Exploit.Win32.CVE-2011-3402.c	38375	5293	110	229.36

What is CVE-2011-3402?

Answer: the ‘Duqu’ exploit

IT Staff: Biggest Nightmares

They all have something in common: exploits

The truth?
Threats are everywhere
WE ARE
ANONYMOUS


Corporate Threat Landscape
Threats from all angles
Java

Defense?

Against military grade weapons, you want the best available defense technologies.

Patch. Whitelist. Default Deny.
Exploit prevention. 0-day defense.
Realtime protection. Cloud protection.
Perimeter. Green zone. Raise awareness.
Access control. Education.


Thank You!

Sicherheit in Rechenzentren

Jörg Schulz

von zur Mühlen'sche GmbH, BdSI

Sicherheitsberatung - Sicherheitsplanung - Rechenzentrumsplanung

Bonn, Berlin, Wien

Alte Heerstr. 1
53121 Bonn
Tel. +49 228 96293-0
Fax +49 228 96293-90

Jörg Schulz
www.vzm.de

VON ZUR MÜHLEN-GRUPPE:

- VON ZUR MÜHLEN´SCHE GmbH
- RZ-Plan - Mit Planung zur Sicherheit.
- Sicherheits-Berater - Sicherheit durch Information.
- SIMEDIA - Sicherheit entsteht durch Wissen.

Makro- und Mikro-Sicht

- **Das BMI befasst sich intensiv mit den Kritischen Infrastrukturen der Wirtschaft – der Makrobetrachtung.**
- **Wir befassen uns mit dem „Mikrokosmos“, der KritIs im Unternehmen (seit 1969) – gewissermaßen der**

„Unkaputtbarkeit“

großer und kleiner Rechenzentren oder Serverräumen

VZM

- **Kritische Infrastrukturen…**
- **…schon 1972 ein Thema der von zur Mühlen‘schen GmbH**
- **Seither über 560 Rechen-zentren beplant oder in der Planung maßgeblich begleitet**
- **In der Zahl sind nur**

  RZs >200 m²

  Nettofläche enthalten

MIT SICHERHEIT MEHR SICHERHEIT®

VZM

1. These

Es gibt keine
Schadensereignisse,
sondern *auslösende* Ereignisse
(oft harmlos),
die zu einem
Schadensprozess
führen.

MIT SICHERHEIT MEHR SICHERHEIT®

2. These

Die erste These verändert das Denken:

Sicherheitsarbeit ist Prozessanalyse mit dem Ziel, den Prozess der Schadensentwicklung zu beeinflussen. Es gilt, die Phasen einer Entwicklung zu erkennen, in der man durch geeignete Maßnahmen in den Prozess eingreifen kann, um diesen zu inhibieren.

3. These

Bei RZ-Planungen werden wichtige Aspekte gar nicht beachtet:

1. **Planungen basieren nicht auf manifestierten und revisionsfähigen Schutzzielen**
2. **RZ-Planungen werden nach HOAI-Leistungen ausgeschrieben**
   Darin sind z.B. folgende essentielle Leistungen nicht enthalten
   - Prüfung der Reorganisation der IT
     (es wird ein neues Haus für eine alte Organisation gebaut)
   - Entwicklungsprognostik durch externe Fachleute
   - Schutzzieldefinitionen
   - Lastenhefte für den Bau und die kritischen Komponenten der IT
   - Härtetests auf Basis realistischer Schadensprozesse

VZM

Beispiel für einen Schadensprozess

- Startup-Unternehmen hat Verfahren zur Züchtung von Kristallen entwickelt
- Wachstum führt zu Erweiterungsbau und Parkplatzbedarf
- LKW liefert Schotter für Parkplatz – berührt Hochspannung

MIT SICHERHEIT MEHR SICHERHEIT®

Folie 7

VZM

Erdschluss>LKW-Brand>Fichte >Funkenflug>Scheune

MIT SICHERHEIT MEHR SICHERHEIT®

Damit nicht genug:

in der Scheune wurden unzulässig

- **Polyurethan-Folien**
- **PVC-Folien**
- **Altreifen**
- **Düngemittel**
- **Chemieabfälle**

etc. gelagert.

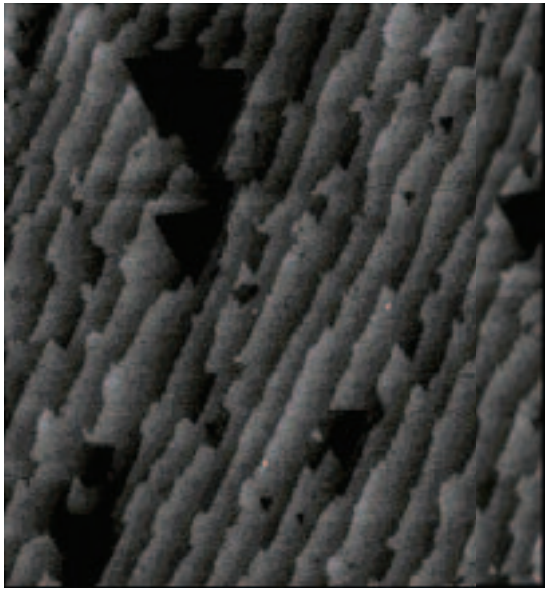
VZM

- **Wind dreht abermals**
- **Brandrauch dringt über die Frischluft-Ansaugung in das Unternehmen:**
  - in alles, was nicht Reinraumfertigung war
  - Labor
  - Büros
  - Rechenzentrum
    - kommerzielle IT und
    - Prozess- IT

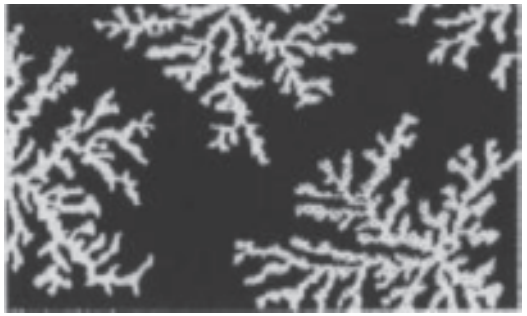
MIT SICHERHEIT MEHR SICHERHEIT®

Damit nicht genug: Sekundärschaden

Korrosive Gase drangen ein



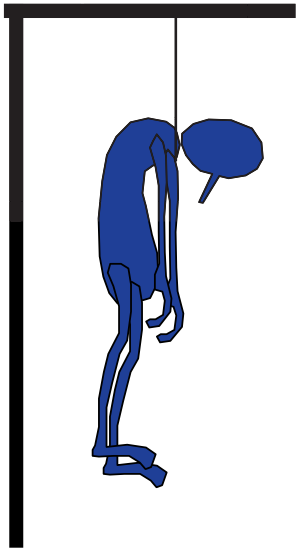
Und so sahen dann die Kontaminationen auf Platinen unter dem Mikroskop aus...



VZM

Warum das alles?

- Es gab keine manifestierten Schutzziele
- Türen und Brandschutzklappen nicht über BMA angesteuert
- Klimaplaner baute 1 Stück Lüftungsanlage
- BMA-Planer baute 1 Stück Brandmeldeanlage
- Bauherr verließ sich auf Planer
- Es gab keine Szenario-Bestimmungen
- Es gab ein enges Budget



Heute gibt es kein Budget mehr:

Zahlungsunfähigkeit

MIT SICHERHEIT MEHR SICHERHEIT®

Verurteilung hilft nicht, Schaden nicht versicherbar

...det zurückgewiesen. Der Beschluß ist nicht anfechtbar (Aktenzeichen 3 U 16/04).

Fünf Jahre Haft im Ansbacher Giftmüllprozeß

ANSBACH, 20. Juli (dpa). Im Ansbacher Giftmüllprozeß ist der angeklagte Landwirt am Dienstag zu fünf Jahren Haft verurteilt worden. Das Landgericht sprach den Siebenunddreißigjährigen der vorsätzlichen Boden- und Gewässerverunreinigung in besonders schweren Fällen schuldig. Das Gericht sah es als erwiesen an, daß er von 1998 bis 2002 mindestens 2500 Tonnen giftiger Industrieabfälle auf seinen und gepachteten Äckern in Neuendettelsau illegal entsorgt hat. Der Mann habe aus reinem Gewinnstreben gehandelt, sagte der Vorsitzende Richter Hans Blummoser. Für die illegale Entsorgung kassierte der Landwirt rund 97 000 Euro. Ende 1998 stand der Mann vor dem finanziellen Ruin. Da habe er den Entschluß gefaßt, mit der Entsorgung von Industriemüll Geld zu verdienen. Dafür habe er Unterlagen gefälscht und Genehmigungen vorgetäuscht, die er nicht besaß.

...aren an

MIT SICHERHEIT MEHR SICHERHEIT®

VZM

Sicherheit – ein Querschnittsthema

- **Neben Ingenieurwissen zu**
  - Architektur
  - Statik
  - Klimatechnik
  - Elekrotechnik
  - Nachrichtentechnik
  - Informatik
  - Brandschutz
- **gehören Systemanalyse-, Revisions- und Dokumentations-Profis in ein Planungsteam für hochverfügbare Rechenzentren.**

Und alle müssen miteinander reden!

MIT SICHERHEIT MEHR SICHERHEIT®

Zur 3. These

RZ-Planungen werden (vor allem) bei der öffentlichen Hand fast ausschließlich nach HOAI-Leistungen ausgeschrieben Darin sind z.B. folgende essentielle Leistungen nicht enthalten

- Prüfung der Reorganisation der IT
  (es wird ein neues Haus für eine alte Organisation gebaut)
- Entwicklungsprognostik durch externe Fachleute
- Schutzzieldefinitionen
- Lastenhefte für den Bau und die kritischen Komponenten der IT
- Härtetests auf Basis realistischer Schadensprozesse

VZM

Ausnahme:

Für dieses RZ wurden im Vorfeld 5 Konzernstandorte

1. untersucht
2. ihre Konsolidierung geplant
3. die zu erwartenden Höheneinheiten je Rack sowie sonstigen Bedarfe errechnet
4. Zukunftsvorhaben abgeschätzt
5. Bedarf an Rechnerfläche ermittelt und
6. eines der modernsten RZs der BRD gebaut

- Genau diese Leistungen sind in HOAI-Ausschreibung nicht enthalten
- Ausgeschrieben wird von Hochbauamt (im ö. Dienst) oder der Bauabt.
- IT-Fachleute und Experten für Hochverfügbarkeit werden als „Störer“ oft zunächst außen vor gelassen und zu spät eingeschaltet
- Dabei müssen sie in die Grundlagenermittlung einbezogen werden, denn

ihre Anforderungen sind die Planungsgrundlagen !

Sicherheitsarbeit heißt

zu Ende DENKEN

und nicht

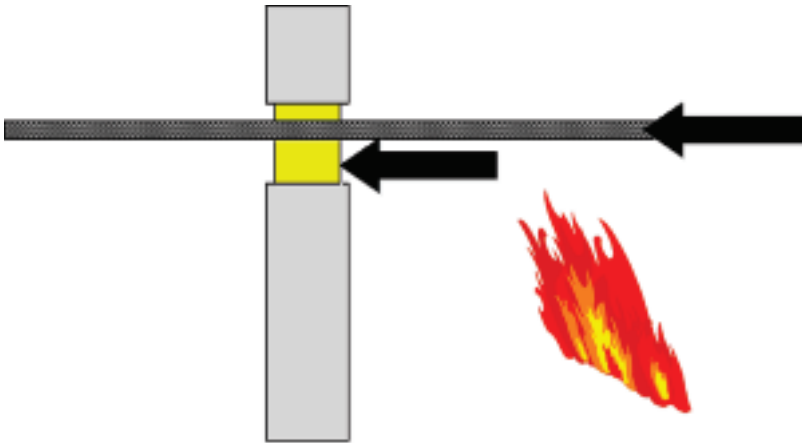
Checklisten abarbeiten

Zu Ende Denken erfordert Detailwissen und ist Detailarbeit bis hin zum Härtetest.

MIT SICHERHEIT MEHR SICHERHEIT®

Aber zunächst ein „kleines“ Beispiel:

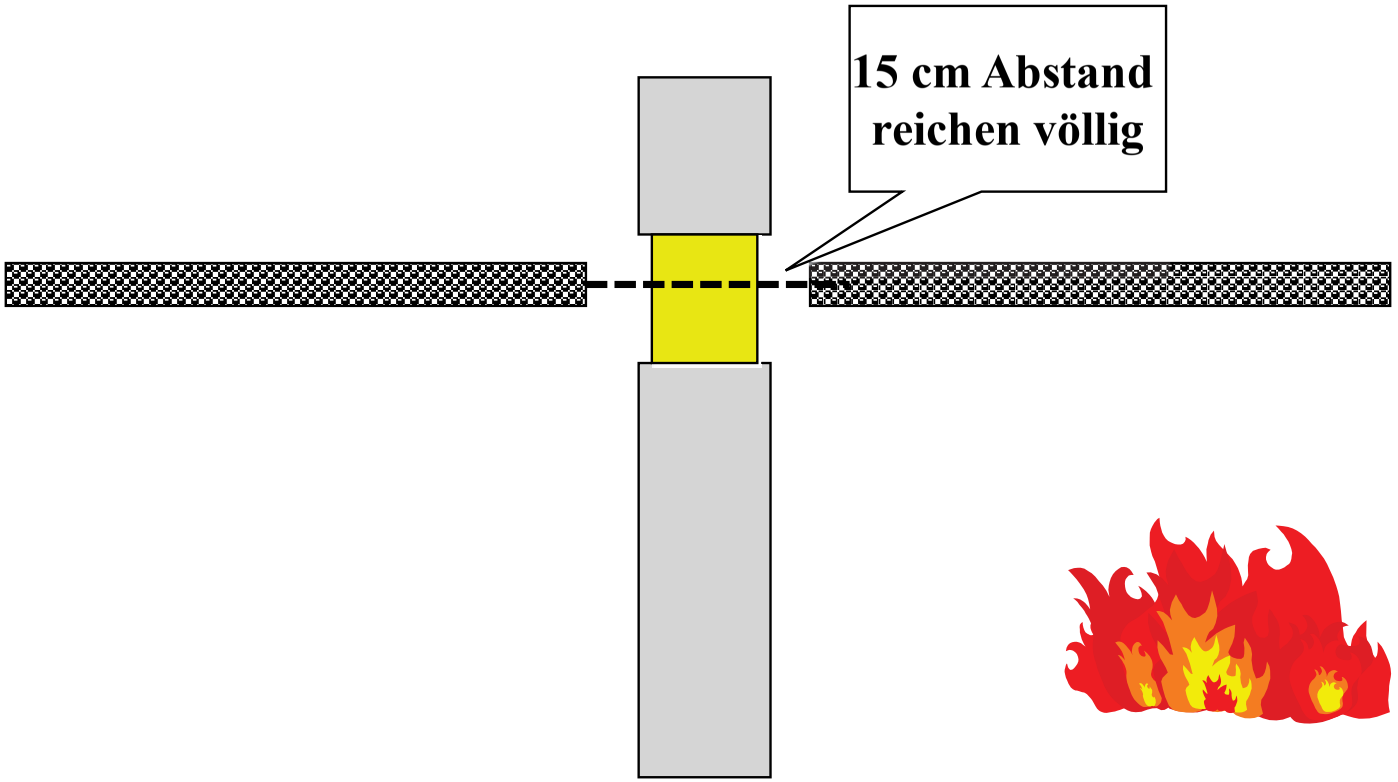
- Bei einem Großbrand wurden durch die Ausdehnung von Kabeltrassen, die sich erwärmt hatten, die Kabelschotts herausgedrückt. Der Rauch konnte sich ausbreiten. Sanierungsschaden über 25 Mio €.



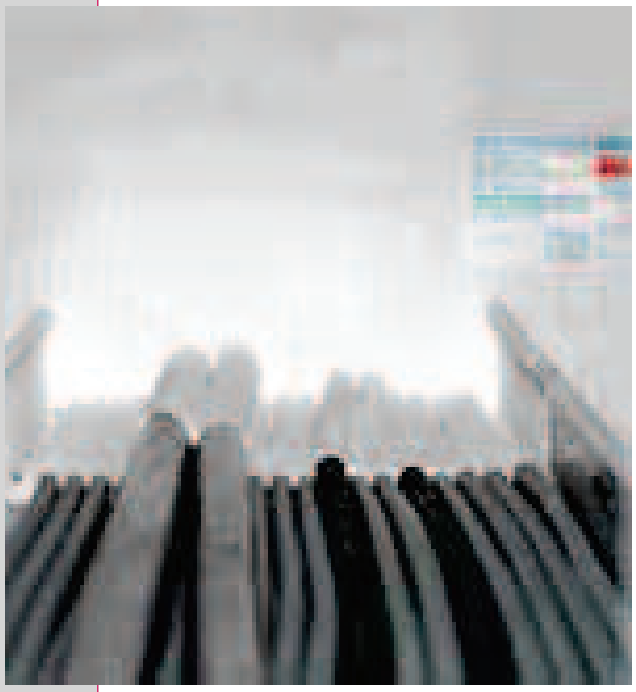
- Die Schotts waren fachgerecht um die durchgeführten Trassen gelegt und mit Prüfsiegel versehen.
- Der Nachbarbrandabschnitt verrauchte also normgerecht.

Lösung ganz einfach

- vor und hinter der Wand Blechtasse abschneiden
- Ausdehnung drückt dann nicht mehr



Schottungen falsch und richtig



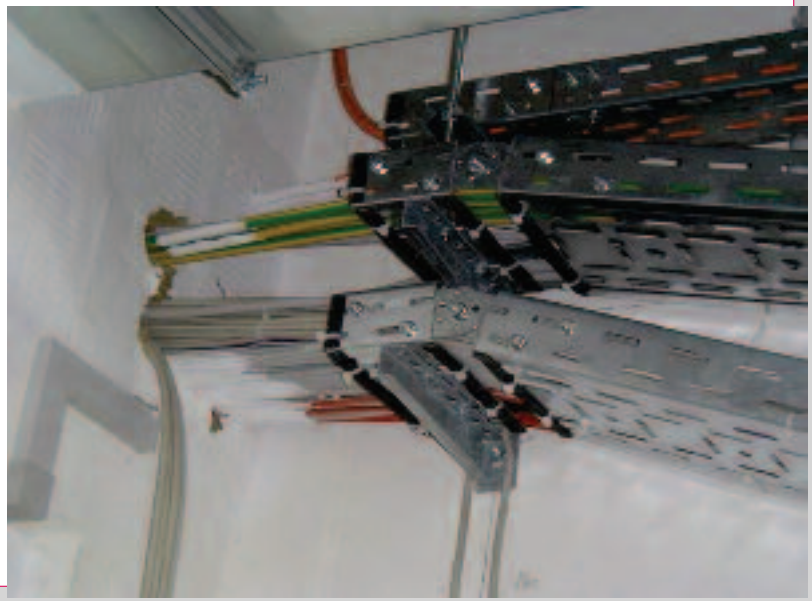
durchgeführtes Schott mit Zertifizierung

abgeschnittenes Schott

Aber: in Prozessen zu Ende denken

- Kabel bewegen sind
- Entgratung ist immer unsorgfältig
- Scheuergefahr!
- Maßnahme: Gummilippen an die Kante
- Bewegung der Kabel lässt sie herunter fallen
- Maßnahme: mit Kabelbindern befestigen

- Schadensprozess damit inhibiert !



Härtetests

- Wer nicht testet, verschieb den Test auf den Eintritt des Schadensprozesses
- Abnahmeprüfungen der Errichter sind keine Härtetests

Danke für Ihre Aufmerksamkeit !
Jörg Schulz
von zur Mühlen'sche GmbH, BdSI
Sicherheitsberatung - Sicherheitsplanung - Rechenzentrumsplanung
Bonn, Berlin, Wien
Alte Heerstr. 1
53121 Bonn
Tel. +49 228 96293-0
Fax +49 228 96293-90
js@vzm.de
www.vzm.de
VZM

brainloop

Brainloop AG

Schutz vertraulicher Dokumente in der Cloud

Roman Böck, Berlin

www.brainloop.de

Document Compliance Management

brainloop

Schutz vertraulicher Dokumente ist ein elementarer Bestandteil der Unternehmens Compliance

„Ein wichtiger Baustein eines Compliance-Konzepts ist der Datenschutz. Denn nur wer verantwortungsvoll mit personenbezogenen Daten umgeht und nicht mit dem Gesetz in Konflikt gerät, ist für seine Kunden vertrauenswürdig."
(Quelle: Sophus Group (2011): „Compliance leicht gemacht")

Gründe für Dokumentenschutz

brainloop

§

- Deutscher Corporate Governance Kodex (DCGK)
- Aktiengesetz (AktG)
- Transparenz- und Publizitätsgesetz (TransPubG)
- Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)
- Bundesdatenschutzgesetz (BDSG)
- USA: Sarbanes Oxley Act

Gesetzliche & Compliance-Anforderungen

- Risikomanagement
- Vertraulichkeit
- Nachvollziehbarkeit

Uneingeschränkter Austausch

- Dokumentenaustausch mit Partnern und Kunden
- Über Firewalls, Zeitzonen und Kontinente hinweg

Schutz von unternehmenskritischen Daten

- Spionage
- Fehlhantierung
- interner Datenschwund

Vertrauliche Dokumente werden sehr häufig ungeschützt per E-Mail versendet

brainloop

Grafik 4: Welche vertraulichen/geschäftskritischen Informationen versenden Sie per E-Mail?

Grafik 10: Welche Informationen werden per E-Mail ungeschützt versendet?

Quelle: Deutschland sicher im Netz e.V. (2011), „IT-Sicherheitslage im Mittelstand 2011“

… sogar in Aufsichtsorganen von Unternehmen

brainloop

Wie werden den Aufsichtsratsmitgliedern Berichterstattungen, Protokolle, Einladungen zu Sitzungen und weitere Informationen übermittelt?

Quelle: KPMG (2012): „Klischee und Wirklichkeit – Der Aufsichtsrat in Deutschen Unternehmen“

Zahlreiche Studien belegen die wachsende Bedeutung der IT Sicherheit

brainloop

Quelle: IDC (2012), „Cloud Computing in Deutschland 2012",

…die Top Herausforderungen der IT Security sind

brainloop

Cloud Security (42 %)

Abwehr neuer Angriffsszenarien (42%)

Sicherheit mobiler Endgeräte (39 Prozent).

Quelle: IDC (2011) „IT Sicherheit in Deutschland“: in digitalbusinessCLOUD 6/2012

Handlungsempfehlungen von „Deutschland sicher im Netz e.V.“

brainloop

Deutschland sicher im Netz empfiehlt den Unternehmen ganz konkret:

Stärken Sie Ihren Umgang mit Compliance-Vorgaben.
Benennen Sie einen Compliance-Verantwortlichen, erstellen Sie eine Compliance-Richtlinie, sensibilisieren Sie Mitarbeiter für das Thema, etablieren Sie einen Berechtigungs-Vergabe-Prozess und führen Sie eine Schutzbedarfsanalyse durch.

Verwenden Sie sichere E-Mail.
Verschlüsseln und signieren Sie E-Mails mit sensiblem Inhalt, oder schützen Sie zumindest die Anhänge. Eine gute Alternative ist der Einsatz von so genannten Datentresoren zum Austausch mit Kunden und Partnern.

Schützen Sie Ihre mobilen Daten.
Verwenden Sie eine Festplattenverschlüsselung für Notebooks, setzen Sie eine unternehmensweite Synchronisationslösung ein (statt individuelle Angebote), erstellen Sie ein Sicherheitskonzept, schützen Sie besonders kritische Dokumente direkt am Dokument, z.B. mit Rights Management Lösungen und ersetzen Sie passwort-basierte Anmeldeverfahren durch stärkere Authentifizierungsmechanismen.

Gewährleisten Sie die Funktionsfähigkeit Ihrer IT-Infrastruktur.
Erstellen Sie Notfallpläne und testen Sie regelmäßig das Einspielen von Backups.

8

Quelle: Deutschland sicher im Netz e.V. (2011), „IT-Sicherheitslage im Mittelstand 2011“

Status Quo - Cloud Computing in Deutschland (I) Überblick

brainloop

28 %

der deutschen Unternehmen stehen dem Thema Cloud-Computing aufgeschlossen und interessiert gegenüber. Bei den Großunternehmen sind es sogar knapp 60 Prozent.

28 %

der deutschen Unternehmen nutzen bereits irgendeine Form von Cloud-Computing.

27 %

der deutschen Unternehmen nutzen Private Cloud-Computing, weitere 21 Prozent planen oder diskutieren den Einsatz von Private Clouds.

6 %

der deutschen Unternehmen nutzen Public Cloud-Computing, weitere 7 Prozent planen oder diskutieren den Einsatz von Public Clouds.

Über

60 %

aller Cloud-Nutzer und Cloud-Planer werden in den nächsten zwei Jahren ihre Ausgaben für Cloud-Dienste erhöhen.

81 %

aller Public Cloud-Nutzer und 58 Prozent aller Private Cloud-Nutzer beurteilen ihre bisherigen Erfahrungen als positiv.

Quelle: KPMG: (2012), „Cloud-Monitor 2012“

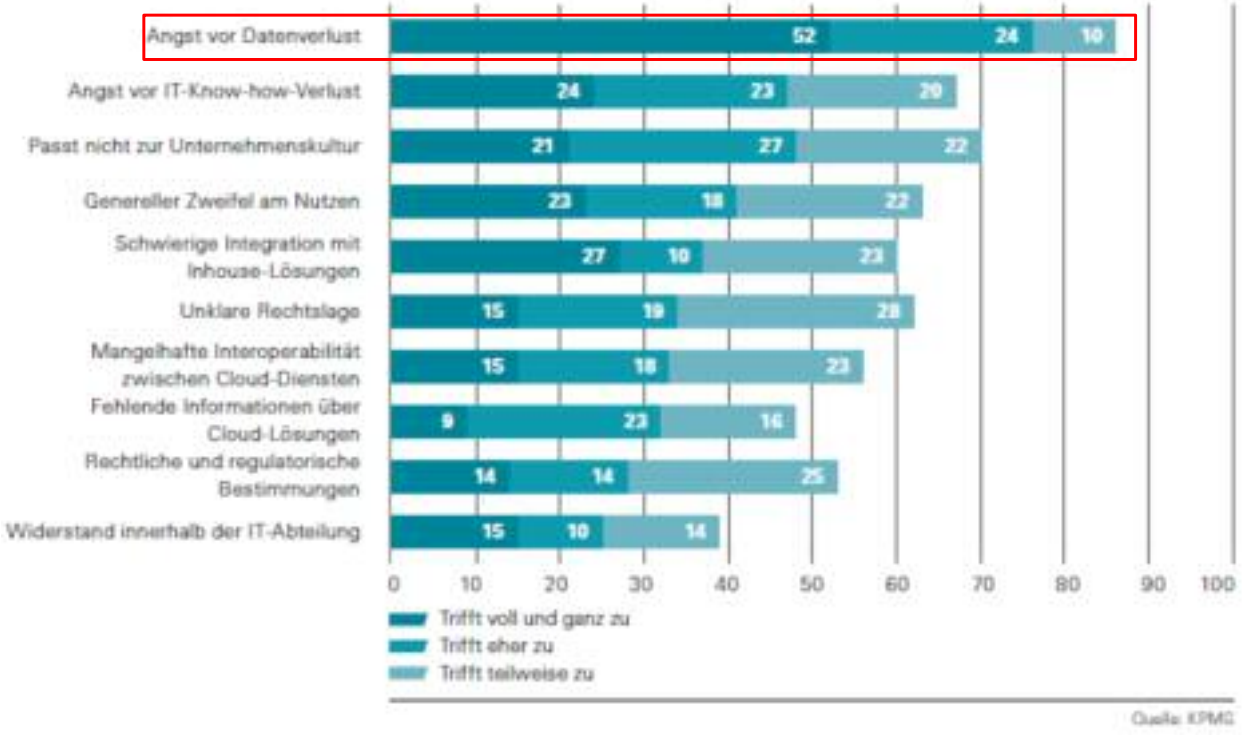
Status Quo - Cloud Computing in Deutschland (II)
Hürden der Nutzung

brainloop

Abbildung 13

Mögliche Hürden der Public Cloud-Nutzung

Anteil (gewichtet) der Unternehmen in Prozent, für die Public Cloud-Computing kein Thema ist; n = 319

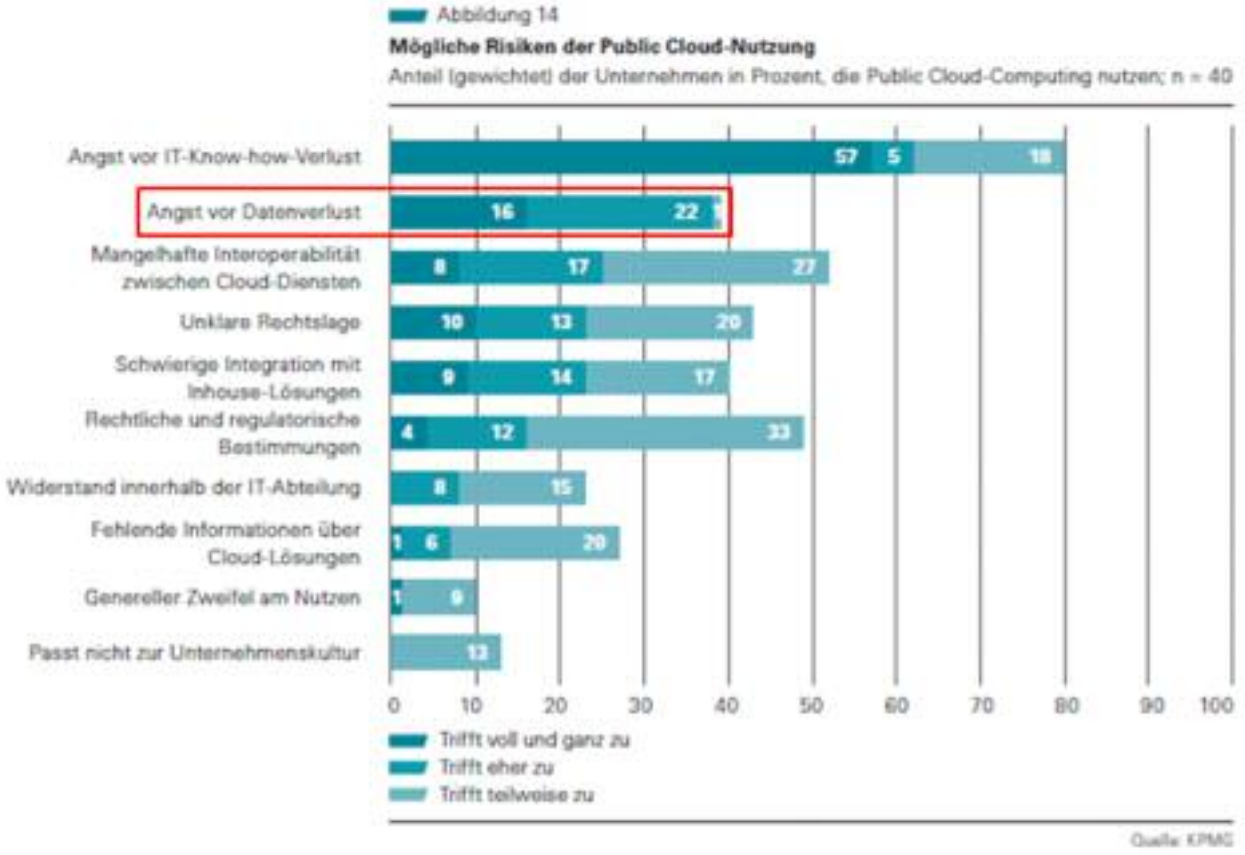


Quelle: KPMG

Quelle: KPMG (2012): „Cloud-Monitor 2012“

Status Quo - Cloud Computing in Deutschland (III)
Risiken der Cloud Nutzung

brainloop



Quelle: KPMG (2012), „Cloud-Monitor 2012“

Ist Datensicherheit und damit effektiver Schutz vertraulicher Daten in der Cloud möglich?

brainloop

Wesentliche technischen und organisatorischen Maßnahmen des Datenschutzes bei der Verarbeitung personenbezogener Daten („TOM“, gem. Anlage zu § 9 BDSG):

Sicherheitsfeatures Secure Dataroom (Beispiele):

- Zutrittskontrolle -> **Hochsicheres RZ in Deutschland, zertifizierte Prozesse**
- Zugangskontrolle -> **2-Faktor Authentifizierung, Operator Shielding**
- Zugriffskontrolle -> **Berechtigungssystem, Reporting, Audittrail**
- Weitergabekontrolle -> **Durchgängige Verschlüsselung, Adobe LCM**
- Eingabekontrolle -> **Revisionssicherer Audittrail inkl. umfassendem Reporting**
- Verfügbarkeitskontrolle -> **Redundante Datensicherung, katastrophensicherer Betrieb**
- Trennungskontrolle -> **Chines Walls, Berechtigungskonzept**
- Auftragskontrolle -> **Nutzungsvertrag mit ADV, DIN ISO 27001 Zertifizierung**

Auf Grundlage einer entsprechenden Sicherheitsarchitektur ist Sicherheit in der Cloud heute schon realisierbar!

12

Risiken beim Austausch vertraulicher Unternehmensdaten

brainloop

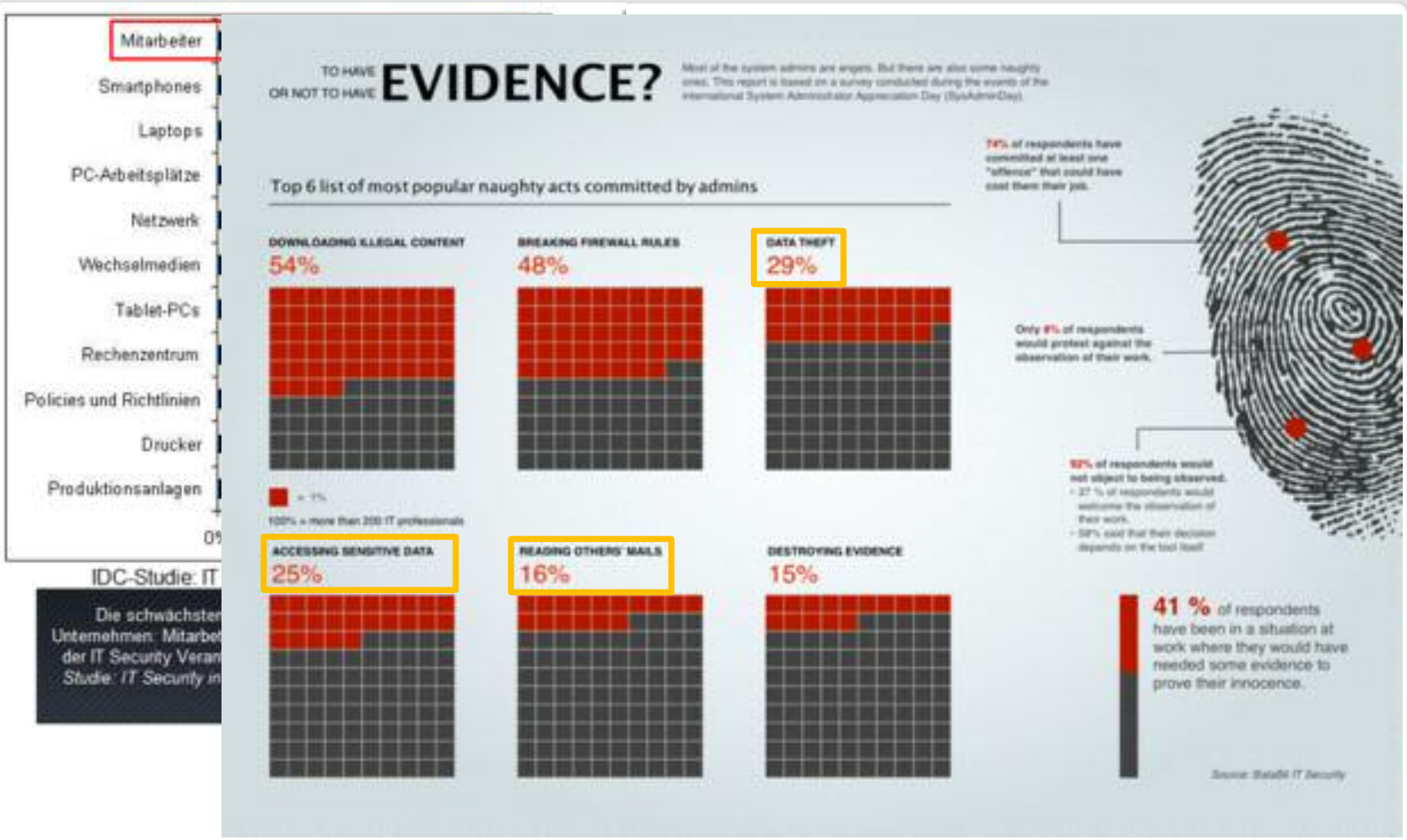
- Ungeschütztes Versenden per E-Mail
- Flüchtigkeitsfehler
  - Fehladressierung per E-Mail (ähnlicher Name aus Outlook- Vorschlagsliste)
  - Versenden nichtaktueller Versionen (z.B. mit noch internen Vermerken oder verborgenen Texten)
  - Ungewollte bzw. unkontrollierte Weitergabe des Empfängers
- „Cyber-Attacken“ bei der Übermittlung per E-Mail, Filetransfer
- Weitergabe auf ungeschützten lokalen / mobilen Datenträgern und via öffentlichen Cloud-Tools
- Ausspähen beim lokalen Druck auf Abteilungsdruckern und senden an unbeaufsichtigte Faxgeräte
- Verlust von Papierakten

13

Quelle: Corporate Trust (2012), „Studie: Industriespionage“

Der Faktor Mensch ist gemäß aktueller Studien der größter Risikofaktor für Datenabfluß/-pannen

brainloop



Quelle: BalaBit IT Security (2011), "Evaluation of the Survey Among IT Professionals"

Mögliche Konsequenzen wenn Dokumente/ Daten in die falschen Hände geraten

brainloop

- Quartals-/Jahreszahlen, M&A-Details dringen zu früh an die Öffentlichkeit
  - Manipulation des Börsenwertes → Börsenaufsichtsbehörde
  - Nichtzustandekommen des Rechtsgeschäftes
- Personenbezogene Daten geraten in falsche Hände
  - Verstoß gegen Bundesdatenschutzgesetz
    → Haft- u. Strafmaß
- Vertragsdetails gelangen an Dritte
  - Verletzung Vertrauens- und Vertragsverhältnis zw. Geschäftspar
    → Aufkündigung der Geschäftsbeziehung, bis hin zu Schadensersatzforderungen
- ...
- In jedem Fall wird die Reputation des Unternehmens geschädigt

15

Schutz vor Industriespionage wird immer wichtiger – Auszüge Corporate Trust Studie

brainloop

Wie hoch schätzen Sie den Gesamtschaden, welcher der deutschen Wirtschaft jährlich durch Industriespionage entsteht?

- **4,2 Milliarden Euro**

Wie hoch schätzen Sie die Häufigkeit der finanziellen Schäden durch Industriespionage ein?

- Häufigkeit der finanziellen Schäden durch Industriespionage ist deutlich angestiegen. 2012 haben **82,8 Prozent** der geschädigten Unternehmen einen finanziellen Schaden erlitten

ggf auch interessant: Kann der Schaden durch Spionage finanziell beziffert werden?

- Kein finanzieller Schaden nachweisbar: 17,1 %
- Schaden bis 10.000 Euro: 10,3 %
- Schaden zwischen 10.000 Euro und 100.000 Euro: 45,2%
- Schaden zwischen 100.000 Euro und 1 Mio. Euro: 18,2 %
- Schaden über 1 Mio. Euro: 9.2 %

Worin sehen Sie in Zukunft das häufigste Risiko für Industriespionage?

- 63,7 Prozent sehen die zunehmende Verwendung **mobiler Geräte** wie Tablets oder Smartphones als größte Gefahr an

16

Quelle: Corporate Trust (2012), „Studie: Industriespionage“

Beispiele aktueller Datenpannen

19.10.2012, 14:46 Uhr
Finanzielles Desaster

Datenleck bei Faceb
verurteilt

Unternehmen muss zwei Millionen

AFP – Sa., 27. Okt 2012

E-Mail | Empfehlen 0 | Twitt

Foto anzeigen

Weil sie vor dem Börsengang von Facebook vertrauliche Daten herausgegeben hat, ist ...

Quelle: 15.11.2012 Heise online

Konfettiregen aus geheimen Dokumenten

Vertrauliche Akten landeten bei der Erntedankparade in den Straßen von New York.

Empfehlen 8 | +1 0 | Twittern 0

Peinliche Datenpanne: Die Geheimnisse der New Yorker Behörden lagen buchstäblich auf der Straße. Wie nun bekannt wurde, gingen vertrauliche Dokumente bei der traditionellen Thanksgiving-Parade als Konfettiregen auf den Feiernden nieder. Nicht etwa als kleine Papierschnipsel, sondern als lange Streifen – und auch noch horizontal geschnitten, so dass alles gut lesbar war.

„Das Zeug landete auf der Schulter eines Freundes. Es war überall", berichtete der Student Ethan Finkelstein, der am Donnerstag wie zahlreiche andere Menschen an Macy's Thanksgiving Day Parade in den Straßen von New York teilgenommen hatte. Finkelstein und sein Freund sahen sich die Papierschnipsel näher an: „Das sieht ja aus wie eine Sozialversicherungsnummer." Sie untersuchten die grob geschnittenen Konfetti und entdeckten Telefonnummern, Adressen, vertrauliche Polizeidokumente und weitere Sozialversicherungsnummern. Diese sind für viele US-Amerikaner der wichtigste Nachweis ihrer Identität.

Quelle: http://kurier.at/politik/weltchronik/konfettiregen-aus-geheimen-dokumenten/1.480.615

Weltweite Datenverluste 2011

brainloop

- Allein 2011 gingen weltweit mehr als **223 Mio. Datensätze verloren**, die u. a. Finanzinformationen, Sozialversicherungsnummern, medizinische Daten und andere Personaldaten enthielten.*

- An der Spitze der Hauptverlustwege steht die Kategorie „**Internet und E-Mail**“. Diese Kanäle sind weiterhin aufgrund ihrer Einfachheit am beliebtesten; danach folgen Verluste über Papierunterlagen...*

*Quelle: Analysezentrum InfoWatch Globale Studie zu Verlusten von Unternehmens- und vertraulichen Daten, 2011

brainloop

„Data may be as valuable as gold, yet it can slip through your fingers like water…“

Malcolm Marshal, Partner Information Protection and Business Resilence, KPMG in the UK

Herzlichen Dank für Ihre Aufmerksamkeit!

Kontakt
Roman Böck
Sales Director
+49 89 444 699-163
Email: roman.boeck@brainloop.com

Quellen - Übersicht

brainloop

	Informationssicherheits- und Notfallmanagement: Trends 2012	Ibi Research GmbH, 2012
	Compliance leicht gemacht	Sophus Group, 2011
	IT-Sicherheitslage im Mittelstand 2011	Deutschland sicher im Netz e.V. , 2011
	IT Sicherheit in Deutschland 2011	IDC, in digitalbusinessCLOUD 6/2012
	Cloud Computing in Deutschland 2012	IDC, 2012
	Cloud-Monitor 2012	KPMG, 2012
	Informationssicherheits- und Notfallmanagement Trends 2012	ibi research an der Universität Regensburg, 2012
	IT-Sicherheit als politische Aufgabe	TeleTrusT Deutschland e.V. , 2010
	Studie zur IT-Sicherheit in kleinen und mittleren Unternehmen	Bundesamt für Sicherheit in der Informationstechnik, 2011
	Die IT-Sicherheitsbranche in Deutschland im Auftrag des Bundesministeriums für Wirtschaft und Technologie	Booz & Co
	Plopp oder top: Die IT-Luftblasen des Jahres 2012	www.gulp.de/kb/mk/die-it-luftblasen-des-jahres-2012.html
	Klischee und Wirklichkeit – Der Aufsichtsrat in Deutschen Unternehmen	KPMG, 2012
	Globale Studie zu Verlusten von Unternehmens- und vertraulichen Daten 2011	INFOWATCH, 2011

Quellen - Übersicht

	Cloud Computing und Consu m e r i z a t i o n o f I T i n Deutschland 2012	IDC, 2012
	Top 6 list of most popular prohibited activities in the workplace among IT staff	Balabit IT Security, 2011
	Studie: Industriespionage 2012	Corporate Trust, 2012 – Aktuelle Risiken für die Deutsche Wirtschaft durch Caberwar


7. BfV/ASW-SICHERHEITSTAGUNG
SCHUTZ VOR SOCIAL ENGINEERING
BERLIN, 27. JUNI 2013
MANFRED STRIFLER, DEUTSCHE TELEKOM AG
ERLEBEN, WAS VERBINDET.

MITARBEITER SIND DAS WICHTIGSTE GUT EINES UNTERNEHMENS

„Engagement zeigen nur Mitarbeiter, die die strategischen Ziele und Werte des Unternehmens verstehen und sich emotional mit dem Unternehmen verbunden fühlen“.

Quelle: Global Workforce Study 2012

IHRE SEKRETÄRIN IST FÜR IHR BUSINESS UNERSETZLICH

Sie...

- ist die Vertraute im Vorzimmer
- fängt lästige Anrufe ab
- behält den Überblick
- ...

ALS WELTWEIT AGIERENDES UNTERNEHMEN IST DIE DEUTSCHE TELEKOM FÜR SOCIAL ENGINEERING EIN POTENTIELLES ANGRIFFSZIEL

Die Story „Moment Mal.“

- „Moment mal.“, um noch mal nachzudenken
- 7. Sinn und „lass auch mal deinen Bauch sprechen„
- 3 Botschaften appellieren an die Selbstverantwortung der Mitarbeiter
  - Ich lass mich **nicht unter Druck setzen**
  - Ich lass mich **nicht täuschen**
  - Ich lass mich **nicht einwickeln**

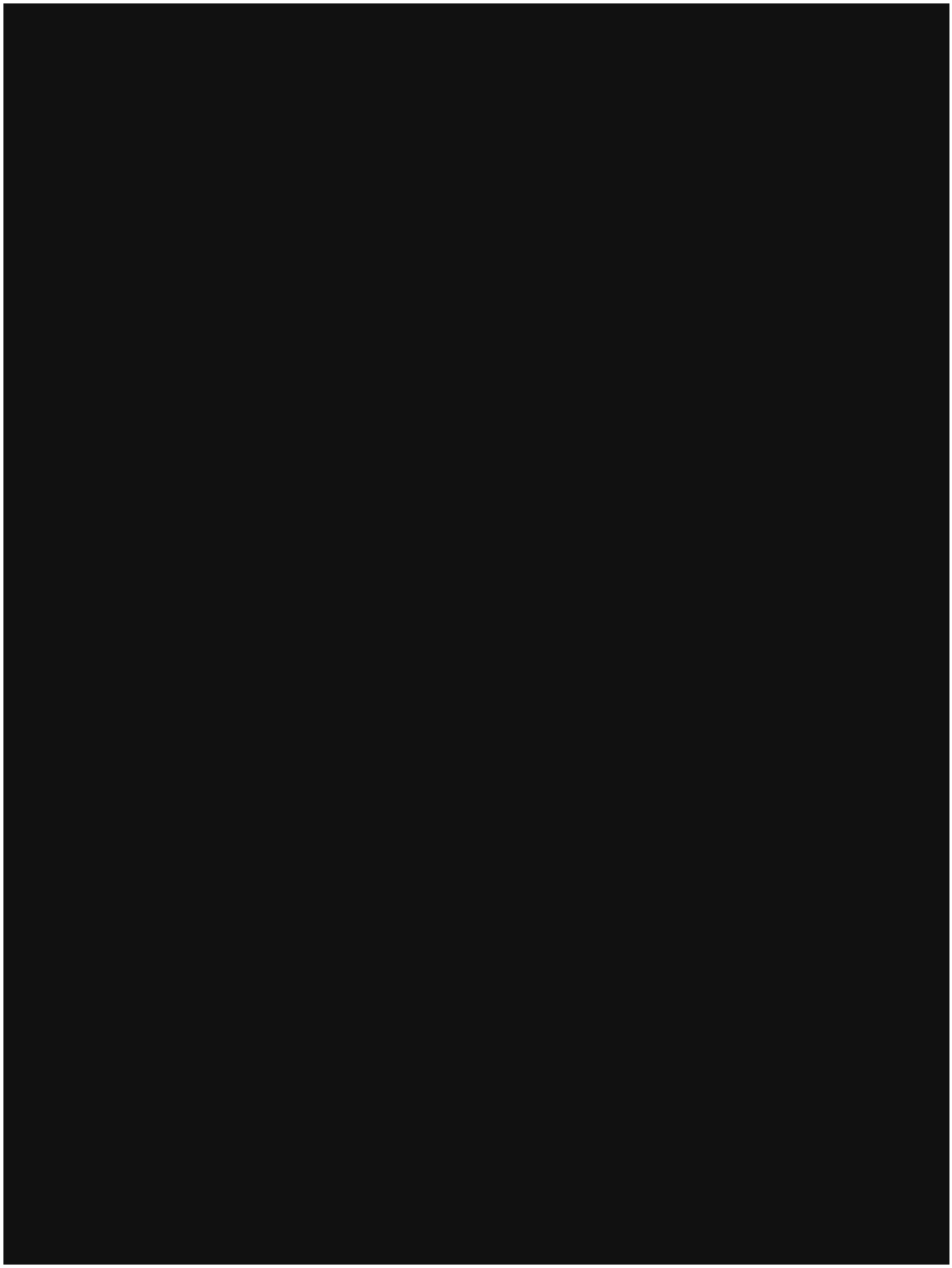
Die Social Engineering Kampagne “Moment mal”.

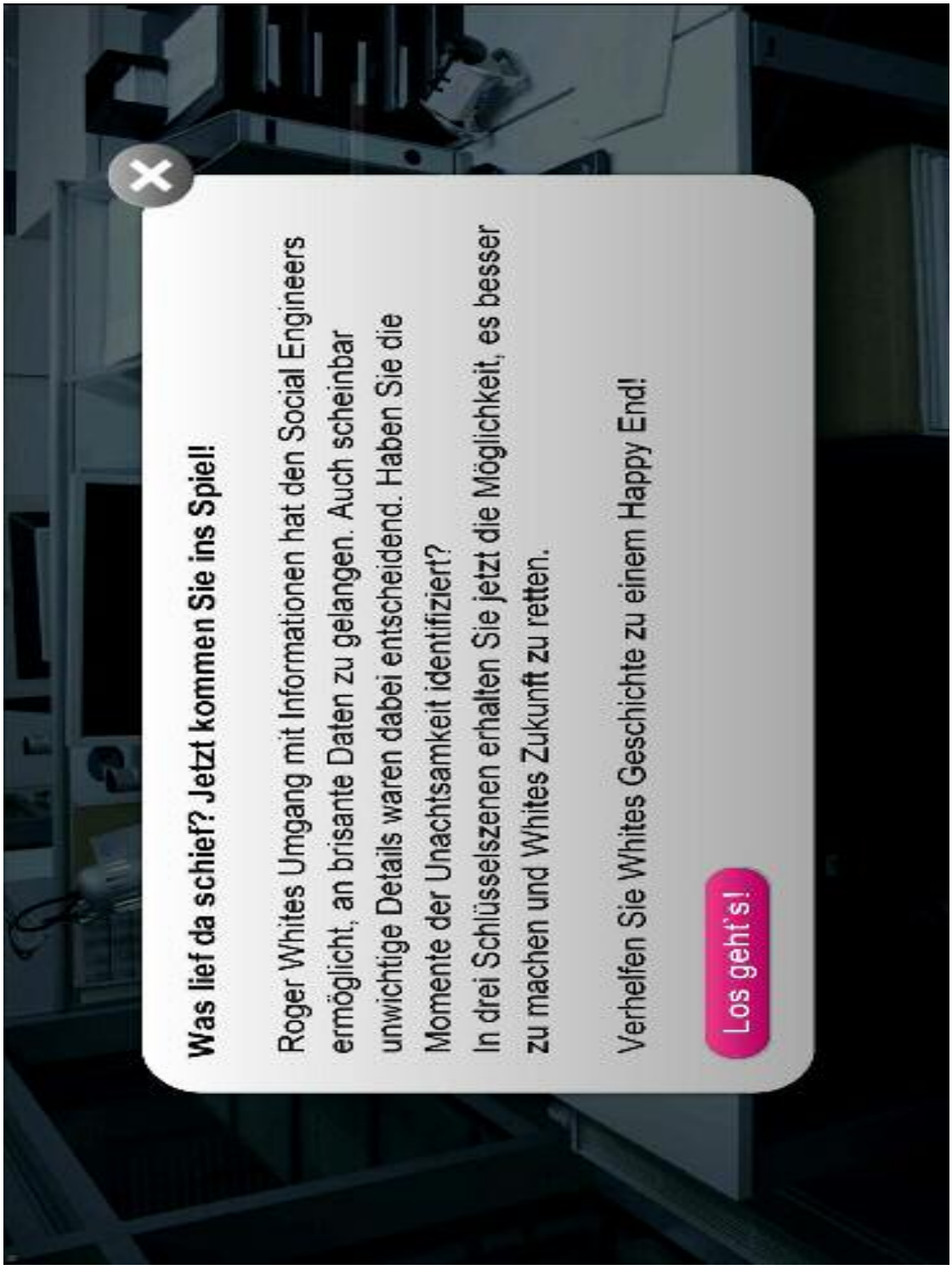
Deutsche Telekom AG, Group Business Security.

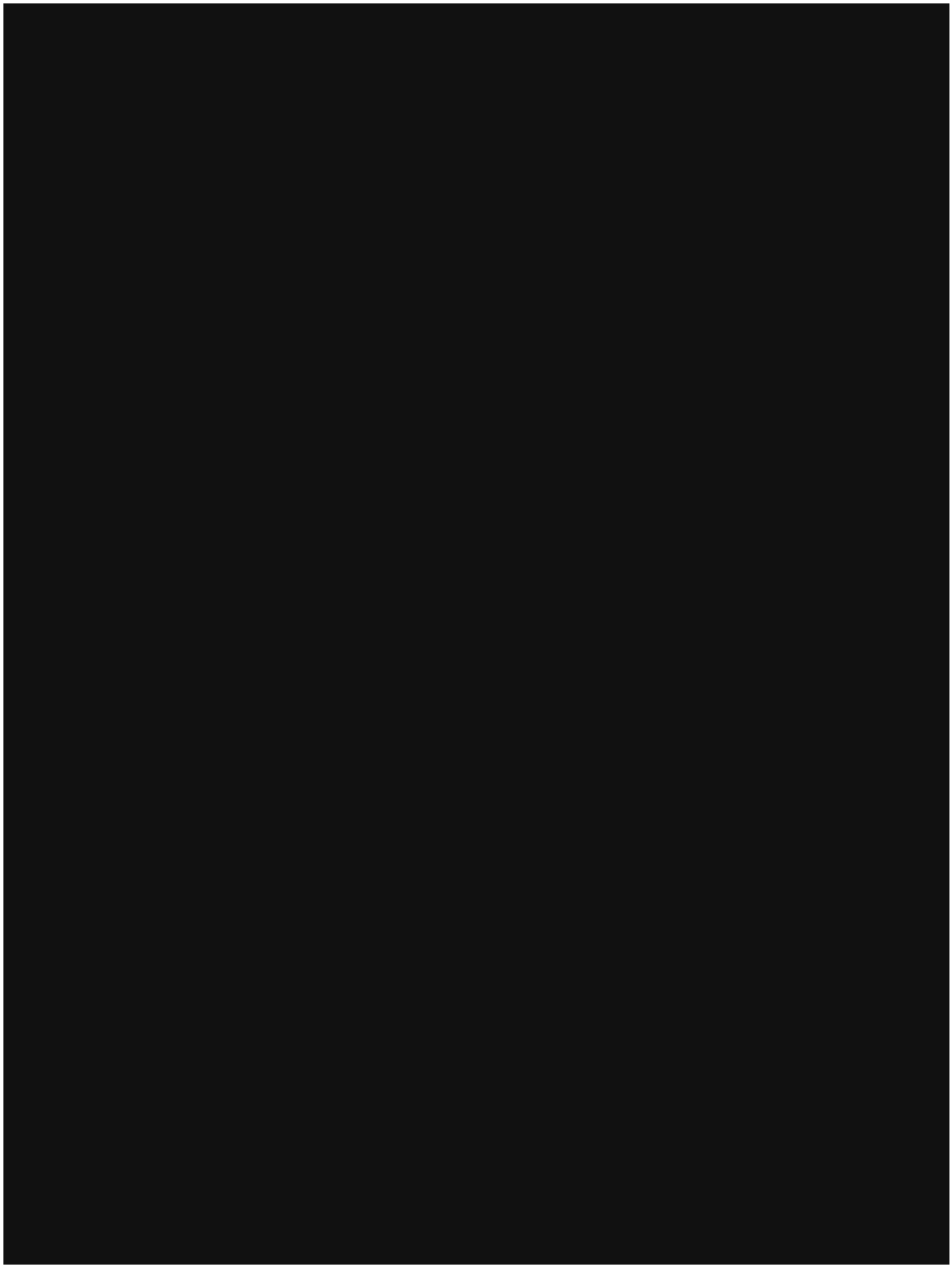
BLUFF CITY – DER FILM: EIN WAHRER HOLLYWOOD - THRILLER

Film ab…

BLUFFCity
THE MOVIE
BLUFF CITY - DER FILM
ERLEBEN, WAS VERBINDET.

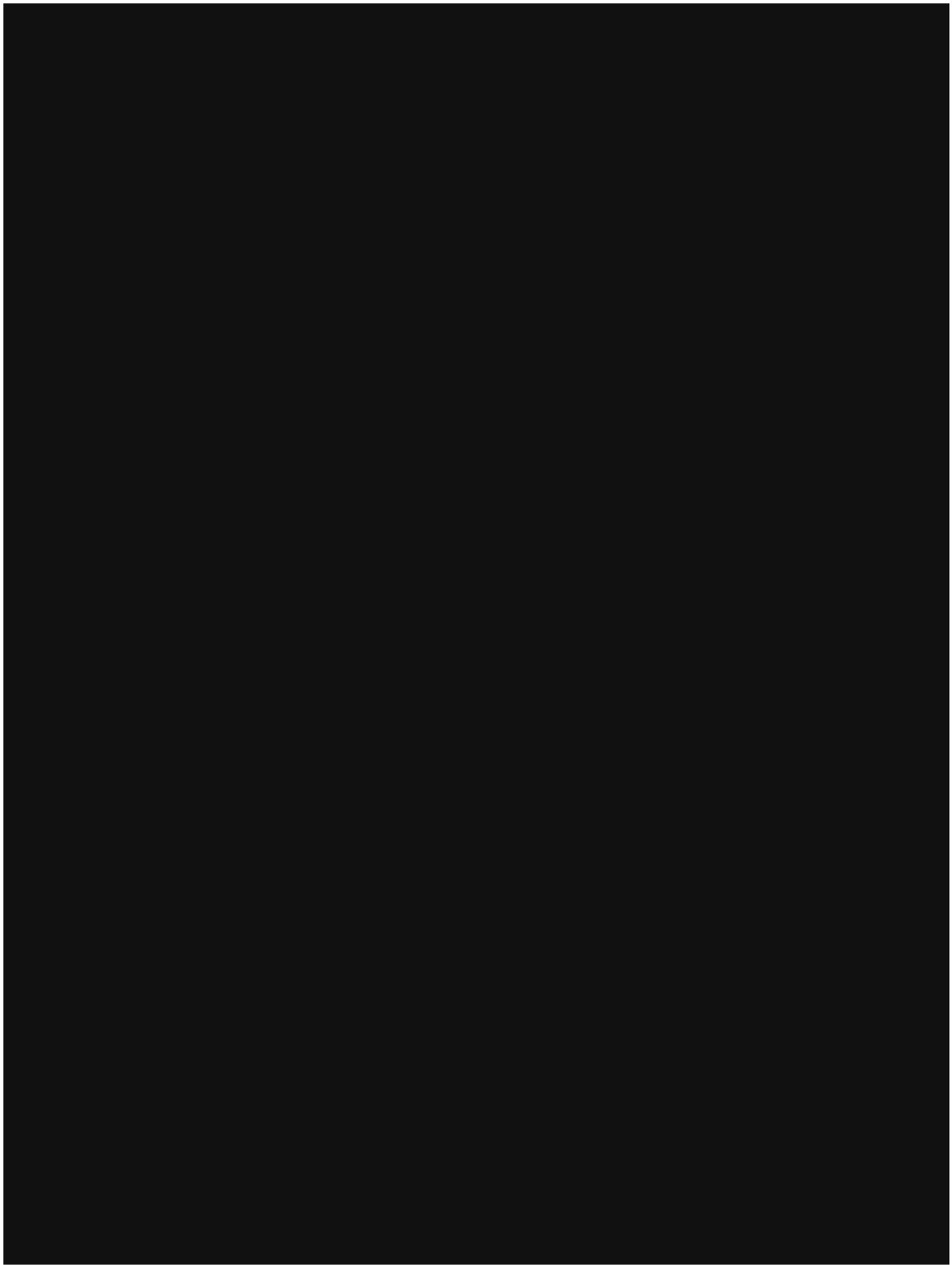



Was lief da schief? Jetzt kommen Sie ins Spiel!
Roger Whites Umgang mit Informationen hat den Social Engineers ermöglicht, an brisante Daten zu gelangen. Auch scheinbar unwichtige Details waren dabei entscheidend. Haben Sie die Momente der Unachtsamkeit identifiziert?
In drei Schlüsselszenen erhalten Sie jetzt die Möglichkeit, es besser zu machen und Whites Zukunft zu retten.
Verhelfen Sie Whites Geschichte zu einem Happy End!
Los geht's!

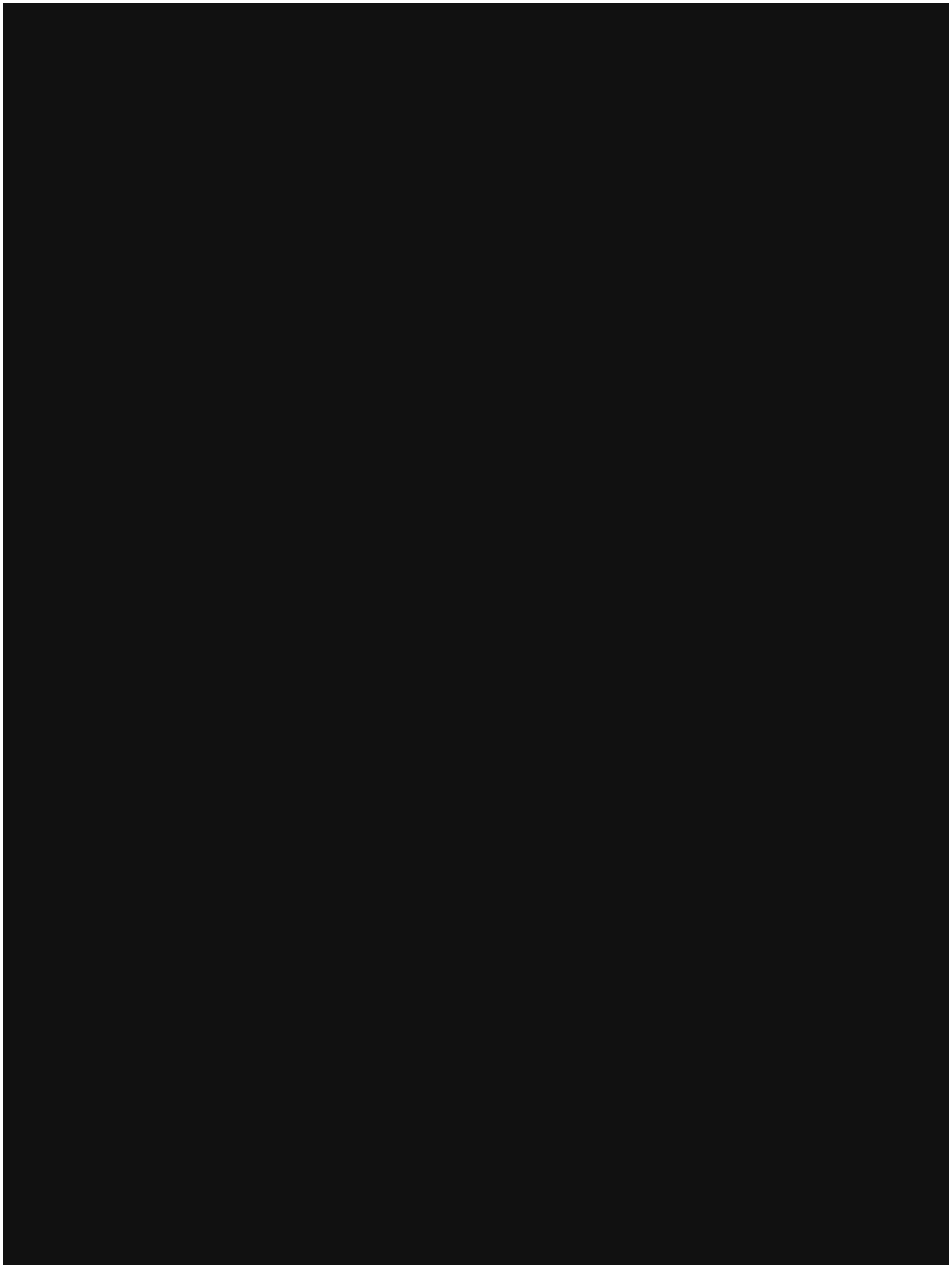


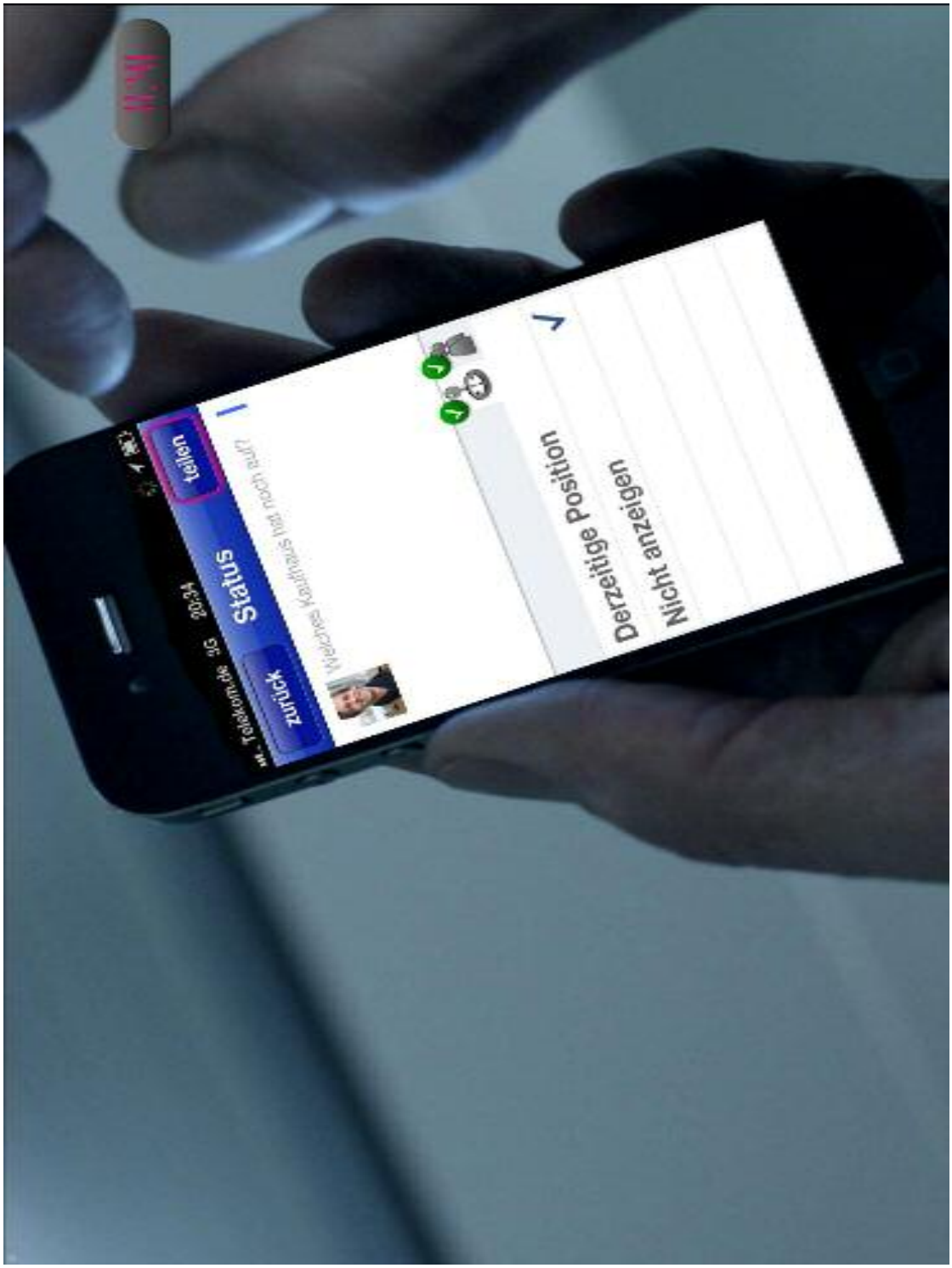
Arbeitsplatz absichern.
Auch in stressigen Situationen ist es wichtig, Ihren Arbeitsplatz beim Verlassen vor Fremdzugang zu schützen. Sie sollten dabei auf digitale und analoge Informationen achten.
Entdecken Sie mit Ihrem Mauszeiger Objekte auf Whites Schreibtisch, die sensible Informationen enthalten und sehen Sie, wie diese vor Fremdzugang gesichert werden können.
Los geht`s!
WEITER

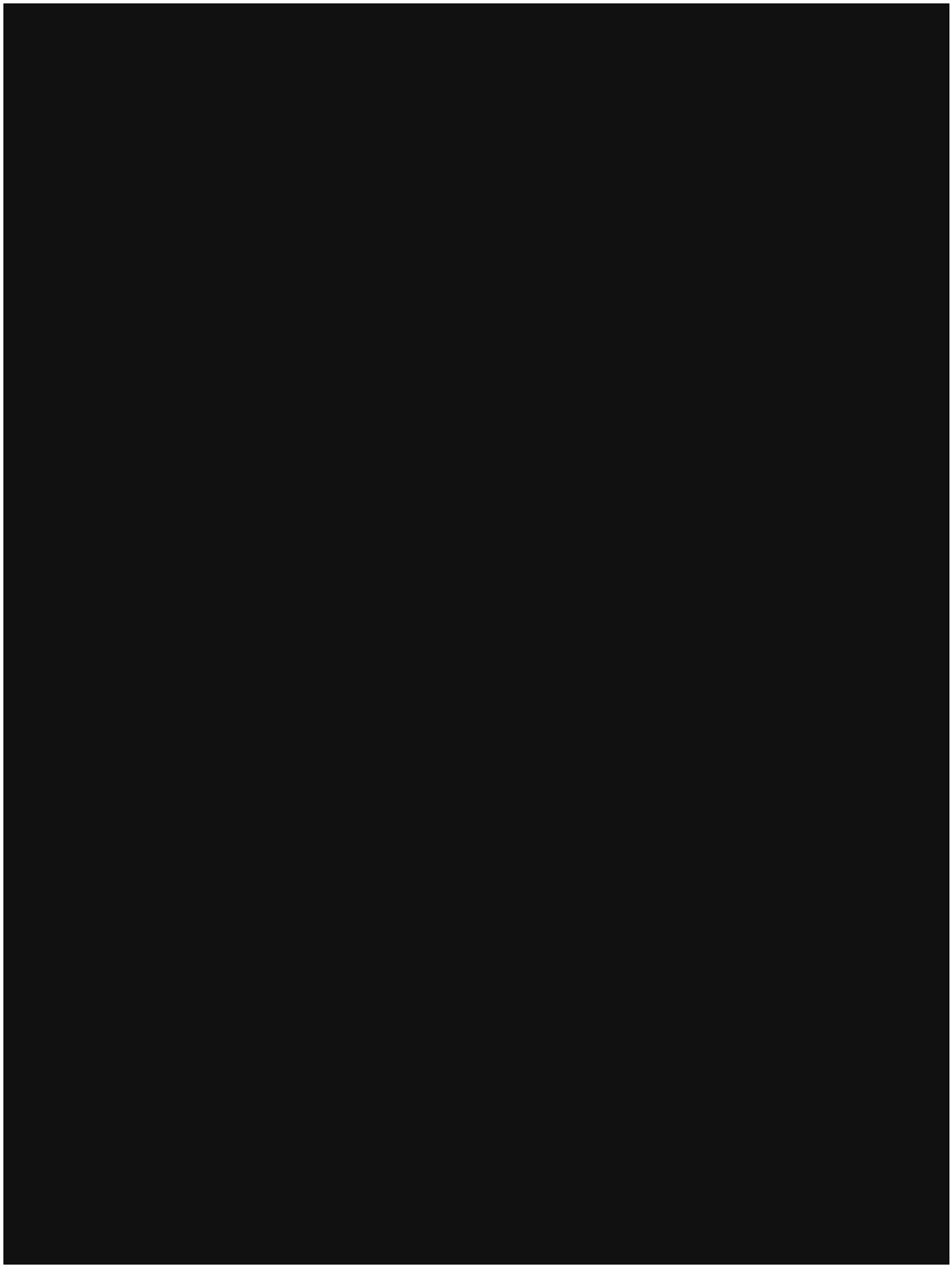

WEITER
Jahresbericht 2011



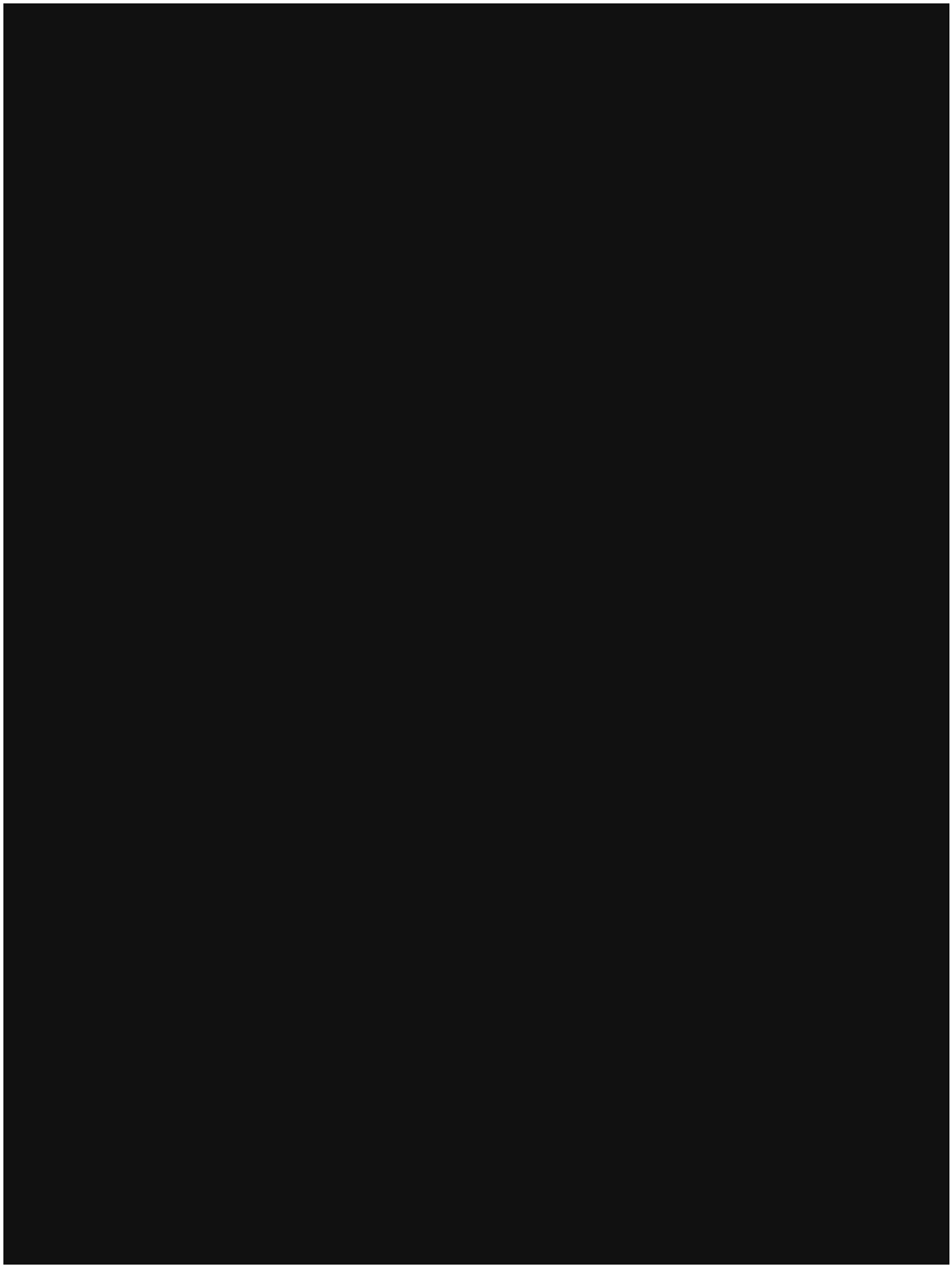

15:00
WEITER

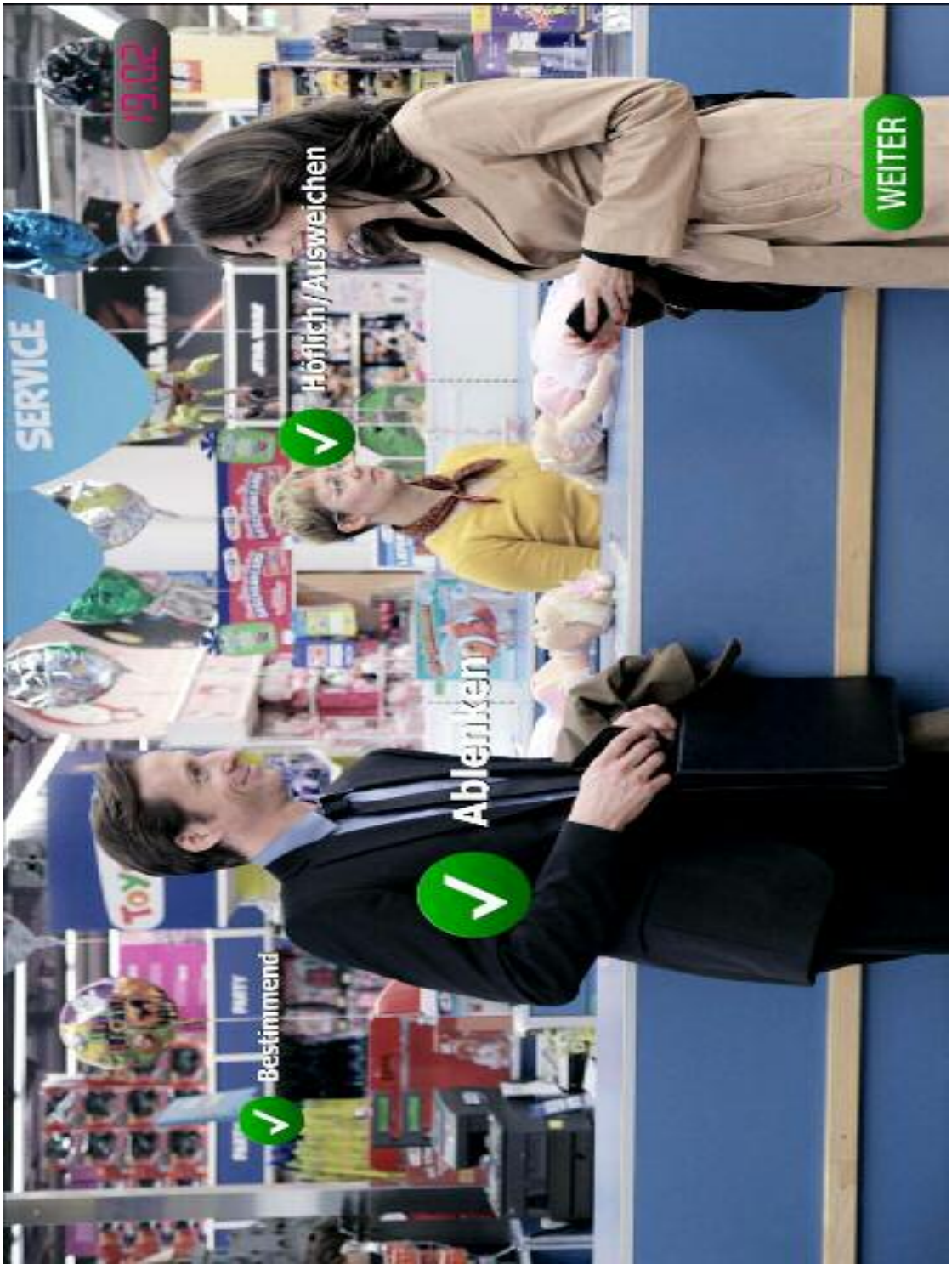


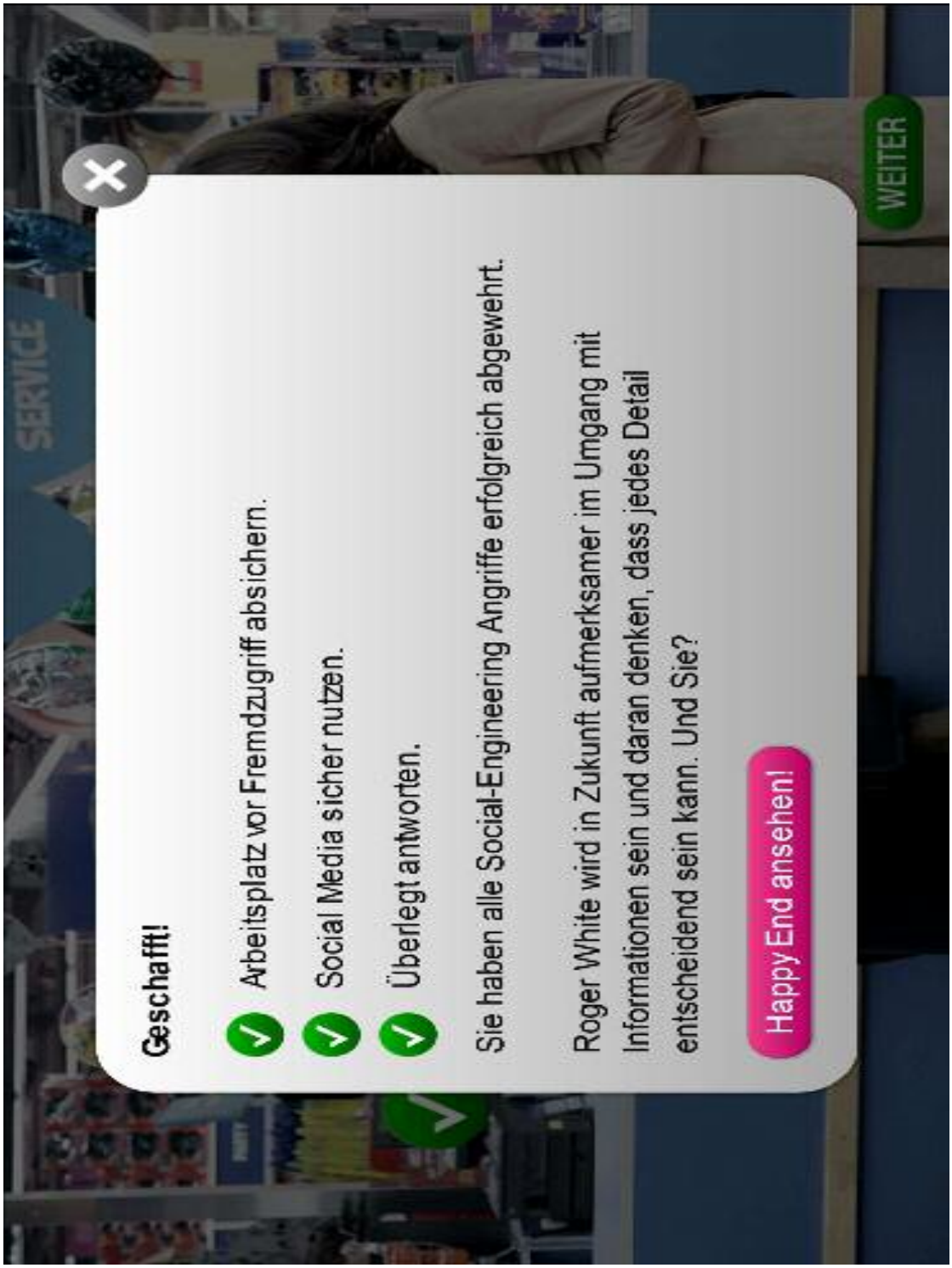

zurück
Status
teilen
Derzeitige Position
Nicht anzeigen

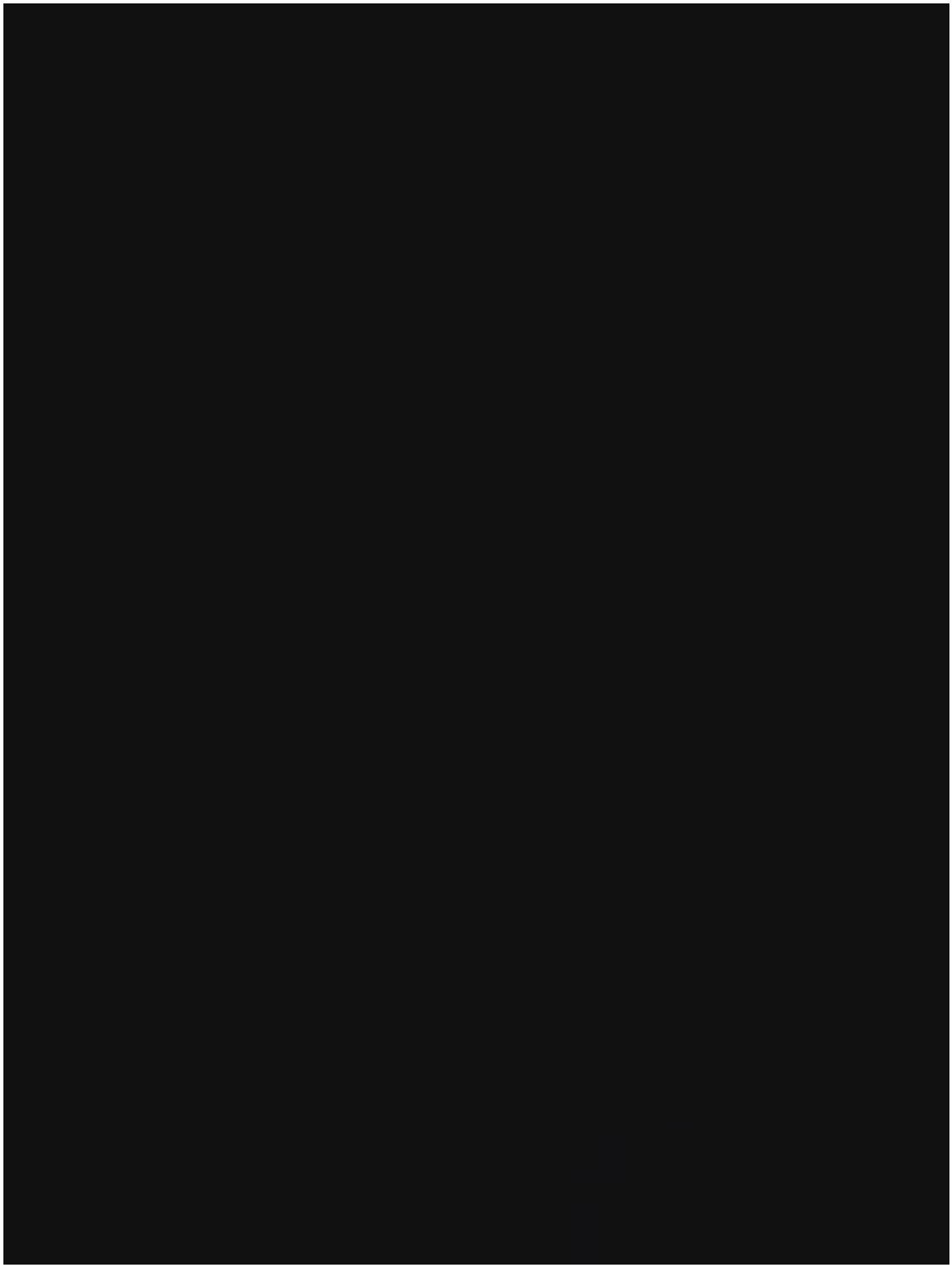



SERVICE
16,25
Ablenken
Beeinflussend
WEITER




Bestimmend
Ablenken
Höflich/Ausweichen
WEITER
SERVICE
19.02


SERVICE
Geschafft!
Arbeitsplatz vor Fremdzugriff absichern.
Social Media sicher nutzen.
Überlegt antworten.
Sie haben alle Social-Engineering Angriffe erfolgreich abgewehrt.
Roger White wird in Zukunft aufmerksamer im Umgang mit Informationen sein und daran denken, dass jedes Detail entscheidend sein kann. Und Sie?
Happy End ansehen!
WEITER



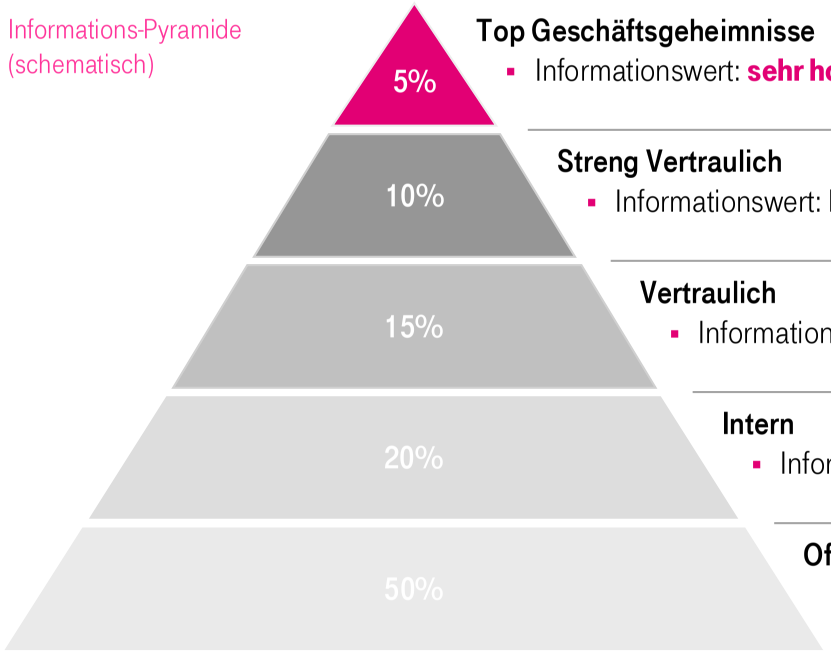
DIE „MOMENT MAL“ MAßNAHME: PRÄVENTION UND LÖSUNGSANSATZ

Exemplarisches Beispiel

DIE BESCHAFFUNG VON VERTRAULICHEN INFORMATIONEN KANN ÜBER VIELE WEGE ERFOLGEN

INFORMATIONEN SIND ABHÄNGIG VON IHRER WICHTIGKEIT ZU KENNZEICHNEN

Informations-Pyramide (schematisch)



Top Geschäftsgeheimnisse
- Informationswert: **sehr hoch**

Streng Vertraulich
- Informationswert: hoch

Vertraulich
- Informationswert: mittel

Intern
- Informationswert: niedrig

Offen
- Informationswert: sehr niedrig

TOP GESCHÄFTSGEHEIMNISSE SIND BESONDERS ZU SCHÜTZEN

Bedrohung

Nachrichtendienste und Wettbewerber

Herausforderung

Schutz der Top-Geschäftsgeheimnisse

Lösung

Maßgeschneiderte Sicherheitsmaßnahmen

- Schutzmaßnahmen
  - Technisch
  - Nicht-Technisch
- Spezielle Awareness-Programme

Überleitung Top Business Secrets / AHS Lauschabwehr

(Folie ausgeblendet)

ANGEZAPFT – ABGEHÖRT – ABGEZOCKT
BEISPIELE AUS DER GESCHÄFTSWELT

Im Meeting

ANGEZAPFT – ABGEHÖRT – ABGEZOCKT
BEISPIELE AUS DER GESCHÄFTSWELT

Im Meeting

Am Arbeitsplatz

ANGEZAPFT – ABGEHÖRT – ABGEZOCKT
BEISPIELE AUS DER GESCHÄFTSWELT

Im Meeting

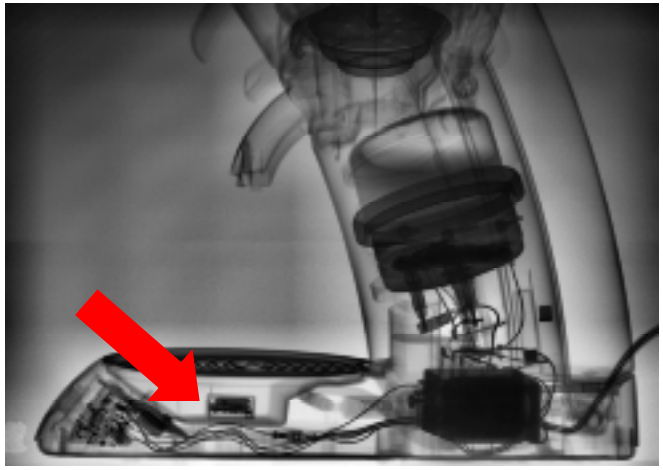
Am Arbeitsplatz

USB-Stick

PRAXISBEISPIEL (1/4)
RÖNTGENANALYSE EINER MANIPULIERTEN KAFFEEMASCHINE

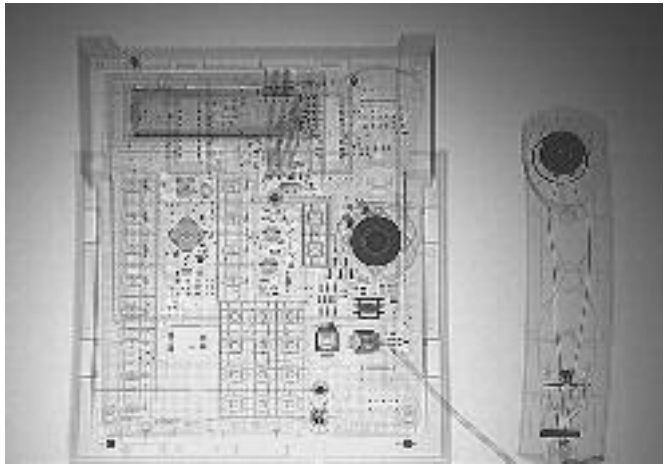
Referenzbild

Untersuchungsobjekt

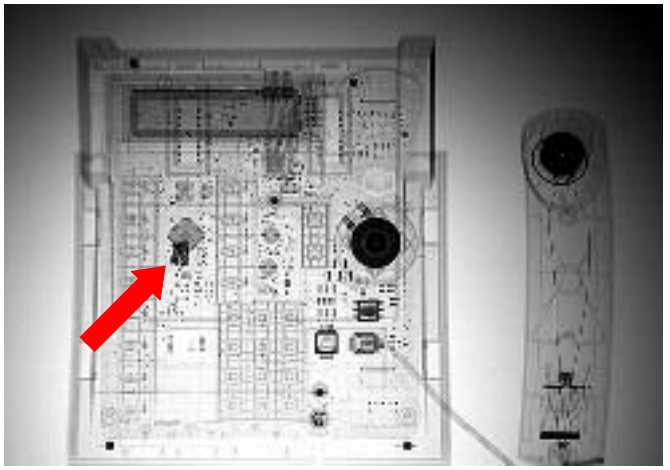


PRAXISBEISPIEL (2/4)
RÖNTGENANALYSE EINES MANIPULIERTEN TELEFONS

Referenzbild

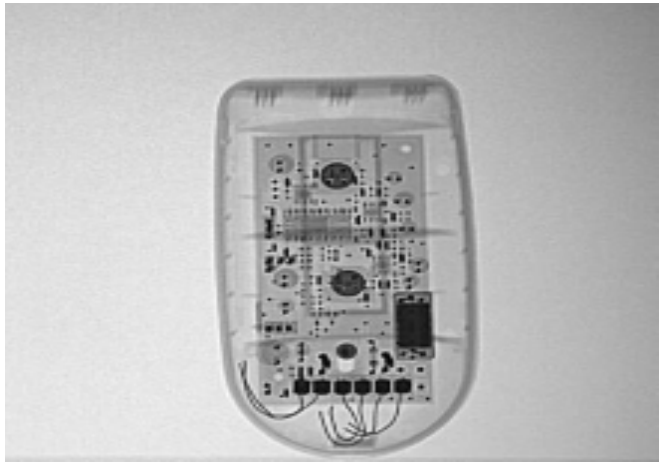


Untersuchungsobjekt

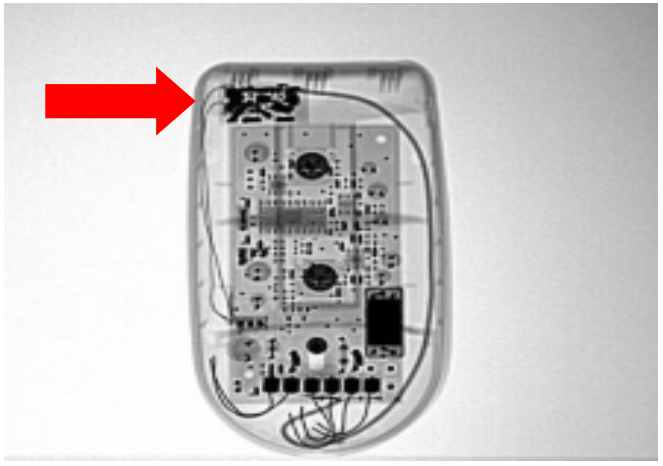


PRAXISBEISPIEL (3/4)
RÖNTGENANALYSE EINER MANIPULIERTEN COMPUTERMAUS

Referenzbild

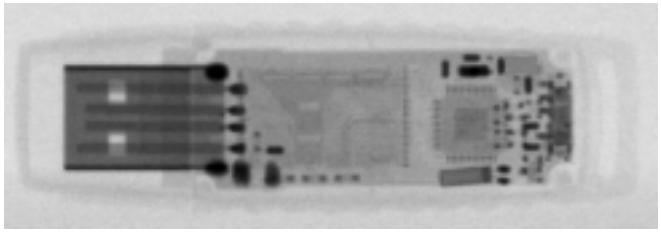


Untersuchungsobjekt

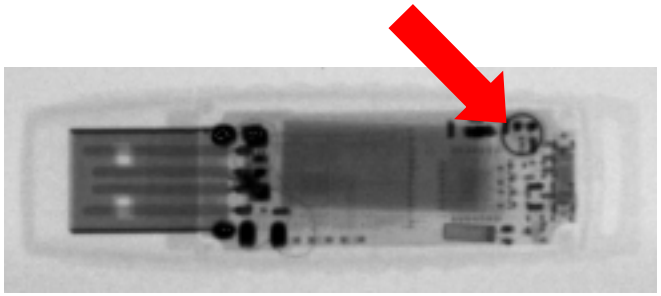


PRAXISBEISPIEL (4/4)
RÖNTGENANALYSE EINES MANIPULIERTEN USB-STICKS

Referenzbild



Untersuchungsobjekt



ES GIBT MÖGLICHKEITEN DEN SCHUTZ IHRER TOP-GESCHÄFTSGEHEIMNISSE ZU ERHÖHEN

Know-How ist die Basis Ihres Unternehmenserfolg

- Stärken Sie das Sicherheitsbewußtsein Ihrer Mitarbeiter
- Legen Sie die Anforderung zum Schutz Ihrer Top-Geschäftsgeheimnisse fest
- Schützen Sie Ihre „Kronjuwelen“ vor Spionageaktivitäten

GROUP BUSINESS SECURITY
KONTAKT

Deutsche Telekom AG

Manfred Strifler

Group Business Security

Leiter Sicherheits- und Business Continuity Management

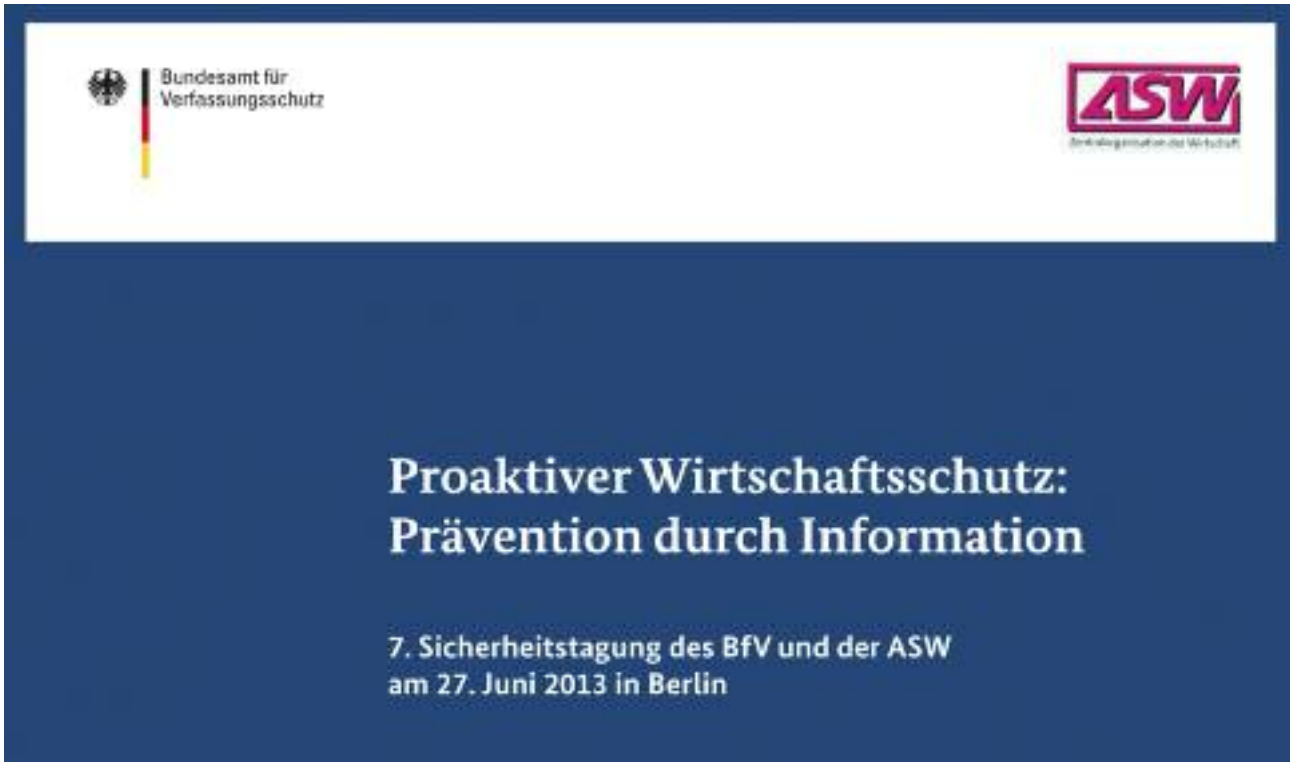
Friedrich-Ebert-Allee 140, 53113 Bonn

Tel.: +49 228 181-75626

E-Mail: manfred.strifler@telekom.de

VIELEN DANK!

Bildmaterial



Referent Mag. Martin Weiss, Ministerialrat im österreichischen BVT

Fachforen: v.l. Jörg Schulz, VON ZUR MÜHLEN`SCHE GmbH,
Stefan Tanase, Kaspersky Lab., Stefan Becker, LKA NRW

Abschlussdiskussion mit den Referenten

Wirtschaftsschutz
ist
Teamwork