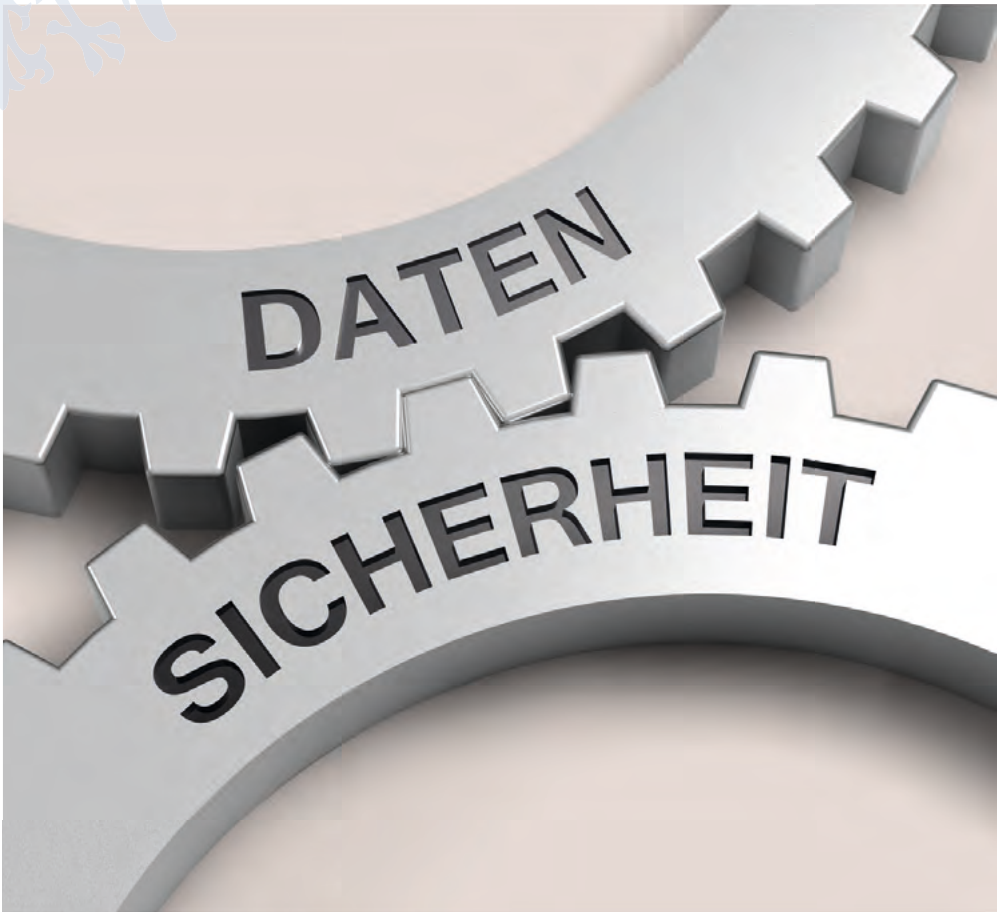
GEFAHRENATLAS DATENSICHERHEIT

STICHWORTSAMMLUNG MIT HINWEISEN



IHK Industrie- und Handelskammer Frankfurt am Main

INHALT

Vorwort 4

I. Anleitung zur Interpretation des Gefahrenatlasses 5

II. Gefahrenatlas – ABC für Datensicherheit 6

III. Verweise auf Institutionen, hilfreiche Dokumentationen 28

IV. Empfehlungen der Projektgruppe Datensicherheit 32

Impressum 33

VORWORT

Eine repräsentative Umfrage im Auftrag des Digitalverbandes Bitkom e.V. unter mehr als tausend Sicherheitsexperten in verschiedenen Unternehmen (Quelle: Public Security News, 4. Juli 2015) erbrachte detaillierte Ergebnisse zu Phänomenen der Bedrohung durch IT-Wirtschaftskriminalität. Danach besteht bei 60 Prozent der Unternehmen in Deutschland die Auffassung, dass diese nicht ausreichend gegen Datendiebstahl, Wirtschaftsspionage oder Sabotage geschützt sind. Hierzu passt auch die Äußerung des DIHK-Präsidenten Dr. Eric Schweitzer in einer Pressemitteilung im August 2014: „Großkonzerne sind sich der Risiken der Industriespionage in der Regel viel bewusster als kleinere Unternehmen und wappnen sich entsprechend. Diese Sensibilisierung müssen wir auch bei kleineren und mittleren Unternehmen noch stärker erreichen."

Gerade dieses Ziel verbindet die Projektgruppe „Datensicherheit" des IHK-Ausschusses Wirtschafts- und Unternehmensberatungen mit dem vorliegenden Gefahrenatlas. Er versetzt interessierte Unternehmen aus dem Kammerbezirk in die Lage, notwendige Awareness-Initiativen auf Basis vorhandenen Informationsmaterials zum Thema IT- und Datensicherheit durchzuführen. Wir wollen damit auch der Erfahrung Rechnung tragen, dass die Sicherheit der Unternehmen in einer digitalen Welt nicht von der Technik selbst bedroht wird, sondern vielmehr von den Menschen, die die Technik noch immer unbedarft nutzen. Folglich ist auch hier der Ansatz zur entsprechenden Prävention zu finden. Der Gefahrenatlas ist als Sammlung potenzieller Gefahrenquellen zu sehen, zu denen es Hinweise gibt, wie vertiefend eingestiegen werden kann.

I. ANLEITUNG ZUR INTERPRETATION DES GEFAHRENATLASSES

Der Gefahrenatlas spricht eine große Vielfalt von Bereichen wie

- Unternehmen
- Geschäftspartner
- Mitarbeiter
- Gesetze
- Behörden
- Technologielieferanten
- Internetserviceanbieter

an, die jeweils ausführliche Betrachtungen wert wären.

Für die Kompaktheit und Übersichtlichkeit wurden die Hinweise in die Tabelle „ABC für Datensicherheit" strukturiert und sehr knapp formuliert zusammengefasst. Für die Erläuterung fremder Begriffe kann man die Internet-Suchmaschinen zu Rate ziehen.

Die Tabellenspalte „Hilfe geben" soll Hinweise auf Experten liefern, die in mittleren und großen Unternehmen in den genannten Organisationseinheiten (z.B. Personal, IT-Experten, Datenschutz usw.) zusammengefasst sind. Auf weitergehende Differenzierungen zu den Organisationseinheiten in größeren Unternehmen, wie z.B. Grundsatzabteilung, Risikomanagement, Compliance, Revision, Providermanagement usw., wurde hier bewusst verzichtet.

Kleine und mittlere Unternehmen verfügen oft nicht über diese Organisationseinheiten und werden sich bei Bedarf an externe Dienstleister mit der genannten Expertise wenden müssen.

II. GEFAHRENATLAS – ABC FÜR DATENSICHERHEIT

STICHWORTE	RISIKEN	ERLÄUTERUNGEN, HINWEISE	HILFE GEBEN
AGB	Unbedarfte Nutzung von Services, Geräten und Software ohne Kenntnis der damit verbundenen Geschäftsbedingungen kann z.B. Rechteabtretung, verdeckte Datenübermittlung bedeuten.	Es ist sehr zu empfehlen, die Allgemeinen Geschäftsbedingungen (AGB) zu beachten und bei kritischen Fragen Experten einzuschalten.	▌IT-Experten ▌Datenschutz ▌Juristen
Apps	Bisweilen ungeklärte Produktsicherheit, intransparente Nebenfunktionen, evtl. Datenweiterleitung an Unbekannt. Datenmissbrauch, oft für Werbung, unbemerkter Datentransfer über Apps (Android-/ iOS-Apps).	Sensibilisierung, Awareness-Schulung. AGB und App-Funktionen genau lesen. App-Einstellungen auf Smartphone/Tablet insbes. bzgl. Datenschutz überprüfen, anpassen. Regeln für App-Nutzung auf Mobile Devices aufstellen.	▌Personalfachleute ▌IT-Experten ▌Datenschutz
Arbeitsvertrag, Eintritt	Ein ungeregelter Eintrittsprozess birgt sehr viele Risiken für Unternehmen und Mitarbeiter.	Verpflichtungserklärung, Unterwerfungsklausel, Datenschutzerklärung, Zugangsrechte, Offenlegung Nebentätigkeiten. Einweisung in Verantwortlichkeiten im Unternehmen, geltende Regeln, Prozesse, Arbeitsmittel, wo erhält man Hilfe und Auskunft.	▌Personalfachleute ▌IT-Experten ▌Datenschutz
Arbeitsvertrag, Austritt	Ein ungeregelter Austrittsprozess birgt sehr viele Risiken für Unternehmen und Mitarbeiter.	Checkliste, Laufzettel, Abgabeüberwachung, Vollständigkeitserklärung, Postfachüberwachung, Zugangsrechte aktualisieren. Rückgabe von Arbeitsmitteln und Daten. Übergabe von internen/ externen Kontakten.	▌Personalfachleute ▌IT-Experten ▌Datenschutz
Audio- und Fotoaufnahmegeräte	Fotos, Audioaufnahmen, offene/geheime Mitschnitte.	Nutzerordnung, Gebrauchsregeln Dos/Don'ts, Benutzercodierung, Zugangsprotokoll führen. In einer Besucherregelung die Nichtbenutzung bzw. temporäre, geschützte Verwahrung von Aufnahmegeräten berücksichtigen.	▌IT-Experten ▌Securitymanagement ▌Abteilung Öffentlichkeitsarbeit
Audits, Überprüfung	Unterlassung von Überprüfungen lässt Risiken unentdeckt.	Regeln zur Überprüfung der Sicherungsmaßnahmen, z.B. durch Revision, IT-Sicherheitsbeauftragte, Datenschutzbeauftragte.	▌IT-Experten ▌Securitymanagement
Awareness, Security-Awareness	Mangelnde Aufmerksamkeit, Sorglosigkeit, Kontrollverlust.	Sensibilisierung durch Regeln und Schulung. Ohne Risikokenntnisse keine Risikovorsorge möglich.	▌IT-Experten
Benutzer	Missbrauch durch unberechtigte Datenzugriffsrechte, oft durch neue Aufgabenzuordnungen oder Unachtsamkeit bei der Vergabe von Rechten.	Berechtigungskonzept durch Organisation, Personal, IT erarbeiten, lfd. aktuell halten, mit Veränderungen im Verantwortungsbereich synchronisieren, Recht einbeziehen.	▌Organisation ▌Personalfachleute ▌IT-Experten
Berechtigungen	Siehe Benutzer.		

STICHWORTE	RISIKEN	ERLÄUTERUNGEN, HINWEISE	HILFE GEBEN
Besucher, Gäste	Spionage, Ausspähungen. Einblicke in das Unternehmen, in Dokumente, Fotos, Aushänge (Lauschangriff von innen und außen).	Besucherregelung für Netzwerkzugang, Zutritt, Registrierung, Einblick, Begleitung/Aufsicht. Awareness-Schulungen, Sensibilisierung der Mitarbeiter. Hinterlegung von risikobehafteten Geräten (Audio, Foto) der Besucher.	▌Organisation ▌Personalfachleute ▌IT-Experten ▌Besucher-Empfang
Bürogeräte, Nutzung	Spionage, Ausspähungen, Missbrauch. Sensible Daten öffentlich zugänglich bzw. gespeicherte Daten von Unberechtigten leicht reproduzierbar.	Einsatz Codekarten. Sensibilisierung, Awareness-Schulungen.	▌IT-Experten
Bürogeräte, Wartung	Missbrauch des Datenspeichers von Kopierer, Scanner, Fax, Beamer usw., unkontrollierte Fernwartungszugänge, Manipulationen.	Regeln für Wartungsdienste, Fernwartungszugänge, Aufsicht. Bei Austausch alle Daten löschen, ggfs. vorher sichern.	▌IT-Experten
BYOD (Bring your own device)	Aushebeln der Unternehmenssicherheit, da private Endgeräte vom Arbeitgeber nur sehr bedingt kontrollierbar sind. Verbindung mit der Unternehmens-IT ohne Beachtung der Sicherheitsregeln.	Grundsätzlicher Ausschluss oder sehr gut geregelter Anschluss an das Unternehmensnetz. Unternehmen haben sehr begrenzte Rechte bei privaten Geräten. In den USA schon Abwärtstrend zu Non-BYOD.	▌IT-Experten ▌Juristen
Cloud-Nutzung	Überwiegend unbekannte Datenlagerungsorte. Oft fremder Rechtsraum mit unbekannten und unzureichenden Rechtsnormen.	Bedingungen für Datenlagerung und -umzüge klären. Aufklärung zu Datenverwalter und -verwendung, AGB beachten etc. Auf unbekannte Rechtsnormen achten. Mindestschutz: Datenverschlüsselung, Kontrollen.	▌IT-Experten ▌Juristen
Compliance	Normverletzungen, regelwidriges Verhalten, Störungen der Geschäftsabläufe, evtl. schwerwiegende Schäden, Gefährdung des Firmenvermögens.	IT-Compliance-Regeln (gesetzliche, unternehmensinterne, moralisch-ethische Regeln) aufstellen, Schulungen, Kontrolle, Compliance-Checks. Ggfs. Kontrolle durch Whitehacking.	▌Juristen ▌Personalfachleute ▌Orga-/IT-Experten ▌Datenschutz
Cybercrime	Kriminelle Handlungen unter Nutzung von IT (Hardware, Software). Unterwanderung der Sicherheitsbarrieren.	Auffälligkeiten beobachten, Prävention, Virenschutz, E-Mail-Anhänge fremder Absender nicht öffnen, Risikoprozesse identifizieren und Kontrollen sicherstellen, nur Software aus vertrauenswürdigen Quellen installieren, keinen Anweisungen von Anrufern folgen, unbekannte Sachverhalte mit hoher Skepsis prüfen.	▌IT-Experten ▌Landesämter für Verfassungsschutz ▌Landeskriminalämter ▌Bundeskriminalamt ▌IT-Verbände ▌Internetseite des BSI
Cyberspace	Siehe Cloud-Nutzung		
Daten (versteckt in Dokumenten)	Vertraulichkeitsverletzungen, unbeabsichtigte Offenlegung von Datenquellen, Imageverlust.	Unbekannte, automatisch gespeicherte, versteckte Informationen, z.B. Dokumentbeschreibungen in MS Office (siehe Reiter Datei) Notizenblätter bei PPT-Folien zeigen Quellen und Wege der Dokumente auf. Awareness-Schulung der Anwender.	▌Organisation ▌IT-Experten

STICHWORTE	RISIKEN	ERLÄUTERUNGEN, HINWEISE	HILFE GEBEN
Datensicherheit	Mangelndes Risikobewusstsein.	Schulungsmaßnahmen, Aufklärung, Sicherungskonzept, unternehmensindividuelle Regeln aufstellen. IT-Sicherheitsbeauftragte IT-Sicherheitsgesetz, ISO 27001 https://www.bsi.bund.de	▌Juristen ▌Personalfachleute ▌Organisation ▌IT-Experten ▌Datenschutz
Datensicherungen	Datenverlust, Missbrauch, Förderung krimineller Handlungen, etwa Sabotage durch nachlässigen Umgang mit Datensicherheit/-schutz bzw. kein Datensicherheits/-schutz-Konzept.	Unternehmensspezifische Regeln, Kontrolle durch Notfallübung.	▌IT-Experten
Datenspeicher, externe	Datendiebstahl, Missbrauch, Einschleusung von Viren, Trojanern.	Unternehmensspezifische Regeln zur IT-Sicherheit für die Verwendung von USB-Sticks, SSD-Karten und vglb. Datenträgern aufstellen, Sicherheitsmaßnahmen und Kontrollen durchführen.	▌Organisation ▌IT-Experten
Datenspeicher, externe	Geräteausmusterungen mit ungelöschten Restdaten, Folgen: Vertraulichkeitsverletzungen, hohes Missbrauchsrisiko.	Regeln für sichere Datenlöschung bei endgültigem Ausmustern bzw. bei temporärer Weitergabe (Ausleihe, Wartung). Professionelle Vernichtung von Papier und Datenträgern. Separate Behälter, vertragliche Vernichtungsvereinbarung mit Entsorger.	▌IT-Experten
Datenzugriffe, extern	Datendiebstahl, Missbrauch, Einschleusung von Viren, Trojanern.	Unternehmensspezifische Regeln zur IT-Sicherheit für den Fern-Zugang auf Unternehmensdaten. Sicherheitsmaßnahmen und Kontrollen durchführen.	▌IT-Experten
Denial of Service (DoS)	Die Nichtverfügbarkeit eines Dienstes, der eigentlich verfügbar sein sollte, z.B. durch Überlastung von Infrastruktursystemen oder einen mutwilligen Angriff auf eine IKT-Komponente, kann Betriebsprozesse erheblich stören.	Aktuell erkannte Störungen sofort mit IT-Experten klären, ggfs. Unternehmensleitung informieren.	▌IT-Experten
Digitalisierung	Missbrauch, Fälschung, Manipulation durch sehr leichte, oft sorglose Vervielfältigung und Verbreitung von Daten.	Sensibilisierung der Mitarbeiter, Awareness-Schulungen mit Negativbeispielen.	▌Personalfachleute ▌IT-Experten
E-Banking	Fremder Kontozugang durch Phishing, materielle Verluste. Abgreifen von Kontozugangsdaten über Manipulationen am Geldautomaten oder dem Mobile-Phone-Verfahren mit TAN.	Aufklärung, Sensibilisierung, Bedienungsanleitungen der Banken beachten, Browserchronik und Cookies löschen.	▌Personalfachleute ▌IT-Experten ▌Kontoführende Bank
E-Mail	Dateneinblick, Missbrauch.	E-Mails bieten Experten leicht Einblicke, wie das System Postkarte leichte Einblicke Fremder ermöglicht. Kein Versand vertraulicher Daten per E-Mail. Verschlüsselung wo angebracht, unterschiedliche Krypto-Verfahren nutzen. Mitarbeitersensibilisierung ratsam.	▌Organisation ▌IT-Experten ▌Personalfachleute
E-Mail, Viren	Einfalltor für Trojaner, Vireneinschleusung.	E-Mail-Anhänge mit sehr großer Vorsicht behandeln, bei Misstrauen von IT-Experten prüfen lassen.	▌IT-Experten

STICHWORTE	RISIKEN	ERLÄUTERUNGEN, HINWEISE	HILFE GEBEN
Facebook	Siehe Apps.		
Fotogeräte	Fotoaufnahmen, geheime.	Siehe Audio, Besucher.	
Gäste (Besucher, Führung)	Siehe Besucher.		
Geschäftspartner, Dienstleister	Gefahren für Datensicherheit. Dienstleister geht fahrlässig mit Auftraggeberdaten um.	Klare Vertragsregelungen, Audits, Kontrolle, Sanktionen.	▌Organisation ▌Juristen ▌IT-Experten
Geschäftspartner, Dienstleister	Veränderungen der Dienstleistungsrahmenbedingungen ohne Abstimmung, z.B. Serverumzug, Datenverlagerung, Cloud-Nutzung.	Klare Vertragsregelungen, Audits, Kontrolle, Sanktionen.	▌Organisation ▌Juristen ▌IT-Experten
Hacking	Diebstahl, Infiltration, IT-Missbrauch, materieller Schaden, Reputationsschäden.	IT-Sicherheitskonzept, Netzsegmentierung, Virenschutz, Passwortänderungen, Schulung IT und User. Auftrag für die Suche nach Sicherheitslücken durch Whitehacking, Penetrationstests.	▌Geschäftsführung ▌IT-Experten ▌Datenschutz
Hardware	Missbrauch, Datendiebstahl durch unklare Produktsicherheit, integrierte Chip-Funktionen, unsicherer Hersteller. Hardwareausmusterung mit Restdaten.	IT-Sicherheitskonzept, Awareness-Schulungen, Gerätefunktionen (Datensammlung, -weiterleitung) genau prüfen, vor Weitergabe professionelle Datenlöschung.	▌IT-Experten ▌Datenschutz
Homeoffice	Aushebeln der Unternehmenssicherheit, da private Endgeräte vom Arbeitgeber nur sehr bedingt kontrollierbar sind. Verbindung mit der Unternehmens-IT ohne Beachtung der Sicherheitsregeln.	Klare Regeln und Schutzmaßnahmen für den Umgang mit Unternehmensdaten vom/im Homeoffice. Kontrolle.	▌IT-Experten ▌Datenschutz
Industrie 4.0	Beeinflussung digitaler Produktionssteuerung.	Datensicherungskonzept, Ausfallszenario, Frühwarnsystem, Notfallmanagement, Qualitätskontrolle.	▌IT-Experten ▌Engineering ▌Securitymanagement
Internetzugang	Materieller Schaden, Reputationsschäden. Einfalltor für Trojaner, Vireneinschleusung für den einzelnen PC sowie in das verbundene Netzwerk und an die Kommunikationspartner.	IT-Sicherheitskonzept, klare Umsetzung, regelmäßige Überprüfungen.	▌IT-Experten ▌Datenschutz ▌Juristen
Intransparenz der Abhängigkeiten	Unklare Verantwortlichkeiten für Datennutzung bergen viele Risiken = kleine Ursachen, große Wirkungen.	Intransparente Vernetzungen von Geschäftsprozessen, Infrastruktur, IKT, Daten, Mitarbeiter, Lieferanten, Kapital, Geschäftsordnung. Rollen/Berechtigungskonzept erstellen, IT-Governance überwachen. Awareness-Schulungen.	▌Personalfachleute ▌Organisation ▌IT-Experten ▌Datenschutz
IT-Governance	Beliebige Schäden durch fehlendes IT-Regelwerk, mangelnde IT-Organisation.	IT-Governance bestehend aus der Regelung von Prozessen und Organisationsstrukturen, die Unternehmensstrategie und -ziele unterstützen.	▌Personalfachleute ▌Organisation ▌IT-Experten ▌Datenschutz

STICHWORTE	RISIKEN	ERLÄUTERUNGEN, HINWEISE	HILFE GEBEN
IT-Grundausbildung	Naivität. Die beste Risikoabwehr sind informierte Mitarbeiter, Unkenntnis erhöht das Risikopotenzial erheblich.	Eine qualifizierte IT-Grundausbildung, regelmäßige Aktualisierung sorgt für Sensibilisierung sowie Awareness und bietet hohen Schutz vor Risiken.	▌Personalfachleute ▌Organisation ▌IT-Experten ▌Datenschutz
IT-Grundschutz	Nichtbeachtung der Regeln und Erfahrungen.	In der Norm ISO 27001 sowie in Erfahrungen des BSI sind Regeln aufgestellt, deren Beachtung dringend empfohlen wird.	▌IT-Experten Internet ▌BSI-Homepage
IT-Infrastruktur	Schäden durch fehlenden Überblick der HW/SW, Intransparenz der Geräte, Systeme, Anwendungen. Lizenzverletzungen.	Inventarverzeichnis, Assetmanagement durch IT-Experten.	▌IT-Experten
IT-Sicherheit	Naivität, Unbedachtsamkeit, Fahrlässigkeit, mangelndes Verantwortungsbewusstsein.	Nicht alle IT-Experten sind auch IT-Sicherheitsexperten, deren Einbezug jedem Unternehmen dringend empfohlen wird.	▌IT-Securityexperten ▌IT-Sicherheitsgesetz, ISO 27001
Kreditkarten	Finanzieller Schaden, Reputationsschaden durch Datenklau, Reproduktion, Missbrauch.	Keine vollständigen KK-Daten (Nr., Gültigkeit, Prüfziffer) unverschlüsselt speichern bzw. übermitteln. KK nicht unkontrolliert in fremde Hände geben.	▌Personalfachleute ▌Finanzabteilung
Kundendaten	Missbrauch kann hohe materielle Schäden und Reputationsschäden verursachen. Vertrags- und/oder Vertraulichkeitsverletzungen gefährden das Unternehmen.	Umgang und Aufbewahrung von Kundendaten regeln. Sensibilisierung der Mitarbeiter, Awareness-Schulungen.	▌Orga-/IT-Experten ▌Datenschutz ▌Juristen
LinkedIn	Siehe Apps.	In LinkedIn (und anderen Internetplattformen) unternehmensbezogene Informationen kontrollieren.	▌Personalfachleute ▌IT-Experten ▌Datenschutz
Messenger-dienste	Siehe Apps.	Dringende Empfehlung: AGBs dieser Anbieter genau lesen und evtl. Konsequenzen beachten.	▌Geschäftsführung ▌Personalfachleute ▌IT-Experten
Mitarbeiter	Mangelnde Sensibilisierung, mangelnde Überwachung.	Regeln für Verantwortlichkeiten/Rollen aufstellen, Berechtigungssystem etablieren, Sensibilisierung der Mitarbeiter, Awareness-Schulungen, Complianceaktivitäten, Kontrolle, Sanktionen.	▌Personalfachleute ▌IT-Experten ▌Datenschutz
Mitarbeiter	Naivität, Unachtsamkeit, mangelndes Risikobewusstsein.	Regeln für Verantwortlichkeiten/Rollen aufstellen, Berechtigungssystem etablieren, Sensibilisierung der Mitarbeiter, Awareness-Schulungen, Kontrolle, Sanktionen.	▌Personalfachleute ▌IT-Experten ▌Datenschutz
Mitarbeiter	Sabotage, Missbrauch Unternehmensdaten, Kriminalität. Datenentwendung, Verseuchung durch Kopie von Unternehmensdaten auf private PCs/Datenträger und zurück.	Regeln für Verantwortlichkeiten und Rollen aufstellen, Berechtigungssystem etablieren, Sensibilisierung der Mitarbeiter, Awareness-Schulungen, Kontrolle, Sanktionen.	▌Organisation ▌Personalfachleute ▌IT-Experten ▌Datenschutz

STICHWORTE	RISIKEN	ERLÄUTERUNGEN, HINWEISE	HILFE GEBEN
Mobiles: Smartphones, Tablets	Datenauslagerung auf bekannte/unbekannte Datenträger durch Datensynchronisation o.ä. kann Providern und App-Anbietern Einblick und Missbrauchsmöglichkeiten bieten.	IT-Sicherheitskonzept erstellen, Umsetzung regeln, regelmäßige Überprüfungen. Benutzerschulungen für Awareness und Schutzeinstellungen bei mobilen Geräten.	▌IT-Experten ▌Datenschutz
Mobiles: Smartwatch, USB-Sticks	Datenspeicher offen für unberechtigte Einblicke.	IT-Sicherheitskonzept, klare Umsetzung, regelmäßige Überprüfungen. Benutzerschulungen.	▌IT-Experten ▌Datenschutz ▌Personalfachleute
Mobile Geräte, Smartphone und -watch, Tablets	Vermischung privater und geschäftlicher Daten.	IT-Sicherheitskonzept, klare Umsetzung, regelmäßige Überprüfungen. Benutzerschulungen.	▌IT-Experten ▌Datenschutz ▌Personalfachleute
Mobile Geräte mit Aufnahme-funktionen	Unautorisierte Fotos, Audioaufnahmen für fremde Zwecke.	IT-Sicherheitskonzept, klare Umsetzung, regelmäßige Überprüfungen. Benutzerschulungen.	▌IT-Experten ▌Datenschutz ▌Personalfachleute
Mobile Geräte	Unbekannte, aktive Funktionalitäten wie automatische Datenüber-mittlungen, Ortungsdienste, Datenzugriffe von Apps.	IT-Sicherheitskonzept, klare Umsetzung, regelmäßige Überprüfungen. Benutzerschulungen.	▌IT-Experten ▌Datenschutz ▌Personalfachleute
Mobile Geräte, Apps	Siehe Apps.		▌IT-Experten ▌Datenschutz
Mülleimer	Vertrauliche Dokumente, unachtsam weggeworfen, bieten Risikopotenzial.	Sensibilisierung der Mitarbeiter, Awareness-Schulungen. Schredder, vertrauliche Aktenvernichtungsbehälter	▌Organisation ▌Datenschutz
Netzwerke	Zugriffsschutz unangemessen, nachlässig, nicht aktuell.	IT-Sicherheitskonzept. Berechtigungskonzept. Schulungen. HW-/SW-Schutz. Whitehacking, Penetrationstests.	▌IT-Experten ▌Datenschutz
Öffentlichkeit Einblick gewähren, Missbrauch fördern	Vertraulichkeitsverletzungen. Fremder Einblick durch PC-Gebrauch in öffentlichen Räumen oder durch Nutzung öffentlicher, unverschlüsselter WLAN-Verbindungen. Vertrauliche Daten in Telefonaten in der Öffentlichkeit nennen.	IT-Sicherheitskonzept, IT-Governance. Sensibilisierung der Mitarbeiter, Awareness-Schulungen. Schutzgeräte, Schutzartikel, Schutzmaßnahmen.	▌Organisation ▌IT-Experten ▌Datenschutz ▌Personalfachleute
Organisation (Intransparenz der Abhängigkeiten)	Siehe IT-Governance.		▌IT-Experten ▌Datenschutz
Papierkorb (elektronisch)	Vertraulichkeitsverletzungen. Ermöglicht die Rekonstruktion gelöschter Daten, sofern nicht geleert. Papierkorbleerung nach Benutzung fremder PCs.	Überprüfung der eigenen Arbeitsmethoden. Sorgfältiger Umgang mit dem elektronischen Papierkorb.	▌IT-Experten ▌Datenschutz

STICHWORTE	RISIKEN	ERLÄUTERUNGEN, HINWEISE	HILFE GEBEN
Papierkorb (physisch)	Siehe Mülleimer.		▌Organisation ▌Datenschutz
Passwort	Fremder Zugang zu eigenen Daten, Systemen, Netzen.	IT-Sicherheitskonzept, IT-Governance. Sensibilisierung der Mitarbeiter, Awareness-Schulungen. Regelmäßige Passwort-Wechsel.	▌IT-Experten ▌Datenschutz
PCs, Notebooks	Missbrauch, Sabotage usw. durch nachlässige Bedienung von Zugangssicherungen.	Siehe Passwort.	▌IT-Experten ▌Datenschutz
PCs, Notebooks	Missbrauch, Sabotage durch Ausmusterung mit Restdaten.	Siehe Datenspeicher, externe.	▌IT-Experten ▌Datenschutz
PCs, Notebooks	Missbrauch, Sabotage durch Verlust ungeschützter Geräte.	Festplattenverschlüsselung, zumindest für Userdaten, einführen.	▌IT-Experten ▌Datenschutz
Personaldaten, Personendaten	Mangelnder Schutz von Personendaten. Aktivitäten in fremdem Namen mit fremden Rechten. Vertraulichkeitsverletzungen. Rechtswidrige Handlungen.	IT-Sicherheitskonzept, IT-Governance. Verpflichtungserklärungen, Sensibilisierung der Mitarbeiter, Awareness-Schulungen.	▌Personalfachleute ▌IT-Experten ▌Datenschutz
Phishing	Abgreifen von vertraulichen Daten durch Viren, Trojaner, Kamera. Beobachtung mit dem Ziel Missbrauch, kriminelle Handlungen. Gilt insbesondere für Einkäufe, Zahlungsverkehr.	IT-Sicherheitskonzept, IT-Governance. Sensibilisierung der Mitarbeiter, Awareness-Schulungen. Regelmäßige Passwort-Wechsel, Gerätefunktionen und Softwareeinstellungen kontrollieren.	▌Personalfachleute ▌IT-Experten ▌Datenschutz
Prävention (Awareness)	Unkenntnis schützt vor Schaden nicht. Die beste Risikoabwehr sind informierte Mitarbeiter, Unkenntnis erhöht das Risikopotenzial sehr erheblich.	Die Benutzung von IT-Systemen, der Umgang mit Daten erfordert ein Mindestmaß an IT-Kenntnissen und Fähigkeiten, die jeder Benutzer erlernen muss. Diese Prävention ist unverzichtbar. Qualifizierungen durch IT-Schulungen, Seminare, Internetangebote wie Webinare, Videos usw.	▌Personalfachleute ▌IT-Experten
Quelle	Unbekannte Quellen bergen hohe Sicherheitsrisiken, z.B. Viren-/Trojaner-Import durch das Öffnen von Mailanhängen unbekannter Absender.	Gesundes Misstrauen, Verlässlichkeit der Quelle prüfen, Spam-Filter, Awareness-Aktivitäten, Sensibilisierung, IT-Schulung.	▌IT-Experten ▌Personalfachleute
Rechte	Mögliche Straftaten. Fahrlässige Verletzung des Urheberrechtes kann als Datenklau, Missbrauch von Daten, gewertet und verfolgt werden.	Datenschutz, Urheberrechte beachten, Datensicherheit, (BDSG, KunstUrhG, StGB, Gebührenpflichtigkeit, Persönlichkeitsrechte), Kenntnis einschlägiger Rechtspositionen, Unrechtsbewusstsein entwickeln. Geschäftsanweisung, Schulung durch Juristen, anwaltlicher Rat.	▌Juristen ▌Datenschutz

STICHWORTE	RISIKEN	ERLÄUTERUNGEN, HINWEISE	HILFE GEBEN
Risikomanagement (IT, Daten)	Gefahrendefinition, Präventionsmaßnahmen, Planung der Schadensbehebung, Ausfallfolgen. Cyberattacken aus den eigenen Reihen sind keine Ausnahme.	Überwachung von Rechtsverletzungen durch IT-Angriffe, Cybercrime, Ansprechperson für Verdachtsfälle, IT-Beauftragte, Compliance, Festlegung von Informationswegen, Beteiligung Betriebsrat, Cyber-Security-Standards, VdS-Richtlinie 3473 „Standard bei Implementierung eines Managementsystems für Informationssicherheit (ISMS)".	▌Organisation ▌IT-Experten ▌Geschäftsführung ▌Juristen
Schadsoftware	Sabotage, Beeinflussung von softwareabhängigen Verfahren, IT-gesteuerte Produktionsbereiche, Veränderung von relevanten Daten usw. Ständig online bedeutet auch ständig angreifbar!	Geschäftsanweisungen, Sensibilisierung, Verdachtsraster, Überwachung. BSI-Studie „Schutz vor Cyberangriffen".	▌IT-Experten ▌Datenschutz ▌Geschäftsführung
Schulung	Wenig informierte Anwender können hohe Risiken verursachen.	IT-Ausbildung ist die Grundlage für Verständnis und Vorsicht.	▌IT-Experten
Schutzbedarfsanalyse	Kritische IT-Bereiche (Software, Hardware, Netze) sind nicht identifiziert und daher nicht ausreichend geschützt.	Die Schutzbedarfsanalyse wird in der Regel durch einen externen Experten durchgeführt. Im Rahmen der Schutzbedarfsanalyse werden die Einheiten identifiziert, die kritisch für das Unternehmen sind und daher eines besonderen Schutzes bedürfen. Die IT-Sicherheit muss dafür noch stärkere Schutzmechanismen umsetzen als für andere Einheiten.	▌Organisation ▌Sicherheitsberater mit Spezial-know-how
Sensibilität	Siehe Awareness		▌IT-Experten ▌Geschäftsführung ▌Compliance Revision
Server	Ausmusterung, Lagerung, Veräußerung von Rechnern, Mobilgeräten sowie Zwischenspeicher mit Restdaten aufgrund von Unkenntnis (wissentlich oder durch Gleichgültigkeit). Zentrale Server und Serverräume vor unberechtigtem Zugriff schützen.	Löschung oder Austausch bzw. Vernichtung der Festplatte und der Daten auf einem Zwischenspeicher; Zutittsregelung für Serverraum, besondere Verschluss-Einrichtungen, Beaufsichtigung von Wartungsarbeiten.	▌Organisation ▌IT-Experten ▌Securitymanagement
Social Engineering	Ausspähung, Missbrauch. Unbedarfte Verknüpfung privater mit geschäftlichen Daten. Durch aktive Teilnahme sind Daten dauerhaft im Netz, Anreize für menschliche Verhaltensschwächen werden genutzt (z.B. Imponiergehabe mit Firmendaten, Mobbing usw.).	Breites Feld für gezielte Wirtschaftsspionage, Produktausspähung und Instrumentalisierung unsensibler, unzuverlässiger Firmenangehöriger, Gefahrenhinweise, Überwachungsprogramme, Sanktionierung, Unternehmensbezogene Informationen, die von Personen erstellt wurden, überwachen.	▌IT-Experten ▌Securitymanagement ▌Verfassungsschutz ▌Polizei ▌Medien ▌Verbände der Sicherheitswirtschaft
Social-Media-Software	Datenschutzrisiken durch unbekannte Funktionen in Messengerdiensten und Social-Media-Applikationen	Siehe Social Engineering.	▌Kenntnis der AGB der Produkte

STICHWORTE	RISIKEN	ERLÄUTERUNGEN, HINWEISE	HILFE GEBEN
Software-wartungen, -updates	Unzureichende Aktualisierungen gefährden Anpassung von Standards des jeweiligen Produkts.	Softwareprodukte bieten regelmäßig Aktualisierungen durch Updates. Verbesserung der Schutzmechanismen sollte regelmäßig genutzt werden.	▌IT-Experten
Software-wartungen, -updates	Unzuverlässige Fernwartungen, Download angeblicher Schutzsoftware kann Sicherungen unterlaufen.	Zu empfehlen sind firmeneigene Wartungsvorgänge durch eigenes Personal oder Inhouse-Maßnahmen durch Dienstleister des Vertrauens (entsprechende Vertragsgestaltung, Referenzen, Zertifizierungen).	▌IT-Experten ▌Juristen ▌Revision
Software-wartungen, -updates	Kriminelle Software-Einschleusungen über Wartungsaktivitäten.	Regelung der Nutzung externer Speicher, Verwendung von Schutzsoftware, Gefahrenfrüherkennung und Verdachtsgewinnung durch Sensibilisierung, Auswertung von Warnhinweisen.	▌IT-Experten ▌Interne Kommunikation ▌Verfassungsschutz ▌Polizei ▌Medien ▌Verbände der Sicherheitswirtschaft
Software-wartungen, -updates	Schadsoftware.	Siehe Bürogeräte, Wartung.	
Soziale Netzwerke, Social Media	Siehe Social Engineering, Messengerdienste.		
Spam	Einschleusung von Viren oder Trojanern durch gefälschte E-Mails sowie Formulierung in E-Mails mit Anreizen, Anlagen mit Schadinhalten zu öffnen.	Die erhebliche Gefahr liegt darin, dass der Angriff auf Daten, Datenfluss und Datenbeeinflussung usw. nicht ohne weiteres erkannt wird. Spam-Filter, Warnhinweise und Sensibilisierung sind erforderlich.	▌IT-Experten
Speichermedien	Nutzung oder Zulassung fremder Speichermedien, USB-Sticks usw. können Schadsoftware, Viren usw. in einen Rechner oder in mobile IT-Geräte einbringen.	Siehe Softwarewartungen und -updates. Nutzungsregelung.	▌IT-Experten ▌Geschäftsführung

STICHWORTE	RISIKEN	ERLÄUTERUNGEN, HINWEISE	HILFE GEBEN
Telefon	Einbringen elektronischer Bauteile (Wanzen) in Festnetzgeräte zum Mithören sowie Aufzeichnen von Gesprächen im Rahmen von Spionage und sonstiger Ausspähung.	Bei Verdachtsfällen Absuche nach Veränderungen im und am Gehäuse, Inanspruchnahme von Spezialisten zur Abklärung. Büroanordnung zur Nutzung und zum Verschluss sensitiver Räume.	▌IT-Experten ▌TK-Experten
Telefonanlagen (analog und VoIP)	(Fern-)Wartungszugänge. Manipulationen bei unzureichender Zugangssicherung.	Aufklärung einfordern. Zugangssicherung einrichten, Wartungsdienst kontrollieren.	▌IT-Experten ▌TK-Experten
Telefonanlagen (analog und VoIP)	Wahlwiederholung und Anrufbeantworter können vertrauliche Daten rekonstruieren.	Sensibilisierung der Mitarbeiter, Awareness-Schulungen, Bedienungsanleitungen.	▌IT-Experten ▌TK-Experten
Terroristische Aktionen	Ausspähung, Sabotage durch Viren, Trojaner, Gewährung fremder Einblicke, Unachtsamkeit der IT-Benutzer.	Blacklist, Screening. Kenntnisnahme terroristischer Strategien und einschlägiger Warnungen, insbesondere in Bezug auf „Weiche Ziele" wie „Kritische Infrastrukturen", Sensibilisierung für atypische Vorgänge und Wahrnehmungen.	▌Geschäftsführung ▌IT-Experten ▌Securitymanagement
Trojaner	Angriffe, Ausspähung, Sabotage.	Einbringen von Schadsoftware über E-Mail-Verkehr, externe Datenträger, Hacking (vergleiche „Spam")	▌Geschäftsführung ▌IT-Experten ▌Datenschutz
Unternehmens-dokumente	Unangemessene Aufbewahrung, Verwahrung von Dokumenten und Datenträgern sowie Vernachlässigung der Sicherung von Archivräumen. Nicht vorhandene Zutrittsregelungen und offene Büroräume fördern Einblicknahme und Verlust von Dokumenten.	Überprüfung der Verwahrsicherheit, Büroordnungen, einschlägige Geschäftsanweisung und Verbesserung der Verschluss-Einrichtungen. Gesetze: § 257 HGB, § 147 AO.	▌Organisation ▌Securitymanagement
Verschlüsselung	Data Leakage. Ungewollter Datenabfluss durch unbedarfte Einsichtgewährung bei IT-Geräten, Datenträgern, E-Mails, externe Serverzugänge. Datenträger wie Festplatten und USB-Sticks können in falsche Hände gelangen.	Vertrauliche Daten sollten verschlüsselt werden. Damit sind die Risiken bei PC-Verlust, Datenträgerverlust, Datenübertragung per E-Mail o.ä. erheblich reduzierbar. Verschlüsselungssoftware schützt nur, wenn sie auch aktiviert ist.	▌Organisation ▌IT-Experten ▌Securitymanagement
Virenschutz	Data loss.	Das Ausführen von Schadcodes muss aktiv unterbunden werden. Viren, Trojaner und Adware können durch eine zentrale Lösung verhindert werden. Als zentrale Lösung empfehlen sich Virenscanner auf allen Geräten (regelmäßiges Update erforderlich), Firewall und Server.	▌IT-Experten ▌Virensoftware-hersteller
Whitehacking	Entdecken von Möglichkeiten, in das System einzudringen (unberechtigter Zugang).	Unter Whitehacking versteht man die Beauftragung von Spezialisten, konkrete Lücken aufzudecken, die von den eigenen IT-Experten nicht erkannt wurden.	▌IT-Experten ▌Berater mit Spezial-Know-how

STICHWORTE	RISIKEN	ERLÄUTERUNGEN, HINWEISE	HILFE GEBEN
Wissen, Ausbildung	IT-Sicherheit ist ein erfolgskritisches Thema und muss im täglichen Umgang gelebt werden.	Der aufgeklärte Mitarbeiter hilft, Gefahren zu mindern! Das Thema „IT-Sicherheit" sollte in das Bewusstsein aller Mitarbeiter gerückt werden. Der Mensch in seinem Verhalten ist das schwächste Glied in der Sicherungskette.	▌Geschäftsführung ▌Personalfachleute ▌IT-Experten
WLAN	Datenverkehr über unverschlüsselte Zugänge.	WLAN sollte ausschließlich mit WPA-/WPA2-Verschlüsselung ausgerüstet sein. Die Konfiguration des Routers ist dabei sehr wichtig. Mitarbeiter sollten keine eigenen WLANs betreiben.	▌IT-Experten ▌Datenschutz
XING	Siehe unter Apps, Soziale Netzwerke, LinkedIn.		▌Personalfachleute ▌IT-Experten ▌Datenschutz
Zertifizierung	Nachweispflicht für Zertifizierung im Kundenverhältnis kann nicht erfüllt werden.	In einigen Branchen ist der sichere Umgang mit Informationen und Waren notwendig. Hierzu werden von Geschäftspartnern Zertifikate eingefordert, z.B. ISO-Zertifikate.	▌IT-Experten ▌Datenschutz ▌BSI
Zugang, Zugriff	Sabotage, Datenklau und Datenverlust, Diebstahl und Manipulation.	Der nicht körperliche Zugang über IT-, TK-, TV-, Foto-, Audio-Geräte ist vergleichbar dem Zutritt zu regeln und zu sichern.	▌Personalfachleute ▌IT-Experten ▌Datenschutz
Zutritt	Sabotage, Datenklau und Datenverlust, Diebstahl und Manipulation.	Zutritt von Personen zu Räumen regeln. Zutrittssicherung in Bereiche mit erhöhter Sicherheitsanforderung kann mit einfachen Mitteln (Schlüssel, Transponder, Zahlencode, ID-Karte) erreicht und kontrolliert werden. Mitarbeiterpflichten, Schließkonzept, Widerstandszeitwert prüfen, Mechatronic-Überwachung, Selektion besonders gefährdeter Bereiche, Schlüsselverwaltung.	▌Organisation ▌Personalfachleute ▌Securitymanagement ▌Fachberatung

III. VERWEISE AUF INSTITUTIONEN, HILFREICHE DOKUMENTATIONEN

ANBIETER	**IHK Frankfurt am Main**
INTERNET (URL)	www.frankfurt-main.ihk.de/branchen/mediacity/tk_it/it-sicherheit

ANBIETER	**IHK Hessen innovativ**
INTERNET (URL)	www.ihk-hessen-innovativ.de

ANBIETER	**Fachmesse IT-Sicherheit „it-sa“**
INTERNET (URL)	www.it-sa.de

ANBIETER	**Bundesamt für Sicherheit in der Informationstechnik (BSI)**
INTERNET (URL)	www.bsi.bund.de

ANBIETER	**Glossar des BSI**
INTERNET (URL)	www.bsi.bund.de Suchbegriffe: Glossar, IT-Grundschutz

ANBIETER	**Marktplatz IT-Sicherheit des Instituts für Internet-Sicherheit – (ifis)**
INTERNET (URL)	www.it-sicherheit.de

ANBIETER	**Initiative Wirtschaftsschutz**
INTERNET (URL)	www.wirtschaftsschutz.info

ANBIETER	**Bundesministerium für Wirtschaft und Energie (BMWi)**
INTERNET (URL)	www.bmwi.de/DE/Themen/Digitale-Welt/it-sicherheit

ANBIETER	**Polizei Hessen**
INTERNET (URL)	www.polizei.hessen.de/Praevention/Sicherheit-im-Internet

ANBIETER	**Zentrale Ansprechstelle Cybercrime (ZAC) des LKA Niedersachsen**
INTERNET (URL)	www.lka.niedersachsen.de Suchbegriff: ZAC

ANBIETER	**Fraunhofer-Institut für Sichere Informationstechnologie**
INTERNET (URL)	www.sit.fraunhofer.de

ANBIETER	**IT-Sicherheitsgesetz**
INTERNET (URL)	www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/it-sicherheitsgesetz

ANBIETER	**Bundesdatenschutzgesetz** (BDSG)
INTERNET (URL)	www.gesetze-im-internet.de/bdsg_1990

ANBIETER	**Kunsturhebergesetz** (KunstUrhG)
INTERNET (URL)	www.gesetze-im-internet.de/kunsturhg

ANBIETER	**Aufbewahrung von Unterlagen gem. § 257 HGB**
INTERNET (URL)	www.gesetze-im-internet.de/hgb/__257.html

ANBIETER	**Aufbewahrung von Unterlagen gem. § 147 AO**
INTERNET (URL)	www.gesetze-im-internet.de/ao_1977/__147.html

ANBIETER	**BITKOM e.V.**
INTERNET (URL)	www.bitkom.org

ANBIETER	**IT for work e.V.**
INTERNET (URL)	www.it-for-work.de/Inhalte/Kompetenz

ANBIETER	**Deutscher Datenschutzrat Online-Werbung**
INTERNET (URL)	www.meine-cookies.org/DDOW

IV. EMPFEHLUNGEN DER PROJEKT-GRUPPE DATENSICHERHEIT

Die Projektgruppe Datensicherheit schließt die Erarbeitung dieses Gefahrenatlasses mit der Erkenntnis, dass die Risiken durch die unbedachte sowie missbräuchliche Nutzung moderner Informationstechnologie und Applikationen ein exponentielles Wachstum haben.

Somit kann ein Gefahrenatlas wie dieser nie vollständig und längere Zeit gültig sein.

Menschen, die moderne Informations- und Kommunikations-Technologie (IKT) für berufliche und private Zwecke nutzen und die Risiken weitgehend kontrollieren wollen, empfehlen wir dringend eine hohe Achtsamkeit, verbunden mit einem gesunden Misstrauen gegenüber allen vermeintlich kostenfreien Angeboten, sowie zielorientierte und laufende Weiterbildungsmaßnahmen für ihre IKT-Aktivitäten.

IMPRESSUM

HERAUSGEBER
Industrie- und Handelskammer
Frankfurt am Main
Börsenplatz 4
60313 Frankfurt am Main

HINWEIS
Arbeitsergebnis der Projektgruppe Datensicherheit des Ausschusses Wirtschafts- und Unternehmensberatungen, IHK Frankfurt am Main

PROJEKTGRUPPE
Wolfhard Hoffmann, WISAG Sicherheit & Service Holding GmbH & Co. KG
Karen Hoyndorf, Compass Group Deutschland GmbH
Gerhard Neidhöfer, ACG Automation Consulting Group GmbH

REDAKTION
Dr. Matthias Schoder
Geschäftsführer, Geschäftsfeld Finanzplatz, Unternehmensförderung, Starthilfe,
IHK Frankfurt am Main

KONTAKT
Telefon +49 69 2197 1370
E-Mail m.schoder@frankfurt-main.ihk.de

GRAFIK
Hyprath Kommunikation, Bad Nauheim

TITELBILD
Fotolia_106340098_M - © Coloures-pic

DRUCK
Hausdruckerei, IHK Frankfurt am Main

Stand: Juni 2016

Stichwortsammlung mit Hinweisen
Zeitraum: März 2015 bis Januar 2016

IHK Frankfurt am Main, Juni 2016

www.frankfurt-main.ihk.de

Industrie- und Handelskammer
Frankfurt am Main
Börsenplatz 4
60313 Frankfurt am Main

IHK-Service-Center
Schillerstraße 11
60313 Frankfurt am Main
Telefon +49 69 21 97-0
Telefax +49 69 21 97-14 24
info@frankfurt-main.ihk.de

IHK-Geschäftsstelle Bad Homburg
Louisenstraße 105
61348 Bad Homburg
Telefon +49 6172 12 10-0
Telefax +49 6172 22 61 2
homburg@frankfurt-main.ihk.de

IHK-Geschäftsstelle Hofheim
Kirschgartenstraße 6
65719 Hofheim
Telefon +49 6192 96 47-0
Telefax +49 6192 28 89 4
hofheim@frankfurt-main.ihk.de

IHK Industrie- und Handelskammer Frankfurt am Main