IHK Industrie- und Handelskammer Nürnberg für Mittelfranken

Merkblatt
Informationssicherheit im Mittelstand

Innovation I Umwelt

VORWORT

Industriespionage im Cyberspace ist inzwischen Realität und kein Ausnahmefall mehr. Das Bundesamt für Informationssicherheit (BSI) schätzt den dadurch entstehenden Schaden auf jährlich bis zu 50 Milliarden Euro. Für Großkonzerne stellen Investitionen in Verteidigungsmaßnahmen in Abwehr von Cyberattacken keine große Überwindung dar, ganz im Gegensatz zu kleinen und mittleren Unternehmen, denen nicht genügend finanzielle Mittel und Know-how zur Verfügung stehen. Die Schäden entstehen den betroffenen Unternehmen auf verschiedenen Ebenen. Der Verlust von Informationen und des Alleinstellungsmerkmals können sich existenzgefährdend auswirken, daher spielt der Schutz sensibler Informationen und Systeme eine besondere Rolle.

Das vorliegende Merkblatt[1] ist eine Zusammenfassung des Leitfadens[2] zur Informationssicherheit in kleinen und mittleren Unternehmen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und soll kleine und mittlere Unternehmen auf die Gefahren, denen betriebliche IT-Systeme ausgesetzt sind, informieren und sensibilisieren.

[1] http://www.ihk-nuernberg.de/informationssicherheit
[2] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzUeberblick/LeitfadenInformationssicherheit/leitfaden_node.html

Industrie- und Handelskammer
Nürnberg für Mittelfranken

INHALT

SCHÄDEN

Technische Defekte, menschliche Fehler oder mutwillige Beschädigungen und Zerstörungen sind häufige Ursachen für Störungen oder Ausfälle von IT-Systemen und Infrastruktur. IT-Systeme und Netzwerke sind gezielten Hackerangriffen und Bedrohungen durch Schadprogramme (Malware) ausgesetzt. Die gezielten Angriffe erfolgen zunehmend von der organisierten Kriminalität und Wirtschaftsspionage mit dem Hauptmotiv, einen finanziellen Vorteil zu erzielen. Durch den wirtschaftlich begründeten Trend, Produkte und Informationssysteme in industriellen Bereichen zu vernetzen, erhöhen sich die verwundbaren Punkte gerade bei KMUs. Viele davon können durch einfache Mittel beseitigt und so für die Informationssicherheit besonders schwerwiegende Fehler vermieden werden. Die häufig auftretenden Ursachen sind im Folgenden beschrieben.

Unzureichende Informationssicherheits-Strategie

Informationssicherheit wird im Vergleich mit anderen Faktoren wie Kosten, Marktpreise, Wettbewerbsfähigkeit **unterbewertet** und eher als Kostentreiber und als Behinderung betrieblicher Abläufe angesehen. Sicherheitsvorfälle können schnell zu einem Risiko für das reibungslose Funktionieren der Unternehmensprozesse führen.

Aufgrund von zusätzlich entstehenden Kosten, Zeitmangel und einer fehlenden Aufgabenzuweisung, finden **keine regelmäßigen Überprüfungen** auf Konformität mit den **Sicherheitsvorgaben** statt. Ohne einen verlässlichen Prozess kann kein angemessenes Sicherheitsniveau dauerhaft erreicht und aufrecht erhalten werden.

Nicht vollständige, veraltete oder den Mitarbeitern **nicht bekannte Sicherheitsrichtlinien** sowie fehlende vertragliche Vereinbarungen mit Mitarbeitern und externen Unternehmen können zu Verstößen im Bereich Sicherheit führen.

Ebenso problematisch sind **fehlende Kontrollmechanismen** hinsichtlich der Sicherheitsziele sowie die **fehlenden Konsequenzen** für Mitarbeiter im Falle von Sicherheitsverstößen. Beide Sachverhalte erhöhen das Risiko für Schadensfälle wie zum Beispiel Know-how-Verlust, Imageschäden, Produktionsausfälle etc.

Schlecht konfigurierte und administrierte IT-Systeme

Rollen und **Benutzerregeln** sind in KMUs **nicht restriktiv** genug, da die Administration meist zeitintensiv und mit technischem Aufwand verbunden ist. Durch die geringere Anzahl der Mitarbeiter in KMUs ist zwischen der Einschränkung von Rechten und Nicht-Beeinflussung der betrieblichen Prozesse ein Kompromiss zu finden.

Durch **Konfigurations- und Administrationsfehler** entsteht eine Vielzahl an **Sicherheitslücken**. Benutzung vorhandener Sicherheitsfunktionen von Betriebssystemen und Anwendungen können das Sicherheitsniveau in KMUs deutlich erhöhen.

Unsichere Vernetzung und Internetanbindung

Die **Anbindung** von **Systemen** und **Applikationen** an das **Internet** erfordern **spezielle Kenntnisse und Erfahrungen**. Aufgrund der Personal- und Kostensituation in KMUs sind diese nicht immer vorhanden. Daher werden sensitive Informationen, Daten und IT-Systeme nicht immer ausreichend von offenen Netzen abgeschottet. Bei **Outsourcing** der IT an externe Dienstleister müssen **Mindestanforderungen technisch** aber auch **vertraglich** angemessen und wirksam **eingerichtet** werden.

Vernachlässigung von Sicherheitserfordernissen

Aus **Bequemlichkeit** werden **Sicherheitsmechanismen ausgehebelt**, wie z. B. das unverschlüsselte Versenden vertraulicher Dokumente über Emails, Nichtbeachtung von Passwortregeln, Computer beim Verlassen des Arbeitsplatzes werden nicht gesperrt, Büro nicht abgeschlossen, etc.

Durch die rasant **steigende Komplexität** von **IT-Systemen**, **Netzen** und **Anwendungen** sind Anwender und Administratoren **nicht ausreichend sensibilisiert**. Eine kleine Anzahl an IT-Mitarbeitern eines KMUs nur mit Handwerkzeug ausgestattet, stehen eine Überzahl an Hackern gegenüber.

Das Personal eines Unternehmens ist **Angriffsziel** für **„soziale Attacken"** beispielsweise bei **Wirtschaftsspionage**. Menschliche Schwächen werden bei Angriffen auf die Systeme ausgenutzt, da das **Personal** von KMUs **unzureichend** auf diese Vorfälle **vorbereitet** und **geschult** ist.

Mangelhafte Wartung von IT-Systemen

Erforderliche **Sicherheitsupdates** (Patches) werden oftmals **nicht rechtzeitig installiert**. Das Einspielen der Patches beansprucht Zeit und es kann nicht sichergestellt werden, dass durch die Installation nicht andere Beeinträchtigungen ausgelöst werden. Trotzdem können offen gebliebene Sicherheitslücken zu Schäden und erheblichen Störungen betrieblicher Prozesse führen.

Sorgloser Umgang mit Passwörtern und Sicherheitsmechanismen

Aufgeschriebene Passwörter am Arbeitsplatz sowie zu kurze oder **leicht** zu **erratende Passwörter** machen es Angreifern leicht, ein Passwort zu knacken. An Kollegen **weitergegebene Passwörter** können zum Problem werden, wenn diese das Unternehmen verlassen. Über soziale Netzwerke wenden **Angreifer** zunehmend **psychologische Tricks** an, um an das Wissen von Unternehmen oder Zugang zu sensiblen Informationen zu gelangen.

Aus Bequemlichkeit, Unwissen oder Zeitmangel werden eingebaute **Sicherheitsmechanismen** von Anwendungen und Systemen **ausgehebelt**.

Unzureichender Schutz vor Einbrechern und Elementarschäden

Gebäude und **Räume** werden **ungenügend** gegen **unbefugten Zutritt geschützt**. Sensible Daten auf mobilen Geräten werden selten verschlüsselt, was bei Diebstahl ein Problem darstellt. Ein größeres Problem stellt der Verlust von Daten durch Diebstahl, Vandalismus oder Elementarschäden dar, denn diese lassen sich nur unter Mühen wiederherstellen oder wiederbeschaffen. Ebenfalls stellt der Missbrauch entwendeter Daten eine große Gefahr dar.

Brände, **Überschwemmungen**, **Stromausfälle** sind seltene Ereignisse, jedoch mit **fatalen Folgen**. Brandschutzmaßnahmen, Schutz vor Wasserschäden und Sicherstellung der Stromversorgung sollen als wichtiger Bestandteil der Informationssicherheit verstanden werden. Hierfür müssen gleichzeitig organisatorische und personelle Maßnahmen ergriffen werden.

MAßNAHMEN

Der Schutz der Daten und der eingesetzten Informationstechnik ist für gewöhnlich nur durch die Etablierung von Regeln und Mechanismen in verschiedenen Bereichen möglich. Die aufgeführten Schadensszenarien können unterschiedliche Ursachen haben, meist ist es eine Kombination von Schwachstellen und Versäumnissen. Im Folgenden werden für typische Bereiche der Informationssicherheit wirkungsvolle Maßnahmen, die auch ein günstiges Kosten-/ Nutzerverhältnis aufweisen, dargestellt.

Informationssicherheitsmanagement, Personal, Organisation

Technische Sicherheitsmaßnahmen sollten daher Teil eines umfassenden Informationssicherheitsmanagementsystems (ISMS) sein, welches mit dem Plan-Do-Check-Act (PDCA)-Zyklus einen geeigneten Regelkreis abbildet und ebenso personelle wie organisatorische Sicherheitsmaßnahmen enthält.

Sicherheitsmaßnahmen
• Die Gesamtverantwortung für Informationssicherheit wird von der **Leitungsebene** übernommen, mit dem Ziel, die wichtigsten Aspekte der Sicherheitsstrategie zu beschreiben. • Die Leitungsebene muss einen **Beauftragten** benennen und mit angemessenen Ressourcen ausstatten, der die Informationssicherheit fördert und den Sicherheitsprozess steuert und koordiniert. • Alle Sicherheitsmaßnahmen werden systematisch in einem **Sicherheitsprozess** dokumentiert und regelmäßig aktualisiert. • **Regelmäßige Überprüfung** und **Aktualisierung** des Sicherheitsprozesses, Sicherheitskonzeptes, Leitlinie zur Informationssicherheit und Organisationsstruktur zur Informationssicherheit.

Infrastruktursicherheit

Die bauliche Infrastruktur zum Betrieb der Systeme und Netze gilt als „erste Verteidigungslinie" und muss angemessen vor Umwelteinflüssen, Unfällen und Zutritt Fremder geschützt werden.

Sicherheitsmaßnahmen
• **Schützenwerte Räume** oder **Gebäudeteile** müssen sich außerhalb der gefährdeten Bereiche befinden. Diese sind mit Zutrittsregelungen und Zutrittskontrollen technisch und organisatorisch zu versehen.

- Strom- und Datenverkabelung sowie ein Überspannungsschutzkonzept sollen den einschlägigen Normen und Vorschriften entsprechen. Ebenso ist ein IT-bezogenes Brandschutzkonzept zu erstellen und umzusetzen.
- Infrastrukturkomponenten wie Strom- und Datenversorgung, Klimaanlage etc. sollen skalierbar geplant und regelmäßig gewartet und kontrolliert werden.

Schutz vor Schadsoftware und Software-Schwachstellen

Schadsoftware kann die Integrität und Verfügbarkeit von Daten und Programmen in allen Unternehmensbereichen beeinträchtigen. Trojaner, die die Authentisierungsinformationen auslesen, gefährden die Vertraulichkeit gespeicherter und verarbeiteter Informationen. Stärker gefährdet sind geheime Firmendaten oder die Verfügbarkeit wichtiger Anwendungen und Dienste. Die wesentliche Schutzmöglichkeit besteht im Einsatz von Anwendungen (Scannern), welche in der Regel die Schadsoftware anhand von Erkennungsmustern aufspüren. Ein wirkungsvolles Patchmanagement ist die beste „Verteidigungsstrategie", um Schwachstellen in Betriebssystemen und Software zu beheben, um Angreifern das Eindringen in Systemen und die illegitime Aneignung von Rechten zu verwehren.

Sicherheitsmaßnahmen

- Schutzprogramme sind auf **allen IT-Systemen einzurichten**, die regelmäßig zu pflegen und aktualisieren sind.
- Sicherheitsrelevante **Paches und Updates** für Betriebssysteme und Middleware sind auf allen IT-Systemen zeitnah zu installieren.
- **Mitarbeiter** sollen **informiert** und **sensibilisiert** sein, wie eine Infektion des Systems mit Schadsoftware zu verhindern ist, wie eine Schadsoftware erkannt werden kann und wie im Notfall zu reagieren ist.
- **Infizierte IT-Systeme müssen isoliert werden** und dürfen bis zur vollständigen Bereinigung nicht produktiv eingesetzt werden.

Sichere Nutzung mobiler IT-Systeme

Die Verwendung mobiler Endgeräte und deren Synchronisierung erfordern eine Übertragung der Daten über das Internet und eine externe Speicherung der Informationen (Kontaktdaten, Termine, Daten). Logische und physische Schnittstellen können Schwachstellen generieren, über die Angriffe gegen das interne Firmennetz wirksam werden könnten.

Sicherheitsmaßnahmen
• Mobile **Datenträger** und **Datenträger** in mobilen Geräten müssen **verschlüsselt** werden. • Verwendung von **Mobile-Device-Management-Software** (MDM) zur zentralen Verwaltung der Systeme. • Verwendung einer **Zwei-Faktor-Authentifizierung**: Wissen (z. B. Passwort) mit Besitz (z. B. Token, Chipkarte, RFID-Karte) oder Biometrie (z. B. Fingerabdruck) kombinieren. • **Eingeschränkte Rechte** von Benutzern verhindern die Installation zusätzlicher Software. • Die Kommunikation sollte über eine **Verschlüsselte Leitung** (VPN) über das Firmennetzwerk erfolgen.

Datensicherung und Notfallprävention

Ein Notfall ist ein Schadensereignis, bei dem wesentliche Abläufe eines Unternehmens über das Ausmaß einer Störung hinaus nicht wie vorgesehen funktionieren. Daher ist ein Aufbau und Betrieb eines Notfallmanagement-Prozesses notwendig. Dadurch wird die Wahrscheinlichkeit des Auftretens eines Notfalls und die daraus entstehenden negativen Folgen gemindert. Hierfür sind geeignete Vorbeugemaßnahmen zu treffen, um die Robustheit und Ausfallsicherheit zu erhöhen. Maßnahmen sind zu treffen, die bei Eintritt eines Notfalls die Ausfallzeit minimieren.

Sicherheitsmaßnahmen
• **Notfallpläne** müssen vorhanden, jedem Mitarbeiter bekannt und mit Sofortmaßnahmen vertraut sein. • **Regelmäßige Datensicherungen** (Backups) und deren Überprüfung sind wichtiger Bestandteil der Sicherheitsmaßnahmen. Der Aufbewahrungsort der Datensicherung soll getrennt von den Daten und von Elementarschäden und Zugriff unbefugter geschützt sein. • Hard – und Software sind zu **inventarisieren** und hinsichtlich der Verfügbarkeitsanforderungen zu bewerten.

Sichere Konfiguration und ständiger Wartung der IT-Systeme

Falsche Nutzung der in Betriebssystemen und Anwendungssoftware vorhandenen Sicherheitsfunktionen mindern das Sicherheitsniveau in Unternehmen. Wichtig ist die Installation, Konfiguration, Administration und Wartung der IT-Systeme. Für die Benutzerrechte installierter Anwendungen, Dienste und Konten sollte folgendes Prinzip gelten: „so viel wie nötig und so wenig wie möglich". Hierbei ist zwischen der Rechteeinschränkung und Nichtbeeinflussung der betrieblichen Prozesse ein Kompromiss zu finden.

Sicherheitsmaßnahmen
• Betriebssystemkomponenten, Anwendungen und Tools sollten vor der Installation festgelegt und nur Medien und Dateien aus einer sicheren Quelle verwendet werden. Nicht benötigte Programme und Dienste sollten deaktiviert oder deinstalliert werden. • **Berechtigungen** für Systemverzeichnisse und Dateien die den Vorgaben der Sicherheitsrichtlinien nicht mehr entsprechen bzw. Benutzerkonten ausgeschiedener Mitarbeiter sind zeitnah zu deaktivieren oder zu löschen. • Durch eine **restriktive Zugriffsrechtvergabe** auf Dateien und Ordnern, erhält jeder Benutzer nur auf die für seine Aufgaben relevanten Informationen Zugriff. • Durch **regelmäßiges Auswerten** der sicherheitsrelevanten Ereignisse in **Logfiles** können eventuelle Attacken festgestellt werden.

Sichere Architektur des Unternehmensnetzwerkes und dessen Schnittstellen

KMUs benötigen wie andere Unternehmen eine lokale Infrastruktur (Netz) die auf die betrieblichen Abläufe optimiert ist und eine hohe Verfügbarkeit aufzeigt. Das lokale Netz ist mit dem Internet und in der Regel auch mit anderen Netzen gekoppelt. Hier gilt die Vorteile der Vernetzung unter gleichzeitiger Beibehaltung eines hohen Sicherheitsniveaus zu gewährleisten.

Sicherheitsmaßnahmen
• **Sicherheitsanforderungen** sind neben den betrieblichen Anforderungen bei der Planung der Netztechnologie und Netzwerktopologie zu **berücksichtigen**. • Das gesamte Netz des Unternehmens muss durch ein entsprechendes **Sicherheitsgateway** (Firewall) geschützt sein. In einer Demilitarisierten Zone (DMZ) bieten Systeme öffentliche Dienste nach außen und gleichzeitig ist das interne Netzwerk vor unberechtigten Zugriffen von außen geschützt. • **Geschultes Personal** sollte die Firewall-Software und –Einstellungen administrieren, das **Netzwerk** ständig **überwachen** und Schwachstellen beseitigen und regelmäßig die sicherheitsrelevanten Protokolle auswerten.

Schulung und Sensibilisierung des Personals

Da IT-Systeme, Netze und Anwendungen immer komplexer werden, ist für das IT-Personal und Benutzer eine Weiterbildung hinsichtlich Informationssicherheit unumgänglich. Für KMUs sind Weiterbildungen meistens nicht mit unentbehrlichen Kosten verbunden und sollten daher sehr zielgerichtet und effizient erfolgen.

Sicherheitsmaßnahmen
• Ein **Schulungs- und Sensibilisierungskonzept** (Zielgruppen, Schulungsformen, Schulungsanbietern, Schulungsinhalten und Schulungsprozess) ist zu erstellen und in drei bis neun Monaten durchzuführen. • **Regelmäßiger Prüfung** des Konzeptes auf Wirksamkeit und bei Verbesserungsbedarf die Gründe hinterfragen.

Sichere Passwörter und andere Authentifizierungsmittel

Authentifizierung ist ein elementarer Sicherheitsmechanismus, die ein Benutzer auf drei verschiedene Wege erreichen kann:

- Nachweis der Kenntnis einer Information (z.B. Passwort)
- Verwendung eines Besitztums (z.B. Chipkarte)
- Gegenwart eines Merkmals des Benutzers selbst (Biometrie)

Für Hochsicherheitsbereiche ist ein Mechanismus, der zwei Bereiche kombiniert verwendet empfehlenswert.

Sicherheitsmaßnahmen
• Vom Hersteller vergebene **Standard-Passwörter müssen geändert werden**. • Passwörter müssen **gängige Mindestanforderungen** an **Komplexität** erfüllen und Passwortregeln sollten **verbindlich** festgelegt und den Mitarbeitern **kommuniziert** werden. • Bei Systemen/Anwendungen mit **erhöhten Sicherheitsanforderungen** ist **eine Zwei-Faktor-Authentifizierung** erforderlich.

Sichere Email und Internet-Nutzung

Wer die Informationsbeschaffung, Kommunikation und Geschäftsabwicklung über das Internet abwickelt, bedient sich an einem unsicheren Übertragungsmedium und greift auf Funktionen und Daten deren Integrität und Authentizität des Kommunikationspartners nicht gegeben sind. Email als meistgenutzter Kommunikationsdienst bietet keinen Schutz. Der Inhalt kann ausgelesen und verfälscht werden. Verschlüsselung kann jedoch die Vertraulichkeit und eine elektronische Signatur die Integrität und Authentizität von Emails kostengünstig gewährleisten. Die Absicherung der Internetnutzung ist eine große Herausforderung für KMUs, die aber durch technische und organisatorische Maßnahmen zu bewältigen ist. Hier ist ein Kompromiss zwischen Funktionalität und Informationssicherheit zu finden.

Sicherheitsmaßnahmen
• Für Mitarbeiter **klare und verbindliche Richtlinien** für E-Mail- und Internet-Nutzung definieren. • Schutzbedürftige E-Mails müssen **verschlüsselt** und **elektronisch signiert** werden. • Dateianhänge unbekannter **E-Mail-Sender** sind mit Sorgfalt und **Vorsicht** zu behandeln. • **Nichtbenötigte Funktionen** in Email-Client-Programmen und im Web-Browser sollten **deaktiviert** werden um die mögliche Angriffsfläche zu reduzieren.

Sicherheit bei der Beteiligung Dritter

Einfache Wartungsarbeiten, Nutzung von Cloud-Diensten, oder Outsourcing-Konstellationen generieren unterschiedliche Gefahrenquellen für die Informationssicherheit sobald eine Beteiligung Dritter besteht. Alleine oder zusammen mit Mitarbeitern oder einem Hintermann, könnten Dritte zum Beispiel gezielte Angriffe durchführen, unabsichtlich Fehler machen oder selbst das Opfer eines Angriffs werden. Abwehrstrategien sind auf unterschiedliche Ebenen möglich.

Sicherheitsmaßnahmen
• **Qualifikationen** und **Zertifikate** bei der Auswahl von geeigneten Dienstleister verwenden. • **Anforderungen** und **Rahmenbedingungen** zur Informationssicherheit zu allen Geschäftsbeziehungen **vertraglich vereinbaren**, die alle Phasen des Lebenszyklus und Beendigung der Beziehung einschließen. • Das **Sicherheitskonzept zwischen beauftragender Firma und Dienstleister ist abzustimmen**. Alle sicherheitsbezogenen Rechte und Pflichten sind abzudecken und eindeutig jeder Seite zuzuweisen. • Die **beauftragende** Firma mit hohen **Verfügbarkeitsanforderungen** sollte bei Ausfall eines Dienstleisters, um innerhalb des Unternehmens keine gefährdende Unterbrechungsdauer zu erzeugen, **Ersatzlösungen aktivieren** können.

Einhaltung von Regelungen und Vorschriften: Compliance

Eine elektronische Information wird der papiergebundenen Information gleichgestellt. In Zusammenhang mit der elektronischen Signatur und ausgehend von der Änderung des BGB wurden in Deutschland entsprechend Gesetze und Verordnungen angepasst. In Deutschland gibt es Compliance –Anforderungen, nur wurden diese nicht so bezeichnet. Hierzu gehören aus der deutschen Steuer- und Handelsgesetzgebung beispielsweise HGB, AO, GDPdU, GoBS ebenso wie in der Finanzwirtschaft das Thema Risikocontrolling nach Basel II, Kon-TraG usw. KMUs verfügen im Gegensatz zu großen Konzernen nicht über die Ressourcen für eine dedizierte Organisationsstruktur für Compliance. Die Durchführung von Compliance-Aktivitäten und dessen Integration in das ISMS kann dem Beauftragten für Informationssicherheit übertragen werden, jedoch trägt die Leitung die Verantwortung. KMUs können aus ihrer Rechtsform (z.B. Aktiengesellschaft, GmbH, OHG) ableiten, welche fordernden Kontrollstandards (BSI-Standards oder ISO 27000) die Compliance gegenüber einer Wirtschaftsprüfung sowie ihren Kunden herstellen.

Sicherheitsmaßnahmen

- In Bezug auf das Compliance-Management ist mindestens ein **geeigneter Verantwortlicher festzulegen** und zu benennen, sowie eine strukturierte Übersicht der Gesetze, Vorschriften und Verträge.
- Ebenso muss der **Schutzbedarf** bereits **vorhandener Unternehmenswerte bekannt** sein, eventuell ist eine **Risikoanalyse** erforderlich.
- Um Verstöße gegen die Anforderungen zu vermeiden, können geeignete Maßnahmen identifiziert und umgesetzt werden. Bei Verstößen müssen die Aktionen zur Korrektur, Schadensbegrenzung, und Sanktionierung bekannt sein.
- **Regelmäßig** ist zu **überprüfen**, ob die **Sicherheitsvorgaben eingehalten** werden und ob die rechtlichen Rahmenbedingungen **noch aktuell** sind.
- Alle Personen im Umgang mit Informationen und IT-Systemen sollen auf ihre Sorgfaltspflicht hingewiesen werden.

Redaktion

Dr. Robert Schmidt, robert.schmidt@nuernberg.ihk.de

Knut Harmsen, knut.harmsen@nuernberg.ihk.de

Claudiu Bugariu, claudiu.bugariu@nuernberg.ihk.de

Ansprechpartner:

Claudiu Bugariu, B.Sc.

Industrie- und Handelskammer Nürnberg für Mittelfranken

Geschäftsbereich Innovation | Umwelt

Informationssicherheit

Tel.: +49 911 1335-439

Fax: +49 911 1335-122

E-Mail: claudiu.bugariu@nuernberg.ihk.de

Blog: www.ihk-nuernberg.de/blogs/informationssicherheit

Stand: November 2013