

## Experteninterview: Sichere E-Geschäftsprozesse in KMU und Handwerk

Prof. Dr. Günther Neef, Andreas Gabriel und Ekkehard Diedrich im Gespräch mit dem ECC Handel

**ECC Handel: Welche IT-Sicherheitslösungen erachten Sie grundsätzlich als unumgänglich?**

**Gabriel:**

Hier muss zwischen drei grundsätzlichen Ansatzpunkten unterschieden werden:

1. IT-Sicherheit: Die Bereiche Datensicherung, Bekämpfung von Computerschädlingen, Sicherung des Netzwerks (Firewall) und Update der Programme müssen für jedes Unternehmen obligat sein.
2. Organisation: Im Unternehmen müssen geltende Richtlinien vorliegen, in denen die grundlegenden Arbeitsweisen geregelt sind wie z. B. „private Nutzung von E-Mail und Internet“ oder „die Weitergabe von Daten“. Die Mitarbeiter sind aktuell zu belehren.
3. Datensicherheit und Datenschutz sind als gemeinsames Ganzes zu betrachten. Sicherheits- und Datenschutzbeauftragter kann im Unternehmen nicht ein und dieselbe Person sein, auch nicht der Administrator.

**Prof. Neef:**

Die generelle Gefährdungssituation hat im vergangenen Jahr qualitativ und quantitativ neue Dimensionen erreicht. Zur Gewährleistung der erforderlichen Sicherheit in unseren Unternehmen, die immer stärker von der Anwendung der IT-Technologien geprägt werden, ist deshalb ein ganzheitlicher Ansatz zur IT- und Informationssicherheit erforderlich. Dies bedeutet, dass sowohl die erforderlichen Elemente und Maßnahmen zur technischen Basissicherheit wie Virens Scanner, Firewall, Spamfilter, Update-Management usw. als auch organisatorische Strukturen wie Sicherheitspolicy, Rechteverteilung, Regelungen zur E-Mail und Internet-Nutzung, Verfahrensanweisung zur Datensicherung usw. auf der Basis der zu realisierenden Geschäftsprozesse umgesetzt und aktualisiert werden müssen.

**Diedrich:**

Datensicherung und Schutz gegen Schadsoftware halten wir für unabdingbare Voraussetzungen.

## **ECC Handel: Welche Maßnahmen erachten Sie für unerlässlich, um eine ausreichende Website-Sicherheit zu gewährleisten?**

### **Gabriel:**

Die Entscheidung, welche Sicherungsmaßnahmen auszuwählen sind, hängt maßgeblich davon ab, welche Geschäftsprozesse über die Webseite abgewickelt werden. Die Erstellung der Inhalte muss in jedem Fall rechtskonform erfolgen und das Impressum gemäß der gesetzlichen Vorgaben aufgebaut sein.

Sobald eine Interaktion mit dem Kunden erfolgt, z. B. in Form eines Online-Shops, sind tiefere Maßnahmen zu ergreifen. Doch bevor diese angegangen werden, sollten sich die Verantwortlichen bewusst machen, ob sie diese Aufgaben selbst leisten können oder aber einen kompetenten IT-Dienstleister damit beauftragen.

### **Prof. Neef:**

Im KMU- und Handwerksbereich werden unternehmensrepräsentierende sowie funktionelle Websites in hohem Maße bei externen Providern gehostet. Damit kommt der Auswahl des Providers und seinem möglichst zertifizierten Sicherheitssystem eine hohe Bedeutung zu. Andererseits sollten bei der Erstellung/Programmierung der Websites durch eigene Web-Programmierer oder bei beauftragten Dienstleistern bewährte Methoden der „sicheren Programmierung“ wie z.B. Prüfung/ Authentifizierung von Nutzereingaben, Erkennung und Filterung von Cross Site Scripting (XSS) und SQL-Injection usw. zur Anwendung kommen.

### **Diedrich:**

KMUs und Handwerksbetriebe betreiben ihre Websites oft z. B. aus Kapazitätsgründen nicht selbst. Somit sind die Auswahl des Dienstleisters und damit verbundene Vertragsbedingungen (Sicherheitsfeatures, QoS) entscheidend.

## **ECC Handel: Welche Bedeutung messen Sie der IT- und Informationssicherheit im E-Commerce bei? Gibt es für Unternehmen, die einen Online-Shop betreiben, besondere Sicherheitsgefahren?**

### **Gabriel:**

In meinen Augen ist Informationssicherheit überhaupt erst die Grundlage dafür, E-Commerce betreiben zu können. Daher verstehe ich die von vielen Entscheidungsträgern oft gestellte Frage nach den Kosten nicht. Vielmehr sollte hinterfragt werden, welche Möglichkeiten eine voll funktionstüchtige und vor allem sichere IT bieten.

Für Online-Shops existieren bereits heute zahlreiche Gütesiegel, mit denen man sich beschäftigen sollte, wenn man im Bereich des B2B bzw. B2C einsteigen möchte. Unsere Beratungspraxis hat immer wieder gezeigt, dass die Bezahlabwicklung für den Erfolg eines Online-Angebotes das „Zünglein an der Waage“ ist.

### **Prof. Neef:**

Online-Shops, die letztendlich mit monetären Flüssen verbunden sind, sind bzw. waren schon immer ein besonderes Angriffsziel. Hinzu kommt die weltweite Publizitäts- und Zugriffsmöglichkeit zu Online-Shops, die im Internet ihre Produkte und Leistungen anbieten. Somit hängt der Erfolg eines Online-Shops nicht nur vom strategischen Konzept ab, sondern wird auch in hohem Maße durch sein Sicherheitskonzept mitbestimmt. Neben der Gefahr der möglichen Schädigung des Shop-Betreibers sind es vor allem die Gefahren für potenzielle Kunden, indem ihre sensiblen Daten wie Adressdaten, Kontendaten u.ä. missbraucht und damit für weitere kriminelle Handlungen benutzt werden können.

### **Diedrich:**

Die Bedeutung erachte ich als sehr hoch, insbesondere die Einhaltung gesetzlicher Vorschriften (Archivierung, Nachweisbarkeit, Datenschutz). Bei Online-Shops: Verfügbarkeit (ist z. B. der Provider gegen DoS-Angriffe aufgestellt), Integrität und Vertraulichkeit (Güte der Authentisierung und Autorisierung als Schutz gegen unbefugte Zugriffe).

**ECC Handel: Mit der zunehmenden Verbreitung von Smartphones wird der seit langem vorhergesagte Durchbruch des Mobile Business immer wahrscheinlicher. Welche Sicherheitslücken sehen Sie im mobilen Geschäftsverkehr?**

**Gabriel:**

Viele Mobiltelefone werden bereits heute als Datenspeicher, Browser und Prozessunterstützer eingesetzt, daher müssen diese auch mit der gleichen Sorgfalt behandelt werden wie z. B. Laptops.

In meinen Augen muss vor allem dem Verlustrisiko angemessen begegnet werden – z. B. durch Verschlüsselung der Inhalte und einem hohen Passwortschutz.

**Diedrich:**

Sicher ein komplexes Thema – ein Aspekt als Beispiel: Verlust des Gerätes (verloren, gestohlen) - wie stark ist das Authentisierungsverfahren, sind die Daten im Gerät verschlüsselt?

**ECC Handel: Das Internet ist schon länger keine Einbahnstraße mehr. Unternehmen und Kunden profitieren von den interaktiven Anwendungen des Web 2.0. Welche Gefahren sehen Sie durch diesen bidirektionalen Daten- und Informationsstrom für die IT-Sicherheit?**

**Gabriel:**

Das BSI hat in seinem Lagebericht 2009 eindringlich davor gewarnt, dass ein unsachgemäßes Engagement in sozialen Netzwerken dramatische Gefahren mit sich bringen kann, bis hin zum Identitätsdiebstahl. Die freiwillige und vielleicht sogar unüberlegte Freigabe personenbezogener Daten ist in meinen Augen die größte Bedrohung des Web 2.0. Wenn man bedenkt, dass man mit nur acht Charakteristika jede Person auf diesem Planeten erkennen kann, muss jeder für den sorgsam Umgang mit seinen Daten sensibilisiert werden.

Darüber hinaus sind noch viele Nutzer nicht in ausreichendem Maße für den Umgang mit den „neuen“ Diensten wie z. B. Twitter geschult. Daher wird hier noch eine Vielzahl von Problemen auf uns zukommen.

**Diedrich:**

Die Gefahren haben sich im Prinzip nicht geändert – die Angriffsfläche ist breiter geworden. Somit ist mehr Aufwand und Sorgfalt für IT- und Informationssicherheit angesagt.

**ECC Handel: Die Datensicherung in einem Unternehmen nimmt unabhängig von der rechtlichen Verpflichtung auch aus organisatorischer Sicht eine besondere Stellung ein. Was sagen Sie zu der Bedeutung und zur aktuellen Umsetzung in KMU?**

**Gabriel:**

Eine funktionsfähige Datensicherung ist die Basis einer jeden Sicherheitsstrategie. Dies haben auch die meisten KMU erkannt und damit begonnen, angemessene Schutzmaßnahmen zu treffen. Doch an drei Stellen sind immer noch Defizite zu finden:

1. Die Sicherungen werden leider noch immer nicht getestet. Nur wenn man absolut sicher sein kann, dass die gesicherten Daten auch wirklich in vollem Umfang vorhanden sind, kann von einer erfolgreichen Datensicherung gesprochen werden.

2. Die Dokumentation von Prozessen ist – trotz zahlreicher Warnungen – eine der am meist vernachlässigten Themenstellungen. Auch in KMU müssen die Schlüsselprozesse beschrieben werden, um kritische Situationen meistern zu können. Das Backup darf hier auf keinen Fall fehlen!
3. Es muss bei der Planung der Datensicherung unterschieden werden, welches Ziel überhaupt erreicht werden soll: Ausfallsicherheit oder Datensicherung. Ein bloßes Kopieren der Daten (= Backup) ermöglicht noch lange nicht eine unterbrechungsfreie Weiterführung der Arbeitsprozesse (= Ausfallsicherheit).

#### **Prof. Neef:**

Die maschinenlesbaren Daten sind für Unternehmen, in denen wesentliche Geschäftsprozesse elektronisch abgewickelt werden, von existenzieller Bedeutung. Der Verlust dieser Daten oder selbst eine teilweise Nichtverfügbarkeit führen zu gewaltigen Problemen bei der Auftragsabwicklung, der Kundenbetreuung oder der Abrechnung und Dokumentation. Obwohl diese Risikofaktoren weitestgehend auch bei Geschäftsführungen bekannt sind, zeigen Erfahrungen, die bei Sicherheitsprojekten mit KMU abgehoben wurden, dass die Datensicherung vielfach der Verantwortung von Administratoren übertragen wird und häufig keine oder nur relativ unverbindliche unternehmensspezifische Regularien in KMU vorhanden sind. Hier besteht für die Zukunft aktueller Handlungsbedarf, durch Erfahrungen und Handlungsempfehlungen die Datensicherung in KMU auf eine rechtssichere Basis zu stellen

#### **Diedrich:**

Bei unseren Stammtischen IT-Sicherheit ist das Thema Datensicherheit in jedem Fall Thema Nr.1. Aus unserer Erfahrung kommt man dabei schnell zu der Frage: Mit welchem Datenverlust kann ein Unternehmen noch überleben? Bei der Umsetzung des Themas erleben wir die komplette Bandbreite, von „gar nicht“ bis „hervorragend“.

## **ECC Handel: Wie sollten Unternehmen die Mitarbeiter zu sicherheitsrelevanten Themen schulen? Welche Abstände empfehlen Sie für eine Auffrischung dieses Wissens?**

### **Gabriel:**

Selbstverständlich muss jeder neu eingestellte Mitarbeiter intensiv geschult werden – unabhängig davon ob es sich um einen Auszubildenden oder ein Mitglied der Geschäftsführung handelt. Bereits zu Beginn der Tätigkeit muss jedem klar sein, welche Rechte und Pflichten mit seinem Arbeitsvertrag einhergehen. Nach dieser Basiseinweisung sind weiterführende Maßnahmen zu treffen. Da Schulungen i. d. R. als kostspielig und zeitraubend eingestuft werden, empfehlen wir die folgenden Vorgehensweisen:

Bei jeder Schulung – unabhängig vom Thema – werden die Teilnehmer zu Beginn 5 bis 10 Minuten an die grundlegenden Aspekte der IT- und Informationssicherheit erinnert.

Des Weiteren, häufen sich bei uns die Anfragen, an Betriebsversammlungen Kurzpräsentationen (Dauer: max. 60 Minuten) zu halten, um die Belegschaft für das Thema Sicherheit erneut zu sensibilisieren. Dieses Angebot wird auch deshalb gut angenommen, weil die Teilnehmer wertvolle Impulse für den privaten Umgang mit dem PC erhalten.

### **Prof. Neef:**

Mit der zunehmenden Nutzung des Internets und seiner zahlreichen Funktionalitäten nimmt auch in KMU die Gefährdung zu, durch falsche Verhaltensweisen der damit konfrontierten Mitarbeiter möglichen Angriffen, Malware oder anderen sicherheitsrelevanten Formen das Eindringen in unternehmensinterne Informationssysteme zu ermöglichen. Eine arbeitsplatz- bzw. arbeitsaufgaben-spezifische Schulung der Mitarbeiter ist ein wesentlicher Faktor zur Gewährleistung sicherer Geschäftsprozesse. Die Analyse der Dynamik von Angriffsstrukturen und anderen Gefährdungselementen zeigt eine Verringerung der Reaktionszeiten. Deshalb sollten Mitarbeiter in Abhängigkeit von der unternehmensspezifischen Gefährdungssituation im Zeitraum von 1-3 Monaten zu spezifischen Schwerpunktthemen geschult und trainiert werden.

### **Diedrich:**

So generell wie die Frage gestellt ist, lässt sich das unserer Meinung nach nicht beantworten. Je nach Risikosituation des einzelnen Unternehmens müssen hier sicher individuelle Lösungen gefunden und ggf. adaptiert werden.

## **ECC Handel: Sicherheitsgefahren für ein Unternehmen drohen nicht nur aus der virtuellen Welt. Welche Bedeutung messen Sie betriebsfremden Personen als potenzielle Gefahr bei? Wie sollten Unternehmen hier reagieren?**

### **Gabriel:**

Leider wird die Bedrohung durch betriebsfremde Personen bei kleinen Unternehmen vielmals unterschätzt. Doch gerade die konsequente Umsetzung der in der Anlage zu § 9 des Bundesdatenschutzgesetzes geforderten Zutritts- und Zugangskontrolle muss bei den Verantwortungsträgern fest verankert werden.

Der Zutritt zum Betriebsgelände darf nur so erfolgen, dass der „Besucher“ auch wahrgenommen wird. Dieser sollte während der gesamten Dauer seines Aufenthaltes nie die Möglichkeit bekommen, an betriebseigene Informationen zu gelangen. Dies kann u. a. durch die konsequente Sperrung des PCs und einer sog. Clean-Desk-Philosophie erreicht werden, bei der alle Mitarbeiter gewissenhaft darauf achten müssen, dass zu keiner Zeit sensible Daten offen zugänglich auf dem eigenen Schreibtisch zu finden sind. Darüber hinaus ist es auf keinen Fall unverschämt, wenn fremde Personen auf dem Gang angesprochen werden. Dies suggeriert bei Geschäftspartnern eher ein hohes Maß an Aufmerksamkeit.

### **Prof. Neef:**

Auch im KMU- und Handwerksbereich haben in den letzten Jahren verstärkt Sicherheitssysteme für den Zugang bzw. zum Aufenthalt von Personen im Unternehmen Eingang gefunden. Dennoch wird häufig aus Gründen wie Hilfsbereitschaft, Unterstützung aller Aufgaben im Unternehmen oder falsch verstandener Arbeitsdisziplin fremden Personen im Unternehmen ein breiter Aktionsradius zugestanden. Das Zulassen von Einloggen in betriebliche Systeme, das Weitergeben von Passwörtern die Bereitstellung von Arbeitsplatzcomputern oder mobiler Technik aus dem Unternehmensbestand können zu nicht kalkulierbaren Gefährdungen führen. Durch Schulungen für das Personal sowie durch organisatorische Regelungen zur Betreuung/Begleitung betriebsfremder Personen in Verbindung mit den installierten Lösungen (Protokollierung aller Aktivitäten, Gastzugänge mit eingeschränkten Rechten usw.) bieten erst die erforderliche Sicherheit.

### **Diedrich:**

Hier ist oft Leichtfertigkeit im Spiel – die genannte Gefahr wird unserer Meinung nach total unterschätzt. Was tun: Eine „Politik“ des „Aufgeräumten Schreibtischs“ und Authentisierung an den Geräten erzwingen wären z. B. zwei wichtige Maßnahmen. Thema „social engineering“ spielt hier große Rolle.

## **ECC Handel: Mobile Datenträger, wie bspw. USB-Sticks, sind heute ebenso praktisch wie selbstverständlich. Doch auch hier droht den Unternehmen ein Angriff auf die IT-Sicherheit. Was empfehlen Sie als Maßnahme?**

### **Gabriel:**

Von diesen Datenträgern gehen grundsätzlich zwei große Gefahren aus: Oftmals werden USB-Sticks ohne vorherige Sicherheitsprüfung verwendet und daher gelten sie als maßgebliche Ursache für die Verbreitung von Computerschädlingen.

Aber gerade weil die Verwendung dieser Speichermedien so einfach ist, können Sie ohne umfangreiche Vorbereitungen zum unerlaubten Kopieren von Daten verwendet werden. Dieser Bedrohung müssen gerade die Unternehmen begegnen, die mit sehr sensiblen oder innovativen Daten arbeiten. Eine praktikable Lösung ist auch in diesem Fall die verschlüsselte Speicherung der Daten. Einige Programme unterstützen den Kopierschutz auf USB-Datenträger in der Art, dass sie alle Dateien, die verschoben werden, grundsätzlich verschlüsseln, so dass sie für den Besitzer des Speichersticks unbrauchbar sind. Nur der Mitarbeiter mit dem richtigen Passwort kann den Zugang freischalten.

Von der grundsätzlichen Sperrung der USB-Anschlüsse halte ich nichts, da mit diesem Schritt zu viele Einschränkungen einhergehen. Vielmehr muss für die notwendige Sensibilisierung Sorge getragen werden.

### **Prof. Neef:**

Mobile Datenträger haben sich durch ihren relativ geringen Preis, ihre geringe Größe und ihre zunehmende Speicherkapazität zu einer wichtigen Möglichkeit zum Datentransport entwickelt. Wesentliche Gefährdungspotenziale bestehen im unkontrollierten Einlesen von Daten, bei Verlust durch Diebstahl beim Transport sowie beim Einschleusen von Malware, Viren und anderer Schadsoftware. Während ein prinzipielles Verbot diese Datenträger oder die Beseitigung der Nutzungsmöglichkeiten meistens zu Behinderung im Arbeitsprozess sowie zu Frust bei den Mitarbeitern führen, ermöglichen technische und organisatorische Regelungen zum Umgang und zur Nutzung dieser Datenträger eine effiziente Arbeit. Neben den technischen Überprüfungen wie Akzeptanz nur registrierter Datenträger, Überprüfung der Datenträger vor ihrer Verwendung sowie Einsatz von Verschlüsselungstechnologien kommt der Schulung und Verantwortung der Mitarbeiter zu sicherheitskonformer Nutzung eine hohe Bedeutung zu.

### **Diedrich:**

Einfach, aber oft nicht durchzuhalten: Keine Disketten- und CD-Laufwerke in den Anwengeräten und USB-Schnittstelle deaktivieren. Ansonsten helfen nur saubere Autorisierungsverfahren.

### **ECC Handel: Sollten Unternehmen Sicherheitsvorfälle dokumentieren? Wenn ja, in welcher Form und Regelmäßigkeit?**

#### **Andreas Gabriel:**

Die Dokumentation von Sicherheitsvorfällen wird von den beiden Standardwerken im Bereich der Sicherheit, dem Grundschutzkatalog des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und der ISO 27001, explizit gefordert. Daher stellt sich nicht die Frage "ob" eine Erfassung von möglichen Problemen erfolgt, sondern vielmehr "wie".

Sicherlich wird kein Mitarbeiter freudestrahlend zu seinem Vorgesetzten gehen, um eine persönliche Unzulänglichkeit, ein Versäumnis oder gar einen Fehler einzugestehen. Es muss ein System geschaffen werden, mit dem es für jeden möglich ist, "barrierefrei" Sicherheitsvorfälle zu melden – denn nur durch diese Vorgehensweise kann ein stetiger Verbesserungsprozess in Gang gehalten werden.

Für den Fall, dass die Liste der gemeldeten Probleme sehr kurz bleibt, sollten die Verantwortungsträger diese positive Tatsache mit der Erhebung ausgewählter Kennzahlen aus dem Sicherheitsbereich manifestieren, denn dieser "Beweis" untermauert bei jeder Betriebsprüfung die gute Arbeit und sorgt für eine positive Grundstimmung.

#### **Prof. Neef:**

IT-Sicherheit ist kein einmal erreichter, statischer Zustand, sondern ein dynamischer kontinuierlich zu erneuernder Prozess. Analog zur Qualitätssicherung müssen auch auf dem Gebiet der IT-Sicherheit kontinuierlich Sicherheitsvorfälle dokumentiert werden und daraus resultierende Maßnahmen abgeleitet und umgesetzt werden. Die Standardreihe ISO 27000 gibt hierzu allgemeine Vorgaben, die jedoch unternehmensspezifisch auszurichten sind.

## Die Experten



### **Andreas Gabriel, MECK**

Herr Gabriel arbeitet seit Juli 2000 als Forschungsassistent am Lehrstuhl für Betriebswirtschaftslehre und Wirtschaftsinformatik von Prof. Dr. Rainer Thome (Universität Würzburg). Im Rahmen seiner Tätigkeit war er mehrere Jahre als Netzwerk- und Serveradministrator tätig und konnte bereits in dieser Zeit Erfahrungen im Bereich der Informationssicherheit sammeln. Seit 2003 ist er für das Netzwerk Elektronischer Geschäftsverkehr (NEG) aktiv und kooperiert intensiv mit mittelständischen Unternehmen. Das Hauptaugenmerk seiner täglichen Arbeit spiegelt sich in seiner Tätigkeit im Begleitprojekt „Sichere Geschäftsprozesse in KMU und

Handwerk“ wieder.

Im Mai 2006 absolvierte er erfolgreich die Ausbildung zum Certified Lead Auditor für den Sicherheitsstandard ISO:IEC 27001:2005 beim BSI, seit 2009 ist er Datenschutzbeauftragter. Bereits seit mehreren Jahren ist er als Referent und Dozent bei IHKs, Handwerkskammern und anderen Bildungsträgern tätig. Seit kurzem ist er ebenfalls als Dozent für den Weiterbildungsstudiengang Master of Business Administration der Universität Würzburg tätig.



### **Prof. Dr. Günther Neef, SAGeG**

Professor Günther Neef beschäftigt sich seit ca. 15 Jahren im Rahmen verschiedener Projekte mit Lösungen zur IT-Sicherheit. Neben der technischen Betrachtungsweise haben vor allem organisatorische Modelle zur IT-Sicherheit zu neuen Ansätzen geführt. Im Rahmen eines Begleitprojektes für sichere E-Geschäftsprozesse ist Professor Neef für die prozessorientierte Gestaltung von IT-Sicherheitslösungen verantwortlich, die in Zusammenarbeit mit KMU und Handwerksunternehmen erarbeitet und erprobt wurden. Für den Transfer von IT-Sicherheitslösungen

arbeitet er im Kompetenzzentrum elektronischer Geschäftsverkehr/SAGeG Chemnitz mit und ist Sprecher einer regionalen CERT-Struktur für IT-Sicherheit.



### **Ekkehard Diedrich, TeleTrusT**

Herr Diedrich erlangte seinen Hochschulabschluss im Jahre 1986 als Dipl.-Ing. für Nachrichtentechnik. Seit April 2009 ist er bei TeleTrusT Deutschland e.V. als Referent in der Geschäftsstelle in Berlin tätig. Verantwortlich ist Herr Diedrich neben der Geschäftsstellenarbeit u.a. für TeleTrusT-Projekte, so auch für die TeleTrusT-Beteiligung als Projektpartner am Transferprojekt zum Verbundprojekt „Sichere E-Geschäftsprozesse in KMU und Handwerk“. Davor war er fast 20 Jahre im Forschungs- und Entwicklungsbereich Telekommunikation tätig.



### **Andreas Duscha, ECC Handel**

ist seit Januar 2004 Projektmanager beim ECC Handel am Institut für Handelsforschung, in dem er zuvor als studentischer Mitarbeiter tätig war. Schwerpunktmäßig beschäftigt er sich mit Fragen des E-Commerce, dabei insbesondere mit der IT-Sicherheit, mit Methoden der Online-Kundenakquisition, Verfahren des Suchmaschinenmarketings, Web 2.0-Aspekten sowie mit Einsatzmöglichkeiten der RFID-Technologie. Seinen Abschluss als Diplom-Wirtschaftsinformatiker erhielt er 2004 an der Universität zu Köln. Er ist Doktorand bei Prof. Dr. Müller-Hagedorn, Seminar für Allgemeine Betriebswirtschaftslehre, Handel und Distribution der Universität zu Köln.

In einem Video-Interview geht Andreas Duscha auf das Verbundprojekt „Sichere E-Geschäftsprozesse in KMU und Handwerk“ ein und gibt wichtige Informationen zum Thema der IT-Sicherheit. Das Interview ist einzusehen unter:

[http://www.ecc-handel.de/netzsicherheit\\_und\\_informationssicherheit.php](http://www.ecc-handel.de/netzsicherheit_und_informationssicherheit.php)

Der vorliegende Interviewband ist Bestandteil des vom Bundesministerium für Wirtschaft und Technologie (BMWi) geförderten Verbundprojekts "Sichere E-Geschäftsprozesse in KMU und Handwerk". Unter dem Dach des Netzwerks Elektronischer Geschäftsverkehr (NEG) sind neben dem ECC Handel Köln auch das SAGeG Chemnitz, TeleTrusT Berlin, das MECK Würzburg und das if(is) Gelsenkirchen an diesem Projekt beteiligt.

Weitere Informationen erhalten Sie unter:

<http://www.ec-net.de/sicherheit>.

### **Das Netzwerk Elektronischer Geschäftsverkehr (NEG)**

Das NEG ([www.ec-net.de](http://www.ec-net.de)) ist ein Verbund von bundesweit 29 regionalen Kompetenzzentren für den elektronischen Geschäftsverkehr und einem Branchenzentrum für den Handel (ECC Handel). Diese geben Mittelstand und Handwerk eine konkrete Hilfestellung beim Einstieg ins E-Business. Die Kompetenzzentren und Ihre Angebote werden durch das Bundesministerium für Wirtschaft und Technologie (BMWi) gefördert. Sie informieren kompetent mit langjähriger Erfahrung, neutral und kostenlos.

### **E-Commerce-Center Handel (ECC Handel)**

Das ECC Handel ([www.ecc-handel.de](http://www.ecc-handel.de)) wurde 1999 als Forschungs- und Beratungsinitiative unter der Leitung des Instituts für Handelsforschung an der Universität zu Köln ins Leben gerufen. Das Ziel ist es, insbesondere kleine und mittelständische Handelsunternehmen zum Thema E-Commerce zu informieren. Zahlreiche Aspekte des E-Commerce im Handel hat das ECC Handel in eigenen Studien untersucht. Es wird vom BMWi gefördert und ist in das NEG eingebunden.

### **Kontakt**

Andreas Duscha

Tel: 0221 943607-70

E-Mail: [a.duscha@ecc-handel.de](mailto:a.duscha@ecc-handel.de)