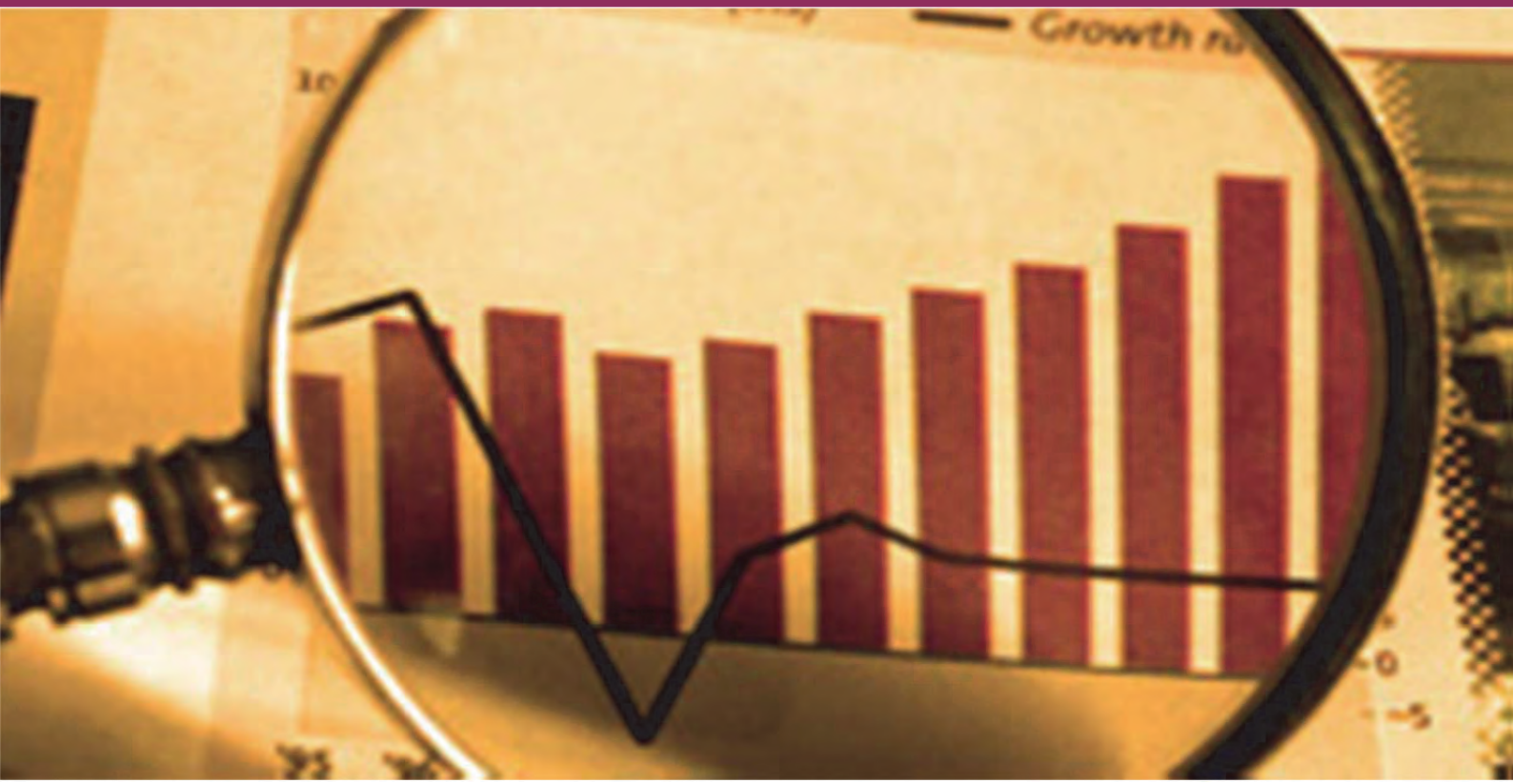


IT-SICHERHEIT UND IKS IM STEIRISCHEN MITTELSTAND

AKTUELLER STAND UND BEDEUTUNG

NOVEMBER 2016

PROF. (FH) DR. HELMUT MICHL | PROF. (FH) MAG. GREGOR REAUTSCHNIG

SANDRA KRIENDLHOFER | ROBERT MAGNES, BA | VERENA MAIER | KENO MISCHLING | CORNELIA PEUKER, BA | MICHAELA STOISER | CARMEN TSCHIGGERL

FH-STUDIENRICHTUNG RECHNUNGSWESEN & CONTROLLING

ENERGIE STEIERMARK

CAMPUS 02 GRAZ
FACHHOCHSCHULE DER WIRTSCHAFT

Inhalt

Sämtliche geschlechtsspezifischen Formen beinhalten aus Gründen der Einfachheit und Textökonomie auch die weiblichen Formen.

Vorwort

Cyberkriminalität ist nicht sofort sichtbar, wird oft erst spät entdeckt und kann dennoch verheerende Konsequenzen für ein Unternehmen nach sich ziehen. Damit ist diese spezielle Form der Kriminalität nicht nur ein Hindernis für die Digitalisierung und bedroht das Vertrauen in den technischen Fortschritt, sondern verunsichert Unternehmen im Zusammenhang mit dem Einsatz von IT. Sicherheitslösungen mit dem Schwerpunkt auf Erkennung und Beseitigung von Sicherheitsvorfällen sind nicht immer effektiv. Um sich gegen fortschrittliche und bisher unbekannte Bedrohungen zur Wehr zu setzen, ist eine kombinierte Strategie aus Erkennung und Prävention notwendig.

Das Interne Kontrollsystems (IKS) steht im Kontext mit dem IT-Risikomanagement und indirekt mit der IT-Security eines Unternehmens. Das IKS soll u.a. dafür sorgen, dass innerhalb von Unternehmensprozessen, also Business- wie auch IT-Prozessen, die Risiken minimiert werden, indem ausreichende "Kontrollmechanismen" implementiert werden. Ein unternehmerisches IKS besteht aus systematisch gestalteten, technischen und organisatorischen Regeln des methodischen Steuerns und Kontrollen zum Einhalten von Richtlinien und zur Abwehr von Schäden (die durch eigene Mitarbeiter oder Externe verursacht werden können). Die Maßnahmen können sowohl prozessunabhängig, als nachträgliche Kontrollen als auch prozessabhängig als präventive Regeln durchgeführt werden.

Die Interne Revision unterstützt die Organisation bei der Aufrechterhaltung wirksamer Kontrollen, indem sie deren Effektivität und Effizienz bewertet sowie kontinuierlich Verbesserungen fördert. Sie ist aber nicht für die Einführung spezifischer interner Kontrollverfahren verantwortlich. Dies obliegt der Geschäftsleitung und den operativ verantwortlichen Führungskräften.

Ziel der vorliegenden Studie war es, bei steirischen mittelständischen Unternehmen, explizit bei den IT-verantwortlichen Personen, zu erheben wie der Stand von allgemeinen und spezifischen Sicherheitsvorkehrungen im unternehmerischen Bereich eingeschätzt und darüber hinaus die generelle Bedeutung allgemeiner und spezifischer Sicherheitsrisiken beurteilt wird. Aus dieser Abfragekombination sollte sich eine mögliche Diskrepanz zwischen einer generell hohen Einschätzung eines Risikos und einer möglichen zu niedrigen Einschätzung der Umsetzung von Gegenmaßnahmen im eigenen Unternehmen als kritische Kombination erheben lassen. Es sollten aber nicht nur Defizite erhoben werden, sondern durch die Fragekombination sollte sich auch ableiten lassen, ob für hoch eingeschätzte Risiken bereits unternehmerische Vorsorge getroffen wurde.

Bereits im Vorfeld der Studie konnte mit Hilfe des Kooperationspartners, der Energie Steiermark AG, festgestellt werden, wie unbestreitbar wichtig die IT für alle Unternehmensprozesse ist und dass die entsprechende Risikovorsorge mitunter nicht nur technische Realisierungen benötigt, sondern, dass der Faktor Mensch bzw. Mitarbeiter intensiv in die Vorsorge miteinbezogen werden muss.

Im Zuge der Vorarbeiten für die Erstellung der Studie wurden von der Energie Steiermark AG Workshops an der FH CAMPUS 02 zu den Themen IKS und IT-Sicherheit abgehalten. Wir wollen uns deshalb speziell bei Herrn Dr. Markus Fally und Frau Mag. (FH) Lydia Kutil, MSc LL.M. als Leiter und Vertreterin der Internen Revision und Herrn Wolfgang Galler als Leiter der Konzern-IT der Energie Steiermark AG für den interessanten und wertvollen Input herzlich bedanken.

Prof. (FH) Dr. Helmut Michl
Studienrichtung RWC
CAMPUS 02
Fachhochschule der Wirtschaft GmbH

Prof. (FH) Mag. Gregor Reautschnig, StB
Studienrichtung RWC
CAMPUS 02
Fachhochschule der Wirtschaft GmbH

Für den Kooperationspartner Energie Steiermark AG:

Dr. Markus Fally
Leiter Interne Revision
Energie Steiermark AG

Mag. (FH) Lydia Kutil, MSc LL.M.
Internen Revision
Energie Steiermark AG

FH CAMPUS 02

Als Fachhochschule der Wirtschaft hat sich die FH CAMPUS 02 in Graz deutliche Schwerpunkte gesetzt: Die akademische Qualifizierung für berufliche Aufgaben in Kernfeldern des unternehmerischen Erfolgs, den stetigen Wissenstransfer zwischen Wirtschaft und Fachhochschule sowie die Förderung der Entwicklung persönlicher Sozial-, Führungs- und Wirtschaftskompetenzen. Die enge Vernetzung mit der Wirtschaft sichert den unmittelbaren Praxisbezug durch aktuelle Projekte mit konkreten Aufgabenstellungen aus den Unternehmen.

Rechnungswesen & Controlling

Die Studienrichtung Rechnungswesen & Controlling bildet die Schnittstelle zwischen topaktuellem Know-how und dem Bedarf der Wirtschaft. Zu folgenden drei Themenfeldern werden wissenschaftliche Studien und praxisnahe Analysen erarbeitet:

- **Controlling & Finance in der KMU-Praxis**
  Entwicklung unternehmensspezifischer **Controlling- und Finance-Lösungen**: z.B.
  - Der Controller/die Controllerin 4.0 – Anforderungsprofil, Kompetenzprofil und künftige Herausforderungen
  - Anwendungshäufigkeit, Ausgestaltung und Nutzen von Controlling-Instrumenten in heimischen KMU
  - Analyse und Identifikation von Verbesserungspotenzialen in betrieblichen Abläufen sowie deren Implikationen auf den Unternehmenserfolg
  - KMU-Finanzierung
  - Prozessmodellierung und -optimierung im Controlling
  - Kostenmanagement – Analyse von Effizienz steigernden Maßnahmen im internen Rechnungswesen
  - Analyse der Anforderungen an Jungunternehmer
  - Alternative Finanzierung von Neugründungen – Crowdfunding
  - Insolvenzprophylaxe durch die Identifizierung von Steuerungsgrößen für KMU

- **Treuhandwesen & Corporate Riskmanagement**
  Unternehmensspezifische Anforderungen an Steuerplanung, **Risikomanagement** oder das interne Kontrollsystem: z.B.

  - Analyse neuer Rechnungslegungsvorschriften, u.a. in der Finanzberichterstattung
  - Analyse von Gesetzesänderungen im Steuerrecht, mit Fokus auf Einkommen- und Körperschaftsteuer
  - Steuerbelastungsvergleich und Rechnungslegung auf Mikro- und Makroebene
  - Interne Kontrollsysteme (IKS) und IT-Sicherheit in Österreich
  - Ergebnisse und Aspekte der Digitalisierung bzgl. der Rechnungslegung sowie Analyse deren Auswirkungen
  - Corporate Riskmanagement als Bestandteil eines ganzheitlichen Unternehmensführungsmodells
  - Risikomanagement und Risikocontrolling in KMU (Risikoidentifikation und Risikobewertung, Risiko-Reporting und Risikosteuerungsmodelle, Prozessorientiertes Risikomanagement)
  - Risikomanagement entlang der betrieblichen Wertschöpfungskette

- **Nachhaltige Unternehmensführung & gesellschaftliche Verantwortung**
  Konzepte für ein **Sustainability Management und Accounting**: z.B.

  - Konzepte und Instrumente des Nachhaltigkeitsmanagement
  - Konzepterstellung für ein nachhaltiges Controlling und Reporting
  - Studien zur Umsetzung von Nachhaltigkeitsmaßnahmen in Unternehmen
  - Erstellung von Nachhaltigkeitsberichten
  - Umwegrentabilitätsstudien für Sport- & Kulturevents

Kernaussagen

IT-SICHERHEIT UND IKS IM STEIRISCHEN MITTELSTAND

- Die Umfrageergebnisse brachten insgesamt hohe Werte hinsichtlich der Bedeutungseinschätzung von Maßnahmen der IT-Sicherheit. Die befragten steirischen Mittelständler bewerten die Umsetzung dieser Maßnahmen im Unternehmen überwiegend als gut.
- Im Bereich spezifischer Einzelmaßnahmen, wie der Verwaltung der Passwörter oder Benutzerberechtigungen, der Datensicherung oder dem Einrichten von Firewalls, herrscht hohes Problembewusstsein; der Umsetzungsgrad war gemäß der Selbsteinschätzung der Unternehmen hoch.
- Überwiegend gute Werte weisen die Einzelmaßnahmen im Zusammenhang mit dem Zahlungsverkehr auf: eine sehr hohe Bedeutung wird klaren Vertretungsregeln und der strengen Trennung der Durchführung elektronischer Überweisungen von der Genehmigung beigemessen; die Selbsteinschätzung fiel dabei gut aus. Lediglich bei der Verwaltung von Lieferantenstammdaten zeigte sich Verbesserungspotenzial. So gaben 23% der Unternehmen an, bei Änderungen von Lieferantenstammdaten das Vier-Augen-Prinzip nicht anzuwenden.
- 54% der befragten steirischen Mittelständler wenden keinen IT-Standard an. Rund 23% setzen zumindest einen IT-Standard ein; die restlichen 23% verwenden mehr als einen Standard. Von denjenigen Unternehmen, die sich an einen Standard halten, wurde die Umsetzungsqualität von rund der Hälfte mit gut oder sehr gut bewertet.
- Es besteht noch bei vielen Unternehmen Handlungsbedarf hinsichtlich übergeordneter Maßnahmen, die den besonderen Rückhalt des Managements benötigen, wie zum Beispiel die Einbettung in das unternehmensweite Risikomanagementsystem, die regelmäßige Berichterstattung an das Management oder bewusstseinsbildende Maßnahmen und Mitarbeiterschulungen.
- Die Bedeutung regelmäßiger externer Audits und Penetration Tests (umfassende Sicherheits-Checks per simulierten Hacker-Angriff) wird nach Meinung der Verfasser von den steirischen Unternehmen unterschätzt. Bei der Selbsteinschätzung belief sich die Durchschnittsnote (nach dem Schulnotensystem) auf den niedrigen Wert von 3,1.

1. Einleitung

Leistungserstellungs- und Leistungsaustauschprozesse mittels Informations- und Kommunikationstechnik über öffentliche Netzwerke sind einer inhärenten Sicherheitsproblematik unterworfen. Der öffentliche Aspekt des Internets birgt Gefahren in sich: Manipulation, Spionage oder Sabotage von Informationen und Informationssystemen sind eine akute Gefahr bei der Nutzung elektronischer Medien. Informationen, Daten und Prozesse der Unternehmen sind in zunehmendem Maße IT-Sicherheitsrisiken ausgesetzt.[1]

IT-Sicherheit hat den Schutz von Informationen und sensibler Unternehmensdaten zu gewährleisten und sorgt für eine gesicherte Kommunikation unternehmensintern oder mit den Kunden und Lieferanten. Der Schutz gestaltet sich mitunter komplex: neben den Bestandteilen der IT-Infrastruktur selbst (u.a. Netzwerke, Systeme, Applikationen), sind auch die organisatorischen Faktoren (Schaffung von Verantwortlichkeiten, Weiterbildung/ Sensibilisierung der Mitarbeiter, Rollen und Berechtigungen etc.) bei der Gestaltung miteinzubeziehen.[2]

Um die Sicherheitsanforderungen der Geschäftsprozesse zu erfüllen, müssen nicht nur die IT-Systeme, sondern auch die von ihnen genutzten Ressourcen während der geforderten Zeiten abgesichert nutzbar sein. Die zunehmende Vernetzung mit Kunden und Lieferanten in digitalisierten Geschäftsprozessen vergrößert zudem das Schadenspotenzial.[3] Jedes noch so gut geplante IT-System ist verwundbar. Gezielte Angriffe durch unternehmensexterne Dritte oder eigene Mitarbeiter können zu Verlust oder Manipulation von Daten, Betriebsstillstand oder zur Verbreitung sensibler personenbezogener Daten führen.

Anfang des Jahres wurde das Unternehmen **FACC** Opfer von Internetbetrügern. Eine Mitarbeiterin der Firma erhielt eine vermeintliche Vorstands-E-Mail mit der dringenden Aufforderung, 50 Millionen Euro für eine streng geheime Firmenübernahme im Ausland zu überweisen. Die Betrüger zeigten nicht nur großes Geschick bei der Vortäuschung der Vorstands-E-Mail, sie wussten auch genau Bescheid darüber, wann sich dieser im Ausland befand bzw. gerade unerreichbar war und wen sie für die Überweisung kontaktieren mussten. Der Schaden belief sich auf rund EUR 50 Mio.; der Vorstand wurde mit sofortiger Wirkung abberufen.[4]

Einem anderen Betrugsszenario folgt der sogenannten „Locky"-Virus. Dabei handelt es sich um einen Trojaner, der von den gängigen Antiviren-Programmen teilweise nicht erkannt wird. Von den Betrügern werden täuschend echte Rechnungen per E-Mail verschickt. Öffnet

[1] Vgl. HEITMANN (2007), S. 9.
[2] Vgl. HEITMANN (2007), S. 10 f.
[3] Vgl. MÜLLER (2014), S. 15 f.
[4] O.V. [2016]: Nach Internetbetrug: Chef von Luftfahrtzulieferer FACC muss gehen: in derStandard vom 25.06.2016, http://derstandard.at/2000037606475/Chef-des-Luftfahrtzulieferers-FACC-muss-gehen, [18.10.2016].

der Empfänger den E-Mail-Anhang, breitet sich Locky auf Festplatten und Netzlaufwerken des betroffenen Systems aus und verschlüsselt sämtliche darauf befindlichen Daten. Die Betrüger wollen mit dieser Vorgehensweise Lösegeld erpressen. Erst nach Bezahlung des Lösegeldes werden die Daten wieder entschlüsselt.[5]

Locky-Virus und der Fall FACC sind typische Beispiele für schädliche Handlungen unternehmensexterner Dritter. Doch auch die eigenen Mitarbeiter können dem Unternehmen großen Schaden zufügen. Geheime Daten werden an Finanzbehörden („Steuer-CD") oder Konkurrenzunternehmen verkauft oder aus persönlichen oder politischen Gründen den Medien zugespielt („Panama Papers" oder ähnliche „Leaks").

Datenverlust kann durch Böswilligkeit oder aus Versehen verursacht werden. IT-Sicherheit bleibt nicht auf den Schutz vor externen Zugriffen beschränkt. Schutz vor Datenverlust umfasst auch Maßnahmen gegen höhere Gewalt, wie technische Gebrechen, Feuer- oder Wasserschäden. Schutzmaßnahmen sollen des Weiteren verhindern, dass an sich autorisierte Benutzer Fehler begehen, die sie nicht beabsichtigten. Es muss über Wege nachgedacht werden, wie versehentlicher und vorsätzlicher Datenverlust verhindert werden kann.[6]

Häufig liegt es am fehlenden Problembewusstsein, dass Mitarbeiter zu Opfern von Internetbetrügern werden. Beispielsweise versuchen so genannte „Phisher" über gefälschte E-Mails oder Internetseiten an persönliche Daten wie Konto- und Kreditkarteninformationen, Ausweis- und Reisepassnummern sowie Benutzernamen und Passwörter zu gelangen.[7]

Die angeführten Beispiele zeigen auch die enge Verflechtung von IT-Systemen mit dem internen Kontrollsystem. Das Funktionieren interner Kontrollen hängt immer häufiger von IT-gestützten Prozessen ab. Umgekehrt helfen Maßnahmen des internen Kontrollsystems dabei, den Betrieb des IT-Systems zu gewährleisten; wie beispielsweise die restriktive Vergabe von Zutrittsberechtigungen. Flankierend können das Vier-Augen-Prinzip oder Genehmigungsgrenzen Lücken der IT-Sicherheit schließen. Unternehmen müssen sich der Bedrohungen bewusst sein und durch entsprechendes Risikomanagement Systemmängel entdecken und beseitigen.

Ziel der Studie war es, den Umsetzungsstand ausgewählter Maßnahmen der IT-Sicherheit in den Unternehmen des steirischen Mittelstandes zu erheben. Im Rahmen eines Studierendenprojektes wurden anhand der Literatur die gängigsten Bedrohungen aufgelistet und kategorisiert. Die Bedrohungen lassen sich grob in schädliche Handlungen durch unternehmensexterne Dritte, schädliche Handlungen durch Mitarbeiter sowie höhere Gewalt einteilen. Im nächsten Schritt wurden Maßnahmen anhand einschlägiger IT-Standards erhoben, die ein

[5] Vgl. BEIERSMAN [2016]: Studie: Ransomware Locky für 6 Prozent aller Malware-Angriffe im September verantwortlich vom 21.10.2016, http://www.zdnet.de/88281428/studie-ransomware-locky-fuer-6-prozent-aller-malware-angriffe-im-september-verantwortlich/, [18.10.2016].
[6] Vgl. FRISCH (2003), S. 359.
[7] Vgl. VOLKMER/SINGER (2008), S. 118.

Schutzschild gegen die erwähnten Bedrohungen bilden. Der abgeleitete Maßnahmenkatalog stellte in der Folge die Basis der vorliegenden Umfrage dar, die anhand eines Online-Fragebogens durchgeführt wurde.

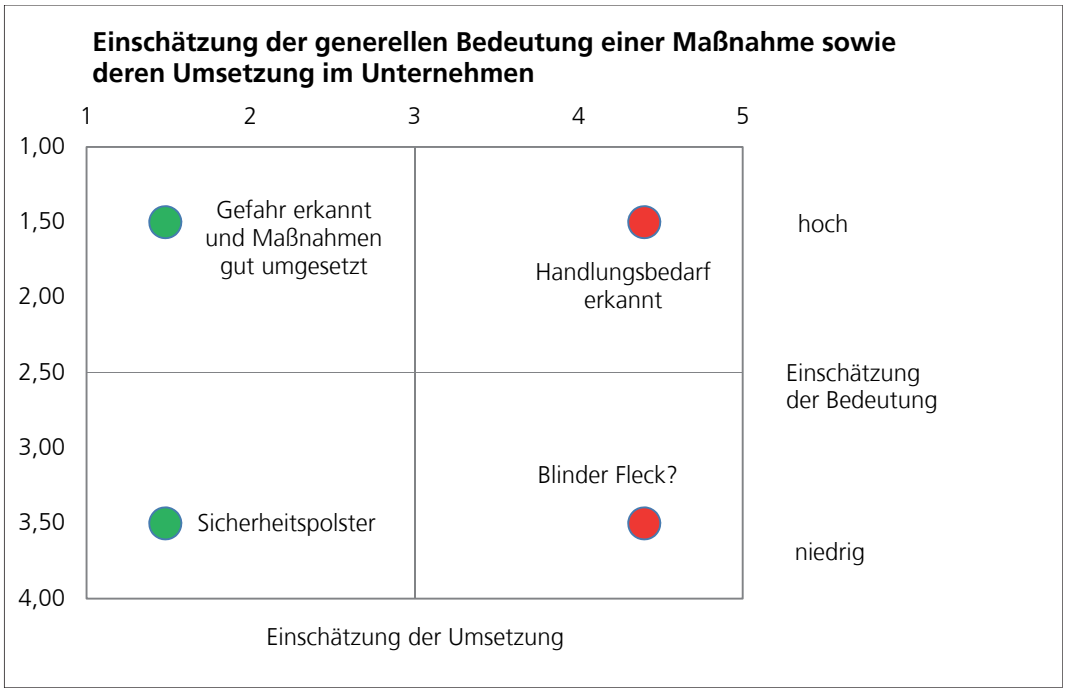
Im Rahmen der Erhebung war es nicht Ziel, die Unternehmen einer Qualitätsprüfung zu unterziehen. Stattdessen wurden die für die IT zuständigen Mitarbeiter – IT-Leiter oder ggf. Geschäftsführer – gebeten, eine Selbsteinschätzung vorzunehmen. Die IT-Zuständigen sollten für jede Maßnahme beurteilen, **wie gut oder schlecht diese im Unternehmen umgesetzt ist** und diese Einschätzung gemäß dem Schulnotensystem bewerten. So konnte für jede Maßnahme eine Durchschnittsnote der Umsetzung ermittelt werden.

Aufgrund des raschen technischen Fortschritts und der Findigkeit von Cyberkriminellen herrscht große Dynamik beim Aufkommen neuer Bedrohungsszenarien. Dem folgen mit zeitlicher Verzögerung immer neue Gegenmaßnahmen. Gerade kleinere Betriebe stehen vor der Frage, welche der unzähligen Maßnahmen nun tatsächlich umgesetzt werden müssen und welche nicht?

Die steirischen Mittelständler wurden daher im Rahmen der Studie auch befragt, **für wie bedeutend Sie eine Maßnahme generell halten**. Die Einstufungsskala reichte von 1 (besonders wichtig) bis 4 (unwichtig)[8]. In diesem Zusammenhang ist zu beachten, dass im Rahmen der Studie keine Aussagen darüber getroffen werden sollen, ob eine Maßnahme tatsächlich wichtig ist oder nicht. Erhoben wird nur, welche Maßnahmen für die Mehrzahl der Befragten von Bedeutung sind und welche nicht.

Die erhobenen Einschätzungen hinsichtlich der Bedeutung einer Maßnahme als auch deren Umsetzungsqualität im Unternehmen, lassen tiefere Analysen zu, wenn man die Ergebnisse zueinander in Bezug setzt. Stellt man die Ergebnisse in Form eines Portfolios dar, wird ein rascher Erkenntnisgewinn nach dem in folgender Abbildung dargestellten Muster möglich:

[8] Es wurde deshalb eine vierstufige Skala gewählt, um eine Tendenz zur Mitte zu vermeiden. Bei der Einschätzung der Umsetzungsqualität erschien dagegen das Schulnotensystem geeigneter. (Anm. der Verfasser)



Im linken oberen Quadranten des Portfolios finden sich jene Maßnahmen, deren Bedeutung für die IT-Sicherheit als hoch erachtet wird (Werte von 1 bis 2) und für die die Umsetzung im Unternehmen sehr gut benotet wurde. Anders formuliert: das Unternehmen hat die Gefahr erkannt und durch proaktives Handeln bereits gebannt. Das Unternehmen hat die betreffenden Risiken im Griff.

Im rechten oberen Quadranten finden sich ebenfalls Maßnahmen, denen eine hohe Bedeutung beigemessen wird. Allerdings wird deren Umsetzung im Unternehmen schlecht bewertet. Man ist sich darüber im Klaren, dass Handlungsbedarf besteht.

Im linken unteren Quadranten finden sich gut umgesetzte Maßnahmen, welche als unwichtig angesehen werden. Unternehmen haben einen Sicherheitspolster, da sie auch – nach eigener Auffassung – weniger bedeutende Mittel ergriffen haben, um die IT-Sicherheit zu gewährleisten.

Nun wäre es logisch konsequent, wenn man jene Maßnahmen, die man für weniger bedeutend erachtet, auch weniger gut umsetzt. Das spart Zeit und Kosten. Was aber, wenn man mit der eigenen Einschätzung der Bedeutung falsch liegt? Vielleicht ist es gerade diese eine Maßnahme, die helfen könnte, das Eintreten eines Risikos zu verhindern? Hier handeln oder besser gesagt „nichthandeln" Unternehmen ohne Netz, haben möglicherweise einen blinden Fleck. Die Bedrohungen werden nicht kleiner, wenn man sie negiert.

Das Portfolio wird im Rahmen der Studie für jedes erhobene Maßnahmenbündel verwendet, um etwaige Handlungspotenziale aufzuzeigen. Doch zuerst erfolgt in Kapitel 2 eine Beschreibung der methodischen Vorgehensweise, der fokussierten Grundgesamtheit und der

Stichprobenauswahl. In Kapitel 3 werden statistische Merkmale der Studienteilnehmer, wie die Unternehmensgröße oder Branchenherkunft zusammengefasst.

Die Detailergebnisse der Umfrage werden in Kapitel 4 und 5 präsentiert und kommentiert. Hinsichtlich der Maßnahmen erfolgte eine Trennung in spezifische (operative) Einzelmaßnahmen, die gegen konkrete Einzelbedrohungen wirken sollen, sowie übergeordnete allgemeinere Maßnahmen, die indirekte Wirkung entfalten. Zu letzteren zählen beispielsweise die Einbindung der IT-Sicherheit in das Risikomanagement oder die Bewusstseinsbildung der Mitarbeiter. Übergeordnete Maßnahmen bedürfen häufig eines besonderen Rückhalts durch die Unternehmensleitung. Sie weisen daher einen höheren Bezug zum Management auf als Einzelmaßnahmen wie beispielsweise die Einrichtung einer Firewall[9].

Die Ergebnisse hinsichtlich der übergeordneten Maßnahmen finden sich in Kapitel 4, jene zu den spezifischen Maßnahmen in Kapitel 5. In Kapitel 6 erfolgt eine resümierende Darstellung der zuvor im Detail beschriebenen Ergebnisse.

[9] Es liegt in der gesetzlichen Verantwortung des Managements, für ein funktionierendes internes Kontrollsystem (IKS) zu sorgen. Durch die enge Verflechtung der IT mit dem IKS resultiert eine besondere Verantwortlichkeit des Managements auch für das Thema IT-Sicherheit. (Anm. der Verfasser)

2. Empirische Erhebung

Untersuchungsgegenstand der vorliegenden Studie ist der steirische Mittelstand. Die Kategorisierung als „mittelständisch" wurde über die Mitarbeiterzahl vorgenommen. Als Grundgesamtheit wurden jene steirischen Unternehmen festgelegt, deren Mitarbeiteranzahl gemäß Herold-Unternehmensdatenbank zwischen 25 und 250 liegt. Nach Abzug jener Organisationen, wie zum Beispiel Schulen oder kommunale Einrichtungen, die ebenfalls in der Herold-Datenbank als Unternehmen geführt werden, ergab sich eine Grundgesamtheit von 631 Unternehmen.

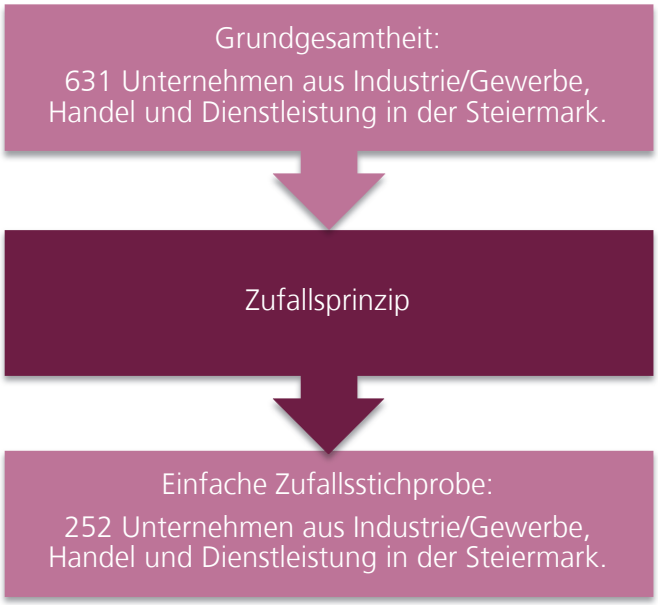
Grundgesamt der empirischen Untersuchung

Bei der Festlegung der für die Teilerhebung notwendigen Stichprobe wurde die einfache Zufallsstichprobe zur Auswahl der Untersuchungsobjekte angewendet. Um ein Vertrauensniveau von 95%, einen Stichprobenfehler von 10% bei Antwortverteilung von 50%, bezogen auf die Grundgesamtheit von 631, zu erreichen, war eine Mindeststichprobengröße von 84 Unternehmen erforderlich. Dieser Umfrage liegt unter der Annahme einer Rücklaufquote von 33,33% eine Stichprobe von 252 Unternehmen zu Grunde.

Die Unternehmen wurden nach dem Zufallsprinzip aus der Grundgesamtheit ausgewählt. Bei der Ziehung stellte sich heraus, dass einige Unternehmen derselben Unternehmensgruppe angehören. Dies hätte zu einer Verzerrung der Umfrageergebnisse geführt, weshalb immer nur ein Unternehmen pro Unternehmensgruppe in die Stichprobe aufgenommen wurde.

Entscheidend für das Ergebnis einer empirischen Studie ist die Identifikation der richtigen Ansprechperson, die stellvertretend für das jeweilige Unternehmen den Fragebogen ausfüllen soll. In der gegenständlichen Studie wurden als Personenkreis die IT-Zuständigen ausgewählt (IT-Leitung oder Geschäftsführung). Die 252 Unternehmen der Stichprobe wurden im nächsten Schritt telefonisch kontaktiert und der jeweilige IT-Zuständige hinsichtlich der Umfrageteilnahme befragt. Die Untersuchung wurde in Form eines standardisiertem Webfragebogens der Umfragesoftware Rogator durchgeführt.

Stichprobenermittlung für die Praxisstudie

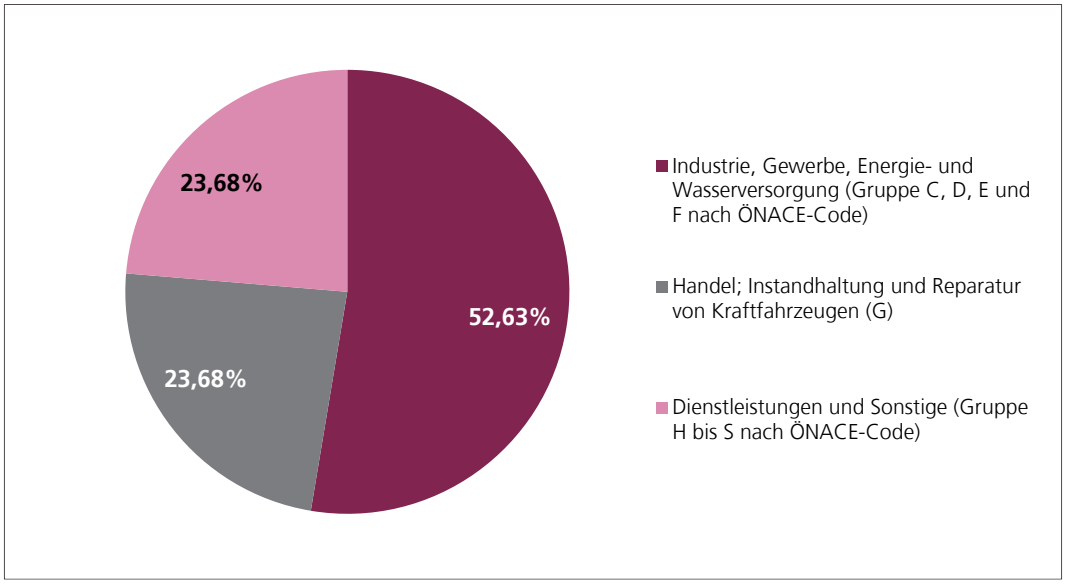


3. Charakterisierung der Studienteilnehmer

Im Zuge der vorliegenden Erhebung wurden die IT-Zuständigen angesprochen. Die Charakterisierung der Studienteilnehmer für diese Arbeit erfolgte über Unternehmensgröße, Branche und Abschlussprüfungspflicht. Die Unternehmensgröße wurde dabei über die Mitarbeiterzahl charakterisiert.

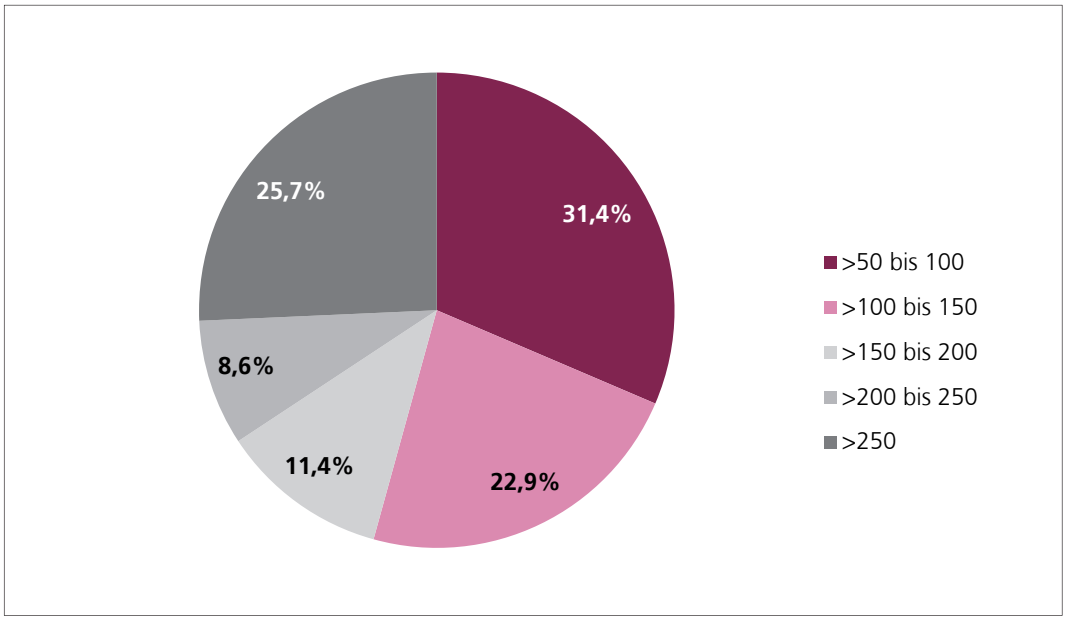
Für die Grundgesamtheit der Studienteilnehmer wurden steirische Unternehmen aus den verschiedensten Branchen ausgewählt. Die Verteilung der befragten Unternehmen zeigt folgendes Bild:

Studienteilnehmer nach Branchen



Den mit 52,63 % größten Anteil repräsentiert die Gruppe Industrie, Gewerbe, Energie- und Wasserversorgung. 23,68 % der befragten Unternehmen stammen aus der Gruppe Handel, Instandhaltung und Reparatur von Kraftfahrzeugen, weitere 23,68 % sind der Gruppe Dienstleistung und Sonstige zugeordnet.

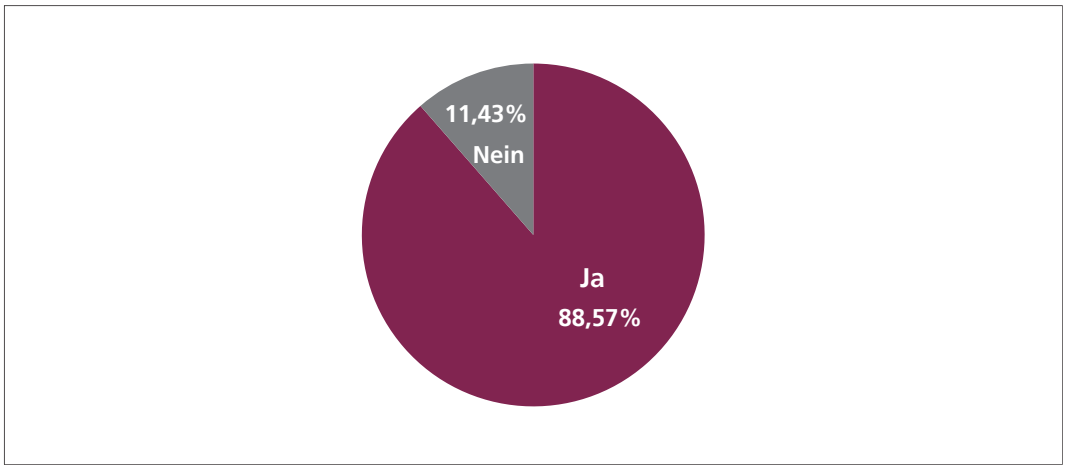
Studienteilnehmer nach Mitarbeiteranzahl



Die meisten der befragten Unternehmen (31,5 %) beschäftigen zwischen 50 und 100 Mitarbeiter. 22,9 % der Unternehmen beschäftigen zwischen 101 bis zu 150 Mitarbeiter. Rund 11,4 % der Unternehmen beschäftigen zwischen 151 und 200 Mitarbeiter, weitere 8,6 % zwischen 201 und 250 Mitarbeiter. Dass 25,7 % der Unternehmen eine Mitarbeiteranzahl über 251 angegeben haben, ist auf zweierlei Gründe zurückzuführen: Entweder erfolgte die Beantwortung nicht für die ausgewählte Einzelgesellschaft, sondern für die gesamte Unternehmensgruppe oder die in der Herolddatenbank angeführten Mitarbeiterdaten wurden nicht aktualisiert.

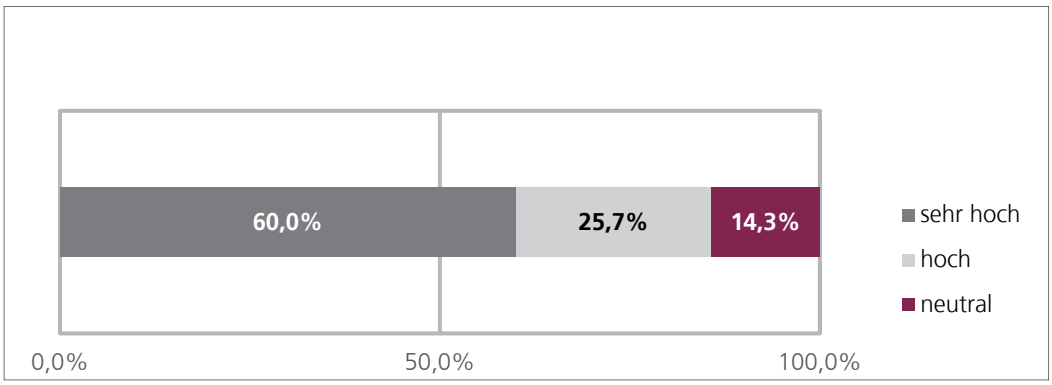
Eine weitere Charakterisierung der Studienteilnehmer erfolgt über das Kriterium, ob das Unternehmen der Abschlussprüfungspflicht unterliegt oder nicht.

Studienteilnehmer mit und ohne Abschlussprüfungspflicht



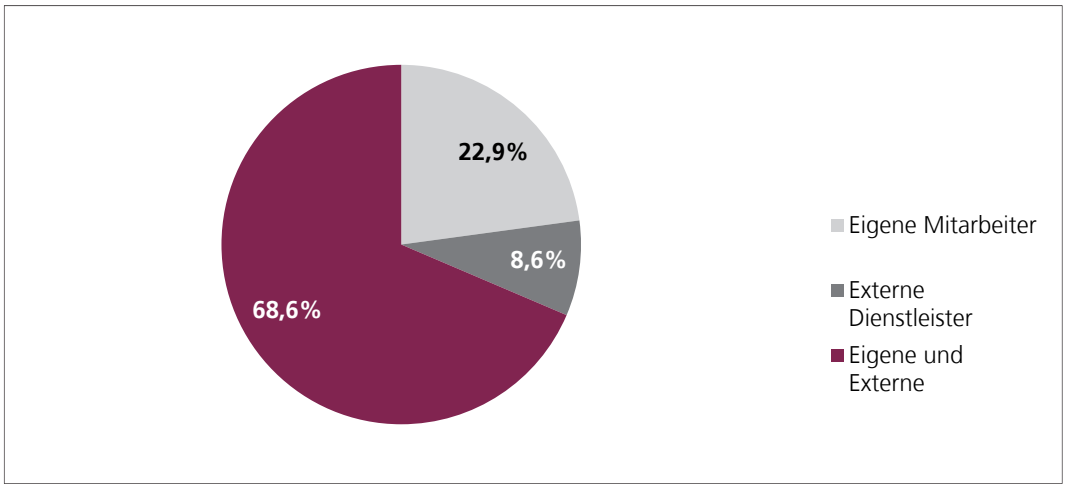
Wie aus der Abbildung hervorgeht, liegt bei 88,57 % der befragen Unternehmen die Abschlussprüfungspflicht vor. Bei den restlichen 11,43 % besteht keine Pflicht zur Abschlussprüfung. Prüfungspflichtige Unternehmen sollten grundsätzlich eine höhere Qualität bei internem Kontrollsystems und IT-Sicherheit erreichen als nicht prüfungspflichtige. Der hohe Anteil der prüfungspflichtigen Unternehmen unter den Studienteilnehmern sollte im Rahmen vorliegender Studie zu insgesamt besseren Ergebnissen bei der Umsetzung allgemeiner und spezifischer Maßnahmen der IT-Sicherheit führen.

Bedeutung der IT für das Unternehmen



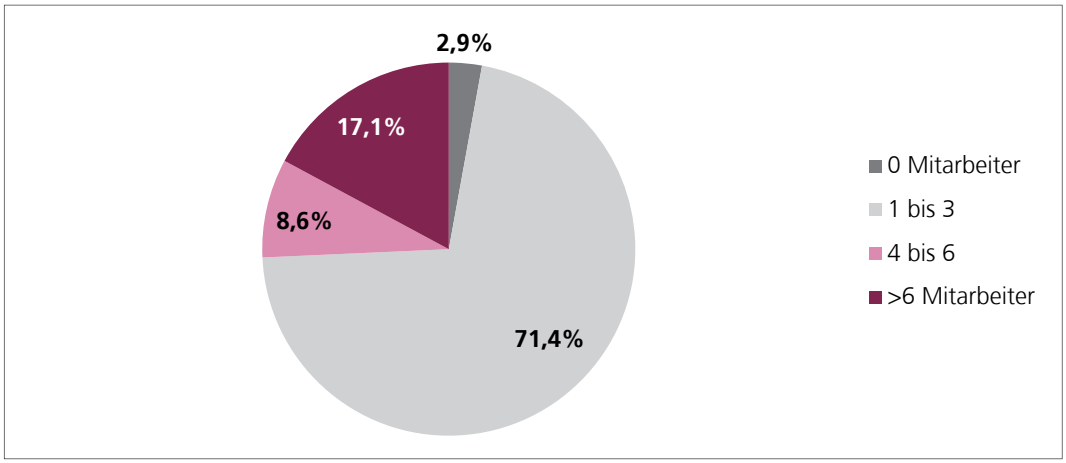
60 % der Unternehmen schätzen die Bedeutung der IT für das Unternehmen und dessen Kernprozesse als sehr hoch ein. 25,7 % bewerten die Bedeutung der IT als hoch, weitere 14,3 % schätzen diese Frage neutral ein. Insgesamt kann festgestellt werden, dass die Bedeutung der IT für mehr als 85% der Befragten hoch bzw. sehr hoch ist.

Zuständigkeit für die Wartung und Aktualisierung der IT-Systeme



Hinsichtlich der Zuständigkeit für Wartung und Aktualisierung der IT-Systeme geben 68,6 % der Unternehmen an, sowohl eigene Mitarbeiter als auch externe Dienstleister einzusetzen. Bei 22,9 % der Unternehmen sind ausschließlich eigene Mitarbeiter zuständig. Die restlichen 8,6 % haben die Zuständigkeiten gänzlich an externe Dienstleister vergeben.

Studienteilnehmer nach Anzahl der beschäftigten IT-Mitarbeiter



71,4 % der befragten Unternehmen beschäftigen zwischen 1 und 3 Mitarbeiter in der IT. Mehr als 6 Mitarbeiter setzen 17,1 % der Unternehmen ein. 8,6 % der Unternehmen beschäftigen zwischen 4 und 6 Mitarbeiter. 2,9 % beschäftigen keine Mitarbeiter in diesem Bereich.

4. Umsetzung und Bedeutung allgemeiner Maßnahmen der IT-Sicherheit

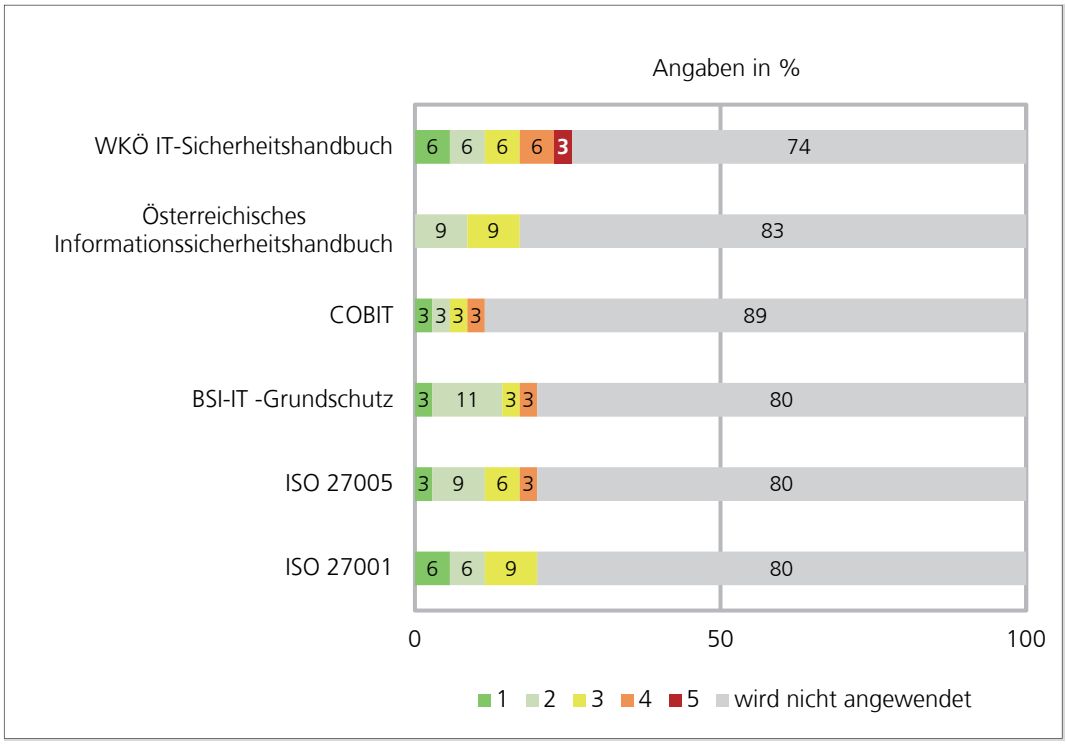
Aufgrund der zunehmenden Bedeutung der IT-Sicherheit, orientieren sich viele Unternehmen vermehrt an kodifizierten Mindeststandards. Ein Beispiel ist die Umsetzung und Zertifizierung nach ISO 27001[10]. Die Norm kann in das Managementsystem des Unternehmens integriert werden, um einen systematischen Prozess zur Minimierung der IT-Risiken umzusetzen. Weitere Normen bzw. Standards sind das WKÖ IT-Sicherheitshandbuch, das Österreichische Informationssicherheitshandbuch, COBIT, ISO 27005 oder der BSI-IT Grundschutz.

Die Umsetzung entsprechender Normen oder Standards bringt Unternehmen dazu, Ziele, Programme und Prozesse festzulegen. Dabei sollen Risiken identifiziert und bewertet sowie Maßnahmen zur Risikominimierung abgeleitet werden. Wichtiger Output der Umsetzung von Standards sind die Einführung von IT-Richtlinien, bewusstseinsbildende Maßnahmen unter den Mitarbeitern und die Festlegung klarer Verantwortlichkeiten. Das konsequente Beobachten und Überwachen der eingeleiteten Maßnahmen sollen einen kontinuierlichen Verbesserungsprozess initiieren und sind integraler Bestandteil typischer IT-Standards.[11]

In der Praxis gibt es keine absolute IT-Sicherheit. Es wird regelmäßig ein Restrisiko bestehen bleiben, da die Kosten für die Reduktion der Risiken progressiv ansteigen und diese ab einer bestimmten Umsetzungsintensität nicht mehr für das Unternehmen tragbar sind. Durch die rasche Weiterentwicklung der Technik entstehen zudem neue Sicherheitslücken und Angriffsmöglichkeiten. Was heute als sicher angesehen wird, kann in Kürze als unsicher gelten.[12]

[10] „IT – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen"
[11] Vgl. KERSTEN/REUTER/SCHRÖDER (2008), S 35 ff.
[12] Vgl. KERSTEN/KLETT (2015), S.6.

Anwendung von IT-Standards bzw. Empfehlungen

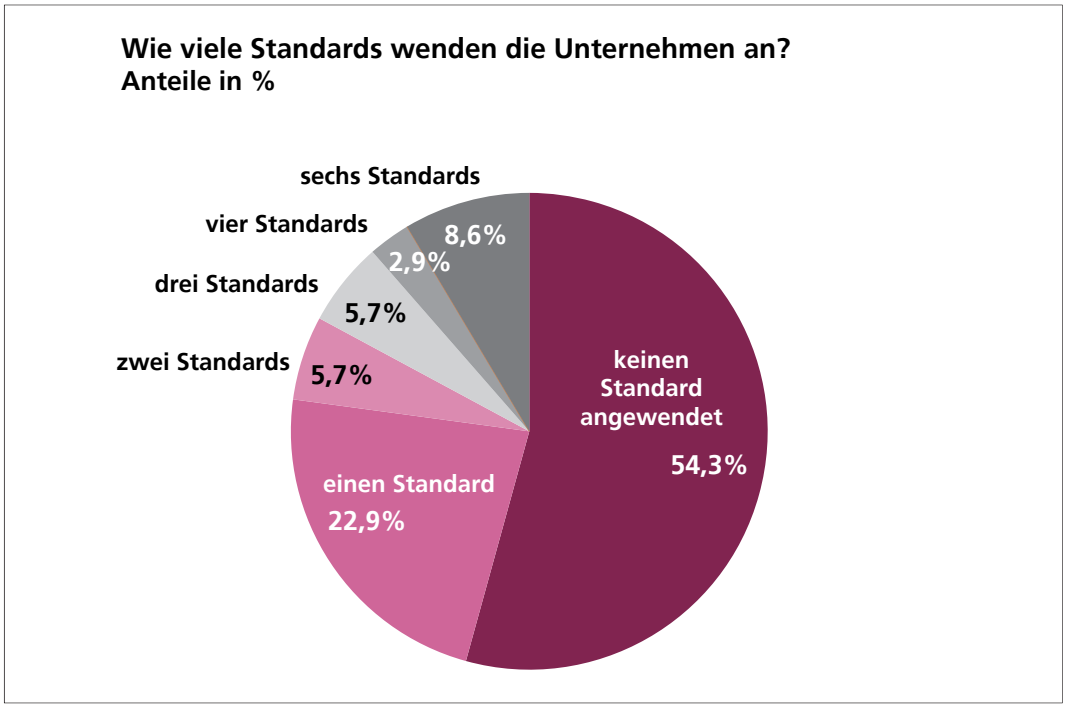


Im Rahmen der Umfrage wurde erhoben, welche Standards und Richtlinien bzw. übergeordnete Maßnahmen der IT-Sicherheit in den Unternehmen angewendet werden. Dabei wurden die IT-Zuständigen auch um eine Einschätzung der Qualität der Umsetzung in Form des Schulnotensystems gebeten.

Hinsichtlich der Anwendung von Standards zeigt sich bei den mittelständischen Unternehmen der Steiermark ein gewisser Aufholbedarf. Am häufigsten, nämlich von 26% der Unternehmen, wird das WKO IT-Sicherheitshandbuch eingesetzt; gefolgt von den Normen BSI-IT Grundschutz, ISO 27005 und ISO 27001 mit jeweils 20%. Das Österreichische Informationssicherheitshandbuch wenden 17% der befragten Unternehmen an. Die geringste Einsatzquote weist COBIT mit 11% der Befragten auf.

Von den Unternehmen, die eine Richtlinie anwenden, sind viele laut Eigeneinschätzung mit der Qualität der Umsetzung noch nicht restlos zufrieden. Die Note Sehr Gut geben sich bei der Umsetzung des WKÖ IT- Sicherheitshandbuches nur 6% aller Unternehmen (inklusive der nicht anwendbaren Fälle). Die Norm ISO 27001 haben ebenfalls nur 6% der Unternehmen sehr gut umgesetzt. Bei der Umsetzung des Österreichischen Informationssicherheitshandbuches gab sich kein einziges der betroffenen Unternehmen eine sehr gute Bewertung. Sehr gut bis gut schätzen sich je nach Norm 6% (bei COBIT) bis 14% (BSI-IT Grundschutz) ein.

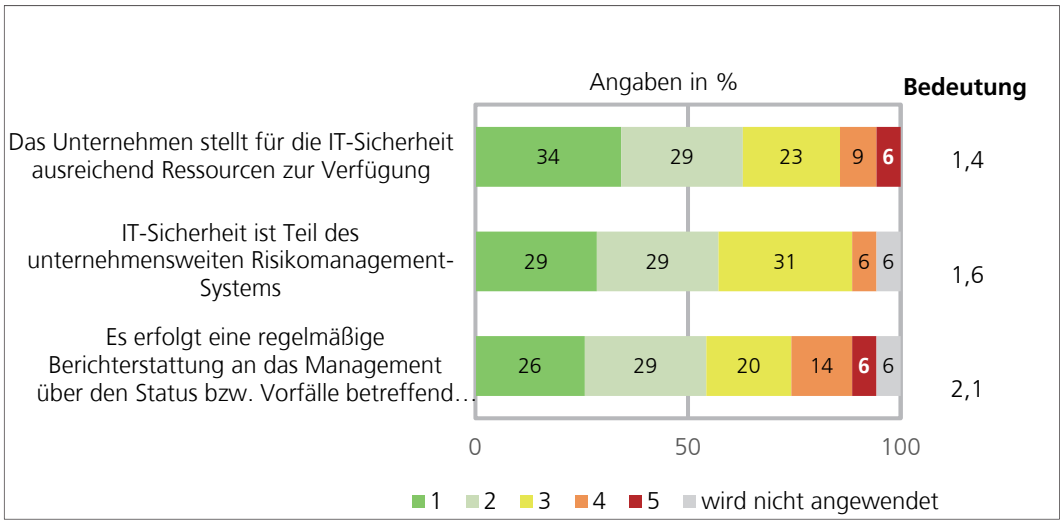
Die hohen Anteile der Nicht-Anwendung vermitteln auf den ersten Blick ein schlechtes Bild der Lage. Da bei dieser Fragestellung Mehrfachantworten möglich waren, stellte sich des Weiteren heraus, dass viele Unternehmen mehr als einen Standard anwenden. Es stellt sich somit die Frage, wie viele Unternehmen keine Standards anwenden und falls doch, wie viele Standards? In der folgenden Abbildung werden die Anteile der Unternehmen dargestellt, die keinen, einen oder mehr Standards einsetzen.



Mehr als die Hälfte der befragten Unternehmen wenden keinen Standard an, rund 23% zumindest einen. Die restlichen 23% geben an, mehr als einen Standard einzusetzen, wobei sich gezeigt hat, dass diese Unternehmen laut Selbsteinschätzung einzelne Standards besser, andere weniger gut umgesetzt haben.

Der hohe Anteil an Unternehmen, die keine Standards oder Normen anwenden lässt den Schluss zu, dass noch großer Handlungsbedarf besteht, denn die konsequente Umsetzung von IT-Standards führt zu einer Professionalisierung der IT und hilft, alle Facetten der IT-Sicherheit in vollem Umfang zu betrachten.

Umsetzung von übergeordneten Maßnahmen mit direktem Bezug zum Management

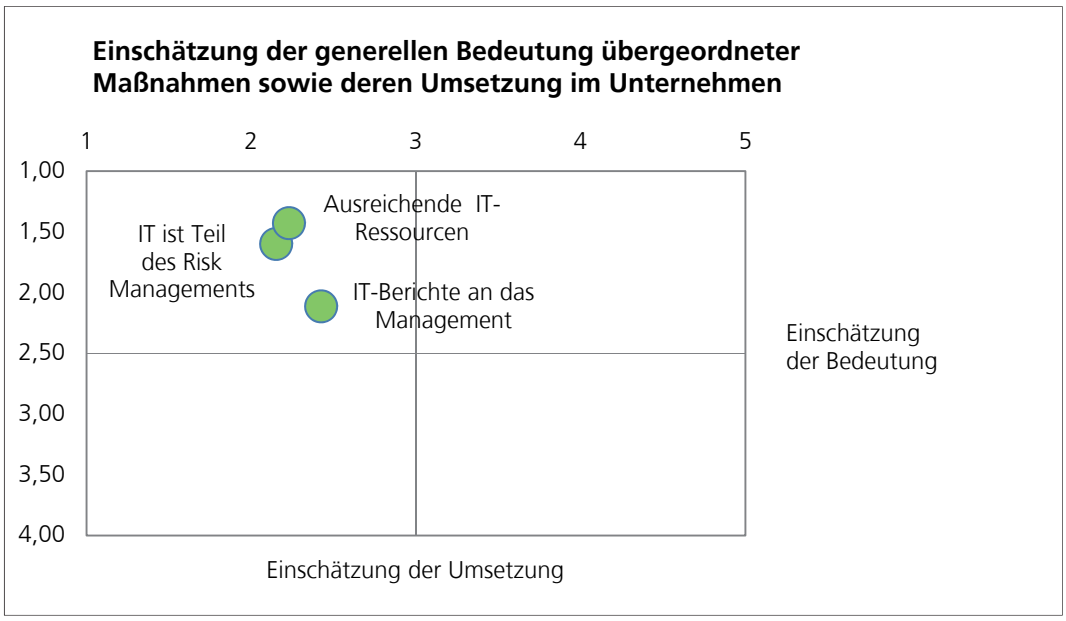


Bei den in der Abbildung dargestellten Fragestellungen handelt es sich um übergeordnete Maßnahmen bzw. Rahmenbedingungen mit engem Konnex zur Unternehmensleitung und entsprechend großer Hebelwirkung. Der Anwendungsgrad ist dabei überwiegend hoch. Die IT-Zuständigen wurden einerseits um eine generelle Einschätzung der Bedeutung gebeten (mit 1 = hohe Bedeutung bis 4 = geringe Bedeutung). Des Weiteren sollten Sie die Qualität der Umsetzung im eigenen Unternehmen gemäß Schulnotensystem beurteilen (1 = Sehr Gut bis 5 = Nicht Genügend).

Die größte Bedeutung wird dem Thema Ressourcenausstattung beigemessen. Der Durchschnittswert 1,4 zeigt dies deutlich, bei nur sehr geringer Varianz der Antworten. Rund 63 % der mittelständischen Unternehmen schätzen die Ressourcenausstattung der IT-Sicherheit als sehr gut oder gut ein. Im Gegensatz dazu beurteilen 15 % der IT-Zuständigen die Ressourcenausstattung mit Genügend oder Nicht Genügend.

Die Einbettung der IT-Sicherheit in das unternehmensweite Risikomanagement-System stellt eine grundlegende Maßnahme mit großer Hebelwirkung dar. Hinsichtlich Bedeutung wurde mit 1,6 kein Spitzenwert erreicht. Mit 58 % schätzt mehr als die Hälfte der Unternehmen diese Einbettung als sehr gut oder gut ein. Der Anteil unzufriedener Unternehmen ist mit 6 % relativ gering. Dass die IT-Sicherheit nicht Teil des Risikomanagement-Systems ist, kommt nur bei 6 % der Befragten vor. Die regelmäßige Berichterstattung an das Management wird als weniger bedeutend eingeschätzt (Wert von 2,2). Immerhin 55 % der Studienteilnehmer schätzen die Berichterstattung als sehr gut oder gut ein. Die geringere Bedeutung findet ihren Niederschlag im hohen Anteil jener Unternehmen, die die Berichterstattung mit genügend oder nicht genügend beurteilen; immerhin 20 %.

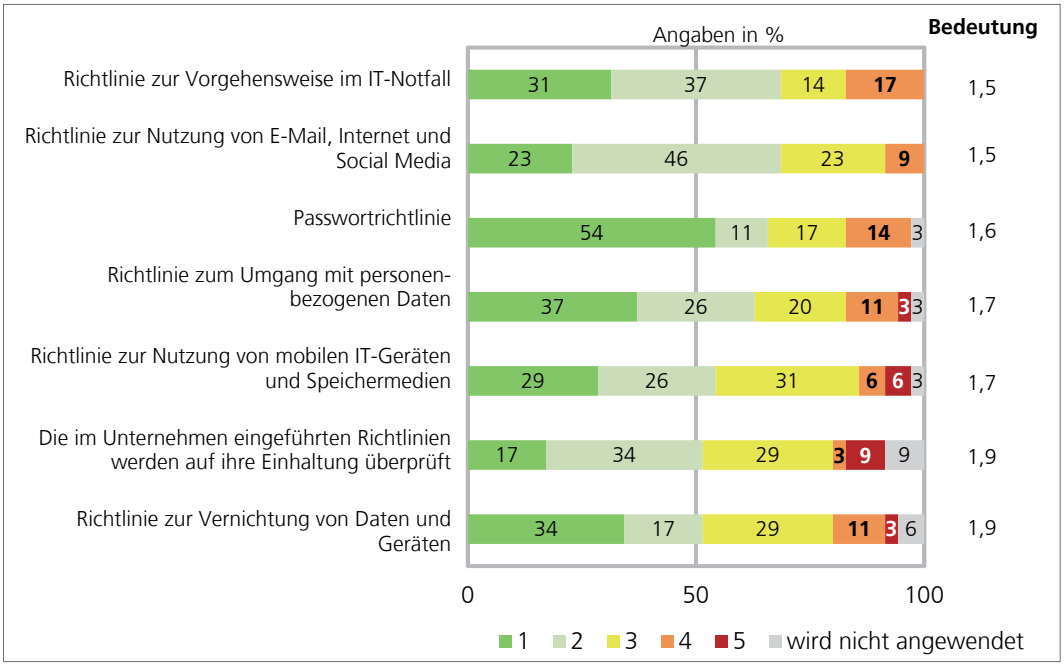
Setzt man die Einschätzung der Unternehmen hinsichtlich der allgemeinen Bedeutung einer Maßnahme in Bezug zur Selbsteinschätzung der Umsetzungsqualität, lassen sich die Umfrageergebnisse in eine Portfoliostruktur bringen, die sich wie folgt darstellt:



Auf der X-Achse des Portfolios findet sich die Schulnotenskala für die Einschätzung der Maßnahmenumsetzung von 1 bis 5; auf der Y-Achse die Einschätzung der generellen Bedeutung einer Maßnahme von 1 (hoch) bis 4 (geringe Bedeutung). Im linken oberen Quadranten befinden sich somit jene Maßnahmen, die als wichtig und als gut bis sehr gut umgesetzt eingeschätzt wurden. Bei der Ermittlung der Durchschnittsnote für die Umsetzungsqualität wurden jene Studienteilnehmer ausgeklammert, die bei der Maßnahme „nicht anwendbar" angekreuzt haben.

Die ausreichende Ressourcenausstattung der IT-Sicherheit wurde von den Unternehmen mit durchschnittlich 2,23 benotet. Die Einbettung der IT-Sicherheit in das unternehmensweite Risikomanagement bewerteten die Befragten mit 2,15 durchschnittlich etwas besser. Am schlechtesten fiel die Einschätzung der Umsetzungsqualität hinsichtlich der regelmäßigen Berichterstattung an das Management mit einem Durchschnittswert von 2,42 aus.

Anwendung von Richtlinien im Unternehmen



Es zeigte sich, dass die abgefragten Richtlinien einen sehr hohen Anwendungsgrad in den Unternehmen aufweisen. Richtlinien zu IT-Notfällen oder zur Nutzung von E-Mail, Internet und Social Media wurden in allen mittelständischen Betrieben erlassen. Bei allen angeführten Richtlinien ergaben die Selbsteinschätzungen zu mehr 50 % die Noten Sehr Gut oder Gut.

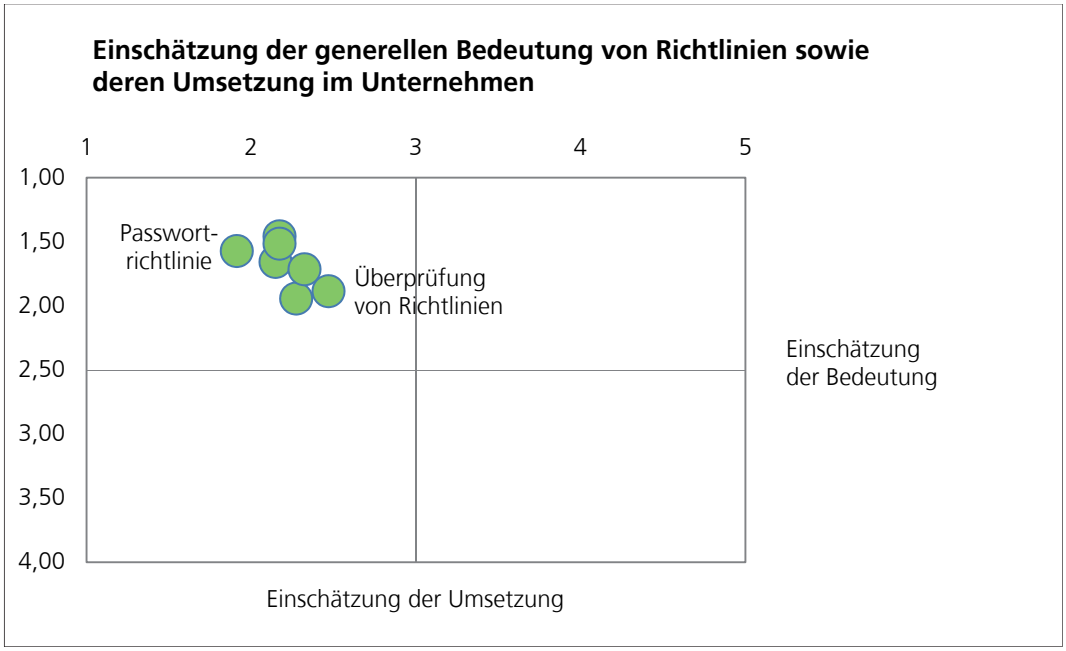
Als Spitzenreiter stellte sich die Passwortrichtlinie heraus, für die die Umsetzungsqualität von mehr als 54 % der mittelständischen Unternehmen als sehr gut angesehen wird. 14 % der IT-Zuständigen vergaben dabei die Note Genügend. Auch bei den Richtlinien für IT-Notfälle und zur Nutzung von E-Mails, Internet und Social Media korrelieren Wichtigkeit (1,5 bei geringer Varianz) mit der Einschätzung der Umsetzungsqualität bei den Unternehmen.

Etwas weniger bedeutend wird eine Richtlinie zur Datenvernichtung erachtet, wenngleich auch hier mit 51% Sehr Gut oder Gut eine hohe Umsetzungsqualität erreicht wurde.

Es wurde darüber hinaus gefragt, ob die im Unternehmen eingeführten Richtlinien regelmäßig auf ihre Einhaltung überprüft werden. Überwachungsmaßnahmen wie diese sollen eine ständige Qualitätsverbesserung im Unternehmen bewirken. Die Bedeutung dieser Maßnahme wurde 1,9 als relativ gering angesehen, was den höchsten Wert bei der Nichtanwendung von 9% erklärt. Ebenfalls 9% der Unternehmen benoten die Umsetzung der Richtlinienüberwachung mit Nicht Genügend. Der Anteil der sehr guten Umsetzung ist mit 17% am geringsten aller Fragestellungen dieses Fragekomplexes. Ähnlich den übergeordneten Maß-

nahmen mit direktem Bezug zum Management, wäre hier ein Verbesserungspotenzial gegeben.

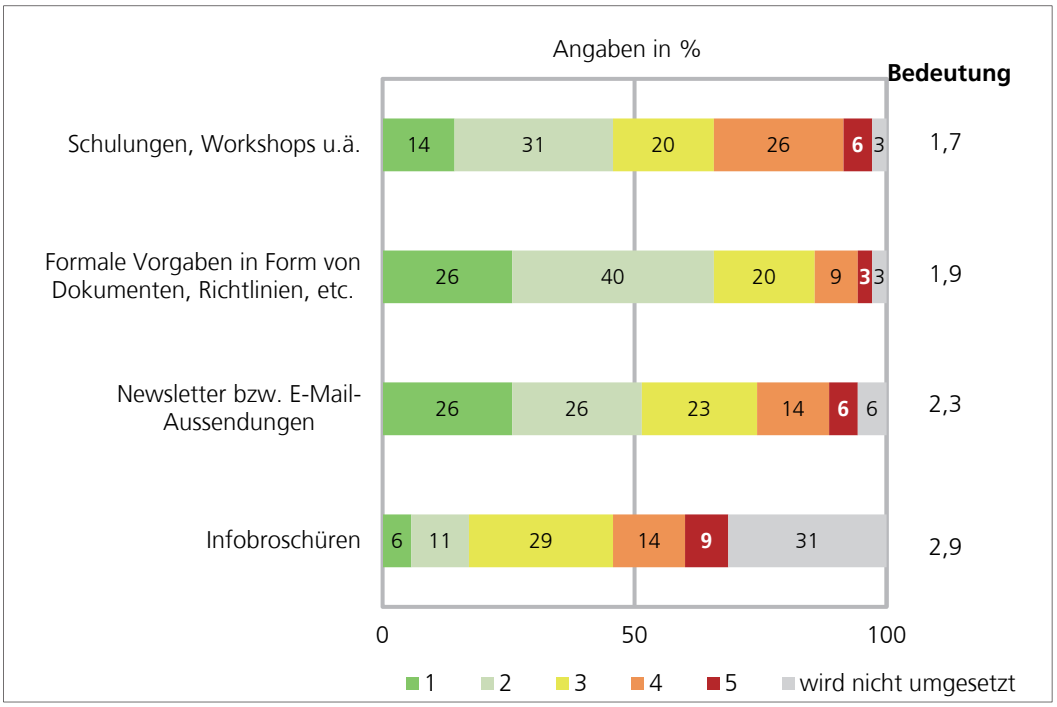
Setzt man die Einschätzung der Bedeutung mit jener der Umsetzungsqualität zueinander in Beziehung, ergibt sich folgendes Portfolio:



Das Portfolio zeigt ein ausgewogenes Bild: die Bedeutungseinschätzungen erreichen für alle abgefragten Richtlinien relativ hohe Werte (zwischen 1,5 und 1,9). Die durchschnittlichen Einschätzungen der Umsetzung fielen generell gut aus (s.a. Tabelle unten). Aus Darstellungsgründen musste auf die Beschriftung aller Datenpunkte verzichtet werden. Die Punkte des Koordinatenkreuzes lassen sich anhand der unten dargestellten Tabellen den einzelnen Richtlinien zuordnen. Die Koordinaten für die Passwortrichtlinie (äußerster linker Punkt) betragen auf der X-Achse 1,91 (Umsetzung) und auf der Y-Achse 1,57 (Bedeutung).

Maßnahme	Einschätzung der Umsetzung	Einschätzung der Bedeutung
Passwortrichtlinie	1,91	1,57
Richtlinie zum Umgang mit personenbezogenen Daten	2,15	1,66
Richtlinie zur Vorgehensweise im IT-Notfall	2,17	1,46
Richtlinie zur Nutzung von E-Mails, Internet und Social Media	2,17	1,51
Richtlinie zur Datenvernichtung und Geräteentsorgung	2,27	1,94
Richtlinie zur Nutzung von mobilen IT-Geräten und Speichermedien	2,32	1,71
Die im Unternehmen eingeführten Richtlinien werden regelmäßig auf ihre Einhaltung überprüft.	2,47	1,89

Umsetzung bewusstseinsbildender Maßnahmen im Unternehmen

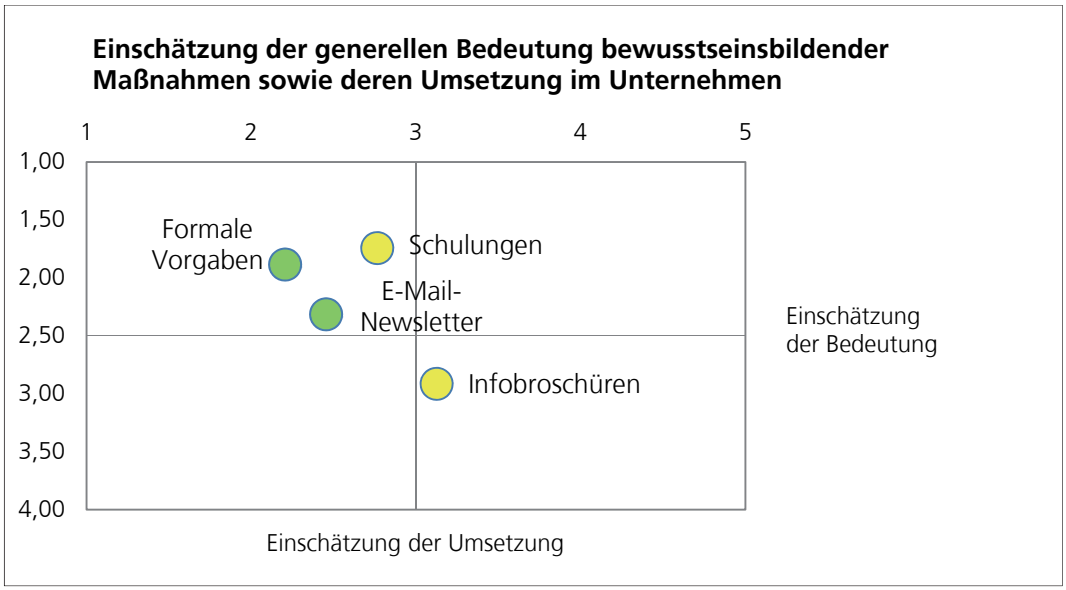


Die Gewährleistung der IT-Sicherheit hängt zu großen Teilen von der technischen Infrastruktur im Unternehmen ab. Es wäre ein großer Fehler, die Anwender nicht einzubeziehen. Viele Attacken werden erst durch unwissende oder achtlose Mitarbeiter ermöglicht. Bewusstseinsbildenden Maßnahmen kommt daher eine hohe Bedeutung zu. Knapp 97 % der mittelständischen Unternehmen führen Schulungen und Workshops für IT-Sicherheit im Unternehmen durch. Davon beurteilen 45 % die Umsetzung mit Sehr Gut oder Gut. Beachtlich ist jedoch der hohe Anteil unzufriedener IT-Verantwortlicher, denn 26 % beurteilen die Umsetzung mit Genügend und 6 % mit Nicht Genügend.

Deutlich besser werden bewusstseinsbildende Maßnahmen in Form von Richtlinien benotet. Mehr als die Hälfte der Studienteilnehmer schätzen die Umsetzung von formalen Vorgaben sehr gut oder gut ein. Der Anteil genügender oder nicht genügender Beurteilungen liegt mit 12 % deutlich unter jenem betreffend Schulungen.

Deutlich geringer wird die Bedeutung von Newslettern (2,3) oder Infobroschüren (2,9) angeführt. Entsprechend nehmen die Anteile jener Unternehmen zu, die diese Maßnahmen nicht umsetzen. Auf Infobroschüren verzichten mehr als 31% der Unternehmen. Vom Rest wird die Umsetzungsqualität überwiegend mit Befriedigend (29%) oder Genügend (14%) bewertet.

Das Portfolio aus der Einschätzung der Bedeutung und der Umsetzung im Unternehmen zeigt folgendes Bild:



Den Mitarbeiterschulungen wurde mit dem Wert 1,7 die größte Bedeutung beigemessen. Die Umsetzung im eigenen Unternehmen fällt dagegen mit einer durchschnittlichen Bewertung von 2,76 deutlich ab. Hier besteht Handlungsbedarf.

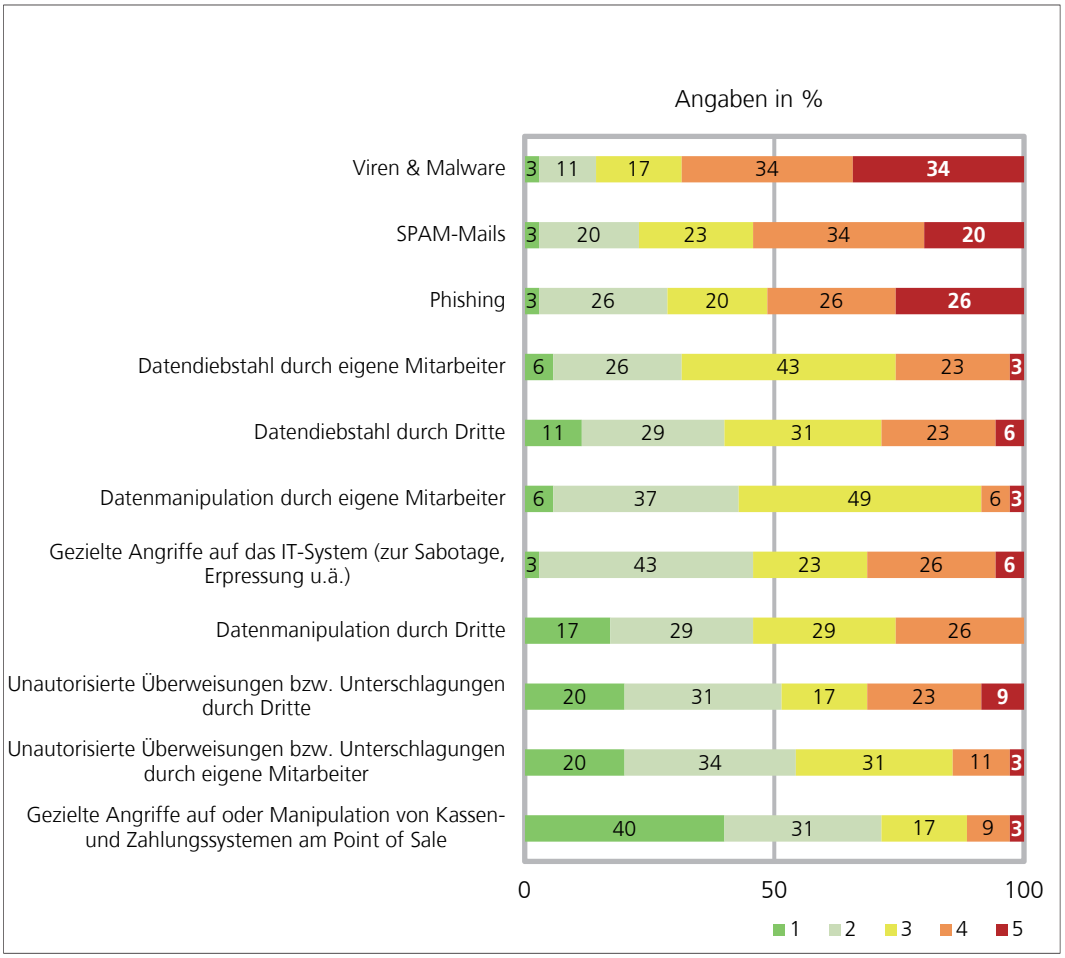
Formale Vorgaben (Durchschnittswert 2,21) und E-Mail-Newsletter (2,45) wurden hingegen betreffend Umsetzung besser eingeschätzt. Die als weniger bedeutend erachteten Infobroschüren werden hinsichtlich der Umsetzung durchschnittlich mit 3,13 benotet.

Maßnahme	Einschätzung der Umsetzung	Einschätzung der Bedeutung
Formale Vorgaben	2,21	1,89
E-Mail-Newsletter	2,45	2,31
Schulungen	2,76	1,74
Infobroschüren	3,13	2,91

5. Umsetzung und Bedeutung spezifischer Maßnahmen der IT-Sicherheit

In Kapitel 5 wird der Fokus auf eine Vielzahl von Einzelmaßnahmen gelegt. Die IT-Zuständigen sollten wieder die generelle Bedeutung einer Maßnahme und darüber hinaus die Umsetzungsqualität im eigenen Unternehmen beurteilen. Am Beginn des Kapitels steht jedoch die Frage, welche Bedrohungen der IT-Sicherheit – von Viren, Phishing bis zur Datenmanipulation durch eigene Mitarbeiter – von den IT-Zuständigen als am größten eingeschätzt werden. Daran anschließend wurde erhoben, welche dieser Bedrohungen in den Unternehmen bereits schlagend wurden.

Bedrohungen für die IT-Sicherheit und den elektronischen Zahlungsverkehr

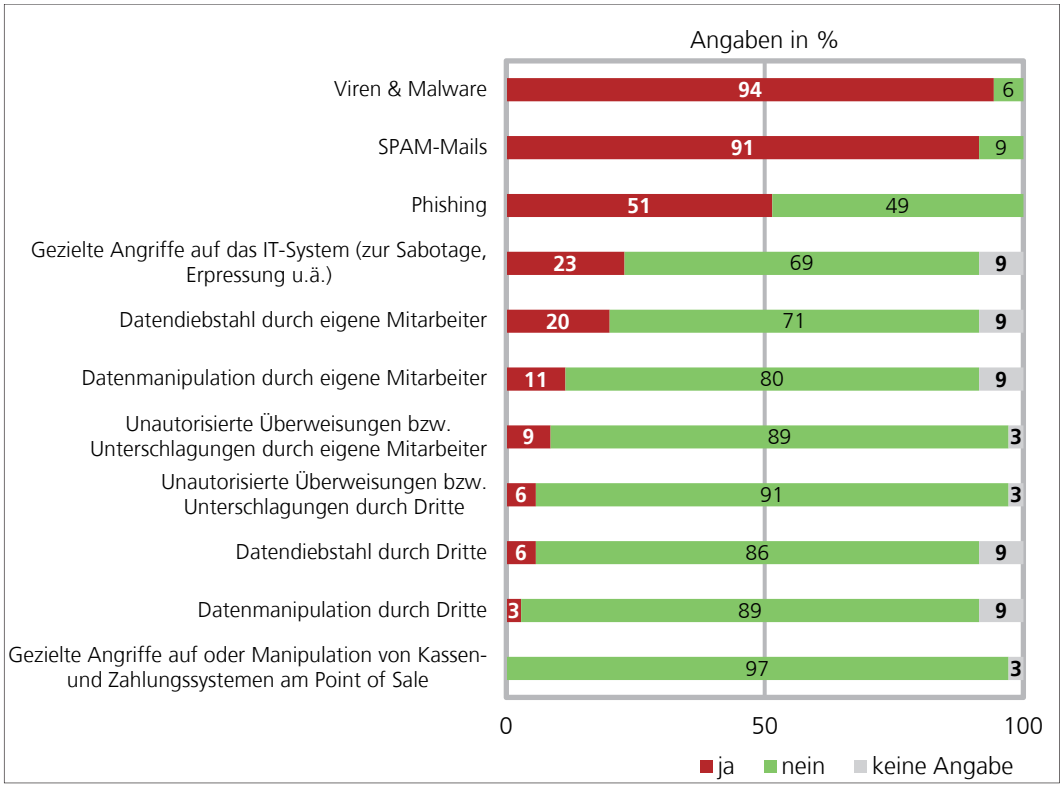


In der oben dargestellten Grafik ist das Ausmaß der Bedrohungen dargestellt, wobei 1 ein geringe Bedrohung symbolisiert und 5 eine hohe. Es erfolgte eine Reihung der Bedrohungen anhand des Anteils der kumulierten niedrigen Einschätzungen der Stufe 1 bzw. 2: je niedriger der Anteil der niedrigen Einschätzungen der Stufen 1 und 2, desto höher wird das Bedrohungspotenzial eingeschätzt.

Die häufigste Bedrohung sehen die Studienteilnehmer in Viren und Malware, Spam-Mails sowie Phishing-Attacken. Das könnte daher rühren, dass viele bereits mit diesen Risiken konfrontiert wurden, wie sich auch aus der nachfolgenden Fragestellung ergibt. Auf Platz vier folgt bereits die Bedrohung des Datendiebstahls durch eigene Mitarbeiter, die von 2/3 der Befragten als mittelstark bis stark eingeschätzt wurde. Etwas geringer wird das Risiko des Datendiebstahls durch unternehmensexterne Dritte eingeschätzt.

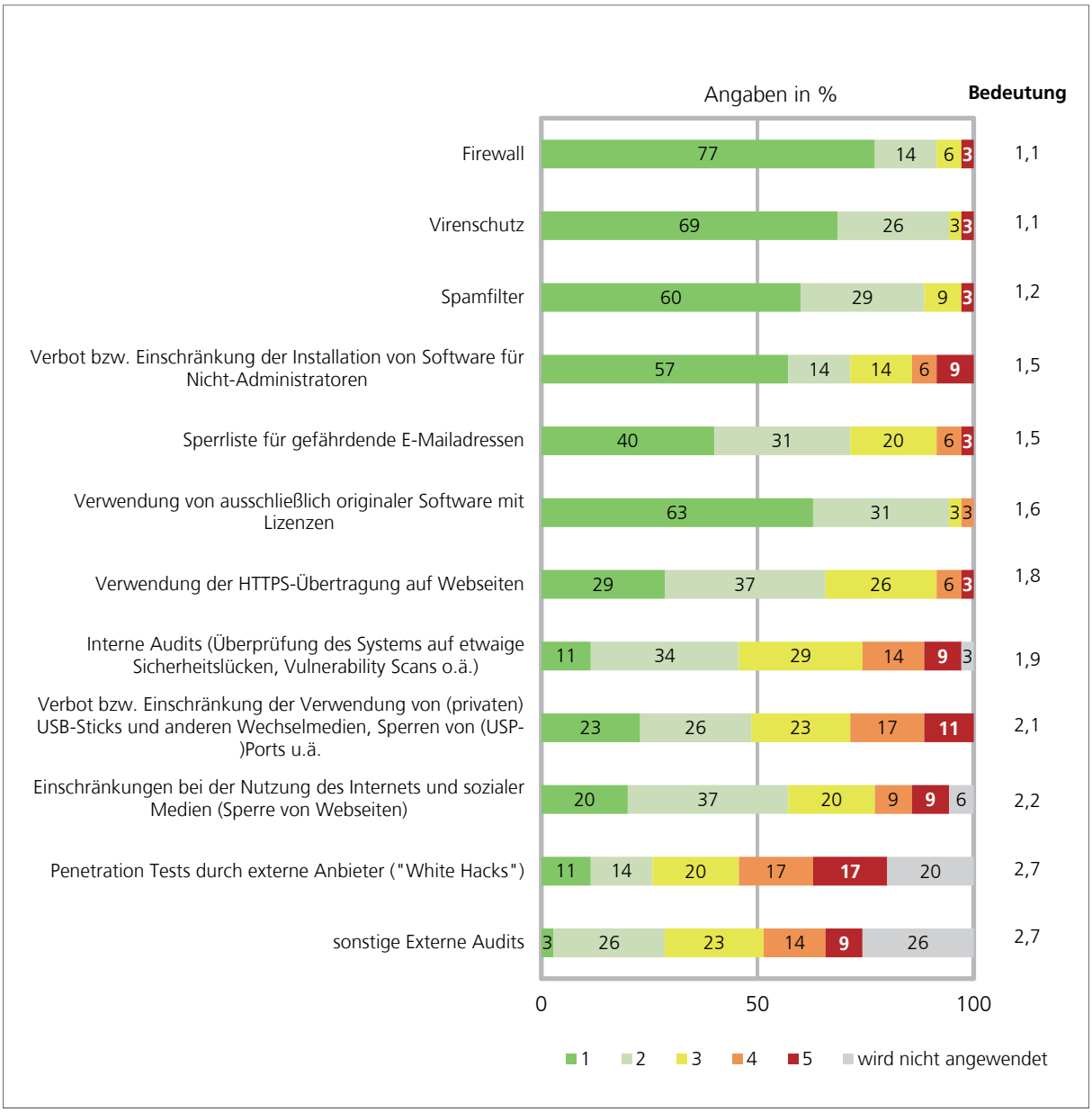
Das Risiko unautorisierter Überweisungen und Unterschlagungen von Geld wird deutlich geringer eingeschätzt: jeweils weniger als 50% gehen von einer mittelstarken bis starken Bedrohung aus. An letzter Stelle rangieren Angriffe auf oder die Manipulation von Kassen- und Zahlungssystemen am Point of Sale. Von einer mittelstarken bis starken Bedrohung gehen rund 29% der Unternehmen aus.

Im Unternehmen eingetretene Bedrohungen



Die Frage, welche Bedrohungen bereits im Unternehmen eingetreten sind, führte zu ähnlichen Ergebnissen. 94 % der Studienteilnehmer gaben an, bereits mit Viren und Malware konfrontiert gewesen zu sein. Von Spam-E-Mails sind rund 91 % der Befragten betroffen. Mehr als die Hälfte (51%) verzeichnete Fälle von Phishing. Deutlich geringer ist der Anteil jener Unternehmen, die gezielten Hacker-Attacken zur Sabotage oder Erpressung ausgesetzt waren (23%), knapp gefolgt von Datendiebstahl durch Mitarbeiter mit 20%. Von Datenmanipulation durch eigene Mitarbeiter waren 11 % der Studienteilnehmer betroffen.

Maßnahmen, die das Risiko eines Befalls mit Schadsoftware minimieren

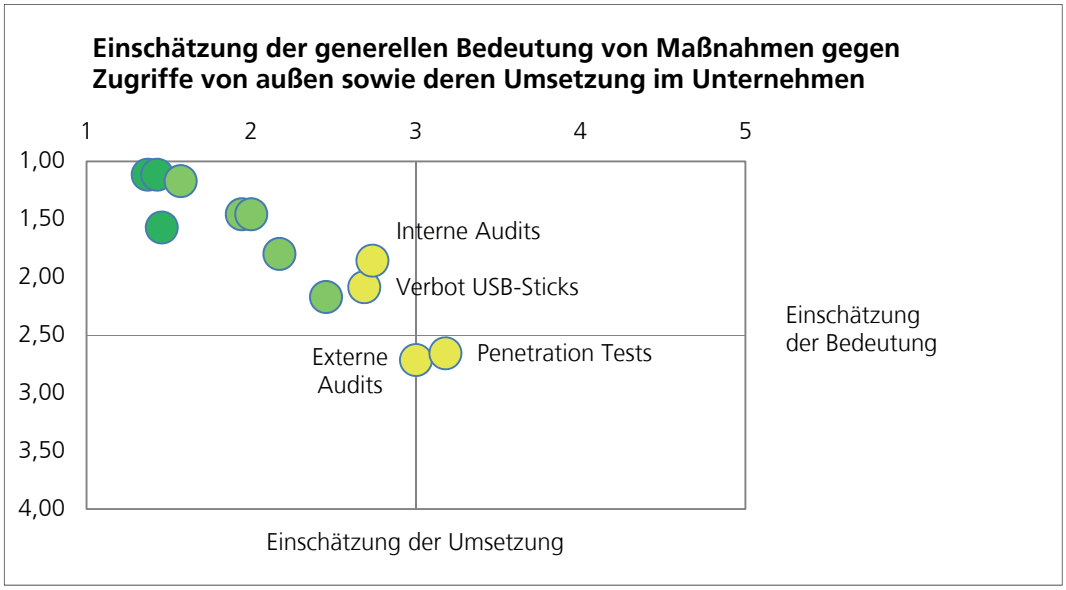


Die obige Abbildung zeigt gängige Einzelmaßnahmen der IT-Sicherheit gereiht nach der Einschätzung der Bedeutung. Dabei zeigt sich, dass die jene Maßnahmen, die von den Unternehmen als besonders wichtig angesehen werden auch die besten Noten hinsichtlich Umsetzungsqualität erreichen konnten. Die Einrichtung von Firewalls, Virenschutz-Programmen und Spamfiltern wird in überwiegendem Maße mit Sehr Gut oder Gut bewertet (mehr als 90% der Unternehmen).

Weniger gut schätzen sich die Unternehmen hinsichtlich der Einrichtung von Sperrlisten gefährlicher E-Mail-Adressen ein, obwohl deren Bedeutung als hoch erachtet wird. Dem Verbot privater Wechselmedien und USB-Sticks sowie Einschränkungen der Internet-Nutzung wird eine deutlich geringere Bedeutung zugemessen (Einschätzung der Bedeutung >2), bei

relativ hoher Zufriedenheit mit der Umsetzungsqualität. Ein deutlicher Abfall in der Bedeutung war bei den sogenannten Penetration Tests bzw. externen Audits festzustellen. Entsprechend hoch sind die Anteile der Nichtanwendung und entsprechend gering die Anteile der sehr guten bis guten Selbsteinschätzungen. 25% der Unternehmen schätzen sich bei der Durchführung von Penetration Tests sehr gut bis gut ein.

Setzt man die Einschätzung der Bedeutung mit jener der Umsetzungsqualität zueinander in Beziehung, ergibt sich folgendes Portfolio:



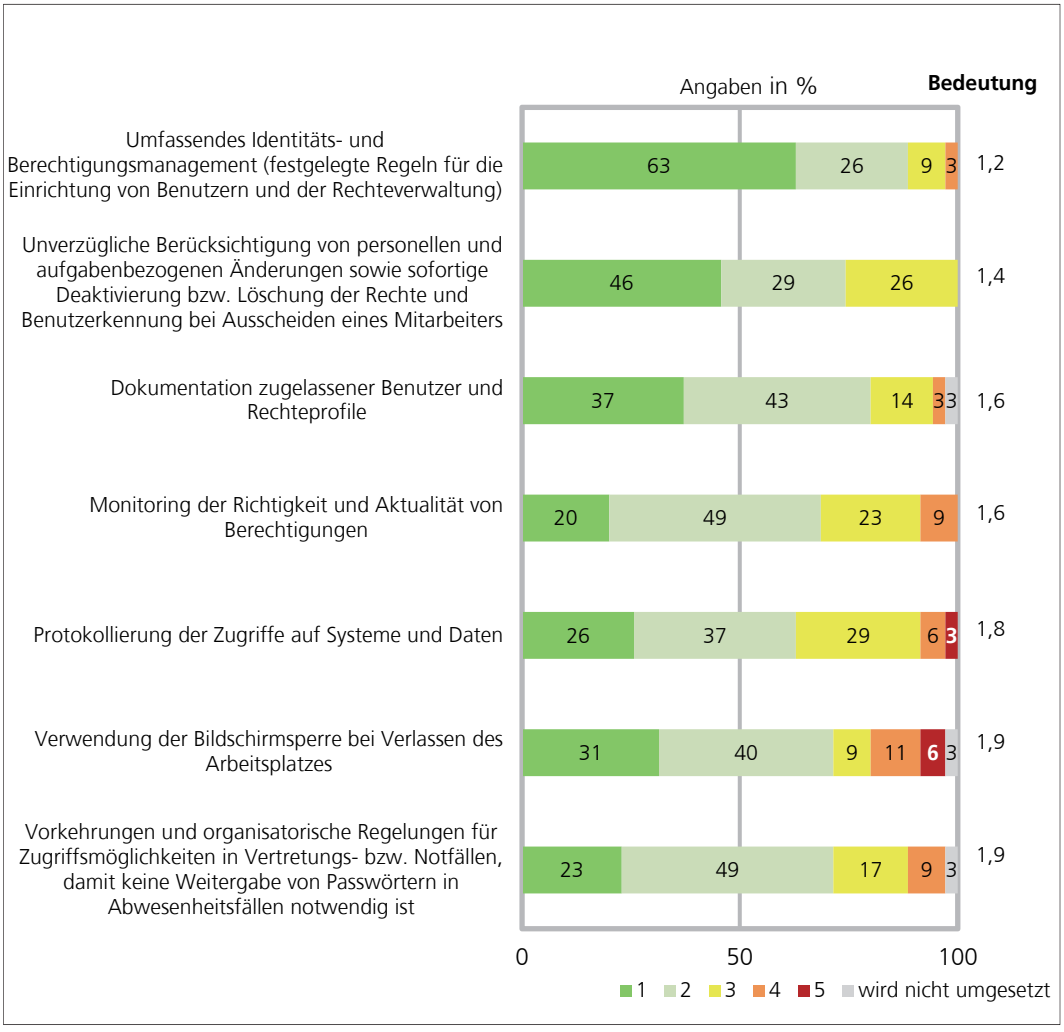
Die Korrelation der Bedeutungseinschätzung mit der entsprechenden Bewertung der Umsetzungsqualität geht aus dem Portfolio klar hervor. Die durchschnittlichen Bewertungen der Umsetzungsqualität sowie die Bedeutungseinschätzungen stellen sich wie folgt dar:

Maßnahme	Einschätzung der Umsetzung	Einschätzung der Bedeutung
Firewall	1,37	1,11
Virenschutz	1,43	1,11
Verwendung von originaler Software mit Lizenzen	1,46	1,57
Spamfilter	1,57	1,17
Verbot der Installation von Software für Nicht-Administratoren	1,94	1,46
Sperrliste für gefährdende E-Mail-Adressen	2,00	1,46
Verwendung der HTTPS-Übertragung auf Webseiten	2,17	1,80
Nutzungseinschränkungen des Internets und sozialer Medien	2,45	2,17
Verbot bzw. Einschränkung der Verwendung von USB-Sticks	2,69	2,09
Interne Audits (Sicherheitslücken, Vulnerability Scans o.ä.)	2,74	1,86
Sonstige Externe Audits	3,00	2,71
Penetration Tests durch externe Anbieter ("White Hacks")	3,18	2,66

In der Tabelle erfolgte eine Reihung nach den Durchschnittsbewertungen sowie eine Trennung der mit Sehr Gut bewerteten Maßnahmen von den gut bzw. befriedigend benoteten. Die letzten vier Plätze belegen dabei das Verbot der Nutzung von USB-Sticks, interne und externe Audits bzw. Penetration Tests. Bei den internen Audits ist trotz einer höheren Bedeutungseinschätzung eine geringere Umsetzungsqualität festzuhalten.

Was die Durchführung externer Audits und Penetration Test betrifft, stellt sich die Frage, ob deren Bedeutung für die IT-Sicherheit von den Unternehmen nicht unterschätzt wird. Nach Meinung der Verfasser sollten diese regelmäßig durchgeführt werden.

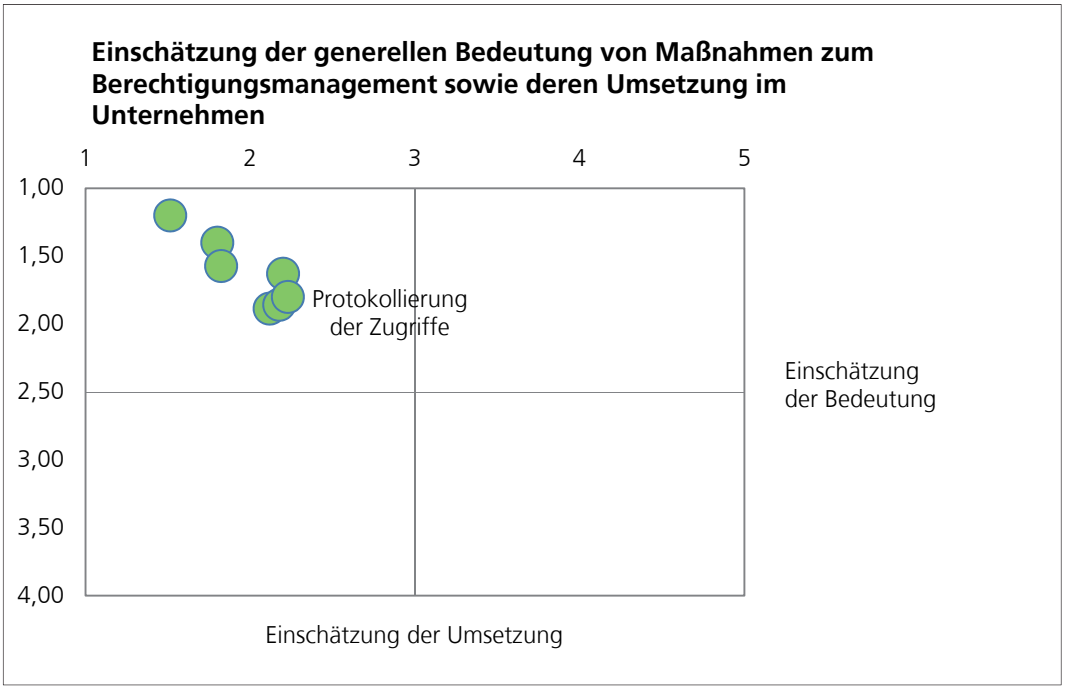
Maßnahmen im Zusammenhang mit dem Berechtigungsmanagement



Hinsichtlich Organisation und Verwaltung eines umfassenden Berechtigungsmanagements ergab sich ein durchwegs gutes Bild. Die Bedeutung des Berechtigungsmanagements wird als sehr hoch angesehen; hinsichtlich der Umsetzung schätzen sich bei allen Fragestellungen mehr als 50% der Unternehmen als sehr gut bis gut ein. Beispielsweise ergab sich bei der Maßnahme „unverzüglicher Berücksichtigung von personellen und aufgabenbezogenen

Änderungen“ keine einzige bloß genügende oder nicht genügende Selbsteinschätzung. Auch die Dokumentation der Benutzerrechte wird von 80% der Unternehmen mindestens gut umgesetzt.

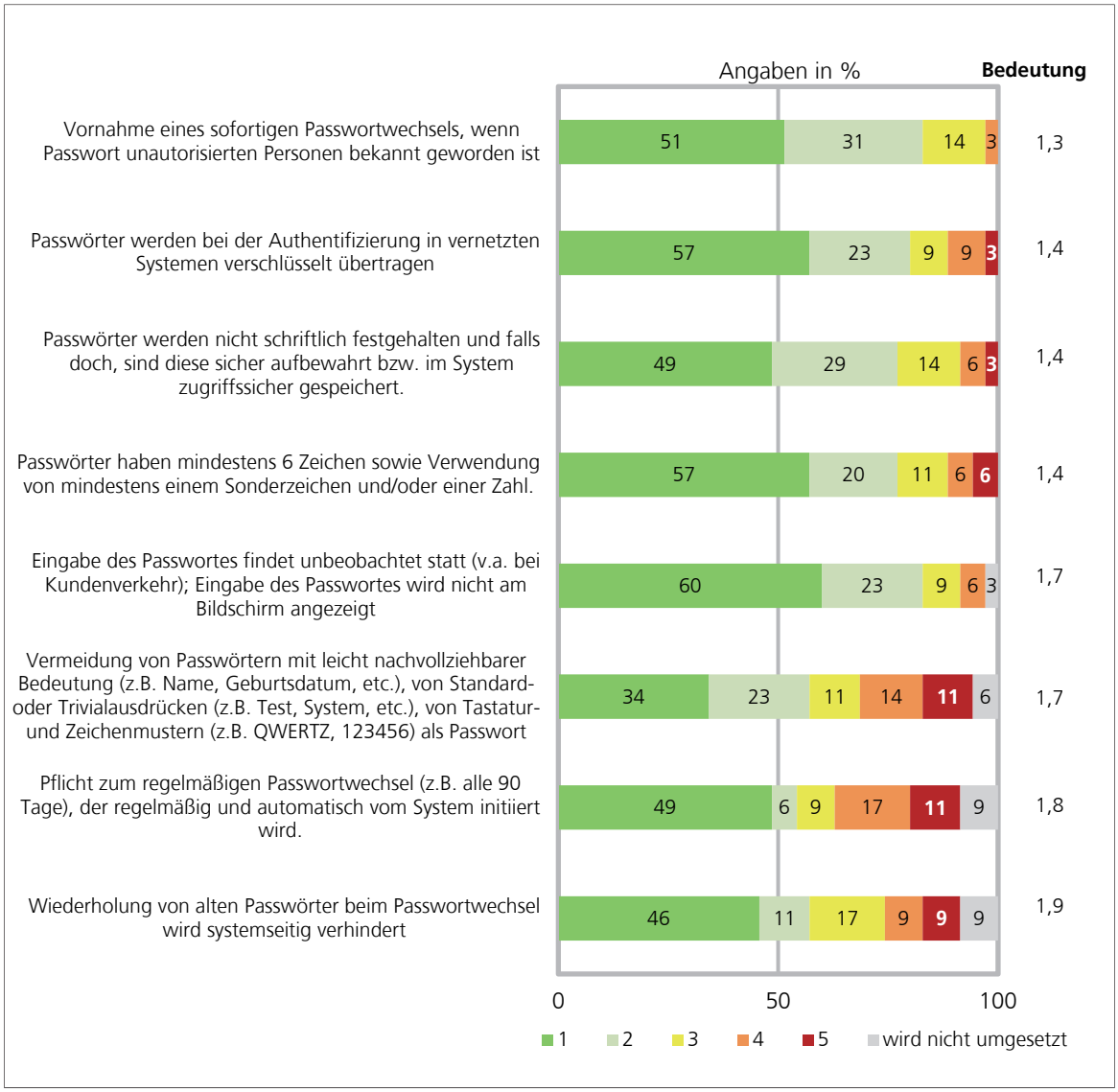
Das Portfolio aus der Einschätzung der Bedeutung und der Umsetzung im Unternehmen zeigt folgendes Bild:



Im Zusammenhang mit den Maßnahmen des Berechtigungsmanagements wird von den Unternehmen generell eine gute Umsetzung angegeben. Am besten schneidet die Maßnahme „Umfassendes Identitäts- und Berechtigungsmanagement“ mit der Note 1,51 ab. Die Einschätzungen betreffend Bedeutung und Umsetzung im Unternehmen weisen eine hohe Korrelation auf. Die einzelnen Durchschnittsnoten je Maßnahme zeigt die folgende Tabelle.

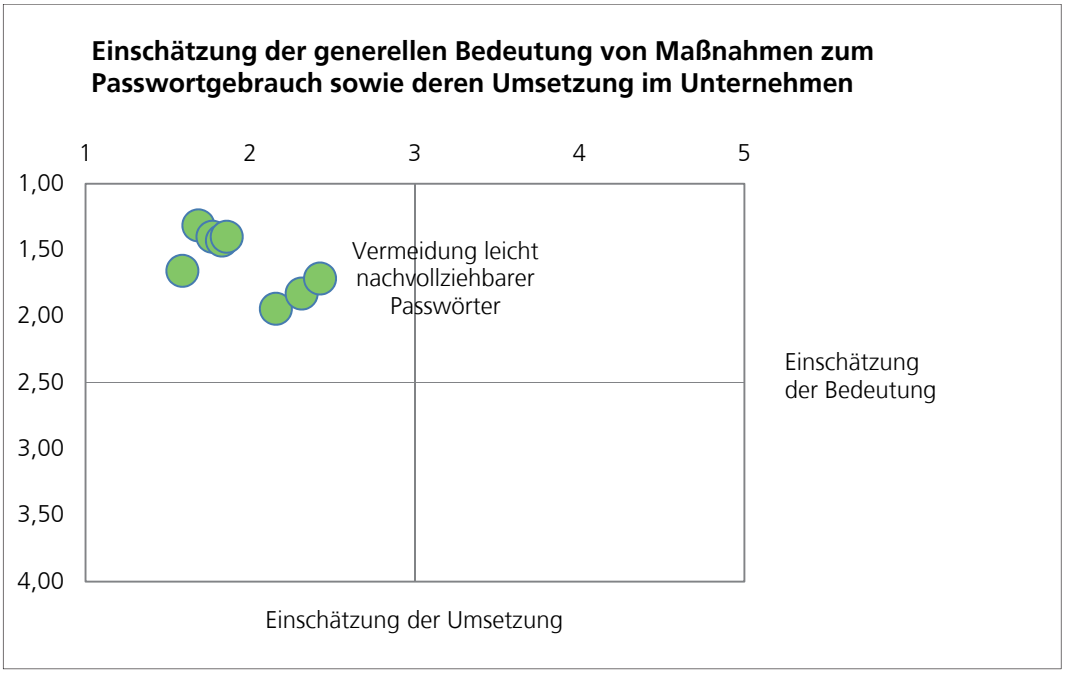
Maßnahme	Einschätzung der Umsetzung	Einschätzung der Bedeutung
Umfassendes Identitäts- und Berechtigungsmanagement	1,51	1,20
Unverzügliche Berücksichtigung von personellen und aufgabenbezogenen Änderungen	1,80	1,40
Dokumentation zugelassener Benutzer und Rechteprofile	1,82	1,57
Vorkehrungen für Zugriffsmöglichkeiten in Vertretungs- bzw. Notfällen	2,12	1,89
Verwendung der Bildschirmsperre bei Verlassen des Arbeitsplatzes	2,18	1,86
Monitoring der Richtigkeit und Aktualität von Berechtigungen	2,20	1,63
Protokollierung der Zugriffe auf Systeme und Daten	2,23	1,80

Maßnahmen zum Passwortgebrauch



Ein zentrales Instrument gegen unbefugte Zugriffe ist der Gebrauch von Passwörtern. Im Zusammenhang mit der Passwortverwaltung ergab sich ein ähnlich guter Eindruck wie beim zuvor behandelten Management der Benutzerberechtigungen. Wie aus obiger Abbildung hervorgeht, korreliert die Einschätzung der Bedeutung mit der erreichten Umsetzungsqualität im Wesentlichen. Hinsichtlich Verschlüsselung, Passwortdokumentation, Passwortkomplexität oder Geheimhaltung erreicht der Anteil sehr guter Selbsteinschätzungen Werte von 49% bis zu 60%. Nur 9% setzten die systemseitige Verhinderung von Passwort-Wiederholungen sowie die systemseitige Verpflichtung zum regelmäßigen Passwortwechsel nicht um.

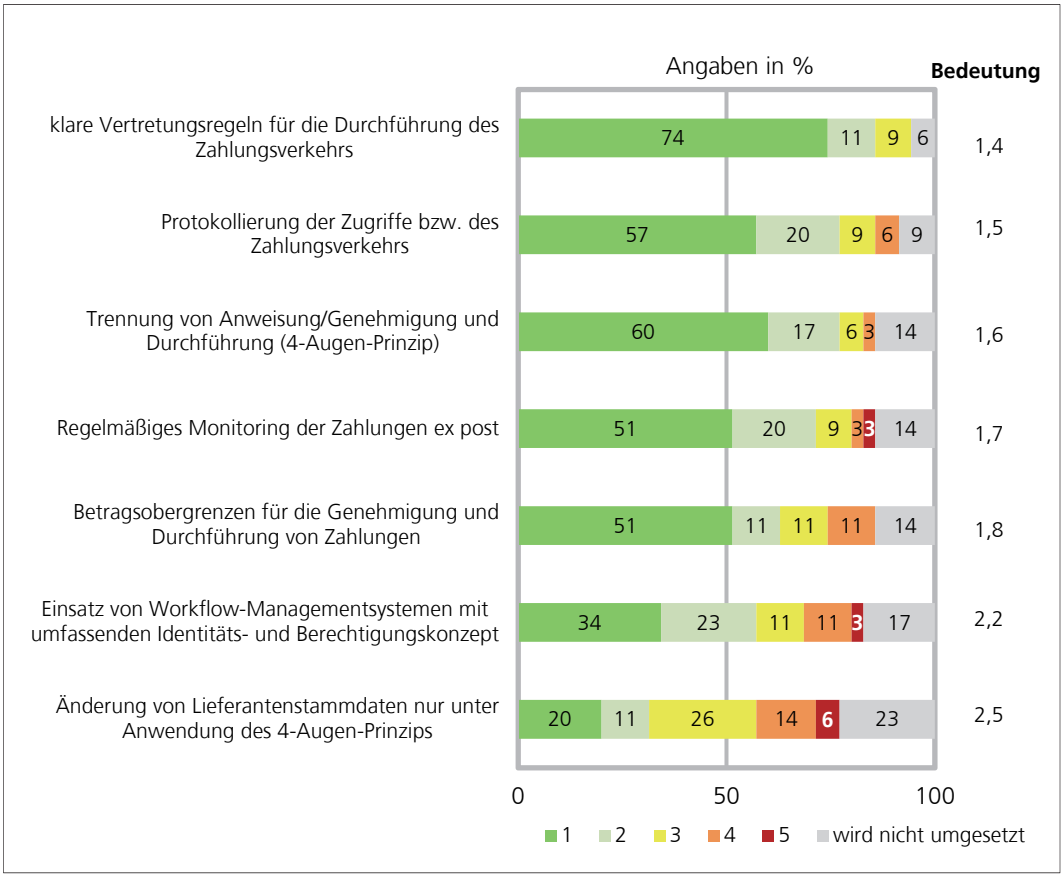
Das Portfolio aus der Einschätzung der Bedeutung und der Umsetzung im Unternehmen ist auf der nächsten Seite dargestellt.



Wie schon zuvor bei den Maßnahmen zum Berechtigungsmanagement, zeigen auch die Maßnahmen zum Passwortgebrauch ein konsistentes Bild: bei hoher Bedeutungseinschätzung geben die Unternehmen insgesamt gute Bewertungen der Umsetzung an, wie auch die Tabelle zeigt:

Maßnahme	Einschätzung der Umsetzung	Einschätzung der Bedeutung
Eingabe des Passwortes findet unbeobachtet statt bzw. wird nicht am Bildschirm angezeigt	1,59	1,66
Vornahme eines sofortigen Passwortwechsels, wenn Passwort unautorisierten Personen bekannt geworden ist	1,69	1,31
Passwörter werden bei der Authentifizierung in vernetzten Systemen verschlüsselt übertragen	1,77	1,40
Passwörter haben Mindestlänge und Sonderzeichen	1,83	1,43
Passwörter werden nicht schriftlich festgehalten und falls doch, zugriffssicher gespeichert.	1,86	1,40
Wiederholung alter Passwörter wird systemseitig verhindert	2,16	1,94
Pflicht zum regelmäßigen Passwortwechsel	2,31	1,83
Vermeidung von Passwörtern mit leicht nachvollziehbarer Bedeutung	2,42	1,71

Maßnahmen des elektronischen Zahlungsverkehrs

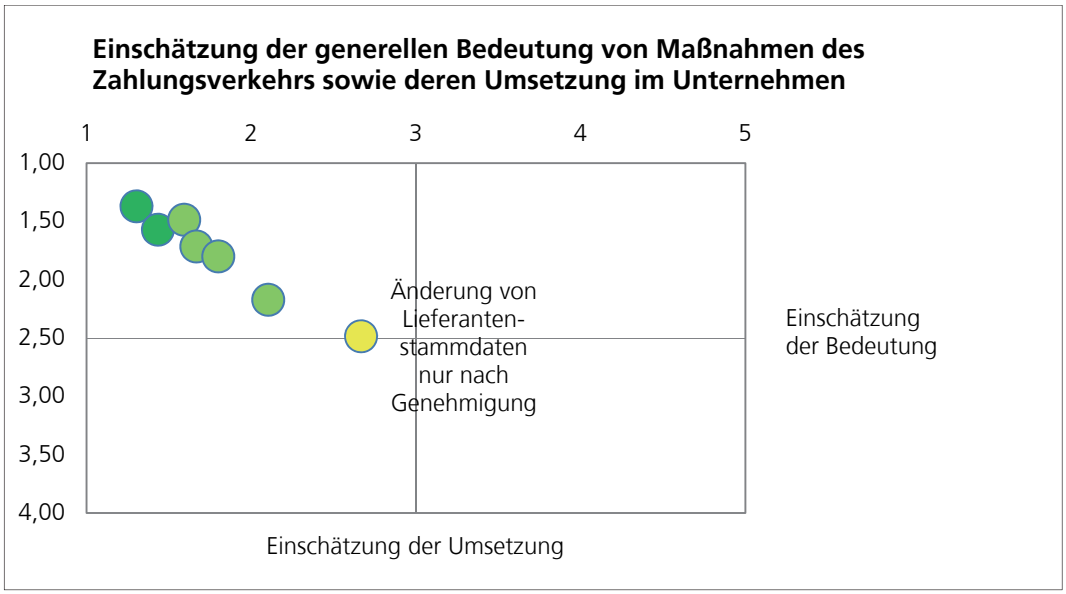


Überwiegend gut erscheinen die Ergebnisse hinsichtlich der Umsetzungsqualität im Zahlungsverkehr. Die klare Trennung von Genehmigung und Durchführung schätzen 60% der Unternehmen als sehr gut ein. Die Protokollierung sowie das nachträgliche Monitoring bewerten ebenfalls mehr als die Hälfte der Unternehmen mit Sehr Gut. Die Ergebnisse korrelieren dabei mit der Bedeutungseinschätzung bei geringer Varianz.

Betrachtet man den Anteil der Unternehmen, die ähnliches nicht umgesetzt haben, lassen sich allerdings Verbesserungspotenziale erkennen: 14% der Befragten geben keine Trennung von Genehmigung und Durchführung, keine entsprechenden Genehmigungsgrenzen oder kein regelmäßiges Monitoring des Zahlungsverkehrs an.

Die relativ geringste Bedeutung hat die Anwendung des 4-Augen-Prinzips bei Änderung von Lieferantenstammdaten oder der Einsatz von Workflow-Managementsystemen im Zahlungsverkehr. Das Risiko des Anlegens von Scheinlieferanten wird somit nach Meinung der Verfasser unterschätzt.

Das Portfolio aus der Einschätzung der Bedeutung und der Umsetzung im Unternehmen stellt sich wie folgt dar:

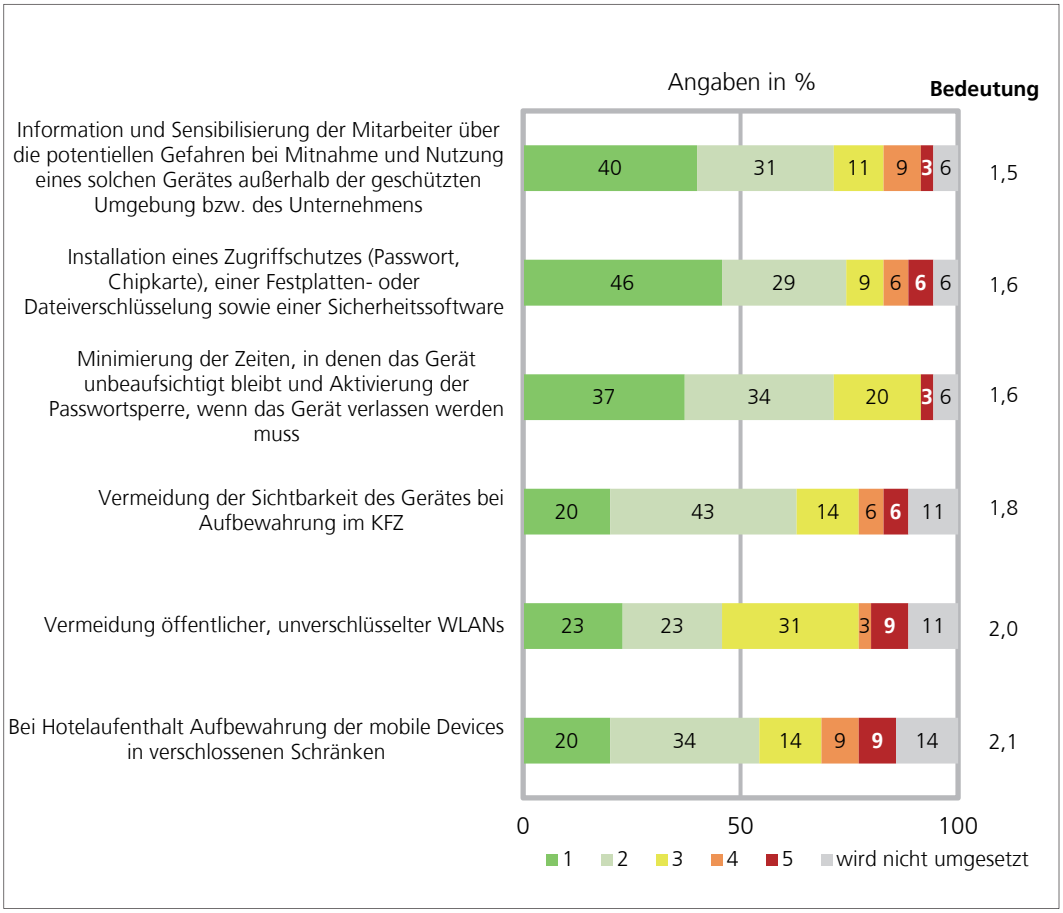


Klare Vertretungsregeln und die Trennung von Genehmigung und Durchführung von Zahlungen werden nicht nur als besonders wichtig eingeschätzt, sondern hinsichtlich der Umsetzung im eigenen Unternehmen im Durchschnitt sehr gut benotet. Schlechter schneidet nur die Veränderung von Lieferantenstammdaten unter Einsatz des Vier-Augen-Prinzips ab. Hier besteht für die Unternehmen noch Verbesserungspotenzial sowohl was das Risikobewusstsein als auch die Umsetzung betrifft.

In der Tabelle sind die einzelnen Maßnahmen mit den Werten der Umsetzung sowie der Einschätzung der Bedeutung aufgelistet:

Maßnahme	Einschätzung der Umsetzung	Einschätzung der Bedeutung
Klare Vertretungsregeln für die Durchführung des Zahlungsverkehrs	1,30	1,37
Trennung von Genehmigung und Durchführung (4-Augen-Prinzip)	1,43	1,57
Protokollierung der Zugriffe bzw. des Zahlungsverkehrs	1,59	1,49
Regelmäßiges Monitoring der Zahlungen ex post	1,67	1,71
Betragsobergrenzen für die Genehmigung und Durchführung von Zahlungen	1,80	1,80
Einsatz von Workflow-Managementsystemen mit umfassenden Identitäts- und Berechtigungskonzept	2,10	2,17
Änderung von Lieferantenstammdaten nur unter Anwendung des 4-Augen-Prinzips	2,67	2,49

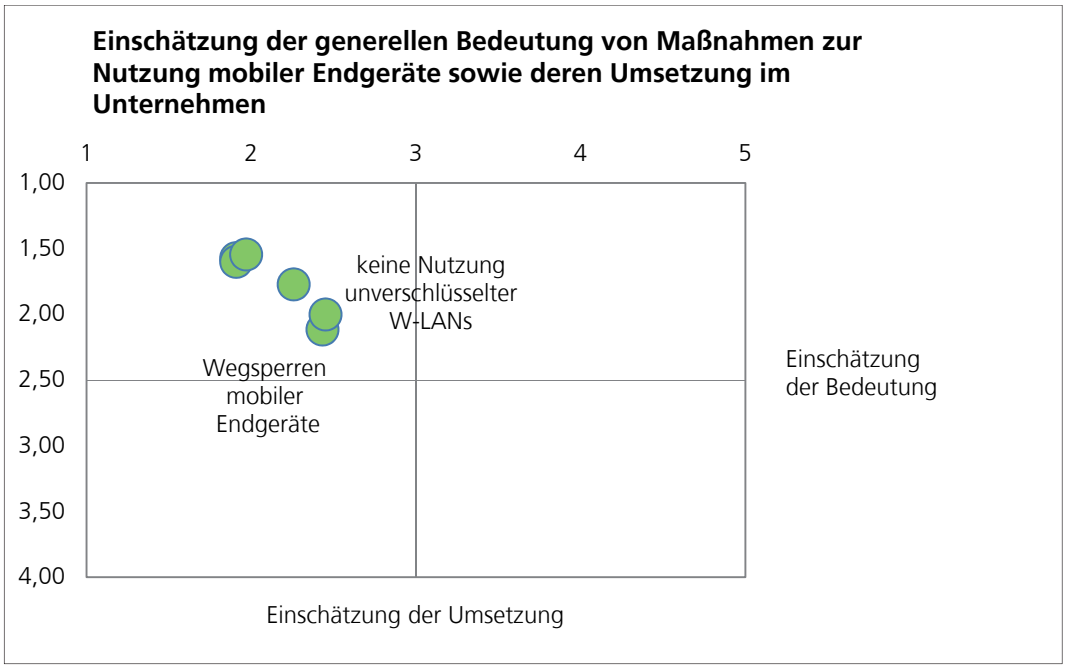
Maßnahmen in Bezug auf die sichere Nutzung mobiler Endgeräte



Mobile Endgeräte sind aufgrund ihrer häufigen Nutzung außerhalb des Unternehmens einer deutlich größeren Gefährdung ausgesetzt als beispielsweise Server oder Stand-PCs. Die Studienteilnehmer wurden daher um eine Einschätzung der Bedeutung entsprechender Maßnahmen zum Schutz mobiler Endgeräte gebeten. Die drei wichtigsten Maßnahmen sind laut Meinung der IT-Zuständigen die Sensibilisierung und Information der Mitarbeiter, der Passwortschutz sowie die Minimierung der Zeiten, in welchen die mobilen Endgeräte unbeaufsichtigt bleiben. Die Umsetzungsqualität schätzten rund 70% bis 75% der Unternehmen als sehr gut bis gut ein. Dass in PKW verstaute mobile Endgeräte für Passanten nicht sichtbar sein sollten, sehen rund 63% der Unternehmen als gut bis sehr gut umgesetzt an.

Geringere Bedeutung wird der versperrten Aufbewahrung in Hotels oder der Vermeidung unverschlüsselter öffentlicher W-LANs beigemessen. Da die Nutzung eines unverschlüsselten W-LANs eine besonders hohe Bedrohung für firmenkritische Daten darstellen kann, besteht hier nach Meinung der Verfasser noch erhebliches Potenzial beim Risikobewusstsein.

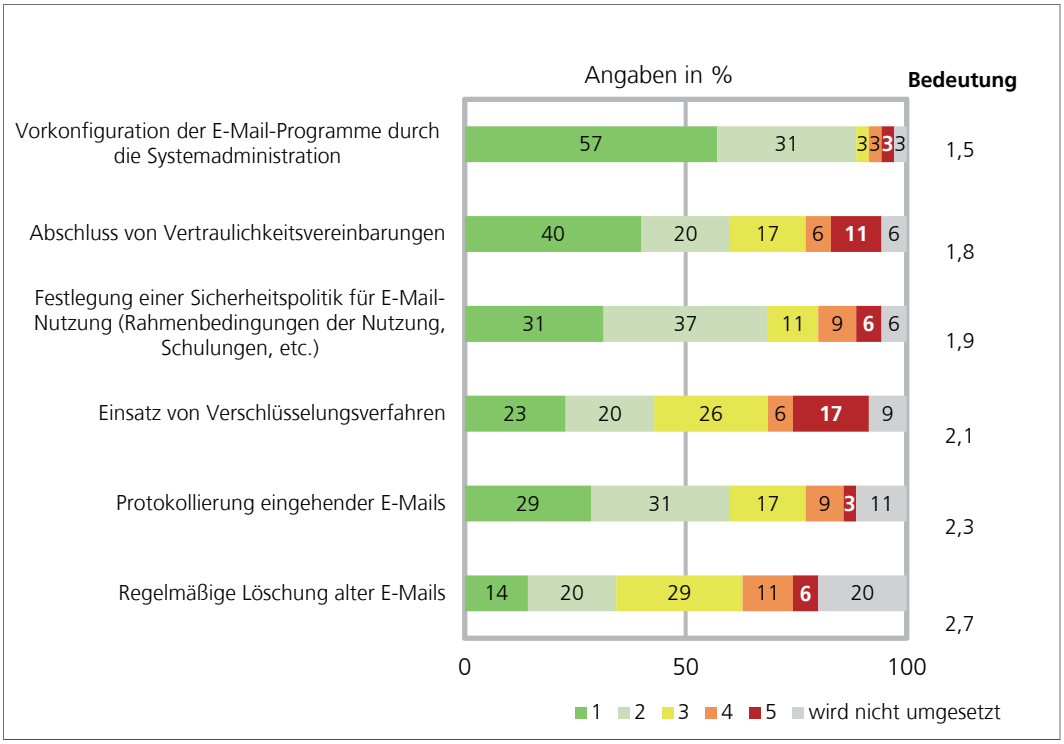
Das Portfolio aus der Einschätzung der Bedeutung und der Umsetzung im Unternehmen zeigt folgendes Bild:



Wie bereits oben erwähnt, könnte das Risikobewusstsein hinsichtlich der Nutzung unverschlüsselter W-LANs und des Versperrens mobiler Endgeräte in Hotels ausgeprägter sein. Die Einschätzungen der Umsetzung im Unternehmen erreichen im Durchschnitt gute Werte, wie auch die Tabelle zeigt:

Maßnahme	Einschätzung der Umsetzung	Einschätzung der Bedeutung
Installation eines Zugriffschutzes sowie einer Festplatten- oder Dateiverschlüsselung	1,91	1,57
Minimierung der Zeiten, in denen das Gerät unbeaufsichtigt bleibt	1,91	1,60
Sensibilisierung der Mitarbeiter über die potentiellen Gefahren bei Mitnahme und Nutzung eines mobilen Endgerätes	1,97	1,54
Vermeidung der Sichtbarkeit des Gerätes bei Aufbewahrung im KFZ	2,26	1,77
Bei Hotelaufenthalt Aufbewahrung der mobilen Endgeräte in verschlossenen Schränken	2,43	2,11
Vermeidung öffentlicher, unverschlüsselter WLANs	2,45	2,00

Maßnahmen im Zusammenhang mit dem Informationsaustausch per E-Mail

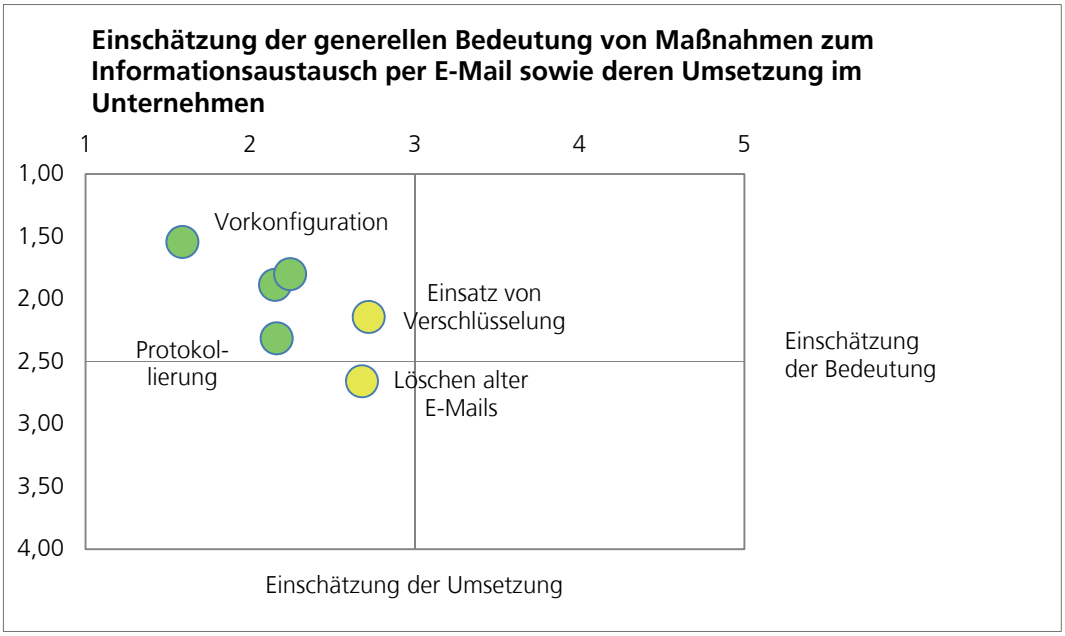


E-Mail hat sich als zentrales Kommunikationsmittel in den Unternehmen durchgesetzt. Umso mehr sind die damit verbundenen Risiken zu beachten: E-Mails können abgefangen und derart vertrauenswürdige Daten an unbefugte Personen gelangen; über E-Mails werden Viren oder ähnliche Schadsoftware verbreitet oder falsche Identitäten vorgetäuscht.

Am wichtigsten eingeschätzt und mit 57% Sehr Gut am besten umgesetzt wird die Maßnahme der Vorkonfiguration von E-Mail-Programmen durch die Systemadministration. Die Unterzeichnung von Vertraulichkeitsvereinbarungen oder die Festlegung einer E-Mail-Sicherheitspolitik fällt davon deutlich ab.

Vergleichsweise geringe Bedeutung erhielten der Einsatz von Verschlüsselungsverfahren, die Protokollierung eingehender E-Mails und die Löschung alter E-Mails. Die Einsatzqualität von Verschlüsselungsverfahren bewerteten 17 % der Befragten mit Nicht Genügend. 20% der Unternehmen setzen das regelmäßige Löschen alter E-Mails nicht um.

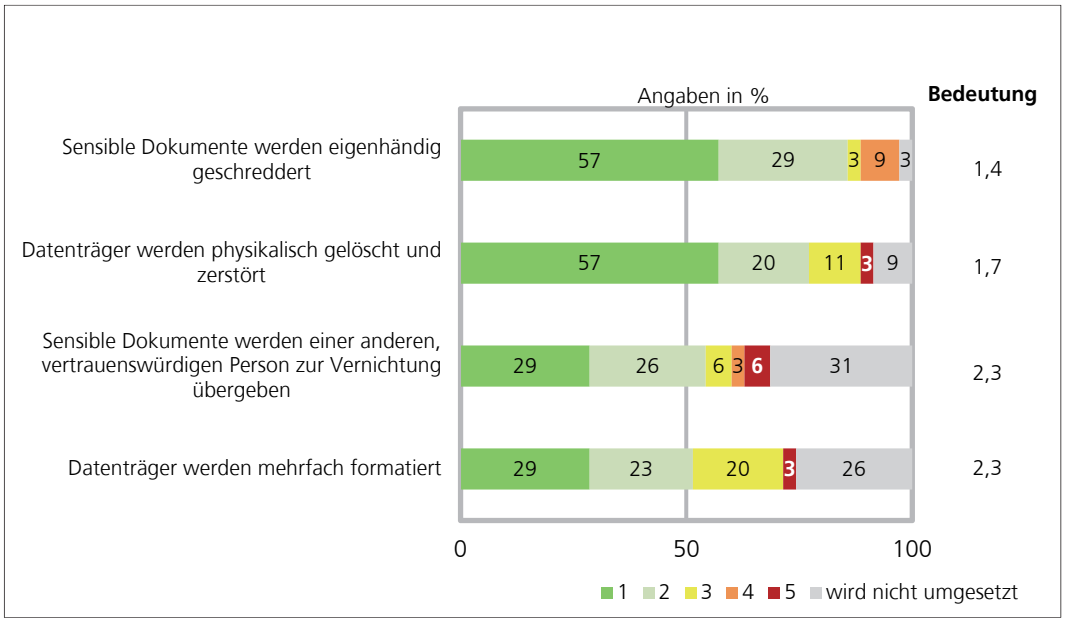
Das Portfolio aus der Einschätzung der Bedeutung und der Umsetzung im Unternehmen zeigt ein differenziertes Bild:



Beim Informationsaustausch per E-Mail besteht der eine oder andere Verbesserungsbedarf: so geben sich die befragten Unternehmen beim Löschen alter E-Mails nur die Durchschnittsnote 2,68; beim Einsatz von Verschlüsselungsverfahren fällt die Selbsteinschätzung mit 2,72 noch schlechter aus. Alle anderen Maßnahmen werden von den Unternehmen besser umgesetzt, wovon die Vorkonfiguration der E-Mail-Programme mit einer Durchschnittsbenotung von 1,59 bei der Selbsteinschätzung am besten abschneidet.

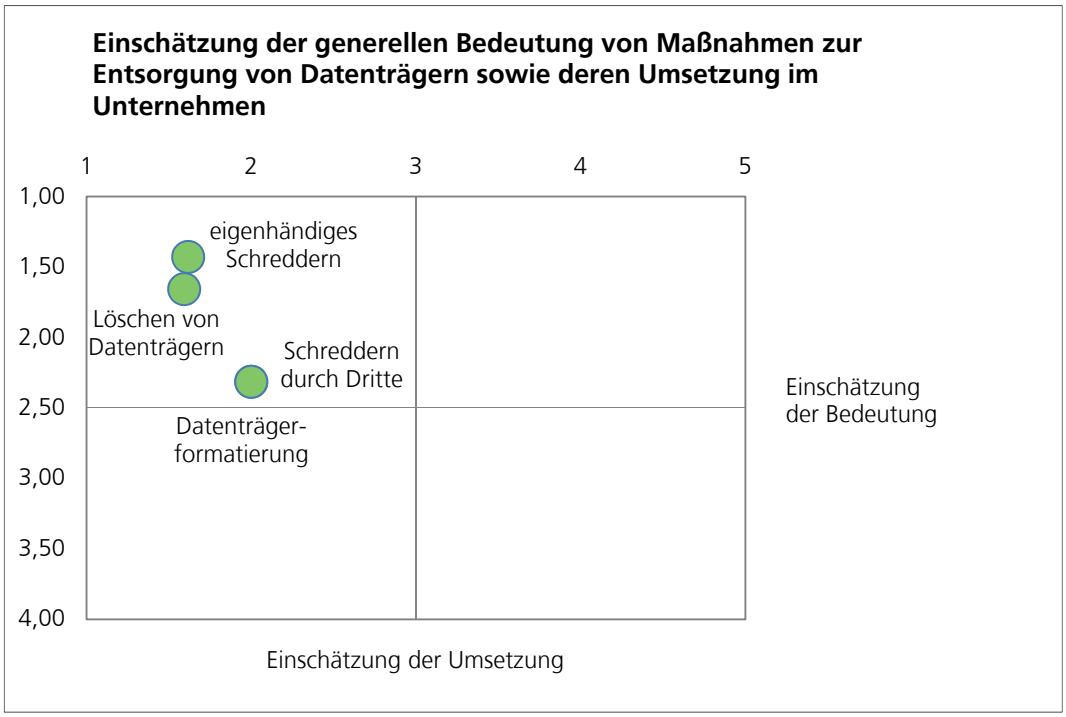
Maßnahme	Einschätzung der Umsetzung	Einschätzung der Bedeutung
Vorkonfiguration der E-Mail-Programme durch die Systemadministration	1,59	1,54
Festlegung einer Sicherheitspolitik für E-Mail-Nutzung	2,15	1,89
Protokollierung eingehender E-Mails	2,16	2,31
Abschluss von Vertraulichkeitsvereinbarungen	2,24	1,80
Regelmäßige Löschung alter E-Mails	2,68	2,66
Einsatz von Verschlüsselungsverfahren	2,72	2,14

Maßnahmen der Datenträger-Entsorgung



Im Rahmen vorliegender Umfrage wurden mit dem Begriff Datenträger Festplatten, CD-Roms, USB-Sticks aber auch Papierdokumente umschrieben. Betreffend Vernichtung alter Datenträger gaben die Unternehmen dem eigenhändigen Schreddern und Vernichten den klaren Vorzug: 31% der Unternehmen verzichten auf das Auslagern dieser Tätigkeit. Darüber hinaus erzielte die eigenhändige Vernichtung deutlich bessere Noten bei der Umsetzungsqualität als das ausgelagerte Schreddern, bei welchem 6% der Befragten die Note Nicht Genügend anführten.

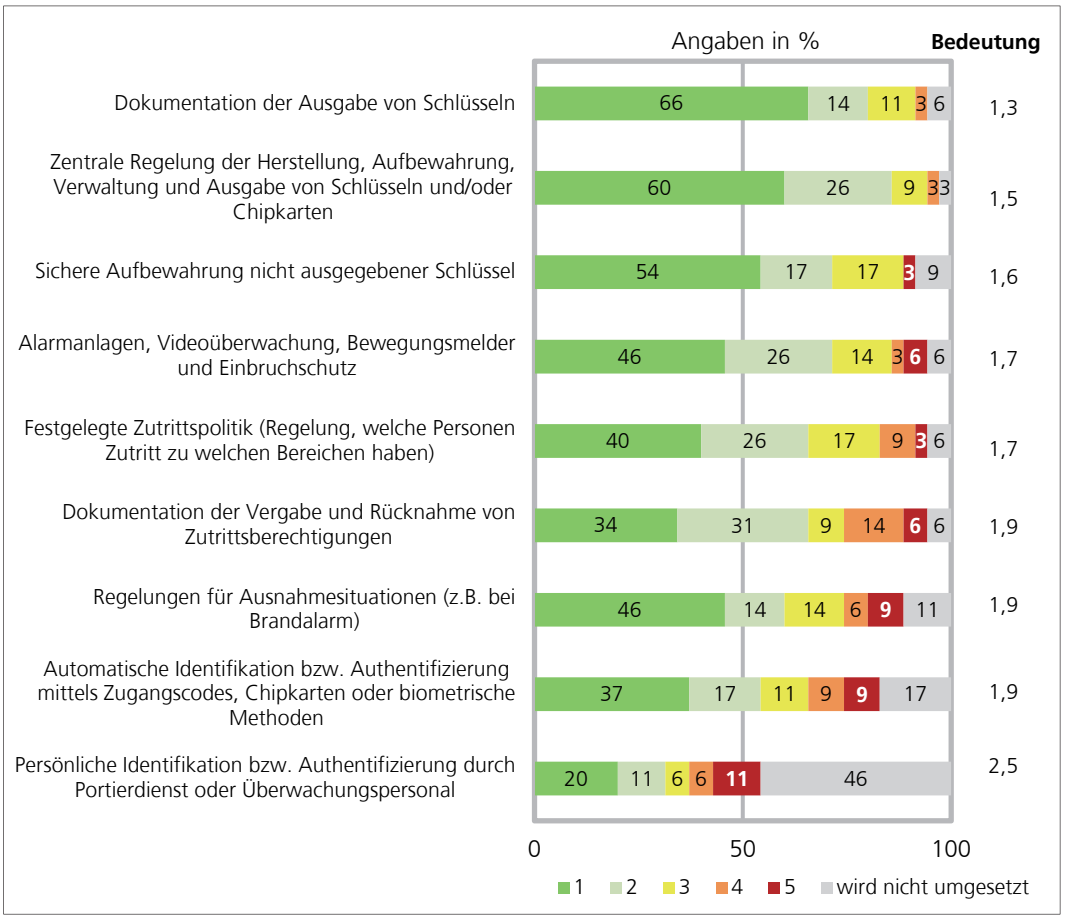
Das entsprechende Portfolio stellt sich wie folgt dar:



Die geringste Bedeutung wird dem Schreddern durch unternehmensexterne Dritte und der mehrfachen Formatierung von Daten beigemessen. Hinsichtlich der Umsetzung schätzen sich die Unternehmen im Durchschnitt gut ein, wie auch die Tabelle zeigt:

Maßnahme	Einschätzung der Umsetzung	Einschätzung der Bedeutung
Datenträger werden physikalisch gelöscht und zerstört	1,59	1,66
Sensible Dokumente werden eigenhändig geschreddert	1,62	1,43
Datenträger werden mehrfach formatiert	2,00	2,31
Sensible Dokumente werden einer anderen, vertrauenswürdigen Person zur Vernichtung übergeben	2,00	2,31

Maßnahmen gegen unberechtigten Zutritt sensibler Unternehmensbereiche

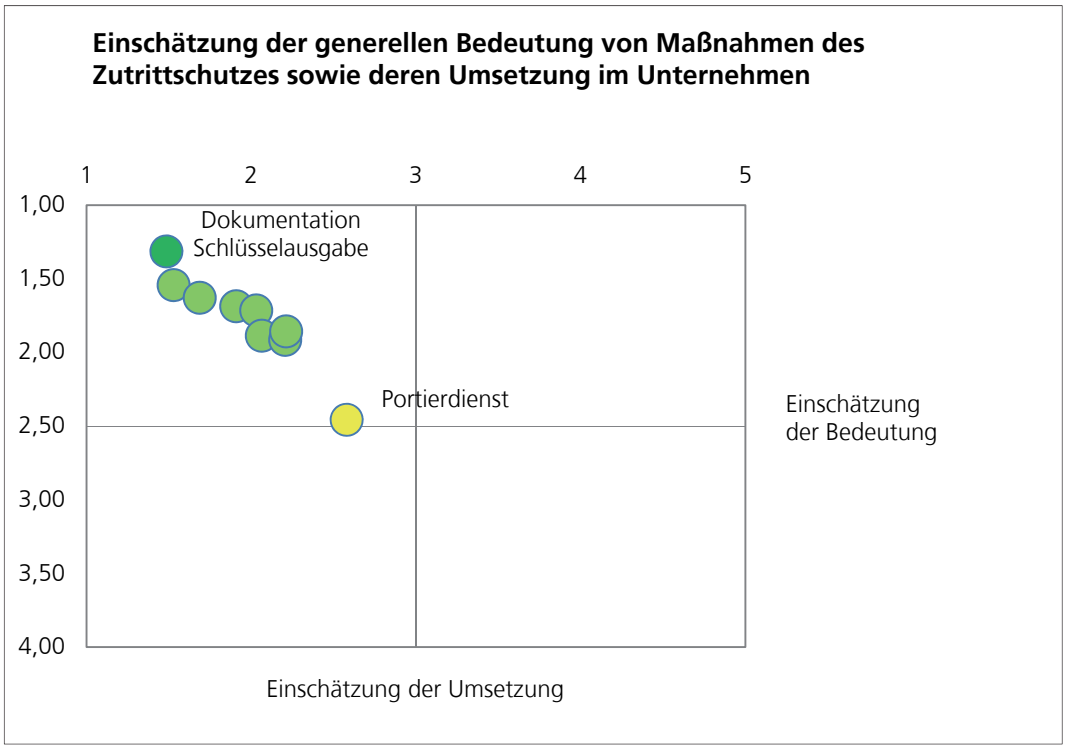


Für alle sensiblen Unternehmensbereiche gilt es, besondere Schutzmaßnahmen gegen unberechtigten Zutritt zu ergreifen. Die Fokussierung der IT-Sicherheit auf Cyberkriminalität und Schutz der Systeme darf nicht dazu führen, althergebrachte, „analoge" Wege der Betriebsspionage außer Acht zu lassen. Unversperrte Serverräume können eine Einladung für Datendiebe oder Saboteure sein.

Hinsichtlich Bedeutung des Zutrittsschutzes und der Umsetzungsqualität ausgewählter Maßnahmen zeigten sich im Wesentlichen korrelierende Ergebnisse. Der Verwaltung bzw. Dokumentation der Schlüsselausgabe wurde die größte Bedeutung beigemessen. Die Umsetzung dieser Maßnahmen im eigenen Unternehmen schätzen über 80 % der Befragten als sehr gut oder gut ein.

Die persönliche Identifikation bzw. Authentifizierung durch einen Portierdienst oder Überwachungspersonal halten hingegen 46 % der Studienteilnehmer für nicht notwendig; 11 % beurteilen die eigene Umsetzung mit einem nicht genügend. Ein Grund dürfte die geringe Unternehmensgröße mittelständischer Betriebe sein, welche die Beschäftigung eigener Portiere aus Kostengründen verhindert. Aus demselben Grund dürften die Ergebnisse bezüglich Chipkarten, Zugangscodes o.ä. schlechter ausgefallen sein.

Das entsprechende Portfolio zeigt ein konsistentes Bild:

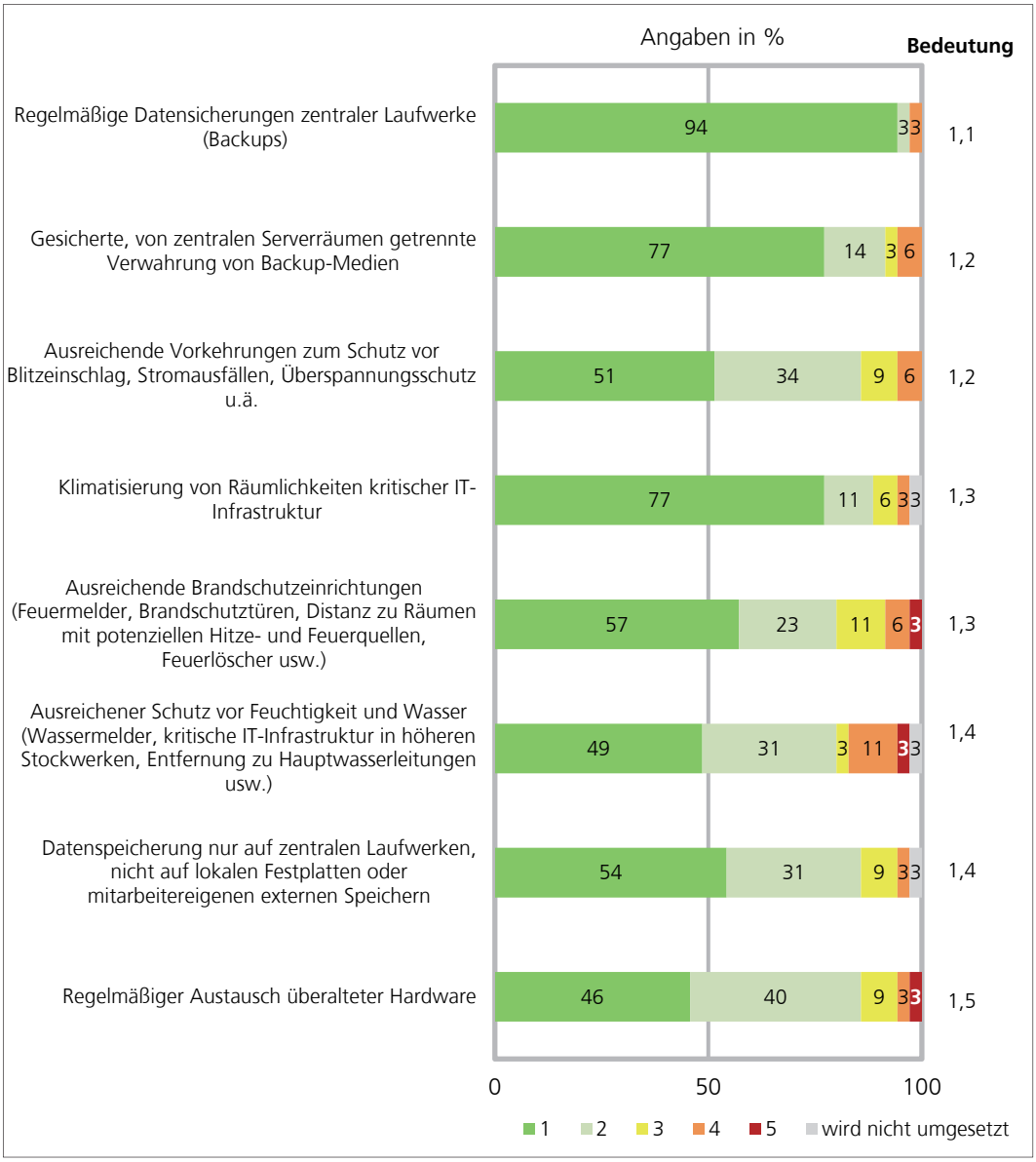


Die Einschätzung der generellen Bedeutung korreliert mit dem Umsetzungsgrad. Am besten wird laut Eigeneinschätzung die Dokumentation der Schlüsselausgabe umgesetzt mit einer Benotung von durchschnittlich 1,48. Am unbedeutendsten eingeschätzt und am wenigsten gut umgesetzt werden Portierdienste; wohl aus den bereits oben angeführten Gründen.

Alle anderen Maßnahmen werden laut Selbsteinschätzung gut umgesetzt.

Maßnahme	Einschätzung der Umsetzung	Einschätzung der Bedeutung
Dokumentation der Ausgabe von Schlüsseln	1,48	1,31
Zentrale Regelung der Herstellung, Aufbewahrung, Verwaltung und Ausgabe von Schlüsseln und/oder Chipkarten	1,53	1,54
Sichere Aufbewahrung nicht ausgegebener Schlüssel	1,69	1,63
Alarmanlagen, Videoüberwachung, Bewegungsmelder u.ä.	1,91	1,69
Festgelegte Zutrittspolitik	2,03	1,71
Regelungen für Ausnahmesituationen	2,06	1,89
Automatische Identifikation bzw. Authentifizierung mittels Zugangscodes, Chipkarten oder biometrische Methoden	2,21	1,91
Dokumentation der Vergabe von Zutrittsberechtigungen	2,21	1,86
Persönliche Identifikation bzw. Authentifizierung durch Portierdienst oder Überwachungspersonal	2,58	2,46

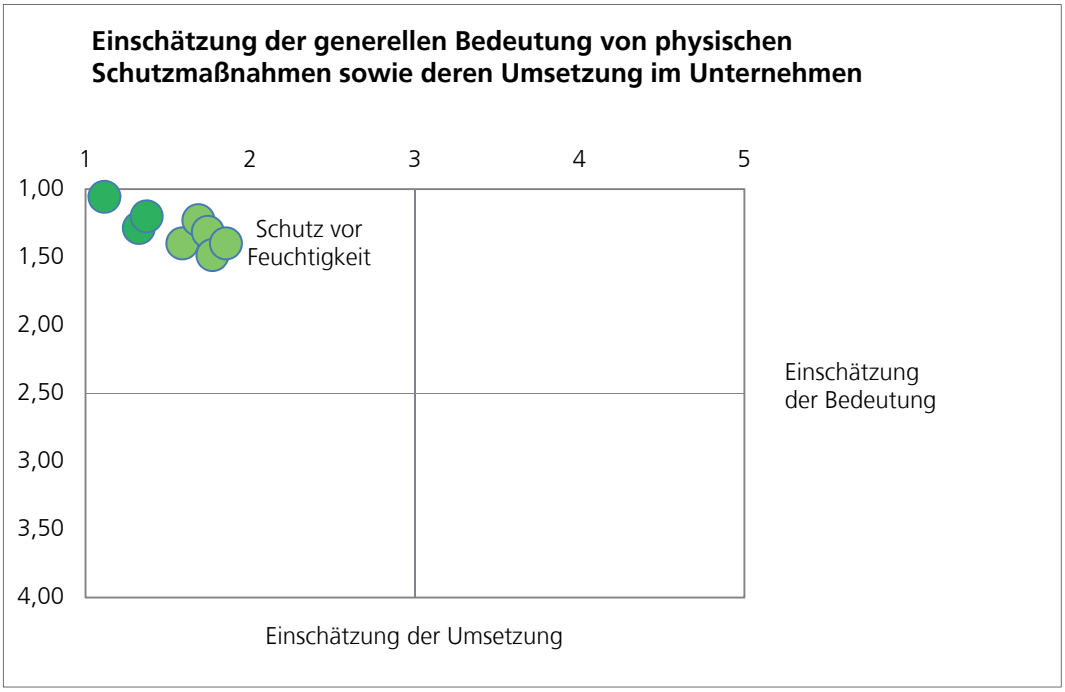
Maßnahmen zum Schutz gegen Witterungseinflüsse, Feuer oder technische Gebrechen



Schutzmaßnahmen gegen Witterungseinflüsse, Feuer oder technische Gebrechen zählen zum Standardrepertoire anerkannter Qualitätssicherungsnormen und funktionierender interner Kontrollsysteme. Dementsprechend hoch fielen die Bedeutungseinschätzungen durch die Unternehmen in diesem Bereich aus. Die regelmäßige Datensicherung zentraler Laufwerke (Backups) und die gesicherte Aufbewahrung dieser Backup-Medien in gesonderten Räumen werden offensichtlich als Kernaufgaben der IT mit hoher Priorität angesehen, wie der hohe Anteil von 91% bis 97% sehr guter und guter Bewertungen zeigt. Die Sicherung der Daten auf zentralen Laufwerken wird ebenfalls von 85% der Unternehmen als sehr gut bis gut beurteilt.

Auch in Sachen Schutz vor Blitzschlag, Feuer, Feuchtigkeit oder starken Temperaturschwankungen sind hohes Problembewusstsein und hohe Umsetzungsqualität zu konstatieren.

Wie wichtig die Datensicherung und physische Schutzmaßnahmen für die Studienteilnehmer sind und wie gut die Umsetzung in den Unternehmen nach Einschätzung der Befragten erfolgt, zeigt auch das Portfolio



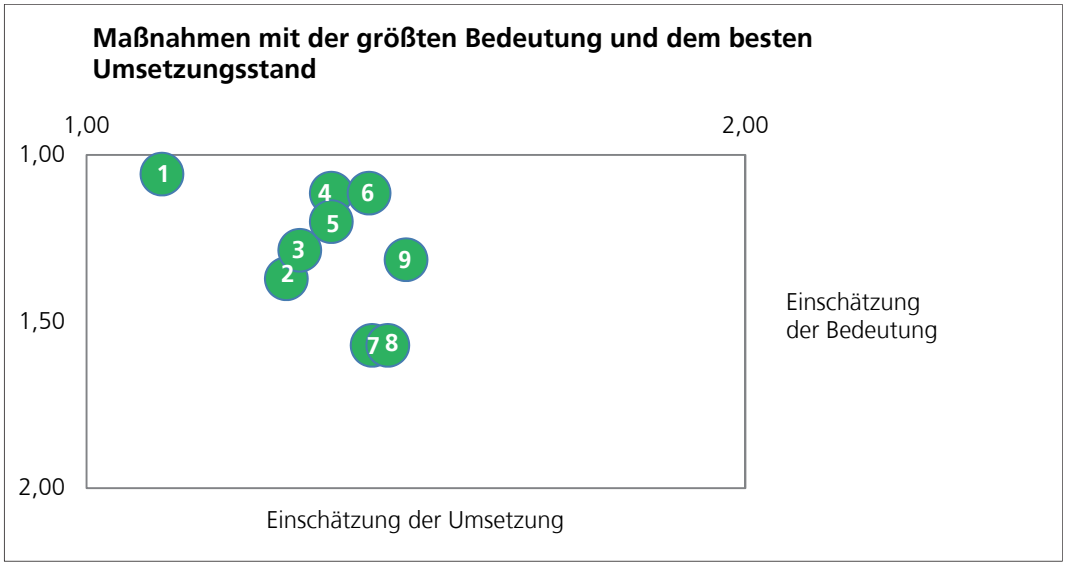
Risikobewusstsein und Umsetzungsqualität erreichen im Zusammenhang mit den Fragestellungen der Datensicherung und physischen Schutzvorkehrungen die besten Ergebnisse, wie auch die Tabelle zeigt:

Maßnahme	Einschätzung der Umsetzung	Einschätzung der Bedeutung
Regelmäßige Datensicherungen zentraler Laufwerke	1,11	1,06
Klimatisierung von Räumlichkeiten kritischer IT-Infrastruktur	1,32	1,29
Gesicherte, von zentralen Serverräumen getrennte Verwahrung von Backup-Medien	1,37	1,20
Datenspeicherung nur auf zentralen Laufwerken	1,59	1,40
Ausreichende Vorkehrungen zum Schutz vor Blitzeinschlag, Stromausfällen, Überspannungsschutz u.ä.	1,69	1,23
Ausreichende Brandschutzeinrichtungen	1,74	1,31
Regelmäßiger Austausch überalterter Hardware	1,77	1,49
Ausreichender Schutz vor Feuchtigkeit und Wasser	1,85	1,40

6. Resümee

Zusammenfassend kann den mittelständischen Unternehmen der Steiermark bei Risikobewusstsein und Umsetzung ausgewählter Maßnahmen ein durchaus gutes Zeugnis ausgestellt werden. Insbesondere bei spezifischen Einzelmaßnahmen, wie zum Beispiel im Zusammenhang mit der Verwaltung von Passwörtern und Benutzerberechtigungen sowie im Bereich Datensicherung und Schutz vor Feuer oder Wasser, besteht nach Einschätzung der Unternehmen eine hohe Umsetzungsqualität bei hohem Problembewusstsein.

Das folgende Portfolio fasst noch einmal all jene Maßnahmen mit den besten Benotungen zusammen, denen auch eine hohe Bedeutung beigemessen wurde. Zur besseren Darstellung wurde der Ausschnitt des Portfolios vergrößert: die Notenskala spannt sich nur mehr von 1 bis 2 (statt 1 bis 5), jene für die Bedeutungseinschätzung von 1 bis 2 (statt 1 bis 4).



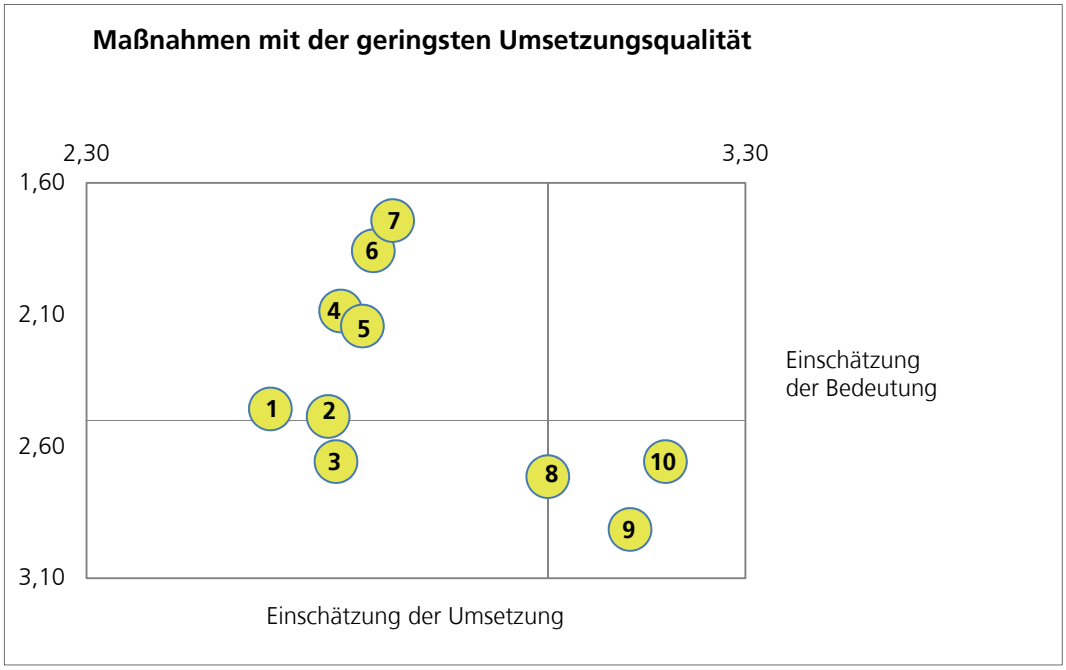
Nr.	Maßnahme	Einschätzung der Umsetzung	Einschätzung der Bedeutung
1	Regelmäßige Datensicherungen	1,11	1,06
2	Klare Vertretungsregeln bei Zahlungsverkehr	1,30	1,37
3	Klimatisierung kritischer IT-Räumlichkeiten	1,32	1,29
4	Firewall	1,37	1,11
5	Gesicherte Verwahrung von Backup-Medien	1,37	1,20
6	Virenschutz	1,43	1,11
7	Strenges 4-Augen-Prinzip beim Zahlungsverkehr	1,43	1,57
8	Verwendung von originaler Software mit Lizenzen	1,46	1,57
9	Dokumentation der Ausgabe von Schlüsseln	1,48	1,31

Was Datensicherheit (Nr. 1) und Zahlungsverkehr (Nr. 2) betrifft, zählen die aufgelisteten Maßnahmen jedenfalls zu den Mindestanforderungen der IT-Sicherheit. Sie werden üblicherweise vom Jahresabschlussprüfer regelmäßigen Stichproben unterzogen und zwar im Rahmen der Prüfung des internen Kontrollsystems und der IT. Umso erfreulicher, dass gerade hier die besten Durchschnittsnoten erreicht wurden – zumindest nach der Selbsteinschätzung der Unternehmen.

Ergänzend zu den oben dargestellten Top-Ergebnissen lässt sich feststellen, dass auch im Zusammenhang mit der Nutzung mobiler Endgeräte im Außendienst, der Datenträgerentsorgung und beim Informationsaustausch mit E-Mail durchwegs gute Ergebnisse erzielt werden.

Verbesserungsbedarf besteht bei den übergeordneten Maßnahmen. Mehr als die Hälfte der befragten Unternehmen wendet keinen IT-Standard wie zum Beispiel ISO 27001 oder COBIT an. Auch die Einbettung in das unternehmensweite Risikomanagementsystem, die regelmäßige Berichterstattung an das Management oder bewusstseinsbildende Maßnahmen zeigen bei vielen Unternehmen Handlungspotenziale auf. Aufgrund des engen Konnexes dieser Maßnahmen zur Unternehmensleitung ist hier die oberste Managementebene gefordert, dem Thema IT-Sicherheit höhere Priorität einzuräumen.

Im Einzelnen fanden sich auch schlechtere Einschätzungen der Umsetzungsqualität. Das folgende Portfolio fasst diese zusammen, wobei auch hier der Ausschnitt vergrößert wurde: die Notenskala spannt sich von 2,3 bis 3,3, die Skala der Bedeutung von 1,6 bis 3,1.



Nr.	Maßnahme	Einschätzung der Umsetzung	Einschätzung der Bedeutung
1	Persönliche Authentifizierung durch Portierdienst oder Überwachungspersonal	2,58	2,46
2	Änderung von Lieferantenstammdaten nur unter Anwendung des 4-Augen-Prinzips	2,67	2,49
3	regelmäßige Löschung alter E-Mails	2,68	2,66
4	Verbot bzw. Einschränkung von USB-Sticks	2,69	2,09
5	Einsatz von Verschlüsselungsverfahren	2,72	2,14
6	Interne Audits	2,74	1,86
7	Schulungen	2,76	1,74
8	sonstige Externe Audits	3,00	2,71
9	Infobroschüren	3,13	2,91
10	Penetration Tests durch externe Anbieter	3,18	2,66

Einzelne Maßnahmen sind aufgrund der Unternehmensgröße aus Kostengründen nur schwer umsetzbar. So wird sich nicht jedes Unternehmen einen Portierdienst (Nr. 1) leisten (können). Das Herausgeben von Infobroschüren (Nr. 9) kann man als unzeitgemäß bzw. unwirtschaftlich betrachten.

Mehr Augenmerk gelegt werden sollte auf die Verschlüsselung von Geräten und E-Mail und die strenge Einhaltung des Vier-Augen-Prinzips in der Lieferantenstammdaten-Verwaltung. Die Unternehmen könnten auch Überlegungen zur Optimierung des Datenaustausches anstellen: ob das Versenden kritischer Daten per E-Mail oder deren Austausch mittels USB-Sticks ohne spezielle Sicherheitsvorkehrungen noch zeitgemäß ist, bleibt fraglich.

Aus Sicht der Verfasser verbesserungswürdig erscheinen die Punkte Mitarbeiterschulungen (Nr. 7) und das Durchführen interner (Nr. 6) und externer Audits (Nr. 8). Sogenannte „White Hacker" können mittels Penetration Tests (Nr. 10) unbekannte Schwachstellen der IT-Systeme aufdecken helfen. Auf den kritischen Blick externer Experten sollte man keinesfalls verzichten; das Kostenargument zählt dabei nicht. Denn letztlich gilt gerade im Rahmen der IT-Sicherheit von Unternehmen – aber auch im privaten Bereich: „Better safe than sorry!"

ABC der IT-Risiken

Mit dem IT-Risiko wird die Wahrscheinlichkeit beschrieben, mit der eine interne oder externe Bedrohung aufgrund der Verwundbarkeit des Informationssystems zu negativen materiellen und/oder immateriellen Auswirkungen im Unternehmen und seinen Partnern führt. Die Folgen können kurz-, mittel- und langfristig wirken, wie etwa Imageschäden. Das Eintreten von IT-Risiken kann erhebliche negative Konsequenzen in den operativen Geschäftsprozessen zeitigen.[13]

IT-Systeme können das Einfallstor für schädliche Handlungen Dritter sein oder bei mangelhafter Sicherheitsarchitektur Mitarbeitern und Dritten Gelegenheiten für kriminelle Taten bieten. Neben den selteneren Fällen echter krimineller Energie, sollte man auch Vorsorge gegen Vorfälle höherer Gewalt oder menschliches Versagen treffen.

Im diesem Abschnitt findet sich eine detaillierte Auflistung möglicher IT-Risiken. Die angeführten Risikobeschreibungen wurden anhand der Quellen Klinger/Klinger[14], Löffler/Ahammer[15], Sowa/Duscha/Schreiber[16] und der Homepage des Bundesamtes für Sicherheit in der Informationstechnik[17] erstellt.

Adware:

Hierbei handelt es sich um Programme, die dazu dienen, Werbung auf dem Computer anzuzeigen, Suchanfragen auf Werbe-Webseiten umzuleiten und marketingrelevante Daten zu erfassen, wie zB die Art der besuchten Webseiten, um gezielt Werbung anzuzeigen. Schädlich ist diese Arte von Werbung vor allem dann, wenn sie für Spionage eingesetzt wird und die Daten weiterversendet, zusätzlich kann durch Adware ein hoher Computer-Ressourcenverbrauch entstehen.

Anlegen eines fiktiven Lieferanten, um Geld abzufischen:

Hat eine Person die Befugnis Lieferanten im System anzulegen und Geld zu überweisen, so kann diese Person einen fiktiven Lieferanten mit einer separaten Bankverbindung anlegen und so durch Scheingeschäfte Geld abfließen lassen.

---

[13] Vgl. KNOLL (2014), S. 17.
[14] Vgl. KLINGER/KLINGER (2011).
[15] Vgl. LÖFFLER/AHAMMER (2011).
[16] Vgl. SOWA/DUSCHA/SCHREIBER (2015).
[17] Vgl. O.V (2011): Gefährdungskataloge, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html [25.10.2016].

Ausfall (Krankheit, Unfall, etc.) des IT-Verantwortlichen:

Mangelnder Support bei auftretenden Problemen kann zu unnötig langem Ausfall des IT-Systems bzw. Betriebsverzögerungen oder schlimmsten Falls zu einem Betriebsstillstand führen.

BYOD bzw. Mobile Devices:

Durch private Nutzung von Mobiltelefonen, Laptops und dergleichen können bei verseuchten Geräten leicht Firmendaten in die falschen Hände geraten. Auch durch den Verlust des Gerätes sind die Firmendaten nicht vor unautorisiertem Zugriff geschützt.

Daten gelangen aufgrund nicht ordnungsgemäßer Entsorgung von Datenträgern an Dritte:

Dokumente mit vertraulichen oder personenbezogenen Inhalten werden mit dem Altpapier entsorgt ohne vorher unlesbar gemacht zu werden. Ähnliches gilt für nicht mehr gebrauchte Datenträger wie z.B. defekte Festplatten, Sicherungsbänder oder USB-Sticks.

Daten gelangen aufgrund unverschlüsselter E-Mails an Dritte:

Per E-Mail verschickte Informationen, Verträge oder Absprachen werden ohne Verschlüsselung versendet und können von Dritten abgefangen werden

Datenverlust aufgrund eines Brandes oder Blitzeinschlages:

Es gehen Daten aufgrund eines Brandes oder Blitzeinschlages verloren.

Datenverlust aufgrund eines Stromausfalles:

Es gehen Daten aufgrund eines Stromausfalles verloren.

Datenverlust aufgrund eines Wasserschadens:

Es gehen Daten aufgrund eines Wasserschadens verloren.

Datenverlust aufgrund Programmfehler:

Während der Verwendung oder Eingabe von Daten kommt es zu einem Absturz des Programms.

Datenverlust bzw. Spionage durch Diebstahl von mobilen Endgeräten:

Wenn in der Firma mit Smartphones, Tablets gearbeitet wird, können diese Geräte leicht gestohlen werden bzw. bei auswärtigen Terminen liegen gelassen und so können unbefugt an Daten kommen. Durch die private Nutzung dieser Geräte wird das Risiko zusätzlich erhöht.

DDoS – Denial of Service:

Hier wird der Internetzugang, das Betriebssystem oder die Dienste eines Hosts mit einer größeren Anzahl von Anfragen von übernommenen Rechnern belastet, als diese verarbeiten können, woraufhin reguläre Anfragen nicht oder nur sehr langsam beantwortet werden. Dabei ist es jedoch aus Sicht des Kriminellen wesentlich effizienter, Programmfehler auszunutzen, um eine Fehlerfunktion (wie einen Absturz) der Serversoftware auszulösen, worauf diese auf Anfragen ebenso nicht mehr reagiert.

Defacement von Websites:

Verunstaltet wird der eigentlich sichtbare Bereich der Webseite durch Hacker, indem fremde Texte oder Grafiken eingebunden werden.

Dialer:

Dialer sind Wählprogramme auf online Endgeräten, die eine teure Verbindung aufbauen können. Betrügerische Dialer werden heimlich auf fremde Geräte geschmuggelt, wählen unbemerkt eine teure (Mehrwert-)Rufnummer, trennen die Verbindung nicht oder bauen sie automatisch wieder neu auf. Der Schaden macht sich durch eine hohe Rechnung bemerkbar.

EDV-Mitarbeiter:

EDV-Mitarbeiter geben Daten an Dritte weiter, bzw. ermöglichen einen Zutritt von Dritten ins IT-Netz durch Lücken im Sicherheitsnetz oder EDV Mitarbeiter gehen mit vertraulichen Daten leichtsinnig um wie z.B. die Weitergabe von vertraulichen Daten im Bereich der EDV-Systeme an Freunde, Bekannte etc.

Eigene Webseite als Gefahrenquelle:

Besondere Vorsicht ist geboten, wenn ein Unternehmen eine komplexere Webseite betreibt – beispielsweise mit einem Kontaktformular, einem Gästebuch, einem Kundenforum oder mit einem eigenen Online-Shop. Meist setzen Kleinunternehmen hierfür fertige Tools wie Foren-Software oder Content-Management-Systeme für den Webauftritt ein. Diese Programme sind vergleichsweise schnell installiert und können auch von Nicht-Fachleuten bedient werden. Dabei wird aber vergessen, dass gerade weitverbreitete Tools von Hacker besonders gerne angegriffen werden. Angreifer wissen welche Lücken in welcher Software bzw. Softwareversion stecken und nutzen diese aus. Das Unternehmen bemerkt möglicherweise längere Zeit nicht, weil es die typischen Angriffstechniken nicht kennt, dass seine Webseite ein Sicherheitsrisiko darstellt.

Eigenerstellte IT-Systeme:

Werden von der IT-Abteilung IT-Systeme selbst erstellt, so kann es zu Risiken kommen, da der Programmierer Schwachstellen bewusst oder unbewusst einbauen könnte und dolose Handlungen möglich wären.

E-Mail-Viren:

Durch das Öffnen von Anhänge oder mitgeschickten Links bei E-Mails kann ein Virenbefall stattfinden. Bekanntes Beispiel ist der Locky-Virus. Dieser verschlüsselt die Daten des PC oder sperrt diesen. Die Hacker entschlüsseln die Daten bzw. entsperren den Rechner erst wieder, wenn Lösegeld (oft in der virtuellen Währung Bit Coins) bezahlt wird. Ein weiteres Beispiel ist Ransomware. Das sind Schadprogramme, mit deren Hilfe ein Eindringling eine Zugriffs- oder Nutzungsverhinderung der Daten sowie des gesamten Computersystems erwirkt. Dabei werden Daten auf einem fremden Computer verschlüsselt oder der Zugriff auf sie wird verhindert, um für die Entschlüsselung oder Freigabe ein „Lösegeld" zu fordern. Locker ransomware sperrt den Computer, crypto ransomware verschlüsselt Dateien.

Fake President Fraud:

Eine dritte, externe Person gibt per gefälschter oder übernommener E-Mail an die Geschäftsführung zu sein und ordert, dass eine sofortige Überweisung auf eine fremde Kontoverbindung notwendig ist.

Fehlende oder unzureichende Konzeption des Identitäts- und Berechtigungsmanagements:

Unberechtigte Zugriffe durch Mitarbeiter: es kann passieren, dass der zuständige Administrator keine Informationen über personelle Veränderungen erhält. So kann es vorkommen, dass ein Benutzerkonto eines ausgeschiedenen Mitarbeiters nicht gelöscht wird. Zusätzlich besteht die Gefahr, dass Mitarbeiter, die in eine neue Abteilung versetzt werden, ihre alten und nun nicht mehr benötigten Berechtigungen behalten und dadurch mit der Zeit umfangreiche Gesamt-Berechtigungen ansammeln.

Fehlendes oder unzureichendes mandantenfähiges Administrationskonzept für Speicherlösungen:

Bei der gemeinsamen Nutzung von IT-Systemen durch unterschiedliche Institutionen, wie sie im Cloud Umfeld weit verbreitet ist, existiert, bedingt durch ein fehlendes oder unzureichendes Rollenkonzept, die Gefahr eines mandantenübergreifenden administrativen Zugriffs. Da Administratoren in der Regel über sehr weitreichende Berechtigungen verfügen, stellt dies eine erhebliche Bedrohung aller Sicherheitsziele einer Institution dar. Insbesondere im Zusammenhang mit dem Servicemodell Infrastructure as a Service (IaaS), das häufig in Verbin-

dung mit Cloud Storage zur Anwendung kommt, besteht die Notwendigkeit zum Einsatz eines mandantenfähigen Administrationskonzeptes.

Geldabfluss aufgrund Online-Geschäfte/Online-Banking:

Finanzielle Mittel gehen verloren, da keine persönliche Unterschrift notwendig ist und mehrere Personen die notwendigen Zugangsdaten besitzen.

Geschäftsgeheimnisse/Kontaktdaten/Unternehmensdaten verkaufen/weitergeben:

Jemand kopiert/sichert Geschäftsgeheimnisse/Kontaktdaten/Unternehmensdaten und gibt diese weiter, um damit Geld zu verdienen.

Integrierte Cloud-Funktionalität:

Daten werden außerhalb der Grenzen der EU in Staaten ohne ausreichenden Datenschutz gespeichert. Anbieter von Cloud-Diensten unterliegen unter Umständen einer für die Wahrung kritischer Geschäftsgeheimnisse problematischen Jurisdiktion. Verträge kommen meist implizit über Allgemeine Geschäftsbedingungen der Cloud-Anbieter zustande und genügen österreichischen Datenschutzanforderungen nicht.

IT-Hardware wird defekt oder es kommt zu einem Systemabsturz:

Durch veraltete IT-Hardware bzw. unregelmäßigen Wartungen kann es zu einem Systemabsturz kommen, wodurch es zu Datenverlust oder zu Betriebsverzögerungen oder -stillstand kommt.

Nutzung von nicht-betrieblicher oder nicht-originaler Software:

Durch Nutzung von nicht-betrieblich angeschaffter Software können Schadprogramme eingeschleust werden, welche zu Datenverlust bzw -diebstahl führen können.

Outsourcing der IT (Abteilung):

Durch die Fremdvergabe der IT-Tätigkeit an (unseriöse) Dritte entstehen Sicherheitslücken, wodurch es zu Datendiebstahl etc. kommen kann.

Pass-the-Hash Angriffe:

Gibt der Benutzer im Zuge einer Passwort-basierenden Authentifizierung sein Passwort ein, wird zunächst aus dem Passwort ein Hash-Wert errechnet. Dieser wird zu einem Authentifizierungsserver übertragen und mit dem in einer Datenbank gespeicherten Hash verglichen. Stimmen die Werte überein, gilt der Benutzer als authentifiziert. Gelingt es nun einem Angreifer Passwort-Hashes zu erbeuten, kann er versuchen aus den Hashes auf die Passwörter zurück zurechnen.

Phishing:

Phishing wird der Trick genannt, geheime Daten, z.B. für das Online-Banking oder Zugriffsdaten, herauszulocken. In der Regel werden dazu betrügerische E-Mails oder Chatnachrichten versendet, in denen dazu aufgefordert wird auf Links zu klicken oder Dateianhänge zu öffnen und anschließend mit persönlichen Daten zu füllen.

Portscans:

Jeder PC braucht offene Ports für Internet-abhängige Anwendungen. Ports sind die „Ein- und Ausgangstore" eines Rechners. Jedes Datenpaket erreicht dank einer Portnummer sein richtiges Ziel. Man benötigt also zwingend einige offene Ports, um mit dem Internet kommunizieren zu können.

Rootkits:

Rootkits erlauben Angreifern, Daten von infizierten Computern zu stehlen. Rootkits werden üblicherweise tief im Betriebssystem versteckt und so programmiert, dass sie meist lange Zeit unentdeckt bleiben. Rootkits werden im gleichen Teil des Betriebssystems gestartet, in dem auch alle installierten Programme laufen. Sie richten Schaden an, indem sie sich in die Prozesse der gestarteten Programme einschleichen oder den Speicherbereich überschreiben. Eine andere Art von Rootkits läuft auf unterster Ebene des Betriebssystems und gibt dem Angreifer die komplette Kontrolle über einen Computer.

Snooping:

Unter Snooping versteht man das Abhören einer Verbindung auf einem Broadcast-Medium, einem Chat oder der Internettelefonie.

Social Engineering:

Dies sind zwischenmenschliche Beeinflussungen durch Kollegen mit dem Ziel an vertrauliche Informationen zu kommen.

Spoofed Invoice Fraud:

Nachdem ein Unternehmen eine Rechnung an ein anderes Unternehmen per E-Mail geschickt hat, folgt später ein zweites E-Mail von einer neu registrierten und ähnlich klingenden / aussehenden Domain-Namen. In der neuen E-Mail gibt es einen neuen Passus, der eine Änderung des Empfängerkontos verlangt. Mögliche angegebene Gründe dafür: Die Finanz sperrte ein Konto wegen Audit o.ä. Kommt es zu Rückfragen durch das Unternehmen B, wird vom Angreifer geantwortet, das wiederum teils mit gefälschten Dokumenten. Erkennt Unternehmen B diesen Angriffsversuch nicht, überweist es das Geld somit auf ein falsches Konto, nämlich jenes des Angreifers.

Spyware:

Spyware sind Programme, die sich ohne das Wissen und ohne aktives Zutun des PC-Nutzers auf dem Rechner installieren und dort unerwünschte Aktionen ausführen. Spyware spioniert Informationen über den Nutzer oder dessen Surfverhalten aus, sammelt diese und schickt sie über das Internet an interessierte Dritte. Gelegentlich manipuliert Spyware sogar die Einstellungen des Rechners oder verändert die Startseite oder sorgt dafür, dass ständig Werbung eingeblendet wird.

Systemausfall aufgrund Inkompatibilitäten veralteter IT-Infrastrukturen:

Durch die Inkompatibilitäten veralteter IT-Infrastrukturen kann es zu Kapazitätsengpässen führen, die einen Ausfall eines Teil- bzw. Komplettsystems zur Folge haben.

Trojaner:

Trojaner verstecken sich in scheinbar nützlichen Programmen, gelangen so unbemerkt auf den Computer und beginnen dann Schaden anzurichten oder schädliche Komponenten aus dem Internet nachzuladen. Die meisten Trojaner zielen darauf ab, auf dem infizierten Rechner Daten zu sammeln (Passwörter, Kreditkartennummern, Eingabe über die Tastatur etc.) und anschließend an den "Lenker" des Trojaners zu übermitteln.

Umgehung der Sicherheitssysteme

Sicherheitssysteme können bewusst umgangen werden, da zb. Ehemalige Mitarbeiter wissen wie die IT-Systeme funktionieren, da diese Personen selbst in der Abteilung IT-Sicherheit gearbeitet haben.

Unbeabsichtigte Vernichtung/Änderung von Daten etc.:

Mitarbeiter benutzen Programme etc. ohne Kenntnis über die Funktionen oder über das Ausmaß einer unbeabsichtigten Löschung.

Unberechtigter Zugriff:

Mitarbeiter greifen unberechtigt auf Daten, Netzwerke zu da Sie jemanden vertreten, der diese Zugriffsberechtigungen hat; sie die Berechtigungen noch haben obwohl sie versetzt wurden; die Passwörter leicht zu knacken sind bzw. Mitarbeite ihre PCs beim Verlassen des Arbeitsplatzes nicht sperren.

Ungünstige klimatische Bedingungen:

Ungünstige klimatische Bedingungen wie Hitze, Frost oder hohe Luftfeuchtigkeit können zu Schäden verschiedenster Art führen, beispielsweise zu Fehlfunktionen in technischen Komponenten oder zur Beschädigung von Speichermedien. Überschreitet die Umgebungstemperatur gewisse Grenzen dieses Bereiches nach oben oder unten, kann es zu Arbeitsausfällen, Betriebsstörungen oder zu Geräteausfällen kommen. So wird z. B. in einem Serverraum

durch die darin befindlichen Geräte elektrische Energie in Wärme umgesetzt und daher der Raum aufgeheizt. Bei unzureichender Lüftung kann die zulässige Betriebstemperatur der Geräte überschritten werden. Zu Lüftungszwecken werden unerlaubt Fenster von Serverräumen geöffnet. In der Übergangszeit (Frühjahr, Herbst) kann das bei großen Temperaturschwankungen dazu führen, dass durch starke Abkühlung die zulässige Luftfeuchte überschritten wird. Bei der Lagerung von digitalen Langzeitspeichermedien können zu große Temperaturschwankungen oder zu große Luftfeuchtigkeit zu Datenfehlern und reduzierter Speicherdauer führen. Einige Hersteller geben die optimalen Lagerbedingungen für Langzeitspeichermedien mit Temperaturen von 20 bis 22°C und einer Luftfeuchtigkeit von 40% an. Auch analoge Speichermedien, wie Papier oder Mikrofilme, benötigen bestimmte Lagerbedingungen.

Unzureichende Auswahl des Cloud-Dienstanbieters:

Häufig werden bei der Auswahl des Cloud-Dienstanbieters wichtige Faktoren wie beispielsweise dessen Reputation, Anbieter-Rankings, öffentlich zugängliche Pflichtenhefte der Dienstanbieter, Verpflichtungen zur Einhaltung von Gesetzen und Richtlinien oder erworbene Zertifizierungen nicht oder nur unzureichend berücksichtigt. Der Cloud-Markt ist für Auftraggeber wenig transparent, es fehlen standardisierte Angebote der Cloud-Dienstanbieter. Daraus können Sicherheitsprobleme beim Cloud-Dienstanbieter (zum Beispiel bei mangelhafter Verfügbarkeit) resultieren. Diese sind häufig mit finanziellen Einbußen für die nutzende Institution verbunden, wenn diese auf die Verfügbarkeit der Services angewiesen ist, um ihrerseits einen Service erbringen zu können.

Verlust von Daten bei Weitergaben:

Bei Datenweitergabe wird die Datei von einer nicht autorisierten Person abgefangen.

Würmer:

Ein Wurm ist ein schädliches Programm, das sich schnell selbst kopiert und verbreitet. Ein Wurm nutzt alle Möglichkeiten sich im Internet über E-Mails oder durch Sicherheitslücken selbst zu verschicken. Dafür durchforstet der Wurm sämtliche Adressbücher und Adresslisten, die er in den E-Mail-Programmen am Computer entdeckt. Durch den selbst initiierten Massenversand können Würmer enorme Netzwerkressourcen verbrauchen und können damit einen enormen finanziellen Schaden anrichten.

Zugriff auf Firmen Mailaccount über WLAN:

Durch den Zugriff auf Firmen Mail Accounts etc. über öffentliche WLAN Netze können sich Hacker Zugang zu Firmendaten verschaffen.

Zutritt von nicht berechtigten Dritten bzw. Einbruch:

Nicht mit der Befugnis ausgestattete Personen betreten den unerlaubten Bereich und gelangen zu vertraulichen Informationen.

Zutritt nicht berechtigter Mitarbeiter:

Mitarbeiter betreten unerlaubte Bereiche und stehlen dabei Festplatten, Datenträger oder kopieren sensible Daten.

Literatur

FRISCH, A. [2003]: Unix System Administration, 2. Auflage, Köln: O´Reilly Verlag, 2003.

FRÖSCHLE, P. [2011]: IT Sicherheit & Datenschutz, in: Praxis der Wirtschaftsinformatik (2011),Volume 281.

HEITMANN, M. [2007]: IT-Sicherheit in vertikalen F&E-Kooperationen der Automobilindustrie, Bochum: Deutscher Universitäts Verlag, 2008.

KERSTEN, H./KLETT G. [2015]: Der IT Security Manager, 4. Auflage, Wiesbaden: Springer Verlag, 2015.

KERSTEN, H./REUTER J./ SCHRÖDER K. [2008]: IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz, Wiesbaden: Friedr. Vieweg & Sohn Verlag, 2008.

KLINGER, M/KLINGER O. [2011]: ABC der Gestaltung und Prüfung des Internen Kontrollsystems (IKS) im Unternehmen, 3. Auflage, Wien: Linde Verlag, 2011.

KNOLL, M. [2014]: Praxisorientiertes IT-Risikomanagement: Konzeption, Implementierung und Überprüfung, Heidelberg: dpunkt.verlag, 2014.

LÖFFLER, H/AHAMMER M. [2011]: Handbuch zum internen Kontrollsystem, 2. aktualisierte Auflage, Wien: Linde Verlag, 2011.

MÜLLER, K. [2014]: IT Sicherheit, 5. bearbeitete und erweiterte Auflage, Wiesbaden: Springer Verlag, 2014.

SOWA, A./DUSCHA P./SCHREIBER S. [2015]: IT-Revision, IT-Audit und IT-Compliance, Wiesbaden: Springer Verlag, 2015.

VOLKMER, T./SINGER, M. [2008]: Tatort Internet, München: Markt+Technik Verlag, 2008.

Anhang

Folgender Fragebogen wurde für die Umfrage verwendet:

1.	**Statistischer Teil**
1.1	In welcher/n Branche/n gemäß ÖNACE-Liste ist Ihr Unternehmen tätig?
1.1.1	Industrie, Gewerbe, Energie- und Wasserversorgung (Gruppe C, D, E und F nach ÖNACE-Code)
1.1.2	Handel; Instandhaltung und Reparatur von Kraftfahrzeugen (G)
1.1.3	Dienstleistungen und Sonstige (Gruppe H bis S nach ÖNACE-Code)
1.2	Wie viele Mitarbeiter sind im Unternehmen beschäftigt?
1.2.1	>50 bis 100
1.2.2	>100 bis 150
1.2.3	>150 bis 200
1.2.4	>200 bis 250
1.2.5	>250
1.3	Unterliegt ihr Unternehmen der Abschlussprüfungspflicht durch einen Wirtschaftsprüfer?
1.3.1	Ja
1.3.2	Nein
1.4	Wie schätzen Sie auf einer Skala von 1 (=sehr hoch) bis 5 (=gering) die Bedeutung der IT für das Unternehmen und deren Kernprozesse ein?
1.5	Wer ist in Ihrem Unternehmen für die Wartung und Aktualisierung Ihrer IT-Systeme zuständig?
1.4.1	Eigene Mitarbeiter
1.4.2	Externe Dienstleister
1.4.3	Eigene und Externe
1.6	Wie viele Mitarbeiter sind in Ihrem Unternehmen im Bereich IT tätig?
1.5.1	0 Mitarbeiter
1.5.2	1 bis 3
1.5.3	4 bis 6
1.5.4	>6 Mitarbeiter
1.7	Wie wurde der Fragebogen ausgefüllt?
1.7.1	Nicht ausgefüllt
1.7.2	Unvollständig ausgefüllt
1.7.3	Vollständig ausgefüllt
1.8	Warum wurde der Fragebogen nicht vollständig ausgefüllt
1.8.1	Keine Ansprechperson
1.8.2	Keine Zeit/Interesse
1.8.3	Sonstiges
2.	**IT-Sicherheit allgemein**
2.1	Sie finden unten IT-Standards bzw. Empfehlungen angeführt. Kreuzen Sie an ob der jeweilige Standard in Ihrem Unternehmen angewendet wird und falls ja, benoten Sie die Qualität der Umsetzung des Standards im Unternehmen gemäß dem Schulnotensystem (1= sehr gut bis 5 nicht genügend)
2.1.1	ISO 27001
2.1.2	ISO 27005
2.1.3	BSI-IT -Grundschutz
2.1.4	COBIT
2.1.5	Österreichisches Informationssicherheitshandbuch
2.1.6	WKÖ IT-Sicherheitshandbuch

2.2	Wie gut oder schlecht werden die folgenden Maßnahmen im Unternehmen umgesetzt? Treffen Sie eine Einschätzung von sehr gut (1) bis nicht genügend (5)!
2.2.1	IT-Sicherheit ist Teil des unternehmensweiten Risikomanagement-Systems
2.2.2	Es erfolgt eine regelmäßige Berichterstattung an das Management über den Status bzw. Vorfälle betreffend IT-Sicherheit.
2.2.3	Das Unternehmen stellt für die IT-Sicherheit ausreichend Ressourcen zur Verfügung
2.3	Sie finden unten mögliche Richtlinien zur IT-Sicherheit aufgelistet. Kreuzen Sie an ob die jeweilige Richtlinie in Ihrem Unternehmen angewendet wird und falls ja, benoten Sie die Qualität der Umsetzung der Richtlinie im Unternehmen gemäß dem Schulnotensystem (1= sehr gut bis 5 nicht genügend)
2.3.1	Richtlinie zur Vorgehensweise im IT-Notfall (Virenbefall, etc.)
2.3.2	Richtlinie zur Nutzung von E-Mails, Internet und Social Media
2.3.3	Richtlinie zur Nutzung von mobilen IT-Geräten (Notebook, Tablet, Smartphone usw.) und Speichermedien
2.3.4	Richtlinie zur Datenvernichtung und Geräteentsorgung
2.3.5	Passwortrichtlinie
2.3.6	Richtlinie zum Umgang mit personenbezogenen Daten
2.3.7	Die im Unternehmen eingeführten Richtlinien werden regelmäßig auf ihre Einhaltung überprüft (bspw. durch Interne Revision, Management, Vorgesetzte, IT, externe Audits usw.)
2.4	Wie schätzen Sie die Umsetzung folgender bewusstseinsbildender Maßnahmen im Unternehmen ein (IT-Security Awareness)?
2.4.1	Formale Vorgaben in Form von Dokumenten, Richtlinien, etc.
2.4.2	Schulungen, Workshops u.ä.
2.4.3	Newsletter bzw. E-Mail-Aussendungen
2.4.4	Infobroschüren
2.4.5	Sonstige Informationsmaßnahmen (bitte anführen)
3.	**Spezifische Maßnahmen der IT-Sicherheit**
3.1	Wie schätzen Sie die Umsetzung folgender Maßnahmen im Unternehmen ein, die das Risiko eines Befalls mit Schadsoftware (Viren, Trojaner usw.) bzw. schädlicher Handlungen Dritter (Cybercrime generell) minimieren helfen sollen (Schulnotensystem)?
3.1.1	Virenschutz
3.1.2	Firewall
3.1.3	Spamfilter
3.1.4	Sperrliste für gefährdende E-Mail-Adressen
3.1.5	Verbot bzw. Einschränkung der Verwendung von (privaten) USB-Sticks und anderen Wechselmedien, Sperren von (USP-)Ports u.ä.
3.1.6	Einschränkungen bei der Nutzung des Internets und sozialer Medien (Sperre von Webseiten)
3.1.7	Verbot bzw. Einschränkung der Installation von Software für Nicht-Administratoren
3.1.8	Verwendung von ausschließlich originaler Software mit Lizenzen
3.1.9	Verwendung der HTTPS-Übertragung auf Webseiten
3.1.10	Interne Audits (Überprüfung des Systems auf etwaige Sicherheitslücken, Vulnerability Scans o.ä.)
3.1.11	Penetration Tests durch externe Anbieter ("White Hacks")
3.1.12	sonstige Externe Audits

3.2	Wie schätzen Sie das Ausmaß der unten angeführten Bedrohungen für die IT-Sicherheit und den elektronische Zahlungsverkehr in ihrem Unternehmen ein (von 1 keine Bedrohung bis 5 sehr starke Bedrohung)
3.2.1	Phishing
3.2.2	Viren & Malware
3.2.3	SPAM-Mails
3.2.4	Datendiebstahl durch Dritte
3.2.5	Datendiebstahl durch eigene Mitarbeiter
3.2.6	Datenmanipulation durch Dritte
3.2.7	Datenmanipulation durch eigene Mitarbeiter
3.2.8	Gezielte Angriffe auf das IT-System (zur Sabotage, Erpressung u.ä.)
3.2.9	Gezielte Angriffe auf oder Manipulation von Kassen- und Zahlungssystemen am Point of Sale
3.2.10	Unautorisierte Überweisungen bzw. Unterschlagungen durch Dritte
3.2.11	Unautorisierte Überweisungen bzw. Unterschlagungen durch eigene Mitarbeiter
3.3	Welche der unten angeführten Bedrohungen sind im Unternehmen bereits eingetreten (ja/nein/keine Angabe)?
3.3.1	Phishing
3.3.2	Viren & Malware
3.3.3	SPAM-Mails
3.3.4	Datendiebstahl durch Dritte
3.3.5	Datendiebstahl durch eigene Mitarbeiter
3.3.6	Datenmanipulation durch Dritte
3.3.7	Datenmanipulation durch eigene Mitarbeiter
3.3.8	Gezielte Angriffe auf das IT-System (zur Sabotage, Erpressung u.ä.)
3.3.9	Gezielte Angriffe auf oder Manipulation von Kassen- und Zahlungssystemen am Point of Sale
3.3.10	Unautorisierte Überweisungen bzw. Unterschlagungen durch Dritte
3.3.11	Unautorisierte Überweisungen bzw. Unterschlagungen durch eigene Mitarbeiter
3.4	Wie schätzen Sie die Umsetzung bzw. Anwendung der folgenden Maßnahmen im Unternehmen ein, die unberechtigte Zugriffe auf das System verhindern sollen?
3.4.1	Umfassendes Identitäts- und Berechtigungsmanagement (festgelegte Regeln für die Einrichtung von Benutzern und der Rechteverwaltung)
3.4.2	Dokumentation zugelassener Benutzer und Rechteprofile
3.4.3	Monitoring der Richtigkeit und Aktualität von Berechtigungen
3.4.4	Unverzügliche Berücksichtigung von personellen und aufgabenbezogenen Änderungen sowie sofortige Deaktivierung bzw. Löschung der Rechte und Benutzerkennung bei Ausscheiden eines Mitarbeiters
3.4.5	Vorkehrungen und organisatorische Regelungen für Zugriffsmöglichkeiten in Vertretungs- bzw. Notfällen, damit keine Weitergabe von Passwörtern in Abwesenheitsfällen notwendig ist
3.4.6	Verwendung der Bildschirmsperre bei Verlassen des Arbeitsplatzes
3.4.7	Protokollierung der Zugriffe auf Systeme und Daten

3.5	Wie schätzen Sie die Umsetzung bzw. Anwendung der folgenden Maßnahmen zum Passwortgebrauch im Unternehmen ein?
3.5.1	Passwörter haben mindestens 6 Zeichen sowie Verwendung von mindestens einem Sonderzeichen und/oder einer Zahl.
3.5.2	Pflicht zum regelmäßigen Passwortwechsel (z.B. alle 90 Tage), der regelmäßig und automatisch vom System initiiert wird.
3.5.3	Wiederholung von alten Passwörter beim Passwortwechsel wird systemseitig verhindert
3.5.4	Vermeidung von Passwörtern mit leicht nachvollziehbarer Bedeutung (z.B. Name, Geburtsdatum, etc.), von Standard- oder Trivialausdrücken (z.B. Test, System, etc.), von Tastatur- und Zeichenmustern (z.B. QWERTZ, 123456) als Passwort
3.5.5	Eingabe des Passwortes findet unbeobachtet statt (v.a. bei Kundenverkehr); Eingabe des Passwortes wird nicht am Bildschirm angezeigt
3.5.6	Passwörter werden nicht schriftlich festgehalten und falls doch, sind diese sicher aufbewahrt bzw. im System zugriffssicher gespeichert.
3.5.7	Vornahme eines sofortigen Passwortwechsels, wenn Passwort unautorisierten Personen bekannt geworden ist
3.5.8	Passwörter werden bei der Authentifizierung in vernetzten Systemen verschlüsselt übertragen
3.6	Wie schätzen Sie die Umsetzung bzw. Anwendung der folgenden Maßnahmen des elektronischen Zahlungsverkehrs im Unternehmen ein, um unautorisierte Geldabflüsse zu vermeiden? (Ggf. Finanzabteilung konsultieren!)
3.6.1	Trennung von Anweisung/Genehmigung und Durchführung (4-Augen-Prinzip)
3.6.2	Einsatz von Workflow-Managementsystemen mit umfassenden Identitäts- und Berechtigungskonzept
3.6.3	Änderung von Lieferantenstammdaten nur unter Anwendung des 4-Augen-Prinzips
3.6.4	klare Vertretungsregeln für die Durchführung des Zahlungsverkehrs
3.6.5	Betragsobergrenzen für die Genehmigung und Durchführung von Zahlungen
3.6.6	Protokollierung der Zugriffe bzw. des Zahlungsverkehrs
3.6.7	Regelmäßiges Monitoring der Zahlungen ex post
3.7	Wie schätzen Sie die Umsetzung bzw. Anwendung der folgenden Maßnahmen in Bezug auf die sichere (auch unternehmensexterne) Nutzung und Aufbewahrung von mobilen IT-Geräten (Notebooks, Tablets, Smartphones usw.) im Unternehmen ein?
3.7.1	Information und Sensibilisierung der Mitarbeiter über die potentiellen Gefahren bei Mitnahme und Nutzung eines solchen Gerätes außerhalb der geschützten Umgebung bzw. des Unternehmens
3.7.2	Installation eines Zugriffschutzes (Passwort, Chipkarte), einer Festplatten- oder Dateiverschlüsselung sowie einer Sicherheitssoftware
3.7.3	Minimierung der Zeiten, in denen das Gerät unbeaufsichtigt bleibt und Aktivierung der Passwortsperre, wenn das Gerät verlassen werden muss
3.7.4	Vermeidung der Sichtbarkeit des Gerätes bei Aufbewahrung im KFZ
3.7.5	Bei Hotelaufenthalt Aufbewahrung der mobile Devices in verschlossenen Schränken
3.7.6	Vermeidung öffentlicher, unverschlüsselter WLANs
3.8	Wie schätzen Sie die Umsetzung bzw. Anwendung der folgenden Maßnahmen in Bezug auf den Informationsaustausch mit E-Mail im Unternehmen ein?
3.8.1	Abschluss von Vertraulichkeitsvereinbarungen
3.8.2	Festlegung einer Sicherheitspolitik für E-Mail-Nutzung (Rahmenbedingungen der Nutzung, Schulungen, etc.)
3.8.3	Vorkonfiguration der E-Mail-Programme durch die Systemadministration
3.8.4	regelmäßige Löschung alter E-Mails
3.8.5	Protokollierung eingehender E-Mails
3.8.6	Einsatz von Verschlüsselungsverfahren

3.9	Wie schätzen Sie die Umsetzung bzw. Anwendung der folgenden Maßnahmen der Entsorgung von Datenträgern im Unternehmen ein?
3.9.1	Datenträger werden mehrfach formatiert
3.9.2	Datenträger werden physikalisch gelöscht und zerstört
3.9.3	Sensible Dokumente werden eigenhändig geschreddert
3.9.4	Sensible Dokumente werden einer anderen, vertrauenswürdigen Person zur Vernichtung übergeben
3.10	Wie schätzen Sie die Umsetzung bzw. Anwendung der folgenden Maßnahmen zum Schutz vor unberechtigtem Zutritt zu sensiblen Bereichen (IT, F&E, Finanzabteilungen) im Unternehmen ein?
3.10.1	Festgelegte Zutrittspolitik (Regelung, welche Personen Zutritt zu welchen Bereichen haben)
3.10.2	Dokumentation der Vergabe und Rücknahme von Zutrittsberechtigungen
3.10.3	Alarmanlagen, Videoüberwachung, Bewegungsmelder und Einbruchschutz
3.10.4	Persönliche Identifikation bzw. Authentifizierung durch Portierdienst oder Überwachungspersonal
3.10.5	Automatische Identifikation bzw. Authentifizierung mittels Zugangscodes, Chipkarten oder biometrische Methoden
3.10.6	Regelungen für Ausnahmesituationen (z.B. bei Brandalarm)
3.10.7	Zentrale Regelung der Herstellung, Aufbewahrung, Verwaltung und Ausgabe von Schlüsseln und/oder Chipkarten
3.10.8	Sichere Aufbewahrung nicht ausgegebener Schlüssel
3.10.9	Dokumentation der Ausgabe von Schlüsseln
3.11	Wie schätzen Sie die Umsetzung bzw. Anwendung der folgenden Maßnahmen zum physischen Schutz im Unternehmen ein?
3.11.1	Klimatisierung von Räumlichkeiten kritischer IT-Infrastruktur
3.11.2	Regelmäßiger Austausch überalterter Hardware
3.11.3	Datenspeicherung nur auf zentralen Laufwerken, nicht auf lokalen Festplatten oder mitarbeitereigenen externen Speichern
3.11.4	Regelmäßige Datensicherungen zentraler Laufwerke (Backups)
3.11.5	Gesicherte, von zentralen Serverräumen getrennte Verwahrung von Backup-Medien
3.11.6	Ausreichende Brandschutzeinrichtungen (Feuermelder, Brandschutztüren, Distanz zu Räumen mit potenziellen Hitze- und Feuerquellen, Feuerlöscher usw.)
3.11.7	Ausreichende Vorkehrungen zum Schutz vor Blitzeinschlag, Stromausfällen, Überspannungsschutz u.ä.
3.11.8	Ausreichender Schutz vor Feuchtigkeit und Wasser (Wassermelder, kritische IT-Infrastruktur in höheren Stockwerken, Entfernung zu Hauptwasserleitungen usw.)

Autoren

Prof. (FH) Mag. Gregor Reautschnig, StB

ist Professor an der Fachhochschule CAMPUS 02 in Graz und Fachbereichskoordinator für Rechnungswesen & Steuern an der Studienrichtung Rechnungswesen & Controlling sowie Autor einschlägiger Publikationen.

Prof. (FH) Dr. Helmut Michl

ist Professor an der Fachhochschule CAMPUS 02 in Graz und Fachbereichskoordinator für wissenschaftliche und quantitative Methoden an der Studienrichtung Rechnungswesen & Controlling sowie Autor einschlägiger Publikationen.

Notizen

Impressum

Titel

IT-Sicherheit und IKS im steirischen Mittelstand – Aktueller Stand und Bedeutung

Graz 2016
ISBN 978-3-9503272-9-8

Herausgeber

Prof. (FH) Mag. Peter Meiregger, StB | FH CAMPUS 02, Rechnungswesen & Controlling
Prof. (FH) Dipl.-Ing. Dr. Christian Theuermann | FH CAMPUS 02, Rechnungswesen & Controlling

Autoren

Prof. (FH) Mag. Gregor Reautschnig, StB | FH CAMPUS 02, Rechnungswesen & Controlling
Prof. (FH) Dr. Helmut Michl | FH CAMPUS 02, Rechnungswesen & Controlling

Mitwirkung

Sandra Kriendlhofer
Robert Magnes, BA
Verena Maier
Keno Mischling
Cornelia Peuker, BA
Michaela Stoiser
Carmen Tschiggerl

Kontakt/Redaktion

Mag.ª Tanja Mikschofsky, Bakk.

CAMPUS 02 – Fachhochschule der Wirtschaft GmbH
Studienrichtung Rechnungswesen & Controlling

Körblergasse 126, 8010 Graz
Tel.: 0316 6002 - 605
E-Mail: tanja.mikschofsky@campus02.at
www.campus02.at

www.campus02.at

Covermotiv: © Wei Ming - shutterstock.com

ISBN 978-3-9503272-9-8