Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik
FH Zentralschweiz

Information Security & Privacy

Nationale Studie zur Informationssicherheit in Schweizer KMU

hslu.ch/forschung-information-security

Oliver Hirschi, Prof. Armand Portmann

Vorwort

In immer kürzerer Folge berichten die Medien über Sicherheitsvorfälle, die in der Schweiz, in Europa oder anderswo auf der Welt stattfinden. Das Departement Informatik hat diese Entwicklung letztes Jahr zum Anlass genommen, die Schweizer KMU zum Thema Informationssicherheit zu befragen.

Seit längerem ist bekannt, dass nicht nur grosse Firmen, beispielsweise aus der Finanzbranche, von den zunehmenden Gefahren aus dem Cyber-Space bedroht sind, sondern auch die in jeder Hinsicht sehr vielfältige Landschaft der Schweizer KMU. Also kleine und mittelständische Betriebe, die in unterschiedlichsten Bereichen tätig sind. Um die geplante Umfrage möglichst breit abzustützen und dadurch dieser Firmenvielfalt Rechnung zu tragen, hat die Hochschule Luzern die Kooperation mit verschiedenen Organisationen und Verbänden gesucht, die das Unterfangen mithilfe ihrer Vernetzung mit den Schweizer KMU unterstützen konnten. Fündig wurde die Hochschule Luzern beim KMU Verband, beim Staatssekretariat für Wirtschaft SECO, bei der Schweizer Kader Organisation SKO und bei economiesuisse. Diesen vier Organisationen gilt ein grosser Dank. Ohne ihre Mithilfe hätte die Umfrage nicht so viel Beachtung gefunden – es haben schliesslich circa 230 Unternehmen mitgemacht.

In vielen KMU fehlt es noch immer an Wissen zum Umgang mit dem Thema Informationssicherheit. Dies bestätigen nicht nur die nun vorliegenden Ergebnisse, sondern auch die anhaltend hohe Nachfrage nach Weiterbildungen im Bereich der Informationssicherheit des Departements Informatik (hslu.ch/information-security-privacy) und auch die Beliebtheit der vom Departement zusammen mit namhaften Schweizer Finanzinstituten getragenen Dienstleistung «eBanking – aber sicher!» (www.ebas.ch).

Wir sind überzeugt, mit der vorliegenden Studie einen wichtigen Beitrag zu mehr Informationssicherheit in den Schweizer KMU zu leisten. Zahlreiche KMU haben sich nur schon durch die Teilnahme an der Studie Gedanken zu deren eigenen Informationssicherheit gemacht. Darüber hinaus können wir mit den vorliegenden Resultaten unsere Engagements im Bereich Informationssicherheit weiter schärfen und gezielt weiterentwickeln.

Rotkreuz, Oktober 2017

Oliver Hirschi

Dozent
Leiter «eBanking – aber sicher!»

Hochschule Luzern – Informatik

Prof. Armand Portmann

Dozent
Kursleiter CAS/MAS Informationssicherheit

Hochschule Luzern – Informatik

Inhaltsverzeichnis

Einleitung

Die dieser Studie zugrundeliegenden Informationen stammen aus einer Online-Umfrage, die das Departement Informatik der Hochschule Luzern zwischen Juli und Dezember 2016 durchgeführt hat. An der Umfrage haben sich circa 230 Schweizer KMU beteiligt.

Die Umfrage war in die folgenden 5 Themengebiete aufgegliedert:

1. Demographie der Unternehmung
2. Bedrohungslage und Verletzlichkeit
3. Governance und Organisation
4. Sicherheitsmassnahmen
5. Spezialthema «E-Banking»

Dabei waren in jedem Gebiet zwischen drei und zehn Fragen zu beantworten, insgesamt etwa 30 Fragen. Die erste Fragengruppe diente der Vermittlung eines Bildes der teilnehmenden Firmen (Branche, Grösse, Region etc.). Über die zweite Gruppe wurden die Bedrohungslage und die Verletzlichkeit in Erfahrung gebracht. Dazu gehört neben der Einschätzung der Gefahrensituation, wie sie beispielsweise von den Medien dargestellt wird, auch die Beurteilung der Gefahren auf der Basis von eigenen Erfahrungen oder Sicherheitsvorfällen. Im gleichen Kapitel waren Fragen zu den genutzten IT-Technologien (Remote-Access, Cloud etc.) zu beantworten. Diese Technologien haben einen Einfluss auf die Verletzlichkeit. Im dritten Kapitel ging es um die Thematik der Steuerung und Kontrolle der Informationssicherheit. Diese Fragen geben Auskunft über die «Maturität» der Informationssicherheit in einer Unternehmung. Werden also bloss ad hoc gerade auftretende Sicherheitsvorfälle behandelt oder gibt es Prozesse, mit denen ein bestimmtes Sicherheitsniveau aufrechterhalten und kontinuierlich verbessert wird. Darauf folgten Fragen zu den konkret angewendeten technischen Sicherheitsmassnahmen. Mit dem Spezialthema «E-Banking» wurde der Fragenkatalog schliesslich abgeschlossen. Diese Zusatzfragen sollen zeigen, welchen Stellenwert das E-Banking in den Schweizer KMU hat.

Auswertung

Demographie der Unternehmungen

Sprachregionen

Von den 230 teilnehmenden Firmen stammen beinahe drei Viertel aus der Deutschschweiz und ungefähr 20 Prozent aus der französischsprachigen Schweiz (inkl. Fribourg und Wallis). Der Rest verteilt sich auf die italienische Schweiz und Liechtenstein, das in der Umfrage auch berücksichtigt wurde.

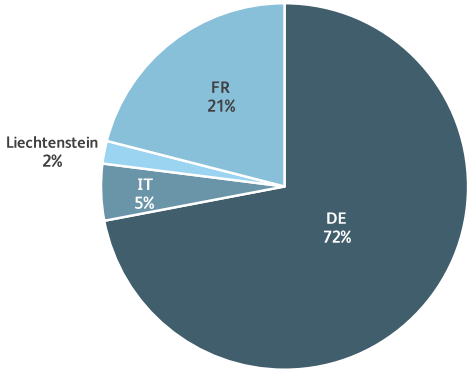

Abbildung 1: Sprachregionen (De: Deutschschweiz, Fr: französischsprachige Schweiz, IT: italienische Schweiz)

Unternehmensgrössen

Bei der Unternehmensgrösse stellen Firmen mit weniger als zehn Mitarbeitenden die grösste Gruppe. Sie machen fast 60 Prozent aus. Es haben also viele sehr kleine Unternehmen mitgemacht. Die restlichen 40 Prozent verteilen sich etwa in gleichem Umfang auf Firmen mit 10 bis 49 respektive mit 50 bis 249 Mitarbeitenden.

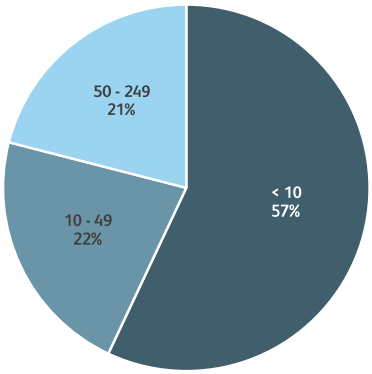

Abbildung 2: Unternehmensgrössen (Anzahl Mitarbeitende)

Branchen

Die Untersuchung der Branchenzugehörigkeit der teilnehmenden Firmen zeigt, dass die Dienstleistungsbranche die grösste Gruppe stellt. Es ist nicht verwunderlich, dass innerhalb dieser Gruppe Dienstleistungen der Informationstechnologie am stärksten vertreten sind. Firmen, die sich in diesem Bereich betätigen, sind sich meist der Gefahren bewusst und zeigen deshalb eine grössere Affinität zum Thema der Studie. Mit der gleichen Begründung kann die grosse Resonanz bei der Rechts- und Steuerberatung, der Wirtschaftsprüfung, der allgemeinen Unternehmensberatung und auch beim Gesundheits- und Sozialwesen erklärt werden. Überrascht hat im Gegensatz dazu die kleine Resonanz bei der Branche der Energie- und Wasserversorgung, handelt es sich doch um so genannte «kritische Infrastrukturen», also um Anlagen, die für die Gesellschaft von sehr grosser Bedeutung sind. Dies steht in gewisser Weise im Widerspruch zur feststellbaren Tendenz, die bei den Betreibern kritischer Infrastrukturen eine Zunahme des Bewusstseins für das Thema Informationssicherheit zeigt. Allerdings gibt es vergleichsweise wenige Betreiber solcher Anlagen, welche wahrscheinlich über den Verteiler nicht erreicht wurden.

Abbildung 3: Branchen

Funktion

Grossmehrheitlich, nämlich zu fast 70 Prozent, wurde die Umfrage von einem Mitglied der Geschäftsleitung beantwortet. Dies überrascht nicht, da die Risiken der Informationssicherheit, wie alle anderen Risiken, mit denen eine Firma konfrontiert ist, letztlich in der Verantwortung der Geschäftsleitung liegen. Etwas überrascht hat jedoch die Tatsache, dass nur knapp acht Prozent der Umfrageteilnehmenden bei der Funktion Informationssicherheitsbeauftragter, Chief Information Security Officer (CISO) oder eine vergleichbare Funktion angegeben haben. Dies deutet darauf hin, dass eher wenige der teilnehmenden Firmen diese Rolle überhaupt besetzt haben.

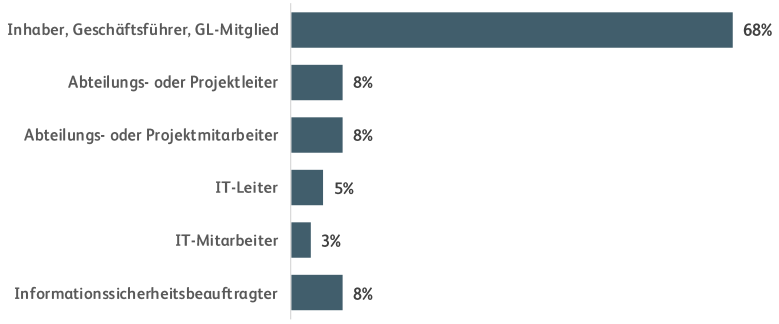

Abbildung 4: Funktion

Bedrohungslage und Verletzlichkeit

Motivation für Informationssicherheit

Vor den Fragen zur Bedrohungslage und Verletzlichkeit wurden die Teilnehmenden der Umfrage nach der Motivation ihrer Unternehmung gefragt, sich mit dem Thema Informationssicherheit zu beschäftigen. Es war zu erwarten, dass die Sicherstellung des Geschäftsbetriebs und der Geschäftserfolg die Haupttreiber für die Auseinandersetzung mit dem Thema sind. Fragen nach der Compliance sind zwar auch wichtig, belegen aber mit einigem Abstand nur den dritten Platz.

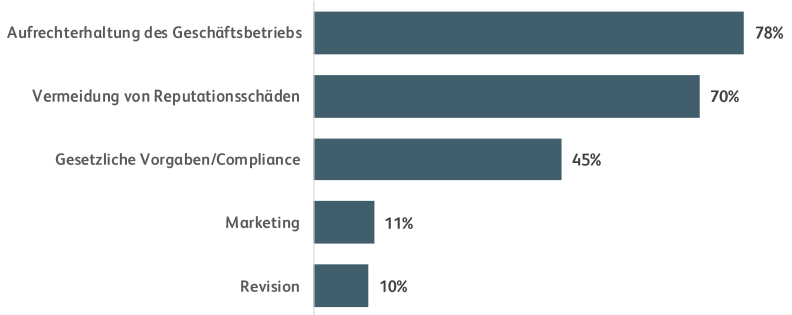

Abbildung 5: Was veranlasst Ihre Firma, sich mit dem Thema Informationssicherheit auseinanderzusetzen?

Informationssicherheitsvorfälle

53 Prozent der Unternehmen gaben an, keine Sicherheitsvorfälle in den zwölf Monaten vor der Umfrage gehabt zu haben. Im Umkehrschluss bedeutet dies, dass fast die Hälfte der teilnehmenden Firmen von Sicherheitsvorfällen betroffen waren (mehrheitlich wurden «1 – 5 Vorfälle im vergangenen Jahr» genannt). Böswillige Angriffe von aussen (Malware, Phishing, Denial of Service etc.) machen dabei den grössten Anteil aus. Interessanterweise wurden aber auch technisches oder menschliches Versagen oft erwähnt. Diese Vorfälle bedingen andere, tendenziell einfacher umzusetzende Massnahmen als die kaum vorhersehbaren Angriffe von aussen.

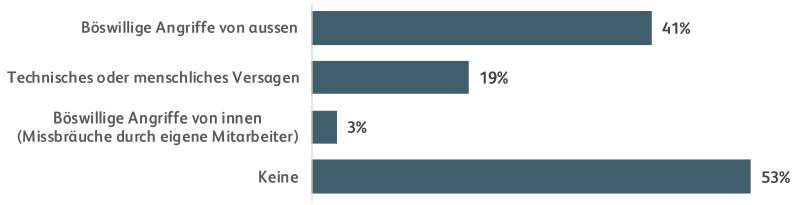

Abbildung 6: Welche Informationssicherheitsvorfälle gab es im vergangenen Jahr in Ihrer Unternehmung?

Beeinträchtigung des Kerngeschäfts

Obwohl unsere Statistik in den Unternehmen ziemlich viele Sicherheitsvorfälle ausweist, blieb die damit verbundene Beeinträchtigung des Kerngeschäfts glücklicherweise mehrheitlich sehr klein, wie die folgende Grafik zeigt:

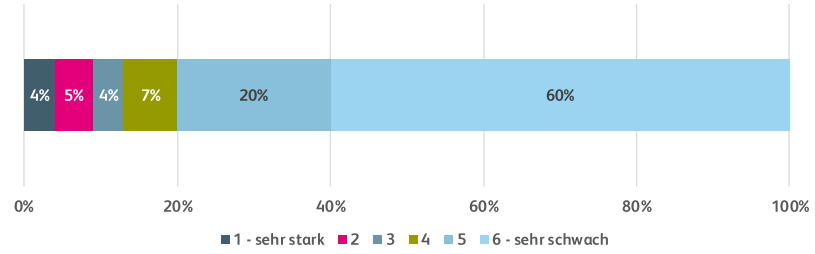

Abbildung 7: Wie beurteilen Sie die Beeinträchtigung Ihres Kerngeschäfts durch die Informationssicherheitsvorfälle im vergangenen Jahr?

Dies liegt daran, dass auch glimpflich abgelaufene Vorfälle, wie beispielsweise ein durch den Virenscanner aufgedeckter Malwarebefall oder eine erkannte Phishing-Mail als Vorfall gewertet wurden.

Der Abschluss des Umfrageteils zum Thema «Bedrohungslage und Verletzlichkeit» setzte sich mit der Einschätzung zukünftiger Bedrohungen der Informationssicherheit auseinander. Grundlage für die Einschätzung bildeten unter anderem Fragen zu den Möglichkeiten, Unternehmensdienste wie beispielsweis E-Mail auf privaten Geräten zu nutzen oder Fragen zum Einsatz von Cloud-Diensten. Beide Aspekte vergrössern die Angriffsfläche einer Unternehmung in sicherheitstechnischer Hinsicht.

Freigeschaltete Unternehmensdienste

Wie zu erwarten, war das geschäftliche E-Mail mit fast 65 Prozent Stimmen der am häufigsten genannte freigeschaltete Unternehmensdienst. Mit knapp halb so vielen Nennungen folgen dahinter Lösungen, die den ganzen Desktop zur Verfügung stellen oder Zugriff auf Netzlaufwerke erlauben (VPN). Überraschend: Fast 17 Prozent der Firmen gaben an, Ihren Mitarbeitenden gar keine Zugriffe auf Unternehmensdienste zu gewähren.

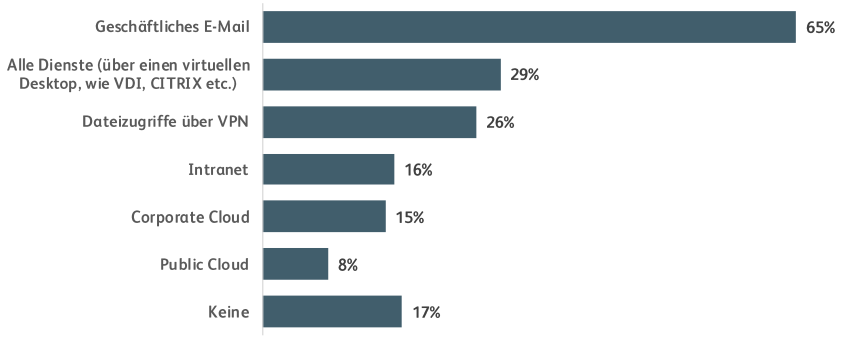

Abbildung 8: Welche Unternehmensdienste können die Mitarbeitenden mit deren privaten Geräten (Smartphone, Tablet, Notebook, Desktop-Computer etc.) nutzen?

Cloud-Dienste

Cloud-Dienste erfreuen sich grosser Beliebtheit. Dies war zu erwarten und widerspiegelt sich darin, dass nur circa 30 Prozent der Firmen angegeben haben, gar keine Services aus der Cloud zu beziehen.

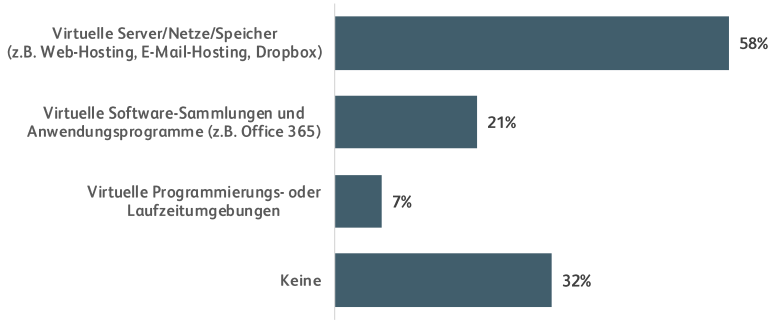

Abbildung 9: Welche Cloud-Dienste nutzt Ihre Unternehmung?

Wert von vertraulichen Informationen

Einen Einfluss auf die Einschätzung zukünftiger Bedrohungen hat auch die Menge und die Art von vertraulichen Informationen, die in einer Unternehmung bearbeitet werden und natürlich die Schäden, die bei deren missbräuchlichen Veröffentlichung entstehen. In diesem Kontext zeigt sich die folgende Situation:

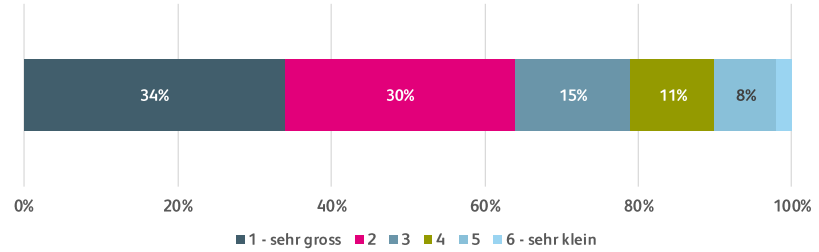

Abbildung 10: Wie beurteilen Sie den Schaden für Ihre Unternehmung bei Veröffentlichung von vertraulichen Informationen Ihres Kerngeschäfts?

Über 60 Prozent der teilnehmenden Unternehmen beurteilen die Schäden, die durch die missbräuchliche Veröffentlichung von vertraulichen Informationen entstehen, als «gross» oder «sehr gross». Dies deutet darauf hin, dass die Geheimhaltung von Informationen in vielen Firmen einen hohen Stellenwert hat.

Einschätzung der zukünftig wichtigsten Bedrohungen

Bei der Einschätzung der zukünftig wichtigsten Bedrohungen der Informationssicherheit zeigt sich das folgende Bild:

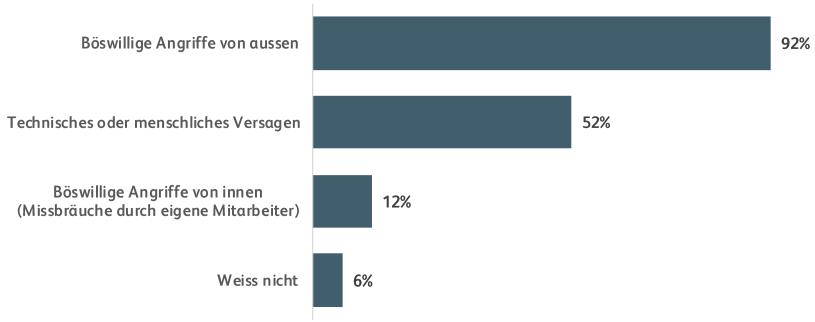

Abbildung 11: Welches sind Ihrer Meinung nach zukünftig die wichtigsten Bedrohungen für die Informationssicherheit Ihrer Unternehmung?

Fast alle teilnehmenden Firmen fühlen sich von böswilligen Angriffe von aussen bedroht. Angriffe von innen scheinen im Gegensatz dazu nur eine untergeordnete Rolle zu spielen.

Governance und Organisation

Der Bereich Governance und Organisation der Informationssicherheit beschäftigt sich mit der Frage, wie die Informationssicherheit in den Unternehmungen gesteuert und kontrolliert wird und welche unterstützenden Organisationsstrukturen vorhanden sind.

Stellenprozente für die Informationssicherheit

Eine zentrale Rolle spielt in diesem Kontext die Frage, wie viele Stellenprozente im Bereich der Informationssicherheit zur Verfügung stehen. Aufgrund des adressierten Firmensegments waren kleine Zahlen zu erwarten. Konkret zeigt sich das folgende Bild:

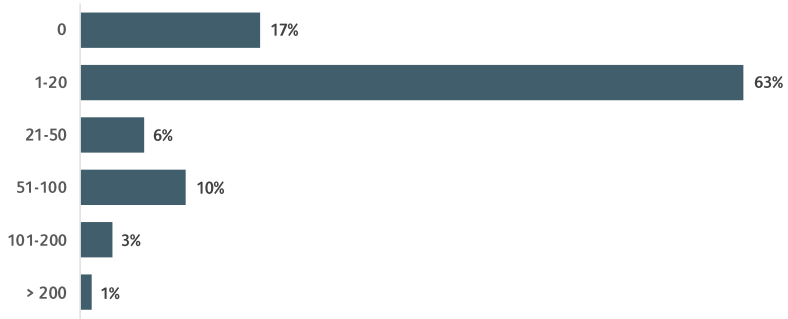

Abbildung 12: Wie viele Stellenprozente stehen in Ihrer Unternehmung für Aufgaben im Bereich der Informationssicherheit zur Verfügung?

Dem grössten Teil der befragten Unternehmungen steht weniger als eine Vollzeitstelle (100 Prozent) für die Betreuung der Informationssicherheit zur Verfügung. 17 Prozent gaben an, für das Thema Informationssicherheit gar keine Ressourcen bereitzustellen.

Informationssicherheitspolitik, Sicherheitskonzepte und Weisungen

Von grossem Interesse sind auch Fragen der Dokumentation der Informationssicherheit. Eine Unternehmung, die Best-Practice-Empfehlungen in diesem Bereich befolgt, sollte über eine Informationssicherheitspolitik[1] verfügen und über zugehörige Sicherheitskonzepte und Weisungen. Gemäss unserer Befragung zeigt sich in diesem Bereich die folgende Situation:

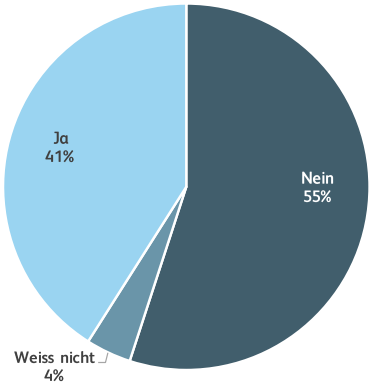

Abbildung 13: Gibt es in Ihrer Unternehmung eine Informationssicherheitspolitik, in der die strategischen Informationssicherheitsziele, die Verantwortlichkeiten und Methoden für die Zielerreichung festgehalten sind?

Immerhin 41 Prozent der Firmen gab an, über eine Informationssicherheitspolitik zu verfügen. Dieser Wert ist ziemlich hoch, vor allem gemessen an der Tatsache, dass die Dotierung der Firmen mit Stellenprozenten für die Informationssicherheit eher klein ist.

Wie zu erwarten war, ist die Verbreitung von Sicherheitskonzepten und Weisungen unter den befragten Firmen grösser als die Verbreitung von Informationssicherheitspolitiken. 56 Prozent deklarierten, sie verfügten über Sicherheitskonzepte und Weisungen. Dies liegt sicherlich daran, dass die unteren beiden Ebenen der so genannten Sicherheitspyramide stärkere Bezüge zu den operativen Tätigkeiten der IT-Abteilungen haben als die Spitze der Pyramide, wo eher strategische und längerfristige Aussagen zur Informationssicherheit gemacht werden.

[1] Strategisches Dokument, das die unternehmerischen Grundsätze der Informationssicherheit definiert.

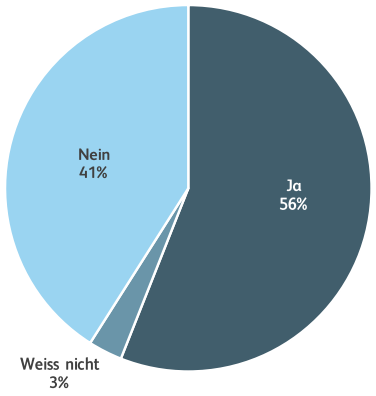

Abbildung 14: Gibt es in Ihrer Unternehmung Konzeptdokumente, Weisungen und/oder Richtlinien, welche die Massnahmen zur Erreichung der Informationssicherheitsziele konkretisieren (z.B. Firewallkonzept, Backupkonzept, IT-Benutzerreglement etc.)?

Risikomanagement

Firmen, die nicht nur Standard-Sicherheitsempfehlungen umsetzen, sondern gezielt, spezifische Schwachstellen in ihrer Infrastruktur und Organisation suchen, bewerten und mitigieren, wenden für diese Aufgaben Instrumente des Risikomanagements an. Der Fragenkatalog enthielt auch eine Frage zu diesem Thema.

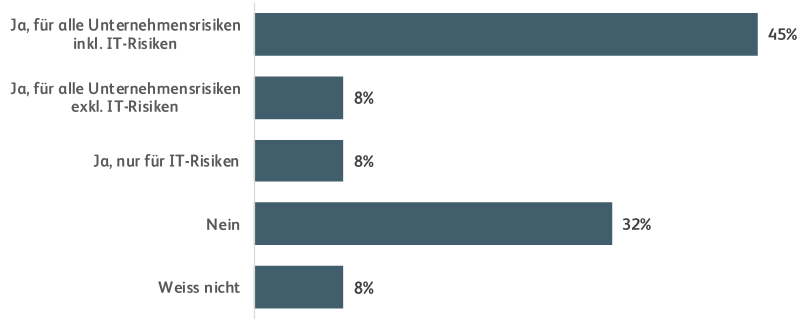

Abbildung 15: Betreiben Sie in Ihrer Unternehmung ein Risikomanagement?

Viele Firmen (45 Prozent), die Unternehmensrisiken erheben, beziehen gemäss Umfrage IT-Risiken mit ein. Allerdings betreibt fast ein Drittel aller Unternehmungen gar kein Risikomanagement, was angesichts der grundsätzlichen Wichtigkeit dieses Instruments sehr überrascht.

Informationssicherheitsstandards

Eine weitere interessante Frage im Kontext Governance und Organisation betrifft Standards und Leitfäden, die zur Unterstützung des Informationssicherheitsprozesses verwendet werden. Vor dem Hintergrund des untersuchten Firmensegments ist es nicht verwunderlich, dass Leitfäden wie das Sicherheitshandbuch

für die Praxis[2] oder das Grundschutzhandbuch vom BSI[3] beliebter sind als Informationssicherheitsstandards (beispielsweise von der ISO[4] oder auch vom BSI), die Vorgaben für ein so genanntes Informationssicherheitsmanagementsystem (ISMS) machen. Dies liegt wohl daran, dass Managementsysteme in der Anwendung ziemlich aufwändig und kompliziert sind.

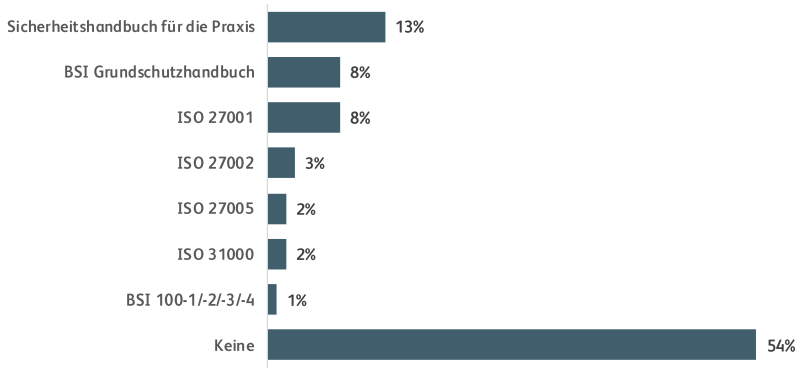

Abbildung 16: Welche Informationssicherheitsstandards berücksichtigen Sie bei der Umsetzung der Informationssicherheit in Ihrer Unternehmung?

Informationssicherheitsmanagementsystem (ISMS)

Das Ergebnis der vorangehenden Frage lässt sich direkt mit den Antworten zur nächsten Frage korrelieren, bei der nach der Existenz eines ISMS gefragt wurde. Gerade mal neun Prozent der Firmen gaben an, ein solches Managementsystem zu betreiben.

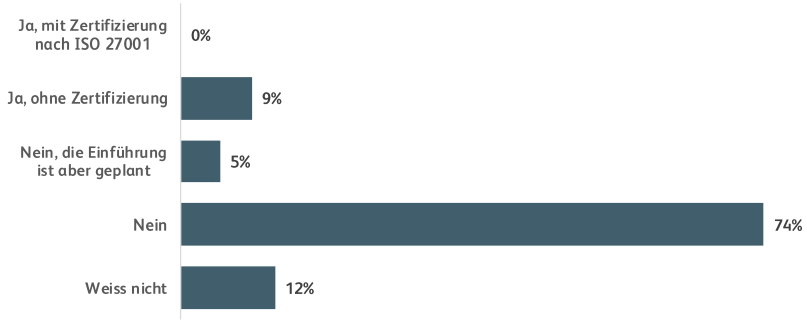

Abbildung 17: Betreiben Sie in Ihrer Unternehmung ein Informationssicherheitsmanagementsystem (ISMS)?

Prüfung von Sicherheitsmassnahmen

Das Fehlen eines Managementsystems für die Informationssicherheit dürfte zumindest bis zu einem gewissen Grad erklären, warum über 50 Prozent der Unternehmungen Informationssicherheitsmassnahmen nur unregelmässig auf ihre Wirksamkeit überprüft, wie die untenstehende Grafik zeigt. Immerhin 17 Prozent der Firmen überprüfen die Massnahmen jährlich.

[2] www.sihb.ch
[3] Bundesamt für Sicherheit in der Informationstechnik, www.bsi.bund.de
[4] International Organization for Standardization, www.iso.org

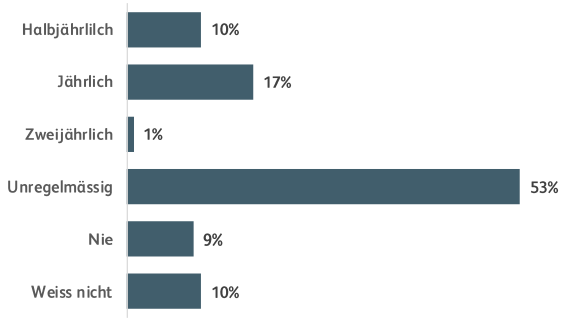

Abbildung 18: Prüfen Sie die Wirksamkeit von implementierten Informationssicherheitsmassnahmen in regelmässigen Abständen?

Awarenessmassnahmen

Die Mitarbeitenden sind bei der Umsetzung von Sicherheitsmassnahmen ein äusserst wichtiger Faktor. Ohne deren Unterstützung lässt sich kein ausreichendes Sicherheitsniveau erreichen. Awareness, das heisst Bewusstseinsbildung für Fragen der Informationssicherheit, ist deshalb ein ganz wichtiger Aspekt im Schulungsprogramm einer jeden Unternehmung. Trotzdem waren über 60 Prozent der befragen Firmen in den zwölf Monaten vor der Umfrage in diesem Bereich gar nicht aktiv.

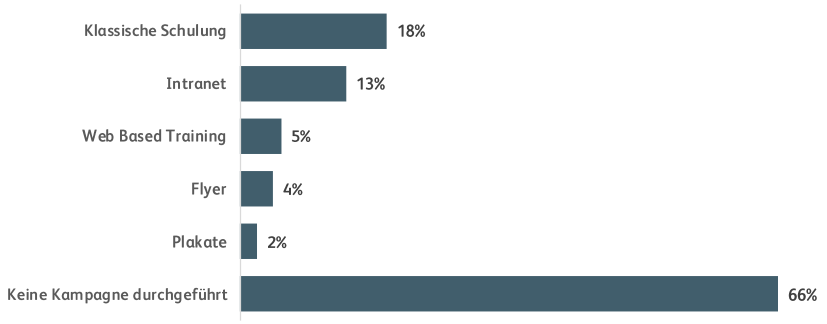

Abbildung 19: Haben Sie im vergangenen Jahr eine Awarenesskampagne zum Thema Informationssicherheit durchgeführt? Falls ja, welches waren die Kernelemente der Informationsvermittlung?

Akzeptanz von Sicherheitsmassnahmen

In direktem Zusammenhang zur Awareness steht die Frage nach der Akzeptanz von Sicherheitsmassnahmen bei den Mitarbeitenden. Die Umfrage hat auch diesen Aspekt beleuchtet und dabei ein erfreuliches Ergebnis gezeigt. Immerhin 21 respektive 34 Prozent der Unternehmungen gab an, dass die Akzeptanz ihrer Sicherheitsmassnahmen bei den Mitarbeitenden «sehr hoch» oder «hoch» sei. 29 Prozent bewerteten die Akzeptanz noch mit «genügend».

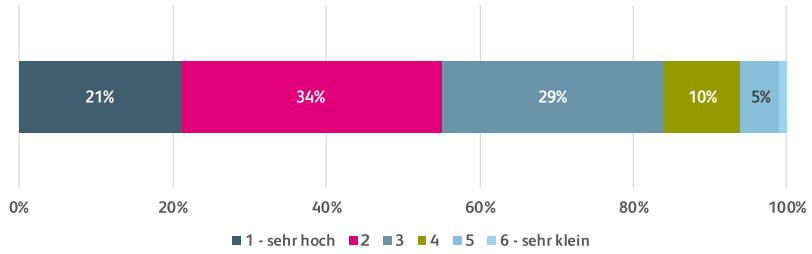

Abbildung 20: Wie beurteilen Sie die Akzeptanz von Sicherheitsmassnahmen bei Ihren Mitarbeitenden?

Weiterbildung

Der letzte untersuchte Aspekt im Zusammenhang mit den Mitarbeitenden betrifft deren spezifische Weiterbildung im Bereich der Informationssicherheit. Wie die folgende Abbildung zeigt, besuchen nur wenige Informationssicherheitsverantwortliche Weiterbildungen mit Fokus Informationssicherheit. Am Beliebtesten sind kurze Fachkurse. Die von den Fachhochschulen und Hochschulen angebotenen CAS- und MAS-Lehrgänge finden im befragten Firmensegment eher wenig Beachtung, genauso wie die Zertifikatsabschlüsse, die von internationalen Organisationen wie ISACA[5] oder (ISC)2[6] angeboten werden.

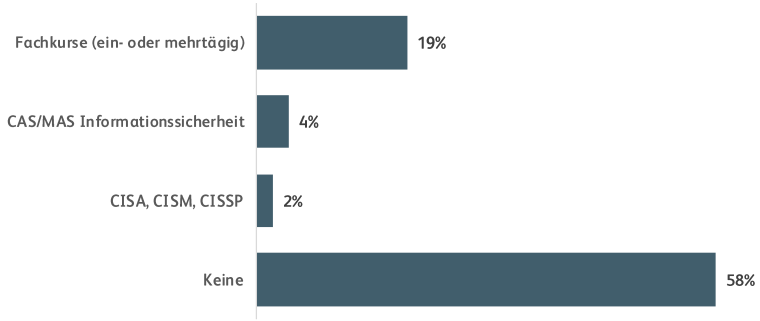

Abbildung 21: Welche Weiterbildungen haben die für die Informationssicherheit verantwortlichen Mitarbeitenden Ihrer Unternehmung besucht?

Sicherheitsmassnahmen

Die klassischen Sicherheitsmassnahmen zum Schutz von Informationen sind auf der technischen Ebene angesiedelt – gemeint sind Virenschutzprogramme, Firewalls, Verschlüsselungslösungen und so weiter. Letztendlich müssen aber die technischen und die im letzten Kapitel beschriebenen organisatorischen Sicherheitsmassnahmen Hand in Hand arbeiten – das eine nützt wenig ohne das andere.

Zu den Top vier technischen Schutzmassnahmen, welche aktuell bei den Teilnehmenden der Umfrage im Einsatz sind, gehören «Backup», «Antivirus-Software», «Firewall» und «Updates». Dies ist insofern erfreulich und nicht verwunderlich, weil dies beispielsweise auch die vier technischen Massnahmen der «5 Schritte für Ihre Computersicherheit» des Web-Portals «eBanking – aber sicher!» sind.

[5] www.isaca.org
[6] Genauer (ISC)2, www.isc2.org

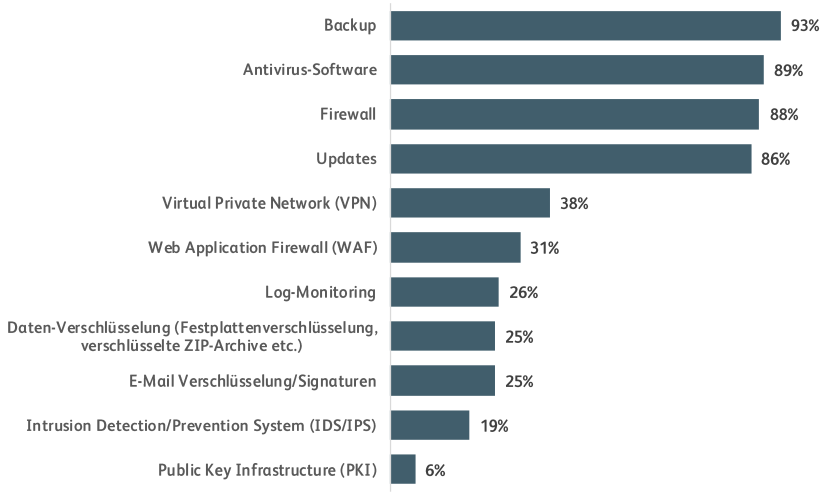

Abbildung 22: Welche technischen Massnahmen werden in Ihrer Unternehmung zum Schutz von Informationen und Systemen eingesetzt?

Rund ein Viertel aller Unternehmungen setzt für die Sicherstellung der Vertraulichkeit und für den Datenschutz auf Verschlüsselungstechnologien – sei dies zur Datenverschlüsselung auf Speichersystemen oder zur E-Mail-Verschlüsselung bei der vertraulichen Kommunikation.

Datenklassifizierung

Datenklassifizierung bildet die Grundlage für die korrekte Handhabung von Daten und ist somit essentiell für den Schutz der Vertraulichkeit von Informationen und für die Einhaltung von Compliance-Anforderungen. Knapp die Hälfte der teilnehmenden Unternehmen klassifiziert ihre Daten. Dabei kommen bei einer Mehrheit der Firmen die drei Stufen «Vertraulich», «Intern» und «Öffentlich» zum Einsatz.

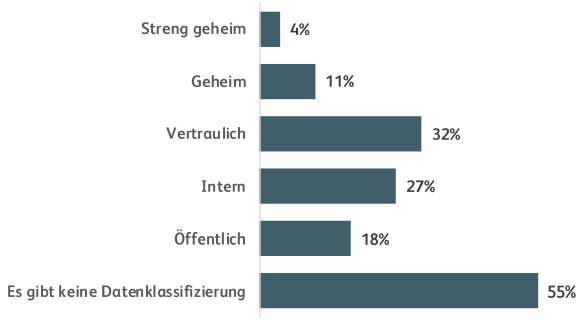

Abbildung 23: Haben Sie in Ihrer Unternehmung eine Datenklassifizierung eingeführt? Wenn ja, mit welchen Stufen?

Umsetzung der Informationssicherheit

Die Umsetzung der Informationssicherheit stellt einerseits einen personellen Aufwand dar und verursacht andererseits Kosten. Erstaunlicherweise sind nicht etwa fehlende finanzielle Ressourcen das Top-Hindernis bei der Umsetzung der Informationssicherheit, sondern das fehlende Know-how (34 Prozent) und fehlende personelle Ressourcen (29 Prozent). Die fehlenden finanziellen Ressourcen kommen erst an dritter Stelle vor dem fehlenden Bewusstsein für Informationssicherheit bei Mitarbeitenden und in der Geschäfts-

leitung. Erfreulicherweise gibt jedes dritte Unternehmen an, dass es bei der Umsetzung der Informationssicherheit keine Hindernisse gibt.

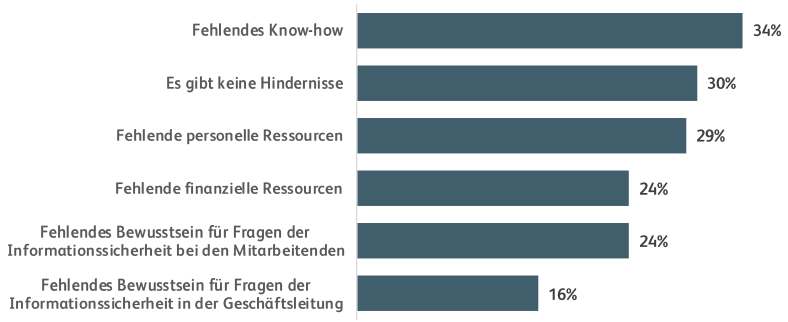

Abbildung 24: Welche Hindernisse gibt es in Ihrer Unternehmung bei der Umsetzung der Informationssicherheit?

Die konkrete Umsetzung von Sicherheitsmassnahmen hat sehr oft auch direkte Auswirkungen auf den Geschäftsbetrieb und ist damit für die Mitarbeitenden direkt spürbar. Sei es, weil ein Prozess anders, d.h. sicherer, abgewickelt oder ein zusätzlicher Prozessschritt für die Sicherheit eingeführt werden muss. Wichtig ist dabei immer, eine gute Balance zwischen Sicherheit und Benutzerfreundlichkeit zu finden, damit die betroffenen Mitarbeitenden bei ihren Tätigkeiten durch die Sicherheitsmassnahmen nicht oder nur marginal eingeschränkt werden.

Die Erfahrungen der Autoren zeigen, dass Massnahmen für die Informationssicherheit bei den Mitarbeitenden sehr oft keine Begeisterungsstürme auslösen. Umso erstaunlicher ist es, dass die Akzeptanz von Sicherheitsmassnahmen bei Mitarbeitenden der teilnehmenden Firmen ziemlich hoch ist. 55 Prozent bewerten die Akzeptanz als «hoch» oder gar «sehr hoch», also deutlich im positiven Bereich.

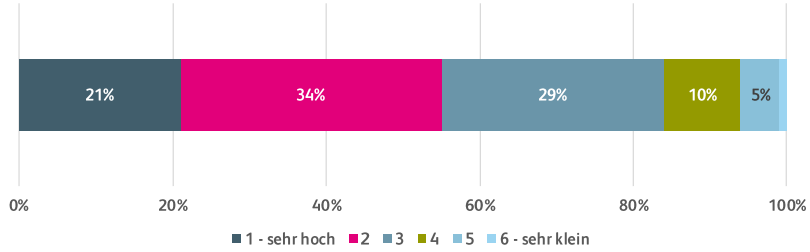

Abbildung 25: Wie beurteilen Sie die Akzeptanz von Sicherheitsmassnahmen bei Ihren Mitarbeitenden?

Spezialthema «E-Banking»

Die elektronische Abwicklung von Finanztransaktionen ist auch bei den KMU äusserst beliebt. Bankgeschäfte zu jeder Zeit und an jedem Ort zu erledigen, ist sehr praktisch. Über zwei Drittel der teilnehmenden Firmen machen dies gleich wie Privatpersonen, nämlich mithilfe des Webbrowsers über den E-Banking Zugang ihres Finanzinstitutes. Ebenfalls eine grosse Mehrheit (65 Prozent) verwendet entweder ein Buchhaltungsprogramm oder eine E-Banking-Software wie z.B. Paymaker, welche die Zahlungen direkt via DTA-Filetransfer zur Bank überträgt.

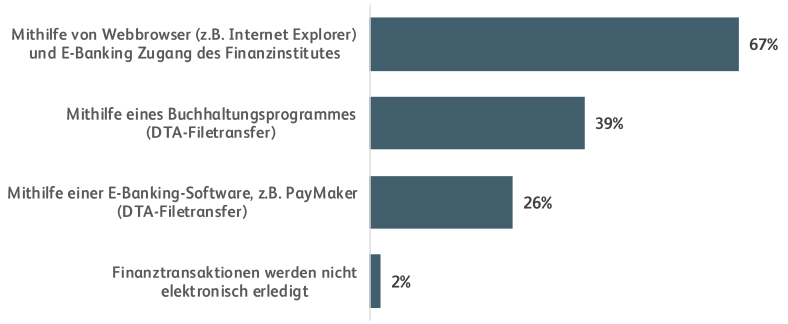

Abbildung 26: Auf welche Art und Weise werden in Ihrer Unternehmung Finanztransaktionen (z.B. Zahlungen) ausgeführt?

Lediglich zwei Prozent der Firmen wickeln ihre Finanztransaktionen nicht elektronisch ab. Über die Hälfte, nämlich 60 Prozent, begründen dies mit Sicherheitsbedenken.

Hier setzt «eBanking – aber sicher!»[7] an. Dieses Web-Portal der Hochschule Luzern – Informatik ist eine unabhängige Plattform, die sowohl Privatkunden der Finanzinstitute als auch KMU dabei unterstützt, die IT-Infrastruktur sicher zu betreiben und dadurch Finanztransaktionen sicher elektronisch abzuwickeln.

[7] https://www.ebas.ch

Fazit / Ausblick

Die Umfrage bestätigt, dass auch die Schweizer KMU für Cyber-Kriminelle lohnenswerte Ziele sind. Schliesslich hüten auch sie ihre «golden Eggs», Geschäftsgeheimnisse also, die für Kriminelle äusserst interessant sein können. Hinzu kommt, dass die Angriffsfläche der KMU durch den Einsatz moderner Technologien wie Remote-Desktops oder Cloud-Anbindungen grösser wird, was ohne geeignete Schutzmassnahmen erfolgreiche Angriffe wahrscheinlicher werden lässt. Nicht zu vergessen sind schliesslich die immer raffinierteren Social-Engineering-Techniken, mit denen Angreifer Zugang zu Systemen zu erschleichen versuchen.

Bei den Schutzmassnahmen haben viele KMU vor allem im Bereich der Governance und Organisation noch Nachholbedarf. Bei den technischen Massnahmen sieht es erwartungsgemäss besser aus. Eine gesamtheitliche Verbesserung der Situation in den KMU setzt voraus, dass die Firmen einerseits mehr Personal für die Informationssicherheit bereitstellen und die betreffenden Mitarbeitenden besser schulen. Bei der Weiterbildung kann die Hochschule Luzern – Informatik mit ihren CAS-Programmen und Fachkursen im Bereich Informationssicherheit einen wertvollen Beitrag leisten. Auch die vom Departement bereitgestellte Dienstleistung «eBanking – aber sicher!» trägt viel zur Verbesserung der Informationssicherheit bei Privatpersonen und vielen KMU bei.

Literaturverzeichnis

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2008). *BSI-Standard 100-1: Managementsysteme für Informationssicherheit*. Bonn: BSI.

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2008). *BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise*. Bonn: BSI.

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2008). *BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz*. Bonn: BSI.

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2008). *BSI-Standard 100-4: Notfallmanagement*. Bonn: BSI.

Bundesamt für Sicherheit in der Informationstechnik (BSI). (10. Oktober 2016). *Cyber-Sicherheits-Umfrage 2016*. Von Allianz für Cyber-Sicherheit: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Micro/UmfrageCS/umfrageCS.html abgerufen

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2016). *IT-Grundschutzkatalog 15. Ergänzungslieferung - 2016*. Bonn: BSI.

EY. (2014). *Get ahead of cybercrime, EY's Global Information Security Survey 2014*. EYGM Limited.

Hochschule Luzern - Informatik. (20. September 2017). *«eBanking – aber sicher!»*. Von https://www.ebas.ch abgerufen

International Organization for Standardization. (2014). *DIN ISO/IEC 27001, Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Managementsysteme - Anforderungen*.

International Organization for Standardization. (2015). *DIN ISO/IEC 27002, Informationstechnik - IT-Sicherheitsverfahren - Leitfaden für das Informationssicherheits-management*.

International Organization for Standardization. (2016). *DIN ISO/IEC 27000, Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Managementsysteme - Überblick und Terminologie*.

Melde- und Analysestelle Informationssicherung MELANI. (20. September 2017). *Lageberichte*. Von Schweizerische Eidgenossenschaft, MELANI: https://www.melani.admin.ch/melani/de/home/dokumentation/berichte/lageberichte.html abgerufen

National Institute of Standards and Technology. (2014). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0*.

National Institute of Standards and Technology. (2017). *Framework for Improving Critical Infrastructure Cybersecurity, Draft Version 1.1*.

PricewaterhouseCoopers LLP. (2014). *Managing cyber risks in an interconnected world, Key findings from The Global State of Information Security® Survey 2015*.

Reisinger, P. (2015). *Informationssicherheit in Deutschland, Österreich und der Schweiz 2015*. St. Pölten: Fachhochschule St. Pölten.

Rieder, C., & Hirschi, O. (2015). *Informationssicherheitshandbuch für die Praxis*. Altdorf: Gisler Druck AG.

Zurich Insurance Company Ltd. (2016). *Mögliche Auswirkungen von Cyberkriminalität auf das Geschäft von kleinen und mittleren Unternehmen (KMU) im Jahr 2016, Umfragebericht für Schweiz*.