Bezahlbare Überprüfung der digitalen Sicherheit von KMU

Evaluation effizienter Methoden und Vorgehensweisen

Zertifikatsarbeit im
CAS Digital Risk Management

Zürcher Fachhochschule
HWZ Hochschule für Wirtschaft Zürich

eingereicht bei:
Ralph Hutter, Leiter CAS Digital Risk Management
Manuel P. Nappo, Leiter MAS Digital Business

vorgelegt von:
Christian Heimann, Lerbermattstrasse 3, 3084 Wabern

Bern, 29. Juni 2018

Management Summary

KMU sind sich dem digitalen Wandel sehr bewusst. Für zwei Drittel der kleinen KMU hat IT-Sicherheit eine hohe Bedeutung – aber nur 20% haben ihre IT-Sicherheit bisher überprüft.

Die menschliche Komponente gewinnt in der digitalen Sicherheit immer mehr an Bedeutung – die Unternehmen kümmern sich aber bis heute hauptsächlich um die technischen Aspekte.

Für IT-Sicherheit steht derzeit erst ein kleiner Teil der Budgets bereit; auch wenn CISOs gerne mehr Mittel hätten. Besorgniserregend ist, dass ein Teil der Unternehmen gar keine Ausgaben für IT-Sicherheit plant. Dass nichts unternommen wird, liegt zum Teil auch an der Vielzahl der am Markt angebotenen technischen IT-Sicherheitsmassnahmen: diese überfordern kleine Unternehmen.

Risk Management in KMU wird oft vom Fachmann eines jeweiligen Bereiches betrieben. Das ist gut, aber ein dedizierter Risk Manager sollte die Gesamtübersicht haben und zwischen den Bereichen abstimmen. Kleine Unternehmen setzen dafür zurecht oft auf externe Dienstleister.

Es stehen verschiedene Mittel zur Überprüfung der digitalen Sicherheit zur Verfügung: Risiko-Analyse, Inventarisierung, Security-Audit, Automated Testing, Penetration Test, Social Engineering Audit. Als Ideengeber stehen Quellen mit frei verfügbaren und wertvollen Informationen bereit, z.B. MELANI, aber auch existierende Rahmenwerke wie ISO-27001 können die richtigen Fragen zur Sicherheitsüberprüfung liefern.

Das beschriebene Szenario «Coiffeur-Salon», in dem Erreichbarkeit und Kundendaten die wichtigsten Assets sind, zeigt, dass mit einem guten Inventar, besonders mit einer guten Übersicht von Zugriffsrechten, bereits viel erreicht werden kann. Das Szenario «Metallbauer» steht für ein Unternehmen mit speziellem Technologie-Know-How, einer dynamischen Systemlandschaft mit IoT und einer grösseren Mitarbeiter-Zahl. Hier kommt das Unternehmen nicht um einen externen Security-Auditor herum; ein gutes Inventar gehört aber auch hier zur Basis-Voraussetzung. Und die Mitarbeiter müssen entsprechend in «digitaler Sicherheit» geschult und trainiert werden.

Abschliessend wird mit dem «Quick Security Measure Test» ein Prototyp eines einfachen Evaluations-Instrumentes vorgestellt, mit welchem jeder Betrieb in Kürze weiss, welche Mittel zur Überprüfung der digitalen Sicherheit gewählt werden sollten. Dieses Hilfsmittel steht allen Unternehmen online unter qsmt.chrissharkman.ch zur Verfügung.

Inhaltsverzeichnis

Management Summary II

Ehrenwörtliche Erklärung V

1. Einleitung 1

1.1. «100 prozentige Sicherheit gibt es sowieso nicht!» 1
1.2. Zielsetzung 1

2. Zustand der digitalen Sicherheit in KMU 2

2.1. KMU und digitale Transformation 2
2.1.1. «Digital» ist omnipräsent 2
2.1.2. Digitale Geschäftsmodelle und Vernetzung 2
2.1.3. Bewusstsein für die digitale Sicherheit 3
2.2. Investitionen in die digitale Sicherheit 4
2.2.1. IT-Kosten 4
2.2.2. Ausgaben für IT-Sicherheit 5
2.2.3. Kosten-Planung und -Verantwortung 5
2.3. Wer und wo sind die Digital Risk Manager und IT-Sicherheitsbeauftragten? 6
2.3.1. Aufgaben eines Sicherheitsbeauftragten 6
2.3.2. Engagement von externen Dienstleistern 6
2.3.3. Job-Markt 7

3. Mittel zur Überprüfung der digitalen Sicherheit 7

3.1. Übersicht «Security Assessment» 7
3.2. Digitales Inventar klären 8
3.2.1. Karte der technischen Umgebung 8
3.2.2. Rechteverwaltung und Zugriffsschutz 8
3.2.3. Security Service Level Agreements 9
3.3. Risikoanalyse mit Fokus auf Informations- und IT-Sicherheit 9
3.3.1. Risikoappetit definieren 9
3.3.2. Aspekte der Risikoanalyse 9
3.3.3. Statistiken vs. Erfahrung 10
3.4. Security Audit 11
3.4.1. Ablauf 11
3.4.2. Anbieterwahl 11

3.5. Automated Testing 12
3.5.1. Wie und was kann automatisch getestet werden? 12
3.5.2. Vorteile durch Regelmässigkeit und Automatisation. 13

3.6. Penetration Test 13

3.7. Audit mit Social Engineering 14
3.7.1. Awareness schaffen!. 14
3.7.2. Herausforderungen und Vorteile von KMU 14

3.8. Ideenbringer für eine Grundsicherheit 14
3.8.1. Das Beste aus Frameworks ziehen 14
3.8.2. Wertvolle Informationen von MELANI 15

4. Szenarien 15

4.1. Klein-Unternehmen, keine eigene Server-Infrastruktur 15
4.1.1. Szenario «Coiffeur-Salon». 15
4.1.2. Empfohlene Mittel 16
4.1.3. Kosten 17

4.2. Mittleres Unternehmen 17
4.2.1. Szenario «Metallbauer». 17
4.2.2. Empfohlene Mittel 17
4.2.3. Kosten 18

5. Quick Security Measure Test 19

5.1. Konzept 19
5.2. Umsetzung des Prototyps 19

6. Fazit / Empfehlungen 20

6.1. Ein Plädoyer für Übersicht 20
6.2. Wertvolle Eigenleistungen 20

Quellenverzeichnis 21

Abbildungsverzeichnis 22

Ehrenwörtliche Erklärung

Hiermit erkläre ich, die vorliegende Arbeit selbstständig und nur unter Benutzung der angegebenen Hilfsmittel und Literatur verfasst zu haben.

Bern, 29. Juni 2018

Christian Heimann

1. Einleitung

1.1. «100 prozentige Sicherheit gibt es sowieso nicht!»

Der Satz «100 prozentige Sicherheit gibt es sowieso nicht, da brauche ich mich gar nicht erst anzustrengen!» ist pure Resignation vor der digitalen Umwelt. Gerade in technologie-entfernteren Gewerben ist die Computertechnik oft mehr Feind als Freund, auch wenn selbst dort bereits wichtige Prozesse über digitale Wege bearbeitet werden. Viele KMU wissen gar nicht, wie es überhaupt um ihre «digitale Sicherheit» steht.

Der Frage, wie man Sicherheit kostengünstig überprüfen kann, geht diese Arbeit nach. Nicht nur Grossbetriebe, sondern auch kleine und mittlere Unternehmen sollten sich die Überprüfung leisten. Die Ressourcen müssen im KMU-Umfeld stets effizient eingesetzt werden. Da stellen sich schnell die Fragen: Was kann automatisiert ablaufen? Wo kann Eigenleistung erbracht werden?

1.2. Zielsetzung

Für das Grossziel, die KMU in der Schweiz «digital sicher» zu machen, soll diese Arbeit ihren Beitrag leisten. Zum einen als Nachschlagewerk über Vorgehen und mögliche Mittel zur Überprüfung von Sicherheit. Zum anderen um mit Hilfe der beschriebenen Szenarien einem technischen Laien eine Vorstellung zu geben, wann diese Mittel in einer Praxissituation anzuwenden wären – und mit welchen Kosten zu rechnen ist.

Mit dem Prototyp eines Schnell-Evaluations-Tests soll der erste Schritt in Richtung digitale Sicherheitsüberprüfung vereinfacht werden. Tipps zu Quellen von freien Inhalten liefern zusätzlich Material, um sich ohne externe Beratung (und dadurch entstehende Kosten) erste, wichtige Fragen zu stellen.

Letztendlich soll die Arbeit die Eingangs erwähnte Vorstellung abbauen, man könne als kleiner Betrieb ja «sowieso nichts machen» für die digitale Sicherheit. Damit wäre Bewusstsein geschaffen – ein erster wichtiger Gewinn für die Sicherheit.

2. Zustand der digitalen Sicherheit in KMU

2.1. KMU und digitale Transformation

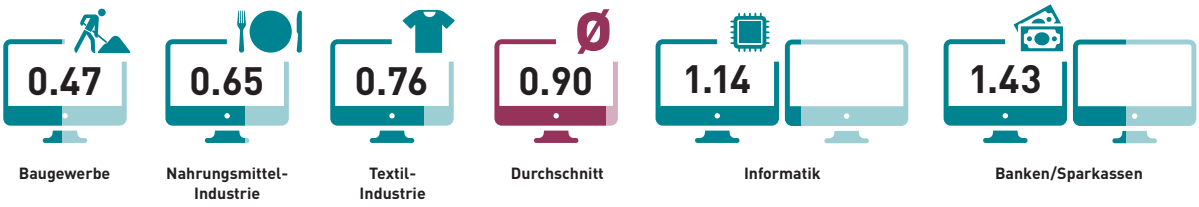
2.1.1. «Digital» ist omnipräsent

Digitalisierung und digitale Risiken sind im Jahr 2018 endgültig in den Massenmedien und im Bewusstsein der breiten Bevölkerung angekommen. In Unternehmen geht es zu diesem Zeitpunkt darum, den Anschluss nicht zu verlieren. 78% der Unternehmen in der Schweiz gehen davon aus, dass die digitale Transformation grosse bis sehr grosse Auswirkungen auf das eigene Unternehmen hat. (Digital Switzerland, 2016)

Für Unternehmen ist es verlockend, grosse Schlagwörter wie «Cloud», «Internet of Things», oder «Big Data» zu verwenden um gut da zu stehen. Die Studie von Digital Switzerland (2017) zeigt aber, dass betreffend digitaler Transformation das fehlende Fachwissen von Mitarbeitenden eine der grössten Herausforderungen darstellt.

Ein Aspekt der digitalen Transformation sind die Computer und Systeme, welche Unternehmensprozesse unterstützen und direkt von Mitarbeitenden bedient werden. Dieser Aspekt ist bereits stark fortgeschritten: Wer beim Gedanken an PCs in der Unternehmenswelt nur an Administrations-Büros und IT-Firmen denkt, hat weit gefehlt. Selbst in IT-fernen Branchen war die Quote von PCs pro Mitarbeiter bereits 2015 sehr hoch, und darin sind im Hintergrund laufende Rechner und Systeme nicht miteingerechnet:

fig. 1 – PCs pro Mitarbeiter



Quelle: Profondia (2016)

2.1.2. Digitale Geschäftsmodelle und Vernetzung

Business-Prozesse werden digital, Schnittstellen werden geschaffen und Kunden werden vermehrt in den Arbeitsprozess miteinbezogen: Durch den Einsatz von digitalen Mitteln entstehen neue Felder und Möglichkeiten, welche sich KMU zunutze machen können.

Die unter dem Titel «Industrie 4.0» geforderte Vernetzung von Systemen, Maschinen und Daten verschiedenster Herkunft verspricht, dass die Übersicht über Kanäle, Komponenten, Mitspieler und Möglichkeiten noch schwieriger werden wird. Um in dieser komplexen Landschaft eine Grund-Sicherheit für alle garantieren zu können, ist der Ansatz «Security by Design» wichtig.

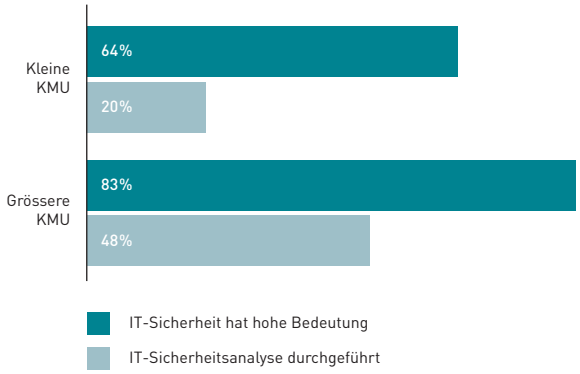
«Sicherheit» soll nicht als blosser Zusatz eines Systems behandelt werden, sondern von Anfang an in den Entwicklungsprozess miteinbezogen sein.

Gerade im exponentiell wachsenden IoT-Bereich ist der Ansatz von «Security by Design» wichtig. Denn gemäss der führenden Forschungs- und Beratungsfirma Gartner (2017) wird die Zahl der IoT-Geräte bis 2020 auf 20'000'000'000 steigen. Und IoT-Geräte sind nicht nur Angriffsziel, sondern können auch selbst zum Angreifer werden (z.B. Missbrauch als Teil eines Botnets). Darum geht es beim Schutz von solchen Elementen in einem System nicht nur um die eigene Sicherheit, sondern auch direkt um die Sicherheit der Allgemeinheit. Gartner geht weiter davon aus, dass 2020 25% aller identifizierbaren Cyber-Angriffe auf Unternehmen eine IoT-Komponente aufweisen, aber weniger als 10% der IT-Sicherheits-Budgets in IoT investiert wird.

2.1.3. Bewusstsein für die digitale Sicherheit

Eine Studie aus Deutschland vom WIK (2017) liefert wertvolle Fakten zum Bewusstsein punkto digitale Sicherheit. Die Erkenntnisse dürften in den Grundzügen mit der Situation von KMU in der Schweiz vergleichbar sein.

fig. 2 – Bedeutung von IT-Sicherheit



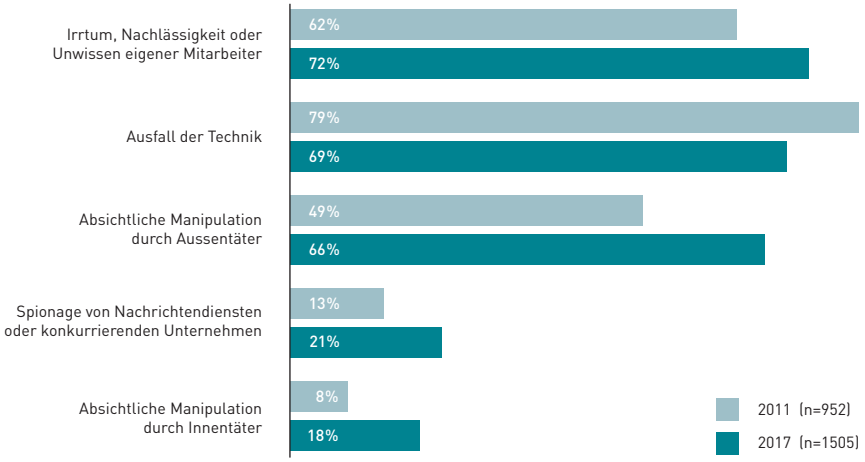
Quelle: WIK (2017, S. 44)

Diese Studie zeigt, dass die Bedeutung der IT-Sicherheit in gut zwei Dritteln der kleinen Unternehmen eine hohe Bedeutung hat. Bei den grösseren KMU sind es sogar 83%, welche der IT-Sicherheit eine hohe Bedeutung zuweisen. Der Unterschied zu den relativ tiefen Zahlen von Betrieben, welche bereits eine IT-Sicherheitsanalyse durchgeführt haben, lässt sich mit einer generellen Unsicherheit zu Risiken und Lösungen erklären.

Die Einschätzung des Schutzbedarfs hat in den letzten Jahren zugenommen. «Die in den letzten Jahren prominent gewordenen Fälle von Datenleaks sowie von Schadprogrammen wie z.B. Verschlüsselungstrojanern haben zu einem gesteigerten Bewusstsein der Unternehmen geführt.» (WIK, 2017, S. 45). Die Unternehmen werden sich also bewusst, welchen Wert ihre Daten haben und welche Risiken IT-Sicherheits-Probleme mit sich bringen können. Am schützenswertesten werden Kunden-, Rechnungs- und Personal-Daten angesehen. (WIK, 2017, S. 45).

Bessere Produkte, Security by Design, einfachere Handhabung von Services sowie breiter abgestützten Lösungen sind nur einige der Elemente, welche dafür sorgen, dass die technische Komponente bei der Betrachtung von IT-Sicherheit an Bedeutung verliert. «Menschliches» hingegen gewinnt an Bedeutung, was die Statistik «Ursachen für IT-Probleme im Zeitvergleich» gut aufzeigt:

fig. 3 – Antworten auf die Frage: «Wo sehen Sie die hauptsächlichen Ursachen für mögliche Probleme und Schadensfälle bei der IT?» Entwicklung im Vergleich zwischen 2011 und 2017



Quelle: WIK (2017, S. 49)

Trotzdem fehlt das Bewusstsein für die Dringlichkeit von Schulungen, um die «menschliche» Komponente robuster zu machen. In 47% der kleinen Unternehmen werden Sensibilisierungen der Mitarbeiter gemacht, regelmässige Schulungen zur IT-Sicherheit gibt es nur in 15% der kleinen Unternehmen. Bei grösseren KMU sind die Werte mit 73% (Sensibilisierung) und 29% (IT-Sicherheitsschulungen für Mitarbeiter) etwas besser. (WIK, 2017, S. 54)

KMU setzen öfter technische Massnahmen um (Firewall, Basisschutz, Verschlüsselung, Datensicherung) als organisatorische (Schulungen, Regeln IT-Nutzung).

Im Notfall haben nur knapp ein Drittel der Klein-Unternehmen einen Notfallplan bereit; bei grösseren KMU sind es 71% (WIK, 2017, S. 55). Ein Notfallplan beschreibt die wichtigsten Rollen, Kompetenzen, Vorgehensweisen und Abläufe, um in der Krisensituation keine Zeit mit strukturellen Fragen zu vergeuden.

2.2. Investitionen in die digitale Sicherheit

2.2.1. IT-Kosten

Die HSLU liefert in einer Studie eine Idee, wie hoch die Gesamt-IT-Kosten in Schweizer KMU sind. Mit in diese Kosten fallen Hardware, Software, Unterhalt- und Service-Gebühren, Support-, Schulungs- und Beratungskosten sowie interne Personalkosten.

fig. 4 – Jährliche IT-Kosten nach Unternehmensgrösse (in CHF)

	1 Mitarbeiter	2 – 5 Mitarbeiter	6 – 19 Mitarbeiter	20 – 50 Mitarbeiter	51 – 100 Mitarbeiter
Mittelwert	7500	13333	31923	96000	268000
Median	5000	15000	25000	75000	250000

Quelle: Winiker & Egle (2015)

Im Vergleich zum Umsatz belaufen sich die IT-Kosten zwischen 0,6% und 6,7%, mit markanten Unterschieden zwischen den Branchen und Unternehmensgrössen. (Winiker & Egle, 2015)

Die internen Personalkosten entstehen durch eigene IT-Mitarbeiter. Über die verschiedenen Branchen hinweg standen gemäss IT Markt Report 2016 (Profondia, 2016) in Klein-Unternehmen 1,8, in mittleren Unternehmen 4,5 IT-Mitarbeiter pro Standort zur Verfügung.

2.2.2. Ausgaben für IT-Sicherheit

«Der prozentuale Anteil der Ausgaben für IT-Sicherheit am IT-Budget insgesamt beträgt ca. 11%». Bei deutschen KMU wurden im 2017 mit durchschnittlich 2600 € Investitionen in die IT-Sicherheit gerechnet, in der Regel proportional zur Unternehmensgrösse ansteigend. Sorgen bereiten müssten einem aber ein Drittel der Unternehmen – diese planten 2017 keinerlei Investitionen in IT-Sicherheit. (WIK, 2017)

Konkrete Zahlen für Schweizer KMU zu den Ausgaben für IT-Sicherheit fehlen. Wahrgenommen werden kann aber Folgendes: Im vergangenen Jahrzehnt wuchs das Verständnis, dass IT-Ausgaben ein entscheidender Posten sind – selbst bei IT-fernen Betrieben. Im kommenden Jahrzehnt muss das Verständnis wachsen, dass die IT-Sicherheit nicht kostenlos zu haben ist.

Der Wunsch nach mehr Budget ist weit verbreitet. So möchten 80% der CISO gerne mehr Mittel für IT-Sicherheit (IDG Research Services, 2016). Dies ist verständlich, angesichts stetig wachsender IT-Ausgaben – auch wenn eines der Hauptanliegen die Effizienzsteigerung und mögliche Kosteneinsparungen ist. (Klossek 2015)

Überforderung und Unsicherheit bremsen trotz dem vorhandenen Bewusstsein die Investitionen: «Die Vielzahl der am Markt angebotenen technischen IT-Sicherheitsmassnahmen überfordert viele, insbesondere kleine, Unternehmen. In zahlreichen Expertengesprächen wurde deutlich, dass KMU angesichts von vorhandenen hochspezifischen Lösungen Schwierigkeiten haben, die für sie relevanten Angebote herauszufiltern.» (WIK, 2017)

2.2.3. Kosten-Planung und -Verantwortung

Nur gerade die Hälfte der KMU macht eine Budget-Planung für die IT-Kosten. Von denen machen 56% die Planung über 1 Jahr, 23% über 3 Jahre. (Winiker & Egle, 2015). Dabei ist die Kosten-Planung ein wichtiges Element in für ein sauberes IT-Kostenmanagement.

Bei Kleinunternehmen rapportieren Verantwortliche für Informationssicherheit fast immer direkt dem CEO (93%); im Schnitt sind 48% dem Geschäftsführer unterstellt. Bei rund einem Drittel ist die übergeordnete Stelle die IT-Abteilung. Wenig förderlich für grosszügige Investitionen in die IT-Sicherheit ist Tatsache, dass in 10% der Unternehmen die IT-Sicherheit direkt dem CFO unterstellt ist (IDG Research Services, 2016).

2.3. Wer und wo sind die Digital Risk Manager und IT-Sicherheitsbeauftragten?

2.3.1. Aufgaben eines Sicherheitsbeauftragten

Der Digital Risk Manager bezeichnet die Person, welche sich primär um die digitale und informationstechnische Sicherheit kümmert. «Die vielleicht grösste Herausforderung der Unternehmens-Führung ist das Ändern der Vorstellung, dass digitale Technologie – und die damit verbundenen technologischen Risiken – ein technisches Problem ist und daher von Technikern verwaltet werden muss, irgendwo vergraben in der IT.»[1] (Heather, 2015)

Die zu bearbeitenden Risiken zeigen aber schnell, dass eine strikte Abgrenzung zwischen digitaler, physischer, Informations- und Personen-Sicherheit weder möglich noch sinnvoll ist. Der Digital Risk Manager muss sich auskennen in den folgenden Bereichen:

- Business Continuity Management
- Datenschutz
- Juristische und regulatorische Vorgaben
- Risk Assessments über die kompletten digitalen Geschäftsmodelle
- Finanzen und Budget
- Digitales Marketing und Kundenvertrauen
- Sicherheitsaspekte von Zulieferern

(Heather, 2015)

Dass der Risk Manager alle Risiken genau verstehen und verwalten soll, ist ein Irrglaube. Anstatt eines Risk Managers sollten alle Team-Mitglieder in ihrem Fachbereich den Hut des Risk Managers aufsetzen – denn Sie kennen die effektiven Risiken ihres Bereichs am besten. Der Risk Manager soll aber den Prozess überwachen und auf eine saubere Umsetzung achten. (Hillson, 2015)

Apostolos Tzouvaras hebt in einem Beitrag zum Thema «Is project risk management really waste of time?» dabei einen wichtiges Element hervor: Risiken zu erkennen erfordert Zeit, Ressourcen und ist anstrengend. Die Verantwortlichen müssen sich dazu zwingen, sich zu überlegen, was überhaupt für Risiken möglich sind. «Die Wahrheit ist, es ist schwierig Dinge zu sehen, die Sie noch nie gesehen haben, und es ist schwierig zu wissen, wohin Sie schauen sollten, um diese zu sehen.»[2] (Tzouvaras, 2015)

2.3.2. Engagement von externen Dienstleistern

«Für kleine und mittelständische Unternehmen ist es von Vorteil, einen externen IT-Sicherheitsbeauftragten zu beauftragen. Denn häufig sind die personellen Ressourcen im eigenen Unternehmen nicht ausreichend gegeben. Ausserdem verfügt ein externer IT-Sicherheitsbeauftragter über das nötige Know-How, ist stets auf dem neuesten Stand und kann Sie damit optimal beraten.» (Wies, 2017)

---

1 Originalzitat: «Perhaps the biggest challenge for leadership is to change the common mindset that digital technology — and, therefore, technology-related risk — is a technical problem, handled by technical people, buried in IT.» (Übersetzung durch den Verfasser)

2 Originalzitat: «The truth is that it is difficult to see things you haven't seen before and it is difficult to know where to look for things you haven't seen before » (Übersetzung durch den Verfasser)

Auch wenn dieses Zitat von einem Anbieter ebendieser Dienstleistungen stammt, so gilt unter den IT-Sicherheitsfachleuten der Konsens, dass nebst aktuellem Know-How Vernetzung eine zentrale Komponente zur Erhaltung von IT-Sicherheit darstellt.

Die IDG Research Services (2016) bestätigen, dass diese Empfehlung, Hilfe von externen Dienstleistern in Anspruch zu nehmen, von Unternehmen auch umgesetzt wird: «Der Aufbau und die Pflege der Sicherheitsarchitektur, die externe Security-Überprüfung und die Evaluierung von Security-Lösungen sind die am häufigsten genannten Gebiete einer Zusammenarbeit mit externen Dienstleistern.»

In der gleichen Studie wird auch aufgezeigt, dass in nur 5,3% der kleinen Unternehmen (< 100 Mitarbeiter) eine betriebsinterne IT-Sicherheitsgruppe geführt wird. Diese kann aus einer oder mehreren Personen bestehen und stellt den Kreis von Sicherheits-Verantwortlichen dar. Bei mittelgrossen Unternehmen sind es rund 31%.

2.3.3. Job-Markt

Ein aktueller Blick über verschiedene Job-Online-Portale zeigt ein Bild, dass derzeit nur Grossfirmen (Swatch, BKW), Verwaltungen (Kantone, Bund) und IT-Dienstleister verschiedenster Art (Compass Security, Swisscom, T-Systems) konkrete IT-Sicherheitsverantwortliche suchen oder weitere dedizierte Stellen im Bereich IT-Security ausgeschrieben haben.

3. Mittel zur Überprüfung der digitalen Sicherheit

3.1. Übersicht «Security Assessment»

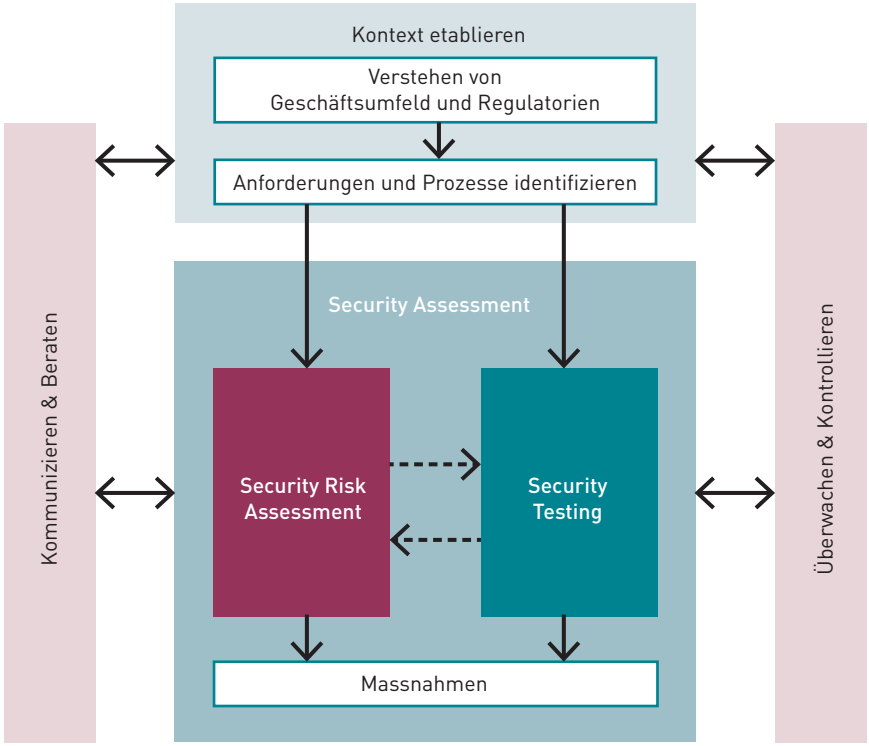
Eine gute digitale Sicherheit sollte das Ziel jedes KMU sein. Es darf nicht sein, dass die in «2.2.2. Ausgaben für IT-Sicherheit» angesprochene Verunsicherung zu Blockaden führt und dadurch Investitionen in die digitale Sicherheit unterlassen werden.

Im Folgenden werden verschiedene Mittel zur Überprüfung der digitalen Sicherheit beleuchtet, um deren Form und Zweck aufzuzeigen.

In dieser Arbeit wird der Begriff «Security Assessment» als umfassenden Begriff über die möglichen Mittel zur Überprüfung der digitalen Sicherheit verwendet. Es beinhaltet die Bereiche «Security Testing», «Security Audit» und «Massnahmen», wobei die Massnahmen aus den Resultaten von Security Testing und Security Audit erarbeitet werden und hier nicht weiter ausgeführt werden. Der Begriff «Assessment» kann mit Einschätzung oder Beurteilung übersetzt werden.

«Security Assessment» stammt aus dem ganzheitlichen Ansatz in der Arbeit über «Combining Security Risk Assessment and Security Testing Based on Standards» von Grossmann & Seehusen (2015). Der Begriff «Security Risk Assessment» umfasst die komplette Risikoanalyse und -behandlung und ist nicht gleich zu setzen mit dem Betriff «Security Audit».

fig. 5 – Bestandteile und Abhängigkeiten eines Security Assessments



Quelle: Grossmann & Seehusen, (2015, o.S.)

3.2. Digitales Inventar klären

3.2.1. Karte der technischen Umgebung

Eine erste Sicherheit kann erlangt werden, wenn ein Unternehmen Klarheit hat, welche Geräte, Systeme und Software im Einsatz stehen. Die Verbindungen zwischen den Elementen sollten bestimmt und geklärt werden. Und die Bereiche mit wertvollen Daten sollten ebenfalls aufgenommen werden.

Die Zustandsanalyse über die technische Umgebung kann in Form einer Karte gezeichnet, aber auch als Liste beschrieben werden. Wenn bereits ein Inventar besteht, so kann dieses gegebenenfalls mit den fehlenden Elementen und Verbindungen ergänzt werden. Das Zusammentragen des Zustands wird intern im Betrieb ausgeführt und generiert dadurch keine externen Kosten.

3.2.2. Rechteverwaltung und Zugriffsschutz

Zu einer Zustandsanalyse gehört eine Zusammenstellung aller Rollen mit deren Rechte pro System. Dies kann in sehr pragmatischer Weise gemacht werden, eine Aufstellung in einer simplen Tabelle reicht (Fuog, 2018). Auch wenn nicht bis ins Detail jede einzelne Berechtigung aufgeführt wird, so wächst bereits durch die Überlegungen das Bewusstsein für Rollen und Zugriffsrechte.

Ein zusätzlicher Aspekt sind die verwendeten User der Systeme. Wie werden deren Passwörter gepflegt? Welche Mitarbeiter haben welche Zugangsdaten und folgedessen welche Rollen?

3.2.3. Security Service Level Agreements

Beim Einkauf von Services externer Dienstleistern sollte überprüft werden, ob im SLA Informations-Sicherheitsbestimmungen definiert sind. Sind besondere Sicherheitsaspekte zu berücksichtigen, macht es Sinn, die Bedingungen in einem expliziten SSLA festzuhalten (Wegener, Milde & Dolle, 2016). Dies bringt zwei Vorteile: Es ist klarer, wo Sicherheitsbestimmungen zu finden sind. Und bei Anpassungen im Bereich Sicherheit muss nicht der gesamte SLA erneut abgesegnet werden.

Spätestens beim Erstellen des digitalen Inventars sollten die Vertrags-Bedingungen im Detail angeschaut und heikle Punkte notiert werden, um in der Risikoanalyse darauf einzugehen.

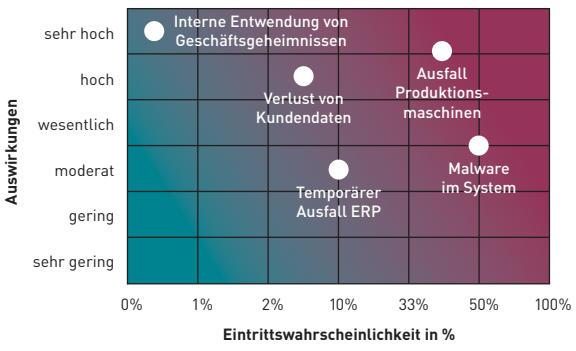
3.3. Risikoanalyse mit Fokus auf Informations- und IT-Sicherheit

3.3.1. Risikoappetit definieren

Ein weiteres, intern zu erarbeitendes Element ist die Risikoanalyse. Doch bevor diese Arbeit in Angriff genommen wird, sollte von der Unternehmensführung der Risikoappetit festgelegt werden. Diese Definition wird beim Einstufen von Risiken zur Richtschnur. Von leitenden Angestellten gewünscht wäre grundsätzlich eine einfach verständliche, praktische, ausführbare und messbare Definition (EY, 2015). In KMU dürfte aber gerade die Messbarkeit schwer zu erreichen sein.

Trotzdem sollte eine Definition gesetzt werden, auch wenn die Aussage generell gehalten wird. Im Rahmen eines KMU zur nachfolgenden Risikoanalyse ist dies genügend. Ein Beispiel wäre «Das Unternehmen geht bewusst Risiken ein, um führend im Bereich X zu bleiben.» Dies gibt eine Idee, dass Risiken eingegangen werden und auch wozu. Eine konservativere Unternehmung könnte ihren Risikoappetit so definieren: «Wir akzeptieren keine Risiken, welche unser Tagesgeschäft unterbrechen könnten.»

fig. 6 – Beispiel einer Risikomatrix



3.3.2. Aspekte der Risikoanalyse

Als Form für die Risikoanalyse bietet sich die Risikomatrix an. Dies ist eine gängige und leicht zu verstehende Darstellung, die wenig Text benötigt und direkt ein Bild der Situation liefert. Es zeigt: Welches Risiko kann welche (in der Regel finanziellen) Auswirkungen haben und tritt mit welcher Wahrscheinlichkeit auf.

Bei der Erfassung von Risiken der digitalen Sicherheit sollte der Fokus auf Informations- und IT-Sicherheit sowie auf die Prozess- und Systemstabi-

fig. 7 – Die vier Möglichkeiten mit Risiken umzugehen

Akzeptieren
(accept)

Vermeiden
(avoid)

Reduzieren
(mitigation)

Übertragen
(transfer)

lität gesetzt werden. Abschätzung von detaillierten Risiken von technischen Komponenten sind nicht möglich und auch nicht nötig, denn bei Bedarf sollte man eine technische Überprüfung durchführen, welche die Ursachen für Risiken direkt zu Tage bringen kann (siehe «3.5. Automated Testing» und «3.6. Penetration Test»).

Physische und personelle Aspekte müssen ebenso miteinbezogen werden wie digitale Zugriffs-/Rollenkonzepte und Prozessabläufe. Auf das Aufführen von Risiken mit sehr geringer Eintrittswahrscheinlichkeit oder sehr geringen Auswirkungen kann grundsätzlich verzichtet werden.

Ist ein Risiko benannt und eingestuft, so stehen einem vier Möglichkeiten zur Wahl: Akzeptieren, Vermeiden, Reduzieren und Übertragen. Mit diesen Möglichkeiten können Risiken behandelt werden; und ändern je nach Massnahme die Position in der Risikomatrix. Strebt man kein Security Audit an, so können direkt aus der Risikoanalyse Massnahmen definiert und umgesetzt werden, um die Sicherheit zu verbessern.

Eine externe Person kann zur Aufstellung einer Risikoanalyse beigezogen werden. Dies kann dienlich sein, um durch «Betriebsblindheit» übersehene Risiken zu positionieren. Wird nachfolgend ein Security Audit gemacht, so wird die Risikoanalyse in diesem Moment noch genauer geprüft und hinterfragt.

3.3.3. Statistiken vs. Erfahrung

In der Risikoanalyse wäre es praktisch, sich auf statistisch gesicherten Werten abzustützen. Doch was, wenn diese in einem Betrieb oder zu gewissen Fragestellungen nicht zu beschaffen sind? Da stellt sich die Frage, kann überhaupt eine saubere Risikoanalyse gemacht werden, ohne statistische Fakten?

David Hillson beschreibt es in einem Blog-Artikel «Top 10 myths of risk» als einen Mythos, dass Risiko-Management unbedingt Statistik benötigt. Die quantitative Risikoanalyse kann gemacht werden, wenn die nötigen Daten, Ressourcen und die nötige Expertise zur Verfügung stehen. In jedem Fall aber wird eine qualitative Risikoanalyse benötigt.

Auf der Grundlage einer qualitativen Risikoanalyse wird in der Regel auch die quantitative Risikoanalyse abgeleitet. Dazu kommt, das viele Risiken auch nicht einfach quantifizierbar sind und deshalb nur durch eine qualitative Risikoanalyse behandelt werden können. (Hillson, 2015)

Egal wie genau eine Risikoeinschätzung ist und wie sorgfältig die darauf getroffenen Massnahmen geplant sind: In jedem Fall sollte für die grössten Risiken ein Krisenplan bestehen, mit geklärten Rollen und Verantwortlichkeiten, sowie Handlungsabläufen und Kontakt-Daten der wichtigsten Partner und Lieferanten.

3.4. Security Audit

3.4.1. Ablauf

Ein Security Audit ist eine Analyse auf organisatorischer Stufe und hat den Zweck, Missstände und Probleme im Bezug auf die Sicherheit aufzudecken. Technische Fragestellungen werden nur am Rand bearbeitet, denn «80% der Probleme lassen sich mit organisatorischen Korrekturen lösen.» (Hüsler, 2018). Sobald der Ist-Zustand klar ist, können daraus auch Massnahmen abgeleitet werden. Von Security Audit Anbietern wird das Vorgehen in zwei Phasen eingeteilt:

Phase 1

1. **Vorgespräch**: Gerade bei sich unbekannten Unternehmen sollte ein Vorgespräch stattfinden. In erster Linie um zu klären, ob man sich überhaupt sympathisch ist. Wichtig ist auch, über die zu auditierenden Bereiche zu sprechen, um zu klären, ob der Anbieter alles abdeckt.
2. **Informations-Beschaffung durch den Betrieb**: Zusammentragen von Informationen. Hier kommt das digitale Inventar und die Risikoanalyse zum Zug. Bestehen weitere Konzepte oder Prozess-Dokumentationen, sollten diese ebenfalls zur Verfügung gestellt werden.
3. **«Big Picture»**: Aus den gesammelten Informationen wird gemeinsam im Gespräch die Ist-Situation zusammengestellt.
4. **Präsentation der Zustandsanalyse**: Der Auditor analysiert die Situation und erstellt daraus eine Präsentation oder eine hilfreiche Zusammenfassung der kompletten Zustandsanalyse.

Phase 2

1. **Definition der Massnahmen**: Auf Basis der gemachten Zustandsanalyse werden im Gespräch zwischen Auditor und Unternehmen Massnahmen zu den aufgedeckten Problemen definiert. Dies können Elemente sein wie: Anbieter wechseln, Produkte zusammenführen, Hierarchien klären, Prozesse definieren.
2. **Umsetzung der Massnahmen**: Das Unternehmen setzt nach Priorisierung die verschiedenen Massnahmen um. Je nach Anbieter wird angeboten, die Umsetzung der Massnahmen zu begleiten. Hier ist Vorsicht geboten: der Tester sollte nicht der Entwickler sein.

3.4.2. Anbieterwahl

Ein Security Audit sollte von einem externen, spezialisierten Unternehmen gemacht werden. Dadurch kann von dessen Erfahrungen profitiert werden. Zudem ist eine externe Person «neutral» und scheut sich nicht, Missstände eindeutig zu benennen.

Bei der Auswahl sollte überprüft werden, welche Spezialitäten der Auditor mit bringt. Ist der Anbieter spezialisiert in Datensicherheit, oder ein wichtiges Unternehmen im Bereich Netzwerk? Dann gilt es zu klären, ob nur die Technik im Fokus steht, oder ob dem Anbieter Prozesse genau so wichtig sind.

Die zusammengetragenen Informationen für ein Security Audit können sehr detailliert über das Unternehmen Auskunft geben. Je nach dem sind darin sogar Geschäfts- und Prozessgeheimnisse enthalten. Die Vertrauensfrage muss sich das Unternehmen vor dem Engagement eines Auditors stellen: «Will man diese Informationen wirklich dem Auditor preisgeben?»

3.5. Automated Testing

3.5.1. Wie und was kann automatisch getestet werden?

Unter Automated Testing versteht man das Aufspüren von Schwachstellen (Vulnerability Scan) durch Analyse von Endpunkten: In einem Netzwerk lassen sich alle Geräte mit eigenem Betriebssystem abfragen. Je nach Konfiguration des Endpunkts werden mehr oder weniger Informationen preisgegeben auf verschiedene Abfragen nach:

- Ping
- Offene Ports
- Aktive Dienste, Software-Versionen der Dienste
- Betriebssystem-Typ und Version
- Standard/Default Credentials für Logins

Mit diesem Vorgehen kann automatisch eine komplette Landkarte der Systeminfrastruktur erstellt werden. Durch die Zusatzinformationen kann erruiert werden, ob bekannte Sicherheitslücken in den verwendeten Programmen und Komponenten bestehen. Und offene Ports, die nicht offen und aktive Dienste, die nicht aktiv sein sollten, werden ebenfalls erkannt und ausgegeben.

Ein gutes Automated Testing liefert nicht nur die Indikationen zu den Schwachstellen, sondern auch direkt Handlungsempfehlungen zur Behebung der Schwachstelle. Eine stufengerechte (VR, IT-Leiter, Operative IT) Visualisierung des Zustands ist ebenfalls wünschenswert – damit lässt sich anschliessend viel einfacher Informieren, Kommunizieren und Entscheiden.

Nicht oder nur schwer automatisierbar sind Elemente wie der Bereich «Backup». Es liesse sich testen, ob ein Backup gemacht wird. Aber zu testen, ob die Daten darin korrekt sind oder ob ein Backup korrekt zurückgespielt werden könnte, ist nicht trivial.

Die ganzen Möglichkeiten der Traffic-Überwachung (Kontrolle des Datenflusses) gehören nicht ins Automated Testing, sondern in den Bereich Monitoring (welcher in dieser Arbeit nicht behandelt wird).

Mittner (2018) stellt klar: Automated Testing soll als Frühwarnsystem funktionieren und für die Analyse des zugewiesenen Bereichs sorgen. Massnahmen können und sollen nicht vom gleichen System umgesetzt werden. Das Prinzip der «Gewaltentrennung» soll eingehalten werden.

3.5.2. Vorteile durch Regelmässigkeit und Automatisation

Werden IT-Verantwortliche gefragt, wie oft eine Sicherheits-Prüfung stattfinden soll, so wird zum Teil ein Intervall zwischen drei und fünf Jahren gewünscht – aber bereits ein Jahr ist für eine technische Umgebung zu lang (Mittner, 2018). IT-Systeme wandeln sich stetig, zusätzliche Geräte werden angeschlossen, neue Sicherheitslücken in Softwarekomponenten werden bekannt.

Selbst bei Kleinunternehmen sind oft mehr Systeme im Einsatz als bei der Inventarisierung zusammengetragen wurden. Die Systeme, welche von den Mitarbeitern im täglichen Geschäft verwendet werden, bilden oft nur einen Teil der Systemlandschaft. Zugänge zu Systemen, welche auf angeschlossenen Geräten wie Router, Switches oder IoT-Geräten laufen, werden im Inventar gerne vergessen. Einem automatisierten Inventar entgehen diese Elemente nicht.

Nebst einem dokumentierten technischen Zustand dient Automated Testing auch als Hilfsmittel um Prioritäten zu setzen. «Probleme werden frühzeitig erkannt und können umgangen werden. Das gibt im Unternehmen Ressourcen frei.» (Mittner, 2018)

In einem Bericht von Matteson (2017) im Blog von TechRepulic wird das Sparpotenzial als gross bezeichnet, wenn automated Testings durchgeführt werden. Die Zeit-Einsparungen werden gegenüber einem manuellen Verfahren auf 56% eingeschätzt.

3.6. Penetration Test

Ein Penetration Test beschreibt das Überprüfen eines Systems durch aktives Angreifen, wie es auch Hacker machen würden. Solche Tests werden grundsätzlich manuell konzipiert und teilautomatisiert ausgeführt.

Der Begriff wird oft mit «Automated Testing» gleichgesetzt, beschreibt aber nicht das Gleiche. Penetration Tests werden spezifisch entwickelt und zum Teil mit sehr hohem Aufwand durchgeführt; für den Bereich KMU wird dies daher nur bei besonders schützenswerten Komponenten in Betracht gezogen.

Wichtig ist, dass bei Penetration Tests keine Ressourcen verschwendet werden mit Elementen, die man auch über ein automatisches Inventar hätte wissen können. Ebenso ist ein Penetration Test in eine «Blackbox» unnötiger Zeitaufwand, Whitebox Testing kommt viel schneller an die echten Probleme heran. Unter Blackbox-Test versteht man, wenn vom Unternehmen vor dem Start des Tests keine Informationen über das System an den Tester abgegeben werden.

3.7. Audit mit Social Engineering

3.7.1. Awareness schaffen!

«Fehlende Security-Awareness der Mitarbeiter gilt als größtes Sicherheitsrisiko.», hält IDG Research Services in der CISO Security Studie 2016 fest. Wenn die technische Umgebung eines Unternehmens ein gutes Sicherheits-Niveau aufweist, so bleibt stets der Risiko-Aspekt «Mensch».

Awareness lässt sich nicht absolut messen. Aber durch Aktionen wie ein simulierter Phishing-Mail-Versand an die eigenen Mitarbeiter kann erruiert werden, wie viele der Mitarbeiter Basis-IT-Sicherheitsaspekte befolgen. Oder man kann überprüfen lassen, wie einfach eine fremde Person physisch in die Räumlichkeiten und bis an die Systeme herankommt – zum Beispiel als Drucker-Service-Fachperson.

Empfohlen ist, bereits vor dem ersten Test entsprechende Schulungen durchzuführen. Nur so erhält man aussagekräftige Daten.

3.7.2. Herausforderungen und Vorteile von KMU

Für KMU ist die Durchführung eines Audits mit Social Engineering-Komponenten eher schwierig und zu teuer; aufgrund der kleinen Anzahl Mitarbeiter sinkt auch die Aussagekraft von Phishing-Simulationen. Die übersichtliche Grösse von KMU hat aber den Vorteil, dass «man sich kennt». So ist es für Angreifer schwieriger, sich für jemanden Auszugeben, der sie nicht sind.

Unabhängig davon, ob über Social Engineering Audit oder rein durch Schulungen vom Thema IT-Sicherheit gesprochen wird; wichtig ist eine Fehlerkultur zu etablieren, in der sich die Leute wagen, über begangene Fehler zu sprechen und Hinweise zu unsicherem Verhalten von Mitarbeitern geäussert respektive angenommen werden können. In kleinen Strukturen ist es einfacher, eine solche, von der Führung gelebte Fehlerkultur zu implementieren.

3.8. Ideenbringer für eine Grundsicherheit

3.8.1. Das Beste aus Frameworks ziehen

Es gibt eine Vielzahl von Rahmenwerken, welche zur Verbesserung von IT-Sicherheit eingesetzt werden können: ISO 27001/2, BSI, NIST, Cobit und BITS um nur ein paar der bekannteren zu nennen. Um solche Frameworks effizient und vollständig umzusetzen, bedarf es Fachpersonen.

Für Ideen, welche zu einer Grundsicherheit führen sollen, reicht es aber, wenn man als KMU das eine oder andere Dokumente querliest. Hier ein paar konkrete Tipps:

- Das Inhaltsverzeichnis der Norm DIN ISO/IEC 27002 «Informationstechnik – IT-Sicherheitsverfahren – Leitfaden für das Informationssicherheits-Management» kann als Themenliste genommen werden, welche Aspekte betreffend digitaler Sicherheit in einem Unternehmen relevant sein können.

- Im NIST-Framework lohnt sich ein Blick auf die fünf Haupt-Aufgaben (Core Functions). Diese sagen aus, welche Phasen durchlaufen werden müssen für eine sichere IT. Direkt dazu wird in Stichworten angegeben, welche Bereiche betroffen sind beziehungsweise welche Papiere, Strategien oder Aufgaben zur jeweiligen Core Function gehören.
- BSI IT-Grundschutz ist eine verdeutschte Form der ISO-Norm und dadurch besser verständlich. Ein Vorteil in der Verwendung des Frameworks liegt zudem darin, dass wesentlich weniger Risikoanalysen erforderlich sind, als bei ISO/IEC 27001 (Wegener, Milde & Dolle, 2016)

3.8.2. Wertvolle Informationen von MELANI

Die Melde- und Analysestelle Informationssicherheit des Bundes ist eine nützliche Quelle mit stets aktuell gehaltenen Merkblättern, Anweisungen und Anleitungen rund um die Informationssicherheit. Die in einer meistens leicht verständlichen Sprache verfassten und kompakt gehaltenen Informationen stehen der Bevölkerung kostenlos zur Verfügung und decken sowohl den Bereich «Privatpersonen» wie auch «Unternehmen» ab.

4. Szenarien

4.1. Klein-Unternehmen, keine eigene Server-Infrastruktur

4.1.1. Szenario «Coiffeur-Salon»

Anhand dieses Szenarios eines Klein-Unternehmens wird aufgezeigt, welche Mittel zur Überprüfung der digitalen Sicherheit angebracht sind und mit welchen Kosten dafür zu rechnen ist.

Beschreibung des Unternehmens	Coiffeur-Salon an zentraler Lage, starke Konkurrenz in unmittelbarer Nähe. Ein Standort, welche den Service-Bereich wie auch das Back-Office enthält.
Grösse	3 Mitarbeiter
Assets	Erreichbarkeit, Kundendaten
Wichtig für das Unternehmen	Verfügbarkeit Telefon-Anschluss Verfügbarkeit Online-Tool zum Buchen von Terminen Gefunden werden im Internet
Topologie	Standard-Router am Internet mit WLAN 1 Laptop Zugriffe auf die Termine auch über Mobile
Verwendete Cloud- und Web-Dienste	Termin-Vereinbarungs-Tool (Produkt) Kundendaten in Outlook 365 Webseite auf Jimdo E-Banking der Hausbank
In Auftrag gegebene Entwicklungen	keine
IoT-Geräte	iRobot Roomba (Staubsauger)

4.1.2. Empfohlene Mittel

Digitale Sicherheit ist auch bei nur drei Mitarbeitern sehr wichtig; die Durchführung soll aber pragmatisch umgesetzt werden. Folgende drei Mittel wären hier im Minimum empfohlen:

Inventarisierung – digitale Betriebsmittel kennen
Die zwei Haupt-Assets, die Verfügbarkeit und die Kundendaten, sind beide abhängig von den gewählten Lösungen punkto Software/Netzwerk.

- **Fokus auf die Zugriffsrechte der Cloud- und Webdienste**: Bei drei Mitarbeitern ist zu klären, wer die Admin-Rechte hat und wer «nur» Mitarbeiter ist. Nur aufgrund von Bequemheit sollten nicht alle User stets mit Admin-Rechten in den Systemen arbeiten.
- **AGB der Cloud- und Webdienste**: Seit dem Wandel zur neuen Datenschutzgrundverordnung im Jahr 2018 wurden viele AGB überarbeitet und dadurch verständlicher. Fokus hier ist das Überprüfen von Informationen zu SLA, SSLA und Datensicherheit (Backup). Die System-Sicherheit von Cloud- und Webdiensten lässt sich vom Kunden nicht überprüfen.
- **Betreffend Router**: Sind noch Standard-Passwörter aktiv? Kann von aussen auf den Router zugegriffen werden? Einfach beim Internet Service Provider nach der Sicherheit des Routers fragen; die Provider sind ebenfalls an einer sicheren Infrastruktur interessiert.

Sicherheit IoT Gerät
Bei dem verwendeten Typ von IoT-Gerät (Roboter-Staubsauger, nicht produktions-/servicerelevant), gilt es, dieses gegen Missbrauch zu schützen. Es darf nicht Teil eines Botnets werden, wo Rechenleistung und Verbindungsmöglichkeiten missbraucht werden um Dritt-Systeme zu schädigen. Wo immer möglich bereits bei der Installation eigene Passwörter setzen.

Marken-Produkte folgen eher dem Ansatz «Security by Design», denn die Unternehmen haben einen Ruf zu erhalten und sehen sich dem Kunden gegenüber oft länger verpflichtet als die Hersteller irgendwelcher No-Name-Produkte. Eine Recherche zum Produkt kann Informationen zur Sicherheit liefern.

Freie Quellen nutzen
Eine explizite IT-Sicherheits-Schulung oder ein Social Engineering Audit ist in der Praxis in diesem Szenario nur schwer denkbar. Aber menschliche Aspekte, welche die digitale Sicherheit beeinflussen, gibt es unzählige. Daher sollte auf folgende freie Quellen zurückgegriffen werden:

- **MELANI Verhaltensregeln**: Die bereitgestellten Informationen dienen der Selbstprüfung des eigenen Verhaltens und dem Kennenlernen der Basis-Verhaltensregeln für einen sicheren Umgang in der digitalen Welt.
- **Schulungseinheit zum Thema Phishing**: An sich direkt eine Massnahme, die aber hier erwähnt sei. Auf YouTube stehen von vielen namhaften Unternehmen Videos bereit, welche den korrekten Umgang mit Phishing-Mails/Webseiten erklären und Tipps geben,

woran man diese «gefälschten» Nachrichten/Webseiten erkennen kann.

4.1.3. Kosten

Wenn ein Mitarbeiter des Unternehmens Affinität zu Technik hat, können die vorgeschlagenen Massnahmen kostenfrei umgesetzt werden – Eigenleistungen nicht miteingerechnet.

Wird ein externes Security-Audit-Unternehmen miteinbezogen für den Inventar-Teil, so fallen für eine komplette Durchführung eines Audits Kosten von ca. 3000 Franken an. Idealerweise stellt der Betrieb so viele Informationen wie möglich selber zusammen und holt sich von den Experten anschliessend eine Meinung dazu ein; ohne Bestandsaufnahme und komplizierte Ausarbeitung der Lage, um ein gutes Kosten-Nutzen-Verhältnis zu gewährleisten und die Überprüfung für den Berieb erschwinglich zu machen.

4.2. Mittleres Unternehmen

4.2.1. Szenario «Metallbauer»

Anhand dieses Szenarios eines mittleren Unternehmens wird aufgezeigt, welche Mittel zur Überprüfung der digitalen Sicherheit angebracht sind und mit welchen Kosten dafür zu rechnen ist.

Beschreibung des Unternehmens	Metallbau-Betrieb, Entwickelt neue Lösungen für Balustraden und Geländer. Ein Standort mit Büro und Produktion. Eigene Produktionsstätte mit einem Maschinenpark, der einen halb-automatisierten Workflow aufweist.
Grösse	60 Mitarbeiter
Assets	Entwicklungen und Pläne von neuartigen Lösungen Metallstärkenberechnung (hochentwickeltes Tool) Kundendaten, Personaldaten
Wichtig für das Unternehmen	Schutz der Entwicklungen/Know-How Halten von wichtigen Mitarbeitern
Topologie	Hauseigenes Netzwerk, Firewall vorhanden Mehrere Cients (PCs) Interner Server mit ERP
Verwendete Cloud- und Web-Dienste	Webseite auf CMS Drupal E-Banking der Hausbank
In Auftrag gegebene Entwicklungen	ERP-Erweiterung «Modul Metallstärkenberechnung» mit Schnittstellen zu Lieferanten
IoT-Geräte	Mehrere CNC- und Fräsmaschinen, welche vom Netz aus direkt angesteuert werden können.

4.2.2. Empfohlene Mittel

Für dieses Szenario, in welchem der Schutz von Geschäfts- und Entwicklungsgeheimnissen eine grosse Rolle spielen, werden folgende minimale Mittel empfohlen:

Inventar und Risiko-Übersicht
Durch die Anzahl von 60 Mitarbeitern, einer Vielzahl von Clients und IoT-Geräten im Netzwerk und einer grossen Menge von unterschiedlichen Betriebssystemen und Programmen auf den Geräten, ist die Systemlandschaft einem konstanten Wandel unterworfen.

- Ein sauberes Inventarisieren und Überprüfen von Geräten, Konfigurationen und Programmen ist nur über Automated Testing möglich. Dies ermöglicht eine regelmässige Wiederholung in kurzen Abständen (z.B. einmal pro Woche).
- Inventar der Zugriffsrechte und Rollen aufzeichnen.
- Risiko-Analyse mit Fokus auf die Datensicherheit (Geheimhaltung, Backup) erstellen.

Für das komplette Inventar und die Risiko-Analyse sollte ein aussenstehender Sicherheits-Auditor beigezogen werden. Dieser hilft, die Analyse zu vervollständigen und mit seinem Expertenwissen die richtigen Schlüsse daraus zu ziehen.

Gezielter Penetration Test
Die Eigenentwicklung sollte in einem gezielten Penetration Test auf die Sicherheit geprüft werden. Die gemachte Risiko-Analyse sollte die realistischsten Szenarien hervorbringen, welche in die Konzeption des Penetration Test miteinfliessen.

Social Engineering / Schulung
Bei 60 Mitarbeitern ist die Bandbreite von Wissens zur digitalen Sicherheit gross. Umso mehr Gewicht muss dem sicheren Umgang mit digitalen Mitteln gesetzt werden.

Die Überprüfung ist in diesem Bereich gleichzeitig die Massnahme. Regelmässige Schulungsaktivitäten und Social Engineering Überprüfungen einzukaufen wäre sicher sinnvoll um «Sicherheit» zum Gespräch unter den Mitarbeitern zu machen. Bei einer Schulung sollte nebst Grundlagen und Phishing ein besonderes Augemerk auf die Wahrung von Geschäftsgeheimnissen gelegt werden; z.B. im Bezug auf den Austausch von Nachrichten in Social Media Kanälen (Facebook, Twitter etc.).

4.2.3. Kosten

Automated Testing Services sind für jährlich ungefähr 2000 bis 3000 Franken einzukaufen und decken damit bereits einen grossen Teil der Inventarisierung ab.

Das restliche Inventar und die Risiko-Analyse können intern vorbereitet werden. Bei dieser Betriebsgrösse und der Wichtigkeit von Datensicherheit ist es aber empfohlen, einen externen Anbieter für das Security Audit beizuziehen. Mit diesem können Inventar und Risiko-Analyse komplettiert werden. Durch die Beihilfe von Automated Testing ist auch hier mit ungefähr 3000 Franken für das Security Audit zu rechnen.

Die Kosten für einen Penetration Test können erst nach genauer Definition geschätzt werden. Pro Test-Tag sollte mit 2000 Franken gerechnet werden. In diesem Szenario könnte mit drei Testtagen eine umfassende Aussage über die Sicherheit und zu den nötigen Massnahmen gemacht werden.

Noch offener ist die Schätzung zu den Kosten von Social-Engineering-Überprüfungen, was vom Kern her gleichzeit Test und Massnahme abdeckt. Es lohnt sich für das Unternehmen, eine angepasste Sensibilisierung durchzuführen. Als minimale Massnahme können auch hier die Verhaltensregeln von MELANI in einer passenden Form (z.B. Schulung) den Mitarbeitern nähergebracht werden. Ein Eindringen einer externen Person ins Unternehmen durch Social Engineering hätte aber bestimmt einen prägenderen Effekt, welcher die Wichtigkeit der Einhaltung von Sicherheitsbestimmungen unterstreichen würde.

Das Total der Schätzung ergibt einen Betrag von ca. 15 000 Franken, was wie ein Initial-Investment angesehen werden muss. Bei einem Umsatz von 10 Millionen wäre dies gerade mal 0.15%. Die jährlichen Kosten für Automated Testing, weitere Schulungen und von gelegentliche Security-Audit-Auffrischungen wären mit einem Beitrag unter 5000 Franken gut investiertes Geld.

5. Quick Security Measure Test

5.1. Konzept

Mit dem Anspruch, Betriebsverantwortlichen innerhalb von wenigen Minuten aufzuzeigen, welche Mittel zur Überprüfung der Sicherheit in einem Unternehmen angebracht wären, wurde ein Prototyp eines Quick Security Measure Test (QSMT) entwickelt.

Der QSMT hat nicht den Anspruch, die Vollständigkeit eines ISO 27001-Standards zu erfüllen. Der Fokus liegt auf der Geschwindigkeit, in der sich auch ein IT-Sicherheits-Laie schnell einen Überblick verschaffen kann – und anschliessend nicht «etwas» für die Sicherheit tut, sondern «das Richtige» tut.

fig. 8 – Ansicht eines Abschnitts der QSMT-Webapplikation

5.2. Umsetzung des Prototyps

Der QSMT ist eine Webapplikation und kann unter qsmt.chrissharkman.ch aufgerufen werden. Eine Kurzanleitung erklärt die Funktionsweise. In vier Abschnitten können mit wenigen Fragen die Weichen für eine günstige Überprüfung der digitalen Sicherheit gelegt werden.

6. Fazit / Empfehlungen

6.1. Ein Plädoyer für Übersicht

Die günstigste Lösung beginnt damit, das Richtige zu tun.

Bevor also in IT-Sicherheit investiert wird, muss ein Unternehmen wissen, wo es denn überhaupt investieren muss. Mit den richtigen Mitteln zur Überprüfung kann diese Frage in kurzer Zeit geklärt werden. Ein QSMT kann erste Anhaltspunkte bringen, welche Überprüfungen sinnvoll sind und welche nicht. Die nötigen finanziellen Mittel für die Ausführung der Sicherheitsanalysen müssen im Unternehmen bereitgestellt werden.

Für jedes Unternehmen ist es sehr wichtig, eine Übersicht über sein Inventar zu haben. In der digitalen Welt noch viel mehr als in der analogen. Das digitale Inventar bringt stets Hinweise, wo Sicherheitsaspekte beachtet werden müssen. Ist die Übersicht da, können für KMU typische, pragmatische Wege eingeschlagen werden.

6.2. Wertvolle Eigenleistungen

Ein Startpunkt zur Überprüfung bieten Quellen mit frei verfügbaren Materialien wie MELANI oder private IT-Sicherheits-Anbieter; komplette Rahmenwerke wie ISO oder NIST zu studieren ist in einer ersten Phase eher übertrieben.

Kommt eine Zusammenarbeit mit einem externen Berater zustande, so kann die verrechnete Zeit effizienter genutzt werden, wenn im Unternehmen die Grundüberlegungen zu Inventar und Risiko bereits vor einem ersten Kontakt gemacht werden.

Die beste Sicherheitsüberprüfung (inkl. allen daraus resultierenden Massnahmen) nützt nichts, wenn sich nicht ein grundsätzliches «Sicherheits-Denken» im digitalen Bereich etabliert. Dieses Denken soll bereits in der Anschaffung von Systemen, Komponenten und Maschinen zum Tragen kommen, aber auch in Arbeitsprozessen und im Umgang mit Mitarbeitern gelebt werden. Ist das Sicherheitsdenken erst einmal in der DNA eines Unternehmens verankert, hat man viele Leistungen bereits gratis; und Massnahmen zur Steigerung der Mitarbeitersensibilität beginnen auf einem höheren Niveau.

Quellenverzeichnis

Digital Switzerland. (2016). Studie des Institute for Digital Business zum Stand der digitalisierung Schweizer KMUs. *Institute for Digital Business HWZ Hochschule für Wirtschaft Zürich.* Abgerufen am 12.06.2018, von https://www.digital-switzerland.ch/digital-switzerland-2016

Digital Switzerland. (2017). Studie des Institute for Digital Business zum Stand der digitalisierung Schweizer KMUs. *Institute for Digital Business HWZ Hochschule für Wirtschaft Zürich.* Abgerufen am 12.06.2018, von https://www.digital-switzerland.ch/digital-switzerland-2017

EY. (2015). Rethinking risk management – Banks focus on non-financial risks and accountability. *PDF-Publikation auf ey.com.* Abgerufen am 17.06.2018, von https://webforms.ey.com/Publication/vwLUAssets/EY-rethinking-risk-management/$FILE/EY-rethinking-risk-management.pdf

Fuog. (06.04.2018). *Telefongespräch* mit Herrn Fuog zum Thema Offertenanfrage Security Audit.

Gartner. (2017). Leading the IoT – Gartner Insights on How to Lead in a Connected World. M. Hung (Hrsg.). Stamford, USA: Gartner, Inc.

Grossmann, J., & Seehusen, F. (2015). Combining Security Risk Assessment and Security Testing Based on Standards. F. Seehusen, M. Felderer, J. Grossmann, & M.-F. Wendland (Hrsg.), *Risk Assessment and Risk-Driven Testing, Third International Workshop, Risk 2015* (o.S.). Cham, Schweiz: Springer International Publishing.

Heather, P. L. (27.05.2015). The Rise of the Digital Risk Officer. *Smarter with Gartner.* Abgerufen am 15.06.2018, von https://www.gartner.com/smarterwithgartner/the-rise-of-the-digital-risk-officer

Hillson, D., (14.04.2015). Top 10 myths of risk. *Association for Project Management apm Blog.* Abgerufen am 31.05.2018, von https://www.apm.org.uk/blog/top-10-myths-of-risk/

Hüsler, R. (06.04.2018). *Telefongespräch* mit Roger Hüsler zum Thema Offertenanfrage Security Audit.

IDG Research Services. (2016). *CISO Security Studie.* München, Deutschland: IDG Business Media GmbH

Klossek, S. (09.12.2015). Mehr Budget für CIOs. *computerworld.ch.* Abgerufen am 11.06.2018, von https://www.computerworld.ch/business/politik/budget-schweizer-cios-1339862.html

Matteson, S., (22.06.2017). Report: Companies are wasting massive amounts of money on ineffective security solutions. *TechRepublic.* Abgerufen am 31.05.2018, von https://www.techrepublic.com/article/report-companies-are-wasting-massive-amounts-of-money-on-ineffective-security-solutions/

Mittner, P. (18.06.2018). *Telefongespräch* mit Pascal Mittner, CEO First Security Technology AG, zum Thema Automated Testing und dem Produkt «First Security Cyber Control».

Profondia. (2016). IT-Markt Report 2016 (Präsentation). *Profondia AG.* Abgerufen am 30.04.2018, von https://www.profondia.com/index.cfm/_api/render/file/?method=inline&fileID=B0924F1C-EC3B-0680-3C9E9543BE9494D2

Red Alert Labs. (11.02.2018). The Importance of Security by Design for IoT Devices. *Red Alert Labs Blog.* Abgerufen am 12.06.2018, von https://www.redalertlabs.com/blog/the-importance-of-security-by-design-for-iot-devices

Ruffieux, J. (07.04.2018). *Telefongespräch* mit Johannes Ruffieux zum Thema Offertenanfrage Security Audit.

Tzouvaras, A., (13.04.2015). Is project risk management really a waste of time? *LinkedIn.* Abgerufen am 31.05.2018, von https://www.linkedin.com/pulse/project-risk-management-waste-time-apostolos-tzouvaras/

Wegener, C., Milde, T., & Dolle, W. (2016). Umsetzung des Informationssicherheits-Programms. C Wegener, T. Milde, & W. Dolle (Hrsg.) *Informationssicherheits-Management, Leitfaden für Praktiker und Begleitbuch zur CISM-Zertifizierung* (o.S.). Berlin, Deutschland: Springer International Publishing.

Weis, E., (28.02.2017). Welche Aufgaben erfüllt ein IT Sicherheitsbeauftragter? *Brandmauer Security IT Blog.* Abgerufen am 09.06.2018, von https://www.brandmauer.de/blog/it-security/welche-aufgaben-erfuellt-ein-it-sicherheitsbeauftragter

WIK. (2017). Aktuelle Lage der IT-Sicherheit in KMU. A. Hillebrand, A. Niederprüm, S. Schäfer, S. Thiele, & I. Henseler-Unger (Hrsg.). Bad Honnef, Deutschland: Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste GmbH

Winiker, M., & Egle, U. (04.09.2015). Studie «IT-Kostenmanagement bei Schweizer Kleinunternehmen». *HSLU, Financal Management Blog.* Abgerufen am 11.06.2018, von https://blog.hslu.ch/financialmanagement/2015/09/04/studie-it-kostenmanagement-bei-schweizer-kleinunternehmen/

Abbildungsverzeichnis

fig. 1 – PCs pro Mitarbeiter. 2
fig. 2 – Bedeutung von IT-Sicherheit 3
fig. 3 – Antworten auf die Frage: «Wo sehen Sie die hauptsächlichen Ursachen für mögliche Probleme und Schadensfälle bei der IT?» Entwicklung im Vergleich zwischen 2011 und 2017 . . . 4
fig. 4 – Jährliche IT-Kosten nach Unternehmensgrösse (in CHF) 4
fig. 5 – *Bestandteile und Abhängigkeiten eines Security Assessments* 8
fig. 6 – Beispiel einer Risikomatrix 9
fig. 7 – Die vier Möglichkeiten mit Risiken umzugehen 10
fig. 8 – Ansicht eines Abschnitts der QSMT-Webapplikation 19

Kontakte mit verschiedenen Security-Audit/Automated Testing anbietern, Schlüsselelemente der Telefonate im April 2018/Juni 2018

nexam IT, Roger Hüsler, 06.04.2018

- 80% der Probleme lassen sich mit organisatorischen Korrekturen lösen
- Vor allem Rollen, Zugriffe, Prozesse klären
- Cloud-Dienste wie Dropbox werden nicht technisch getestet; machen kann man da nichts ausser die AGBs akzeptieren…

Vorgehen Phase 1

- Vorgespräch (Abchecken: Ist man sich überhaupt sympathisch?, Scope definieren)
- Betrieb muss Unterlagen Beschaffen, Informationen Zusammentragen
- Daraus wird dann die Ist-Situation (Big Picture) zusammengestellt
- Auditor macht dann eine Präsentation

Vorgehen Phase 2

- Massnahmen werden definiert (z.B. Anbieter wechseln, Produkte zusammenführen, Hierarchien klären, Prozesse definieren (gerade Austritte etc.)

Learnings die daraus abgeleitet werden:

- Compliance-Regeln oder ein Paper erstellen, welches zu Statuten oder in den Firmen-Verträgen integriert wird; gewisse Absicherungen zu Rechten & Pflichten.

Anbieter vermittelt über Gryps-Offertenportal

Swisspro Solutions, Herr Fuog, 06.04.2018

- Dropbox Business anschauen: zentrale Rechteverwaltung möglich
- Zugänge und Rechte zusammentragen: sehr pragmatisch, einfach in Excel möglich
- Netzwerk als solches nicht so wichtig, wenn nur Router für Internetverbindung gebraucht wird.

Hat keine Richt-Offerte abgegeben.

Futec, Johannes Ruffieux, 7. April 2018

- Fokus setzen: Netzwerk auch überprüfen oder «nur» Datensicherheit? «Security Audit ist ein weiter Begriff.»
- «Bring your own device» (BYOD) ist heute eine Tatsache, auch wenn es die Sache nicht einfacher macht. Mitarbeiterschulung wird mit diesem Aspekt sicher wichtig.

First Security Technology, Pascal Mittner, 18.06.2018

Brandmauer IT Security, Volker Bentz, 19.06.2018

- Hat eine ganz klare Vision: auch die kleinen und mittleren Unternehmen sicher zu machen.
- Identitäts-Management ist der Punkt. Wichtig: Wer hat welche User, wer nutzt welche Accounts wo. Einrichtung von Accounts zentral verwalten.
- Passwort-Verwaltung zentral führen. Z.B. mit plesent password manager: arcmeo/interscale in Zug bietet den an; weitere Möglichkeit mit Password Safe von mateso.
- Cloudservices sind in der Regel sicher. Ist ein Dienst gratis, steht immer ein Geschäftsmodell dahinter.

Vier Punkte sind zu beachten, wenn das Identitäts-Management gut ist:

- Sensibilisierung der Mitarbeiter (Awareness)
- Virenschutz aktuell halten
- Patches pflichtbewusst einspielen
- Informieren

Schreiben an KMU zur Mithilfe an Zertifikatsarbeit

Sehr geehrte Damen und Herren, Wertes -Team

Alle sprechen von digitaler Transformation, dabei sind bei Ihnen bestimmt schon seit einiger Zeit viele Bereiche digital – oder werden zumindest von IT-Systemen unterstützt. Doch wissen Sie, ob Ihr Betrieb im digitalen Bereich sicher ist?

Für eine Arbeit in meinem Lehrgang «CAS Digital Risk Management» an der Hochschule für Wirtschaft Zürich zum Thema «Bezahlbare Überprüfung der digitalen Sicherheit von KMU – Evaluation effizienter Methoden und Vorgehensweisen» gelange ich deshalb an Sie, als KMU in der Region Bern. Ich denke, Sie wären ein geeigneter «Beispiel-Betrieb» aus einem IT-fernen Gewerbe, der mich hierbei unterstützen könnte.

Um was geht es?
Der Satz «100%ige digitale Sicherheit gibt es sowieso nicht, da brauche ich mich erst gar nicht anzustrengen» ist pure Resignation vor der digitalen Umwelt. Dabei muss man zuerst einfach wissen, wie und wo man Sicherheit prüfen kann und soll; um zu erkennen, an welchem Hebel anzusetzen ist.

Ziel der Arbeit ist es, den Beleg zu erbringen, dass eine vernünftige Überprüfung der digitalen Sicherheit für KMU bezahlbar ist – und nicht nur für Grossfirmen erschwinglich ist.

Was das Ihrem Betrieb bringt:
- Sie beschäftigen sich mit dem wichtigen Thema «IT Security»
- Sie erhalten eine Zusammenstellung von sinnvollen Massnahmen zur Überprüfung der digitalen Sicherheit, je nachdem direkt mit entsprechenden Kostenangaben (Offerteneinholung auf Ihre Umgebung abgestimmt). Damit wären Sie bereit, ein optimales und bezahlbares Security Audit in Auftrag zu geben.
- Persönliche Inputs zu IT-Sicherheits-Themen, Ratschläge zur Umsetzung von Massnahmen (Wissen aus meiner Ausbildung)

Was Sie nicht haben werden:
Der Zeitrahmen und der Arbeitsumfang sind grundsätzlich sehr eng gefasst. Daher werden in der Arbeit konkrete Massnahmen-Umsetzungen wie auch das Durchführen eines Security Audits nicht dazugehören.

Was benötige ich von Ihnen?
- Einblick in Ihre System-Architektur, IT-Organisation, Mitarbeiterschulung. (Keinen Einblick in irgendwelche Betriebsdaten)
- Kritische Fragen, echte Problemstellungen in Sachen IT-Sicherheit und -Verwendung, welche Sie im Betrieb haben.
- Zeit mit einer für IT verantwortlichen Person Ihres Betriebes.

Zeit-Rahmen:
Ab heute bis ca. Ende Mai 2018

Wer bin ich eigentlich?
Mein Name ist Christian Heimann, ich bin verheiratet und werde demnächst Vater. Annodazumal bin ich in einem KMU zur Lehre gegangen als Polygraf, habe später Medieningenieur studiert und bin heute als Software-Entwickler im Bereich eLearning tätig. Seit 2009 bin in Bern total zuhause, und freue mich, durch diese Arbeit – und eine Zusammenarbeit mit Ihnen – eine neue Facette der Stadt kennen zu lernen.

Ich danke Ihnen bereits jetzt für die Zeit, welche Sie sich genommen haben. Für Fragen stehe ich Ihnen und Ihrem Team gerne zur Verfügung.

Beste Grüsse

Christian Heimann

Fazit
Nach 7 angeschriebenen Betrieben nur 1 Absage, sonst keine Reaktion. In Zukunft Weg über Telefon wählen für ersten Kontakt. Daher die Wahl Szenarien zu entwickeln.