



INTELLIGENT SECURITY
HANDWERK

Intelligent Security Handwerk

IT-Sicherheit im Handwerk – Tragfähige Geschäftsmodelle in
Abhängigkeit der IT-Infrastruktur

Mittelstand-
Digital 



IT-Sicherheit
IN DER WIRTSCHAFT

Gefördert durch:



Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

INTELLIGENT SECURITY HANDWERK

Das Projekt Intelligent Security Handwerk ist ein vom Bundesministerium für Wirtschaft und Klimaschutz gefördertes Projekt der Initiative IT-Sicherheit in der Wirtschaft.

Intelligent Security Handwerk hat zum Ziel, kleine und mittelständische Unternehmen im deutschen Handwerk zur IT-Sicherheit zu befähigen und sie dadurch bei ihrer Digitalisierung zu unterstützen. Im Zuge des Projekts werden sowohl ein intelligenter IT-Sicherheitsassistent in Form eines Online-Tools sowie entsprechende Weiterbildungsangebote entwickelt. Entsprechend werden Ansätze aus der Managementforschung hinsichtlich Geschäftsmodellen, Fachkräftekompetenzen und der Technologiefolgenabschätzung (Universität Kassel) mit der Expertise zur Gestaltung, Entwicklung und Erprobung von verlässlichen, sicheren, nutzerfreundlichen und zweckdienlichen Anwendungen, Informationsinfrastrukturen und Entscheidungsunterstützungssystemen (Karlsruher Institut für Technologie) kombiniert. Der Transfer in das Handwerk wird durch das Netzwerk des Berufsförderungswerks des Handwerks und der assoziierten Partner sichergestellt.

MITTELSTAND-DIGITAL

Das Projekt Intelligent Security Handwerk ist Teil von Mittelstand-Digital. Das Mittelstand-Digital Netzwerk bietet mit den Mittelstand-Digital Zentren und der Initiative IT-Sicherheit in der Wirtschaft umfassende Unterstützung bei der Digitalisierung. Kleine und mittlere Unternehmen profitieren von konkreten Praxisbeispielen und passgenauen, anbieterneutralen Angeboten zur Qualifikation und IT-Sicherheit. Das Bundesministerium für Wirtschaft und Energie ermöglicht die kostenfreie Nutzung. Weitere Informationen finden Sie unter www.it-sicherheit-in-der-wirtschaft.de.

Inhaltsverzeichnis

1.	Zielsetzung	3
2.	Ablauf der Studie	4
3.	Ergebnisse	6
4.	Tragfähige Geschäftsmodelle für den IT-Sicherheitsassistenten	7
5.	Validierung der Ergebnisse und ergänzende Produkt-Service Innovationen	10
6.	Nutzen für Handwerksbetriebe	13

1. Zielsetzung

Die zunehmende Digitalisierung und der damit einhergehende Einsatz digitaler Technologien erhöht die Risiken für Handwerksbetriebe in Bezug auf IT-Sicherheit. Cyberangriffe verursachen jährlich immense wirtschaftliche Schäden und sind längst nicht mehr nur ein Problem großer Konzerne¹. Gerade kleinere Betriebe geraten immer häufiger ins Visier von Cyberkriminellen, da sie oft nicht über die personellen oder finanziellen Ressourcen verfügen, um sich effektiv zu schützen¹. Der Schutz vor Datenverlust und die Gewährleistung der Funktionsfähigkeit der IT-Systeme sind für den betrieblichen Erfolg unverzichtbar.

So können Handwerksbetriebe, die auf digitale Technologien wie beispielsweise Cloud-Dienste oder digitale Verwaltungssoftware setzen, zwar ihre Produktivität erhöhen, sie stehen jedoch ebenso vor neuen Herausforderungen: Die Sicherung dieser Systeme gegen Cyberangriffe erfordert zusätzliche Maßnahmen, um den Betrieb vor Ausfällen und Datenverlust zu schützen². Insbesondere die Bedenken in Bezug auf die IT-Sicherheit hindern Handwerksbetriebe zurzeit an einer umfassenderen Digitalisierung ihrer Geschäftsmodelle. In einer zunehmend vernetzten und digitalisierten Arbeitswelt spielt die IT-Sicherheit daher eine entscheidende Rolle.

Vorherige Studien, die im Rahmen des Forschungsprojektes „Intelligent Security Handwerk“ bereits durchgeführt wurden, haben gezeigt, dass neben den finanziellen Schwierigkeiten insbesondere die Zeit und das Wissen fehlt, das notwendig ist, um das eigene IT-Sicherheitsniveau zu erhöhen³. Um diese Herausforderung zu adressieren, wurde ein intelligenter IT-Sicherheitsassistent entwickelt, der zur Entscheidungsunterstützung im IT-Sicherheitsmanagement dienen und damit zur Erhöhung des IT-Sicherheitsniveaus von Handwerksbetrieben beitragen soll.

Da die Kommerzialisierung eines solchen Angebots nur mit einem passgenauen Geschäftsmodell gelingen kann⁴, ist das Ziel, tragfähige Geschäftsmodelle für den IT-Sicherheitsassistenten

¹ Bundesamt für Sicherheit in der Informationstechnik (BSI): Die Lage der IT-Sicherheit in Deutschland 2024

² Bitkom Research (2022): Die Digitalisierung des Handwerks

³ Arnold et al. (2022): How Do Technological Frames Feel? Business Model Innovation in Pre-Digital Companies and the Emotional Impact of Digital Technologies

⁴ Chesbrough (2010): Business model Innovation: Opportunities and Barriers

in Abhängigkeit der Komplexität der IT-Infrastruktur zu identifizieren. Nur mit einem attraktiven Geschäftsmodell kann sichergestellt werden, dass der IT-Sicherheitsassistent einen Mehrwert für das deutsche Handwerk bietet und entsprechend vermarktet werden kann.

2. Ablauf der Studie

Um die Gemeinsamkeiten und Unterschiede in Handwerksbetrieben hinsichtlich der Akzeptanz von Geschäftsmodellen für IT-Sicherheitsangebote zu identifizieren, wurde eine umfassende Interviewstudie durchgeführt⁵. Die Untersuchung richtete sich insbesondere an Handwerksunternehmen, die bereits digitale Technologien einsetzen. Dabei wurden eine Vielzahl von Branchen berücksichtigt, darunter Bauwesen, Garten- und Landschaftsbau und Malerhandwerk. Ziel war es, möglichst Betriebe unterschiedlicher Gewerke einzubeziehen, um die Vielfalt des deutschen Handwerks abzubilden.

Die Datenerhebung erfolgte durch persönliche Interviews mit Geschäftsführern, IT-Mitarbeitenden und weiteren Personen, die in den Handwerksbetrieben in die Entscheidungen über die IT-Infrastruktur und IT-Sicherheit involviert sind⁶. Ziel war es, die Anforderungen an IT-Sicherheitslösungen und die Präferenzen für unterschiedliche Geschäftsmodelle zu ermitteln. Dabei wurde zum einen die individuelle Komplexität der IT-Infrastruktur und zum anderen die Zahlungsbereitschaft für IT-Sicherheitslösungen ermittelt. Weiterhin wurde der intelligente IT-Sicherheitsassistent in Grundzügen vorgestellt, um die Attraktivität von und Zahlungsbereitschaft für ein solches Angebot zu ermitteln. Insgesamt wurden 15 Interviews in 10 verschiedenen Handwerksbetrieben durchgeführt, wobei die befragten Unternehmen zwischen 6 und 152 Mitarbeiter beschäftigen.

Zur Erfassung der Komplexität der IT-Infrastruktur der jeweiligen Handwerksbetriebe wurde näherungsweise die Anzahl der im Geschäftsmodell bereits eingesetzten digitalen Technologien ermittelt, da die Komplexität der zu verwaltenden IT-Infrastruktur und Angriffsfläche für Cyberangriffe zunimmt, je mehr digitale Technologien eingesetzt werden. Zur Ermittlung der Zahlungsbereitschaft wurden die befragten Handwerksbetriebe gebeten, anzugeben, welchen Betrag in Euro sie pro Monat in die Sicherstellung der IT-Sicherheit zu investieren bereit sind.

⁵ Eisenhardt (1989): Building Theories from Case Study Research

⁶ Yin (2018): Case Study Research and Applications: Design and Methods

Die befragten Unternehmen wurden in drei Fälle zusammengefasst: Gruppe A umfasst Betriebe mit geringer Komplexität, Gruppe B bezieht sich auf Betriebe mit mittlerer Komplexität, während Gruppe C Betriebe mit hoher Komplexität der IT-Infrastruktur repräsentiert. Diese Kategorisierung hilft dabei, die bevorzugten Geschäftsmodelle für IT-Sicherheitsangebote für Handwerksbetriebe mit unterschiedlich komplexer IT-Infrastruktur zu identifizieren (Tabelle 1).

Tabelle 1: Gruppeneinteilung befragter Unternehmen nach Komplexität der IT-Infrastruktur

Gruppe	Unternehmen	Branche	Gründungsjahr	Mitarbeiteranzahl	Anzahl eingesetzter digitaler Technologien
A	U01	Garten- und Landschaftsbau	1850	85	2
	U07	Sanitär, Heizung, Klima	1930	104	3
	U09	Baugewerbe	1885	152	3
	U10	Aufzugs-, Anlagentechnik	1975	130	3
B	U02	Fenster-/Türenbau	1937	57	4
	U04	Baugewerbe	2002	51	4
	U05	Malerbetrieb	1920	51	4
	U08	Metallbau	1895	50	4
C	U03	Forstwirtschaft	2004	6	7
	U06	Sanitär, Heizung, Klima	2009	10	6

Im Anschluss an die Interviewstudie wurde ein Expertenworkshop mit den assoziierten Partnern dieses Projektes, Handwerksunternehmen und Vertretern handwerksnaher Verbände durchgeführt, um die Ergebnisse zu validieren und gemeinsam einen ersten Entwurf eines möglichen Geschäftsmodells für den intelligenten IT-Sicherheitsassistenten zu entwickeln.

3. Ergebnisse

Die Interviews wurden gezielt durchgeführt, um mögliche Geschäftsmodelltypologien zu identifizieren, die eine effektive Vermarktung des IT-Sicherheitsassistenten ermöglichen. Im Rahmen der Auswertung wurden dabei zwei wichtige Dimensionen betrachtet: die **Komplexität der IT-Infrastruktur** und die **Zahlungsbereitschaft für IT-Sicherheit**.

Dimension 1: Komplexität der IT-Infrastruktur

Um die Komplexität der IT-Infrastruktur zu ermitteln, wurden die befragten Unternehmen nach der Anzahl an digitalen Technologien gefragt, die sie bereits einsetzen. Die Mehrheit der Befragten nutzt mobile Endgeräte, branchenspezifische Software, Server sowie Cloud-Technologien. Darüber hinaus wurden digitale Verwaltungsprogramme, wie die digitale Erfassung von Arbeitszeiten und die Nutzung von digitalen Rechnungs- und Angebotssoftwares, genannt. Die Anzahl der eingesetzten Technologien wurde als Maß für die Komplexität der IT-Infrastruktur verwendet. Um die Präferenzen für Geschäftsmodelle zu analysieren, wurden die Unternehmen in drei Gruppen eingeteilt: Gruppe A umfasst Betriebe mit einem Komplexitätswert von 0 bis 3, Gruppe B umfasst Betriebe mit einem Komplexitätsniveau von 4 bis 5 und Gruppe C weist Werte von 6 bis 7 auf. Die befragten Unternehmen wiesen im Durchschnitt eine Komplexität der IT-Infrastruktur von 4 auf. Zwei Betriebe gaben eine hohe Komplexität der eingesetzten digitalen Technologien an, während vier Unternehmen eine geringe Anzahl an digitalen Technologien einsetzen und somit eine IT-Infrastruktur mit niedriger Komplexität aufweisen. Vier weiteren Unternehmen konnte ein mittleres Komplexitätsniveau zugeordnet werden.

Dimension 2: Zahlungsbereitschaft für IT-Sicherheit

Die Zahlungsbereitschaft für IT-Sicherheit bildet die zweite Dimension zur Bestimmung der bevorzugten Geschäftsmodelltypologien. Die Befragten wurden gebeten anzugeben, wie viel sie bereit sind, in ihre IT-Sicherheit zu investieren oder welche Beträge sie für angemessen halten, um die Sicherheit ihrer IT-Infrastruktur zu gewährleisten. Im Durchschnitt gaben die Handwerksbetriebe an, dass sie bereit wären, etwa 250 Euro pro Monat für IT-Sicherheit auszugeben. Die Ergebnisse zeigen, dass Handwerksbetriebe mit steigender Komplexität der IT-

Infrastruktur eher bereit sind, höhere Summen in den Schutz ihrer IT-Infrastruktur zu investieren (siehe Abb. 2).

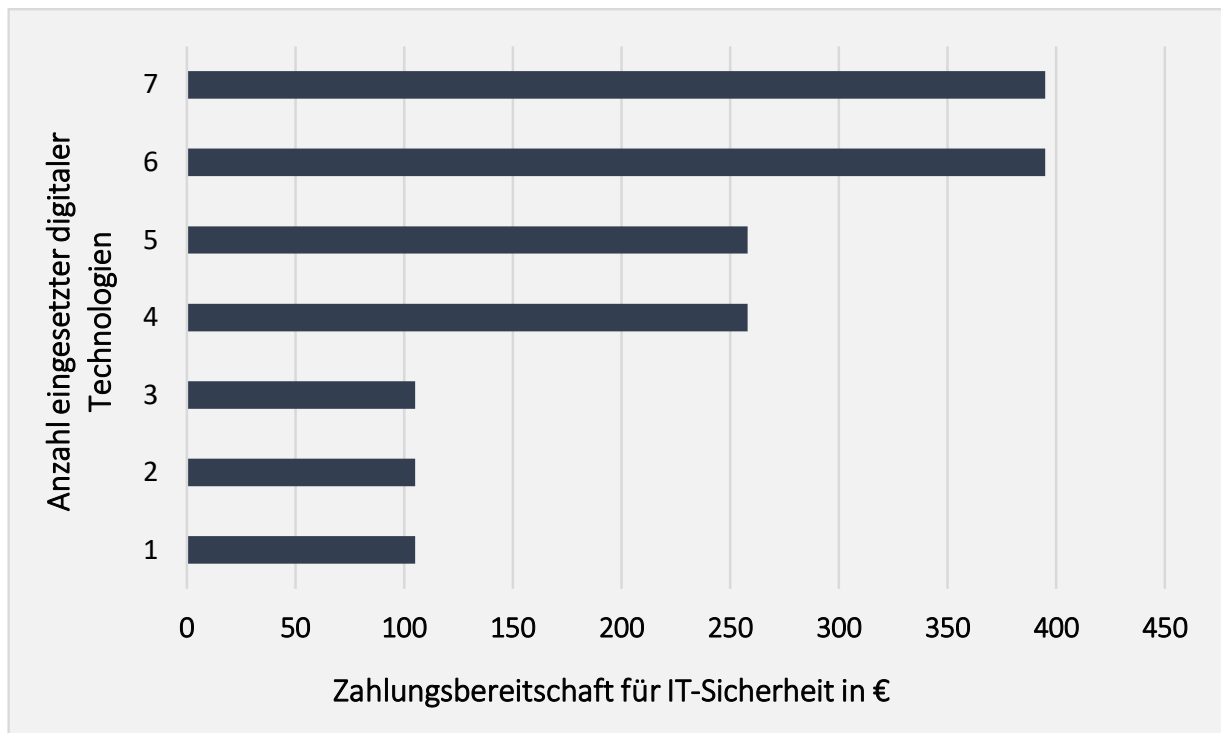


Abbildung 1: Zahlungsbereitschaft für IT-Sicherheit in Abhängigkeit der eingesetzten digitalen Technologien

4. Tragfähige Geschäftsmodelle für den IT-Sicherheitsassistenten

Zur Identifizierung des jeweils bevorzugten Geschäfts- bzw. Abrechnungsmodell wurden den Handwerksbetrieben nach Feststellung der Komplexität der IT-Infrastruktur und Zahlungsbereitschaft fünf verschiedene und von Unternehmen häufig eingesetzte Geschäftsmodelltypologien vorgestellt:

Einmalkauf: Der IT-Sicherheitsassistent wird zu einem festen Preis angeboten und kann nach dem Kauf uneingeschränkt und dauerhaft genutzt werden. Zukünftige Versionen müssen erneut erworben werden.

Abo-Modell: Hierbei werden regelmäßige (monatliche) Zahlungen für den IT-Sicherheitsassistenten verlangt, und das Abonnement kann monatlich gekündigt werden. Es steht immer die neueste Version des IT-Sicherheitsassistenten zur Verfügung.

Pay-per-Use: Der Preis hängt von der tatsächlichen Nutzung des Produkts ab (z.B. Anzahl der Endgeräte).

Freemium: Eine kostenlose Basisversion ist verfügbar, während zusätzliche Funktionen oder erweiterte Inhalte kostenpflichtig erworben werden müssen.

Free-Modell: Das Produkt wird vollständig kostenlos angeboten und durch auf den Kunden personalisierte Werbung finanziert.

Auf Basis dieser Ergebnisse wurde ermittelt, welches Geschäftsmodell für welchen Grad der Komplexität der IT-Infrastruktur (gering/hoch) und welche Zahlungsbereitschaft (gering/hoch) besonders attraktiv ist (siehe Abb. 3). Die Kategorisierung der vier Quadranten erfolgte anhand der **häufigsten** genannten Geschäftsmodelltypologien, die von den Befragten auf einer Skala von 1 (geringe Attraktivität) bis 7 (hohe Attraktivität) bewertet wurden.

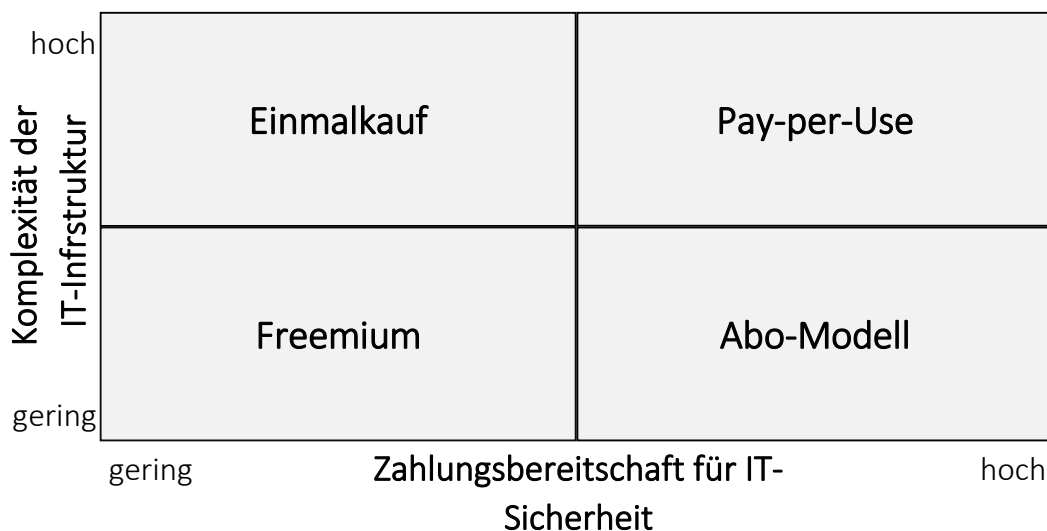


Abbildung 2: Präferierte Geschäftsmodelltypologien des IT-Sicherheitsassistenten

Die Auswertung zeigt vier bevorzugte Geschäftsmodelltypen für einen IT-Sicherheitsassistenten in Handwerksbetrieben, die von der Zahlungsbereitschaft und der Komplexität der IT-Infrastruktur abhängen:

Betriebe mit mittlerer bis hoher IT-Komplexität und einer hohen Zahlungsbereitschaft tendieren zum **Pay-per-Use-Modell**, da sie die Flexibilität schätzen und bereits Erfahrungen mit ähnlichen Abrechnungsmodellen haben. Ein Betrieb beschreibt seine Situation so:

„Wir sind ständig dabei, die IT-Infrastruktur zu erweitern. Wenn ich jetzt viel für die Sicherheit investieren müsste, könnte ich mir so einen IT-Sicherheitsassistenten vorstellen. Das Pay-per-Use wäre so das klassische, was in dem Fall immer Sinn ergibt.“

– Datenschutzbeauftragter im Garten- und Landschaftsbau

Unternehmen mit mittlerer bis hoher IT-Komplexität, jedoch geringer Zahlungsbereitschaft, bevorzugen hingegen den **Einmalkauf**, da sie auf regelmäßige monatliche Zahlungen verzichten möchten. Ein befragtes Unternehmen drückt dies so aus:

„Das finde ich grundsätzlich gut, dann habe ich einmal Kosten und dann ist es weg. Dann habe ich nichts monatlich Wiederkehrendes.“

– Sachverständiger in der Forstwirtschaft

Ein weiteres Unternehmen ergänzt:

„Vom Einmalkauf sind wir hier Fan.“

– IT-Mitarbeiter im Bereich Klimatechnik

Betriebe mit niedriger bis mittlerer IT-Komplexität und einer ebenfalls geringen Zahlungsbereitschaft zeigen hingegen Interesse am **Freemium**-Modell, das es ihnen ermöglicht, den IT-Sicherheitsassistenten zunächst kostenfrei zu testen. Ein Betrieb erklärt dazu:

„Tatsächlich würde ich sagen, dass ich für einen IT-Sicherheitsassistenten nichts zahlen möchte.“

– Geschäftsführer im Bereich Fenster- und Türenbau

Ein weiterer Kommentar verdeutlicht den Nutzen des Freemium-Modells, insbesondere für kleinere Handwerksbetriebe:

„Zum Ausprobieren ist es gerade auch für kleinere Handwerksbetriebe sehr interessant, als gleich so ein Kostenbatzen aufzurufen.“

– Geschäftsführer eines Malerbetriebs

Unternehmen mit niedriger bis mittlerer IT-Komplexität und hoher Zahlungsbereitschaft präferieren dagegen das **Abo-Modell**, da es Flexibilität bietet und eine kurzfristige Kündigung ermöglicht:

„Und wenn es mir nicht gefällt, kann ich es auch wieder kündigen.“

– Buchhalter im Baugewerbe

Das **Free-Modell** wurde von keinem Unternehmen präferiert, da Werbung als störend empfunden wird und der Nutzen unklar ist:

„Also, wenn da Werbung aufpoppt und mich fünf Minuten am Arbeiten hindert, dann ist es doof.“

– Datenschutzbeauftragter im Garten- und Landschaftsbau

„Werbung? Nein, auf keinen Fall.“

– IT-Mitarbeiter im Bereich Klimatechnik

5. Validierung der Ergebnisse und ergänzende Produkt-Service Innovationen

Um die aus der Interviewstudie resultierenden Ergebnisse zu diskutieren und zu validieren wurde ein Workshop mit Experten aus dem Handwerk bzw. Handwerksnahen Kammern und Verbänden durchgeführt. Weiterhin diente der Workshop der Erstellung eines ersten Entwurfs für ein tragfähiges Geschäftsmodell für den intelligenten IT-Sicherheitsassistenten sowie der Identifizierung ergänzender Services, die das Angebot aus Sicht der Beteiligten noch attraktiver machen würden und die Bedürfnisse der Handwerksbetriebe widerspiegeln.

Allgemein umfasst ein Geschäftsmodell die Dimensionen Wertangebot, Wertschöpfung sowie Kosten- und Erlösmodell⁷. Das Business Model Canvas ist ein effektives Werkzeug, um die wesentlichen Bausteine eines Geschäftsmodells im Detail zu analysieren und wird in der Praxis eingesetzt, um neue Geschäftsmodelle zu entwickeln und um bestehende zu innovieren. Im Rahmen des Workshops wurde das Business-Model Canvas angewandt, um für den intelligenten IT-Sicherheitsassistenten ein Geschäftsmodell für Handwerksbetriebe zu entwickeln, das nicht nur finanzielle, sondern auch funktionale Anforderungen optimal abdeckt. Ebenso werden die in diesem Zuge verschiedene Produkt-Service-Innovationen einbezogen. Diese Inno-

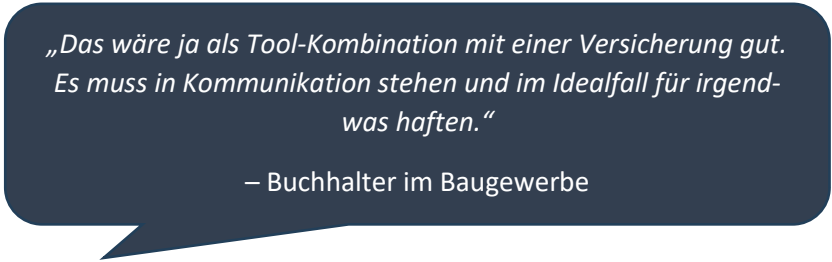
⁷ Spieth & Schneider (2016): Business Model Innovativeness: Designing a Formative Measure for Business Model Innovation

vationen verbessern das Angebot und machen den Assistenten zu einem umfassenden Werkzeug für IT-Sicherheit und betriebliche Unterstützung. Zur Erstellung des Business Model Canvas wurde den Teilnehmenden Fragen gestellt, die in Breakout-Sessions beantwortet und später gemeinsam diskutiert wurden:

- Welche spezifischen Bedürfnisse und Probleme haben Sie im Bereich IT-Sicherheit?
- Welche Funktionen und Eigenschaften des IT-Sicherheitsassistenten sind für Sie besonders wertvoll?
- Über welche Kanäle möchten Sie über IT-Sicherheitslösungen informiert werden und diese erwerben?
- Welche Art von Unterstützung und Betreuung erwarten Sie vom Anbieter?
- Für welche Dienstleistungen und Funktionen sind Sie bereit zu zahlen, und welche Zahlungsmodelle bevorzugen Sie?
- Welche Ressourcen und Kompetenzen sollte der Anbieter haben, um Ihre Anforderungen zu erfüllen?
- Welche Aktivitäten des Anbieters sind für Sie entscheidend, um den gewünschten Nutzen zu erhalten?
- Welche Partnerschaften und Kooperationen des Anbieters sind für Sie wichtig?
- Welche Kostenstrukturen sind für Sie akzeptabel und welche Preis-Leistungs-Verhältnisse erwarten Sie?

Aus den Antworten wurde gemeinsam das Business Model Canvas gefüllt. Zusätzlich wurden die Teilnehmer des Workshops gebeten, Ihre Ideen und Wünsche bezüglich möglicher Produkt-Service-Innovationen zu äußern, die das Geschäftsmodell des intelligenten IT-Sicherheitsassistenten ergänzen könnten.

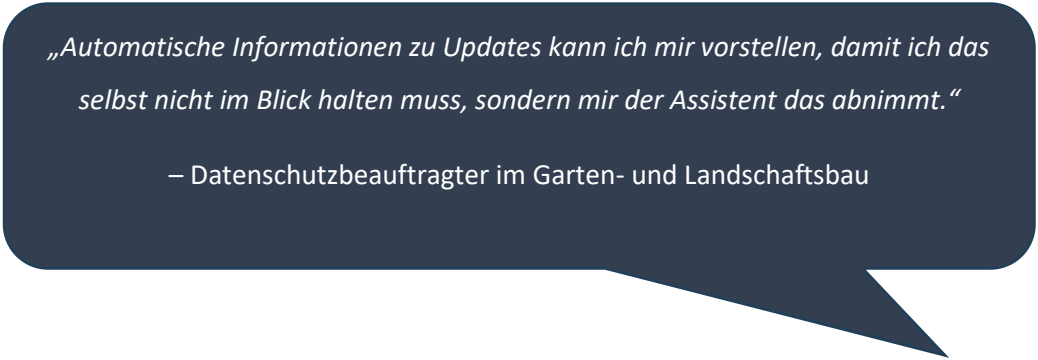
Für die Umsetzung des IT-Sicherheitsassistenten spielen demnach verschiedene Schlüsselpartner eine wesentliche Rolle. Dazu zählen IT-Dienstleister, das Bundesamt für Sicherheit in der Informationstechnik (BSI) und Cyber-Versicherungen. Diese Partner sind entscheidend für die technische Umsetzung, die Bereitstellung von Sicherheitsstandards und die Erweiterung des Dienstleistungsangebots. Durch ihre Zusammenarbeit wird sichergestellt, dass die technischen und sicherheitsrelevanten Anforderungen des IT-Sicherheitsassistenten kontinuierlich erfüllt werden.



„Das wäre ja als Tool-Kombination mit einer Versicherung gut. Es muss in Kommunikation stehen und im Idealfall für irgendwas haften.“

– Buchhalter im Baugewerbe

Was die Wertschöpfung betrifft, so wurden hier bspw. die Pflege und Weiterentwicklung der Sicherheitslösungen, das Management und Feedback-Handling sowie die regelmäßige Wartung des Systems durch IT-Fachkräfte genannt. Diese internen Geschäftsprozesse sollen sicherstellen, dass der intelligente IT-Sicherheitsassistent stets an aktuelle Sicherheitsanforderungen und die spezifischen Bedürfnisse der Nutzer angepasst und kontinuierlich weiterentwickelt wird.



„Automatische Informationen zu Updates kann ich mir vorstellen, damit ich das selbst nicht im Blick halten muss, sondern mir der Assistent das abnimmt.“

– Datenschutzbeauftragter im Garten- und Landschaftsbau

Durch den Einbezug möglicher Produkt-Service-Innovationen entsteht so ein ganzheitliches Geschäftsmodell, das nicht nur die spezifischen Bedürfnisse der Handwerksbetriebe berücksichtigt, sondern gleichzeitig eine Grundlage für die langfristige Nutzung und Weiterentwicklung des IT-Sicherheitsassistenten schafft (siehe Abb. 4).

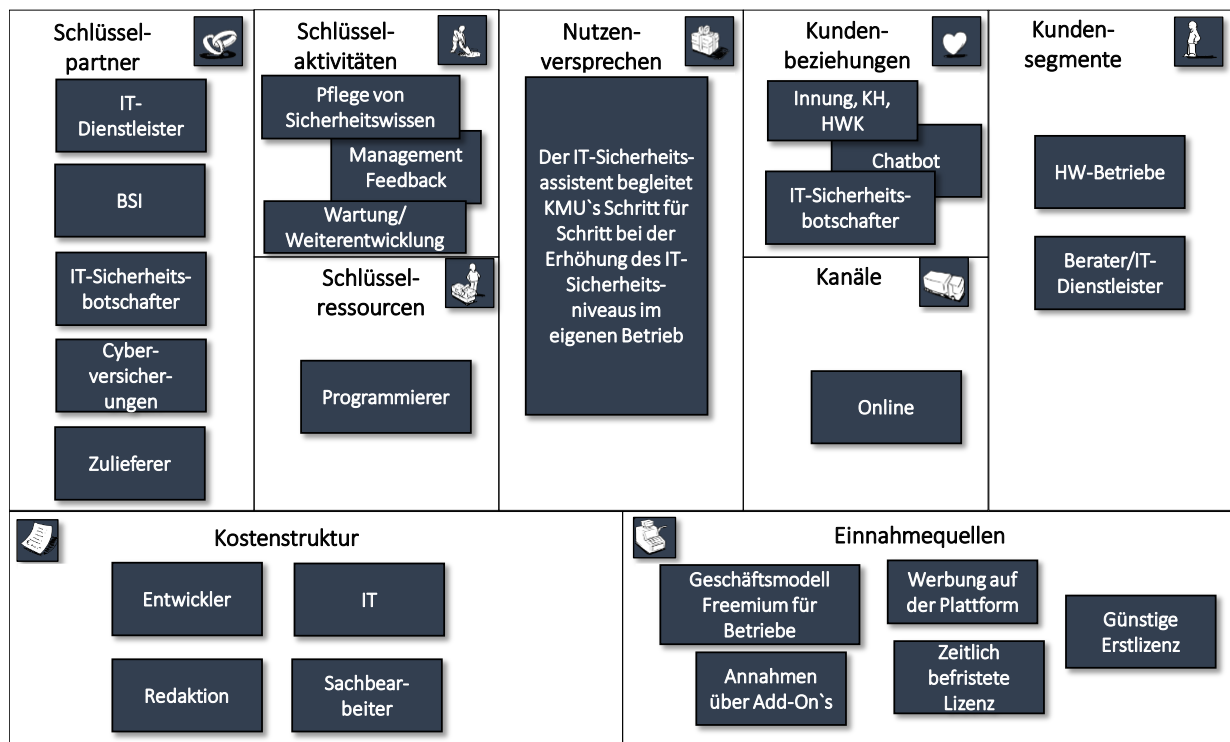


Abbildung 3: Business Model Canvas des IT-Sicherheitsassistenten, Ergebnis der Breakout-Session

6. Nutzen für Handwerksbetriebe

Im Zuge dieser Studie konnten wichtige Erkenntnisse gewonnen werden. Zum einen wurde die Zahlungsbereitschaft von Handwerksbetrieben zur Erhöhung der IT-Sicherheit in Abhängigkeit der Komplexität der eingesetzten IT-Infrastruktur untersucht. Die Studie zeigt, dass Handwerksbetriebe in ihrer Bereitschaft, für IT-Sicherheit zu zahlen, und in der Komplexität ihrer IT-Infrastruktur stark variieren. Es lässt sich aus den Ergebnissen ableiten, dass die Komplexität der eingesetzten IT-Infrastruktur automatisch die Zahlungsbereitschaft für IT-Sicherheit erhöht. Während Betriebe mit geringer Komplexität der IT-Infrastruktur oftmals nicht bereit sind, viel in ihre IT-Sicherheit zu investieren, so ist die Zahlungsbereitschaft bei sehr hoher Komplexität nicht zwingend am höchsten. In dieser Studie sind es die Betriebe mit mittlerer Komplexität, die die höchste Zahlungsbereitschaft zur Sicherstellung der IT-Sicherheit aufweisen.

Weiterhin wurden in der Studie Geschäftsmodelltypen identifiziert, die den jeweiligen Betrieben besonders attraktiv erscheinen, um die Akzeptanz des IT-Sicherheitsassistenten in Handwerksbetrieben zu maximieren. Das Free-Modell wurde aufgrund seiner Eigenschaften von

keinem der befragten Betriebe für geeignet befunden, was nicht zuletzt dem Umstand geschuldet ist, dass Werbung im Kontext von IT-Sicherheit nicht den Eindruck von Seriosität des Angebots erweckt. Insbesondere Handwerksbetriebe mit größerem Budget bevorzugen das Pay-per-Use- oder Abo-Modell, da sie deren Flexibilität schätzen. Diejenigen Betriebe, die eine geringere Zahlungsbereitschaft für IT-Sicherheit aufweisen, entscheiden sich eher für den Einkauf oder das Freemium-Modell.

Im Rahmen des durchgeführten Expertenworkshops wurde ein Entwurf für ein tragfähiges Geschäftsmodell für den intelligenten IT-Sicherheitsassistenten erstellt sowie über ergänzende Serviceangebote diskutiert. Dabei wurde deutlich, dass der IT-Sicherheitsassistent nicht nur als technisches Tool, sondern als umfassende Service-Lösung wahrgenommen wird. Die Handwerksbetriebe wünschen sich bezüglich der Ausgestaltung des intelligenten IT-Sicherheitsassistenten, dass dieser sie nicht nur bei der Erhöhung der Sicherheit ihrer IT-Infrastruktur unterstützt, wie etwa durch automatische Updates, sondern auch bspw. durch Kooperationen mit Versicherungsunternehmen einen umfassenden Mehrwert erzeugt.

Es ist wichtig zu erwähnen, dass die Studie nicht frei von Limitationen ist. Zum Beispiel waren nicht alle Befragten direkt für die IT-Sicherheit in ihren Betrieben zuständig, was zu unterschiedlichen Einschätzungen geführt haben könnte. Zudem wurde hauptsächlich ein größeres Unternehmen mit hoher IT-Komplexität berücksichtigt. Die durchschnittliche Mitarbeiterzahl in der Studie liegt mit 67 deutlich über dem deutschen Durchschnitt von 10 Mitarbeitenden in Handwerksbetrieben, wodurch kleinere Betriebe möglicherweise weniger repräsentiert sind.

Impressum

Prof. Dr. Patrick Spieth
Universität Kassel

Fachbereich 07 – Wirtschaftswissenschaften

Fachgebiet Technologie- und Innovationsma-
nagement sowie Entrepreneurship

Nora-Platiel-Str. 4
34109 Kassel
Tel: +49-561-804-3055

Mail: spieth@uni-kassel.de

Website:
<https://www.uni-kassel.de/fb07/ibwl/time>

Projektwebsite:
<https://intelligent-security-handwerk.de/>
