7 Datenschutz und Datensicherheit

7.1 Beschreibung

Um die Landflucht von Jugendlichen zu unterbinden, wurden im Zuge dieser Projektarbeit unterschiedliche Ansätze vorgestellt, welche bestehende Kommunikationskanäle nutzen oder gänzlich neue Kommunikationskanäle schaffen. Da bei der Nutzung solcher Strukturen oftmals private und sensitive Daten ausgetauscht werden, ist es grundlegend, dass Datenschutz und Datensicherheit bereits bei der Planung solcher Strukturen als integraler Bestandteil angesehen und nicht als zusätzliches, im Nachhinein zu implementierendes Feature betrachtet werden.

Hierbei sind im Grunde zwei kontrahierende Ansichten zu berücksichtigen. Auf der einen Seite haben staatliche Institutionen ein Interesse daran, die in diesen Strukturen anfallenden Daten auszuwerten, um diese beispielsweise zur Verbrechensbekämpfung nutzen zu können und somit das Umfeld der Bürger sicherer zu gestalten. Auf der anderen Seite haben Bürger und insbesondere Jugendliche ein starkes Interesse daran, sensitive Informationen austauschen zu können, ohne dass es dritten Parteien möglich ist, diese einzusehen.

Es ist also äußerst wichtig, in dieser Problemstellung ein gesundes Mittelmaß zu finden. Insbesondere sollen Jugendliche sicher sein können, dass ihre Daten nicht missbraucht werden, da das Gegenteil im schlimmsten Fall dazu führen könnte, dass die neuen Strukturen nicht genutzt werden und die erarbeiteten Lösungsansätze somit nicht zur Lösung der Landflucht beitragen können.

7.2 Probleme

Um Datenschutz und Datensicherheit bereits zu Beginn in das Projekt einfließen zu lassen, müssen zunächst Teilprobleme identifiziert werden, welche zu einer Gefahr für Datenschutz und Datensicherheit werden könnten. Diese Probleme sind in der folgenden Tabelle aufgelistet und mit einem Index versehen, sodass im Folgenden eine eindeutige Zuordnung von Problemen zu Zielen erfolgen kann.

NR	Bezug	Beschreibung
P07.01	Dorf	Fehlende Richtlinien zu Datenfreigabe und Datenweitergabe an Förderer der Projekte
P07.02	Dorf	Fehlendes Bewusstsein der Jugendlichen wie sie mit persönlichen Daten umgehen müssen
P07.03	Dorf	Unsichere Kommunikationskanäle
P07.04	Dorf	Große Angriffsfläche durch eine große Anzahl von Angriffsvektoren und einer Großen Anzahl von Angreiferprofilen (Jugendliche, Script Kiddies, Fortgeschrittene, Hacker)
P07.05	Dorf	Fehlende Richtlinien zur Organisation des Patchmanagements
P07.06	Dorf	Fehlende Richtlinien zur Organisation der Wartung von Soft- und Hardware
P07.07	Dorf	Fehlendes Bewusstsein der Jugendlichen zu sicheren Passwörtern
P07.08	Dorf	Fehlende Richtlinien zur Vergabe von sicheren Passwörtern
P07.09	Dorf	Fehlende Richtlinien zur Speicherung erhobenen Benutzerdaten
P07.10	Dorf	Fehlende Richtlinien zur Absicherung von privaten digitalen Geräten
P07.11	Dorf	Fehlende Richtlinien zur Entsorgung von privaten digitalen Geräten
P07.12	Dorf	Fehlende Richtlinien zur (privaten) Internetnutzung während der Arbeitszeiten
P07.13	Dorf	Fehlende Richtlinien zur Verarbeitung von Metadaten bspw. im Kontext der Erfassung von Verbrauchsdaten (Wasser, Strom, etc.)
P07.14	Dorf	Fehlendes Sicherheitsbewusstsein der Angestellten

Es ist anzumerken, dass sich immer wieder neue Entwicklungen im Bereich des Datenschutzes und der Datensicherheit ergeben und dies zu neuen Probleme führen kann. Daher ist eine ständige Erweiterung/ Überarbeitung notwendig.

7.3 Ziele

Anhand der definierten Probleme können nun korrespondierende Ziele definiert werden (siehe Tabelle 7.3), deren Umsetzung zur Reduzierung des Problemrisikos beiträgt und somit die Etablierung von Datenschutz und Datensicherheit sicherstellt.

NR	Bezug	Beschreibung
Z07.01	P07.01	Definition von Richtlinien zur Datenfreigabe und Datenweitergabe an Förderer der Projekte
Z07.02	P07.02, P07.07	Gesteigertes Bewusstsein der Jugendlichen zum Umgang mit privaten Daten und Nutzung von sicheren Passwörtern
Z07.03	P07.03, P07.04	Absicherung der Kommunikationskanäle und der zugrundeliegenden Infrastruktur
Z07.04	P07.05, P07.06	Definition von Richtlinien zum Patchmanagement und Wartung der Soft- und Hardware
Z07.05	P07.08	Definition von Richtlinen zur Vergabe von sicheren Passwörtern
Z07.06	P07.09	Definition von Richtlinien zur Speicherung von erhobenen Benutzerdaten
Z07.07	P07.10	Definition von Richtlinien zur Absicherung von privaten digitalen Geräten
Z07.08	P07.04	Minimierung der Angriffsfläche durch Definition von Angreiferprofilen
Z07.09	P07.11	Definition von Richtlinien zur Entsorgung von privaten digitalen Geräten
Z07.10	P07.12	Definition von Richtlinien zur (privaten) Internetnutzung während der Arbeitszeiten
Z07.11	P07.13	Definition von Richtlinien zur Verarbeitung von Metadaten
Z07.12	P07.14	Förderung des Sicherheitsbewusstseins von Angestellten

7.4 Rahmenbedingungen

Bei der Umsetzung der definierten Ziele müssen Rahmenbedingungen wirtschaftlicher und technischer Art berücksichtigt werden. Diese werden im Folgenden aufgelistet:

7.4.1 Technische Rahmenbedingungen

NR	Beschreibung
T07.01	Personal zur Wartung von Informationssystemen
T07.02	Personal zur Überprüfung auf Einhaltung der Richtlinien
T07.03	Benötigte Hardware (bspw. für Hardwareverschlüsselung, mobile Geräte, Laptops, Desktop-PC, PDA)
T07.04	Benötigte Software (Verschlüsselungssoftware, Kommunikationssoftware, Schulungssoftware)
T07.05	Benötigter privater Internetzugang

7.4.2 Wirtschaftliche Rahmenbedingungen

NR	Beschreibung
W07.01	Freistellung des Budgets für benötigtes Personal
W07.02	Leitlinien zum Schutz persönlicher Daten müssen festgelegt werden
W07.03	Budget darf nicht überschritten werden
W07.04	Evtl. Budgetkürzungen durch die Stakeholder
W07.05	Kosten für benötigte Hardware
W07.06	Kosten für benötigte Software
W07.07	Zukünftig anfallende Supportkosten
W07.08	Zukünftig anfallende Kommunikationskosten
W07.09	Zukünftig anfallende Entwicklungs- / Wartungskosten
W07.10	Zukünftig anfallende Verwaltungskosten
W07.11	Versteckte betriebsbezogene Endbenutzerkosten (bspw. eigenständige Aneignung von Fachkenntnissen)
W07.12	Versteckte nicht betriebsbezogene Endbenutzerkosten (bspw. für Internetzugang)
W07.13	Einbeziehung der Bürger in die Verantwortung (Finanzierung bspw. durch freiwilliges soziales Jahr oder durch Corporate Volunteering (CV) oder durch Verwendung von Tool SOCIALPOINTS mit gleichzeitigem Sammeln von Sozialpunkten)
W07.14	Gesetzliche Regelungen zu Finanzierung und Fördermöglichkeiten

7.5 Stakeholder

An der Umsetzung und Einhaltung von Datenschutz und Datensicherheit sind verschiedene Institutionen und sowohl private, als auch juristische Personen interessiert und beteiligt. Die definierten Stakeholder haben einen unterschiedlichen Nutzen an der Umsetzung von Datenschutz und Datensicherheit, müssen sich aber auch entsprechenden Erwartungen stellen, um eine Umsetzung von Datenschutz und Datensicherheit zu ermöglichen (siehe Tabelle 7.5).

Bezug	Nutzen und Erwartungen
Datenschutzbeauftragter	Umsetzung der Datenschutzrichtlinie und dauerhafte Kontrolle auf Einhaltung der Richtlinien
Gemeinde	Offen für Umsetzung der Datenschutzrichtlinien sein und bei der Umsetzung behilflich sein
Behörden	Einhaltung der Richtlinien sowie Hilfe bei der Umsetzung der Richtlinien auf dem Land
Jugendliche	Offen für Umsetzung der Datenschutzrichtlinien sein sowie Teilnahme an Bewusstseinsförderungsmaßnahmen
Eltern	Freistellung der Jugendlichen für die Bewusstseinsförderungsmaßnahmen, sowie Teilnahme an diesen
Land- / Stadtrat	Durchsetzung der Datenschutzmaßnahmen
Bürgermeister	Durchsetzung der Datenschutzmaßnahmen
Land	Bereitstellung des benötigten Budgets
Ansässige Unternehmen	Förderung des Projekts - bspw. durch das zur Verfügung stellen von Räumlichkeiten oder Schulungspersonal für Schulungsmaßnahmen oder Hilfestellungen sowie Wartungsmaßnahmen und Weiterentwicklung von Leitlinien, ggf. Einladungen von Experten wie bspw. CHAOS-ComputerClub

7.6 Aufgaben und Rollen

Um die definierten Ziele zu erreichen, ist es notwendig, unterschiedliche Aufgaben durch verschiedene Personen zu bewältigen (siehe Tabelle 7.6). Die Stellen und deren Beschreibung sind im folgenden zu sehen:

Rollenbeschreibung	Aufgaben und Befugnisse	Fähigkeiten	Rollenbesetzung
Managementstelle	Planen, Entscheiden, Steuern, Kontrollieren, Koordinieren, Organisieren, Delegieren	Gesamtüberblick, Koordinationsvermögen, Organisationstalent, Fähigkeit Entscheidungen treffen zu können	Land, Gemeinden, Behörden, Bürgermeister, Unternehmensvertretung, Jugendliche oder Vertreter der Jugendlichen
Expertenstelle	Beratung, Kontrolle	Fachwissen, Durchsetzungsvermögen	Datenschutzbeauftragter, Digitalisierungsbeauftragter, Experte für OS und Netzwerksicherheit, Medien-Administrator (Freigabe / Zensur von Medien)
Sachbearbeiterstelle	Umsetzung, Steuerung	Koordinationsvermögen, Grundverständnis zu Datenschutz und Datensicherheit	Mitarbeiter von Behörden und Unternehmen
Ausführungsstelle	Umsetzung, Steuerung	Koordinationsvermögen, Grundverständnis zu Datenschutz und Datensicherheit	Eltern, Jugendliche

Nr	Kategorie	Bezug	Aufgabe des IM	Rollen des IM
A07.01	Planung	Z07.01 - 12	Planung des benötigten Budgets	Managementstelle
A07.02	Planung	Z07.01, 04 - 07, 09 - 11	Planung der umzusetzenden Datenschutzrichtlinien und Maßnahmen	Managementstelle, Expertenstelle
A07.03	Planung	Z07.02	Planung der Bewusstseins steigernden Maßnahmen für Jugendliche	Managementstelle, Expertenstelle
A07.04	Entscheidung	Z07.01-12	Entscheiden wie viel Budget zur Verfügung stehen wird	Managementstelle
A07.05	Entscheidung	Z07.01, 04 - 07, 09 - 11	Entscheiden welche Datenschutz- und Datensicherheitsrichtlinien umgesetzt werden sollen	Managementstelle, Expertenstelle
A07.06	Entscheidung	Z07.02	Entscheiden welche Bewusstseins fördernde Maßnahmen umgesetzt werden sollen	Managementstelle, Expertenstelle
A07.07	Steuerung	Z07.01, 04 - 07, 09 - 11	Sicherstellung der korrekten Umsetzung der Datenschutz und Datensicherheitsrichtlinien	Sachbearbeiterstelle, Ausführungsstelle
A07.09	Steuerung	Z07.02	Sicherstellung der korrekten Umsetzung der Bewusstsein fördernden Maßnahmen	Sachbearbeiterstelle, Ausführungsstelle
A07.09	Kontrolle	Z07.01 - 12	Kontrolle der Einhaltung des Budgets	Managementstelle
A07.10	Kontrolle	Z07.01, 04 - 07, 09 - 11	Kontrolle der korrekten Umsetzung der Datenschutz und Datensicherheitsrichtlinien	Managementstelle, Expertenstelle
A07.11	Kontrolle	Z07.02	Kontrolle des Erfolgs der Bewusstseins fördernden Maßnahmen	Managementstelle, Expertenstelle

7.7 Werkzeuge

Zur Erfüllung der oben definierten Aufgaben müssen die im folgenden aufgelisteten Werkzeuge durch die zuständigen Rollen verwendet werden.

Bezug	Werkzeuge
A07.01	Kostenkalkulation (Anschaffungskosten + Betriebskosten + Stundenlohn * Stunden * MA-Anzahl)
A07.02	Gesetzesentwürfe, Richtlinien und Best Practices (bspw. ISO 2700X, BSI-Grundschutz)
A07.03	Best Practises (bspw. BSI-Grundschutz)
A07.04	Kosten-Nutzen-Analyse (siehe Abschn. 7.11, 7.12)
A07.05	Kosten-Nutzen-Analyse (siehe Abschn. 7.11)
A07.06	Kosten-Nutzen-Analyse (siehe Abschn. 7.12
A07.07	Kennzahlen durch Metriken (z.B. Anzahl der erfolgreichen Cyber-Angriffe innerhalb eines Jahres)
A07.08	Fragebögen (Auswertung der Sensibilität von Jugendlichen zum Thema Datenschutz)
A07.09	Kostenaufstellung (alle Ausgaben sowie Schätzung zukünftiger Ausgaben sowie Abgleich mit Budgetplanung)
A07.10	Kennzahlen durch Metriken (z.B. Anzahl der erfolgreichen Cyber-Angriffe innerhalb eines Jahres)
A07.11	Kennzahlen durch Metriken (z.B. Anzahl der erfolgreichen Cyber-Angriffe auf Privatpersonen innerhalb eines Jahres), Fragebögen (Auswertung der Sensibilität von Jugendlichen und Mitarbeiter zum Thema Datenschutz)

7.8 Strategien, Maßnahmen und Wirkungen

Im Folgenden erfolgt die Definition von Strategien, der Maßnahmen, welche zu deren Umsetzung dienen sollen und der Wirkungen, welche durch die Umsetzung der Strategien erreicht werden soll.

7.9 Strategien

- Bereitstellung von Richtlinien zur Sicherung von Datenschutz und Datensicherheit durch öffentliche Organisationen wie Gemeinden und Behörden

- Entwicklung eines Sicherheitsbewusstseins auf Seiten der Jugendlichen

7.9.1 Maßnahmen

- Entwicklung der Richtlinien auf Basis von ISO-2700X und BSI-Grundschutz
- Zusammenstellung von leicht verständlichen Informationen für verschiedene Zielgruppen in Abhängigkeit von Altersklassen (Jugendliche, Eltern, Senioren, etc.) bezüglich der Not- wendigkeit und Sicherstellung von Datenschutz und Datensicherheit
- von Schulungen zur Förderung des Sicherheitsbewusstseins der Jugendlichen

7.9.2 Wirkung

- Zum aktuellen Zeitpunkt bestehende Kommunikationskanäle (Smartphones, Laptops, etc.), sowie neu entstehende Kommunikationskanäle (Implantate, Mikrochips, Sensornetzwerke, etc.) werden entsprechend gesichert
- sensitive und persönliche Daten (bspw. Namen, Adressen, Personalausweise, Kontodaten, Kreditkarten, Bilder und Videos) werden sicher verwahrt
- Konformität mit ISO 2700X und BSI-Grundschutz
- Jugendliche entwickeln ein Sicherheitsbewusstsein durch Anwendung des Wissens um Cy- berangriffe, Viren, Trojaner, Einbruchsmöglichkeiten, Verfälschungen etc.
- Jugendliche nutzten die neu etablierten Kommunikationskanäle

7.10 Anforderungen an das IM

Die Umsetzung des Projekt stellt verschiedene Anforderungen an das zugrunde liegende Infor- mationsmanagement, welche im folgenden beschrieben werden.

7.10.1 Planung und Entscheidung

- Definition und Umsetzung der Richtlinien auf Basis von ISO2700X und BSI-Grundschutz

- Erstellen eines Flyers für Jugendliche über personenbezogene Daten und das Wählen von sicheren Passwörtern (A07.03)
- Erstellung eines Videos zur Sensibilisierung der Jugendlichen zum Thema personenbezo- gene Daten (A07.03)
- Organisation von Diskussionsforen, wie bspw. der Besuch des "Chaos Computer Clubs„ oder„der "Piraten (A07.03,04)
- Organisation von Exkursionen zu Cyberabwehrzentren oder zum BSI (A07.03,04)

7.10.2 Steuerung und Kontrolle

- regelmäßige Überprüfung der definierten Richtlinien auf Aktualität (bspw. durch Konsul- tierung der entsprechenden Standards oder Berichte über aktuelle Hacking-Angriffe)
- regelmäßige Umfragen unter den Jugendlichen bzgl. der Nutzung von Kommunikations- kanälen
- Führung von Statistiken bzgl. der Verwendung der technischen Kommunikationskanäle
- Verwendung von IDS/IPS-Systemen zur Erkennung von potentiellen Angriffen und so- mit Ableitung von Kennzahlen bzgl. fehlgeschlagener Angriffe (Abgleich der Anzahl von erfolgten, mit (nicht) erfolgreichen Angriffen)
- Durchführung von Schulungen für Angestellte und Jugendliche zur Sensibilisierung zu dem Thema IT-Sicherheit
- Durchführung von Schulungen für Angestellte und Jugendliche zur Sensibilisierung zu dem Thema Datenschutz
- Durchführung von Schulungen für Jugendliche zu dem Thema Umgang mit personenbe- zogenen Daten
- Veranstaltung von Videoclip-Wettbewerben zur Findung und Veröffentlichung guter Vi- deoclips zu den Themen Datenschutz und Datensicherheit
- Kontrolle des Erfolgs der Schulungsmaßnahmen durch Kennzahlen (bspw.

Anzahl ange- botener Kurse im Verhältnis zur Anzahl Teilnehmer)

7.11 Kosten-Nutzen-Analyse (Staatliche Seite)

Cyber-Angriffe führen neben Systemausfällen und Betriebsunterbrechungen häufig zu Image- schäden. Da im gegebenen Kontext keine Produktivsysteme oder (direkt) Geldwert- schöpfende Systeme zum Tragen kommen, ist ein Imageschaden

als deutlich höheres Risiko als eine Sys- temunterbrechung oder ein Systemausfall einzustufen.
Ein entsprechender Imageschaden, auf- grund von beispielsweise abgefangener Kommunikation oder dem Abgreifen sensitiver Daten,

könnte die Jugendlichen dazu veranlassen, dass Vertrauen in die entsprechenden Kommuni- kationskanäle zu verlieren und somit deren Nutzung einzustellen. Da sich speziell Jugendliche in Gruppen und Cliquen organisieren, würden augenblicklich mehrere Nutzer entfallen, was schlussendlich dazu führen könnte, dass die neu etablierten Kommunikationskanäle ungenutzt betrieben werden, wodurch sämtliche für diesen Kontext aufgebrachten Gelder unnütz würden. Da die Erholung von einem Imageschaden tendenziell sehr schwierig ist, lange dauert und mit hohen Kosten verbunden ist, kann festgehalten werden, dass entsprechende Richtlinien einen hohen Nutzen einbringen.

In der Praxis geschieht die Einführung solcher Richtlinien meist in Form eines nach ISO/IEC
27001 standardisierten ISMS (Information Security Management Systems), welches zum Ziel hat, die Informationssicherheit innerhalb einer Organisation dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern. Die Einführung eines ISMS dauert durchschnittlich zwischen 12 bis 18 Monaten und ist häufig mit Kosten in Millionenhöhe verbunden. Dies resultiert zum einen daraus, dass ein solches Vorhaben mit entsprechendem Personalaufwand verbunden ist (Fachkräfte, Schulungen, Einbeziehung aller Abteilungen, etc.), zum anderen werden aber auch häufig in dieser Thematik erfahrene, externe Berater benötigt, welche ein entsprechendes Honorar verlangen. Eine genaue Bezifferung der Kosten ist allerdings schwierig, da diese von der entsprechenden Behörde, deren Anzahl an Mitarbeitern, der eventu- ell bereits teilweise etablierten Sicherheitsstruktur und den möglicherweise benötigten externen Beratern abhängig sind. Als Faustformel für die Bezifferung der Kosten kann folgende Darstel- lung herangezogen werden:

Kosten für Mitarbeiterzeit * Anzahl benötigter Mitarbeiter + Kosten für

Fachliteratur und Schulung + Kosten für externe Unterstützung + Kosten für die Technologie + Kosten für die Zertifizierung

7.12 Kosten-Nutzen-Analyse (Bürgerliche Seite)

7.12.1 Informationsbroschüren

Es sollten zur Steigerung des Bewusstseins der Jugendlichen im Bezug auf personenbezogene Daten und sichere Passwörter Informationsbroschüren erstellt werden. In Rheinland-Pfalz leben rund 120000 Jugendliche im Alter zwischen 15 und 18 Jahren. Pro Informationsbroschüre sollten demnach rund 125000 Stück bedruckt werden. Bei 2 Informationsbroschüren sind das insgesamt
250000 Exemplare. Nach der Webseite flyeralarm.com kosten 50000 DIN A4 Flyer 944,34 Euro
Brutto. Bei 250000 Stück macht das insgesamt 4721,70 Euro. Auf einen angesprochenen Jugend- lichen wären das rund 0,04 Euro. In einer Umfrage auf statista.com sind 2017 rund 5 Prozent
der Befragten schon einmal Opfer eines Identitätsdiebstahls durch Cyberkriminalität geworden. Nicht selten, ist der Schaden bei einem Identitätsdiebstahl mit mehreren 1000 Euro beziffert, wodurch diese Maßnahme rentable wäre und dem Ende der Privatheit entgegen wirken würde.

7.12.2 Nutzung von sicherer Software

Als zusätzliche Schutzmaßnahmen gegen Cyberkriminalität ist außerdem zu empfehlen, sichere
Software zu verwenden. Hierzu
gehören bspw:

- Die Verwendung von HTTPS statt HTTP wo möglich (bspw. durch HTTPS-Everwhere)
- Die Verwendung von Werbeblockern (bspw. AdBlock-Plus)
- Die Verwendung von Anti-Tracking-Tools (bspw. Ghostery, Disconnect)
- Die Verwendung von Cookie-Managern oder das generelle Blocken von Cookies
- Regelmäßiges Einspielen von Patches und Updates
- Verwendung von alternativen Suchmaschinen (bspw. DuckDuckGo)

Die Nutzung dieser Software ist für den Endnutzer kostenfrei, reduziert aber die Wahrschein- lichkeit Opfer eines Identitätsdiebstahls durch Cyber-Kriminalität zu werden. Da der Schaden eines Identitätsdiebstahls wie bereits angedeutet mehrere Tausend Euro betragen kann, kann dies als kostengünstige, lohnende Maßnahme betrachtet werden.

7.12.3 Erstellung und Verbreitung der Videos zur Steigerung des Sicherheitsbe- wusstseins der Jugendlichen

Um Videos zur Sensibilisierung sowie Steigerung des Bewusstsein der Jugendlichen zum Um- gang mit personenbezogenen Daten sowie dem Gebrach von sicheren Passwörtern werden zwei Mitarbeiter für rund zwei Tage benötigt. Ein Sachbearbeiter im öffentlichen Dienst verdient im Durchschnitt rund 160 Euro Brutto pro Tag, woraus für die benötigten Arbeiten Kosten in Höhe von 640 Euro Brutto entstehen. Diese Kosten entstehen einmalig, woraus aber ein dauerhafter Nutzen entstehen kann.

7.12.4 Durchführung von Schulungen zur Steigerung des Sicherheitsbewusstseins der Jugendlichen

Um eine große Anzahl von Jugendlichen zu erreichen, ist es sinnvoll eine Vielzahl von Schulungen anzubieten. Um dies zu ermöglichen sollte auf geschulte interne Mitarbeiter zurückgegriffen wer- den. Pro Schulungstermin können rund 60 Jugendliche Teilnehmen. Eine Schulung würde rund
2 Stunden dauern. Um alle Jugendliche zu erreichen müssten 2000 Schulungen von je 2 Stun- den durchgeführt werden. Insgesamt sind somit 4000 Stunden (exklusive der Erstellungskosten für die Schulungsmaterialien) zu berechnen. Bei einem durchschnittlichen Stundenverdienst von
20 Euro, wären die Schulungskosten auf 80000 Euro zu datieren. Diese Schulungsmaßnahmen müssten alle 3 Jahre wiederholt werden. Woraus sich diese Kosten multiplizieren. Es wäre ein sinnvoller Beitrag im Zuge des geforderten CSR.

7.13 Fazit

Die Erstellung von Richtlinien zu Datenschutz und Datensicherheit sowie deren Einführung und Durchsetzung im betrieblichen Alltag sind mit hohem Zeitaufwand und entsprechenden Kosten verbunden. Außerdem sind die vorliegenden Richtlinien eher als Basis zu verstehen und bilden noch keine ganzheitliche Lösung zur Sicherung von Datenschutz und Datensicherheit, da diese erst mit Hilfe eines ganzheitlichen Ansatzes

in Form eines ISMS erreicht werden kann. Trotzdem trägt bereits die Sensibilisierung der Jugendlichen im Bereich Datenschutz und Datensicherheit sowie die grundlegende Bereitstellung von Richtlinien dazu bei, ein entsprechendes Grundbewusstsein für die gegebene Thematik zu schaffen.

Durch die Bereitstellung von Richtlinien auf der staatlichen Seite und die Schaffung eines Sicherheitsbewusstseins auf der bürgerlichen Seite, wird ein dualer Ansatz verfolgt, welcher die Sicherheit von bestehenden und neu entstehenden Kommunikationskanälen fördert. Auf diese Weise tragen Datenschutz und Datensicherheit ihren Teil dazu bei, dass die neu etablierten Kommunikationsstrukturen genutzt werden und das Heimatbewusstsein der jugendlichen gefördert wird. Frei nach dem Motto: „Mein Land - Meine Heimat - Mein Dorf“ werden somit soziale Strukturen gebildet und gefördert, welche Jugendliche dazu veranlassen, ihr Dorf als ihren Lebensmittelpunkt wahrzunehmen und somit von einer Abwanderung abzusehen.

Die vorgegebenen Richtlinien sollten in regelmäßigen Abständen durch Prüfung der definierten Kennzahlen auf ihre Wirkung hin geprüft werden. Dies sollte durch Gremien geschehen, in welchen Vertreter von sämtlichen Stakeholdern zugegen sind. Innerhalb dieser Gremien sollten des weiteren Entscheidungen zu weiteren Maßnahmen getroffen werden, falls diese Richtlinien zu überarbeiten oder anzupassen sind.