UNIVERSITÄT
BIELEFELD

Informationssicherheit an der Universität Bielefeld

Ergebnisse einer Umfrage unter Bediensteten

Kurt Salentin
Institut für interdisziplinäre Konflikt- und Gewaltforschung · Universität Bielefeld

Sebastian Strauß
Forschungsinstitut für Kognition und Robotik · Universität Bielefeld

März 2020

Inhalt

Empfohlene Zitierweise

Salentin, Kurt; Strauß, Sebastian (2020): Informationssicherheit an der Universität Bielefeld: Ergebnisse einer Umfrage unter Bediensteten. Universität Bielefeld, Institut für interdisziplinäre Konflikt- und Gewaltforschung und Forschungsinstitut für Kognition und Robotik.

Kontakt:

Kurt Salentin: kurt.salentin@uni-bielefeld.de
Sebastian Strauß: sebastian.strauss@uni-bielefeld.de

0 Executive Summary

Die Einschätzung des Schutzbedarfs der verschiedenen in der Universität Bielefeld (UniBie) verarbeiteten Daten bildet den ersten Aspekt der Informationssicherheitskompetenz (IS-Kompetenz). Sie schwankt erheblich. Sie hängt einerseits von der Datenkategorie ab. Dabei entspricht sie in der Tendenz deren juristischer Einstufung: Personenbezogene Daten (von Studierenden, Bediensteten und Forschungssubjekten) werden als schutzwürdiger bewertet als anonyme Daten. Sie variiert aber auch zwischen Personalkategorien. Vergleichbare Daten werden in der Verwaltung als schutzwürdiger betrachtet denn in Forschung und Lehre.

Als wichtiger Indikator der IS-Kompetenz der Bediensteten hat sich die Selbsteinschätzung erwiesen. Die subjektive Einschätzung der Informationssicherheits-Kompetenz korrespondiert in allen Belangen zuverlässig mit berichtetem Verhalten und Kenntnissen. Anfänger erkennen weniger Daten-Schutzbedarf, begehen mehr Sicherheitsverstöße und kennen sich mit Gefahren für die IS schlechter aus.

Mit der aktuellen Verteilung der Kompetenz kann die UniBie nicht zufrieden sein. Über ein Drittel der Bediensteten arbeitet auf Anfängernïnnenveau. Die Kategorie der *Ahnungslosen*, die nicht einmal den Begriff der Daten-/Informationssicherheit kennen, darf es an einer Universität nicht geben.

Die Angebote der UniBie werden über alle Personalkategorien hinweg als verbesserungsbedürftig wahrgenommen. Erhebliche Teile der Befragten wünschen mehr Informationen zu Datenschutz und Informationssicherheit. Es besteht Unsicherheit im Umgang mit Sicherheitsproblemen, Zuständigkeiten sind nicht geläufig. Die teils vorhandenen Angebote sind offenbar zu wenig bekannt und sollten offensiver beworben werden.

Bei Führungskräften in der Wissenschaft besteht von allen Personalkategorien der größte Kontrast zwischen Sicherheitserfordernissen und praktischem Handeln. Sie verhalten sich riskanter als andere Gruppen. Sie beklagen einen Zielkonflikt zwischen den Sicherheitsvorgaben der Universität auf der einen Seite und den Erfordernissen effizienter Arbeit und internationaler Gepflogenheiten auf der anderen Seite. Massive Anstrengungen sind notwendig, um Wissenschaftlerïnnen mit Tools und Diensten zu versorgen, die sowohl die durch kommerzielle Dienste geweckten Erwartungen erfüllen als auch mit Datenschutz- und -sicherheitserwägungen kompatibel sind.

Die Erhöhung der IS-Kompetenz kann in Organisationen grundsätzlich über zwei verschiedene Zugänge erfolgen: über persönliche Erfahrungen bzw. Einstellungen der Beschäftigten sowie über die Unternehmenskultur in Bezug auf Datensicherheit. Aus der Datenlage geht hervor, dass für die Gesamteffektivität der organisatorischen Sicherheit der UniBie hauptsächlich ersteres, die individuellen Faktoren der Beschäftigten, von wesentlicher Bedeutung ist. Eine Erhöhung der Sicherheit durch das Aufstellen von Leitlinien und Sicherheitsanweisungen ist hier also nicht ausschlaggebend.

Die Ergebnisse zeigen vielmehr, dass individuelle Kompetenzen der Beschäftigten die Anzahl der eingegangen Sicherheitsrisiken verringern. Das Zurückgreifen auf die eigenen oder von der Universität zur Verfügung gestellten Ressourcen stellt den größten Einfluss bei der Vermeidung von Risikoverhalten dar. Eine Stärkung der individuellen Kompetenz durch bspw. regelmäßige Schulungen, verfügbare Hard- und Software-Lösungen oder Aufklärung über aktuelle Risiken erweist sich den erhobenen Daten zufolge als wichtigster Faktor zur Einhaltung der Informationssicherheit.

1 Hintergrund und Ziele

Die Digitalisierung der Welt hat der empirischen Forschung neue Horizonte erschlossen und Akzente verschoben. Neue Disziplinen wie die *Digital Humanities* sind entstanden. Zunächst nur Mittel zum Zweck, haben wissenschaftliche Daten längst einen eigenständigen Wert erlangt, der mit ihrer instrumentellen Bedeutung für die Erkenntnisgewinnung korrespondiert. Dabei sind Daten das Produkt gezielter Investitionen, da sie meist nur mit erheblichem ökonomischen Aufwand beschafft werden können. Sie verheißen den Besitzern mittelbar Vorteile – auch ökonomische – in einem Wettbewerb, der unter Universitäten und anderen forschenden Akteurïnnen, etwa in der Wirtschaft, geführt wird. Publikationen, Patente, Reputation, Forschungspreise, Forschungsmittel und andere finanzielle Anreize sind Währungen, in denen forschende Individuen und Institutionen vergütet werden. Daten sind damit zu einem ebenso wichtigen Produktionsmittel der Wissenschaft geworden wie Fachpersonal, Knowhow und Literatur. Dieses Produktionsmittel ist Gefahren ausgesetzt.

Zeitgleich mit dieser Entwicklung findet eine Digitalisierung der Verwaltung statt, die in Universitäten so weit fortgeschritten ist wie in anderen Organisationen. Digitale Studierenden-, Personal- und Finanzdaten gehören zur Substanz der Universität. Geraten sie in Gefahr, sind die Organisationsziele bedroht.

Die Digitalisierung verändert auch die Kommunikation, denn gegenüber der digitalen Kommunikation hat die analoge an Bedeutung verloren. Sie erzeugt ihre eigenen Risiken, denn neuartige illegitime Zugriffe auf digitale Informationen sind möglich geworden.

- In Zeiten des Briefs, des Telefonats und der persönlichen Vorsprache war die *Identitätsfeststellung* des Gegenübers ungleich trivialer als beim Austausch von E-Mails – wenngleich es etwa viele Varianten des Trickbetrugs immer gegeben hat. Ganz gleich, ob E-Mail, SMS, Social-Media-Post oder Instant-Messaging: Den wahren Absender eine digitalen Nachricht festzustellen, ist mit hohem Aufwand verbunden und in vielen Alltagssituationen praktisch unmöglich.
- Sichere Informationsspeicherung gründete sich früher auf physische Barrieren wie dicke Mauern, verschlossene Türen und Wachpersonal, sicherer Transport auf zuverlässige, oft bewaffnete Boten, Siegellack und dergleichen. Gewiss konnte man auch sie überwinden,

doch ist eine neue Qualität der Unsicherheit erreicht, seit digitale Medien prinzipiell jederzeit weltweit jede Information erreichen, ganz gleich ob sie statisch gespeichert vorliegt oder gerade bewegt wird. Man kann sie stehlen, ohne sich in die physische Nähe des/der legitimen Besitzerïn zu bewegen. Digitale Schutzmauern sind nie undurchdringbar, und viele Datenbestände schützt nicht mehr als die hauchdünne Membran eines Passworts vor der Welt.

- Fast erübrigt es sich darauf hinzuweisen, welches Gefahrenpotenzial die *Stoffungebundenheit* digitaler Information mit sich bringt. Für den Missbrauch analoger Information war ein aufwendiger Medienbruch, etwa eine Kopie, Fotografie oder Bandaufzeichnung, erforderlich, wenn eine Angreiferïn sie nicht physisch erbeutete. Um die Kundïnnenkartei eines Großunternehmens zu stehlen, hätten Diebe mit einem Laster vorfahren müssen. An die Kundïnnendatei gelangt, wer eine unscheinbare Sicherheitslücke auszunutzen versteht. Datenlecks lassen sich in Windeseile nutzen und hinterlassen oft keine Spuren.

Zeitgleich mit den vielen Vorteilen, die die Digitalisierung unzweifelhaft besitzt, erzeugt sie deshalb in erheblichem Umfang neue Risiken. Wenn Daten verloren gehen, unverfügbar oder verfälscht werden und in falsche Hände geraten, drohen Reputationsverlust, Wettbewerbsnachteile, finanzielle Einbußen und auch, aber nicht nur, bei Daten mit Personenbezug, juristische Weiterungen. Die digitalisierte Kommunikation hat neben technischen Risiken auch Angriffsflächen für nichttechnische Angriffe durch Akteurïnnen geschaffen, die das Potential universitärer Daten unerlaubt für eigene Zwecke nutzen wollen. Phishing-Angriffe auf Organisationen und ähnliche Social-Engineering-Techniken sind heute an der Tagesordnung. Sie nutzen menschliche Schwächen, um technische Barrieren zu überwinden. Wehrhaftigkeit gegenüber solchen Angriffen kann sich daher nicht auf technische Maßnahmen beschränken, sie muss auch das Bewusstsein und die Kompetenz der handelnden Menschen, die *information security awareness (ISA)*, im Blick haben. Dies ist der Gegenstand des vorliegenden Berichts. ISA besteht aus Kenntnissen, Kompetenzen und Orientierungen, die jenseits technischer Schutzschichten liegen (zur genauen Begriffsbestimmung siehe Kapitel 9) und die nicht einfach mit den Mitteln formeller Regelwerke hergestellt werden können. Defizite der ISA führen zu problematischem Sicherheitshandeln. Die Informationssicherheitsforschung nutzt deshalb in den letzten Jahren Erkenntnisse und Techniken der Psychologie und der Sozialwissenschaften, um die Rolle des menschlichen Faktors in der Informationssicherheit zu beleuchten. In den USA und in einigen asiatischen Ländern hat diese Forschung eine gewisse Tradition, während sie in der Bundesrepublik noch in Kinderschuhen steckt.

Der Schwerpunkt der bisherigen Studien liegt auf akteursbezogenen Aspekten, und Informationssicherheit wird als Resultat individueller Einstellungen und Handlungen verstanden. Dabei wirkt sich jedoch, so die Annahme, auch der soziale Kontext aus. Vorgesetzte und Kollegïnnen etablieren eine spezifische *Kultur* der Informationssicherheit, die mehr oder weniger internalisiert und handlungswirksam wird. Die spezifische Struktur der Organisation thematisieren die Studien dabei nicht. Zweifel an der Gültigkeit bisheriger Forschungsbefunde ergeben sich aus dem Um-

stand, dass nur Firmen betrachtet wurden - wenngleich dies verständlich ist, weil Unternehmen als Ziel der Datenspionage schon früh ins Blickfeld geraten sind. Es fehlt dagegen an Untersuchungen, die die Universität als spezielle Erscheinungsform der Organisation ernst nehmen.

Den Autoren sind keine organisationswissenschaftlichen Studien zu den Besonderheiten der Informationssicherheit an Universitäten bekannt. Gleichwohl lassen langjährige persönliche Erfahrung auf ungünstige Rahmenbedingungen der Informationssicherheit an einer Universität schließen:

- Die Struktur einer Universität ist komplex, mit einer hierarchisch aufgebauten Zentralverwaltung neben teilautonomen Untersystemen (Fakultäten, Institute), in denen wiederum Lehrstühle wie kleine Unternehmen (böse Zungen sprechen auch von Fürstentümern) ohne Weisungsbindung Forschung betreiben. Die deutschen Universitäten haben inzwischen meist die Rolle der/des Informationssicherheitsbeauftragten (ISB) unterhalb der Leitungsebene etabliert. Daneben weisen manche Universitäten Prorektorïnnen (oder Vizepräsidentïnnen) für Digitales, Informationsmanagement, Informationsinfrastruktur etc. aus, die dann auch die Belange der Informationssicherheit vertreten können. Ihr Einfluss ist jedoch nicht mit IT-Vorständen oder Chief-Information-Officers (CIOs) großer Unternehmen vergleichbar. Der ISB ist mit Planung, Koordination, Beratung, Regelwerkentwicklung und Monitoring beauftragt, kann jedoch nicht sanktionieren. Die Weisungsbefugnis des Rektorats bzw. Präsidiums gegenüber der Verwaltung ist zwar unstrittig. Die wichtigsten Datenproduzentïnnen, die Professorïnnen, haben aber nicht nur in der Gruppenuniversität der 1970er Jahre der Universitätsleitung gegenüber die Forschungsfreiheit nach Art. 5 Grundgesetz auf ihrer Seite. Auch dem Hierachisierungsspielraum der jüngeren Länderhochschulgesetze sind durch die Rechtsprechung des Bundesverfassungsgerichts enge Grenzen gesetzt. Eine Einwirkung auf Professorïnnen, die sich in der Informationsverarbeitung Freiheiten herausnehmen, gestaltet sich daher sehr schwierig. Beinahe resignierend schreibt Renate Lieckfeldt (2011) über die Durchsetzungsfähigkeit eines Rektorats: „Im Hochschulbereich ist Bitten das Mittel der Wahl“. Zu allem Übel sind die Akteurïnnen der Informationssicherheit in den dezentralen Gliederungen (Fakultäten, Institute) meist kleine Rädchen im großen Getriebe, von denen sich die „Halbgöttïnnen der Forschung“ keine Vorschriften machen lassen.
- Universitäten haben seit den 1970er Jahren, also früher als die meisten Firmen und Gebietskörperschaften, eine eigene Informationstechnik-Infrastruktur herausgebildet, deren historisch gewachsener Aufbau aber in der Regel nicht wie in einem Unternehmen konsistent dem Controlling unterzogen und ggf. neustrukturiert wird. Hard- und Softwarearchitekturen sind heterogen und unstandardisiert und leichter angreifbar, weil es für Teile des Gesamtgefüges an spezialisierten IT-Sicherheitsrollen fehlt. Es mangelt neben eindeutig geregelten Kompetenzen oft auch an den nötigen Ressourcen. Die Tarifstruktur des öffent-

lichen Dienstes benachteiligt Universitäten als Arbeitgebende auf einem Bewerberïnnenmarkt.

- Die wissenschaftliche Forschung weist eine hohe Personalfluktuation auf; sie hält sich zudem offen gegenüber der Lehre und der Öffentlichkeit und vernetzt sich aus guten Grund regional und international, so dass die Grenzen der Organisation in allen Richtungen leicht verschwimmen.
- Mit seiner gering ausgeprägten funktionalen Differenzierung gleicht ein Daten erhebender und verarbeitender Lehrstuhl eher einem Kleinst-Handwerksbetrieb, in dem der/die Meisterïn selbst Hand anlegt, als einer hochgradig differenzierten industriellen oder bürokratischen Organisation. Diese Struktur wird zwar den unmittelbar fachlichen Anforderungen der Forschung leidlich gerecht, büßt aber Leistungsfähigkeit in den notwendigen Nebenkompetenzen einer technisierten und verrechtlichten Wissenschaft ein, zu denen die Informationssicherheit und der Datenschutz neben vielen anderen gehören. Trotz der beachtlichen Größe der Gesamtorganisation kann die Universität in ihrem Inneren die Vorteile einer Arbeitsteilung und Spezialisierung in diesen Aufgabenfeldern nicht zum Tragen bringen.
- Die Datenschutzgesetzgebung trägt nicht zur Vereinfachung der Zuständigkeiten bei, da sie die Verantwortung für Verwaltungsdaten und für Forschungsdaten unterschiedlichen Instanzen zuweist. Für die zentralen Aspekte der Informationssicherheit – Operationalisierung, Monitoring, Implementation, Sanktionierung, Schulung etc. - fehlt eine gesetzliche Regelung völlig. Die Universitäten zwingt dieser Umstand, eigene Verantwortungs- und Kompetenzstrukturen und Regelwerke für die Informationssicherheit zu entwickeln und durchzusetzen. Ein Flickenteppich entsteht. Das Fehlen einer verbindlichen normativen Grundlage der Informationssicherheit ist mit dafür verantwortlich, dass diese in der Wahrnehmung nicht den gebührenden Platz einnimmt. In der Folge nehmen wichtige Akteurïnnen auf allen Hierarchieebenen einen Zielkonflikt zwischen ihr und dem Datenschutz einerseits und Produktivität andererseits wahr: Informationssicherheit gilt als lästig.
- Die Generation der aktuell führenden Wissenschaftlerïnnen hat sich ihre IT-Kompetenz noch überwiegend autodidaktisch angeeignet. Es steht zu befürchten, dass sie mit den Risiken der Digitalisierung bislang eher sorglos bis fahrlässig umgeht.
- In der Ausbildung des wissenschaftlichen Nachwuchses spielt die Informationssicherheit bislang keine Rolle. Obwohl erste Studiengänge in Informationssicherheit angeboten werden, fristet die Disziplin außerhalb der Informatik bisher allenfalls ein Schattendasein. Angesichts der in der Breite der Disziplinen voranschreitenden Verlagerung zu evidenzbasierter Erkenntnisgewinnung überrascht es, dass es der Eigeninitiative Studierender überlassen bleibt, ob sie basale Informationsnutzungskompetenzen erwerben. Von einer Kanonisierung von Ausbildungsinhalten in den Studiengängen der anwendenden Wissenschaften

ist keine Spur. Immerhin besteht die Aussicht auf eine vertiefende Kompetenzbildung in Data-Science-Zentren und -Studiengängen. Wenn sie neben ihrem Kerngeschäft, der Analyse, auch Sicherheitsaspekte behandeln und sich mit der fachlichen Anwendung in anderen Disziplinen verschränken, können sie der Informationssicherheit Antrieb verleihen.

- Weiterbildungsangebote für Beschäftigte existieren, müssen aber popularisiert werden, da sie kaum bekannt sind und nicht großflächig angenommen werden.

Man kann resümieren: Die Informationssicherheit findet an Universitäten keine optimalen Voraussetzungen vor. Derzeit ist deshalb unklar, wie es um die Informationssicherheitskompetenz des Personals bestellt ist und wie sich die Praxis gestaltet.

Vor diesem Hintergrund haben wir Bedienstete der Universität Bielefeld befragt, um einen ersten Eindruck von der Lage an einer deutschen Hochschule zu gewinnen. Wir wollen wissen,

- mit welchen Daten gearbeitet wird,
- welche Gefährdung und welcher Schutzbedarf wahrgenommen wird,
- welche Informationssicherheitskultur besteht, d. h. welche Einstellungen und Erfahrungen vorliegen,
- wie der Alltag der Informationssicherheit aussieht,
- welches Risikoverhalten zu beobachten ist,
- wie die Eigenkompetenz in der Informationssicherheit eingeschätzt wird,
- wie die Versorgung mit Informationssicherheitsressourcen durch die Universität bewertet wird.

Diese Erkenntnisse sollen in den inneruniversitären Diskurs einfließen und Anstöße zur Organisationsentwicklung geben.

2 Methode

Diesem Bericht liegen Daten einer Umfrage unter allen Bediensteten der Universität Bielefeld aus dem Frühjahr 2019 zugrunde.

Der Fragebogen setzt sich aus Elementen früherer Studien und Eigenentwicklungen der Autoren zusammen. Er umfasst die Themenbereiche

- dienstlicher Kontakt mit Daten, Einschätzung der Gefährdung der Daten,
- Wahrnehmung der Angebote der Universität zur Datensicherheit,
- die Nutzung von Online-Diensten,
- die Praxis der Datensicherheit am Arbeitsplatz einschließlich der Informationssicherheitskultur,

- die Einschätzung des Gefahrenpotentials von Malware (malicious software)
- sowie einige Angaben zur Rolle der Person in der Organisation.

Eine Druckfassung des Fragebogens befindet sich im Anhang.

Die sonst gebräuchlichen Angaben zur Soziodemographie der Befragten haben wir im Interesse der Akzeptanz der Studie nicht erhoben; die Teilnehmerïnnen sollten die Gewissheit besitzen, sich in einem sensiblen Bereich als Individuen nicht identifizierbar zu machen. Den Eindruck einer Kompetenz- oder Leistungskontrolle wollten wir um jeden Preis verhindern. Daher ist es mangels Daten im Folgenden ausgeschlossen, statistische Zusammenhänge mit Alter, Geschlecht, Qualifikation oder auch der Zugehörigkeit zu einer bestimmten Organisationseinheit (Dezernat, Fakultät, Institut) zu untersuchen. Insgesamt wurden 95 Einzelfragen in 15 Gruppen gestellt. Es handelte sich durchweg um geschlossene Antwortformate, zumeist um vier- oder fünfteilige Zustimmungsskalen (Likertskalen). Wo wir während der Vorarbeiten und im Pretest (s. u.) auf die Möglichkeit stießen, dass einzelne Befragte aus nachvollziehbaren Gründen keine Antwort würden geben können, haben wir die Antwortskala um die Option „weiß nicht“ ergänzt.

Geschlossene Frageformate bilden allein den Relevanzrahmen der Forschenden ab und lassen den Befragten wenig Raum, weitergehende Gesichtspunkte zur Sprache zu bringen – ein bekannter Nachteil quantitativer Forschungsmethoden. Darum haben wir an das Ende des Fragebogens die Gelegenheit zur Rückmeldung in einem Freitextformat eingebaut. Die zahlreichen Kommentare, die an diesem Ort eingingen, helfen die quantitativen Befunde zu verstehen. Wir gehen auf sie in einem eigenen Kapitel am Ende des Berichts ein.

Der Fragebogen durchlief zuvor ein umfangreiches Pretestprogramm, bei dem in den ersten Fassungen unklare Begriffe und Frageformulierungen sichtbar wurden.[1] Einige Erläuterungen und Beispiele sowie präzisierende Antwortanweisungen mussten in der Folge eingefügt werden. Den ursprünglich verwendeten Begriff „Information“ haben wir durchgängig mit „Daten“ ersetzt. Er wäre zwar sachlich angemessener, weil Informationssicherheit sich auch auf Dinge bezieht, die nicht als Daten vorliegen, etwa mündlich kommunizierte Informationen. Es stellte sich aber heraus, dass sich ein solchermaßen abstraktes Konzept in der gebotenen Kürze eines Fragebogens nicht hinreichend kompakt und anschaulich definieren lässt. Im Gegensatz zu „Information“ kann „Daten“ als bekannt vorausgesetzt werden; hierzu wurden keine Verständnisprobleme gemeldet. Der Fragebogen schrumpfte infolge von Kürzungen und Vereinfachungen auf eine Länge, die in 10 bis 15 Minuten zu bearbeiten ist. Mit Rücksicht auf internationale Universitätsangehörige haben wir auch eine englische Sprachversion erstellt.

Der Personalrat der Beschäftigten in Technik und Verwaltung und der Personalrat der wissenschaftlich und künstlerisch Beschäftigten waren über die Befragung informiert und haben keine

1 Wir danken dem Informationssicherheitsbeauftragten der Universität Bielefeld, Herrn Michael Sundermeyer, und dem Leiter Anwenderberatung & Kommunikation im Bielefelder IT-Servicezentrum (BITS), Herrn Frank Michaelis, für sehr hilfreiche Hinweise zur Verbesserung des Fragebogens. Herr Sundermeyer hat uns auch bei der organisatorischen und technischen Realisierung der Umfrage tatkräftig unterstützt.

Bedenken geäußert. Rektor und Kanzler der Universität begrüßten und unterstützten die Befragung. Die Befragten wurden über die Freiwilligkeit und Anonymität der Teilnahme, die Verwendung der Daten und weitere Aspekte im Sinne der Datenschutz-Grundverordnung aufgeklärt.

Die Adressatïnnen setzen sich aus allen Bediensteten der Universität Bielefeld zusammen, die im zentralen E-Mail-Verteiler „Mitarbeiter“ gespeichert sind (N=6.096). Soweit die Verwaltung der Universität es einschätzen kann, erreicht dieser Verteiler die ganz überwiegende Mehrheit der Bediensteten aller Personalkategorien. Da die Registrierung des Personals in den Händen der dezentralen Einheiten liegt und die Zugehörigkeit zur Universität bei manchen Kategorien unklar bleibt, ist nicht ausgeschlossen, dass einzelne Personen übersehen werden. Andererseits rufen nicht alle Bediensteten Mails bei der registrierten Mailadresse ab. Die Zahl der tatsächlich erreichten Personen lässt sich deshalb nicht genau ermitteln.

Am 05.02.2019 erging in deutscher und englischer Sprache per E-Mail eine Einladung zur Teilnahme. Der Fragebogen war in Limesurvey, einer Online-Umfragesoftware, auf einem Server der Universität realisiert worden.[2] Am 04.03.2019 folgte eine Erinnerung. Insgesamt haben 789 Personen an der Befragung teilgenommen, was einer Antwortquote von knapp 13% entspricht. Dies liegt im Bereich dessen, was ohne Incentivierung erwartbar ist. Einige Teilnehmerïnnen haben den Fragebogen nicht vollständig beantwortet. Der Umfang der nutzbaren Stichprobe reduziert sich daher. Die Teilnahme konzentrierte sich auf wenige Tage im unmittelbaren Anschluss an die Einladung und die Erinnerung. 37 Personen nutzten die englische Fragebogenversion. Es handelt sich ausschließlich um Wissenschaftlerïnnen (Teilnehmende aus dem Bereich Forschung und Lehre). Damit haben 8,4% aus diesem Bereich diese Sprachversion gewählt.

3 Befragte und verarbeitete Daten

Befragte

Da der Fragebogen keine demographischen Merkmale der Befragten umfasst, beschränken wir uns auf eine Beschreibung der Aufgabenbereiche innerhalb der Universität und des Vorgesetzten- bzw.- Personalverantwortungsstatus. Der Fragebogen teilt die Beschäftigten in zwei Kategorien ein, die grob die Zweiteilung in Wissenschaft einerseits und Verwaltung und Technik andererseits spiegelt. Innerhalb der Wissenschaft können wir nicht zwischen Forschung und Lehre differenzieren; bei den meisten Bediensteten überlappen diese Tätigkeiten indes so sehr, dass eine klare Aufteilung ohnehin nicht möglich wäre. Im Selbstverständnis vieler Beschäftigter der zweiten Grobkategorie ist eine Unterscheidung zwischen Verwaltung und Technik sowie weiterer Aufgabenbereiche sicher sinnvoll. Wir haben jedoch auch hier darauf verzichtet, spezielle Bereiche wie die Bibliothek oder die Medien- und IT-Dienstleister auszuweisen, weil sich damit in Kombination mit dem Vorgesetztenstatus bestimmte Personenkreise zu sehr hätten eingrenzen lassen.

2 Wir danken Dr. Robert Glowienka für den Zugang zu einer Limesurvey-Installation der Fakultät für Soziologie und Hilfe bei der Nutzung.

Tabelle 3.1: Aufgabenbereich nach Personalverantwortung (Zeilenprozente)

			Tragen Sie Personalverantwortung?		Summe	
			Ja	Nein	N	%
In welchem Aufgabenbereich der Universität arbeiten Sie?	Forschung+Lehre	N	138	305	443	56,1
		%	31,2	68,8	100,0	
	Verwaltung+Technik	N	71	275	346	43,9
		%	20,5	79,5	100,0	
Summe		N	209	580	789	100,0
		%	26,5	73,5	100,0	

Wie Tabelle 3.1 zeigt, haben sich mehrheitlich Beschäftigte aus Forschung und Lehre beteiligt (443/789=56,1%). Insgesamt ein gutes Viertel (26,5%) trägt Personalverantwortung, wobei der Anteil im Bereich Forschung und Lehre höher liegt.[3] Eine Gruppe, die im Folgenden noch eingehender betrachtet wird, sind die Personalverantwortlichen aus Forschung und Lehre, die wir vereinfachend als Professorïnnen bezeichnen. Die 138 Teilnehmerïnnen dieser Kategorie machen 17,5% aller Befragten aus.

Im Sinne einer groben Orientierung haben wir auch um eine Selbsteinschätzung der Kompetenz in Datensicherheitsfragen gebeten (siehe Tabelle 3.2): „Wie schätzen Sie sich selbst im Bereich Datensicherheit ein?“. Nur eine kleine Gruppe (6,0%) hält sich für einë Expertïn. Mehrheitlich stufen sich die Befragten als Fortgeschrittene ein (55,1%). Ein gutes Drittel bezeichnet sich als Anfängerïn. Wir hatten der Antwortskala pro forma noch eine Kategorie für Personen hinzugefügt, die nicht einmal wissen, was mit Datensicherheit gemeint ist. Man muss sie wohl als *ahnungslos* bezeichnen. Wir waren überrascht, dass 9 Personen (1,1%) sich darin einordnen. Diese Zahl ist nicht durch ein sprachlich bedingtes Verständnisproblem zustande gekommen, denn mehrheitlich geht es um Personen, die die deutsche Sprachversion gewählt haben. Die Verteilung der Kompetenzeinschätzung unterscheidet sich weder zwischen den Aufgabenbereichen noch zwischen den Befragten mit und ohne Personalverantwortung wesentlich.[4]

3 statistisch signifikant, Chi²-Test, alpha=1%
4 Chi²-Test, alpha=5%

Tabelle 3.2: Subjektive Datensicherheitskompetenz

Kompetenz	N	%
Experten/Expertin	47	6
Fortgeschrittenen/Fortgeschrittene	435	55,1
Anfänger/Anfängerin	298	37,8
Ahnungslose („Ich weiß nicht, was mit Datensicherheit gemeint ist.“)	9	1,1
Total	789	100

Verarbeitete Daten

Im Interesse der Vertraulichkeit wurden auch Angaben zu den verarbeiteten Daten nur in groben Kategorien erhoben (siehe Tabelle 3.3, Spalte „Summe“). Mehrfachnennungen waren nicht möglich: Nur die am häufigsten verarbeiteten Daten sollten genannt werden. Die meisten Nennungen entfielen auf Forschungsdaten mit zusammen 34,8%. Darunter sind 20,8% anonyme (Zeile 1) und 14,0% personenbezogene Daten (Zeile 2). Es folgen Studierendendaten (21,0%, Zeile 3). Personal- sowie Finanzdaten wurden von je ca. 10% der Befragten genannt. Sonstige anonyme Daten gehen mit 18,0% (Zeile 6) und sonstige personenbezogene Daten mit nur 6,1% (Zeile 7) in die Auszählung ein.

Erwartungsgemäß sind die beiden Aufgabenbereiche in unterschiedlichem Ausmaß mit den Datentypen befasst. Forschung und Lehre haben mehrheitlich mit Forschungsdaten zu tun. In der Summe machen sie hier 56,4% der Nennungen aus. Hinzu kommen 20,6% sonstige anonyme Daten, zu denen wohl wissenschaftliche Texte zu rechnen sind. Allerdings wurden von 17,6% der Befragten auch Studierendendaten genannt. Offenbar stammen diese Angaben von den Sekretariaten der Lehrstühle oder von Lehrenden, die keine eigenen Forschungsdaten erheben.

Verwaltung und Technik haben dagegen – wenig überraschend – selten mit Forschungsdaten und stattdessen mehr mit Studierenden- und Personaldaten (zusammen 47,6%) und Finanzdaten (18,9%) zu tun.

Tabelle 3.3: Genutzte Daten nach Aufgabenbereich

„Mit welchen Daten arbeiten Sie am häufigsten?“ nach Aufgabenbereich

		b1f1 Aufgabenbereich		
Datenart		Forschung und Lehre	Verwaltung und Technik	Summe
(1) anonyme Forschungsdaten	N	150	9	159
	% (Spalte)	35,1%	2,7%	20,8%
(2) personenbezogene Forschungsdaten	N	91	16	107
	% (Spalte)	21,3%	4,7%	14,0%
(3) Studierendendaten	N	75	86	161
	% (Spalte)	17,6%	25,4%	21,0%
(4) Personaldaten	N	6	75	81
	% (Spalte)	1,4%	22,2%	10,6%
(5) Finanzdaten	N	8	64	72
	% (Spalte)	1,9%	18,9%	9,4%
(6) sonstige anonyme Daten, z. B. wissenschaftliche Texte	N	88	50	138
	% (Spalte)	20,6%	14,8%	18,0%
(7) sonstige personenbezogene Daten, z. B. Bilder und Filmaufnahmen	N	9	38	47
	% (Spalte)	2,1%	11,2%	6,1%
(8) Summe	N	427	338	765
	% (Spalte)	100,0%	100,0%	100,0%

Anmerkung: Nur eine Kategorie konnte angekreuzt werden.

4 Einschätzung des Schutzbedarfs von Daten

Wir wollten wissen, wie die strategische Bedeutung der verarbeiteten Daten und ihre Sensibilität eingeschätzt werden. Wir sprechen im Folgenden zusammenfassend vom wahrgenommenen Schutzbedarf der Daten, wobei dieser Begriff weit über die juristische Ebene hinausgeht. Angaben liegen jeweils für die Daten vor, mit denen die Befragten am häufigsten arbeiten (s.o.). Nach der Anweisung „Geben Sie an, inwiefern Sie den folgenden Aussagen zustimmen." lauteten die Fragen:

- „Sie enthalten sensible Informationen."
- „Sie sind für unbefugte Dritte attraktiv."
- „Sie dienen den organisatorischen Abläufen."
- „Es wäre für mich persönlich ein Problem, wenn sie in falsche Hände geraten würden."
- „Es wäre ein Problem für die Universität, wenn sie in falsche Hände geraten würden."

Der vierteiligen Antwortskala von „trifft voll zu" bis „trifft überhaupt nicht zu" haben wir Werte von 4 bis 1 zugewiesen. Daraus berechnen wir Mittelwerte nach Datenart (Tabelle 4.1). Ein hoher Wert steht für hohe Zustimmung.

Tabelle 4.1: Einschätzung des Schutzbedarfs der verarbeiteten Daten

Mit welchen Daten arbeiten Sie am häufigsten?	(1) Sie enthalten sensible Informationen.	(2) Sie sind für unbefugte Dritte attraktiv.	(3) Sie dienen den organisatorischen Abläufen.	(4) Es wäre für mich persönlich ein Problem, wenn sie in falsche Hände geraten würden.	(5) Es wäre ein Problem für die Universität, wenn sie in falsche Hände geraten würden.
(1) anonyme Forschungsdaten	2,34	2,14	1,63	2,68	2,35
(2) personenbezogene Forschungsdaten	3,13	2,25	1,86	3,20	2,97
(3) Studierendendaten	3,25	2,64	3,48	3,23	3,26
(4) Personaldaten	3,39	3,01	3,51	3,20	3,34
(5) Finanzdaten	3,12	2,54	3,35	2,80	2,81
(6) sonstige anonyme Daten, z. B. wissenschaftliche Texte	2,00	1,99	2,37	2,17	2,09
sonstige personenbezogene Daten, z. B. Bilder und Filmaufnahmen	2,68	2,30	2,90	2,95	2,70

Personaldaten werden (Zeile 4) in jeder Hinsicht als besonders kritisch betrachtet, dicht gefolgt von Studierendendaten (Zeile 3). Auch personenbezogenen Forschungsdaten (Zeile 2) und Finanzdaten (Zeile 5) wird sensibler Inhalt zugeschrieben. Wenig überraschend wird anonymen Forschungsdaten eine eher geringe Bedeutung für organisatorische Abläufe (Zeile 1, Spalte 3) beigemessen. Die Einschätzungen in den fünf Dimensionen korrespondieren sehr deutlich miteinander. Abgesehen von der Bewertung der Bedeutung der Daten für organisatorische Abläufe ergeben sich Pearson-Korrelationen von 0,6 bis 0,7 zwischen den Bewertungsdimensionen. Je sensibler der zugeschriebene Informationsgehalt, desto attraktiver scheinen die Daten den Befragten für unbefugte Dritte und desto größer die erwarteten Probleme, wenn sie in falsche Hände geraten würden. Dies gilt ungeachtet der Tatsache, dass die Mittelwerte der Dimensionen sich deutlich unterscheiden.

Weitere, hier nicht im Detail dargestellte Analysen zeigten Unterschiede in der Bewertung bestimmter Datenarten je nach Tätigkeitsbereich. So werden etwa Studierendendaten von Befragten aus Forschung und Lehre statistisch signifikant als weniger sensibel und weniger attraktiv für Dritte gehalten, und Wissenschaftlerïnnen sehen auch weniger Probleme für sich, wenn solche Daten in falsche Hände geraten würden. Auch in anderen Konstellationen zeigen sich Unterschiede, die allerdings oft nicht statistisch signifikant sind. Mithin stellt sich die Frage, ob es sich um einen generellen Effekt handelt.

Ein tabellarischer Vergleich innerhalb der Datenkategorien ist unergiebig, weil die beiden Tätigkeitsbereiche sich typischerweise mit verschiedenen Datentypen befassen und ein auf einen spezifischen Datentyp beschränkter Vergleich immer nur auf kleine Fallzahlen zurückgreifen kann. So arbeiten etwa nur sechs Personen in Forschung und Lehre vorwiegend mit Personaldaten, gegenüber 75 in der Verwaltung. Derart kleine Fallzahlen sind sehr anfällig für Zufallseinflüsse und eignen sich nicht für statistische Tests. Wir wenden deshalb ein Verfahren an, das gleichzeitig alle Datentypen und alle Befragten einbezieht: eine sog. Regression mit Dummy-Variablen. Ein weiterer Vorteil dieses Verfahrens gegenüber Mittelwertvergleichen liegt in ihrer Fähigkeit zu ceteris-paribus-Aussagen, also Aussagen über den Einfluss eines Merkmals unter Konstanthaltung aller anderen Merkmale. Es spielt daher keine Rolle, dass sich die Datenprofile zwischen den Tätigkeitsbereichen unterscheiden.

Wir machen uns die Ähnlichkeit der obigen Dimensionen (sensibel, attraktiv, im Verlustfall problematisch für die Person selbst und die Universität) zunutze, um daraus ein einziges zusammenfassendes Maß zu erzeugen. Wir müssen dann die Dimensionen nicht separat betrachten, sondern fassen diejenigen, die hochgradig korrelieren, zu einem Summenindex zusammen,[5] den wir Datensensibilität nennen.

Der obigen Tabelle 4.1 entsprechend, nehmen wir an, dass diese bei allen Befragten zunächst von dem Datentyp abhängt, mit dem jemand arbeitet. Die Analyse soll zeigen, wie stark sich die Wahrnehmung der Sensibilität bei einer bestimmten Datenart von einer Referenzkategorie unter-

5 Der Reliabilitätskoeffizient Cronbachs alpha der vier Variablen beträgt 0,843.

scheidet. Als Referenz legen wir die sonstigen anonymen Daten fest. Ferner wollen wir einen Einfluss des Tätigkeitsbereichs und der Personalverantwortung prüfen. Damit werden wir sehen, wie sich Befragte aus Technik und Verwaltung von solchen aus Forschung und Lehre unterscheiden und ob die Personalverantwortung sich auswirkt. Schließlich geht die Annahme ein, dass mit der selbst eingeschätzten Datensicherheitskompetenz auch ein Gefühl für die Konsequenzen von Datenvorfällen steigt. Es ist ja denkbar, dass etwa die Kenntnis technischer Hintergründe der Datenspionage sich auf das Sicherheitsempfinden und damit auf die Schutzbedarfswahrnehmung auswirkt. Aufgrund der Art und Weise, in der die Datensicherheitskompetenz abgefragt wurde, vergleichen wir die einzelnen Stufen. Als Referenzkategorie dienen hier Expertïnnen. Wir testen, ob niedrigere Kompetenz mit einer niedrigeren Schutzbedarfswahrnehmung einhergeht.

Tabelle 4.2: Determinanten des wahrgenommenen Schutzbedarfs

		Unstandardisierte Regressionskoeffizienten		
		B	Standardfehler	Signifikanz
	Konstante	2,425	,128	,000
Referenz: sonstige anonyme Daten	Anon.ForschDat	,390	,086	,000
	Persbez.ForschDat	,882	,094	,000
	Studierend.daten	,990	,083	,000
	Personaldaten	1,004	,109	,000
	Finanzdaten	,647	,111	,000
	SonstPersonbezDat	,484	,126	,000
Referenz: Verwaltung und Technik	Forschung+Lehre	-,237	,068	,001
Referenz: keine Personalverantwortung	Personalverantwortg.	,088	,059	,136
Datensicherheits-kompetenz, Referenz: Expertïn	Fortgeschritten	-,212	,115	,067
	Anfängerïn	-,285	,118	,016
	„keine Ahnung“	-,785	,258	,002

Das Ergebnis enthält Tabelle 4.2. Sie gliedert sich in Einflussgrößen (Koeffizienten) der Datenarten, des Tätigkeitsbereichs und der Personalverantwortung sowie den Datensicherheits-Kompetenzstufe. Angegeben ist für ein Merkmal jeweils, wie sich der wahrgenommene Schutzbedarf verändert, wenn eine Person dieses Merkmal im Vergleich mit der Referenzkategorie trägt. Wie man im oberen Teil der Ergebnistabelle erkennt, werden im Vergleich mit der Referenzkategorie der sonstigen anonymen Daten alle anderen Datenarten als sensibler eingestuft. Der Abstand ist bei Personaldaten (B=+1,004) und Studierendendaten (B=+0,990) am größten. Das Ergebnis entspricht in etwa dem des Mittelwertvergleichs.

Der oben in Einzelkonstellationen sichtbar gewordene Unterschied zwischen den Tätigkeitsbereichen zeigt sich auch bei dieser Globalbetrachtung. Befragte aus Forschung und Lehre sehen einen vergleichbaren Datenbestand durchweg als weniger sensibel an (B=-0,237). Die Differenz ist nicht gewaltig, aber signifikant. Personalverantwortung wirkt sich nicht signifikant aus.

Je geringer die Datensicherheitskompetenz nach Selbsteinschätzung ausfällt, desto schwächer ist die Schutzbedarfswahrnehmung ausgeprägt. Mit jeder Stufe unter den Expertïnnen fällt die Wahrnehmung um einen bestimmten Betrag. Anfängerïnnen sehen vergleichbare Daten um B=-0,285 weniger schutzbedürftig an. Zwar ist die Differenz zu den Fortgeschrittenen zu den Expertïnnen (B=-0,212) statistisch nicht ganz signifikant, die Tendenz liegt jedoch auch hier dem Betrag nach vor.

5 Informationssicherheitskompetenz

Erkennung von Schadsoftware

Ein einfacher Indikator der Kompetenz der Befragten in Informationssicherheitsfragen ist die Vertrautheit mit technischen Konzepten, die im Zusammenhang mit Schadsoftware (Malware) stehen. In der Annahme, dass die Vertrautheit mit technischen Begriffen anzeigt, ob Wirkungsweisen und Schadpotential von Malware bekannt sind, haben wir deshalb die Frage gestellt: „*Jeden Tag begegnet uns eine Fülle neuer Fachbegriffe. Sie sehen hier eine Liste solcher Begriffe. Was davon stellt eine Gefahr für die Datensicherheit dar? Geben Sie bitte eine spontane Einschätzung ab, ohne zu recherchieren. Sollten Sie davon etwas nicht kennen, kreuzen Sie bitte ‚weiß nicht' an.*" Antwortmöglichkeiten waren ja, nein, weiß nicht. Es war natürlich nicht sinnvoll, nur Schädlingstypen aufzuführen, da es dazu verleitet hätte, immer 'ja' anzukreuzen, weshalb wir auch ungefährliche Software aufgeführt haben.

Schadsoftware:

- Trojaner
- Krypto-Miner
- Phishing
- Keylogger
- Rootkit
- Ransom-Software

ungefährliche Software:

- Patch
- Firewall
- Antivirus-Software

- Backup

Bei dem vorgegebenen Antwortmuster war es prinzipiell möglich, die Antwort zu raten. Es ist daneben bekannt, dass Personen, die als besonders kompetent gelten wollen, lieber eine falsche Antwort geben, als Unkenntnis einzugestehen. Um sicherzustellen, dass solche Personen erkannt werden, haben wir ferner zwei technisch klingende, aber frei erfundene, nicht existierende Softwares aufgeführt:

- Whyte-Tailing
- Zero-Hasher

Die Softwarekategorien wurden unsortiert und ohne Gruppierung vorgelegt (siehe nachfolgende Tabelle). Die Antworten haben wir nach folgenden Regeln ausgewertet: Die Schadsoftwares nicht zu kennen oder als ungefährlich zu bezeichnen, wurde mit je einem Minuspunkt bewertet, ebenso die Unkenntnis einer ungefährlichen Softwarekategorie oder ihre Einschätzung als gefährlich. Diese Vorgehensweise ist zugegebenermaßen rigoros, aber wir halten einen technischen Grundstock für einen integralen Aspekt der IT-Sicherheitskompetenz. Wurden erfundene Konzepte als gefährlich eingestuft, trug auch das zur Abwertung bei. Die richtige Antwort wäre hier „weiß nicht“ gewesen. Die Antwort „nein“ (ungefährlich) wurde nicht negativ gewertet, weil etwas Erfundenes nicht gefährlich sein kann.

Wie der folgenden Tabelle 5.1 zu entnehmen ist, werden Phishing und Schadsoftwaretypen wie Trojaner und Schutzmaßnahmen wie Firewall, Antivirus-Software sowie Backup und Patch recht zuverlässig erkannt. Die Mehrheit der Malware-Spielarten ist den Befragten aber unbekannt; stets hält auch ein erheblicher Teil der Stichprobe sie irrtümlich nicht für gefährlich.

Auch die beiden erfundenen Begriffe werden – korrekterweise – ganz überwiegend als unbekannt markiert. Lediglich die selbsteingeschätzten Sicherheitsexperten glaubten Whyte-Tailing und Zero-Hasher proportional häufiger zu kennen.[6]

6 Wir verzichten an dieser Stelle auf Details. Es besteht ein statistisch signifikanter positiver Zusammenhang zwischen selbsteingeschätzter Kompetenz und Fehleinschätzung der Erfindungen.

Tabelle 5.1: Gefährdungseinschätzung einzelner Softwarekategorien

Software	ja	nein	kenne ich nicht	fehlerhafte Antwort
Trojaner	659	3	7	1,5%
Patch	75	312	249	50,9%
Krypto-Miner	163	124	352	74,5%
Zero-Hasher	49	22	570	7,6%
Firewall	75	569	9	12,9%
Phishing	634	7	23	4,5%
Whyte-Tailing	29	16	592	4,6%
Keylogger	298	52	295	53,8%
Antivirus-Software	73	570	7	12,3%
Backup	77	555	12	13,8%
Rootkit	150	77	410	76,5%
Ransom-Software	241	23	376	62,3%

Für eine Gesamtschau haben wir die Minuspunkte über alle Kategorien summiert. Dabei konnten theoretisch Werte von 0 bis 12 entstehen. Wenn einzelne Konzepte ausgelassen wurden (missing value), haben wir die übrigen Wertungen hochgerechnet, sofern insgesamt mindestens sechs gültige Antworten vorliegen. Weniger als ein Zehntel der Stichprobe hat fünf oder mehr Minuspunkte zu verzeichnen. Der höchste gemessene Fehlerwert war 10. Im Mittel haben die Befragten 3,7 Softwarekategorien falsch eingeschätzt (Tabelle 5.2).

Tabelle 5.2: Schadsoftware: Fehleinschätzungen

Gültige Fälle	Minimum	Maximum	Mittelwert
656	0	10	3,72

Da dieser Wert zunächst mangels Referenzwert schwer absolut zu bewerten ist, betrachten wir seine Variationen innerhalb der Stichprobe. Die Fehlerzahl hängt nicht damit zusammen, in welchem Funktionsbereich Befragte tätig sind und ob sie Personalverantwortung tragen. Allerdings gelingt die Gefahrenerkennung umso besser, je höher die Befragten ihre Fähigkeit in IT-Sicherheitsfragen selbst einschätzen: Anfängerïnnen liegen mehr als doppelt so oft falsch wie Expertïnnen (4,49:1,88), und die wenigen, die nach Selbstauskunft nicht einmal den Begriff Datensicherheit verstehen, beinahe dreimal so oft (5,49, siehe Tabelle 5.3). Insofern erweist sich insgesamt die Selbsteinschätzung der Informationssicherheitskompetenz trotz der partiellen Selbstüberschätzung der Experten bei erfundenen Schädlingen als zuverlässig.

Tabelle 5.3: Fehleinschätzungen nach Datensicherheitskompetenz

Kompetenz	Mittelwert	N
Experten/Expertin	1,88	35
Fortgeschrittenen/Fortgeschrittene	3,35	373
Anfänger/Anfängerin	4,49	240
Ahnungslos („Ich weiß nicht, was mit Datensicherheit gemeint ist.“)	5,49	8
Total	3,72	656

Der Zusammenhang ist statistisch signifikant (Varianzanalyse, alpha=1%).

6 Risikoverhalten

Einer der Ausgangspunkte dieser Studie ist der Konflikt zwischen dem IT-Sicherheits-Regelwerk und anderen Zielen und Anforderungen des Alltags, der sich, so die Annahme, in Regelverstößen äußert. Es war nicht möglich, tatsächliches Verhalten zu erfassen. Die Alternative, berichtetes riskantes Verhalten zu erfassen, muss es vermeiden, durch allzu offensichtliche Frageformulierungen auf dieses Problem hinzuweisen. Die Spannbreite in Frage kommender Verhaltenstatbestände ist im Prinzip riesig. Um verwertbare Daten zu gewinnen, waren wir bestrebt, nur nach solchen Verstößen zu fragen, die nach Kenntnis unserer Beraterïnnen aus Informationssicherheitskreisen eine größere Zahl von Universitätsangehörigen im Rahmen alltäglicher Verrichtungen rund um den Arbeitsplatz tatsächlich begeht und die gleichzeitig entsprechend der universitären Sicherheitsrichtlinien eindeutig zu tun oder zu unterlassen sind. Eingeleitet von der Vorbemerkung „Die folgenden Fragen beziehen sich nur auf Ihren Arbeitsalltag.“ fragten wir „Außerdem interessiert uns in Sachen Datensicherheit: Trifft das Folgende auf Sie zu?“ mit den Antwortkategorien „ja“ und „nein“. Die folgende Übersicht enthält die Wortlaute. Die rechte Spalte gibt an, welche Antwort wir als riskant bewerten.

Tabelle 6.1: Risikoverhalten: Wortlaute

Verhalten	problematisch falls:
Ich alleine kenne das Passwort für meinen dienstlichen PC.	nein
Meine dienstlichen E-Mails werden zu einem privaten Mail-Anbieter (z. B. Gmail, web.de, GMX) weitergeleitet.	ja
Ich schließe mein Büro immer ab, wenn ich es unbeaufsichtigt lasse.	nein
Ich nutze Online-Oberflächen, Anwendungen oder Apps wie Google Docs, Google Translate, Prezi, SplitPDF, um dienstliche Dokumente zu bearbeiten.	ja
Von den Dateien, an denen ich jeweils aktuell arbeite, liegen einige auf dem Desktop meines PCs.	ja
Wenn ich Unterlagen auf einem Gemeinschaftsdrucker ausdrucke, hole ich sie umgehend ab.	nein
Ich schließe an meinen PC in der Universität auch private USB-Sticks an.	ja
Ich schließe an meinen privaten PC auch USB-Sticks der Universität an.	ja
Ich weiß, wie ich die Bildschirmsperre aktiviere.	nein
Ich sperre jedes Mal meinen Bildschirm, wenn ich meinen Arbeitsplatz verlasse.	nein

In der Annahme, dass netzbasierte Speicher-, Planungs- und Kommunikationsdienste im Alltag eine gewisse Rolle spielen, haben wir ferner die Frage gestellt: „Verwenden Sie *selbst* folgende Dienste?“ Antwortmöglichkeiten waren „ja“, „nein“, „kenne ich nicht“. Die Liste bestand aus:

Tabelle 6.2: Problematische Dienste

Dienst	problematisch
DFN-Terminplaner	nein
DFN-Webkonferenzen mit Adobe Connect	nein
Doodle	ja
Dropbox	ja
Google Drive	ja
iCloud	ja
Netzlaufwerke	nein
Sciebo	nein
Skype	ja

Aus Datenschutz- und Informationssicherheitsperspektive betrachten wir – entsprechend der Dienstanweisungen für die Universität Bielefeld – Doodle, Dropbox, Google Drive, iCloud und Skype als unsicher.

Tabelle 6.3 enthält die Antwortverteilungen je Verhaltensweise bzw. Dienst. Weit verbreitet sind offenbar Fahrlässigkeiten wie die Speicherung von Dateien auf dem Windows-Desktop, also eines lokalen Ordners, was mit dem Risiko eines totalen Datenverlusts im Fall eines defekten lokalen Speichermediums verbunden ist. Auch der Transfer von Daten zwischen dienstlichen und privaten PCs mit USB-Sticks gehört zur Tagesordnung. Hier besteht bekanntlich die Gefahr der Schädlingsübertragung. Die Mehrheit weiß zwar, wie die Bildschirmsperre aktiviert wird, aber nur die Hälfte der Befragten macht davon immer Gebrauch. 6,6% lassen dienstliche Korrespondenz an private Maildienstanbieter übertragen. 7,4% geben an, Drittpersonen sei ihr PC-Passwort bekannt.

Der Online-Terminumfragedienst Doodle stellt mit einem Nutzungsgrad von 71,7% das Standardwerkzeug der Terminplanung dar. Die sichere Alternative, der DFN-Terminplaner, ist beinahe der Hälfte der Befragten unbekannt. Mit dem Videokonferenz-, IP-Telefonie- und Messenger-Dienst Skype sind praktisch alle Befragten vertraut, und über ein Drittel (37,8%) nutzt den Dienst. Wiederum ist die sichere Alternative, DFN-Webkonferenzen, beinahe jeder/ m Zweiten nicht bekannt. Der Filehosting-Dienst Dropbox erfreut sich einer vergleichbaren Beliebtheit (34,7% Nutzerïnnen), während die sichere Alternative, Sciebo, deutlich häufiger im Gebrauch ist (54,0%). Die anderen aufgeführten kommerziellen Speicherdienste, Google Drive und iCloud, werden trotz eigentlich bekannter Sicherheitsprobleme von erheblichen Teilgruppen der Bediensteten genutzt. Immerhin bilden die von einem zentralen Dienstleister bereitgestellten universitätsinternen Netzlaufwerke den Standard: Fast 90% der Befragten nutzen sie.

Tabelle 6.3: Riskantes Verhalten und Nutzung problematischer Dienste

Dienst/Verhalten	Nutzung			Fallzahl
	ja	nein	kenne nicht	
nur ich kenne PC-Passwort	92,6%	7,4%		664
dienstliche Mails zu privatem Anbieter	6,6%	93,4%		663
schließe Büro immer ab	88,7%	11,3%		661
nutze Oberflächen wie Google Docs	14,8%	85,2%		660
Dateien liegen auf Desktop	44,6%	55,4%		661
hole Ausdrucke umgehend ab	95,7%	4,3%		624
private USB-Sticks an Uni-PC	55,5%	44,5%		656
Uni-USB-Sticks an privatem PC	35,4%	64,6%		646
weiß wie Bildschirmsperre aktivieren	86,0%	14,0%		657
sperre jedes Mal Bildschirm	49,4%	50,6%		660

DFN-Terminplaner	14,6%	37,7%	47,7%	652
DFN-Webkonferenzen	9,1%	44,1%	46,9%	651
Doodle	71,7%	27,6%	0,7%	678
Dropbox	34,7%	63,8%	1,5%	663
Google Drive	19,2%	76,6%	4,3%	657
iCloud	14,8%	81,1%	4,2%	650
Netzlaufwerke	89,5%	9,5%	1,0%	674
Sciebo	54,0%	36,1%	9,9%	665
Skype	37,8%	61,3%	0,9%	662

Uns interessierte, ob Risikoverhalten und die Nutzung problematischer Dienste sich zwischen Teilgruppen der Bediensteten unterscheiden. Dazu fassen wir die obigen Antworten zusammen. Wir bilden zwei Zählvariablen: Risikoverhalten und Dienstnutzung. Die erste enthält die ungewichtete Summe der problematischen, aber ausgeführten, und der gebotenen, aber unterlassenen Verhaltensweisen. Zu jeder der beiden Gruppen gehören fünf Verhaltensweisen. Die Summe kann daher Werte zwischen 0 und 10 annehmen; maximal kamen 8 zustande. Die zweite zählt die Nutzung der fünf problematischen Dienste (Doodle, Dropbox, Google Drive, iCloud, Skype). Deshalb kann sie Werte zwischen 0 und 5 ergeben. Der Maximalwert 5 kommt auch vor. Im Mittel haben alle Befragten 2,44 problematische Verhaltensweisen und 1,78 genutzte problematische Dienste angegeben (siehe folgende Tabelle). Wir vergleichen nun die Mittelwerte nach Tätigkeitsbereich, Personalverantwortung und subjektiver Datensicherheitskompetenz (Tabelle 6.4).

Die Bediensteten in Forschung und Lehre zeigen sich deutlich risikobereiter als die Angehörigen von Verwaltung und Technik. Sie praktizieren im Durchschnitt 0,99 Risikoverhalten mehr und nutzen 0,8 Dienste mehr. Personalverantwortung geht mit stärkerer Nutzung problematischer Dienste einher; bei sonstigem Risikoverhalten sind die Unterschiede statistisch unbedeutend. Einen klaren Einfluss übt die subjektive Datensicherheitskompetenz aus: Von den Expertïnnen zu den Ahnungslosen steigen die beiden Zählwerte auf das dreifache. Auch subjektive Anfängerïnnen gehen merklich mehr Risiken ein als Expertïnnen und Fortgeschrittene.

Die Differenz zwischen Personen mit und ohne Personalverantwortung haben wir in weiterführenden Analysen getrennt für die beiden großen Tätigkeitsbereiche innerhalb der Universität betrachtet. Eine deutliche Differenz zu Lasten der Personalverantwortlichen besteht demnach nur innerhalb des Bereichs Forschung und Lehre, während sich im Gegenteil in Verwaltung und Technik die Führungskräfte sogar durch vorsichtigeres Verhalten vom sonstigen Personal abheben. So beträgt die Differenz der Zahl genutzter Dienste in der Wissenschaft 0,39 zulasten der Führungskräfte gegenüber einem Wert von –0,17 zugunsten der Führungskräfte in der Verwaltung. Offenbar stechen besonders die Führungskräfte in der Wissenschaft aus der Verteilung aller Personalkategorien heraus. Bei ihnen dürfte es sich mit wenigen Ausnahmen um Professorïnnen handeln.

Diesen Umstand belegen wir in der folgenden Tabelle durch einen Mittelwertvergleich der Führungskräfte in der Wissenschaft mit den restlichen Gruppen (Ende der Tabelle; die subjektive Datensicherheitskompetenz bleibt unberücksichtigt). Die Differenz beträgt 0,74 (3,06-2,32). Offensichtlich verhalten sich nicht Führungskräfte schlechthin, sondern nur Führungskräfte in Forschung und Lehre besonders risikoaffin.

Tabelle 6.4: Riskantes Verhalten und Nutzung problematischer Dienste nach Personalkategorie

Gruppe	Risikoverhalten	N	Dienstnutzung	N
Gesamtmittel	2,44	661	1,78	662
Tätigkeitsbereich				
Forschung und Lehre	2,90	360	2,13	371
Verwaltung und Technik	1,91	301	1,33	291
Personalverantwortung				
ja	(2,65)	178	2,00	178
nein	(2,37)	483	1,69	484
Datensicherheitskompetenz				
Expertïn	1,77	35	1,07	34
Fortgeschritten	2,22	375	1,68	377
Anfängerïn	2,84	243	1,98	244
Ahnungslos	4,00	8	3,00	7
Führungskraft Wissenschaft				
ja	3,06	117	2,39	120
nein	2,32	544	1,64	542

Alle Mittelwertdifferenzen außer Werten in Klammern sind statistisch signifikant voneinander verschieden (Varianzanalyse, alpha<1%).

7 Bewertung der universitären Infrastruktur

Die Beherrschung der Grundlagen und Anwendungen der Informationssicherheit entwickelt sich zu einer Grundkompetenz der modernen Arbeitswelt. Zwar ist auch in anderen Lebensbereichen, nicht zuletzt im Privatleben, ein sicherer Umgang mit Informationen eine Voraussetzung selbstbestimmten Daseins. Gleichwohl gehört es zu den unabweisbaren Aufgaben einer Organisation, die Informationssicherheitskompetenz ihrer Angehörigen auf dem aktuellen Stand zu halten. Den Bediensteten der Universität Bielefeld steht ein breites Informations- und Dienstleistungsangebot im Bereich der Informationssicherheit zur Verfügung. Deren Bewertung durch die Befragten sowie die Einschätzung der eigenen Verhaltenssicherheit bilden weitere Indikatoren der Informationssicherheitskompetenz, die persönliche wie infrastrukturelle Aspekte umfasst. Wir wollten in diesem Zusammenhang wissen, wie es um die Verhaltenssicherheit in Problemsituationen bestellt ist, wie die eigene Informiertheit eingeschätzt wird, welche Erfahrungen im Umgang mit Problemen gemacht wurden und wie es um Kompetenzbildungsangebote bestellt ist. Dazu haben wir die folgenden Fragen gestellt:

Tabelle 7.1: Aussagen zu Informationssicherheitsangeboten: Wortlaute und Antwortverteilung

Wortlaut**	voll*	eher*	eher nicht*	überhaupt nicht*	N
Ich brauche mehr Schulungsangebote zur Datensicherheit.	13,5	42,3	38,8	5,3	673
Für Fragen zur Datensicherheit habe ich innerhalb der Universität ausreichend Informationsquellen.	11,4	48,9	34,8	4,9	630
Ich bin über die Regelungen der Universität zur Datensicherheit gut informiert.	8,0	39,7	43,3	9,0	677
Bei einem Datensicherheitsproblem wüsste ich, an wen ich mich wenden muss.	38,6	33,1	20,1	8,2	682
In Fragen der Datensicherheit bin ich immer sicher, wie ich mich verhalten muss.	4,4	47,9	39,7	7,9	680
Die bisher aufgetretenen Probleme mit der Datensicherheit wurden von den Verantwortlichen zeitnah gelöst.	22,2	49,4	21,6	6,9	334

* Antworttext: stimme ... zu

** Diese Fragebatterie enthielt in der Onlinefassung eine weitere Frage, die aber nicht zu den Informationssicherheitsangeboten zählte.

Nach der Anweisung „Wie schätzen Sie die Angebote der Universität zur Datensicherheit ein? Geben Sie an, inwiefern Sie den folgenden Aussagen zustimmen.“ standen die Antwortkategorien

„stimme voll/eher/eher nicht/überhaupt nicht zu“ zur Verfügung. Im Gegensatz zur ersten Aussage, die eher ein Defizit ausdrückt, beziffern die anderen direkt das Ausmaß der Zielerreichung. Bei kleinen Variationen gilt: Bei grob der Hälfte der Befragten ist noch kein befriedigender Zustand erreicht. Zwar fühlen sich 52% voll oder eher über die Regelungen zur Datensicherheit informiert, aber über ein Viertel (28,3%) weiß nicht, an wen man sich bei einem Datensicherheitsproblem wenden muss, beinahe die Hälfte ist unsicher, wie man sich verhalten muss (47,6%), oder braucht mehr Schulungsangebote zur Datensicherheit (44,1), und knapp 40% sehen nicht ausreichend Informationsquellen. Nur die Hälfte der Befragten (N=334) hat die letzte Aussage beantwortet. Von ihnen waren 28,5% nicht der Meinung, aufgetretene Probleme mit der Datensicherheit seien von den Verantwortlichen zeitnah gelöst worden. Es handelt sich bei diesen Befunden zwar nur um subjektive Einschätzungen, deren Validität als Indikator des realen Umgangs mit Risiken zu prüfen bleibt. Die Universität kann mit ihnen aber gewiss mitnichten zufrieden sein.

Auch hier ist von Interesse, wie die Einschätzung zwischen Personalkategorien variiert. Es ist dazu nicht notwendig, alle Aussagen separat zu diskutieren. Alle Antworttendenzen hängen statistisch stark zusammen,[7] weshalb wir einen Summenindex bilden konnten, der den Mittelwert der Einzelantworten angibt. Wir bezeichnen ihn als Angebotspassung. Seine Werte reichen von 1 (keinerlei Zustimmung) bis 4 (volle Zustimmung zu allen Aussagen). Die Antworten der ersten Aussage, die ja ein Kompetenz*defizit* anspricht, haben wir bei der Mittelwertberechnung durch Komplementärwerte ersetzt.

Tabelle 7.2: Passung dienstlicher Informationssicherheitsangebote (Index) nach Personalkategorie

Gruppe	Passung	N
Gesamtmittel	2,61	686
Tätigkeitsbereich		
Forschung und Lehre	2,53	380
Verwaltung und Technik	2,71	306
Personalverantwortung		
ja	2,68	187
nein	2,58	499
Datensicherheitskompetenz		
Expertïn	3,05	36
Fortgeschritten	2,76	389
Anfängerïn	2,33	253
Ahnungslos	2,50	8

7 Eine explorative Faktorenanalyse ergab eine einfaktorielle Lösung mit Ladungsbeträgen zwischen 0,58 und 0,81.

Führungskraft Wissenschaft		
ja	(2,68)	125
nein	(2,59)	561

Angegeben sind bivariate Mittelwerte. Alle Unterschiede außer Werten in Klammern sind statistisch signifikant voneinander verschieden (Varianzanalyse, alpha<1%).

Die Bediensteten in Technik und Verwaltung sehen die Angebote leicht, aber statistisch signifikant, als passender an als die Kollegïnnen in Forschung und Lehre (siehe Tabelle 7.2). Den Gründen dafür können wir mit unseren Daten nicht nachgehen. Denkbar sind aber Unterschiede in Tätigkeitsprofilen, der Länge der Betriebszugehörigkeit bzw. der höheren Fluktuation unter Wissenschaftlern und in der Folge der Teilnahme an IT-Qualifikationsangeboten wie auch in bereichsspezifischen Sicherheitsbedürfnissen, zu denen die Angebote passen müssen. Es ist leider nicht bekannt, ob Verwaltungsbedienstete generell Schulungsmaßnahmen häufiger wahrnehmen als Wissenschaftlerïnnen. Auch Personalverantwortliche bewerten die Angebote günstiger als ihr Personal. Möglicherweise sind ihnen Angebote besser bekannt. Vorstellbar ist ebenso, dass die Anbieterïnnen je nach Hierarchieebene der Nachfragenden unterschiedlich reagieren.

Schließlich muss zu denken geben, dass sich die Bewertung der Angebote mit fallender subjektiver Datensicherheitskompetenz verschlechtert. Anfängerïnnen schätzen sie im Durchschnitt um 0,72 Einheiten, also eine Dreiviertel-Antwortkategorie, ungünstiger ein als Expertïnnen. Die Gründe dafür sind momentan unklar; auf jeden Fall gehört eine Evaluation der Angebote ins Pflichtenheft der Dienstleister. Die Führungskräfte der Wissenschaft unterscheiden sich hier nicht vom Rest der Befragten.

8 Information Security Awareness als Schutzreaktion vor Datenverlust

Positive oder negative Einstellungen, persönliche Erfahrungen der Beschäftigten sowie die Unternehmenskultur in Bezug auf Datensicherheit können die Einhaltung der Sicherheitsvorschriften verbessern oder beeinträchtigen (Bulgurcu et al. 2010; Colwill 2009; Herath und Rao 2009b). Die Identifizierung dieser persönlichen und organisatorischen Faktoren, welche die Einhaltung der Sicherheitsvorschriften durch Einzelpersonen bedingen, ist für die Gesamteffektivität der organisatorischen Sicherheit von wesentlicher Bedeutung und wird von uns im Folgenden als *information security awareness* (ISA) beschrieben. Auch für die Universität Bielefeld muss erfasst werden, welche Faktoren eine Erhöhung bzw. Verringerung der ISA bedingen, um eine Nachsteuerung zur Verbesserung der Informationssicherheit zu gewährleisten.

Die ISA wird grundsätzlich aus zwei Sichtweisen betrachtet: Zum einen wäre dies das *Ausmaß, in dem die Mitarbeiter[ïnnen] die vorgeschriebenen Verhaltensweisen, die von ihrer Organisation zur Informationssicherheit in Form von Regeln und Vorschriften herausgegeben werden, kennen und verstehen* (Bulgurcu et al. 2010). Diese Sichtweise deckt sich mit Ansichten aus den Anfängen der Forschung zur ISA, die davon ausgehen, dass Sicherheitsbewusstsein ein Zustand ist, in dem sich die Mitarbeiterïnnen der Sicherheitsziele ihres Unternehmens bewusst sind und sich idealerweise dafür einsetzen (Siponen 2000). Diese Vorgaben sind als Verhaltensmuster von dem jeweiligen Dienstherrn für seine Arbeitnehmerïnnen gedacht, damit Situationen, welche der Arbeitgebende als gefährlich einstuft, vermieden werden können. Zum anderen wird die ISA u.a. von Zerr (2007) als gedankliche Auseinandersetzung der Mitarbeiterïnnen mit dem Risiko ihres eigenen Verhaltens beschrieben. Das grundsätzliche Bewusstsein für Informationssicherheit ist hierbei definiert als das *allgemeine Wissen und Verständnis eines Mitarbeite[nden] über mögliche Probleme im Zusammenhang mit der Informationssicherheit und deren Auswirkungen* (Bulgurcu et al. 2010). Dieses Bewusstsein für Informationssicherheit kann durch eigene Lebenserfahrungen aufgebaut werden, wie beispielsweise durch einen Computervirenangriff geschädigt worden zu sein oder Quellen wie Fachzeitschriften gelesen zu haben, und ist individuell äußerst vielfältig.

Sicherheitsrichtlinien als soziale Normen

Soziale Normen stellen in den Sozialwissenschaften gesellschaftlich, organisational und kulturell bedingte Handlungsanweisungen für das Sozialverhalten dar. Solche Normen bringen Erwartungen der Gesellschaft an das Verhalten von Individuen zum Ausdruck.

Die Sicherheitsrichtlinien stellen den Grundsatz des Handelns einer Organisation und ihrer Mitglieder zum Schutz der physischen und IT-Ressourcen dar. Eine solche Sicherheitspolitik beinhaltet stets eine Erklärung der Organisationsabsicht, welche die Ziele und Prinzipien der Informationssicherheit unterstützt, eine Bestimmung der spezifischen Sicherheitsrichtlinien, Standards und Compliance-Anforderungen, eine Definition der allgemeinen und spezifischen Verantwort-

lichkeiten für alle Aspekte der Informationssicherheit sowie eine Erläuterung des Prozesses zur Meldung vermuteter Sicherheitsvorfälle (Lee 2004). Dabei stellen die Sicherheitsrichtlinien nicht nur Standards für das Verhalten der Mitarbeiter bei der Computersicherheit auf, sondern legen auch die mit diesem Verhalten verbundenen Pflichten fest. Durch die Ausarbeitung dieser Richtlinien bildet die Organisation ihre Normen, welche wir für diesen Bericht als normative Überzeugungen im Zusammenhang mit dem Verhalten der Computersicherheit definieren, die von den meisten Mitgliedern einer Organisation geteilt werden. Organisationale Normen über Computersicherheit als externe normative Überzeugungen können eine wichtige Rolle bei der Formulierung nicht nur der verinnerlichten normativen Überzeugungen (moralische Verpflichtung) eines Individuums über Computersicherheit spielen, sondern auch der subjektiven Norm der Einzelnen gegenüber Computersicherheitsverhalten, da die subjektiven Normen eines Individuums in einem organisatorischen Umfeld von Referenzgruppen wie Vorgesetzten oder Kollegïnnen beeinflusst werden können (Taylor 1995).

Organisationale Normen zur Datensicherheit können als soziale Norm einen direkten Einfluss auf die Verhaltensabsichten der Mitarbeiterïnnen haben, da nach der Theorie der sozialen Normen ein Großteil des Verhaltens von Individuen von ihrer Wahrnehmung des Verhaltens anderer Mitglieder ihrer sozialen Gruppe beeinflusst wird (Perkins 1986). Dieser Annahme folgend ist es nicht wahrscheinlich, dass einzelne Mitarbeiterïnnen ein sicherheitskonformes Verhalten zeigen, wenn der Großteil der Organisationsmitglieder die Richtlinien zu der Datensicherheit ignoriert. Analog dazu wird es weniger Personen geben, welche die Richtlinien vollständig missachten, wenn Sicherheitsverhalten von den entsprechenden Bezugsgruppen aktiv eingehalten und befürwortet wird. Es ist dabei zu beachten, dass es nicht zwingend notwendig ist, dass die Richtlinien bzw. ein bestimmtes Verhalten von Kontaktgruppen auch umgesetzt werden müssen, damit es einen Einfluss auf ein Individuum haben kann. Bereits die Wahrnehmung der Einstellung der Kontaktgruppen zu einem bestimmten Verhalten, kann eine Wirkung auf einzelne Beschäftigte haben (Perkins 1986).

Für die Informationssicherheit der Universität ist es deshalb von großer Bedeutung, welche Einstellungen die Beschäftigten zu den Sicherheitsrichtlinien besitzen und ob sie sichtbar sicherheitskonform handeln. Die so entstehende Unternehmenskultur könnte einen starken Einflussfaktor für die ISA darstellen. Je stärker die Sicherheitsrichtlinien in den organisationalen Normen vertreten sind und je stärker sich die Beschäftigten diesen Normen verpflichtet fühlen, desto weniger Risikoverhalten müsste von den Beschäftigten gezeigt werden. Doch auch eine stark ausgeprägte Organisationskultur kann nie allein für die notwendige Sicherheit sorgen, da die individuellen Eigenschaften der Beschäftigten so unterschiedlich sind, dass Richtlinien allein nicht helfen.

Individuelle Aspekte der Beschäftigten

Wird eine Person einer undurchsichtigen Situation ausgesetzt, wie bei einem potenziellen Phishing-Angriff, reagiert sie in der Regel instinktiv und beurteilt die Sachlage unterbewusst stets

auf eventuelle Risiken und die entsprechende Reaktion darauf. Dieses Verhalten wird mit der *Protection Motivation Theory* (PMT) beschrieben (Rogers 1975).

Nach der ursprünglichen Formulierung dieser Theorie initiiert eine Angst-Appell-Kommunikation kognitive Beurteilungsprozesse bezüglich der Schädlichkeit oder Schwere des bedrohenden Ereignisses, der Wahrscheinlichkeit des Auftretens des Ereignisses und der Wirksamkeit einer empfohlenen Bewältigungsreaktion. Dieser kognitive Beurteilungsprozess spiegelt sich anschließend in einer Schutzmotivation wider, welche Aktivitäten zum Schutz für sich Selbst und Andere vor Gefahren weckt, unterstützt und steuert (Maddux & Rogers 1983). Eine Reihe von Studien, die sich auf sicherheitsrelevante Verhaltensweisen von Computern beziehen, haben von der PMT inspirierte Fragen über Personen, die sich der Sicherheitsbedrohungen bewusst sind und Überzeugungen über die wahrgenommene Schwere und Wahrscheinlichkeit der Bedrohung bilden, in ihre Studien aufgenommen und dann die Wirksamkeit der möglichen Reaktion gegen die Überzeugungen bewertet (Anderson & Agarwal 2010). Die meisten von ihnen haben gezeigt, dass die PMT-Dimensionen - wahrgenommene Bedrohungsschwere, wahrgenommene Bedrohungsschwäche, Reaktionswirksamkeit sowie Selbstwirksamkeit - die Einstellung einer Person gegenüber sicherheitsrelevantem Verhalten oder Verhaltensabsichten beeinflussen (Workman et al. 2008; Lee und Larsen 2009; Anderson & Agarwal 2010; Johnston & Warkentin 2010). Selbstwirksamkeit ist die Überzeugung einer Person adaptives Verhalten auszuführen. Selbstwirksamkeitsforscher argumentieren, dass Veränderungen in der Erwartung an die eigene Selbstwirksamkeit und Veränderungen im Verhalten positiv korrelieren (Bandura et al. 1980). Eine breite Palette von PMT-bezogenen Studien hat ergeben, dass Selbstwirksamkeit einen signifikanten, positiven Zusammenhang zwischen Einstellung und Absicht, proaktives Verhalten zu praktizieren, aufweist (Maddux & Rogers 1983; Maddux & Stanley 1986; Tanner et al. 1989). Darüber hinaus haben fast alle sicherheitsrelevanten Studien einschließlich die der Selbstwirksamkeit gezeigt, dass diese Selbstwirksamkeit einen starken Einfluss auf die Einstellung oder das Sicherheitsverhalten einer Person hat (Woon et al. 2005; Anderson & Agarwal, 2010; Johnston & Warkentin 2010). Für die Bewertung der Informationssicherheit in der Universität würde dies bedeuten, dass weniger Sicherheitsverstöße von den Beschäftigen begangen werden, wenn sie davon überzeugt sind, die Gefahren für die Datensicherheit einschätzen und ihr eigenes Verhalten anschließend daran anpassen zu können.

Analyse der Einflüsse auf das Sicherheitsverhalten der Beschäftigten

Um die erwähnten individuellen und organisationalen Aspekte mittels statistischer Verfahren überprüfen zu können, wurden aus der durchgeführten Befragung 31 Aussagen ausgewählt, welche den theoretischen Vorüberlegungen entsprechend einen Einfluss auf das Sicherheitsverhalten der Beschäftigten haben könnten (vgl. Tab. 8.1). Die Teilnehmerïnnen sollten bei diesen Fragen auf einer Skala (von 1 „überhaupt nicht“ bis 4 „voll“) angeben, inwiefern die entsprechende Aussage zutrifft.

Tabelle 8.1: Deskriptive Daten der unabhängigen Variablen

Aussage	N	M	Faktor
Datensicherheit ist bei uns "auf dem Flur" ein Thema.	669	2,49	Organisationale Normen
Meine KollegInnen achten auf die Datensicherheit.	592	2,99	Organisationale Normen
Es stört meine KollegInnen, wenn ich die Datensicherheit ignoriere.	476	2,65	Organisationale Normen
Mein/e Vorgesetzte/r findet es gut, wenn ich mich aktiv um die Datensicherheit bemühe.	505	3,28	Organisationale Normen
Es wird von mir mit Nachdruck erwartet, dass ich die Datensicherheit beachte.	628	2,76	Organisationale Normen
Wer in meiner Umgebung Sicherheitsrisiken eingeht, muss damit rechnen, von den KollegInnen ermahnt zu werden.	588	2,53	Organisationale Normen
In meiner Umgebung kann man die Datensicherheit ignorieren, ohne dass es jemanden interessiert.	607	2,80	Organisationale Normen
Sie enthalten sensible Informationen.	727	2,79	Wahrgen. Bedrohung
Sie sind für unbefugte Dritte attraktiv.	707	2,37	Wahrgen. Bedrohung
Sie dienen den organisatorischen Abläufen.	698	2,65	Wahrgen. Bedrohung
Es wäre für mich persönlich ein Problem, wenn sie in falsche Hände geraten würden.	699	2,85	Wahrgen. Bedrohung
Es wäre ein Problem für die Universität, wenn sie in falsche Hände geraten würden.	703	2,74	Wahrgen. Bedrohung
Ich brauche mehr Schulungsangebote zur Datensicherheit.	674	2,36	Selbstwirksamkeit
Für Fragen zur Datensicherheit habe ich innerhalb der Universität ausreichend Informationsquellen.	631	2,67	Selbstwirksamkeit
Ich bin über die Regelungen der Universität zur Datensicherheit gut informiert.	678	2,47	Selbstwirksamkeit
Bei einem Datensicherheitsproblem wüsste ich, an wen ich mich wenden muss.	683	3,02	Selbstwirksamkeit
In Fragen der Datensicherheit bin ich immer sicher, wie ich mich verhalten muss.	681	2,49	Selbstwirksamkeit
Das Bewusstsein der Beschäftigten für Datensicherheit ist wichtig für die Universität.	675	3,62	Skepsis
Mein individuelles Verhalten beeinflusst die Datensicherheit der Universität.	656	3,06	Skepsis
Das Verhalten von Beschäftigten als Sicherheitsfaktor wird überbewertet.	614	1,76	Skepsis
Ich treffe alle mir möglichen Vorkehrungen gegen Verletzungen der Datensicherheit.	652	3,10	Proaktives Verhalten

Aussage	N	M	Faktor
Ich befürworte die Einhaltung der Datensicherheit.	663	3,64	Proaktives Verhalten
Ich informiere mich aktiv über Datensicherheit.	661	2,79	Proaktives Verhalten
Die Datensicherheit wird von meinen KollegInnen als Hürde im Arbeitsalltag angesehen.	573	2,63	Vorbehalte
Die Wahrung der Datensicherheit erschwert meine Arbeit.	647	2,43	Vorbehalte
Ich bekomme täglich mehr E-Mails, als ich beantworten kann.	654	2,25	Belastung
Ich arbeite oft unter Zeitdruck.	657	3,05	Belastung
In meiner Rolle als MitarbeiterIn der Universität stelle ich ein lukratives Ziel für Cyberkriminelle dar.	641	2,27	-
Wenn ich bemerken würde, dass KollegInnen die Datensicherheit nicht einhalten, würde ich sie darauf ansprechen.	639	3,20	-
Ich hätte ein schlechtes Gewissen, wenn ich die Datensicherheit missachten würde.	664	3,54	-
Die bisher aufgetretenen Probleme mit der Datensicherheit wurden von den Verantwortlichen zeitnah gelöst.	335	2,87	-

N: Fallzahl · M: Mittelwert · Gesamt N = 778

Große Variablensets zeichnen sich oft dadurch aus, dass sich bei einer hohen Zahl an Variablen bzw. Aussagen einige inhaltlich überschneiden. Statistisch drückt sich dies in Korrelationen zwischen den Aussagen aus. Mittels einer exploratorischen Faktorenanalyse können Beziehungszusammenhänge in einem großen Variablenset insofern strukturiert werden, als sie Gruppen von Variablen identifiziert, die stark miteinander korrelieren und diese bündelweise von weniger korrelierenden trennt (Backhaus et al. 2011). Die so gefundenen Gruppen von jeweils hoch korrelierenden Variablen werden als Faktoren bezeichnet. Diese Art der Dimensions- oder Datenreduktion ist sinnvoll, um latente Konzepte aufzudecken, die hinter den Variablenbündeln stecken. Für die 31 in Tabelle 8.1 gelisteten Aussagen ließen sich so sieben Faktoren bestimmen und entsprechend ihrer inhaltlichen Überschneidung benennen (Tab. 2). So können bspw. die Items „Ich bekomme täglich mehr E-Mails, als ich beantworten kann“ und „Ich arbeite oft unter Zeitdruck“ unter dem Begriff „Belastung“ zusammengefasst werden. Die entsprechend den Faktoren zugehörigen Variablen können Tabelle 8.1 entnommen werden. Die Nummerierung der einzelnen Faktoren ist dabei systembedingt.[8] Vier der Aussagen ließen sich nicht eindeutig einem der gefunde-

8 Das Statistikprogramm SPSS sortiert die gefunden Faktoren automatisch nach der Höhe des Eigenwerts der Faktoren, so dass der Faktor mit der niedrigsten Nummer stets den höchsten Eigenwert und somit die größte Varianzaufklärung zeigt während die höchste Faktornummer am wenigstens Varianz erklären kann.

nen sieben Faktoren zuordnen und wurden deshalb aus der Analyse ausgeschlossen (siehe Tabelle 8.1, unten). Die Faktoren *Skepsis* und *Vorbehalte* sind dabei nicht synonym zu verwenden: Skepsis stellt hier die gedanklich negative Vorbelastung in Bezug auf Datensicherheit dar, während Vorbehalte konkrete Hemmnisse für den Arbeitsalltag repräsentieren.

Tabelle 8.2: Ergebnisse Faktorenanalyse

Faktor	Variablenanzahl	Label
1	7	Organisationale Normen
2	5	Wahrgenommene Bedrohung
3	5	Selbstwirksamkeit
4	3	Skepsis
5	3	Proaktives Verhalten
6	2	Vorbehalte
7	2	Belastung

Risikoverhalten

Wie bereits beschrieben wurde der Frageblock aus Tabelle 6.1 aufgrund des Mangels an empirisch messbarem abweichenden Verhalten verwendet. Die gewählten Items fragen Verhalten ab, welches den Sicherheitsrichtlinien der Universität Bielefeld zufolge von den Beschäftigten eingehalten werden soll, um den Missbrauch oder den Verlust von Daten zu verhindern. Zudem werden die meisten dieser Verhaltensweisen bei Nichteinhalten als Gefahr für die Datensicherheit beschrieben (vgl. Universität Bielefeld (2019): Regelungen zur Informationssicherheit an der Universität Bielefeld).

Um dieses Risikoverhalten in einer statistischen Analyse verwenden zu können, wurde eine neue Variable gebildet, welche die Abweichungen von den Sicherheitsrichtlinien insgesamt für jede/n Teilnehmerïn zählt (vgl. Tab. 8.3). Dafür wurden die Items so umgepolt, dass ein „Nein“ sicherheitskonformes und ein „Ja“ abweichendes Verhalten darstellt. Eine Person, welche bspw. die dienstlichen E-Mails an einen privaten Mailanbieter weiterleitet und Online-Oberflächen von Drittanbietern für dienstliche Dokumente nutzt, würde den Wert 2 in dieser Zählvariable erhalten.

Des Weiteren wurde überprüft, ob diese zehn Variablen überhaupt eine Korrelation aufweisen, um sich in einer gemeinsamen Variablen zusammenfassen zu lassen.[9] Die Variablen „Wenn ich Unterlagen auf einem Gemeinschaftsdrucker ausdrucke, hole ich sie umgehend ab.“ sowie „Ich schließe an meinen privaten PC auch USB-Sticks der Universität an.“ mussten aufgrund man-

9 Da hier ausschließlich dichotom ausgeprägte Variablen vorliegen, kann dies nicht über eine Faktorenanalyse geschehen. Aus diesem Grund wurden für alle Variablenkombinationen bivariate Korrelationen berechnet. Die Items, welche mit weniger als drei anderen Variablen aus dem Block mindestens mit 0,1 korrelieren, wurden aus der Auswahl entfernt.

gelnden Zusammenhangs mit den anderen acht Items ausgeschlossen werden, so dass der Maximalwert der neu gebildeten Variable Risikoverhalten nun acht beträgt. Dieser wurde allerdings von niemandem erreicht.

Tabelle 8.3: Zählvariable abweichendes Verhalten (AV)

Abweichungen	Häufigkeit	Prozent	kum. Prozent
0	103	15,2	15,2
1	158	23,2	38,4
2	191	28,1	66,5
3	135	19,9	86,4
4	57	8,5	94,9
5	29	4,3	99,2
6	5	0,7	99,9
7	1	0,1	100,0
8	0	0,0	100,0

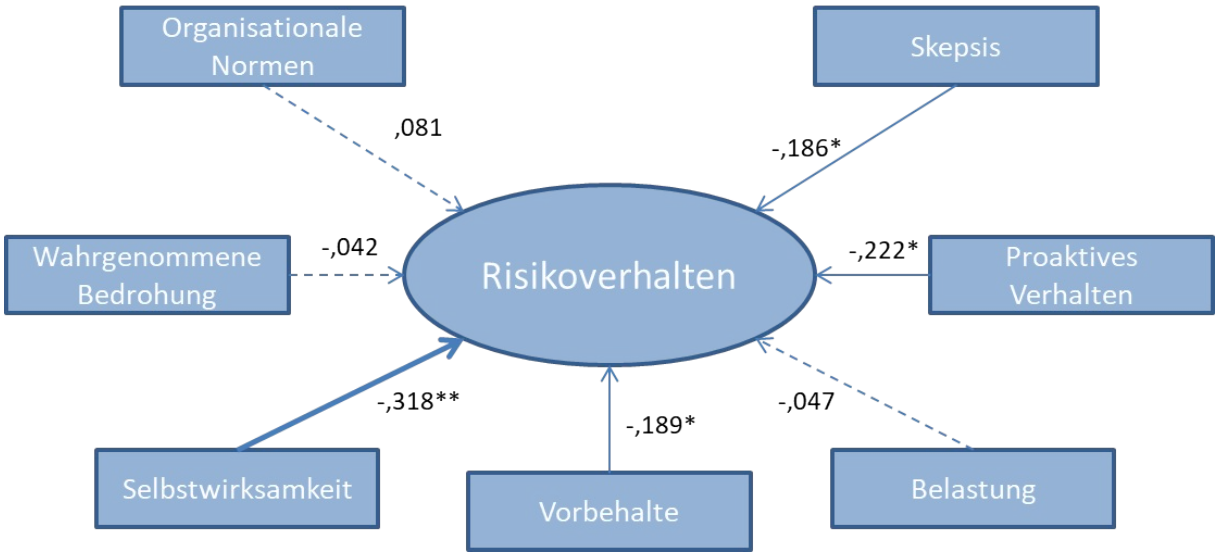
Gesamt N = 679, M=1,98

Aus Tabelle 8.3 lässt sich erkennen, dass die Mehrheit der Befragten (66,5 %) zwei oder weniger Kriterien erfüllen, welche als Risikoverhalten definiert sind. Das obere Ende der Skala bilden lediglich 1,8 % der Beschäftigten, die fünf oder mehr Fällen risikoreichen Verhalten gezeigt haben.

Einflüsse auf Risikoverhalten

Es kann nun mittels einer Regressionsanalyse festgestellt werden, welchen Einfluss die in Tabelle 8.2 gefundenen Faktoren auf das Risikoverhalten der Beschäftigten besitzen. Eine solche Analyse kann Zusammenhänge zwischen einer abhängigen und einer oder mehreren unabhängigen Variablen aufdecken. Für das Modell der Beschäftigtenbefragung könnte dies bspw. bedeuten: Je höher die *Belastung* desto höher das *Risikoverhalten*. Die tatsächlichen Ergebnisse sind in Tabelle 8.4 dargestellt und für eine bessere Lesbarkeit in Abb. 8.1 grafisch dargestellt.

Abbildung 8.1: Effektstärken der Einflüsse auf das Risikoverhalten



Anmerkung: * und ** geben zweiseitige Signifikanz auf dem 90%- bzw. 95%-Signifikanzniveau an

Zunächst ist ersichtlich, dass die Effektstärken der Faktoren *Organisationale Normen*, *Wahrgenommene Bedrohung* und *Belastung* nicht signifikant sind und somit nicht von einem Einfluss auf das *Risikoverhalten* ausgegangen werden kann. Die *Selbstwirksamkeit* weist ein sehr signifikantes Ergebnis auf, während *Skepsis*, *Proaktives Verhalten* und *Vorbehalte* signifikante Werte zeigen. Anhand der unstandardisierten Beta-Koeffizienten aus der Analyse kann die Effektstärke abgelesen werden. Im Fall der *Selbstwirksamkeit* bedeutet dies, dass die Anzahl der Sicherheitsverstöße sinkt, wenn die Selbstwirksamkeit steigt (-,324). Gleiches gilt für *Skepsis* (-,199), *Proaktives Verhalten* (-,224) und *Vorbehalte* (-,189). Dementsprechend bildet der Faktor Selbstwirksamkeit den stärksten Einfluss auf die Häufigkeit der Sicherheitsverstöße. Es lassen folgende Zusammenhänge formulieren:

- Je *größer* die Selbstwirksamkeit der Beschäftigten, desto *geringer* ist das Risikoverhalten.
- Je *geringer* die Skepsis gegenüber Datensicherheit, desto *geringer* ist das Risikoverhalten.
- Je *höher* das proaktive Verhalten der Beschäftigten im Bereich Datensicherheit ausfällt, desto *geringer* ist das Risikoverhalten.
- Je *geringer* die Vorbehalte gegenüber der Datensicherheit, desto *geringer* ist das Risikoverhalten.

Tabelle 8.4: Lineare Regression, AV Risikoverhalten

Faktor	Label	Effektstärke	Signifikanz
1	Organisationale Normen	,081	,398
2	Wahrgenommene Bedrohung	-,042	,645
3	Selbstwirksamkeit	-,318**	,002
4	Skepsis	-,186*	,063
5	Proaktives Verhalten	-,222*	,031
6	Vorbehalte	-,189*	,035
7	Belastung	-,047	,632

R^2 = ,130, Adj. R^2 = ,106

Die Aussagen, welche die Grundlage für die Faktoren *Vorbehalte* und *Skepsis* bilden, wurden während der Aufbereitung des Datensatzes umgepolt, um eine einheitliche Skala verwenden zu können (hohe Werte bedeuten geringe Vorbehalte). Dementsprechend bedeutet das Ergebnis aus der Regression für diesen Faktor, dass die Anzahl der Sicherheitsverstöße steigt, wenn die Beschäftigten Vorbehalte gegen die Datensicherheit haben.

Bedeutung der Ergebnisse

Da der Faktor der *Organisationalen Normen* keinen Einfluss aufweist, kann nicht geschlossen werden, dass weniger Sicherheitsverstöße von Beschäftigten begangen werden, wenn die Sicherheitslinien stark in den organisationalen Normen vertreten sind. Dies bedeutet entweder, dass im Bereich der Datensicherheit die angenommenen Einfluss-Effekte von Peer-Gruppen nicht gelten oder dass diese Effekte in dieser expliziten Organisation weniger stark (bis hin zu überhaupt nicht) vertreten sind. Letzteres lässt sich anhand der Daten aus diesem Survey nicht überprüfen, da die Erhebung nur in der Universität Bielefeld stattfand und eine Vergleichbarkeit für das Vorhandensein einer sozialen Beeinflussung in anderen Organisationen nur möglich wäre, wenn dort die gleiche Befragung durchgeführt worden wäre. Aus den Antworten den Frageblocks 10 (siehe Anhang) wird jedoch deutlich, dass Datensicherheit kein regelmäßiges Gesprächsthema in der Universität ist, da die Befragten häufig angaben, nichts über das Sicherheitsverhalten über ihre Kollegïnnen und Vorgesetzten sagen zu können.

Eine mögliche Erklärung für den fehlenden Einfluss organisationaler Normen auf die Datensicherheit könnte die mangelnde Überprüfbarkeit sein. Ob ein/e Mitarbeiterïn einen privaten oder einen dienstlichen USB-Stick verwendet, ist nicht auf Anhieb ersichtlich, sodass von den Beschäftigten weder vorbildliches bzw. konformes Verhalten erkannt, noch abweichendes Verhalten sanktioniert werden kann (z.B. durch mündliche Hinweise). Auch was auf dem jeweiligen PC der Beschäftigten passiert, bleibt weitestgehend unsichtbar, da es sich bei Computerarbeitsplätzen in der Regel um Individualplätze handelt. Vor allem, da jede/r Arbeitnehmerïn einen eigenen Benut-

zerïnnen-Account besitzt, welcher für die Kollegïnnen nicht zugänglich ist. Es kann also weder konformes Verhalten beobachtet und somit nachempfunden werden, noch können Abweichungen schnell bemerkt und beeinflusst werden. Es stellt sich hier die Frage, ob das Vorhandensein der Sicherheitsrichtlinien als Gesprächsthema ausreicht, damit eine soziale Norm entsteht, welche einen Effekt auf das Verhalten der Beschäftigten besitzt oder, ob ein solches Verhalten tatsächlich beobachtbar sein muss, um als soziale Norm aufgenommen zu werden. Ein mögliches Problem bei der Durchsetzung der Sicherheitsrichtlinien über die organisationalen Normen könnte also die mangelnde Sichtbarkeit abweichenden bzw. konformen Verhaltens sein.

Die unabhängigen Variablen *Proaktives Verhalten* und *Vorbehalte* weisen beide ein signifikantes Ergebnis und somit einen Einfluss auf das *Risikoverhalten* auf. Je positiver Beschäftigte der Datensicherheit gegenüberstehen, desto weniger Sicherheitsverstöße werden begangen. Der Faktor *Proaktives Verhalten* erscheint hier zunächst tautologisch, da davon auszugehen ist, dass jemand, der einen hohen Wert bei sicherheitskonformen Verhaltensvariablen aufweist, auch weniger Sicherheitsverstöße begeht. Die Variablen, welche diesen Faktor repräsentieren, bilden jedoch eher eine reflektierte Bewertung über das eigene Verhalten ab, als konkrete Handlungsweisen wie in der abhängigen Variablen. Es könnte also auch formuliert werden, dass Beschäftigte weniger Sicherheitsverstöße begehen, wenn sie davon überzeugt sind, ihren individuell Beitrag zum Datenschutz geleistet zu haben. Beschäftigte, welche die Sicherheitsrichtlinien als Hindernis für den Arbeitsalltag ansehen, werden zudem weniger stark darauf achten, diese einzuhalten, damit sie ihren eigenen Arbeitsprozess optimieren können. Diese Annahme erscheint logisch vor dem Hintergrund, dass das Einhalten der Richtlinien immer auch mit einem Mehraufwand verbunden ist und das Ignorieren keinen unmittelbaren Nachteil mit sich bringt.

Die Betrachtung der Faktoren auf der Personenebene liefert ein sehr deutliches Ergebnis. *Skepsis* und *Selbstwirksamkeit* zeigen starke Einflusseffekte, während *Wahrgenommene Bedrohung* sowie *Belastung* keine Wirkung auf das Einhalten der Sicherheitsrichtlinien besitzen. Laut *Protection-Motivation-Theory* müsste zumindest die Wahrnehmung der Bedrohung und eine damit einhergehende Reaktionswirksamkeit beeinflussende Effekte aufweisen. Bei genauerer Betrachtung der Variablen wird allerdings deutlich, dass hier auch ein mangelndes Wissen über die Relevanz der eigenen Daten die Ursache darstellen könnten, während das grundsätzliche Bewusstsein der eigenen Angreifbarkeit eher in dem Faktor *Skepsis* zu finden ist. Diese müsste dementsprechend den Label-Zusatz *Bewusstsein* erhalten, da der zugrundeliegende Faktor auch Variablen enthält, die eine Selbsteinschätzung über die eigene Rolle innerhalb der Datensicherheit darstellen.

Aus den Ergebnissen für den Faktor der *Selbstwirksamkeit*, welcher zu einem großen Teil die eigene Kompetenz im Bereich Datensicherheit einschließt, lässt sich das Konzept der PMT für die Beschäftigten der Universität bestätigen: *Wenn sich Beschäftigte im Klaren darüber sind, dass Verstöße gegen die Sicherheitsrichtlinien ein Problem sind und dass sie selbst etwas dagegen tun können, besteht eine Chance, dass ein Verhalten gezeigt wird, welches Verstößen vorbeugt*. Sollten die Beschäftigten nun aufgrund ihrer eigenen Kompetenz wissen, wie ein Datensicherheitsproblem er-

kannt und wie damit umgegangen werden muss, sinkt die Höhe des eigenen *Risikoverhaltens* deutlich. Eine Person, die sich der Sicherheitsbedrohungen bewusst ist und Überzeugungen über die wahrgenommene Schwere und Wahrscheinlichkeit der Bedrohung bildet, kann also einschätzen, ob aus Risikoverhalten Probleme für die Person selbst oder die Organisation entstehen. Dies resultiert aus dem hohen Einfluss des Faktors Selbstwirksamkeit, da dieser ein bestimmtes Maß an Wissen voraussetzt, sich mit Problemsituationen auseinandersetzen zu können. Wer sich selbst zu helfen weiß oder weiß, wo sie/er Hilfe suchen kann, ist mutmaßlich auch in der Lage, Sicherheitsverstöße zu erkennen und diese bereits im Vorfeld zu vermeiden. Es kann also festgestellt werden: *Je höher die eigene Kompetenz im Bereich Datensicherheit von den Beschäftigten eingeschätzt wird, desto weniger Sicherheitsverstöße werden begangen*. Einen weiteren Beleg dafür stellt die bereits erwähnte Validierung der eingangs im Survey gestellten Selbsteinschätzung der Teilnehmenden als Expertïn, Fortgeschrittene/r oder Anfängerïn dar. Diejenigen Personen, die sich selbst als Expertïnnen klassifiziert haben, wiesen bei der Abfrage der zwölf Fachtermini eine deutlich niedrigere Quote an Fehleinschätzungen auf, als die anderen beiden Gruppen und die Fortgeschrittenen eine niedrigere Fehlerrate als die Anfängerïnnen (vgl. Kap. 5).

Es kann grundsätzlich festgehalten werden, dass sich aus der Datenlage keine nennenswerten Einflüsse auf die Einhaltung der Sicherheitsrichtlinien bedingt durch organisationalen Normen der Universität Bielefeld ergeben. Die Ergebnisse zeigen, dass individuelle Kompetenzen und das Wissen der Einzelnen eine verringernde Wirkung auf die Anzahl der getätigten Sicherheitsverstöße aufweisen. Dementsprechend handelt es sich hier um einen Zusammenhang, innerhalb dessen das individuelle Profil der Beschäftigten, welches nicht oder nur wenig von der Organisation geprägt wurde, für die Entstehung und Einhaltung einer Sicherheitskultur verantwortlich ist. Ein sicherheitskonformes Verhalten durch das Aufstellen von Richtlinien durch den Arbeitgebenden konnte nicht als ausreichend zur Vermeidung von Sicherheitsverstößen festgestellt werden. Das Zurückgreifen auf die eigenen oder von der Universität zur Verfügung gestellten Ressourcen stellt den größten Einfluss bei der Vermeidung von Risikoverhalten dar. Der Information Security Awareness Begriff kann für die Universität Bielefeld also als bewusste, gedankliche Auseinandersetzung der Beschäftigten mit den möglichen Problemen für die Informations- bzw. Datensicherheit auf Grundlage des vorhandenen Wissens verstanden werden. Je intensiver sich die Beschäftigten mit diesen Problemen auseinandersetzen, desto geringer ist die Wahrscheinlichkeit, dass sie risikoreiches Verhalten im Bereich Datensicherheit zeigen.

9 Kommentare der Befragten

Die vorstehenden Kapitel haben Fragen zu Themenkomplexen ausgewertet, die aus der Sicht der Forschenden die Lage der Datensicherheit charakterisieren. Geschlossene Fragen reproduzieren aber vorhandenes Wissen und sind bekanntermaßen ungeeignet, Probleme abzubilden, die über die Perspektive der Forschenden hinausgehen. Wir haben deshalb am Ende des Fragebogens Gelegenheit zu weiteren Aussagen gegeben („Hier finden Sie Platz für inhaltliche Anmerkungen.“).

Davon haben 90 Personen Gebrauch gemacht. Die Äußerungen umfassen einige schlichte Grußformeln („Viel Erfolg!“). Mehrheitlich kommentieren sie aber die Themen der Befragung auf einer inhaltlichen Ebene. Es liegen einige detaillierte Schilderungen vor. Der längste Eintrag umfasst 1.304 Zeichen bzw. 224 Wörter. Wir reproduzieren thematisch geordnet Auszüge im Wortlaut. Offensichtliche Schreibfehler haben wir im Interesse der besseren Lesbarkeit korrigiert. Wo wir zum Schutz der Vertraulichkeit Namen und Bezeichnungen entfernen mussten, ist dies durch Ellipsen in eckigen Klammern kenntlich gemacht.

Informationsbedürfnis und Kritik an der Informationspolitik

Zunächst wird ein Wunsch nach mehr Information und Beratung zu Datensicherheits- und Datenschutzfragen offensichtlich. Der Datenschutz war zwar nicht Gegenstand der Umfrage, wird aber im Zusammenhang mit der Informationssicherheit gesehen. Scheinbar hat sich auch bei vielen Befragten der Eindruck festgesetzt, auf die Konsequenzen der im Jahr zuvor in Kraft getretenen europäischen Datenschutz-Grundverordnung (DS-GVO) nicht ausreichend vorbereitet zu sein.

> „Ich wünsche mir mehr Datenschutz-Schulungen“
>
> „Es wäre total hilfreich, mehr Datenschulungen zu haben zu Datensicherheit und Forschungsdaten usw. Ich fühle mich überhaupt nicht gut vorbereitet in Sachen Datensicherheit, ich arbeite als Mitarbeiterin mit personenbezogenen Daten und wünsche mir einfach ein erweitertes und intensives Supportsystem hierbei von der Uni Bielefeld.“
>
> „Ich würde mich über mehr konkrete Infos zur Datensicherheit, und wie sie sich praktikabel umsetzen lässt, freuen (z.B. Darf ich Studierenden ihre Noten per Email mitteilen? Falls weder uneingeschränkt ja oder nein, unter welchen Umständen ja oder nein?)“
>
> „Einheitliche Anweisungen zur Umsetzung der DSVGO aus der Zentralen Verwaltung wären wünschenswert und hilfreich. Gerne mehr Schulungsangebote zu diesem Thema für Wissenschaftler, die mit Forschungsdaten arbeiten“
>
> „Ich würde mich über zusätzliche Angebote zur Datensicherheit, wie z.B. eine Schulung freuen!“
>
> „Eine Fortbildungsreihe der Uni mit unterschiedlichen Fokussierungen wäre super.“

„Sciebo nutze ich auf Eigeninitiative, da ich nur noch an einem Laptop arbeite um eine doppelte ‚Dateiführung' zu vermeiden. Vorher waren meine Daten nur gesichert, wenn ich an ein manuelles Backup gedacht hatte. Ich denke hier gibt es deutlichen Schulungsbedarf. Gefahr ist ja nicht nur der Datenklau über Dritte, sondern auch einfach das Verlieren von Unterlagen. Bei mir wäre auch eine Katastrophe, wenn ich mit dem Fahrrad einen Unfall hätte und der Laptop einfach Schrott."

„Eine kurze Anleitung für jede(n) Mitarbeiter(in) und alle Neueinstellungen zur Handhabung der Datensicherheit müsste verpflichtend sein!"

„Ich erkenne ein ‚kleines' Dilemma... Wie wäre es mit verpflichtenden Schulungen für alle Uni-Mitarbeiter*innen?"

„Another big security issue is that often emails from the BITS informing us about suspicious/ phishing emails are only written in German. As a lot of the scientists are not native German speakers, I think this poses an important security risk. Always write these emails in German AS WELL as English."

Den Wunsch nach mehr Information tragen manche Befragte in einem unzufriedenen Ton vor:

„Als wissenschaftlicher Mitarbeiter kriegt man GAR KEINE Informationen, wie man sich im Sinne der Datensicherheit verhalten soll."

„[Der Datenschutz] sollte kundenorientierter arbeiten und ansprechbarer sein und nicht nur Links mit sehr langen allgemeinen Hinweisen versenden, die bei konkreten Fragen nicht hilfreich sind, da allgemein"

„Cybersecurity is of utmost importance in this digital age. Would be great if we as University employees, are notified swiftly about any possible threats. [...]"

„Mir fehlen Empfehlungen bzw. klare Regelungen von oben, durch die Vorgesetzten, die Uni insgesamt. Alles was ich für den Datenschutz tue oder auch nicht ist mir selbst überlassen. Es prüft niemand nach. Informationen über geltende Regeln an der Uni muss man sich selbst suchen. Der Internetauftritt der Uni ist dazu viel zu unübersichtlich."

„Von Datensicherheit erfahre ich eher aus dem Radio, als von der Uni."

„Viele Fragen zur DSGVO wurden immer noch nicht beantwortet. Problem ist der personelle Engpass. So laviert man sich so durch. Das war wenig vorausschauend von Seiten der Universität."

„Es gibt keine Fortbildungen für Informatik oder PC Gebrauch an der Uni. Unser IT und Datensicherheitsbeauftragter arbeitet alleine mit 2 studentischen Hilfskräften und ist für eine gesamte Fakultät zuständig. Auch meine studentischen Hilfskräfte müssten geschult werden, dazu sehe ich mich nicht in der Lage. Die Regelungen der Uni sind nicht klar was Datensicherheit auf PC angeht und man muss sie sich mühsam erfragen/aneignen. Wenn man an die Uni kommt, wird einem das nicht in einer Einführungsveranstaltung für Forschende/Lehrende beigebracht. Solche Dinge verändern sich ständig und müssten kontinuierlich in Fortbildungen angeboten werden."

Nicht allen Bediensteten, so muss man das letzte Zitat deuten, sind die durchaus vorhandenen Fortbildungsangebote der Universität bekannt.[10] Andererseits muss die Universität überlegen, wie sie eine Kultur der Fortbildung so etablieren kann, dass die Nutzung für breitere Kreise zu einer Selbstverständlichkeit wird. Die Anregung, die Kommunikation mit Bediensteten konsequent zweisprachig zu halten, dürfte mit wenig Aufwand umsetzbar sein.

Dilemmata der Wissenschaftlerïnnen

Den quantitativen Daten zufolge verhalten sich insbesondere Wissenschaftlerïnnen in Führungspositionen risikobereiter als andere Gruppen. Eine Reihe von Einträgen begründet dies mit fachlichen Zwängen und Defiziten der von der Universität bereitgestellten Infrastruktur:

> „Forschung ist international. Ohne internationale Standards haben universitäre Datenschutzrichtlinien nur den Effekt, Kollaboration mit externen Kollegen zu erschweren. Das gilt insbesondere für Cloud-Datenspeicherung und Videotelefonie. Sciebo ist als Alternative zu Dropbox zwar nett gedacht, aber die Beschränkung auf teilnehmende Universitäten in NRW macht es weitgehend unbenutzbar. In Sachen Videotelefonie gibt es de facto keine Alternative zu Skype. Realistisch gesehen, sind Skype und Dropbox für junge Forscher unverzichtbar. Wie so oft ist der Gruppenzwang stärker als der gute Wille zum Datenschutz. Es wäre töricht, die Kommunikation mit einem gestandenen internationalen Experten über Skype oder Dropbox auszuschlagen, nur um die Datenschutzrichtlinien der Universität Bielefeld zu wahren. Als Nachwuchswissenschaftler an der Universität Bielefeld kann ich nicht von Professoren aus Princeton oder Harvard verlangen, meine Kommunikationswege zu nutzen, ohne den Abbruch des Kontakts in Kauf zu nehmen."

> „Als Stipendiat (Doktorand) war mir bis vor kurzem der Dienst sciebo versperrt (nur für Mitarbeiter, ich bin offiziell Student). Auch auf explizite Nachfrage wurde sciebo nicht für Doktoranden freigeschaltet. Mir ist Datensicherheit sehr wichtig (weswegen ich einen bei mir privat selbst gehosteten vergleichbaren Cloud-Dienst nutze), aber bei bei einer solchen Ignoranz gegenüber Doktoranden seitens der IT-Verantwortlichen kann ich alle KollegInnen verstehen, die auf Dropbox / Google Drive / ... ausweichen."

> „Der Uni fehlt eine praxistaugliche Kollaborationsplattform für die Bearbeitung sensibler Forschungsdaten mit externen. Einige Forschungsdaten müssen inhouse bleiben, dürfen also nicht in sciebo liegen und sollen trotzdem von anderen bearbeitet werden können. Die FH Bielefeld hat so etwas bereits im Einsatz. Bei uns werden Workarounds und Lösungen gefunden, die nicht sicher sind."

> „[Es] werden Cloud-Dienste abgelehnt. Stattdessen arbeiten wir mit teilweise anwenderunfreundlicher Software, die vom Anbieter nicht mehr im vollen Umfang weiterentwickelt wird."

> „Die Uni muss einen vollwertigen legalen Ersatz für Google-Docs und Overleaf/Sharelatex bereit stellen, wenn wir Wissenschaftler ‚legal' und effizient kooperieren können sollen."

10 z. B. die Schulungen „IT-Sicherheit für Sekretariate", „IT-Sicherheit für Mitarbeiterinnen und Mitarbeiter", „Daten sicher handhaben: Ablage, Verschlüsselung, Backup", „Phising und Social Engineering Angriffe - Erkennen und vermeiden" des Dezernats Personal und Organisation

„Der sichere Umgang mit Daten in Forschungsprojekten, die teilweise außerhalb der Universität stattfinden, ist kompliziert. Die Uni hat dafür kaum taugliche zentrale Infrastrukturen, und jeweiligen IT-Beauftragten sind unterschiedlich gut in der Lage, Lösungen anzubieten, die über das ‚pro forma' hinausgehen. Meiner Erfahrung gemäß schleift hier sehr viel."

„Leider ist das Angebot des BITS eher schlecht, so dass viele Kollegen Clouddienste nutzen oder wichtige Daten ohne Backup auf externen Datenträgern lagern."

„Wieso muss man sciebo alle 6 Monate verlängern, kein Wunder dass dann viele lieber auf die amerikanischen Dienste zugreifen"

Wissenschaftlerïnnen sind häufig an Arbeitsplätzen außerhalb des Campus tätig. Sie nutzen dabei regelmäßig private Hard- und Software. Die fehlende Abgrenzung zwischen inner- und außeruniversitären Arbeitsplätzen drückt einerseits die – erwünschte - Offenheit der Wissenschaft aus. Andererseits ergibt sie sich aber schlicht aus dem Mangel an Büroarbeitsplätzen für den wissenschaftlichen Nachwuchs und Gastwissenschaftlerïnnen und an Ressourcen, um Wissenschaftlerïnnen mit leistungsfähigen Dienstgeräten auszustatten. Die Nutzung privater Geräte (bring your own device, BYOD) wird von den Sicherheitsverantwortlichen der Universität als potentielles Problem betrachtet, weil die zuverlässige Versorgung mit Sicherheitsupdates sowie die fachgerechte Systemkonfiguration bei Privatgeräten nicht gewährleistet ist. Manche Befragte äußern sich dazu; sie beklagen Sachzwänge und fehlende Regelungen:

„I mostly use my private computer because it is faster"

„Gerade für wiss. Mitarbeiter ist die Grenze zwischen Beruf und Privat fließend. Genauso, wie wir häufig am Wochenende arbeiten, arbeiten wir häufig im Home Office an unseren privaten Rechnern. Wenn das nicht gewünscht ist, bräuchten wir klare Regelungen dafür oder Laptops der Uni für das Home Office."

„Ich benutzte eigentlich nur meinen privaten Laptop, da ich sehr viel von zu Hause aus oder unterwegs arbeite und. Dienstliche E-Mails werden auf Outlook und Thunderbird heruntergeladen."

„Wir haben noch nicht einmal für jeden einen Dienstrechner, sondern es wird einfach davon ausgegangen, dass wir alles mit dem privaten Laptop machen. Wenn dadurch dann aber was schiefgehen sollte, z.B. ein Virus ins Netzwerk eingeschleppt wurde, werden wir zur Verantwortung gezogen."

Weitere Probleme auf der Ebene der Organisation

Eine weitere Gruppe von Rückmeldungen berichtet von der leichtfertigen Handhabung von Datenschutz- und Datensicherheitsfragen in der Arbeitsumgebung. Auch Vorgesetzte werden genannt, die ein schlechtes Beispiel vorleben.

„Arbeite in [Einrichtung], Datensicherheit wird großzügig [...] "ausgelegt"... soll mich nicht so anstellen!"

„Der Umgang mit MitarbeiterInnen-Daten lässt hier noch zu wünschen übrig. Hier wären Top-down-Schulungen der Personen mit Personalverantwortung vielleicht ganz sinnvoll."

„Uni BI geht mir durch den öffentlich möglichen Zugang zum PEVZ zu großzügig mit personenbezogenen Daten um: Tel., E-Mail, Funktion, Raum. Diese Daten gehören in ein Intranet."

„Mir ist aufgefallen, dass sehr viele Lehrende in höheren Positionen eher Dropbox als Sciebo nutzen. Generell sollte mehr Aufklärung dazu stattfinden. Auch zum Angebot, dass das Projekte auch zusätzlichen Platz bekommen könne, auch Leute außerhalb von NRW dazu eingeladen werden können etc. Die Ignoranz zu dem Thema vor allem von Vorgesetzten ist haarsträubend! Das BITS ist oft keine Hilfe in solchen Belangen, obwohl die meisten Studenten und Angestellten dies als erste Anlaufstelle nutzen."

„Universitätsweite Regeln, Richtlinien, etc. bringen wenig, wenn sie von den Mitarbeitern und vor allem Vorgesetzten abgelehnt werden. Es macht ja doch jeder Prof. was er für richtig hält (s. Nutzung von Outlook, corporate design)."

„Es ist deprimierend, wenn der Vorgesetzte anordnet, dass ich eine Datenschutzverletzung begehen soll."

„Leider wird die Datensicherheit und Datenschutz von Seiten der obersten Universitätsleitung nicht vorgelebt, sondern immer wieder bewusst ignoriert."

„Auch [Name einer verantwortlichen Person] konnte bis heute nichts ausrichten. Es wurde nur kurze Zeit Hinweis beachtet von Vorgesetzten. Dann aber nach kurzer Zeit alter Trott. Atteste u.a. Personaldinge liegen offen herum"

„Mein Eindruck ist leider, dass in meinem Arbeitsumfeld Datenschutz als etwas angesehen wird, was theoretisch/formell existiert und bedeutet, dass man irgendwo mit einer Textpassage über den Datenschutz informieren muss. In der Praxis heißt dies aber noch lange nicht, dass man sich gewissenhaft daran hält - nach dem Motto ‚Das macht doch niemand so, das bekommt auch sowieso niemand mit'."

„Nach meinem Empfinden fehlt bei vielen Mitarbeitern der Universität das Gefühl und Verständnis dafür, dass Datenschutz durch jeden einzelnen umgesetzt werden muss und nicht ein alleiniges Thema der IT ist das man an diese einfach abgeben kann. Es fehlt die Bereitschaft sich mit dem Thema freiwillig zu befassen."

Eine Anmerkung benennt „infrastrukturelle[n] Probleme[n] der Universität, die einen sicheren Umgang mit Daten an der Universität erschweren/verhindern interessant; z.B. geringes Budget, nicht ausreichend Ressourcen für IT-Support, hellhörige Räume ..."

Teils werden unpraktikable oder auch fehlende Vorschriften beklagt.

„Auf der anderen Seite sind die Abläufe innerhalb der Uni teils so bürokratisch überfrachtet, unbeständig oder unorganisiert, dass man sich auch gar nicht an die Vorgaben halten will (s. Bestellprozess, Corporate Design Farbenänderung, [...])"

„Immer stärker mit Daten zu arbeiten ist sehr zeitaufwendig, was im normalen Arbeitsalltag und in den Tätigkeitsbeschreibungen nicht berücksichtigt wird. Die Informationen zur Daten-

sicherheit wird immer umfassender und der Umgang damit bürokratischer. Die Datensicherheit wird gegenüber den erfolgreichen Angriffen auf die Datensicherheit immer im Nachteil sein."

„Es sollte dringend ein Workflow für Datensicherheit/-schutz etabliert werden, der bis in die Fakultäten reicht. Hier sollten explizit keine wissenschaftlichen MitarbeiterInnen (inkl. ProfessorInnen) für den Datenschutz zuständig sein."

„Man kann es mit dem Datenschutz von Studierenden auch übertreiben. Wenn ich Studierende per Mail kontaktieren will, erstellt das eKVV eine verschlüsselte Adresse. Diese funktionieren aber nie, was das HRZ aber nicht einsieht. Aus meiner Sicht ist diese Funktion völlig überflüssig, in den Teilnehmer*innenlisten meiner Seminare können doch durchaus die Uni-Mail-Adressen angezeigt werden, dafür sind sie schließlich da!"

Klärung basaler Konzepte

Die Autoren der Befragung gingen bei der Konzeption des Fragebogens von einem Konsens über das Konzept Information und ihre Schutzwürdigkeit aus. Schon der Pretest des Fragebogens ließ Zweifel daran aufkommen, weshalb der Begriff *Information* durch *Daten* ersetzt wurde. Einigen Kommentaren zufolge kann man jedoch ein ausreichend sicheres Urteil über die Schutzwürdigkeit von Daten aus juristischer Sicht und vor dem Hintergrund der Eigeninteressen der Universität nicht unbedingt voraussetzen. Da nicht nur die Verwaltung, sondern auch die Forschung einer fortschreitenden Verrechtlichung unterworfen ist, sollten Unklarheiten, wie sie die folgenden Zitate belegen, Anlass zu weiteren Anstrengungen in der Aufklärung und Weiterbildung geben.

„Aus der Auswahl, mit welchen Forschungsdaten man zu tun hat, wird nicht klar, welcher Auswahlpunkt für Naturwissenschaftler, die nicht mit medizinischen / personenbezogenen Daten arbeiten (z. B. Chemiker, Physiker), geeignet ist."

„Der Begriff ‚Daten' sollte spezifiziert werden."

„I think the questions are very vague in terms of what is meant by data and data security. For example I am working mostly with biological data. Is this person-related scientific data? I know who collected the data. But it is not data containing information about persons."

„Maybe you should define "data" more clearly. Certainly things like CVs and job applications are important to keep under wraps, but honestly, scientific measurement data are supposed to be publicly available."

10 Zusammenfassung und Fazit

Die im Frühjahr 2019 unter Bediensteten der Universität Bielefeld durchgeführte Umfrage zur Informationssicherheit war ein erster Schritt zur Beleuchtung der besonderen Probleme im Umgang mit Daten in einer Organisation, die sich von Wirtschaftsunternehmen in mancher Hinsicht unterscheidet.

Sie deckt ein eingeschränktes Themenspektrum ab. Nur wenige Angaben zur Person konnten erhoben werden, ebenso wie exemplarisch eine begrenzte Auswahl alltäglicher Verhaltensweisen. Nichtsdestoweniger zeichnen sich klare Tendenzen ab.

An der Umfrage haben sich mehrheitlich Bedienstete aus dem Aufgabenbereich Forschung und Lehre, in erheblichen Umfang aber auch aus Verwaltung und Technik beteiligt. 27% tragen Personalverantwortung. Die Mehrheit der Befragten (55%) sieht sich in Datensicherheitsfragen auf Fortgeschrittenenniveau, über ein Drittel dagegen als Anfängerïn.

Wenig Überraschendes ergibt sich hinsichtlich der verarbeiteten Daten. Vorwiegend werden Forschungsdaten (personenbezogene, auch anonyme) verarbeitet, und zwar ganz überwiegend von Befragten in Forschung und Lehre. Es folgen Studierendendaten, die in beiden Aufgabenbereichen eine Rolle spielen. Finanz- und Personaldaten haben nur für die Verwaltung eine Bedeutung.

Personal-, Studierenden- und personenbezogene Forschungsdaten werden als besonders schutzwürdig und sensibel wahrgenommen. Generell unterliegt die Wahrnehmung der Schutzwürdigkeit Schwankungen innerhalb der Befragten. Ein Missbrauchspotenzial sehen Bedienstete in der Verwaltung eher als Forschende und subjektive IT-Sicherheitsexperten eher als Anfängerïnnen.

Die subjektiv eingeschätzte Informationssicherheitskompetenz sagt auch viel über den Kenntnisstand hinsichtlich Schadsoftware aus. Wer sich für eine Anfängerïn hält, ist mit Malware wesentlich weniger vertraut als jemand, die sich als Expertïn sieht.

Die Bediensteten nutzen in nennenswertem Umfang internetbasierte kommerzielle Dienste, die der IT-Sicherheitsbeauftragte und die Datenschutzbeauftragte der Universität als Sicherheitsproblem einstufen. Sie praktizieren ebenso am Arbeitsplatz riskante Verhaltensweisen. In dieser Hinsicht fallen besonders Wissenschaftlerïnnen auf, und innerhalb dieser Gruppe wiederum die Führungskräfte, sprich die Professorïnnen. Hier zeichnet sich eine große Herausforderung für die IT-Dienstleisterïnnen und die Sicherheitsverantwortlichen ab. Die Befragten aus Forschung und Lehre berufen sich auf besondere Anforderungen an die Werkzeuge der wissenschaftlichen Kommunikation, Datenhaltung und -analyse. Sie nehmen für sich in Anspruch, unsichere Werkzeuge zu nutzen, so lange die Universitäten keine gleichwertigen sicheren Alternativen zur Verfügung stellen. Der Speicherdienst Sciebo zeigt, dass solche Angebote durchaus attraktiv sein können

und wahrgenommen werden. Es wird aber noch erheblicher Aufwand vonnöten sein, um Forschende durch komfortable Angebote von der Nutzung problematischer Dienste abzuhalten.

Die von den Sicherheitsverantwortlichen mit Sorge betrachtete ungeregelte Nutzung eigener IT-Geräte (BYOD) ist offenen Rückmeldungen zufolge auch aus Sicht mancher Bediensteter ein Problem; sie erfolgt nicht immer freiwillig, da Beschaffungsmittel der Hochschulen begrenzt sind. Wir können den Umfang dieses Phänomens nicht quantifizieren; weitere Untersuchungen sollten dies empirisch klären.

Ein ähnliches Bild haben Fragen nach der Passung von Beratungs- und Informationsdiensten ergeben. Ein nach Meinung der Autoren zu großer Teil der Bediensteten hält die Angebote der Universität noch nicht für ausreichend und fühlt sich in der Folge nicht gut auf dem Umgang mit Sicherheitsrisiken vorbereitet. Darunter befinden sich mehr Wissenschaftlerïnnen und Befragte, die die eigene Sicherheitskompetenz niedrig einschätzen.

Es liegt daher nahe, Bedarfe zukünftig genau zu identifizieren und Informationssicherheitsangebote stärker auf Zielgruppen zuzuschneiden. Unseren Erkenntnissen zufolge ist ein Bedarf derzeit leicht beim Personal in Forschung und Lehre auszumachen. Auch die Selbsteinschätzung der Sicherheitskompetenz hat sich über alle Verhaltensindikatoren hinweg als Anzeiger potentieller Sicherheitsprobleme erwiesen. Es dürfte nicht schwer sein, gezielt diejenigen anzusprechen, die sich für Anfängerïnnen in IT-Sicherheitsfragen halten.

Literatur

Anderson, C.L.; Agarwal, R. (2010). Practicing safe computing: a multi-method empirical examination of home computer user security intentions. MIS Quarterly, Vol. 34 No. 3,pp. 613-643.

Bandura, A.; Adams, N.E.; Hardy, A.B.; Howells, G.N. (1980). Tests of the generality of self-efficacy theory. Cognitive Theory and Research, Vol. 4 No. 1, pp. 39-66.

Backhaus, Klaus; Erichson Bernd; Weiber, Rolf. (2011). Fortgeschrittene multivariate Analysemethoden. Springer-Lehrbuch. Berlin [u.a.]: Springer.

Bulgurcu, Burcu. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly, 2010, 34, 3, 523.

Colwill, Carl. (2009). Human factors in information security: the insider threat - who can you trust these days?. Information Security Technical Report, Vol. 14 No. 4, pp. 186-196.

Herath, Tejaswini; Rao, H.R. (2009). Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. Decision Support Systems, Vol. 47 No. 2, pp. 154-165.

Johnston, Allen C.; Warkentin, Merril. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. MIS Quarterly, 2010, 34, 3, 549.

Lee, Y.; Larsen, K.R.T. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. European Journal of Information Systems, Vol. 18 No. 2, pp. 177-187.

Lee, Sang M. (2004). An integrative model of computer abuse based on social control and general deterrence theories. Information & Management, 2004, 41, 6, 707.

Lieckfeldt, Renate (2011). Die Bitte ist das richtige Mittel. DUZ – Magazin für Wissenschaft und Gesellschaft, 16.09.2011, https://www.duz.de/beitrag/!/id/6/die-bitte-ist-das-richtige-mittel

Maddux, J.E.; Rogers, R.W. (1983). Protection motivation and self-efficacy: a revised theory of fear appeals and attitude change. Journal of Experimental Social Psychology, Vol. 19 No. 5, pp. 469-479.

Maddux, J.E. and Stanley, M. (1986). Self efficacy theory in contemporary psychology: a review. Journal of Social and Clinical Psychology, Vol. 4 No. 3, pp. 249-255.

Perkins, H. Wesley. (1986). Perceiving the Community Norms of Alcohol Use Among Students: Some Research Implications for Campus Alcohol Education Programming., 1986, 21, 9-10, 961.

Rogers, R.W. (1975). A protection motivation theory of fear appeals and attitude change. Journal of Psychology, Vol. 91 No. 1, pp. 93-114.

Siponen, Mikko (2000). A conceptual foundation for organizational information security awareness. Information Management & Computer Security, 2000, Vol. 8 No. 1, pp. 31-41.

Tanner, J.F. Jr, Day, E.; Crask, M.R. (1989). Protection motivation theory: an extension of fear appeals theory in communication. Journal of Business Research, Vol. 19 No. 4, pp. 267-276.

Taylor, Shirley. (1995). Understanding Information Technology Usage: A Test of Competing Models. Information Systems Research, 1995, 6, 2, 144.

Universität Bielefeld. (2019). Regelungen zur Informationssicherheit an der Universität Bielefeld. https://www.uni-bielefeld.de/informationssicherheit/Regelungen/index.html zuletzt abgerufen am: 29.05.2019

Woon, I.M.Y., Tan, G.W.; Low, R.T. (2005). A protection motivation theory approach to home wireless security. Proceedings of the 26th International Conference on Information Systems, Las Vegas, NV, December 11-14.

Workman, M.; Bommer, W.H.; Straub, D. (2008). Security lapses and the omission of information security measures: a threat control model and empirical test. Computers in Human Behavior, Vol. 24 No. 6, pp. 2799-2816.

Zerr, Konrad. (2007). Schwerpunkt - Security Awareness - Security-Awareness-Monitoring. Datenschutz Und Datensicherheit. DuD: Recht Und Sicherheit in Informationsverarbeitung Und Kommunikation, 2007, 31, 7, 519.

Daten an der Universität Bielefeld

1 Ihre Arbeit

a In welchem Aufgabenbereich der Universität arbeiten Sie?

- ◯ Forschung und Lehre
- ◯ Verwaltung und Technik

b Tragen Sie Personalverantwortung?

- ◯ ja
- ◯ nein

c Wie schätzen Sie sich selbst im Bereich Datensicherheit ein?
Als …

- ◯ Experten/Expertin
- ◯ Fortgeschrittenen/Fortgeschrittene
- ◯ Anfänger/Anfängerin
- ◯ Ich weiß nicht, was mit Datensicherheit gemeint ist.

An Ihrem Arbeitsplatz haben Sie Zugang zu unterschiedlichen Daten. Wir unterscheiden zwischen anonymen Daten (ohne Bezug zu identifizierbaren Personen) und personenbezogenen Daten.

2 Mit welchen Daten arbeiten Sie *am häufigsten*?

*Bitte kreuzen Sie **nur eine** Kategorie an.*

- ◯ anonyme Forschungsdaten
- ◯ personenbezogene Forschungsdaten
- ◯ Studierendendaten
- ◯ Personaldaten
- ◯ Finanzdaten
- ◯ sonstige anonyme Daten, z. B. wissenschaftliche Texte
- ◯ sonstige personenbezogene Daten, z. B. Bilder und Filmaufnahmen

3 Nun geht es um Ihre Einschätzung der Daten, mit denen Sie am häufigsten arbeiten.

Geben Sie an, inwiefern Sie den folgenden Aussagen zustimmen.

		stimme ... zu				
		voll	eher	eher nicht	überhaupt nicht	weiß nicht
a	Sie enthalten sensible Informationen.	○	○	○	○	○
b	Sie sind für unbefugte Dritte attraktiv.	○	○	○	○	○
c	Sie dienen den organisatorischen Abläufen.	○	○	○	○	○
d	Es wäre für mich persönlich ein Problem, wenn sie unkontrolliert an unbefugte Dritte gerieten.	○	○	○	○	○
e	Es wäre ein Problem für die Universität, wenn sie unkontrolliert an unbefugte Dritte gerieten.	○	○	○	○	○

4 Wie schätzen Sie die Angebote der Universität zur Datensicherheit ein?

Geben Sie an, inwiefern Sie den folgenden Aussagen zustimmen.

		stimme ... zu				
		voll	eher	eher nicht	überhaupt nicht	weiß nicht
a	Ich brauche mehr Schulungsangebote zur Datensicherheit.	○	○	○	○	○
b	Für Fragen zur Datensicherheit habe ich innerhalb der Universität ausreichend Informationsquellen.	○	○	○	○	○
c	Ich bin über die Regelungen der Universität zur Datensicherheit gut informiert.	○	○	○	○	○
d	Bei einem Datensicherheitsproblem wüsste ich, an wen ich mich wenden muss.	○	○	○	○	○
e	In Fragen der Datensicherheit bin ich immer sicher, wie ich mich verhalten muss.	○	○	○	○	○
f	Das Bewusstsein der Beschäftigten für Datensicherheit ist wichtig für die Universität.	○	○	○	○	○
g	Die bisher aufgetretenen Probleme mit der Datensicherheit wurden von den Verantwortlichen zeitnah gelöst.	○	○	○	○	○

Die folgenden Fragen beziehen sich nur auf Ihren Arbeitsalltag.

5 Verwenden *Sie selbst* folgende Dienste?

		ja	nein	kenne ich nicht
a	DFN-Terminplaner	○	○	○
b	DFN-Webkonferenzen mit Adobe Connect	○	○	○
c	Doodle	○	○	○
d	Dropbox	○	○	○
e	Google Drive	○	○	○
f	iCloud	○	○	○
g	Netzlaufwerke	○	○	○
h	Sciebo	○	○	○
i	Skype	○	○	○

6 Verwenden *Ihre direkten KollegInnen* folgende Dienste?

Siehe Liste aus Frage 5

7 Verwendet *Ihr/e Vorgesetzte/r* folgende Dienste?

Siehe Liste aus Frage 5

8 Denken Sie bei den folgenden Fragen an Ihre direkten KollegInnen.

Geben Sie an, inwiefern Sie den folgenden Aussagen zustimmen.

		trifft ... zu				
		voll	eher	eher nicht	überhaupt nicht	weiß nicht
a	Datensicherheit ist bei uns „auf dem Flur“ ein Thema.	○	○	○	○	○
b	Meine KollegInnen achten auf die Datensicherheit.	○	○	○	○	○
c	Die Datensicherheit wird von meinen KollegInnen als Hürde im Arbeitsalltag angesehen.	○	○	○	○	○
d	Es stört meine KollegInnen, wenn ich die Datensicherheit ignoriere.	○	○	○	○	○
e	Mein/e Vorgesetzte/r findet es gut, wenn ich mich aktiv um die Datensicherheit bemühe.	○	○	○	○	○

9 Wir möchten nun wissen, wie Sie persönlich über die Datensicherheit am Arbeitsplatz denken.

Geben Sie an, inwiefern die folgenden Aussagen zutreffen.

		trifft ... zu			
		voll	eher	eher nicht	überhaupt nicht
a	Ich hätte ein schlechtes Gewissen, wenn ich die Datensicherheit missachten würde.	○	○	○	○
b	Es wird von mir mit Nachdruck erwartet, dass ich die Datensicherheit beachte.	○	○	○	○
c	Wer in meiner Umgebung Sicherheitsrisiken eingeht, muss damit rechnen, von den KollegInnen ermahnt zu werden.	○	○	○	○
d	In meiner Umgebung kann man die Datensicherheit ignorieren, ohne dass es jemanden interessiert.	○	○	○	○
e	Wenn ich bemerken würde, dass KollegInnen die Datensicherheit nicht einhalten, würde ich sie darauf ansprechen.	○	○	○	○

10 Nun geht es um die Verantwortung für die Sicherheit der Daten, mit denen Sie am häufigsten arbeiten.
Wie sehr sind Ihrer Meinung nach die nachfolgend genannten Personen für diese Sicherheit verantwortlich?

		voll	überwiegend	teilweise	überhaupt nicht
a	meine/r direkte/r Vorgesetzte/r	○	○	○	○
b	meine MitarbeiterInnen (für die ich Personalverantwortung trage)	○	○	○	○
c	der/die IT-BetreuerIn	○	○	○	○
d	ich selbst	○	○	○	○
e	andere	○	○	○	○

11 Inwiefern stimmen Sie den folgenden Aussagen zu?

		stimme ... zu				
		voll	eher	eher nicht	überhaupt nicht	weiß nicht
a	Mein individuelles Verhalten beeinflusst die Datensicherheit der Universität.	○	○	○	○	○
b	In meiner Rolle als MitarbeiterIn der Universität stelle ich ein lukratives Ziel für Cyberkriminelle dar.	○	○	○	○	○

12 Jeden Tag begegnet uns eine Fülle neuer Fachbegriffe. Sie sehen hier eine Liste solcher Begriffe. Was davon stellt eine Gefahr für die Datensicherheit dar?

Geben Sie bitte eine spontane Einschätzung ab, ohne zu recherchieren. Sollten Sie davon etwas nicht kennen, kreuzen Sie bitte „weiß nicht" an.

		ja	nein	weiß nicht
a	Trojaner	○	○	○
b	Patch	○	○	○
c	Krypto-Miner	○	○	○
d	Zero-Hasher	○	○	○
e	Firewall	○	○	○
f	Phishing	○	○	○
g	Whyte-Tailing	○	○	○
h	Keylogger	○	○	○
i	Antivirus-Software	○	○	○
j	Backup	○	○	○
k	Rootkit	○	○	○
l	Ransom-Software	○	○	○

13 Für den Arbeitsalltag gibt es zahlreiche Empfehlungen zur Datensicherheit. Wie gehen Sie in den entsprechenden Situationen damit um?

Wir möchten Sie noch einmal darauf hinweisen, dass die Befragung anonym ist und wir an Ihrer persönlichen Meinung interessiert sind.

Geben Sie an, inwiefern die folgenden Aussagen für Sie zutreffen.

		trifft ... zu			
		voll	eher	eher nicht	überhaupt nicht
a	Ich treffe alle mir möglichen Vorkehrungen gegen Verletzungen der Datensicherheit.	○	○	○	○
b	Ich befürworte die Einhaltung der Datensicherheit.	○	○	○	○
c	Ich informiere mich aktiv über Datensicherheit.	○	○	○	○
d	Ich arbeite oft unter Zeitdruck.	○	○	○	○
e	Die Wahrung der Datensicherheit erschwert meine Arbeit.	○	○	○	○
f	Das Verhalten von Beschäftigten als Sicherheitsfaktor wird überbewertet.	○	○	○	○
g	Ich bekomme täglich mehr E-Mails, als ich beantworten kann.	○	○	○	○

14 Außerdem interessiert uns in Sachen Datensicherheit: Trifft das Folgende auf Sie zu?

		ja	nein
a	Ich alleine kenne das Passwort für meinen dienstlichen PC.	○	○
b	Meine dienstlichen E-Mails werden zu einem privaten Mail-Anbieter (z. B. Gmail, web.de, GMX) weitergeleitet.	○	○
c	Ich schließe mein Büro immer ab, wenn ich es unbeaufsichtigt lasse.	○	○
d	Ich nutze Online-Oberflächen, Anwendungen oder Apps wie Google Docs, Google Translate, Prezi, SplitPDF, um dienstliche Dokumente zu bearbeiten.	○	○
e	Von den Dateien, an denen ich jeweils aktuell arbeite, liegen einige auf dem Desktop meines PCs.	○	○
f	Wenn ich Unterlagen auf einem Gemeinschaftsdrucker ausdrucke, hole ich sie umgehend ab.	○	○
g	Ich schließe an meinen PC in der Universität auch private USB-Sticks an.	○	○
h	Ich schließe an meinen privaten PC auch USB-Sticks der Universität an.	○	○
i	Ich weiß, wie ich die Bildschirmsperre aktiviere.	○	○
j	Ich sperre jedes Mal meinen Bildschirm, wenn ich meinen Arbeitsplatz verlasse.	○	○

Vielen Dank!