Informationssicheres Verhalten automatisiert messen

Maximilian Janik · Kristin Weber · Andreas E. Schütz · Tobias Fertig

Hochschule für angewandte Wissenschaften Würzburg-Schweinfurt
maximilian@janik.xyz
{kristin.weber | andreas.schuetz | tobias.fertig}@fhws.de

Zusammenfassung

Um Informationen im Unternehmen zu schützen, ist die Sensibilisierung der Beschäftigten eine wichtige Aufgabe im Rahmen des Informationssicherheitsmanagements. Die Effektivität von Security-Awareness-Maßnahmen ist allerdings nur schwer messbar, wodurch die Rechtfertigung ihrer Kosten schwerfällt. Diese Arbeit stellt einen Weg vor, informationssicherheitsrelevantes Verhalten technisch zu messen. Dadurch kann der Erfolg von Security-Awareness-Maßnahmen genauer beurteilt werden. Es werden Kennzahlen vorgestellt, mit denen das Verhalten der Beschäftigten an ihren stationären Computern an sicherheitsrelevanten Stellen in datenschutzkonformer Weise aufgezeichnet und ausgewertet wird. Ein Prototyp demonstriert anhand einer Kennzahl die Machbarkeit des Konzepts.

1 Motivation und Zielsetzung

In der Informationssicherheit nimmt der Mensch eine zentrale Rolle ein. Das Verhalten der Beschäftigten am Arbeitsplatz und außerhalb des Unternehmens beeinflusst die Vertraulichkeit, Integrität und Verfügbarkeit von sensiblen Unternehmensinformationen: Sei es ein verlorenes Smartphone, ein versehentlich auf dem Schreibtisch liegen gelassenes vertrauliches Dokument oder ein fremder USB-Stick, der aus Unwissenheit über mögliche Gefahren verwendet wird. Zudem nutzen Kriminelle den „Faktor Mensch“ gezielt als Schwachstelle mit Techniken wie Phishing, Malware und Social Engineering aus [ISAC17, 11]. Der ehemalige Social Engineer Kevin Mitnick drückt es wie folgt aus: „Es ist oft ein Kinderspiel, die menschliche Firewall zu knacken. Das erfordert außer einem Telefonanruf keine Investitionen und beinhaltet nur ein minimales Risiko.“ [MiSD11, 20] Um der Belegschaft ihre wichtige Rolle bewusst zu machen, muss sie für Informationssicherheit sensibilisiert werden [Heli09; WeSc18]. Ein verbreitetes Mittel zur Sensibilisierung ist die Durchführung von Security-Awareness-Maßnahmen.

Um finanzielle Unterstützung für Security-Awareness-Maßnahmen auf Führungsebene zu erhalten, sollte deren Wirtschaftlichkeit nachgewiesen werden. Während die Kosten für diese präventiven Informationssicherheitsmaßnahmen noch vergleichsweise einfach zu ermitteln sind, ist der Nutzen bzw. Erfolg meist schwer nachweisbar [Lubi06; Heli09, 12f]. Eine hohe Security Awareness führt in der Regel zur Verringerung der Eintrittswahrscheinlichkeit von Informationssicherheitsrisiken und damit idealerweise zur Abwesenheit von Informationssicherheitsvorfällen und deren negativen Auswirkungen auf das Unternehmen. Anders ausgedrückt, Investitionen in Informationssicherheit zeigen ihren Nutzen darin, dass nichts passiert: „… den Nutzen von IT-Sicherheit kann man weder sehen noch spüren.“ [Fede06, 4].

P. Schartner · N. Pohlmann (Hrsg.) · D•A•CH Security 2018 · syssec (2018) 1-12.

Diese Arbeit zeigt einen Weg, um das informationssicherheitsrelevante Verhalten der Belegschaft in Unternehmen technisch zu messen. Ein IT-System zeichnet das Verhalten der Beschäftigten an ihren stationären Computern an sicherheitsrelevanten Stellen datenschutzkonform auf und wertet die Messergebnisse aus. Wird vor und nach der Durchführung von Security-Awareness-Maßnahmen gemessen, zeigt sich in der Veränderung der Messergebnisse idealerweise der Erfolg der Maßnahmen.

Im Folgenden wird das Verständnis von Security Awareness und verschiedene Ansätze zur Messung von Security Awareness erklärt. Anschließend betrachtet die Arbeit Vorgaben des Datenschutzes, die beim Messen von Sicherheitsverhalten beachtet werden müssen und beschreibt anschließend exemplarisch messbare Kennzahlen. In Kapitel 5 wird die grundlegende Funktionsweise eines solchen IT-Systems mit Hilfe eines Prototyps demonstriert. Am Ende folgt eine Diskussion über die Auswertung und Interpretation der Messergebnisse und schließlich ein Resümee mit Ausblick.

2 Security Awareness

Im Forschungsbereich Security Awareness steht der „Faktor Mensch“, also die Personen, die Informationssysteme und -technik nutzen, im Fokus. Unternehmen, die ihre Informationen schützen möchten, müssen sich darauf verlassen können, dass ihre Belegschaft die hierfür getroffenen Regelungen und Richtlinien befolgen. Mit der Steigerung der Security Awareness der Beschäftigten wird versucht, dieses informationssicherheitskonforme Verhalten zu fördern. [Heli09, 11] beschreiben Security Awareness als Zusammenspiel von Kognition (Beschäftigte wissen was zu tun ist), Handlungsabsicht (Beschäftigte möchten informationssicherheitskonform handeln) und Organisation (Beschäftigte können sich in ihrem Umfeld informationssicherheitskonform verhalten). Die Erhöhung der Security Awareness ist ein komplexes und andauerndes Vorhaben, das auf die Verhaltensänderung der Zielgruppe hin zu einem informationssicherheitskonformen Verhalten abzielt [BaSN15].

Maßnahmen zur Erhöhung der Security Awareness können das menschliche Verhalten jedoch nicht direkt beeinflussen [ScWe17]. Stattdessen müssen die Einflussfaktoren Wissen und Fähigkeiten, Salienz, Gewohnheit, Verhaltensabsicht und die Einschränkungen aus dem Umfeld adressiert werden (vgl. Abbildung 1, erstellt in Anlehnung an [ScWe17, 5]). Eine Person mag wissen, dass das geschäftliche Smartphone mit einer PIN gesichert werden soll. Wenn sie jedoch nicht von der Wichtigkeit dieser Verhaltensweise überzeugt ist, wird sie vermutlich trotzdem keine PIN nutzen. Hier muss erst die Verhaltensabsicht beeinflusst werden. Andere Verhaltensweisen, wie das Sperren des Bildschirms bei Verlassen des Arbeitsplatzes, können stark über die Etablierung einer Gewohnheit unterstützt werden. Um Beschäftigte dazu zu bringen, sich informationssicherheitskonform zu verhalten, müssen Security-Awareness-Maßnahmen zielgerichtet auf diese Faktoren abgestimmt werden. Für zielgerichtete Maßnahmen ist die Analyse der Ist-Situation, also der aktuellen Ausprägung der Einflussfaktoren bei den Beschäftigten und somit der Security Awareness, unerlässlich [BaSN15, WeSc18].

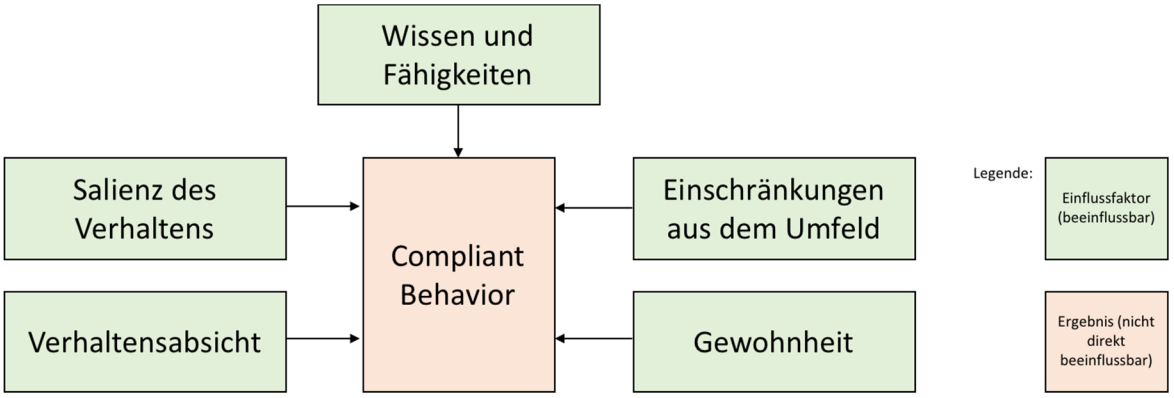

Abb. 1: Einflussfaktoren auf menschliches Verhalten

Sowohl Unternehmen als auch die Wissenschaft beschäftigen sich mit der Frage, wie Security Awareness gemessen werden kann. Eine Liste des „SANS Institute“ [Spit14] zeigt mögliche Metriken, wie die Anzahl infizierter Rechner im Unternehmen sowie Ergebnisse von Umfragen, Brute-Force-Versuchen auf Passwörter, nächtlichen Prüfungen auf nicht gesperrte Computer und Social-Engineering-Angriffen per Telefon oder E-Mail. Die Forschung zeigt Ansätze zur Messung der Security Awareness mittels Befragung [KrKe06, 290ff; HaPo09, 81ff.; WeSc18; FHFP18] und durch das Versenden fingierter Phishing-E-Mails [DoCF07, 74f]. [KANK11] stellen zudem einen Ansatz vor, wie mit Metriken wie Sicherheitsvorfällen, Anrufen beim Help Desk oder der Anzahl der Zugriffe auf unautorisierte Webseiten Security Awareness gemessen werden kann.

Bei der Betrachtung der verschiedenen Methoden aus dem vorhergehenden Absatz zeigt sich, dass es unterschiedliche Auffassungen von Security Awareness gibt. Der Definition von [Heli09] und den Einflussfaktoren von [ScWe17] folgend, wird teilweise mehr das „Compliant Behavior“ (informationssicherheitskonformes Verhalten) und damit das Ergebnis der Security Awareness gemessen, während andere Ansätze sich auf die Security Awareness selbst konzentrieren. Die erste Variante gibt also Auskunft darüber, inwieweit Mitarbeiter die Regelungen des Unternehmens befolgen. Hieraus geht allerdings nicht hervor welche Gründe zu dem jeweiligen Verhalten führen, beispielsweise ob den Mitarbeitern das Wissen oder die Motivation fehlt oder doch eine technische Hürde für unerwünschtes Verhalten verantwortlich ist. Daher sollte bei der Auswahl eines Ansatzes genau geprüft werden, was letztendlich gemessen werden soll.

Eine möglichst standardisierte, wiederholbare und kostengünstige Messmethode ist die automatisierte Erfassung an den stationären Computern der Belegschaft.

3 Datenschutzkonform Messen

Das Erheben von personenbezogenen Daten der Belegschaft, um deren informationssicherheitsrelevantes Verhalten zu analysieren, fällt in den Anwendungsbereich des Datenschutzrechts. Spätestens mit dem Inkrafttreten der DSGVO am 25. Mai 2018 sind Unternehmen für den gesetzeskonformen Umgang mit personenbezogenen Daten stärker sensibilisiert und sind sich der härteren Strafen bewusst. Im Rahmen dieses Papers ist keine umfassende und juristisch einwandfreie Betrachtung dieses Themas möglich. Es werden im Folgenden daher nur einige grundsätzliche Überlegungen zum Datenschutzrecht und anderen Gesetzen aufgeführt, die bei der Entwicklung des Prototyps zu berücksichtigen sind.

Soll eine automatisierte Messung und Analyse des informationssicherheitsrelevanten Verhaltens gesetzeskonform durchgeführt werden, so besteht die einfachste Art darin, die Betroffenen um Erlaubnis zu fragen, nur bei Einverständnis zu überwachen und transparent über alle Maßnahmen zu informieren (Art. 6, 13 DSGVO).

Arbeitgeber haben allerdings grundsätzlich das Recht, Arbeitnehmer zu bewerten und diese Bewertungen auch in der Personalakte zu speichern [Bund79]. Auch eine Kontrolle kann in eine Beurteilung einfließen. Zur Kontrolle der Belegschaft kann es dem Unternehmen gestattet sein, die E-Mail- und Internetnutzung bis zu einem gewissen Grad zu überwachen. Eine Kontrolle kann durchgeführt werden, um die betriebliche Nutzung sicherzustellen und um Schaden abzuwenden und die Einhaltung der Pflichten, die aus dem Arbeitsverhältnis entstehen, zu prüfen. Vor der Durchführung der Kontrollen müssen allerdings eine Verhältnismäßigkeitsprüfung durchgeführt und die Schutzinteressen der Beschäftigten abgewogen werden [Gola14, Rn. 450ff]. Auch ist das Prinzip der Datenminimierung zu beachten (Art. 5 DSGVO). Eine vollständige Kontrolle aller Beschäftigten darf auf keinen Fall durchgeführt werden, dementsprechend ist stichprobenartig vorzugehen [Witt10, 170] [Gola14, Rn. 320 - 328].

Der Eingriff in die Persönlichkeitsrechte der Belegschaft ist so weit wie möglich zu minimieren, wobei alle Umstände der Überwachung zu bedenken sind. Das bedeutet zum Beispiel, dass es eine Rolle spielt, ob es sich um eine heimliche oder offene Überwachung handelt: Beides ist grundsätzlich möglich, doch eine offene Überwachung wird vor Gericht eine größere Zustimmung erhalten als eine heimliche. [BeAb14, 412]

Neben den Betroffenen hat der Betriebsrat ein Interesse daran, personenbezogene Daten zu schützen. Das BetrVG fordert implizit, dass Betriebsräte aktiv daran arbeiten, den Arbeitnehmerdatenschutz zu sichern (§ 75 Abs. 2 BetrVG). Der Betriebsrat besitzt bei der „Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen“ ein Mitbestimmungsrecht (§ 87 Abs. 1 Nr. 6 BetrVG). Eine Kontrolle und Mitgestaltung der geplanten Maßnahmen durch den Betriebsrat ist also bei einer Überwachung einzelner Beschäftigter auf jeden Fall notwendig. [GKKS15, Rn. 1579-1594, 1768-1774]

Das Mitbestimmungsrecht durch den Betriebsrat gilt auch dann, wenn die technische Einrichtung ein Team überwacht und davon auszugehen ist, dass der Überwachungsdruck, der von der technischen Einrichtung ausgeht, auch auf einzelne Teammitglieder durchschlagen kann. Ab welcher Gruppengröße dieser Druck nicht mehr ausreichend zur Geltung kommt, ist nicht geklärt.

An den Prototyp werden aufgrund dieser Überlegungen folgende Anforderungen aus Datenschutzsicht (DSA) gestellt. Die Messungen sollen stichprobenartig personenbezogen, aber pseudonym, erfolgen (DSA1). Die Analyse und Speicherung der Daten soll anonymisiert auf eine größere Gruppe von Beschäftigten bezogen erfolgen. Dazu sollen die pseudonymen Einzelmessungen aggregiert werden (DSA2). Die Gruppengröße ist so zu wählen, dass der Überwachungsdruck gering ist. In schwerwiegenden Verdachtsmomenten soll jedoch die Möglichkeit bestehen, Auswertungen für eine einzelne Person zu erstellen (DSA3). Existieren keine schweren Verdachtsmomente, sollen personenbezogene Daten (pseudonymisierte Einzelmessungen) nach der Aggregation für die Analyse (und damit Anonymisierung) vollständig gelöscht werden (DSA4). Die Häufigkeit der Messungen sollte anpassbar sein, um dem aktuellen Risiko Rechnung zu tragen (DSA5).

Darüber hinaus sollte die Messung immer in Abstimmung mit dem Betriebsrat und dem Datenschutzbeauftragten vorgenommen werden. Es sollte seltener gemessen werden, wenn die Security Awareness der Beschäftigten steigt. Die Betroffenen sollten über die Maßnahmen informiert werden, da eine heimliche Überwachung weniger verhältnismäßig wäre. Um dem Thema Überwachungsdruck zu entgehen, sollte die Messung keine negativen Konsequenzen für das Team haben. Die Ergebnisse sollten ausschließlich der Erfolgsmessung dienen und um zukünftige Informationssicherheitsmaßnahmen zu planen.

Die Kontrolle der Effektivität präventiver Informationssicherheitsmaßnahmen rechtfertigt sich schlussendlich durch die Vermeidung von Informationssicherheitsrisiken. Für Betreiber kritischer Infrastrukturen ist der Nachweis von getroffenen Maßnahmen sogar gesetzlich durch das IT-Sicherheitsgesetz (Art. 1, §8a, Abs. 3) vorgeschrieben.

Grundsätzlich ist zu beachten, dass die private Nutzung von Telekommunikationsanlagen im Unternehmen untersagt sein muss, damit zum Beispiel der Browserverlauf oder andere Kommunikationsdaten erhoben werden dürfen. Ist die private Nutzung nicht verboten, wäre ein Zugriff des Arbeitgebers nach §202a des Strafgesetzbuches strafbar. Auch wenn erkennbar ist, dass es sich – trotz des Verbotes – um private Kommunikation handelt, sollte eine Erhebung unterlassen werden. [Gola14, Rn. 118ff]

4 Automatisiert messbare Kennzahlen

Konzeptionell orientiert sich das Messen des informationssicherheitskonformen Verhaltens am IT-Controlling-Regelkreis (vgl. Abbildung 2, erstellt in Anlehnung an [Kütz10, 4]). Das zu steuernde (zu beeinflussende) Objekt ist das informationssicherheitskonforme Verhalten (Compliant Behavior) der Beschäftigten. Der Nutzen bzw. Erfolg von Security-Awareness-Maßnahmen sollte sich letztendlich in einer Erhöhung der Informationssicherheit zeigen, also durch eine Verbesserung des Verhaltens der Beschäftigten in informationssicherheitsrelevanten Bereichen. Die Beschäftigten werden durch Plakate über die Gefahren und Merkmale von Phishing-E-Mails aufgeklärt. Ist diese Maßnahme erfolgreich, sollten weniger Beschäftigte auf Phishing-E-Mails hereinfallen und die Schäden durch Identitätsdiebstahl oder Datenverluste sinken.

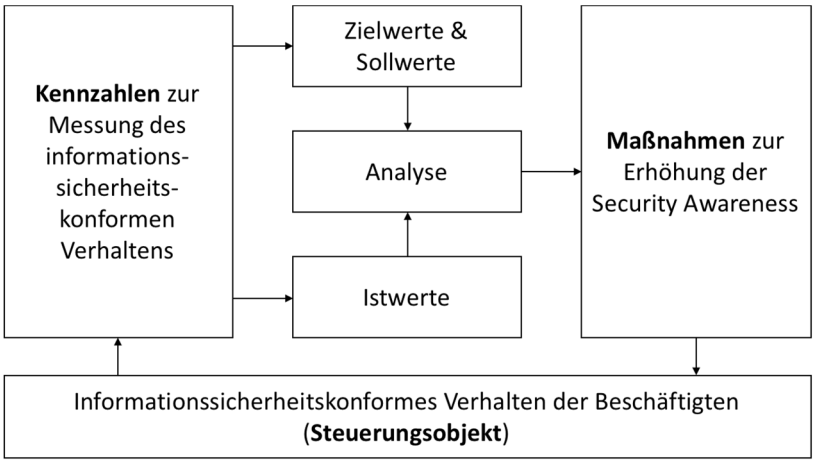

Abb. 2: Compliant Behavior als Steuerungsobjekt im IT-Controlling-Regelkreis

Zunächst muss der Ist-Zustand des informationssicherheitskonformen Verhaltens festgehalten werden, also wie viele Beschäftigte in einem bestimmten Zeitraum auf Links in Phishing-E-

Mails klicken. Als Soll-Zustand wird definiert, dass diese Zahl um 50% sinken soll. Nach der Durchführung der Maßnahmen wird der neue Ist-Zustand mit dem Soll verglichen und der Erfolg der Maßnahmen kann bewertet werden. Für die Messungen des Ist-Zustandes und der Definition der Zielwerte werden Kennzahlen benötigt.

Geeignete Steuerungs-Kennzahlen müssen verschiedene Anforderungen erfüllen (vgl. [Lelk05, 9f.]). Kennzahlen sollten *zielbezogen* sein, also Aussagen über den Zielerreichungsgrad zuzulassen. Sie müssen zeigen, dass sich das informationssicherheitskonforme Verhalten der Beschäftigten verbessert hat. Kennzahlen müssen *beeinflussbar* sein. Änderungen an den gemessenen Werten sollten auf die getroffenen Security-Awareness-Maßnahmen zurückzuführen sein und nicht auf andere Einflüsse. Sie sollten *operationalisierbar* (also messbar) sein und *effizient* erhoben werden können. Die Indikatoren müssen automatisiert über IT-Tools direkt am stationären Computer der Beschäftigten erhoben werden können. Damit sich die Erhebung lohnt, und tatsächlich relevante Rückschlüsse für die Informationssicherheit möglich sind, sollte das entsprechend Verhalten relativ häufig ausgeübt werden, idealerweise mehrmals pro Zeiteinheit (z. B. Tag, Monat). Grundsätzlich gilt, dass die Aussage von Einzelkennzahlen kritisch zu hinterfragen ist, da sie immer nur einen sehr engen Ausschnitt der komplexen Realität darstellen (vgl. [Kütz10, 5]). Verlässlichere Aussagen über das Steuerungsobjekt erhält man durch ein Kennzahlensystem, welches mehrere Einzelkennzahlen in Zusammenhang bringt und somit die Realität mehrdimensional abbildet.

Um die Umsetzbarkeit des Konzeptes zu demonstrieren, wurde als Compliant Behavior das „Sperren des Bildschirms beim Verlassen des Arbeitsplatzes“ gewählt. Dieses Verhalten muss typischerweise von jedem Beschäftigten mehrmals am Tag ausgeübt werden. Verlässt der Beschäftigte den Arbeitsplatz, ist es sinnvoll, dass er den Computer sperrt, um Unbefugten den Zugriff zu verwehren. Diese Verhaltensweise ist vor allem in Großraumbüros oder öffentlichen Gebäuden kritisch. Auf nicht-gesperrten Bildschirmen könnten Dokumente oder E-Mails geöffnet sein, die vertrauliche Informationen enthalten und von Vorbeilaufenden eingesehen werden können. Im Extremfall könnte jemand den Computer nutzen, um gezielt Informationen zu lesen, zu stehlen oder zu manipulieren oder Schadsoftware zu installieren.

Als Kennzahl wird die Zeit der Inaktivität des Nutzenden am Computer gemessen. Wird ein bestimmter Schwellwert überschritten, z. B. 15 min[1], und ist der Bildschirm nicht gesperrt, soll dies als sicherheitskritischer Vorfall registriert werden. Ist nachts ein Bildschirm eines Mitarbeiters nicht gesperrt oder der Computer nicht heruntergefahren, ist das grundsätzlich als sicherheitskritisch einzustufen.

Unter Windows lässt sich automatisiert auslesen, ob der Bildschirm aktuell gesperrt ist oder nicht. Es existiert dafür das sogenannte „SessionSwitch-Ereignis“, welches unter anderem die Möglichkeiten „SessionLock“ und „SessionUnlock“ beinhaltet. Es existiert ebenfalls eine Funktion, mit der abgefragt werden kann, wie viel Zeit seit der letzten Nutzerinteraktion vergangen ist (GetLastInputInfo). Unter Linux und Unix ist die Erfassung von beiden Werten schwierig, da es verschiedene Desktopumgebungen und Loginmanager gibt, die unterschiedlich funktionieren und Informationen preisgeben und speichern.

Aussagen zur Zielerreichung sind durch diese Kennzahl bedingt möglich. Bewegt der Anwendende eine gewisse Zeit lang seine Maus nicht und benutzt auch nicht die Tastatur, besteht das Risiko, dass er den Arbeitsplatz verlassen hat, ohne den Computer zu sperren. Ob tatsächlich

[1] Das Bundesamt für Sicherheit in der Informationstechnik (BSI) schlägt vor, dass nach 15 Minuten Inaktivität Bildschirme automatisch gesperrt werden sollten [BSI13].

ein informationssicherheitskritisches Verhalten vorliegt, kann nicht pauschal beantwortet werden. Es könnte auch sein, dass der Beschäftigte am Arbeitsplatz ein Papierdokument liest, telefoniert oder eine Präsentation hält. Es ist denkbar, Schwellwerte pro Team oder Abteilung zu vergeben, um dem besonderen Schutzbedarf der über den stationären Computer einsehbaren Informationen Rechnung zu tragen.

Die Kennzahl ist durch Security-Awareness-Maßnahmen beeinflussbar. In der Teeküche werden Plakate platziert, die an das Sperren des Bildschirms beim Verlassen des Arbeitsplatzes erinnern. Awareness-Videos weisen auf die negativen Folgen eines nicht-gesperrten Bildschirms hin. Die Richtlinie für das Verhalten am Arbeitsplatz fordert das Sperren des Bildschirms beim Verlassen des Büros. Sind diese Maßnahmen erfolgreich, sollte die Anzahl der aufgezeichneten sicherheitskritischen Vorfälle sinken.

5 Prototyp

Die prototypische Vorgehensweise wurde gewählt, da sie hilft, die Anforderungen an ein Informationssystem exakter zu formulieren und die technische Machbarkeit zu beweisen. Grundsätzlich „vermindert [sie] die Anzahl der unsicheren Annahmen in einem Softwareprojekt“ [PoBl96, 175ff]. Im Rahmen der Arbeit wurde deshalb ein explorativer Prototyp erstellt. Die Anforderungen an den Prototypen wurden innerhalb der explorativen Vorarbeit definiert. Zudem kamen durch die DSVGO weitere Anforderungen dazu, die bereits in Kapitel 3 festgelegt wurden. Der Prototyp konzentriert sich lediglich auf die Funktionalitäten des Systems und demonstriert die Umsetzung ausgewählter Anforderungen.

Der Prototyp testet die Messbarkeit von Kennzahlen und beweist die allgemeine Machbarkeit des Ansatzes inklusive der Datenschutzkonformität. Hierfür wurde eine Client-Server Anwendung entwickelt: Der Server verwaltet Indikatoren und Ereignisse, die der Client zuvor gesammelt hat. Der Client erhebt sicherheitsrelevante Daten an den Arbeitsplatzrechnern der Beschäftigten und sendet diese pseudonymisiert an den Server zur Auswertung und Anonymisierung durch Gruppierung (DSA1, DSA2). Um ein pseudonymisiertes Login zu ermöglichen, werden Abteilungslogins verwendet (DSA1). Alle Clients einer Abteilung nutzen denselben Login zur Authentifizierung. Je größer die Abteilungen gewählt werden, desto höher ist der Anonymisierungsgrad. Besteht ein schwerer Verdacht gegen einzelne Beschäftigte, lässt die Anwendung auch individuelle Logins zu (DSA3). Besteht kein schwerer Verdacht, löscht der Client alle pseudonymisierten Daten (DSA4). Durch die Konfiguration eines Messintervalls werden die Kennzahlen immer stichprobenartig gemessen (DSA1, DSA5). Eine vollständige Aufzeichnung der Aktivitäten einer Person ist somit, aus Datenschutzgründen, nicht möglich.

Ein IT-Admin kann die Logindaten konfigurieren. Die für die Erhebung genutzte Konfiguration wird initial vom Server heruntergeladen. In einem vom Admin konfigurierbaren Intervall prüft die Clientanwendung nun, ob Schwellwerte der aktiven Kennzahlen überschritten wurden. Beispielsweise wird ein Ereignis an den Server geschickt, wenn ein Nutzender den Bildschirm nach einer festgelegten Dauer der Inaktivität nicht sperrt. Im Server wird die Liste der letzten Ereignisse aktualisiert und erhöht den Wert der nicht-kritischen Ereignisse gesamt. Abbildung 3 zeigt einen Ausschnitt des Dashboards eines Servers. Die Tachos sollen hierbei einen schnellen Überblick über die Anzahl der kritischen bzw. nicht-kritischen Vorfälle liefern. Die Graphen zeigen zudem einen zeitlichen Verlauf der Vorfallhäufigkeit in der letzten Woche.

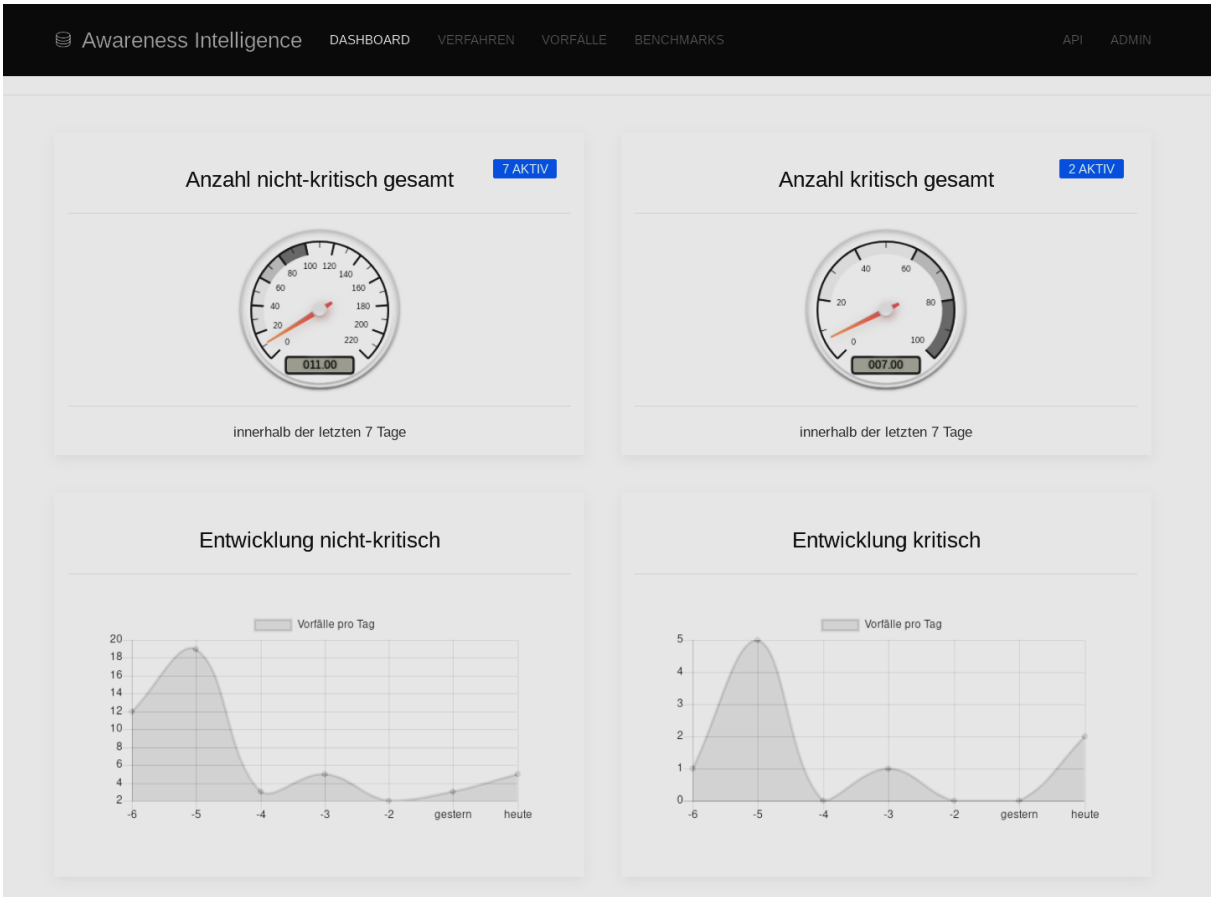

Abb. 3: Ausschnitt des Server Dashboards (Quelle: eigene Darstellung)

Im Rahmen dieser Arbeit ist ein Prototyp entstanden, der bereits einen Großteil der aufgestellten Anforderungen stabil erfüllen kann. Der Server speichert alle Daten persistent ab. Zunächst geschah die Anonymisierung der empfangenen Daten – wenn es die aufgestellten Regeln zuließen – bereits vor dem Speichern in der Datenbank. Aufgrund der Konstellation der verwendeten Frameworks bedeutete das allerdings technisch, dass die Bestätigung der Anfrage – die alle Eingaben zurückschickte, um einen detaillierten Abgleich zu ermöglichen – ebenfalls anonymisierte Daten beinhaltete. Um dem Client zu ermöglichen, falsch verarbeiteten Daten zu widersprechen, wurde die Anonymisierung umgestellt, sodass sie erst direkt nach dem Speichern geschah. Nicht anonymisierte Werte stehen also nun für sehr kurze Zeit pseudonymisiert in der Datenbank. Ein zukünftiges Produkt sollte beide Funktionen, sowohl die Möglichkeit des Widerspruchs und sichere Anonymität, bieten können.

6 Messergebnisse: Auswertung und Interpretation

Welche Verhaltensweisen als informationssicherheitskonform gelten, muss jedes Unternehmen individuell z. B. durch Richtlinien festlegen. Für jede Verhaltensweise wird dann geprüft, wie diese mittels Kennzahlen automatisiert an stationären Computern gemessen werden kann. Ein sinnvolles Kennzahlensystem führt zu verlässlicheren Aussagen als Einzelkennzahlen. Aus

empfohlenen Verhaltensweisen (z. B. [WiHa03, KoRY15, LaTr16, Zina16]) abgeleitet und gegen die o. g. Anforderungen an Kennzahlen geprüft, sind folgende Ideen für weitere automatisiert messbare Kennzahlen entstanden[2]:

- „Als potentiell gefährlich eingestufte E-Mail-Anhänge dürfen nicht geöffnet werden." – Gemessen werden können, wie viel Prozent aller Anhänge vom Anwendenden geöffnet werden (ggf. in Abhängigkeit der Dateiendung) und wie viel Zeit zwischen E-Mail-Abruf und dem Öffnen eines Anhangs vergeht.
- „Public Cloud Angebote dürfen nicht genutzt werden." – Die vom Anwendenden besuchten Internetseiten können erhoben werden, z. B. über die Browserhistorie.
- „Nur erlaubte Anwendungen dürfen installiert werden." – Die auf dem Computer installierten Anwendungen können erfasst werden. Durch Auswertung der laufenden Prozesse können auch portable Anwendungen, die keine Installation benötigen, erkannt werden.
- „Updates und Patches sind zeitnah nach ihrem Erscheinen zu installieren." – Die aktuellen Versionen der installierten Anwendungen und des Betriebssystems können identifiziert werden.
- „Externe Speichermedien wie CDs, externe Festplatten oder USB-Sticks dürfen nicht genutzt werden." – Ob und welche externen Geräte mit dem Computer verbunden sind, kann ermittelt werden.

Sind mehrere Kennzahlen definiert, können diese gemeinsam interpretiert werden. Eine Möglichkeit ist, die zeitliche Reihenfolge des Auftretens von als sicherheitskritisch eingestuften Verhaltensweisen zu analysieren. Beispielsweise ist die Installation einer nicht erlaubten Anwendung nach dem Öffnen eines Anhangs einer E-Mail oder nach Anschluss eines externen Speichermediums als besonders kritisch zu betrachten.

Wie bereits zu Beginn dieser Arbeit erläutert, erlauben die Messergebnisse alleine nur bedingt Rückschlüsse auf die Security Awareness der Belegschaft. Werden zu viele sicherheitskritische Vorfälle registriert, ist zumindest die These erlaubt, dass die Security Awareness schlecht ausgeprägt ist. Umgekehrt bedeuten Messergebnisse, die auf ein informationssicherheitskonformes Verhalten hinweisen, nicht automatisch, dass die Security Awareness hoch ist. Die Belegschaft hält sich vielleicht einfach nur „stur" an die aufgestellten Regeln, ohne diese wirklich zu verstehen oder nachvollziehen zu können.

Aber auch Messungen des „Compliant Behaviors" können einen wertvollen Beitrag für Unternehmen leisten. Unternehmen erhalten einen Überblick darüber, ob und in welchem Umfang verschiedene Verhaltensweisen tatsächlich befolgt werden. Daraus können sie ableiten, für welche Verhaltensweisen eine tiefergehende Analyse der Beweggründe der Beschäftigten durchgeführt werden soll und wo Security-Awareness-Maßnahmen überhaupt notwendig sind. Das Unternehmen kann sich bspw. auf die Verhaltensweisen konzentrieren, bei denen die Beschäftigten besonders schlecht abschnitten. Ein besonders positives Ergebnis könnte auch dazu führen, keine (weiteren) Security-Awareness-Maßnahmen durchzuführen. Und damit dienen die Messergebnisse als Indikator für den Erfolg der Maßnahmen.

Die gemessenen Werte können im Risikomanagement Aussagen darüber geben, wie wahrscheinlich der Eintritt eines bestimmten Schadensfalles im Unternehmen ist. Zeigen die Mess-

[2] An dieser Stelle wird bewusst nicht diskutiert, inwiefern die hier aufgeführten organisatorischen Richtlinien durch technische oder physische Sicherheitsmaßnahmen unterstützt werden können.

ergebnisse, dass ein Großteil der Belegschaft wahllos verdächtige E-Mail-Anhänge von unbekannten Absendern öffnet, erscheint das Risiko einer Schadprogramminfektion in Zukunft entsprechend hoch.

In Kapitel 3 wurde argumentiert, dass die Beschäftigten über die „Überwachung“ informiert werden sollten. Daher ist noch zu prüfen inwieweit die Ergebnisse dadurch verfälscht werden. Dem Hawthorne-Effekt zufolge führt alleine die Beteiligung an Studien zu einer positiven Rückkopplung (vgl. [ChHo08]). Dieser Effekt steigert die Lernmotivation und damit auch den Lerneffekt [Nork91] und kann daher helfen, Beschäftigte zu einem positiven Verhalten zu bewegen. Trotz Hawthorne-Effekt sollte nach erfolgreichen Maßnahmen ein besseres Ergebnis bei der erneuten Messung auftreten.

7 Resümee und Ausblick

Obwohl sich die Forschungsarbeit in diesem Gebiet noch in einem sehr frühen Stadium befindet, hat sich grundsätzlich gezeigt, dass die automatisierte Messung des informationssicherheitskonformen Verhaltens von Beschäftigten am Computer ein gangbarer Weg ist, um Entscheidungen in Bezug auf die Planung von Security-Awareness-Maßnahmen zu treffen. Darüber hinaus können damit der Erfolg und somit die Wirtschaftlichkeit dieser Maßnahmen bewertet werden. Sinkt die Anzahl der Vorfälle in einem festzulegenden Zeitraum, ist der Erfolg prozentual berechenbar. Da jedes Überschreiten des Schwellwertes einer Kennzahl mit Datum gespeichert wird, ist sogar eine kontinuierliche Analyse des Sicherheitsverhaltens möglich. Eine sinkende Anzahl an sicherheitskritischen Vorfällen wirkt sich direkt positiv auf das Informationssicherheitsrisiko aus, wodurch die Rechtfertigung der Kosten präventiver Informationssicherheitsmaßnahmen deutlich einfacher wird.

In dieser Arbeit wurden exemplarisch Kennzahlen für verschiedene Verhaltensweisen ausgewählt, wovon eine ausführlich vorgestellt wurde. In zukünftigen Arbeiten sollten weitere Kennzahlen für informationssicherheitsrelevante Verhaltensweisen definiert werden. Insbesondere eine Erweiterung um Verhaltensweisen im sicheren Umgang mit mobilen Endgeräten ist notwendig. Ziel ist ein System aus automatisiert erhobenen Kennzahlen, welches möglichst umfassend Auskunft über das Steuerungsobjekt Compliant Behavior gibt. Diese Kennzahlen müssen systematisch diskutiert und deren Eignung in entsprechenden Studien untersucht werden.

Werden Durchschnittswerte von mehreren Unternehmen an eine zentrale Stelle anonym übermittelt, so ist auch denkbar, ein Benchmarking zu ermöglichen, womit Unternehmen ihr Messergebnis mit dem Durchschnitt aller Unternehmen vergleichen könnten. Derartige Benchmarks werden zum Beispiel in der Softwareentwicklung eingesetzt [WuPJ17]. Durch die strikte Übermittlung von anonymisierten Durchschnittswerten, arbeitet die zentrale Stelle niemals selbst mit personenbezogenen Daten.

Literatur

[BeAb14] T. B. Behling, R. B. Abel (Hrsg.): Praxishandbuch Datenschutz im Unternehmen: Gestaltungsmöglichkeiten und Strategien für Unternehmen. De Gruyter (2014).

[BSI13] BSI: M 4.2 Bildschirmsperre. (2013). Verfügbar unter: https://www.bsi.bund.de/DE/ Themen/ ITGrundschutz/ ITGrundschutzKataloge/ Inhalt/_content/ m/ m04/ m04002.html. [Zugegriffen: 12-Sep-2017].

[BaSN15] M. Bada, A. Sasse, J. Nurse: Cyber Security Awareness Campaigns: Why do they fail to change behaviour? In: 1st International Conference on Cyber Security for Sustainable Society, Coventry University, Coventry (2015) 118-131.

[Bund79] Bundesarbeitsgericht: Urteil des BAG vom 28. März 1979. (1979). Verfügbar unter: http://www.prinz.law/urteile/BAG_5_AZR_80-77.pdf. [Zugegriffen: 24-Juli-2017].

[ChHo08] M. Chiesa, S. Hobbs: Making sense of social research: How useful is the Hawthorne Effect? In: European Journal of Social Psychology, 38 (2008) 67-74.

[DoCF07] R. C. Dodge, C. Carver, A. J. Ferguson: Phishing for user security awareness. In: Computers & Security 26.1 (2007) 73-80.

[Fede06] H. Federrath: Einwurf. In: M. Mörike, S. Teufel (Hrsg.): Kosten & Nutzen von IT-Sicherheit. HMD, Heft 248, dpunkt.Verlag (2006) 4.

[FHFP18] A. P. Filippidis, C. S. Hilas, G. Filippidis, A. Politis: Information Security Awareness of Greek Higher Education Students - Preliminary Findings. In: 7th International Conference on Modern Circuits and Systems Technologies (MOCAST), Thessaloniki, (2018).

[Gola14] P. Gola: Datenschutz am Arbeitsplatz: Handlungshilfen beim Einsatz von Intranet und Internet, E-Mail und Telefon, Video und GPS, Big Data und Social Media. 5. Aufl. Verl.-Gruppe Hüthig, Jehle, Rehm (2014).

[GKKS15] P. Gola, C. Klug, B. Körffer, D. R. Schomerus (Hrsg.): BDSG: Bundesdatenschutzgesetz: Kommentar. 12. Aufl., C.H. Beck (2015).

[HaPo09] A. Haucke, D. Pokoyski: Das geheime Drehbuch der Security – Awareness in Gestalt- und Tiefenpsychologie. In: M. Helisch, D. Pokoyski (Hrsg.): Security Awareness. Vieweg+Teubner (2009) 75-130.

[Heli09] M. Helisch: Definition von Awareness, Notwendigkeit und Sicherheitskultur. In: M. Helisch, D. Pokoyski (Hrsg.): Security Awareness. Vieweg+Teubner (2009) 9-28.

[ISAC17] ISACA: State of Cybersecurity – Part 2: Current Trends in the Threat Landscape. (2017). Verfügbar unter: http://www.isaca.org/Knowledge-Center/ Research/Documents/state-of-cybersecurity-2017-part-2_res_eng_0517.PDF. [Zugegriffen: 16-Mär-2018].

[KANK11] B. Khan, K. S. Alghatbar, S. I. Nabi, M. Khan: Effectiveness of information security awareness methods based on psychological theories. In: African Journal of Business Management, 26.5 (2011) 10862-10868.

[KoRY15] A. Kohne, S. Ringleb, C. Yücel: Bring your own device: Einsatz von privaten Endgeräten im beruflichen Umfeld – Chancen, Risiken und Möglichkeiten. Springer Vieweg (2015).

[KrKe06] H. A. Kruger, W. D. Kearney: A prototype for assessing information security awareness. In: Computers & Security, 25.4 (2006) 289-296.

[Kütz10] M. Kütz: Kennzahlen in der IT. 4. Aufl., dpunkt.Verlag (2010).

[LaTr16] K. C. Laudon, C. G. Traver: E-commerce 2016: business. technology. society. 12. Aufl., Pearson Education Limited (2016).

[Lelk05] F. Lelke: Kennzahlensysteme in konzerngebundenen Dienstleistungsunternehmen unter besonderer Berücksichtigung der Entwicklung eines wissensbasierten Kennzahlengenerators. Dissertation, Universität Duisburg-Essen (2005). Verfügbar unter: https://duepublico.uni-duisburg-essen.de/ servlets/ DerivateServlet/ Derivate-13370/Dissertation_Lelke.pdf. [Zugegriffen: 20-Jun-2018].

[Lubi06] H. P. Lubich: IT-Sicherheit: Systematik, aktuelle Probleme und Kosten-Nutzen-Betrachtungen. In: M. Mörike, S. Teufel (Hrsg.): Kosten & Nutzen von IT-Sicherheit. HMD, Heft 248, dpunkt.Verlag (2006) 6-15.

[MiSD11] K. D. Mitnick, W. L. Simon, J. Dubau: Die Kunst der Täuschung: Risikofaktor Mensch. 1. Aufl., mitp (2011).

[Nork91] M. E. Nork: Management-Training: Evaluation – Probleme – Lösungsansätze. Rainer Hampp Verlag (1991).

[PoBl96] G. Pomberger, G. Blaschek: Software-Engineering: Prototyping und objektorientierte Software-Entwicklung. 2. Aufl., Hanser (1996).

[ScWe17] A. Schütz, K. Weber: Security Awareness: Nicht nur schulen – überzeugen Sie! In: P. Schartner (Hrsg.): D·A·CH Security 2017. syssec (2017), 1-12.

[Spit14] L. Spitzner: Human Metrics: Measuring Behavior. SANS (2014). Verfügbar unter: https://www. sans. org/ sites/ default/ files/ 2017-12/ STH-Presentation-Human Metrics.pdf. [Zugegriffen: 22-Jun-2018].

[WeSc18] K. Weber, A. Schütz: ISIS12-Hack: Mitarbeiter sensibilisieren statt informieren. In: P. Drews, B. Funk, P. Niemeyer, L. Xie (Hrsg.): Multikonferenz Wirtschaftsinformatik (MKWI) 2018. Leuphana Universität Lüneburg, 6.-9. März 2018, Lüneburg (2018) 1737-1748.

[WiHa03] M. Wilson, J. Hash: Building an Information Technology Security Awareness and Training Program. National Institute of Standards and Technology, NIST SP 800-50 (2003).

[WuPJ17] V. Wu, A. Pipinellis, B. Johnson: Conversational Development Index. GitLab Documentation (2017). Verfügbar unter: https:// docs. gitlab. com/ ce/ user/ admin_area/ monitoring/convdev.html. [Zugegriffen: 16-Sep-2017].

[Witt10] B. C. Witt: Datenschutz kompakt und verständlich: eine praxisorientierte Einführung. Vieweg + Teubner (2010).

[Zina16] L. Zinatullin: The psychology of information security: resolving conflicts between security compliance and human behaviour. IT Governance Ltd (2016).