ISMS: Kompetenz, Awareness, neue Wissenswege

„Plappern gehört zum Handwerk." Der zugegebenermaßen etwas abgewandelte Spruch trifft in unserer digitalen Welt mehr denn je zu. Der Grund ist die umfassende Digitalisierung von allem und jedem. Mensch, Maschine und die schnelllebige Information dazwischen sind zu den Eckpfeilern unserer modernen Lebens- und Arbeitswelt geworden. Doch was des einen Freud ist des anderen Leid. Dampfplauderer am Smartphone in Zügen, dem Flughafen oder in der Hotellobby gehören ebenso zum neuen Zeitgeist, wie ungesicherte Laptops oder Tablets. Wer dann sein mobiles Endgerät verliert, ist im wahrsten Sinne des Wortes vielfach sprach- und orientierungslos. Was für den Privatanwender schon arg, weil heilig und daher unverzichtbar im digitalen Leben, ist für Unternehmen der Gau. So berichtet der Digitalverband Bitkom, dass das „am häufigsten auftretende Delikt (…) der Diebstahl von IT- und Kommunikationsgeräten" sei. Demnach berichten „32 Prozent der Unternehmen (…), dass zum Beispiel Smartphones, Computer oder Tablets gestohlen wurden. Bei einem Fünftel (20 Prozent) wurden sensible physische Dokumente, Bauteile oder Muster entwendet." Das ergab eine aktuelle Umfrage unter 504 Unternehmen des produzierenden Gewerbes ab 10 Mitarbeitern. Im Grunde zeigt diese Tendenz, dass in Unternehmen vieles im Argen liegt. Vor allem beim Thema des sensiblen Umgangs mit Informationen, sprich der Awareness.

Informationssicherheitspannen: Mitarbeiter an erster Stelle

Das Thema der Sensibilisierung vor den Gefahren zunehmender Hackerangriffe, Sabotageakte und Spionagevorfälle ist ein wichtiger Aspekt, ja der Schlüsselfaktor für erfolgreiche Unternehmen im digitalen Zeitalter. Denn Cyberangriffe – gleich, welche Intention dahinter steckt – können alle Bereiche eines Unternehmens treffen und zu einem direkten materiellen Schaden führen. „Die durchgängige Vernetzung macht Systeme anfälliger", weiß Uwe Rühl, Geschäftsführer der RÜHLCONSULTING GRUPPE. Und er ergänzt: „Im schlimmsten Fall sind Unternehmen Cyberangriffen komplett ausgeliefert." Doch, welche Faktoren führen zu Informationssicherheitspannen? Laut Bundesamt für Sicherheit in der Informationstechnik (BSI), nehmen Mitarbeiter den ersten Platz bei den größten Sicherheitslücken ein. Zu diesem Ergebnis kommt eine „Awareness-Umfrage 2015" der „Allianz für Cyber-Sicherheit" – einer Initiative des BSI. Demnach wurde bis dato bei 14 Prozent der über 440 Befragten keine Awareness-Kampagne umgesetzt. Die Gründe liegen vor allem in mangelnder Zeit und wenig Ressourcen, der fehlenden Unterstützung durch die Unternehmensleitung sowie in einem ungenügenden Know-how in Bezug auf Security-Awareness. Doch gerade an diesen Stellschrauben müssen Unternehmenslenker drehen, wenn es zu einem qualitativen Mehr an Awareness in den eigenen Organisationsreihen kommen soll. „Unternehmen und ihre Entscheider müssen das Thema Awareness in der eigenen Organisation ganz oben auf die Agenda setzen, um Mitarbeitern das notwendige Set im Umgang mit unternehmenskritischen Informationen zu vermitteln. Es muss eine Kultur reifen, in der alle an einem Strang ziehen und ihren Beitrag für den Erfolg des Unternehmens leisten. Und dazu gehört ein umsichtiges Verhalten mit dem Wissen der eigenen Firma", so Uwe Rühl. Im Umkehrschluss stellt sich die Frage, wie sich Mitarbeiter stärker in den Sensibilisierungsprozess der jeweiligen Organisation einbinden lassen.

ISMS vielfach unbekannt

Die RÜHLCONSULTING GRUPPE hat jüngst im Rahmen einer Masterarbeit den „Faktor Mensch in der Informationssicherheit" untersuchen lassen.

Konkret ging es um die „Einsatzmöglichkeiten von E-Portfolios zur Erfüllung der Anforderungen der ISO/IEC 27001 an die Sicherstellung der Kompetenz und Awareness". Die in Kooperation an der Donau-Universität Krems erstellte Arbeit zeigt: Wissen und die Wissensvermittlung im Bereich der Informationssicherheit sind entscheidende Bausteine für Unternehmen.

Im Klartext heißt das: Organisationen stehen vor der Herkulesaufgabe, ihren Mitarbeitern ein Informationssicherheitsbewusstsein und die notwendige Kompetenz in diesem Bereich zu vermitteln. Dies lässt sich aus der Rolle ableiten, welche der Mitarbeiter im Bereich Informationssicherheit spielt.

Können Schutzmaßnahmen für Informationen nicht technisch umgesetzt werden, sind Unternehmen darauf angewiesen, dass ihre Mitarbeiter die organisatorischen Vorgaben in Bezug auf Informationssicherheit einhalten. Dies ist umso dringlicher, da es keinen 100-prozentigen Schutz durch technische Lösungen geben kann. Experten verweisen darauf, dass die beste Sicherheitslösung zum Scheitern verurteilt ist, wenn der Mensch nicht mitspielt. Umso wichtiger sind Maßnahmen, um die Sensibilisierung der eigenen Mitarbeiter im Umgang mit dem wichtigsten Rohstoff der Organisationen, sprich Informationen, zu fördern. Im Rahmen der Studie wurden über 170 Unternehmen aus Deutschland, Österreich und der Schweiz befragt. Zu den meistgenannten Branchen gehört die Industrie mit 16 Prozent, gefolgt von Behörden (öffentliche Hand) mit 15 Prozent sowie dem Gesundheitssektor mit 13 Prozent. Im Mittelpunkt stand unter anderem die Frage, bis zu welchem Grad Unternehmen die Anforderungen der ISO/IEC 27001:2013 in Bezug auf Kompetenz und Bewusstsein derzeit umsetzen. Die Ergebnisse zeigen, dass nur 27 Prozent der befragten Unternehmensvertreter wussten, dass in ihrer Organisation ein Informationssicherheitsmanagementsystem (ISMS) nach ISO/IEC 27001 zum Einsatz kommt.

Die meisten Leitlinien und/oder Richtlinien existieren nach Umfrageergebnissen im Bereich der Arbeitssicherheit mit 27 Prozent und der Informationssicherheit/des Datenschutzes mit 26 Prozent. Es folgen die Bereiche Compliance (17 Prozent) sowie die Korruptionsprävention und der Umweltschutz mit jeweils 15 Prozent (siehe Abbildung 1). 84 Prozent der Befragten gaben an, dass in ihrem Unternehmen Leitlinien und/oder Richtlinien zur Informationssicherheit und zum Datenschutz existieren. „Im Grunde zeigt sich einer der häufigsten Mängel in Organisationen darin, dass nur etwas mehr als ein Viertel der Befragten von der Existenz eines ISMS im eigenen Unternehmen wissen", erklärt Uwe Rühl. Und er ergänzt: „Mitarbeiter müssen die Informationssicherheitspolitik des Unternehmens kennen, sonst ist solch ein Vorhaben zum Scheitern verurteilt."

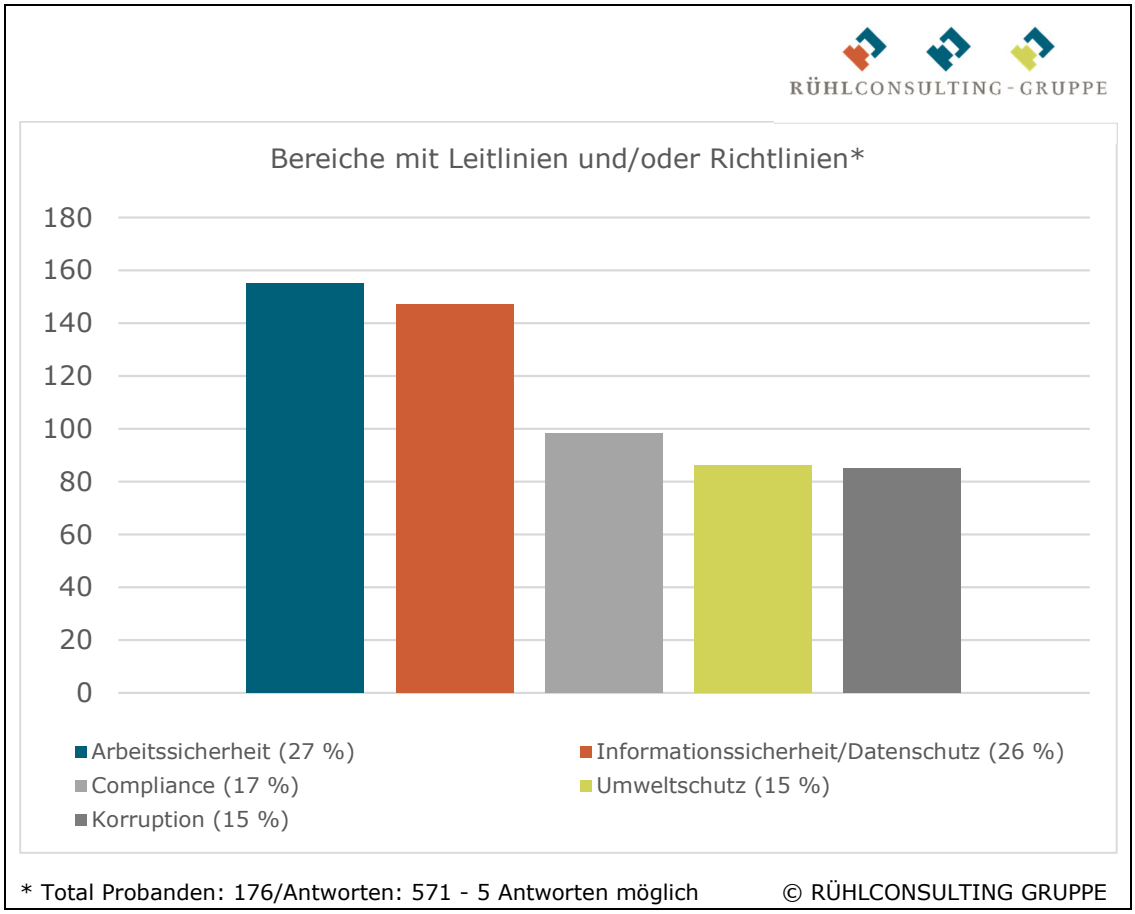

Abbildung 1: Bereiche mit Leitlinien und/oder Richtlinien

Informationssicherheit ist Chefsache

Und darin liegt eine Kernaufgabe der Unternehmensleitung, die einen Gesamtprozess zum ISMS initiieren und deren Wirksamkeit überwachen muss – in der gesamten Organisation. An den Ergebnissen zeigt sich, dass diese Kernaufgabe in Unternehmen zu wenig beachtet wird. Dies deckt sich auch mit Expertenmeinungen, wie der von TeleTrust, dem Bundesverband für IT-Sicherheit. Der Verband kommt in einem Leitfaden zum „Informationssicherheitsmanagement" aus dem Jahr 2012 zu dem Ergebnis: „Heutige Bedrohungen im Zusammenspiel von Menschen, Maschinen und Kommunikationsmedien erfordern, den gesamten Zyklus aller Aktivitäten im Unternehmen organisatorisch, prozessual, physisch und technisch zu betrachten und diesen integriert zu begegnen." Und die Autoren des Leitfadens fügen an: „Ein erfolgreiches Informationssicherheitsmanagementsystem (nachfolgend ISMS genannt) wird ausgehend von der Geschäftsleitung in der Organisation implementiert." Im Klartext heißt das: Informationssicherheit ist Chefsache. Und TeleTrust folgert: „Das Thema Informationssicherheit wird auf dieser Ebene häufig vernachlässigt, da es sich nicht unmittelbar im Tagesgeschäft wiederfindet und ein Bezug zwischen Geschäftszielen und Informationssicherheit oftmals nicht hergestellt wird. Dabei haben Gefährdungen der IT auch einen direkten Einfluss auf die Erreichung der Geschäftsziele, sofern deren Erreichung durch IT-Prozesse unterstützt wird." Unternehmen tun gut daran, sich bei der Einführung eines ISMS externe Unterstützung zu suchen. Wichtig dabei: Das Arbeiten auf Augenhöhe und die professionelle Begleitung des gesamten Prozesses zur ISMS-Einführung.

Dies bestätigt auch Dr. Jan Hadenfeld, Leiter Service Management und Informationssicherheit bei der badenIT, im Rahmen eines Anwenderbeitrags: „Bei der Einführung eines Informationssicherheitsmanagementsystems ist es existenziell, dass die Zusammenarbeit mit dem Dienstleister gleichberechtigt sowie auf dem Prinzip des Vertrauens funktioniert." Beim Tochterunternehmen der badenova AG & Co. KG hat RÜHLCONSULTING im Jahr 2013 – 2014 ein ISMS nach ISO/IEC 27001:2013 erfolgreich eingeführt.

Knackpunkt: Kommunikation und Wissen

Für Dr. Jan Hadenfeld spielt darüber hinaus die interne Informationspolitik eine entscheidende Rolle: „Ohne die Kollegen umfassend abzuholen und zu informieren, werden solche einschneidenden Prozessveränderungen scheitern", warnt Jan Hadenfeld. Und er fügt hinzu: „Gerade ein ISMS lebt davon, dass alle an einem Strang ziehen und ihr Verhalten im Sinne der Gesamtorganisation und letztendlich der Informationssicherheit anpassen." Und Uwe Rühl merkt an: „Mitarbeitern muss ihr Beitrag zur Wirksamkeit des Informationssicherheitsmanagementsystems und der Verbesserung der Informationssicherheit bewusst sein und das geht in erster Linie über eine fundierte Kommunikation in der Organisation." Ein Blick auf die Umfrage und die Felder mit den meisten Schulungsmaßnahmen zeigt, dass 119 Probanden den Bereich Arbeitssicherheit nannten (das entspricht 35 Prozent der Antworten), gefolgt von der Informationssicherheit/Datenschutz mit 85 Probanden, sprich 25 Prozent der Antworten (siehe Abbildung 2).

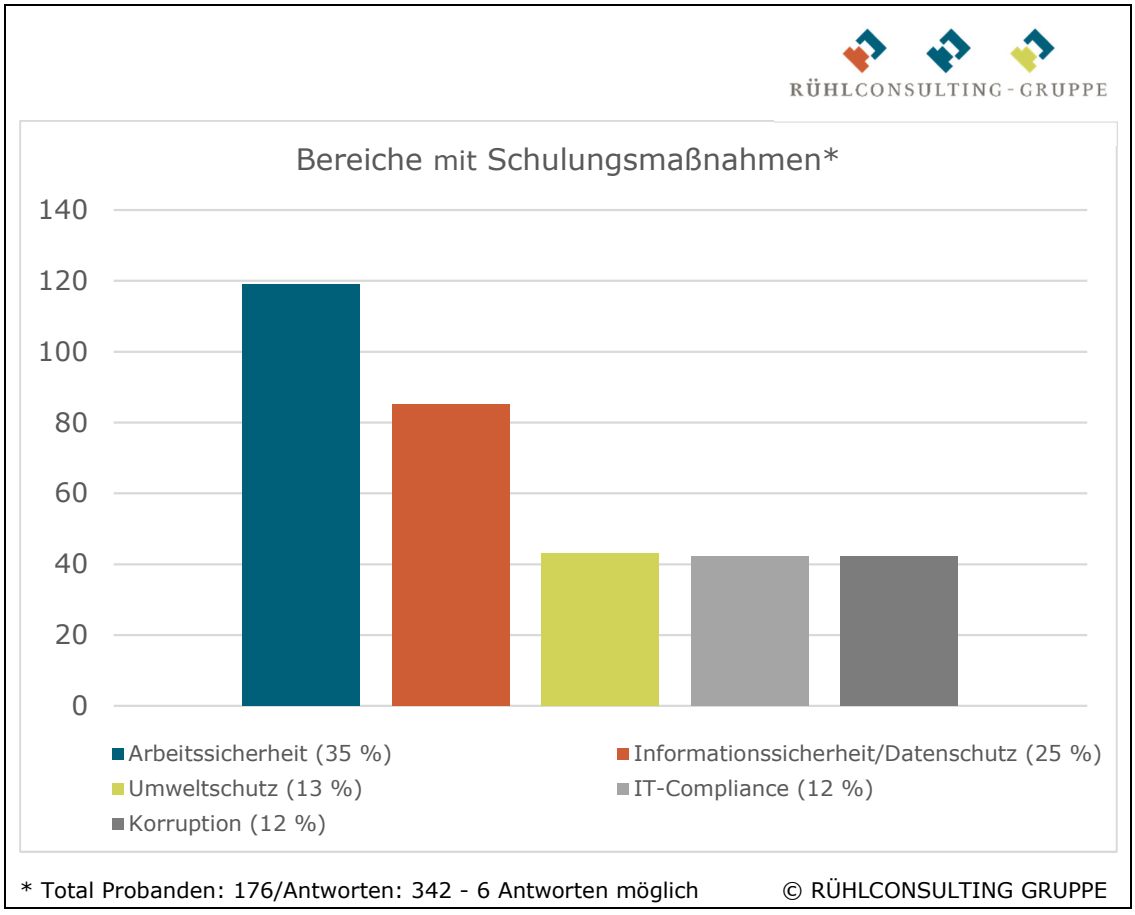

Abbildung 2: Bereiche mit Schulungsmaßnahmen

Interne Seminare sind mit 58 Prozent die häufigste Art der Wissensvermittlung im Bereich Informationssicherheit/Datenschutz. Mit Bezug auf die ISMS-Studie zeigt sich, dass die Kommunikation von Leitlinien im Bereich Informationssicherheit und des Datenschutzes mithilfe elektronischer Dokumente (zum Beispiel PDF) dominiert. 33 Prozent der Befragten nannten elektronische Dokumente als die häufigste Form, gefolgt vom Intranet und WIKIs mit 32 Prozent sowie der Bereitstellung von Leitlinien oder Regelungen in Papierform mit 24 Prozent. 50 Prozent der Befragten gaben an, dass die Bestätigung der Kenntnisnahme und des Verständnisses durch Unterschriften erfolgt. Die Auswertung elektronischer Zugriffe und die Überprüfung anhand von Wissenstests lagen mit 19 und 15 Prozent mit weitem Abstand dahinter. Demnach gaben über die Hälfte der Befragten an, dass das Wissen um Leitlinien oder Richtlinien im Bereich Informationssicherheit und des Datenschutzes zumindest bestätigt werden müsse. Doch genau hier liegt der Knackpunkt, denn eine Bestätigung per Unterschrift lässt keine tatsächlichen Rückschlüsse zum Verständnis der Inhalte zu. „Leider ist die Methode einer reinen Unterschrift keine zielführende Lösung, um das Verständnis im ISMS-Bereich zu fördern und den Mitarbeitern die Auswirkungen bei Nichterfüllung bewusst zu machen", warnt Uwe Rühl.

Zudem fällt im Rahmen der Befragung auf, dass die überwiegende Methode zur Ermittlung vorhandener Kompetenzen im ISMS-Umfeld der Nachweis einer Teilnahme an Schulungen (45 Prozent) und das Vorweisen von Zertifikaten mit 20 Prozent darstellt. Wissenstests wurden demgegenüber nur von 13 Prozent der Befragten benannt. Im Umkehrschluss bedeutet das, dass reine Nachweise des Besuchs der Schulungen in der Kompetenzvermittlung als ausreichend angesehen werden. Eine Information darüber, ob sich die Teilnehmer die dort vermittelten Kompetenzen auch tatsächlich und in ausreichender Weise angeeignet haben, ist kritisch zu hinterfragen. Doch gerade das fundierte Wissen um Inhalte, Prozesse und den praxisnahmen Umgang im ISMS-Umfeld ist entscheidend für den Erfolg von Informationssicherheitsmaßnahmen.

E-Portfolios als Alternative

Im Rahmen der Untersuchung wurde der Einsatz von E-Portfolios als mögliche Alternative zur Vermittlung von Kompetenzen und dem notwendigen Bewusstsein eines ISO/IEC 27001:2013 beleuchtet. Hierzu wurde eigens ein E-Portfolio-Entwurf als „E-Portfolio für Informationssicherheit" auf Basis der Open-Source-Software „mahara" erarbeitet.

Das Prüfungsportfolio soll Mitarbeitern in einem Unternehmen ein Bewusstsein und die notwendige Kompetenz im Bereich der Informationssicherheit vermitteln. Bezüglich der Kenntnisse zu E-Portfolios bestätigt die Befragung, dass E-Portfolios in den befragten Unternehmen größtenteils unbekannt sind (84 Prozent), siehe Abbildung 3.

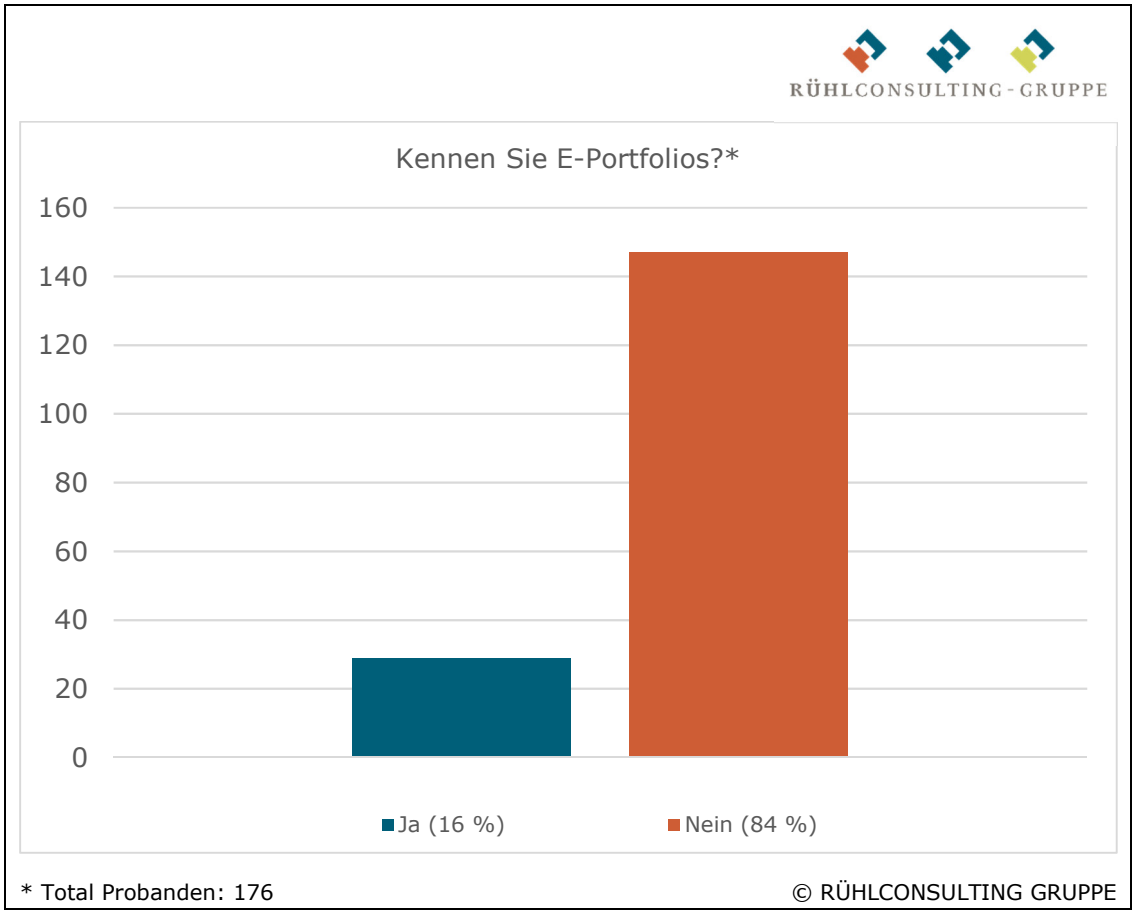

Abbildung 3: Kennen Sie E-Portfolios?

Trotz der Unbekanntheit von E-Portfolios würde ein Drittel der Befragten ein solches im Rahmen von Schulungsmaßnahmen ausprobieren. Allerdings sind auch skeptische Meinungen vertreten. Die meisten Teilnehmer nannten die Akzeptanz (39 Prozent) und die technische Umsetzung (37 Prozent) als größte Herausforderungen beim Einsatz von E-Portfolios.

Um E-Portfolios zielführend zum Ausbau des Informationssicherheitsbewusstseins und der dazugehörenden Kompetenzen einzusetzen, müssen bestimmte Rahmenbedingungen beachtet werden. Vor dem Einsatz von E-Portfolios sollte überprüft werden, ob diese Art der Kompetenzvermittlung zu den Zielen und Werten des Unternehmens passt. Wurde die Entscheidung getroffen, ein E-Portfolio für diesen Zweck einzusetzen, ist eine gute Planung für die Implementierung unerlässlich.

Wichtige Erfolgsfaktoren für den Einsatz von E-Portfolios als Alternative sind unter anderem die Festlegung des Portfoliotyps, Inhalte genau zu planen, eine klare Aufgabenfestlegung sowie die Portfolioarbeit in die Schulungen zu integrieren. Zudem müssen Evaluierungskriterien klar festgelegt und in die Praxis implementiert werden. Letzteres sieht Uwe Rühl als einen entscheidenden Faktor: „Nur wenn solche Maßnahmen praxisnah und flexibel in der jeweiligen Organisation einsetzbar sind, werden den Teilnehmern die Vorteile dieser Lernform deutlich.“ Und das führt am Ende zu mehr Qualität im gesamten ISMS-Prozess. Messbar, handfest und nicht nur geplappert.

E-Portfolio: Was ist das?

E-Portfolios sind eine bestimmte Ausprägung der Portfolioarbeit. Nach Definition der Universität Leipzig handelt es sich bei E-Lernportfolios um „eine Ansammlung von Dokumenten, die es dem Lernenden ermöglichen, den eigenen Lernweg aktiv planen, beschreiten, dokumentieren und reflektieren zu können". Ein E-Portfolio stellt eine Art persönliche Website dar. Die Anwender haben die Möglichkeit, diese im Rahmen gewisser Vorgaben selbst zu gestalten, indem sie Inhalte, zum Beispiel Text- oder Videodateien, hochladen und den eigenen Lernprozess in einem Blog dokumentieren.

Weiterführende Informationen zu den Ergebnissen der Befragung erhalten Interessenten unter: SICHER@RUEHLCONSULTING.de

Autorin

Susanne Keck ist Mitarbeiterin im Bereich IT-Service-Management bei der RÜHLCONSULTING Gruppe und Masterabsolventin an der Donau-Universität Krems zum Thema: „Der Faktor Mensch in der Informationssicherheit: Einsatzmöglichkeiten von E-Portfolios zur Erfüllung der Anforderungen der ISO/IEC 27001 an die Sicherstellung der Kompetenz und Awareness".