KALWEIT ITS

# Effektive Sicherheitsrichtlinien

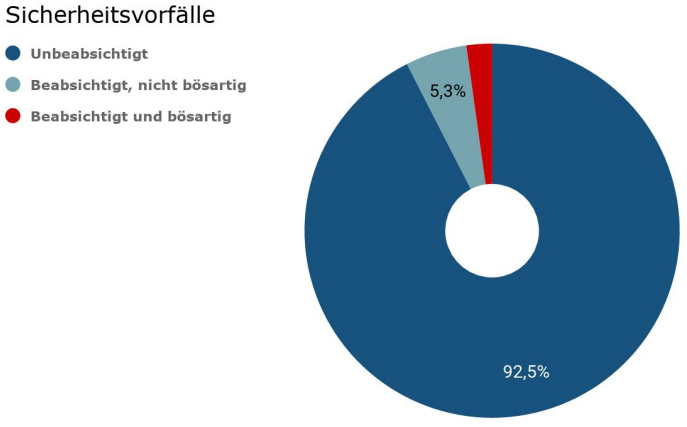
02/2019

# INHALT

# Einleitung

Richtlinien regen nicht zu bewusstem und regelkonformen Handeln an. Sie sind wenig attraktiv formuliert, schränken Menschen in ihrem Handeln ein und schreiben Menschen ihre Kompetenz ab, Situationen selber einzuschätzen zu können und danach zu handeln. Wir sehen hier noch Potential. Zudem steigen wir in die die Hintergründe ein, welche Risiken auf dem Weg zum effektiven Sicherheitsbewusstsein warten.

Das größte Sicherheitsrisiko in Unternehmen bleiben noch immer die Menschen hinten den Systemen. Schon seit Jahren ist bekannt, dass die meisten Sicherheitsvorfälle in Zusammenhang mit menschlichem Fehler stehen. Mitarbeiter sind nicht genügend motiviert, sich selbst um die Sicherheit zu bemühen, weil sie selbst die Konsequenzen nicht spüren müssen. Ein Mitarbeiter bekommt oft nicht mit, dass das Unternehmen aufgrund seines schlechten Passwortes angegriffen wurde. Aus diesem Grund haben Unternehmen auf der ganzen Welt angefangen, Awareness-Programme zur Schulung von Mitarbeitern durchzuführen. Doch das Potential dieser Programme wird bisher nur zu einem Bruchteil ausgeschöpft, wie wir in den nächsten Abschnitten näher erläutern werden. Das Risiko, dass die Mitmenschen nicht wissen, wie sie sich sicher verhalten können, oder schlecht motiviert sind, wird schnell vergessen und jährliche, obligatorische Trainings müssen häufig ausreichen, um dem Risikofaktor Mensch entgegenzuwirken.




*Bei über 92% der Sicherheitsverletzungen sind menschliche Fehler im Spiel[1][2].*

[1] vgl. S. 3, “IBM Security Services 2014 Cyber Security Intelligence Index”
[2] vgl. “Data indicates human error prevailing cause of breaches, incidents”, Mahmood Sher-Jan, 2018

# Risikofaktor Motivation

Regelkonformität durch Sanktionen oder Abschreckung funktioniert nur bedingt. Vor allem fehlt darin die eigene Motivation der Mitarbeiter, sich Wissen und Methoden zum sicheren Handeln anzueignen. Andersherum, sofern schon ausreichend Wissen und Erfahrung vorhanden ist, wirken Richtlinien schnell belehrend, sodass das Gefühl vermittelt wird, dass diese Richtlinien einschränken oder sich gegen die eigene Erfahrung richten. Aus diesem Grund muss klar kommuniziert werden, warum so gehandelt werden soll, wie es in der Vorschrift steht.

Eine innere Motivation ist sehr viel ausschlaggebender als äußere Einwirkungen, wenn es darum geht, im Interesse der Sicherheit der Organisation zu handeln. In manchen Fällen mag es sogar eine negative Korrelation zwischen dem äußeren Zwang und der Intention geben, sich an die Regeln zu halten.

*Im Vergleich zu inneren Überzeugungen haben äußeren Einwirkungen, wie Sanktionen, verschwindend wenig bis sogar negativen Einfluss auf die Motivation, Vorschriften zu befolgen[3].*

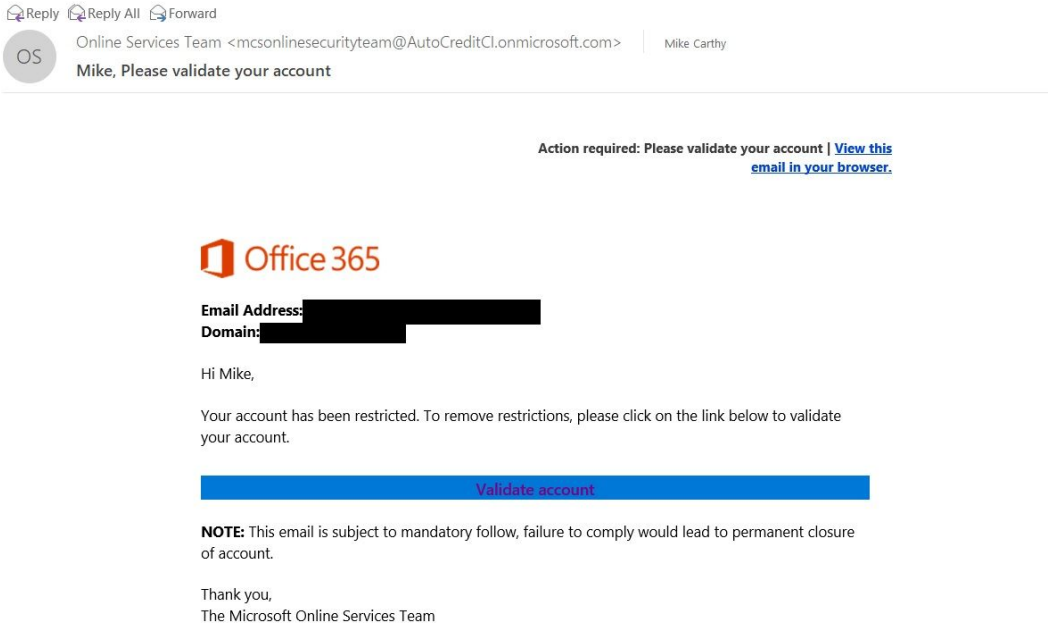
Eine offene Kommunikation steigert die Motivation. Die Wechselwirkung zwischen dem Handeln aus eigener Initiative und einer Kultur des offenen Diskurses über Sicherheit bewirkt, dass die Kollegen nicht nur selbst den Sinn in regelkonformen Handeln sehen, sondern zusätzlich, dass sie sich selbst schulen.

[3] vgl. S. 130, Studies on Employees' Information Security Awareness, Felix Häußinger, 2015 (im Folgenden "SEISA")

# Risikofaktor Training

*Offene Diskussionen über Sicherheit erhöhen die Aufmerksamkeit über das Thema mehr als Präsenzschulungen oder Web Based Trainings[4].*

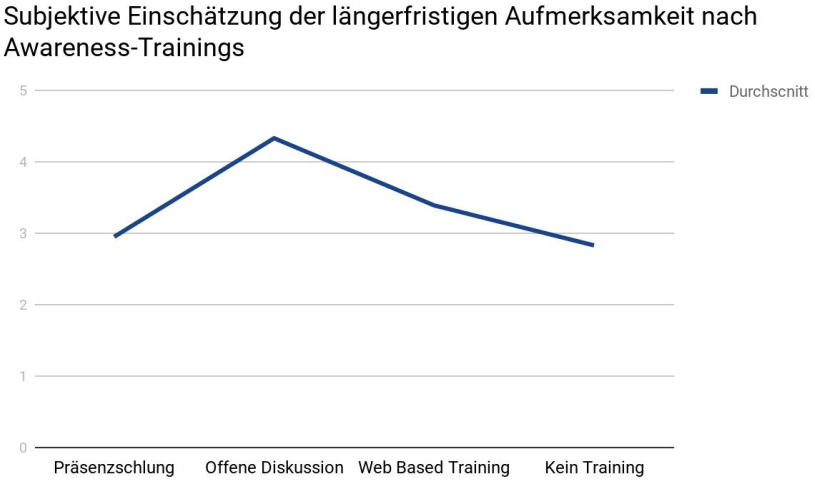
Einzelne Methoden wie Präsenzschulungen umzusetzen, reicht nicht aus, um ein Unternehmen vor internen Risiken zu schützen. Dies ist einfach zu überprüfen: Nach einem obligatorischem Training, zu dem man keine andere Wahl hat, als anwesend zu sein, hat man häufig schnell vergessen, wie zB. eine Spam-Mail aussehen könnte und welche Schritte danach zu befolgen sind. Selbst mit diesem Wissen ist es noch ein Weg hin zur Integration in den Berufsalltag, so dass auch in drei Monaten zwischen all den alltäglichen Mails die Gefahr erkannt wird. Hier ein Beispiel, bei dem unter anderem der Name des Opfers (hier Mike) verwendet wird, um ihn zum Handeln zu überzeugen.




[4] vgl. S. 59, Measuring the Effectiveness of Information Security Awareness Program, Ilirjana Veseli (im Folgenden “MEISA”)

Sich jedoch allein auf eine offene Kommunikation zu stützen, birgt das Risiko, nicht genügend Wissen zu vermitteln und allein Wissen zu vermitteln reicht nicht aus, damit man dieses auch in den Alltag integriert. Die einzelne Präsenzschulung an sich bildet zwar einen ersten Schritt, um Kollegen zu motivieren und zu belehren, jedoch ist die Langzeitwirkung nicht ausreichend abgedeckt.

*Nur eine Minderheit der Teilnehmer von einzelnen Präsenzschulungen nehmen eine langfristige Veränderung ihrer Achtsamkeit wahr[5].*

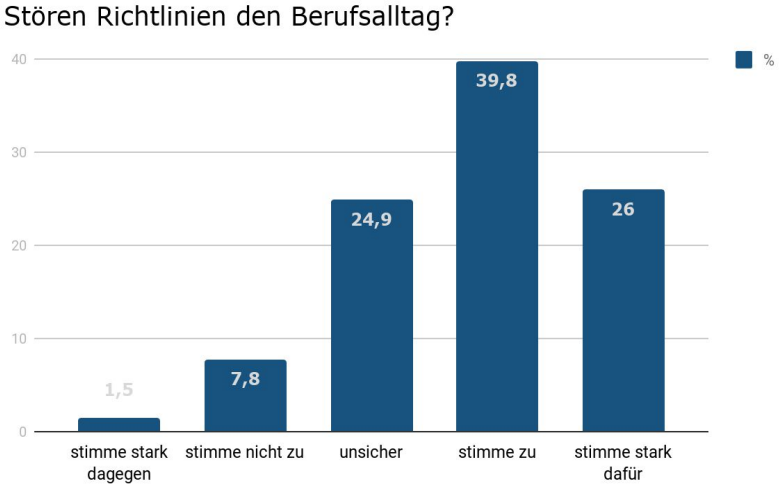



Der Grund für die eingeschätzte Langzeitwirkung für Trainings, die auf offenen Diskussionen über das Thema Sicherheit basieren, ist, dass das Thema mehr in das Bewusstsein der Teilnehmer gerät und dadurch mehr darüber gesprochen wird. Es bleibt nicht bei dem Phänomen des "Teilnehmen und Vergessens", sondern trägt sich in bewussten Gedanken der Teilnehmer.

[5] vgl. S. 59, MEISA

# Risikofaktor Richtlinie

Neben den Möglichkeiten der Mitarbeiterschulungen verbleibt die Herausforderung für Unternehmen, dass Richtlinien zumeist noch immer als Störfaktor gesehen werden und nicht immer auf offene Ohren stoßen. Zusätzliche Arbeit, mehr Bürokratie oder weitere Dokumente, welche auszufüllen sind, werden nicht selten von vielen abgelehnt. Richtlinien, die als Regulierung kommuniziert werden, stoßen auf Unverständnis: Menschen müssen verstehen, warum sie tun sollen, was sie tun sollen. Ansonsten wird der Vorteil vergessen, dass Risiken im Interesse der gesamten gesamten Organisation deutlich vermindert werden, denn jeder Einzelne trägt für den Schutz der Organisation bei. Insbesondere ist dieser Umstand dann zu erkennen, wenn der Handelnde nicht selbst die Folgen seines Verhaltens kennt.




*Eine überwiegende Mehrheit empfindet Sicherheitsrichtlinien als störend oder behindernd[6].*

Beispiel: Mit einer Versicherung gegen Informationssicherheitsvorfälle mag der Versicherte ein sehr viel größeres Risiko eingehen und rücksichtslos handeln, als wenn er keine Versicherung abgeschlossen hätte. Dies erhöht den Fall eines Sicherheitsvorfalles, welcher ungeahnte Folgen haben kann. Im Zweifelsfall zahlt die Versicherung zwar einen Teil des Schadens, die Folgeschäden und Imageprobleme werden dadurch jedoch nicht abgedeckt.

[6] vgl. S. 56, MEISA

# Informationssicherheitsrichtlinien als Chance

Informationssicherheitsrichtlinien mögen in ihrer üblichen Form zB. aufgrund der Länge, der Komplexität oder der Art der Inhalte unattraktiv und uninteressant wirken, jedoch ist nach Häußinger[7] zu schließen, dass, sofern sie attraktiver wären, die Kollegen sehr viel mehr Eigeninitiative zeigten, Risiken abzuwehren.

Dies hat zwei Ursachen:
Zum einen würde die allgemeine Aufmerksamkeit zum Thema Informationssicherheit gestärkt, was wiederum das Sicherheitsbewusstsein erhöht und zum anderen wäre eine der größten Hürden genommen, Richtlinien im Unternehmen bekannt zu machen. Es lässt wenig Zweifel, dass attraktive Richtlinien ein Unternehmen vom Status der Konformität hin zu einem kulturellen Wandel und damit einer erhöhten Sicherheit positiv beeinflusst. Dieser Unterschied gleicht dem Unterschied zwischen einem Fluchtplan und einem Handbuch. Den Fluchtplan kennt kaum jemand auswendig oder interessiert sich hierfür. Ein kurzes Handbuch wirkt sehr viel einladender, weil man den Mehrwert versteht.

Eine unterbewusste Identifikation mit einer attraktiven Richtlinie könnte selbst eine bewusste Abneigung gegen Richtlinien auflockern und ein Werkzeug bieten, den Großteil der Sicherheitsvorfälle zu verhindern. Denn das Ziel sollte es sein, Sicherheit nicht als eine Einschränkung, als Regulierung seines Handlungsspielraumes oder gar als Abschreibung der eigenen Kompetenz zu betrachten, Situationen auch ohne Richtlinie angemessen beurteilen zu kön- nen und darauf basierend angemessen zu handeln. Sicherheit ist eine Chance, keine Regulierung. Denn nur durch Sicherheiten und Standards ist es möglich, Innovation zu nutzen.

[7] vgl. SEISA

# Informationssicherheitsleitlinie der Kalweit ITS

*Die Bereitstellung von kommunizierten Sicherheitsrichtlinien und Möglichkeiten für Mitarbeiter, sich Wissen über das Thema anzueignen, sind zuverlässige Anzeichen für ein gutes Sicherheitsbewusstsein[8].*

Dieser Herausforderung, eine attraktive Leitlinie zur Informationssicherheit umzusetzen, hat sich die Kalweit ITS angenommen. Als Teil ihrer Initiative "Ethical Information Security" hat die Kalweit ITS eine Leitlinie kreiert, die keiner bisherigen gleicht und die Attraktivität des Themas Informationssicherheit in ein neues Licht rücken soll. Auf der nächsten Seite wird das Exemplar in der jetzigen Fassung vorgestellt.

Diese Leitlinie soll die Probleme und Herausforderungen der aktuellen Situation um Awareness und fehlende Motivation angehen. Die Form schafft Aufmerksamkeit und stärkt damit den offenen Austausch über das Thema. Der Inhalt ist so gewählt, dass Sicherheit nicht als Beschränkung verstanden wird, sondern als Möglichkeit, bei dem der Vorteil im Vordergrund steht.

Die erste große Kachel zeigt auf, dass alle Mitarbeiter an einem laufenden Geschäftsbetrieb mitwirken müssen. Die Kachel, die schreibt “a secret has never been told” lässt den Leser daran erinnern, vertraulich mit privaten Daten umzugehen. Sobald private Informationen publik geworden sind, können sie nicht wieder “zurückgeholt” werden.

Zusammenfassend ist die Leitlinie in der Form eine unterstützende Maßnahme, das Sicherheitsbewusstsein zu stärken und die Vorteile in den Vordergrund stellen.

[8] vgl. S. 99ff., SEISA


Die Kalweit ITS

Information Security Policy

The overarching goal of information security is the protection of our working environment and our co-workers.

# Über den Autor

Alexander Kühl ist Unternehmensberater in den Bereichen Risiko- und IS-Management. Zusätzlich zu seiner Tätigkeit als Unternehmensberater hat er diverse Zertifizierungen im Informationssicherheitsmanagement erhalten. Als studierter Informatiker und Philosoph mit ausgeprägtem Verständnis von interkultureller Kommunikation sowie Unternehmenskulturen unterstützt er dabei, die hohen Anforderungen unserer internationalen Kunden zu erfüllen.

“Cybersecurity is dynamisch."

Alexander Kühl, Head of Consulting Services

# Über Kalweit ITS

Wir wollen Cybersecurity für alle verständlich, umsetzbar und selbstverständlich machen. Denn Cybersicherheit ist keine Regulierung, sondern eine Chance für die Digitalisierung.

Ein dezentrales Team, dass Unternehmen als ganzheitlichen Sicherheitsfaktor versteht. Ein Team, dass Sicherheit als soziales Thema versteht und deshalb auch Sozialwissenschaften und Philosophie einsetzt. Denn wir wissen, dass jedes Sicherheitskonzept und jede Sicherheitslösung nur dann wirksam ist, wenn diese auch von den Anwendern akzeptiert wird.

Kalweit ITS - Penetrationstests. Sicherheitsmanagement. Risikomanagement. Consulting. Das sind wir.