Sicherheitskultur aufbauen und pflegen
Agenda

Grundlagen

Workshops

Basis für diesen Vortrag ist der

- Bericht der ENISA (The European Union Agency for Cybersecurity) «Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity»

Sicherheitskultur aufbauen und pflegen
Agenda

Ausgangslage

- Der Mensch ist das grösste Risiko
  … aber auch die grösste Chance

Ziel

- Der Mensch ist das stärkste Glied in der Kette

Vorgaben der Informatiksicherheit / These … Realität?

- Ist es nicht so, dass wir als Informatikverantwortliche mit einem IT-Hintergrund in eine Firma kommen, deren Business wir nicht fundiert genug kennen?
- Wir sind die Fremden, die Eindringlinge, die mit unverständlichen Forderungen kommen und die Mitarbeitenden bei der Erledigung ihrer Arbeit stören
- Adams & Sasse beobachtete 1999, wie nicht funktionierende Passwortrichtlinien die Mitarbeiter zu dem Schluss führten, dass diese Cybersicherheitsmassnahme eingeführt wurde, um ihr Leben zu erschweren, anstatt Schutz zu bieten

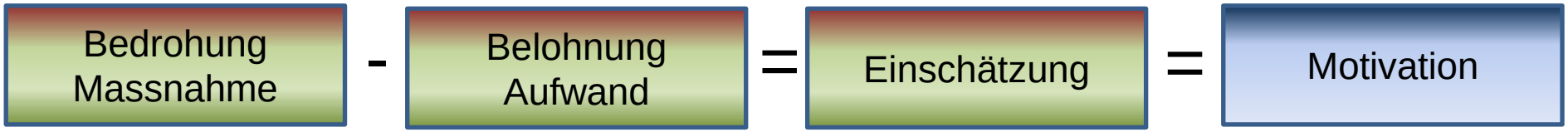
Sicherheitskultur aufbauen und pflegen
Grundlagen

Ziel der Informatiksicherheit ist es, mit einer Sicherheitskultur das Sicherheitsbewusstsein der Mitarbeitenden zu stärken

- Sicherheitskultur ist
  - praxisbezogen
  - auf den Arbeitsplatz der Mitarbeitenden bezogen
- Die aktive Beteiligung der Mitarbeitenden ist besser als eine Verpflichtung auf die Compliance
- Die Organisation schafft eine Sicherheitskultur in der
  - Mitarbeitende entsprechend ihrer Risikostufe geschult werden
  - die Schulung gerne aufgenommen wird
  - die Sicherheitskultur nicht als Schikane empfunden wird

Sicherheitskultur aufbauen und pflegen
Motivationstheorie

Einen wesentlichen Aspekt dieses Ziel zu erreichen finden wir in der Motivationstheorie



Gegen jede Bedrohung gibt es eine Massnahme.
Betrachten wir das Verhältnis Bedrohung / Massnahme.

Jede Bedrohung enthält auch eine Belohnung

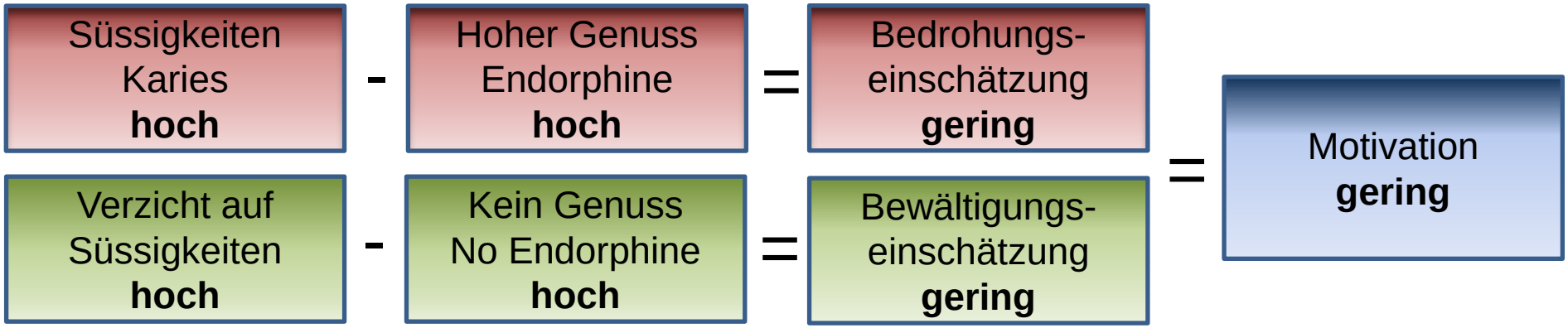
- Bedrohung – Belohnung = Bedrohungseinschätzung (Risiko)

Die Umsetzung einer Massnahme erzeugt einen Aufwand

- Massnahme – Aufwand = Massnahmeneinschätzung (Wirksamkeit)

Wenn wir das Risiko mit der Wirksamkeit vergleichen, ergibt sich daraus die Motivation die Massnahme umzusetzen

Sicherheitskultur aufbauen und pflegen
Motivationstheorie



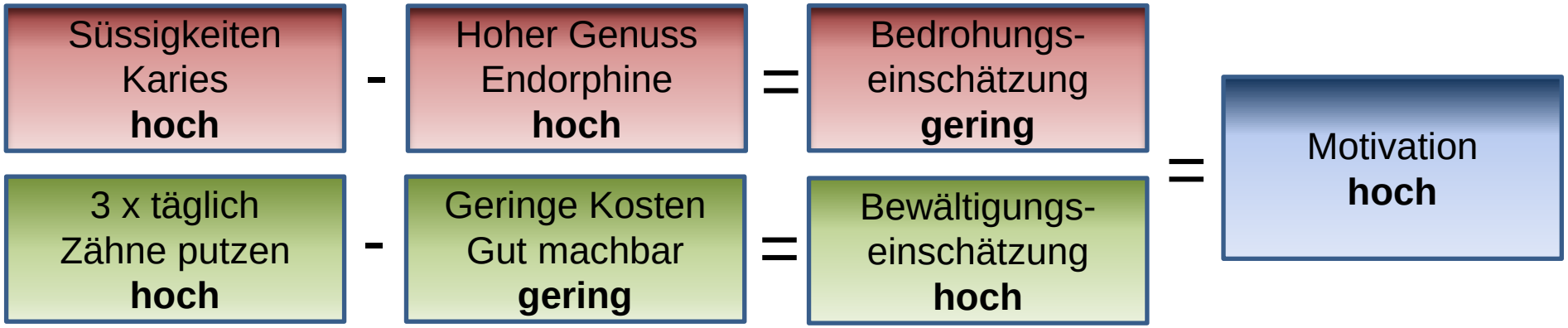
Ein Beispiel

Süssigkeiten naschen beinhaltet das Risiko Karies zu bekommen.
Die Belohnung ist der Genuss und somit sehr hoch, also
Bedrohung – Belohnung ergibt eine sehr geringe Bedrohungseinschätzung.

Die Massnahme auf Süssigkeiten zu verzichten bringt einen hohen Schutz.
Der Aufwand auf Süssigkeiten zu verzichten ist sehr hoch. Niemand will das.
Massnahme – Aufwand ergibt eine sehr geringe Bewältigungseinschätzung.

Das heisst, die Motivation die vorgeschlagene Massnahme umzusetzen ist für den Betroffenen gering.

Sicherheitskultur aufbauen und pflegen
Motivationstheorie



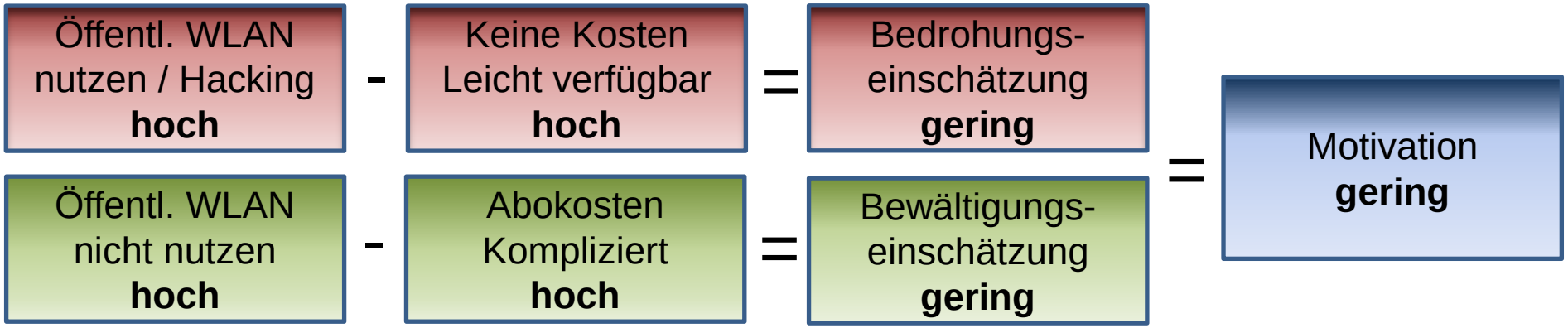
Wenn wir die Massnahme «Verzicht auf Süssigkeiten» durch «3 x täglich Zähne putzen» ersetzen, erreichen wir einen hohen Schutz.

Der Aufwand diese Massnahme umzusetzen ist gering.
Massnahme – Aufwand ergibt eine hohe Bewältigungseinschätzung.

Das heisst, die Motivation die vorgeschlagene Massnahme umzusetzen steigt und ist für den Betroffenen gut machbar.

Was heisst das nun für die Informatiksicherheit?

Sicherheitskultur aufbauen und pflegen
Motivationstheorie

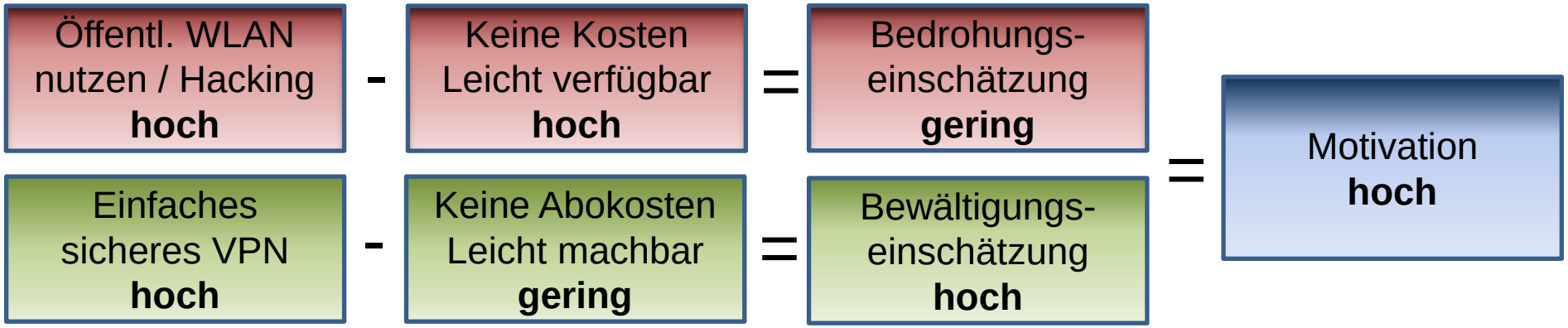


Öffentliches WLAN nutzen beinhaltet das Risiko gehackt zu werden.
Die Belohnung ist ein kostenloser gut nutzbarer Service und somit sehr hoch.
Bedrohung – Belohnung ergibt eine sehr geringe Bedrohungseinschätzung.

Die Massnahme das öffentliche WLAN nicht zu nutzen bringt einen hohen Schutz. Der Aufwand Abokosten und kompliziertes Handling ist sehr hoch.
Massnahme – Aufwand ergibt eine sehr geringe Bewältigungseinschätzung.

Das heisst, die Motivation die vorgeschlagene Massnahme umzusetzen ist für den Betroffenen gering. So wird häufig festgestellt dass an Kadermeetings in Hotels als erstes nach dem Zugangscode gefragt wird !

Sicherheitskultur aufbauen und pflegen
Motivationstheorie



Wenn wir die Massnahme «Öffentliches WLAN nicht nutzen» dadurch ersetzen, dass wir ein «Einfaches sicheres VPN» verfügbar machen, erreichen wir einen hohen Schutz.

Der Aufwand diese Massnahme umzusetzen ist gering.
Massnahme – Aufwand ergibt eine hohe Bewältigungseinschätzung.

Die Motivation die vorgeschlagene Massnahme umzusetzen steigt und ist für den Betroffenen gut machbar.

Das heisst, um erfolgreich zu sein muss die Informatik Massnahmen definieren, welche die Mitarbeitenden motivieren, diese umzusetzen.

Sicherheitskultur aufbauen und pflegen
Unterstützung

Hier ein paar Beispiele, mit welchen Massnahmen die Motivation, der Mitarbeitenden gesteigert werden kann?

Weisung	Unterstützung
Verschlüsselung	Verschlüsselungssoftware anbieten
Speichern Sie keine Daten auf DropBox, OneDrive etc.	Sichere Cloud-Lösung anbieten z.B. trustdrive von Abraxas
Speichern Sie keine Daten auf mobilen Datenträgern	PIN geschützte mobile Datenträger verfügbar machen
Versenden Sie keine grossen Dateien	Sichere Cloud-Lösung anbieten z.B.Webtransfer Kanton ZH
Geräte (z.B. Notebooks und PDA), die am Datennetz der Gemeinde angeschlossen sind, dürfen keine Verbindung über das drahtlose Netz aufbauen.	Kann über die Windows Option «Disabled Upon Wired Connect» gesteuert werden

Sicherheitskultur aufbauen und pflegen
Unterstützung

Weisung	Unterstützung
Verbot von Installationen	Admin-Rechte auf Arbeitsstationen begrenzen
Leiten Sie keine E-Mails weiter	Automatische Weiterleitung ausserhalb der eigenen Domäne verunmöglichen
E-Mail senden: Kontrollieren Sie die Aktualität der Verteilerlisten	Verteilerlisten werden über OU Zugehörigkeit und Rollen definiert
Drucker, Kopierer, Faxgeräte, Ablagekörbli und Papierkörbe sind Orte, an denen oft vertrauliche Informationen liegen	Follow Me Printing als Standardeinstellung. Direct Printing nur auf Antrag
Schreiben Sie nie ein Passwort oder einen PIN-Code auf	Passwortverwaltung verfügbar machen

Sicherheitskultur aufbauen und pflegen
Unterstützung

Weisung	Unterstützung
Clean Desk / Clear Desk Bei Abwesenheit vom Arbeitsplatz dürfen keine sensitiven Informationen offen herumliegen	Alle Türen (hinaus und hinein), Kaffeemaschinen, Drucker durch die Bedienung mit DER Smartcard vorsehen. Ohne die Karte abzuziehen, kann man praktisch nichts machen.
Bei kurzen Absenzen vom Arbeitsplatz müssen Sie Ihren PC mit dem «Screenlock» sperren	Automatisches Sperren nach einer gewissen Zeit
Umgang mit Besuchern, externen Mitarbeitenden und unbekannten Personen	Bauliche Massnahmen. Türknauf. Zustrittskontrolle, Zugang nur mit Smartcard. Besucherbadges, keine unbegleiteten «Externen».

Sicherheitskultur aufbauen und pflegen
Workshops

Wir müssen die Mitarbeitenden motivieren

- Bewältigungseinschätzung stärken
- Motivation stärken

Mit der Frontalschulung vermitteln wir Informationen

Die Frontalschulung ist eine Einwegkommunikation

Mit Workshops erreichen wir die Mitarbeitenden direkt
und involvieren sie in den Entscheidungsprozess
welche Massnahmen wie umgesetzt werden sollen

Die Mitarbeitenden tragen diese Entscheide mit

Damit steigt die Motivation die Massnahmen umzusetzen

Sicherheitskultur aufbauen und pflegen
Workshops

Mit den Workshops soll erreicht werden, dass die Mitarbeitenden bei ihrer täglichen Arbeit

- die Risiken und Gefahren im Umgang mit Informationen und Informatikmittel kennen,
- die Massnahmen gegen die Risiken und Gefahren kennen,
- motiviert sind und sich in der Lage fühlen diese Massnahmen umzusetzen,
- ihre Rolle kennen und sich bewusst sind, welche Konsequenzen ihr Handeln im Umgang mit Informationen und Informatikmittel haben,
- wissen, dass sie nicht allein sind.

Wir sitzen alle im selben Boot.

Ein Angriff bedroht zwar primär den Einzelnen schlussendlich aber das gesamte Unternehmen.

Sicherheitskultur aufbauen und pflegen
Workshops planen

An den Workshops werden die Themen in Gruppen behandelt

Danach kommen die Gruppen zusammen um die Resultate gemeinsam zu diskutieren

Wie viele Gruppen sind pro Workshop sinnvoll?

- Ideal ist ein 1.5-stündiger Workshop mit drei Gruppen
- Um eine gute Durchmischung der Gruppe zu erreichen,
  stellt der Moderator die Gruppen vor dem Workshop zusammen
- Ein Thema pro Workshop
  d.h. jede Gruppe behandelt dasselbe Thema

Je nach Erfahrungen in den ersten Workshops kann dieses Konzept angepasst werden, z.B. vier Gruppen / zwei Themen …

Gruppenarbeit 30'

- Wie gehst du mit E-Mails um … geschäftlich … privat?
- Welchen Stellenwert hat das E-Mail für dich?
- Welche Bedrohungen sind dir im Zusammenhang mit E-Mails bekannt? Wie schützt du dich davor?
- Was ist ein verschlüsseltes E-Mail?
- Was passiert beim Weiterleiten von E-Mails?

Die Gruppe diskutiert die Fragen und hält die Erkenntnisse, weitere Fragen, Anregungen auf dem Flip-Chart fest

Rekapitulation 20'

- Die Gruppen stellen ihre Erkenntnisse vor
- Die Erkenntnisse werden diskutiert
- Der Moderator kommentiert und ergänzt die Diskussionsergebnisse
- Der Moderator stellt Massnahmen vor, welche sich aufgrund der Diskussionsergebnisse ergeben
- Die Massnahmen werden diskutiert
- Der Moderator nimmt die Diskussionsergebnisse auf und lässt sie in die künftige Arbeit der Informatik einfliessen

Die Erkenntnisse werden periodisch in den Personalmitteilungen publiziert

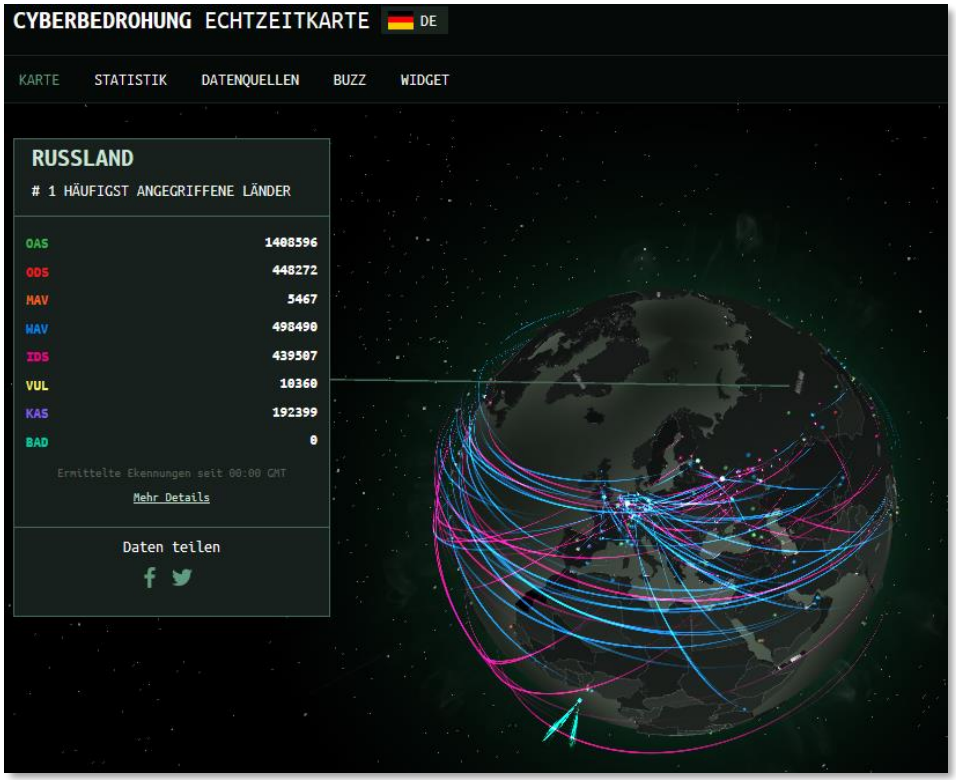
Sicherheitskultur aufbauen und pflegen
Workshops / Zeitplan

Vormittag	Nachmittag	Minuten	Thema	Aktion
10.00 – 10.15	13.30 – 13.45	15'	Begrüssung Ziel und Zweck Workshop-Organisation, Agenda Themen vorstellen Gruppen bilden und Themen verteilen Schriftführer*in pro Gruppe bestimmen. Diese*r erstellt das Protokoll auf dem Flip-Chart.	Einführung
10.15 – 10.45	13.45 – 14.15	30'	Gruppenarbeit	Ausübung
10.45 – 11.05	14.15 – 14.35	20'	Gruppenarbeit besprechen	Rekapitulation
11.05 – 11.20	14.35 – 14.50	15'	Fazit Lessons learned Wie weiter Fragen, Feedback der Teilnehmer*innen	Abschluss
11.20 – 11.30	14.50 – 15.00	10'	Zeitreserve	

Sicherheitskultur aufbauen und pflegen
Workshops / Zeitplan

Workshop am Vormittag zur Begrüssung freiwillig eine halbe Stunde früher starten mit Kafi und Gipfeli
Workshop am Nachmittag zum Ausklang freiwillig eine halbe Stunde länger mit Kafi, Wasser, Orangensaft und Gebäck

In dieser Zeit
https://cybermap.kaspersky.com/de
oder
https://www.sicherheitstacho.eu/start/main
auf einem PC an die Wand beamen



Sicherheitskultur aufbauen und pflegen
Workshops

Themen

- E-Mail
- Surfen im Internet
- Passwörter
- Soziale Netzwerke und Messenger
  (Cybermobbing - anonyme Beleidigungen im Netz)
- PC-Sicherheit, Ipad, ICloud, OneNote, Mobile Geräte
- Datenschutz / Informationsschutz
- Social Engineering
- Sicherheit zu Hause und unterwegs / Home Office

Diese Liste muss jede Gemeinde individuell zusammenstellen und priorisieren (z.B. Home Office ist zur Zeit erste Priorität)

Aufwand

- Drei Gruppen à 5-8 Personen = Workshops mit 15 – 24 Teilnehmenden
- Anzahl Workshops pro 100 Mitarbeitende:

Anzahl Mitarbeitende	Teilnehmende pro Workshop	Workshops
100	15	7
100	18	6
100	21	5
100	24	5

- Zusätzliche Workshops planen für solche die nicht teilnehmen konnten

Sicherheitskultur aufbauen und pflegen
Fazit

Sicherheitskultur aufbauen

- Mit den unterstützenden Massnahmen zu unseren Weisungen stärken wir die Motivation der Mitarbeitenden diese umzusetzen
- Mit den Workshops beziehen wir die Mitarbeitenden ein in die Entscheidung welche Massnahmen wie umgesetzt werden

Sicherheitskultur pflegen

- Neue Arbeitsmittel werden eingesetzt, Bedrohungen ändern sich
- Dadurch ändern auch Weisungen und Massnahmen, welche zeitnah umgesetzt werden müssen

Somit ist Sicherheitskultur ein laufender Prozess
welcher gepflegt werden muss

Sicherheitskultur aufbauen und pflegen
Danke für Deine Aufmerksamkeit …

bbic GmbH

Beat Binder

Im Heugarten 22

8617 Mönchaltorf

beat.binder@bbic.ch

+41 43 521 13 90

+41 79 227 07 31

Hast Du

- Anregungen?
- Fragen?

Brauchst Du

- Beratung?
- Hilfe bei der Umsetzung?
- Doch lieber eine Frontalschulung?

… melde Dich