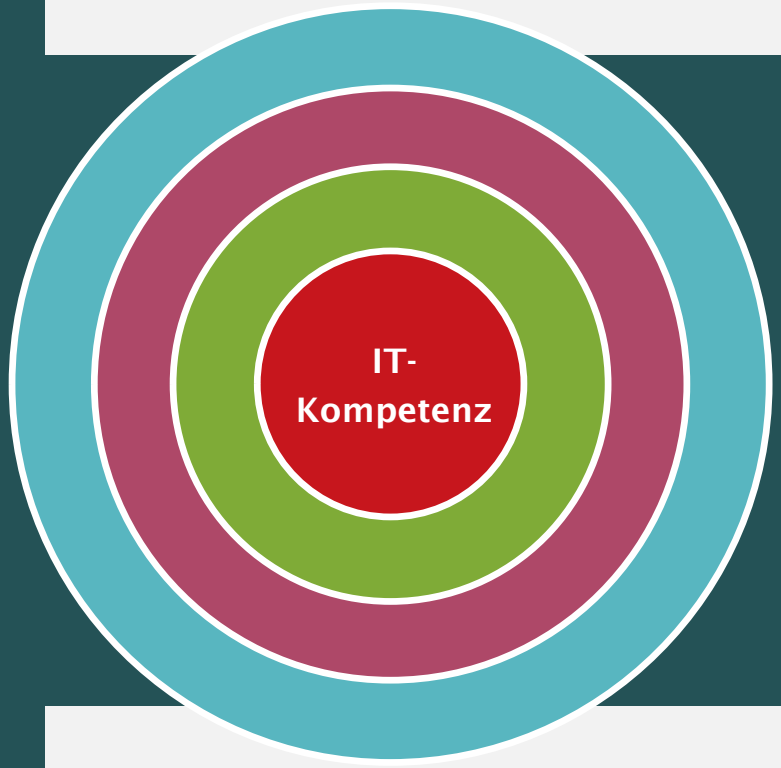
Digital.Kommunal.Sicher –
Informationssicherheit in der Kommunalverwaltung

IT-Kompetenz in Kommunen – Mitarbeiterschulung und -sensibilisierung

Dipl.-Psych Ivona Matas, Köln



Was bedeutet Sensibilisierung?

„Faktor Mensch“

Externe Einflussfaktoren

Gesellschaftlicher Kontext/
Kommunikationswelten

➡ Konkrete Planung von Maßnahmen

Was bedeutet Sensibilisierung?

- **Ziel von Sensibilisierung:** Mitarbeitende sollen befähigt werden, Gefahren zu erkennen, sicherheitsbewusst zu handeln und Cyberkriminalität zu verhindern.
- **Definition von Sensibilisierung:** die prozess- oder impulsgelenkte Zustandsveränderung der Sensibilität
- **Definition von Sensibilität:** der […] erworbene emotionale, kognitive und motivationale Zustand des Menschen für ein bestimmtes Themenfeld
- **Inhalte von Sensibilisierungsmaßnahmen:** Viele Maßnahmen beschränken sich auf technische Inhalte – die menschliche Komponente bleibt außen vor, dabei sind zunehmend Mitarbeitende die Angriffsstellen von Cyberkriminalität.

Was bedeutet und wie funktioniert Sensibilisierung?

- Lernen und Gedächtnis
  - Lernen ist ein komplexer Vorgang, der lebenslang stattfindet, und nicht nur die gezielte Aneignung von Wissen darstellt.
  - Auch das Gedächtnis ist kein „Speicher“, aus dem Gelerntes „abgerufen“ wird, sondern selbst ein aktiver Prozess, der permanent durch Erfahrungen und Veränderungen der Umwelt beeinflusst wird.

- Motivation und Emotionen
  - Lern- wie auch Leistungsmotivation bestimmen die Bereitschaft und die Absicht, sich eigenständig, dauerhaft und wirkungsvoll mit bestimmten Themen zu beschäftigen.
  - Die Gestaltung einer angemessenen Lernatmosphäre kann nachhaltig den Erfolg von Sensibilisierung beeinflussen.

Was bedeutet und wie funktioniert Sensibilisierung?

- Einstellungen
  - Nicht nur fehlendes Know-how führt zu Erfolg von Cyberkriminellen, vielmehr entscheiden persönliche Einstellungen und normative Glaubenssätze von Mitarbeitenden über Erfolg oder Misserfolg von Angriffen.
  - Einstellungen sind wertende Urteile, die sich in Vorurteilen und Wertvorstellungen zeigen. Sie können positiv, negativ oder neutral sein und dabei unterschiedlich intensiv ausfallen (Stärke).
  - Das individuelle Sicherheitsverhalten von Mitarbeitern wird auch von persönlichen Einstellungen und Werten beeinflusst.

Was bedeutet und wie funktioniert Sensibilisierung?

- Ihre Aufgabe ist demnach:
  - die Motivation für Themen der IT-Sicherheit zu stärken,
  - eine förderliche emotionale Gestimmtheit herzustellen,
  - die Einstellungen der Teilnehmenden zu berücksichtigen und
  - gleichzeitig die Arbeitsweise des Gedächtnisses sowie
  - die neuesten Erkenntnisse der Lernpsychologie zu berücksichtigen!

Was bedeutet und wie funktioniert Sensibilisierung?

- Kompetenzwahrnehmung: Information über relevante Themen, Maßnahmen an den eigenen Arbeitsplatz/eigene Aufgaben anpassen; Aufgreifen der eigenen Arbeitsabläufe, individuelle Rückmeldungen
- Selbstbestimmung: Maßnahme nicht als Zwang, Beteiligung an der Auswahl der Inhalte und dem Zeitpunkt der Durchführung; Rückmeldung des Lernerfolgs
- Soziale Bezogenheit: Lernen in kommunikativen Bezügen (kooperatives Lernen/ Teamarbeit) schafft Motivation. Einstellungen werden im sozialen Rahmen schneller sichtbar und können aktiv einbezogen werden.
- Anwendungswert: Konkreter Nutzen und die Relevanz der Inhalte müssen deutlich werden, ebenso der (übergeordnete) Sinn und Zweck der Sensibilisierung; Verknüpfung oder Hinweise auf private Anwendungsmöglichkeiten unterstützen dies. Begeisterung und das „echte“ Interesse der durchführenden Schulungsleiter/ -dozenten können die Einstellungen der Teilnehmer positiv beeinflussen.

Was bedeutet und wie funktioniert Sensibilisierung?

- Lernen und Gedächtnis, Motivation und Emotion, Einstellungen

„Faktor Mensch“

- psychologische Mechanismen und (soziale) Eigenschaften
- Involvement

„Faktor Mensch“

- Welche entscheidende Rolle psychologische Mechanismen, Persönlichkeitsfaktoren und (soziale) Eigenschaften spielen, ist Cyberkriminellen bewusst – und sollte daher auch bei der Sensibilisierung berücksichtigt werden.
- Dabei kommt dem Tatbestand des „Social Engineering“ ein besonderer Stellenwert zu. Laut BSI werden darunter:

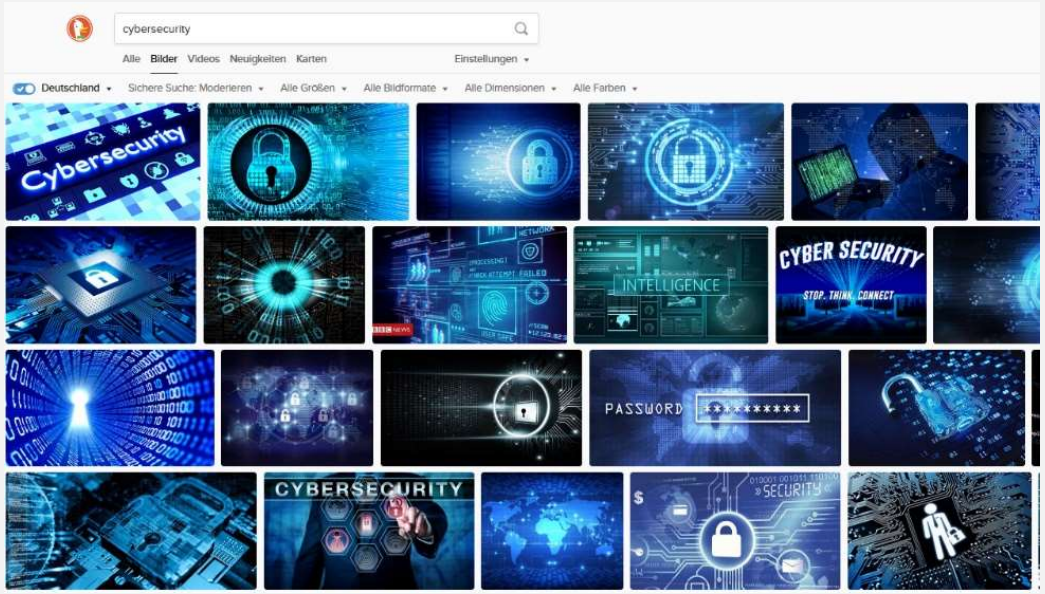
  „Manipulationsversuche zusammengefasst, mit denen Betrüger an vertrauliche Informationen von Unternehmen [und Kommunalverwaltungen!] *oder Privatpersonen kommen wollen. Diese Informationen werden dazu genutzt, Zugang zu IT-Systemen der Opfer und letztlich zu sensiblen Daten verschaffen“.*

„Faktor Mensch“

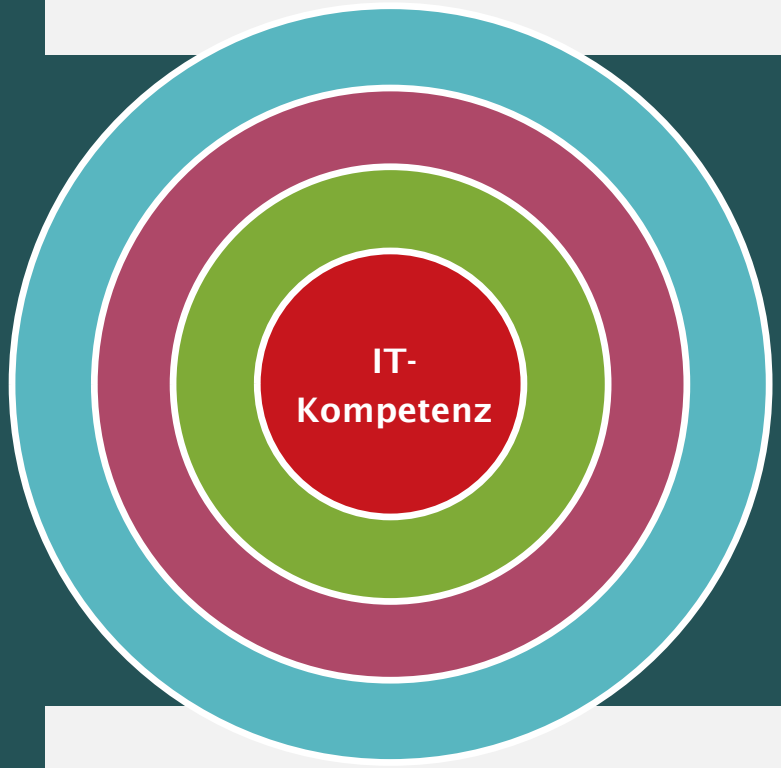
- Nicht alle menschlichen Eigenschaften und Mechanismen eignen sich für die Manipulation durch Cyberkriminelle – hier eine Auswahl:
  - Konsistenz
  - Reziprozität
  - Knappheit
  - Verantwortungsdiffusion
  - Sympathie
  - Neugier
  - soziale Bewährtheit
  - soziale Anerkennung
  - Hilfsbereitschaft
  - Respekt vor Autoritäten
  - Naivität, Gutgläubigkeit

„Faktor Mensch“

- Involvement – oder: Keiner will mehr Hoodies sehen …



- Sensibilisierungsmaßnahmen erfordern Design und Marketing – insbesondere für das nicht immer als Top- Thema wahrgenommene oder gar unbeliebte Thema der IT- oder Cybersecurity!



Was bedeutet Sensibilisierung?

„Faktor Mensch“

Externe Einflussfaktoren

Gesellschaftlicher Kontext/
Kommunikationswelten

➡ Konkrete Planung von Maßnahmen

Externe Einflussfaktoren

- Image und Positionierung von Sicherheit
- Behörden- und Fehlerkultur, Einfluss von Führungskräften
- Marketing der IT-Sicherheit

Gesellschaftliche Veränderungen – veränderte Kommunikationswelten

Externe Einflussfaktoren

„Alle Vorgesetzten MÜSSEN die Informationssicherheit unterstützen, indem sie mit gutem Beispiel vorangehen. Führungskräfte MÜSSEN die Sicherheitsvorgaben umsetzen. Hierüber hinaus MÜSSEN sie ihre Mitarbeiter auf deren Einhaltung hinweisen.“

(BSI. IT Grundschutz ORP.3 Sensibilisierung und Schulung.
Punkt 3.1 Basis-Anforderungen; Hervorhebungen im Original)

Sicherheitskultur ist das „Resultat von individuellen und gruppenspezifischen Werten, Normen und Wissensbeständen, welche das Verhalten im Umgang mit Informationssicherheit beeinflussen“ (Schlienger, 2006).

Ausblick auf eigene Sensibilisierungsmaßnahmen

- Sensibilisierung basiert nicht nur auf der Auswahl von richtigen Anbietern/Tools.
  - Dennoch ist ein Blick auf die zahlreichen Tools wichtig. Es gibt eine Vielzahl von „Online-/digitalen Tools, wie Offline-/analoge Tools mit sozialem Austausch oder ohne soziale Aspekte.

Ausblick auf eigene Sensibilisierungsmaßnahmen

Online-/digitale Tools	Offline-/analoge Tools	
	ohne primär soziale Aspekte	mit sozialem Austausch
Live-Hacking	Leitfigur, Logo, Slogan Maskottchen	(gezielt eingesetzter) „Flurfunk“
Interne soziale Netzwerke/Intranet	Plakate, Poster, Postkarten, Tischkarten, Sicherheitskalender	Vorträge, Präsentationen, Informationsveranstaltungen
Sicherheitsspiele, Planspiele im Intranet	Comics, Cartoons	(moderierte) Sicherheitstreffen (Sicherheits-Pause, -Frühstück, -Talk, -Runde usw.)
Audiobooks, Hörspiele	Mitarbeitermagazin	Mitarbeiterveranstaltungen, Treffen, Aktionen
Web-based-Trainings (WBT)	Begrüßungsmappe	Trainings, Seminare, Workshops
Bildschirmschoner, Desktophintergrund	Leitlinien, Goldene Regeln, Regelwerke	„Unterstützer“/ Mentorenprogramm
(Erklär-)Videos, Filme, Tutorials, Animationen	Gimmicks (Password-Halter, Virus-Bausteine u. Ä.)	Theater, Märchen, Storytelling
E-Mail, E-Newsletter	Aushang, schwarzes Brett, Stopper, Aufkleber usw.	Führungskräftedialoge/gespräche, Coaching

Ausblick auf eigene Sensibilisierungsmaßnahmen

- Eine Untersuchung von Online-Tools zur Erkennung von Phishing-Mails aus dem Jahr 2020* hat ergeben, dass führende Anbieter (Chip, BSI, KlickSafe usw.) in ihren Trainings zwar ausreichend sensibilisieren, den Teilnehmenden jedoch häufig die Handlungssicherheit fehlt, was im Folgenden genau mit einer Mail zu tun ist, die als Phishing identifiziert wurde. Dies sollte daher ebenfalls in die jeweilige Maßnahme aufgenommen werden.
- Planen Sie auch nach einer Maßnahme die notwendige Zeit für eine dauerhafte Konsolidierung ein – mit den notwendigen Wiederholungen bzw. Auseinandersetzungen mit dem jeweiligen Thema).

* Hilt, T., Volkamer, M.: Sensibilisierung für Phishing und andere betrügerische Nachrichten. Vergleich frei verfügbarer Angebote. In: DuD – Datenschutz und Datensicherheit, Springer, 2020

Ausblick auf eigene Sensibilisierungsmaßnahmen

„Klassischer“ Fahrplan

- Klärung von Bedarf und Ziel(en) der konkreten Maßnahme
- Bildung eines Teams
- Konzepterstellung
- Einbindung von Führung (Budget, Freistellung, Zeitaufwand)
- Entwicklung eines (realistischen) Zeitplans
- Entwicklung sog. Sekundärinstrumente (Maßnahmen ankündigen und „bewerben“)
- Überlegungen zu Dokumentation und Reporting, ggf. Evaluation

Vielen Dank für Ihr Interesse!

Dipl.-Psych. Ivona Matas
Weißhausstraße 23
50939 Köln
Tel: 02234 680 4851
Fax: 02234 689 8512
Mobil: 0178 671 2214
Threema-ID: AWJ8T6FB
imatas@posteo.de