



Informationssicherheit: Verantworten, Vorbeugen, Handeln

Themenwochen Führungswissen

Der rote Faden

1. Verantwortlichkeit für Informationen, Werkzeuge und Identitäten
2. Regelungen, Sensibilisierung und Schulungen
3. Verhalten bei Informationssicherheitsvorfällen und Meldepflichten



Foto von Michael Dolnick auf unsplash.com

Statistik

Edkimo Umfrage



<https://edkimo.com/shared/sk04jg3q5pqkl9ii87qk66ykt rh9hk65b7>



Foto von Michael Dolnick auf unsplash.com

Montagmorgen...

Ein Mitarbeiter ruft an:

„Ich habe gerade auf einen Link geklickt – und jetzt sieht mein Bildschirm irgendwie anders aus.“



Verantwortung

Informationen, Werkzeuge und Identitäten im eigenen Bereich

Informationen

- Welche Informationen liegen in meinem Verantwortungsbereich?
- Welche davon sind besonders schützenswert?
- Wer darf darauf zugreifen?
- Wo dürfen sie gespeichert und verarbeitet werden?
- Was wäre die Folge von Verlust, Veränderung oder Offenlegung?



Werkzeuge

- Welche Anwendungen und Dienste nutzt mein Bereich?
- Sind sie für die jeweilige Verarbeitung zugelassen?
- Gibt es Schatten-IT oder private Tools?
- Werden Daten in neue Tools oder KI-Dienste hochgeladen?
- Können Mitarbeitende die Risiken einer Nutzung einschätzen?



Identitäten

- Persönliche Accounts statt gemeinsamer Benutzerkonten
- Rollen und Berechtigungen regelmäßig überprüfen
- Passwörter und MFA schützen
- Zugänge bei Rollenwechseln und Austritten anpassen
- Stellvertretungen sauber regeln



Verantwortung

Informationen, Werkzeuge und Identitäten im eigenen Bereich

Wenn Sie heute Nachmittag in ihren Bereich schauen: Wo liegt der blinde Fleck?

Vorbeugen

Regelungen, Sensibilisierung und Schulungen

Regelungen schaffen den Rahmen

- Welche Regeln sind für meinen Bereich relevant?
- Wo finde ich die gültigen Vorgaben?
- Welche Anforderungen sind besonders kritisch?
- Wann muss ich Fachstellen einbeziehen?

<https://intranet.itz.lwl.org/de/042/informationssicherheit/>



Sensibilisierung: Aus Regeln muss Verhalten werden

- Sicherheitsvorfälle und Verdachtsfälle im Team besprechen
- Ungewöhnliche Anfragen gemeinsam reflektieren
- Sicheren Umgang mit vertraulichen Informationen thematisieren
- Neue Tools und KI-Anwendungen bewusst hinterfragen
- Fehler als Lernchance nutzen – statt sie zu vertuschen



Vorbild sein

- Nutze ich selbst sichere Kommunikationswege?
- Gehe ich sorgfältig mit Zugangsdaten um?
- Lasse ich Geräte unbeaufsichtigt?
- Nutze ich private Geräte oder Tools für dienstliche Informationen?
- Ignoriere ich Sicherheitsvorgaben, wenn es schnell gehen muss?



Handeln

Verhalten bei Informationssicherheitsvorfällen und Meldepflichten

Vorfälle: Schnelle Reaktion

ERKENNEN

- Was ist passiert?
- Wann war das?

ABSICHERN

- Schaden begrenzen und
- Vorgaben beachten

MELDEN

- Unverzüglich an UHD
- an die vorgesehenen Stellen (DSB, RPA)



ABER:

Nicht gemeldet werden müssen:

- Spam-Mails
- Phishing-Mails
- Ohne dienstlichen Bezug

Wenn keine Interaktion stattgefunden hat:

- Anhang geöffnet, Link angeklickt, geantwortet, Informationen eingegeben



Vorfall: „CEO Fraud“

Angreifer

- Gibt sich als FK aus
- Fordert Gutscheine/Überweisung

Hintergrund

- Organisationsstrukturen öffentlich verfügbar

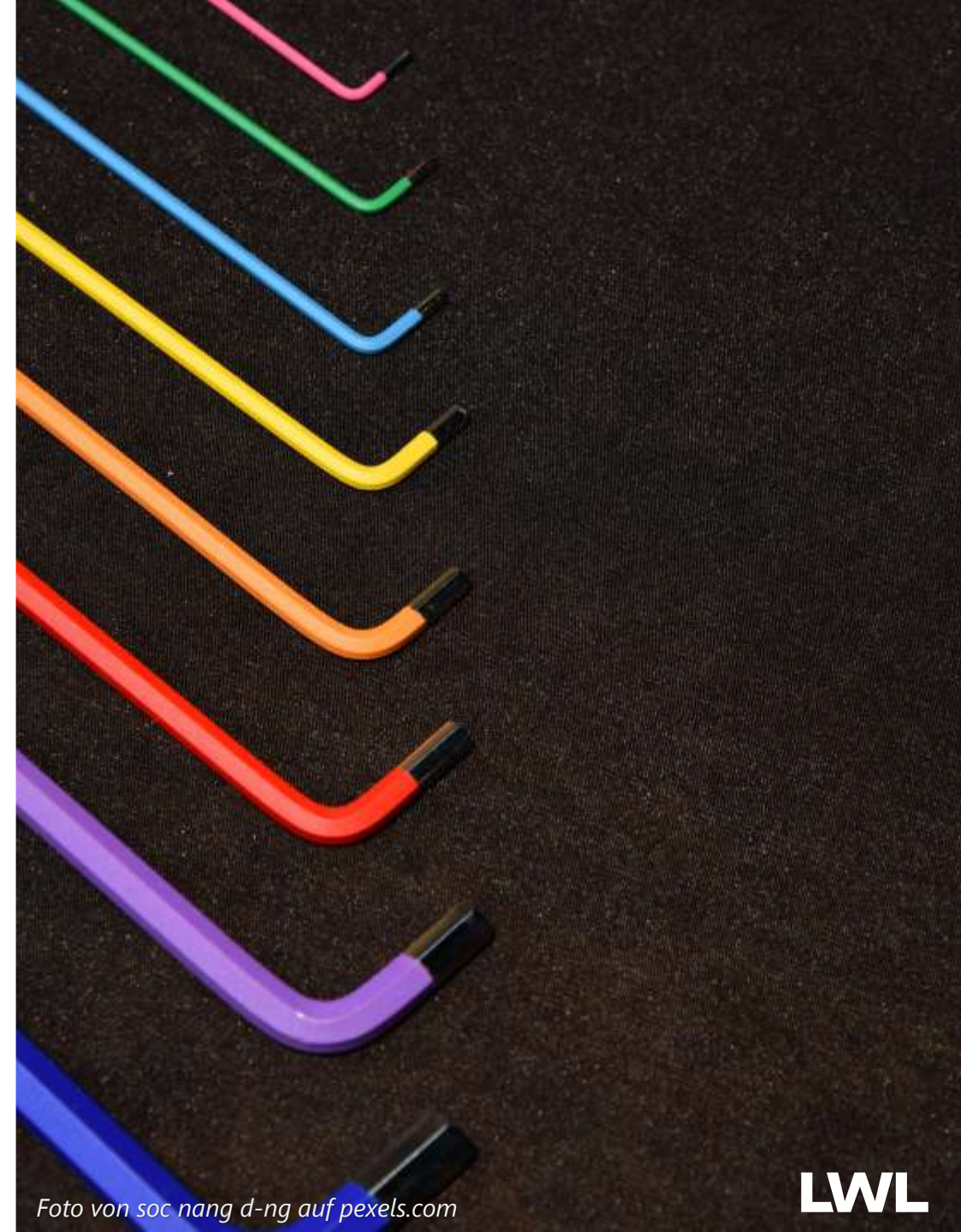
Mitarbeitende

- Misstrauisch sein
- Immer Rückfragen ☎️



Drei Dinge zum Mitnehmen

1. Ich bin verantwortlich dafür, dass Informationen in meinem Bereich angemessen geschützt werden.
2. Sicherheit entsteht durch Regeln – aber vor allem durch Verhalten.
3. Bei einem Vorfall gilt: lieber einmal zu früh melden als einmal zu spät.



Landschaftsverband Westfalen-Lippe (LWL)

Warendorfer Str. 22
48145 Münster
Tel.: 0251 591-5186
informationssicherheit@lwl.org

intranet.itz.lwl.org/de/042/informationssicherheit/

LWL

Für die Menschen.
Für Westfalen-Lippe.

