



PROJEKTARBEIT



CYBER SECURITY ADVISOR

23.01.2025

ÜBER MICH

Schon lange in der IT unterwegs und dank meiner Weiterbildung jetzt auch im Schutz der Systeme bestens gerüstet. Denn IT ohne Sicherheit ist wie ein Auto ohne Sicherheitsgurt – es läuft, bis es kracht.

In dieser Präsentation geht es um Speichermedien, die Folgen eines nachlässigen Umgangs und um die Korrektur durch eine Richtlinie.



AGENDA

1. Das Unternehmen – TransLingua GmbH
Einblicke in unsere Mission und Herausforderungen

2. Der Vorfall, der uns die Augen öffnete
Was geschah und warum mussten wir handeln?

3. Die identifizierten Probleme
*Daten, die im Dark Web landen.
USB-Sticks ohne Regeln.
Sensible Infos im Altpapier.*

4. Klassifizierung und Umgang mit Wechselspeichermedien
Schritt für Schritt zu mehr Sicherheit

5. Kontrolle der internen, externen und papierbasierten Medien
So schützen wir, was wichtig ist

6. Kontinuität der Sicherheit
Sicherheit ist ein Prozess, keine einmalige Aufgabe

7. Fragen?

Projektarbeit IHK Cyber Security Advisor



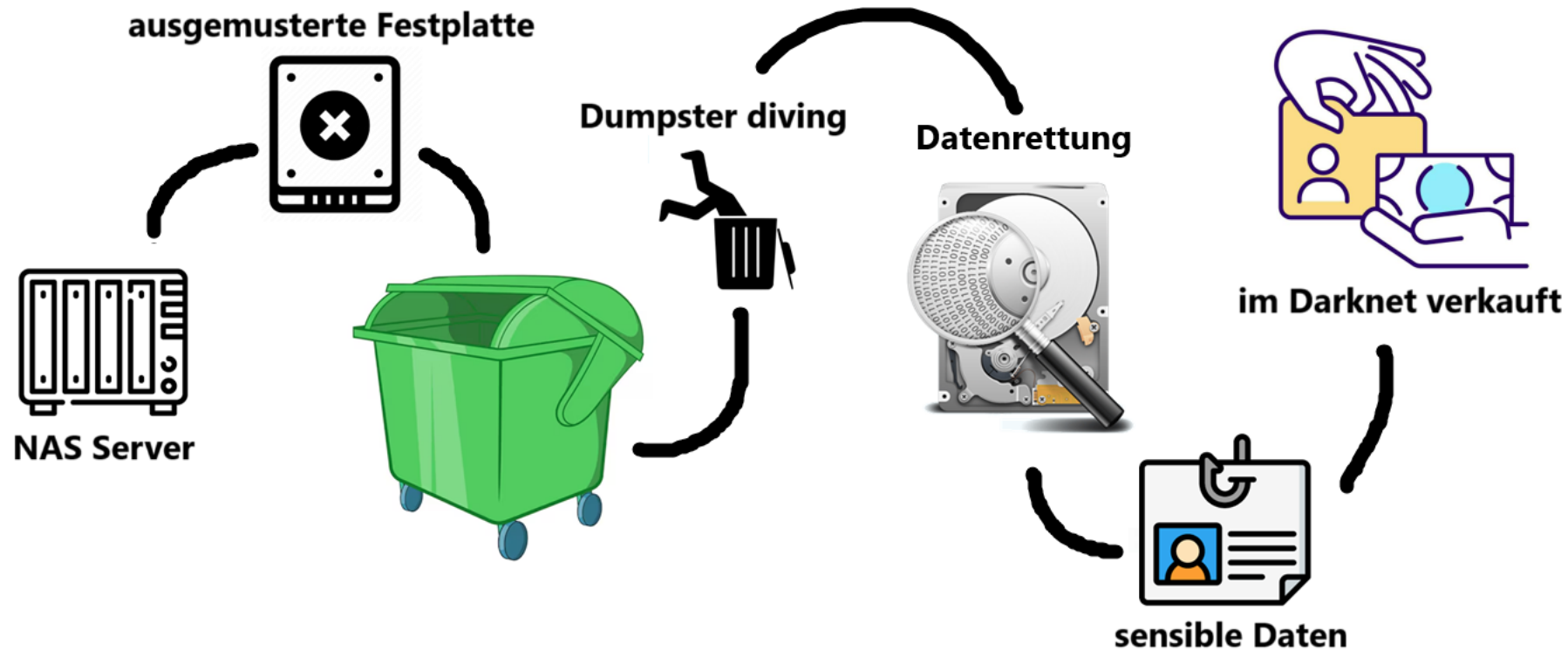
TransLingua GmbH

Durch Worte verbunden

Projektarbeit IHK Cyber Security Advisor



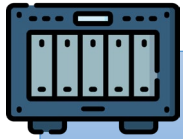
WIE EINE NACHLÄSSIGE HANDLUNG DIE FIRMA TRANSFORMIERTE



Internes Audit hat folgende Schwachstellen aufgedeckt:

- unsachgemäße Entsorgung interner Server-Festplatten,
- unkontrollierte Schnittstellen, die externe Datenträger zulassen (z. B. USB-Sticks),
- unzureichende Aktenvernichtung in Papierform.

SPEICHERMEDIEN DEFINIEREN UND PROBLEME LÖSEN



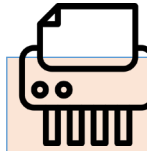
Interne Datenträger

Speichermedien, die fest in IT-Systemen verbaut oder direkt Teil der Geräte sind, wie Festplatten (HDD, SSD) in Servern, Laptops, Tablets, Multifunktionsgeräten oder Druckern.



Externe Datenträger

Speichermedien, die physisch angeschlossen, entfernt oder transportiert werden können, wie USB-Sticks, externe Festplatten, SD-Karten, CDs, DVDs, Blu-rays oder ähnliche tragbare Medien.



Papier Datenträger

Nicht-digitale Medien, die Informationen in physischer Form enthalten, wie Papierdokumente, Ausdrücke oder analoge Datenträger.



Wiederverwendbare Datenträger wipen, um vorherige Daten irreversibel zu löschen.

Ausgemusterte Datenträger sicher durch einen zertifizierten Drittanbieter entsorgen.



Lösungen

Windows Server-Gruppenrichtlinien (GPOs) konfigurieren, um das Anschließen externer Datenträger zu unterbinden.

Zwangsverschlüsselung autorisierter Datenträger.



Sichere Aktenvernichtung leicht zugänglich machen, ab Sicherheitsstufe P-4.

Standardisierte Prozesse zur Aktenvernichtung werden durch den Datenschutzbeauftragten überwacht.

KONTINUITÄT DER SICHERHEIT

Überwachung, Audits, Schulungen und der Umgang mit Verstößen.

Überwachung:

Zentrale Gruppenrichtlinien (GPOs)
& Protokollierung der Zugriffe

Audits:

Intern und extern

Schulungen:

Awareness-Programme &
Onboarding

Verstöße:

Dokumentation &
disziplinarische Maßnahmen

Maßnahme	Verantwortlich	Häufigkeit
Dokumentation & Maßnahmen bei Verstößen	IT-Abteilung Personalabteilung	Bei Vorfällen
<ul style="list-style-type: none">• Interner Verschlüsselungsstatus• Externe Zwangsverschlüsselung• Zugriffsprotokolle	IT-Abteilung	Monatlich
<ul style="list-style-type: none">• Status der Wechselspeichermedien• Identifikation & Klassifizierung• Interne Verschlüsselung• Schnittstellenblockierung• Aktenvernichtung	IT-Abteilung Datenschutzbeauftragter	Vierteljährlich
<ul style="list-style-type: none">• Interne Audits	IT-Abteilung	Halbjährlich
<ul style="list-style-type: none">• Externe Audits• Schulungen & Awareness	Externe Auditoren HR-Abteilung	Jährlich

Alle Maßnahmen erfolgen gemäß den in Deutschland und weltweit anerkannten Standards.

An abstract graphic on the left side of the slide, consisting of several overlapping, tilted rectangular outlines in white. These lines create a complex, layered geometric pattern that extends from the top-left towards the center of the frame.

FRAGEN?

Projektarbeit IHK Cyber Security Advisor