M365 SECURITY BEST PRACTICES MIT TENFOLD

HANKE Ernst I 10. April 2024 I Bechtle Austria

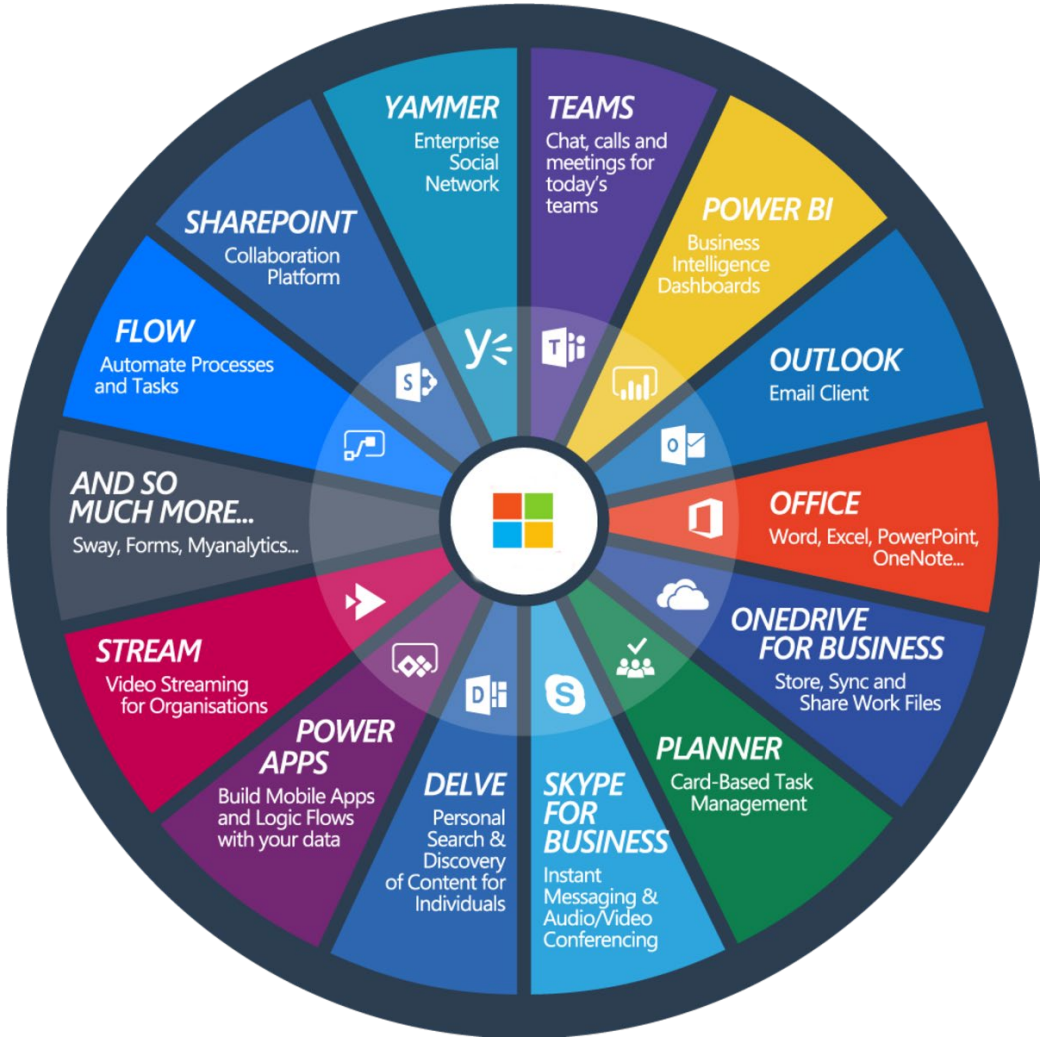
SPEAKER

Hanke Ernst
Team Lead Identity & Access Management
Bechtle Austria

- Verantwortlich für Identity & Access Management Beratung
- Azure Solutions Architect

E-Mail: ernst.hanke@bechtle.com

M365 Überblick



NUTZEN & RISIKO VON MICROSOFT TEAMS

tenfold

+ VORTEILE +

+ Einfache Kommunikation via Nachrichten
+ Konferenzen mit Audio- und Video-Optionen
+ Teilen und Bearbeiten von gemeinsamen Daten
+ Fachbenutzer bestimmen selbst, wer Zugriff auf Daten hat

! GEFAHREN !

! Keiner kann noch sagen, wer auf welche Daten Zugriff hat

! Eingerichtete Zugriffe bleiben für immer bestehen

! Sensible Daten werden sowohl intern als auch extern exponiert

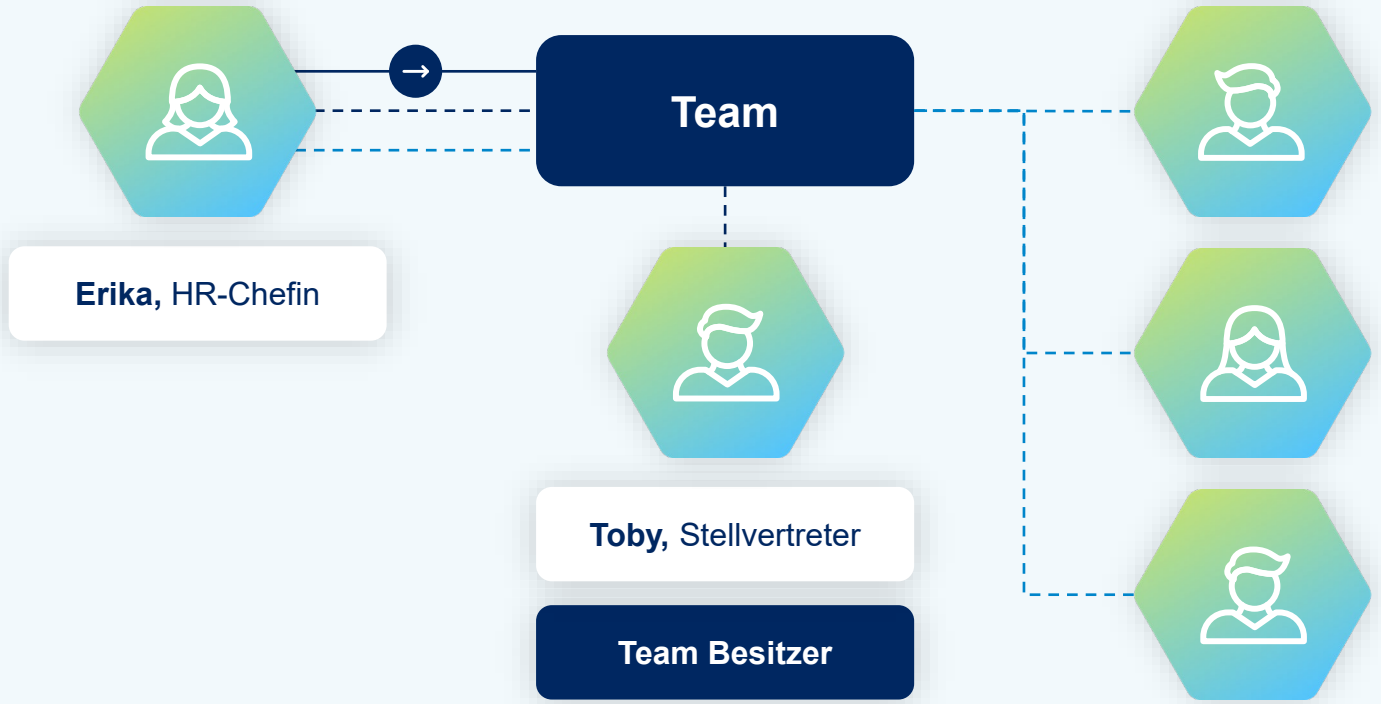
! Haftungsrisiken durch Nichteinhalten wichtiger Compliance-Vorschriften

DAS TEAM – DIE PERSONALABTEILUNG

tenfold

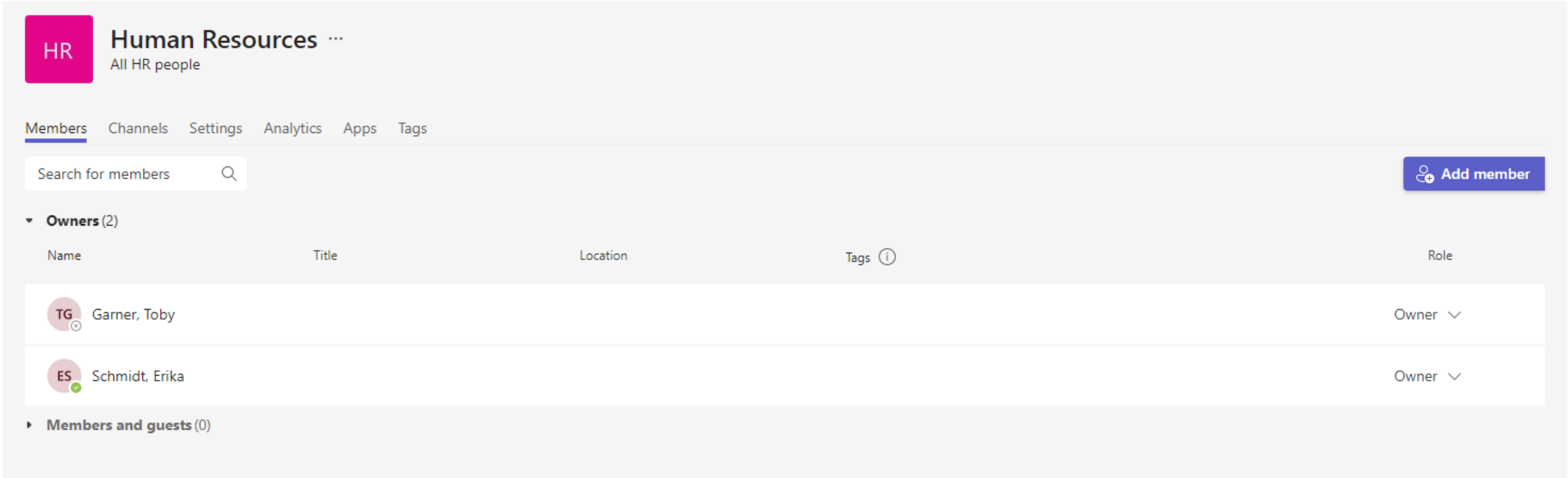
SCHRITT 1: TEAM ANLEGEN

- Erika, die HR-Chefin legt das Team an
- Sie ernennt auch den Stellvertreter Toby zum Besitzer
- Danach lädt sie alle Mitarbeiter aus der Abteilung ein

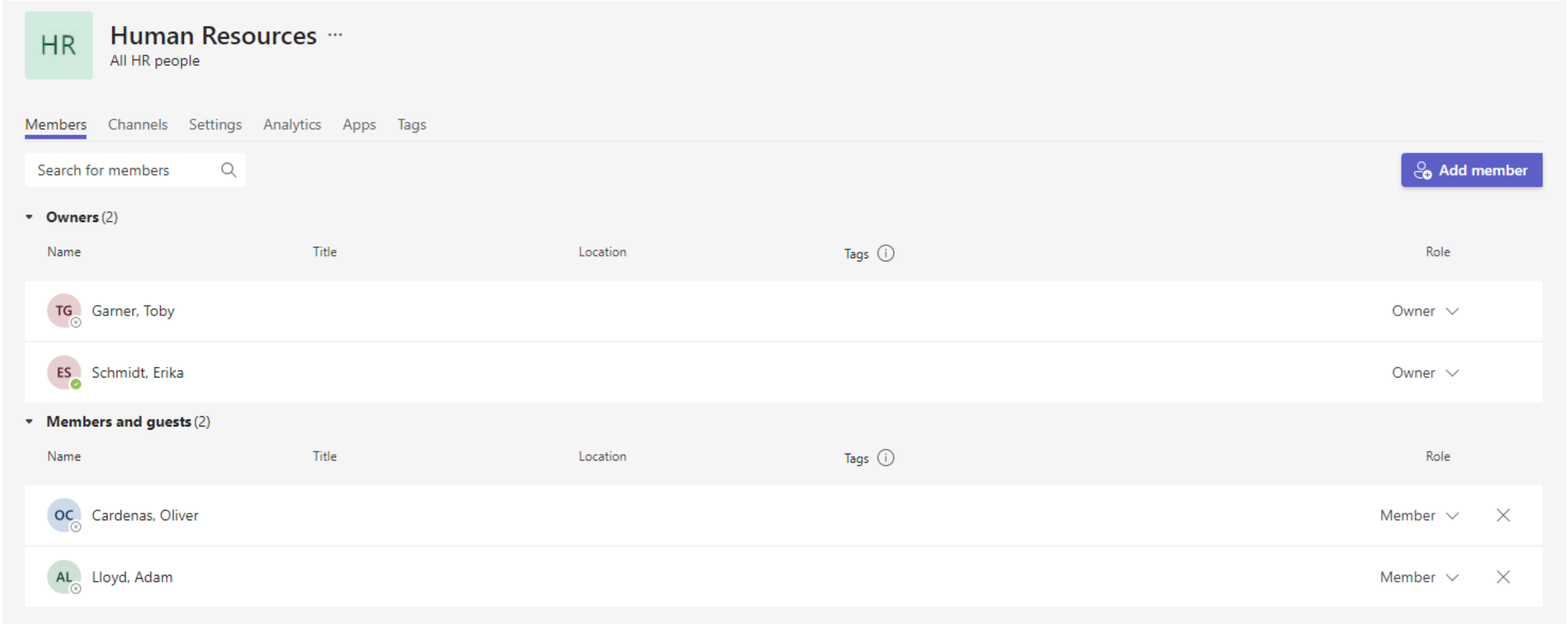


TOBY IST EBENFALLS TEAM-OWNER

tenfold

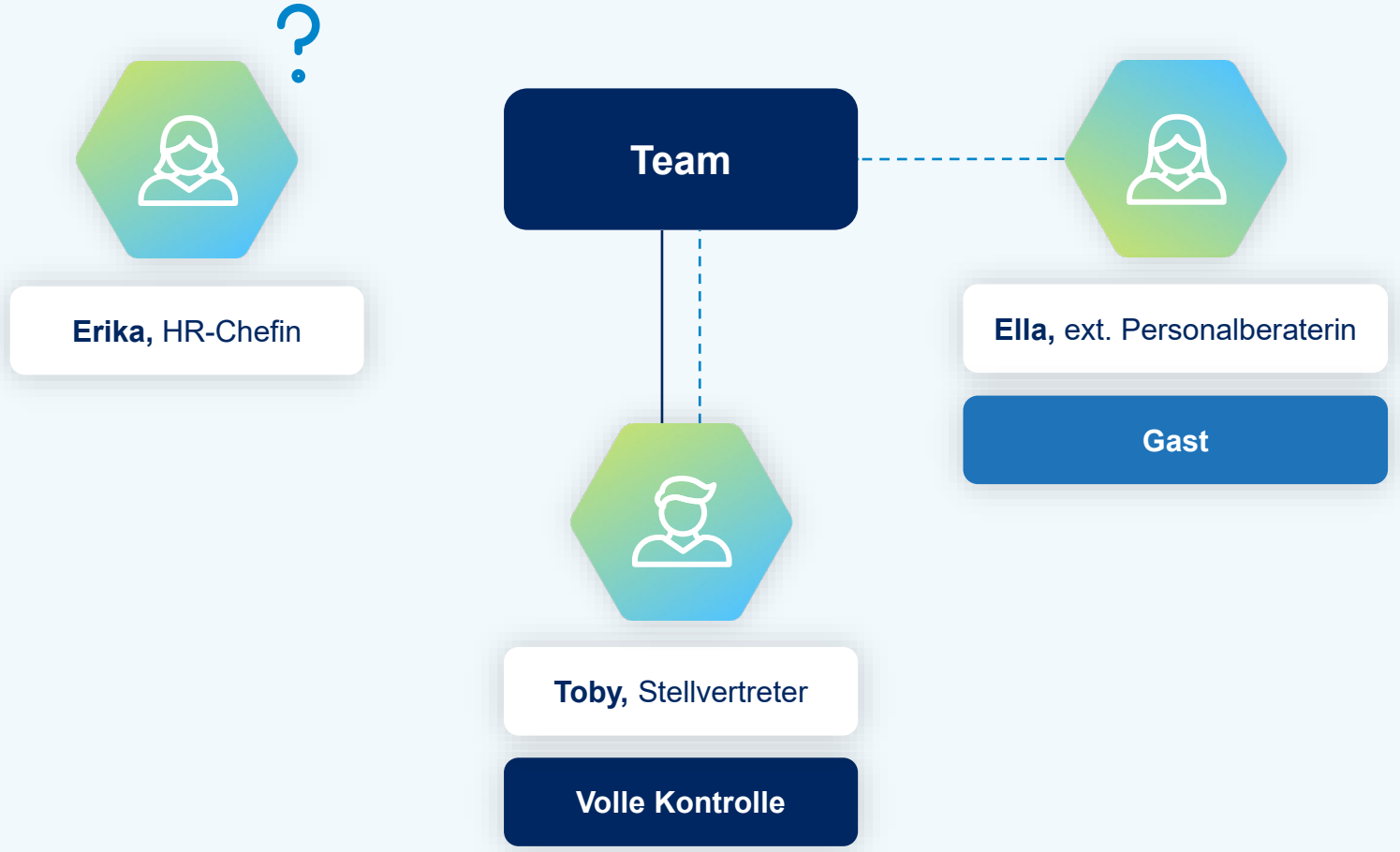


DIE MITGLIEDER SIND HINZUGEFÜGT

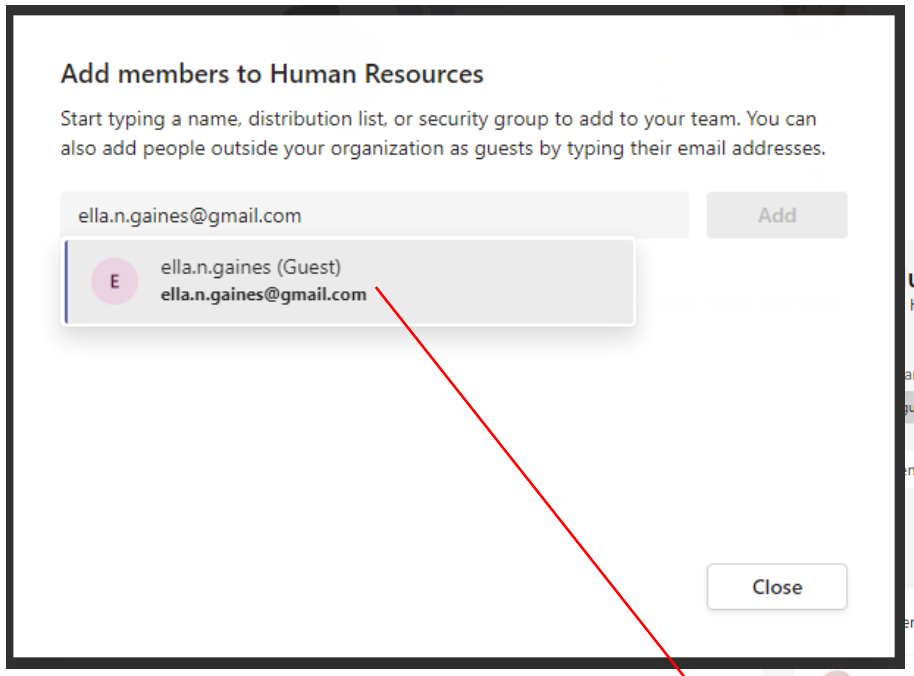


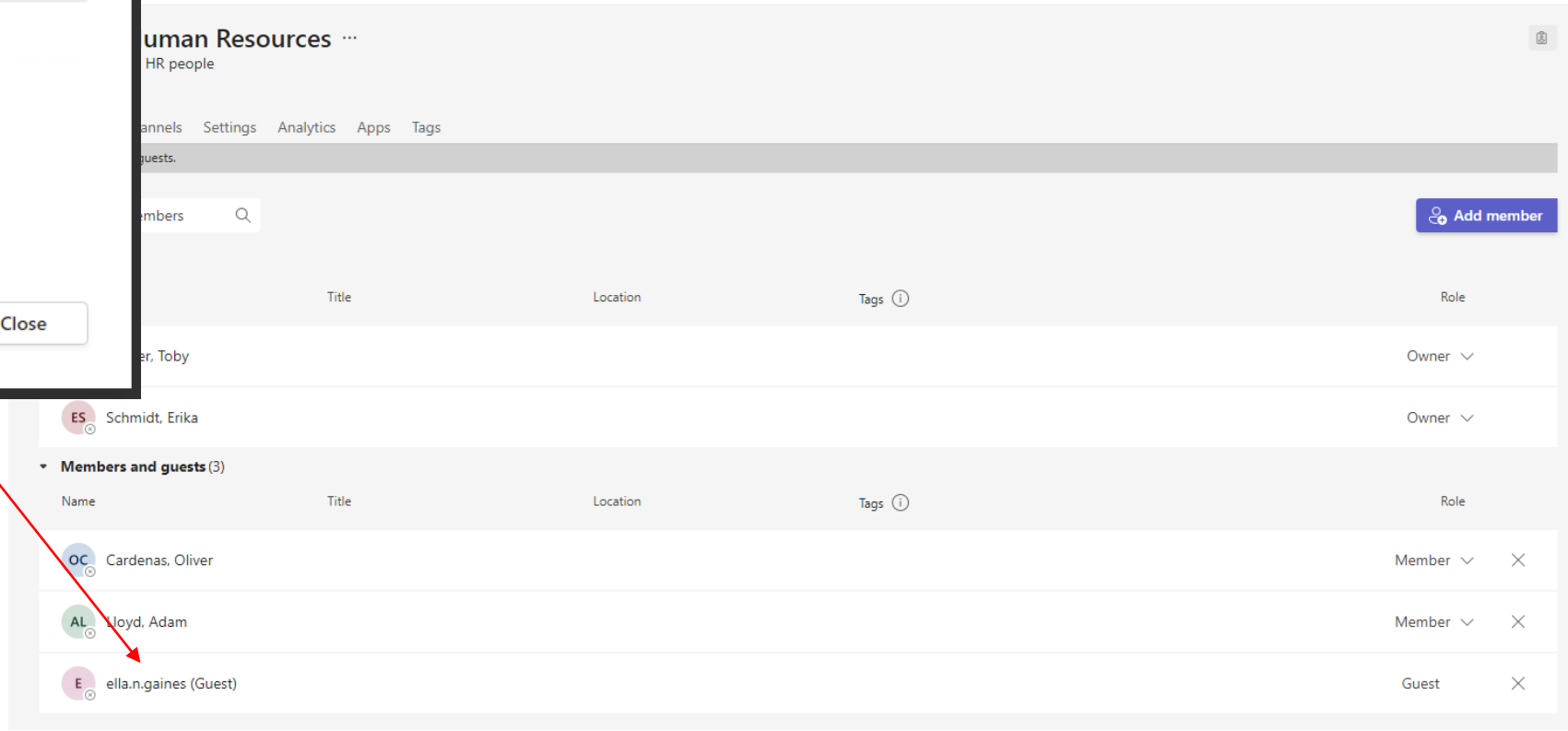
SCHRITT 2: TOBY ERWEITERT DAS TEAM

- Toby, der Stellvertreter, hat auch volle Kontrolle über das Team
- Er lädt die externe Personalberaterin Ella als Gast in das Team ein
- Erika als Verantwortliche bekommt davon nichts mit



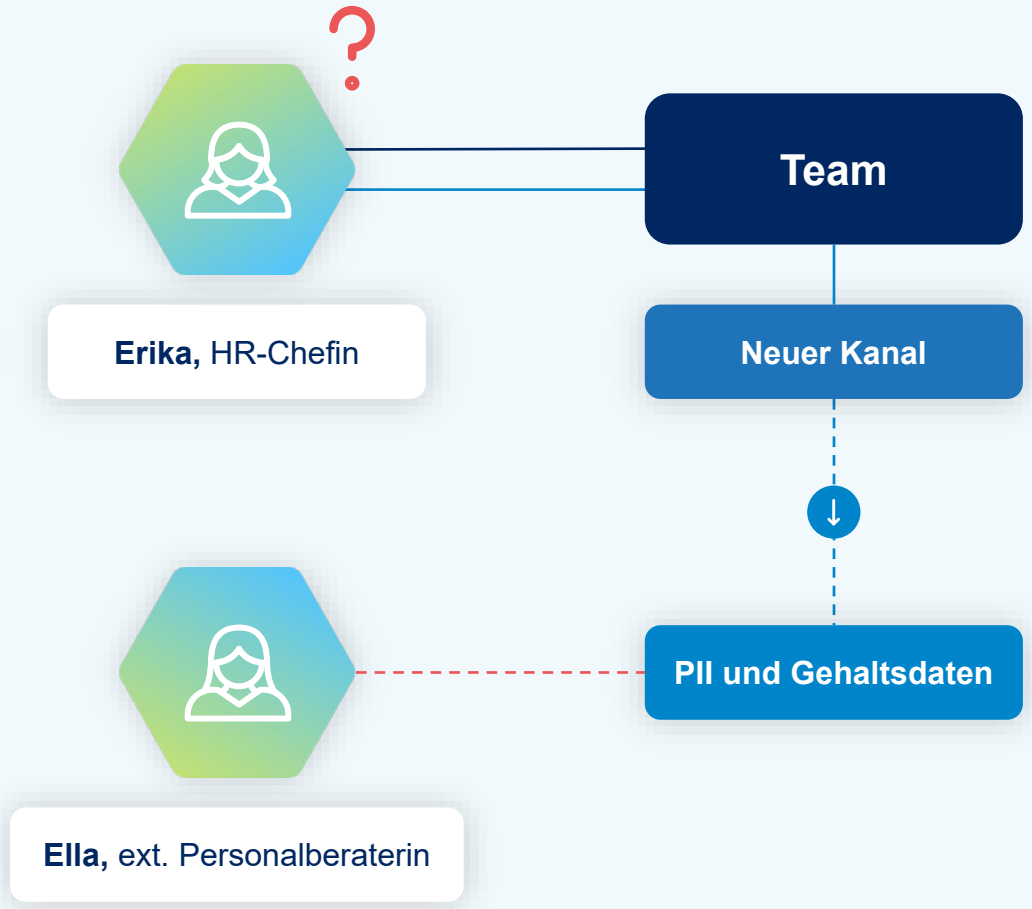
GASTBENUTZER WIRD HINZUGEFÜGT





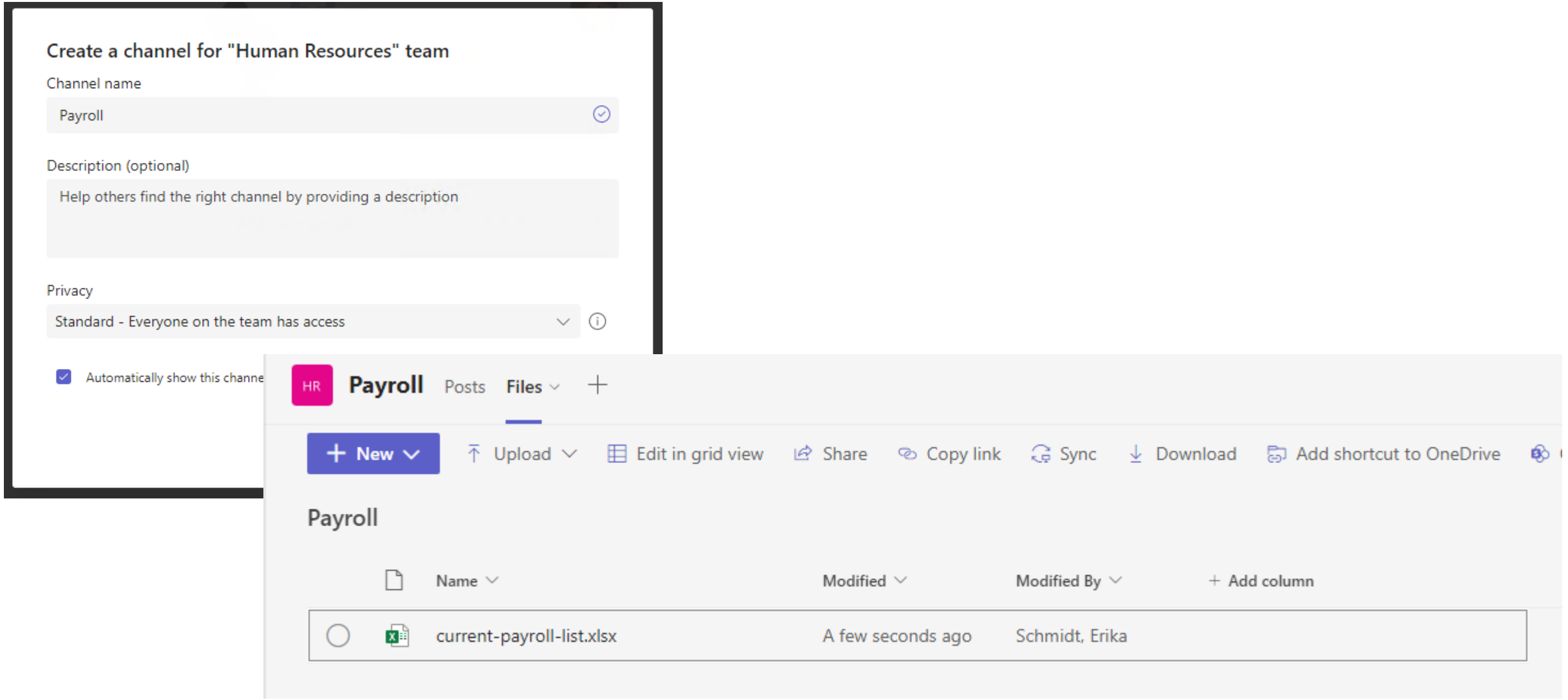
SCHRITT 3: ERIKA TEILT SENSIBLE DATEN

- Erika erzeugt einen neuen Kanal innerhalb des Teams
- Darin teilt sie eine sensible Liste mit PII und Gehaltsdaten
- Dass Ella auf diese Daten Zugriff erhält, weiß Erika nicht

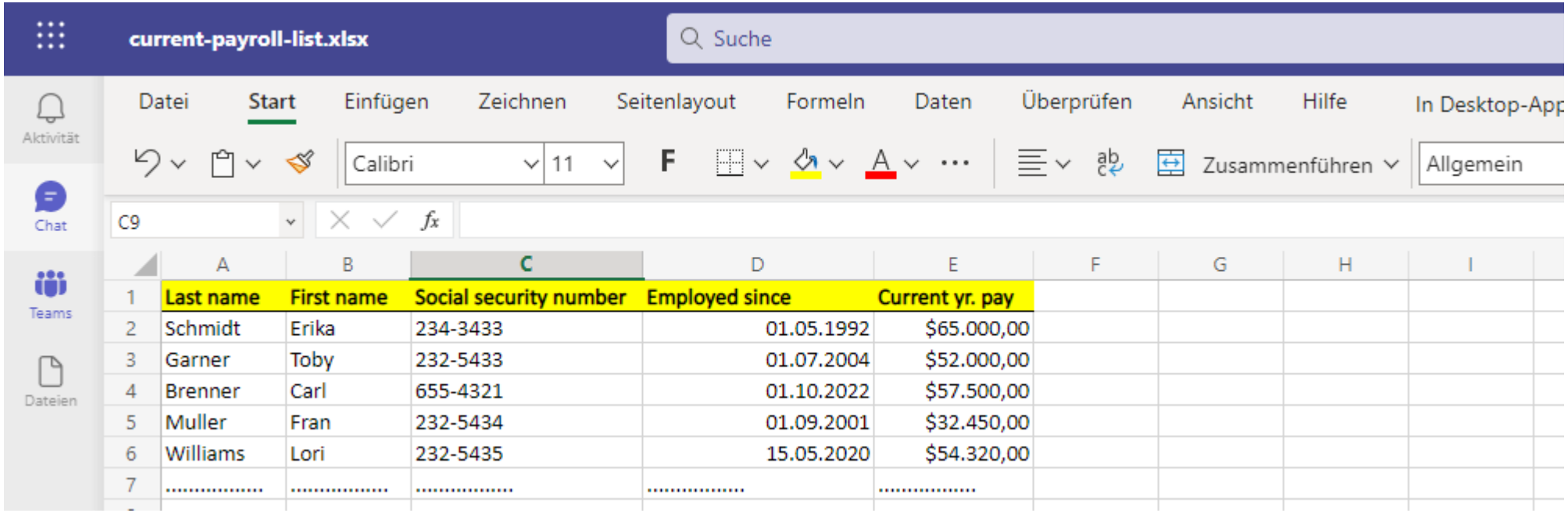


TEILEN DER SENSITIVEN DATEN IM KANAL

tenfold



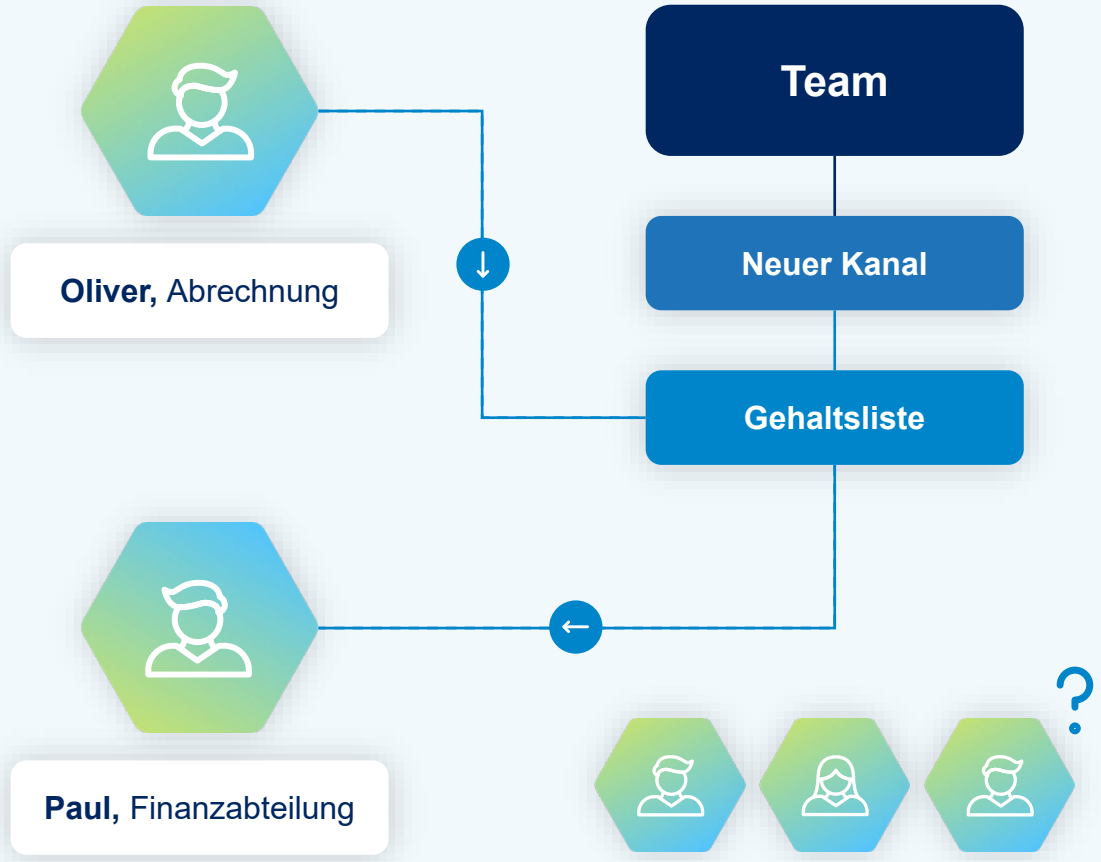
GASTBENUTZER HAT UNBESCHRÄNKT ZUGRIFF



	A	B	C	D	E	F	G	H	I
1	Last name	First name	Social security number	Employed since	Current yr. pay				
2	Schmidt	Erika	234-3433	01.05.1992	$65.000,00				
3	Garner	Toby	232-5433	01.07.2004	$52.000,00				
4	Brenner	Carl	655-4321	01.10.2022	$57.500,00				
5	Muller	Fran	232-5434	01.09.2001	$32.450,00				
6	Williams	Lori	232-5435	15.05.2020	$54.320,00				
7	.....	.....	.....	.....	.....				

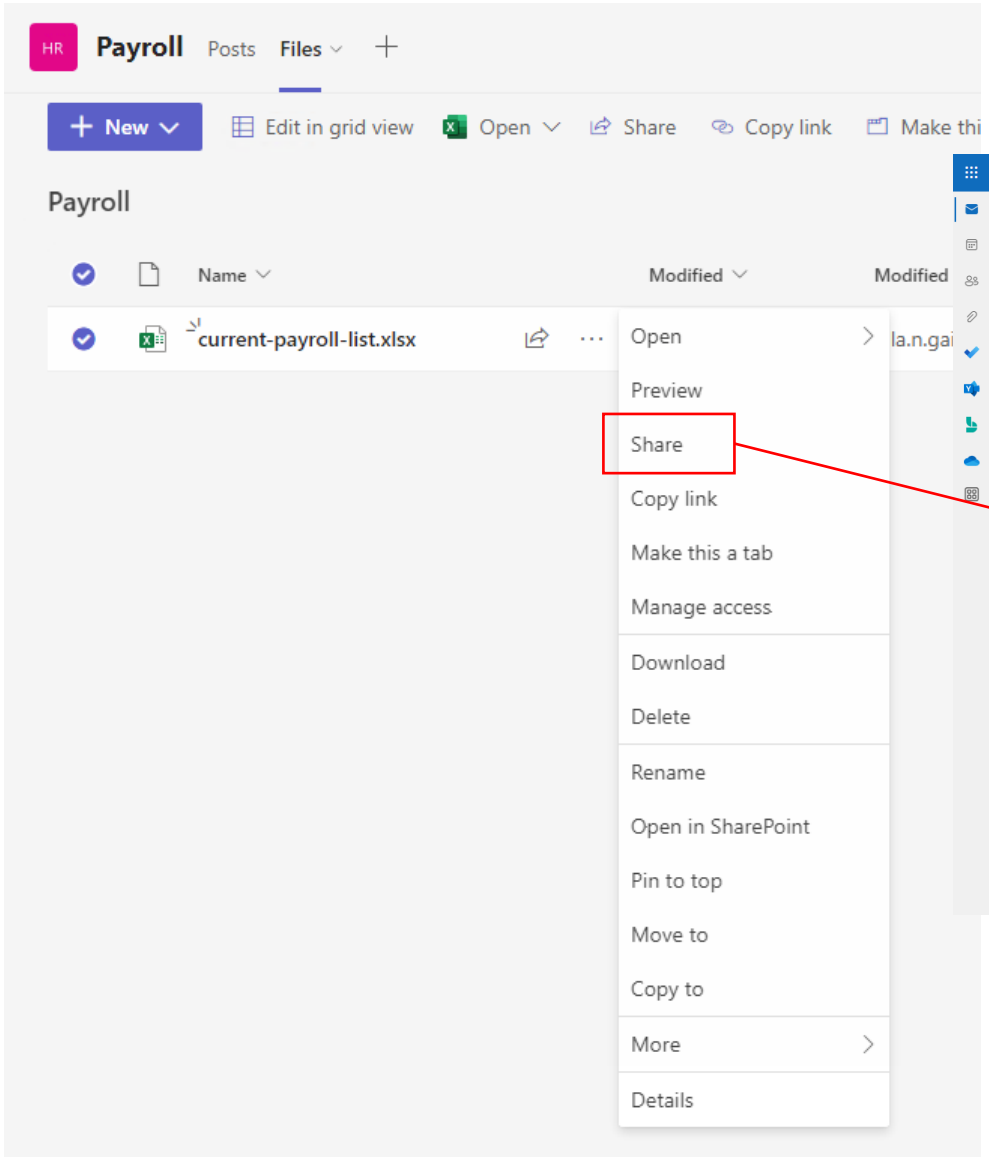
SCHRITT 4: DATEN WERDEN VIA LINK GETEILT

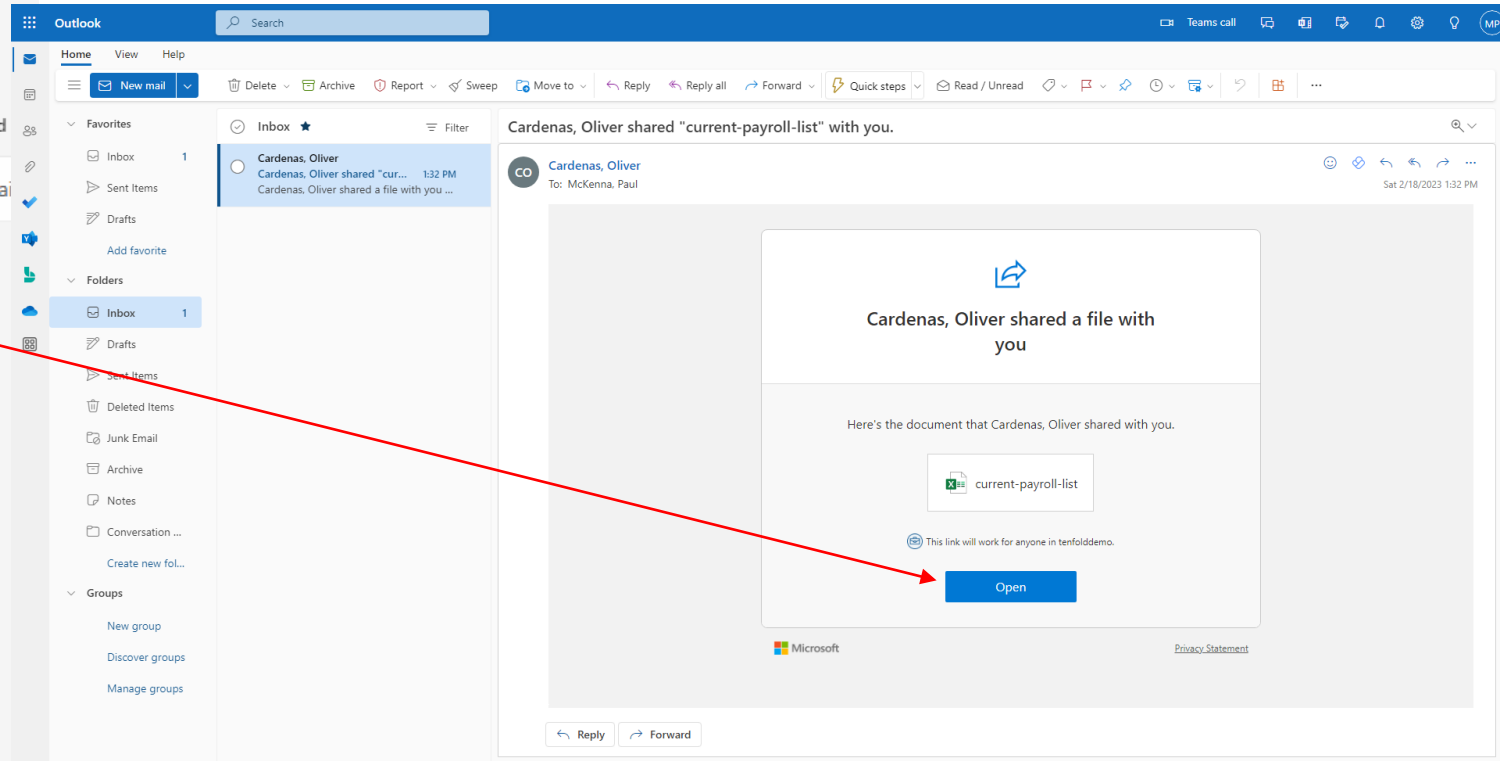
- Oliver aus der Personalabteilung ist verantwortlich für die Abrechnung
- Er möchte die Gehaltsliste mit Paul aus der Finanzabteilung teilen
- Daher erstellt er einen Sharing-Link für die Excel-Datei
- Außer Oliver weiß niemand, dass jetzt auch Paul Zugriff hat



JEDER KANN ZUSÄTZLICHEN ZUGRIFF VERGEBEN

tenfold

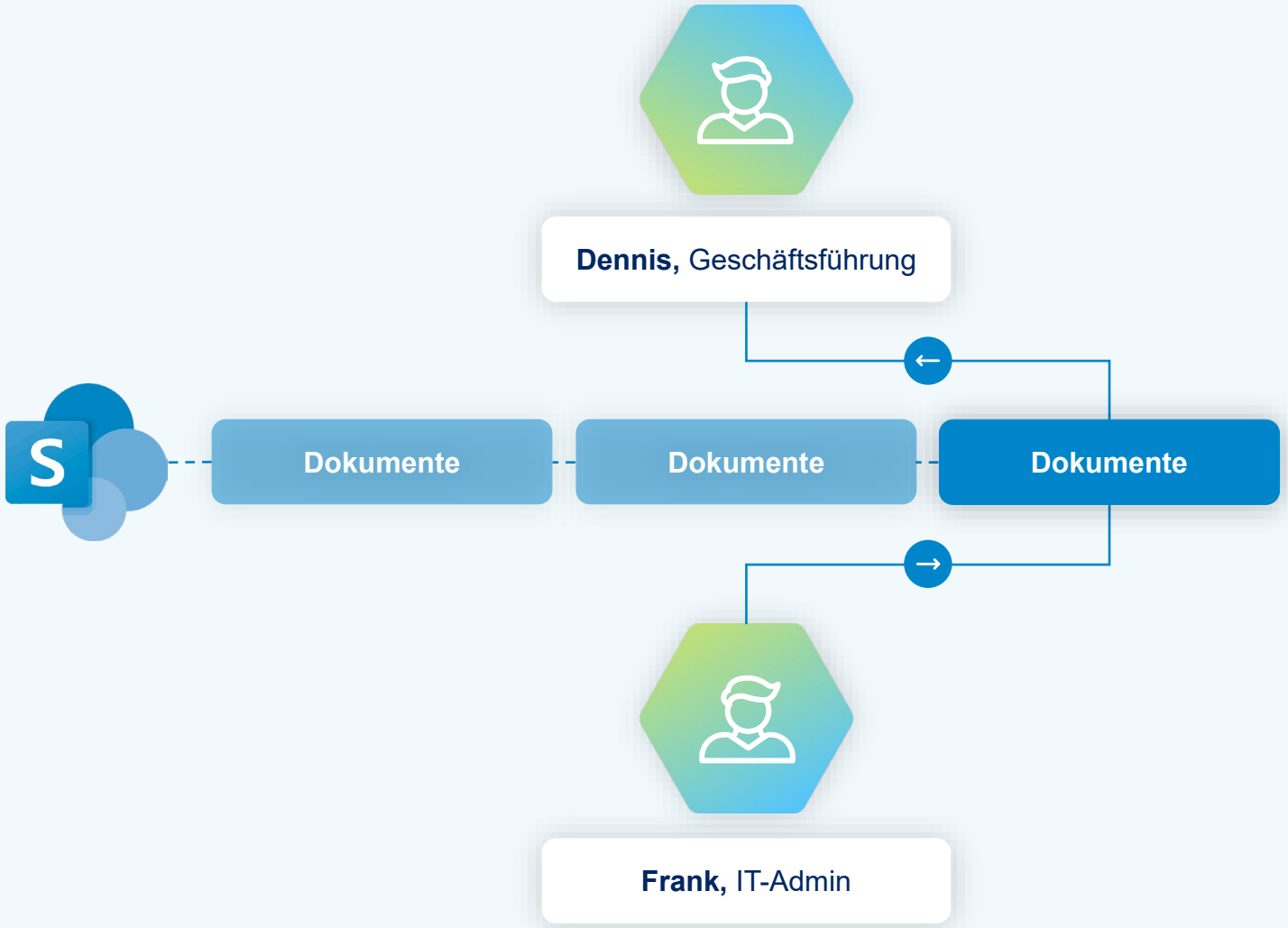




tenfold-security.com

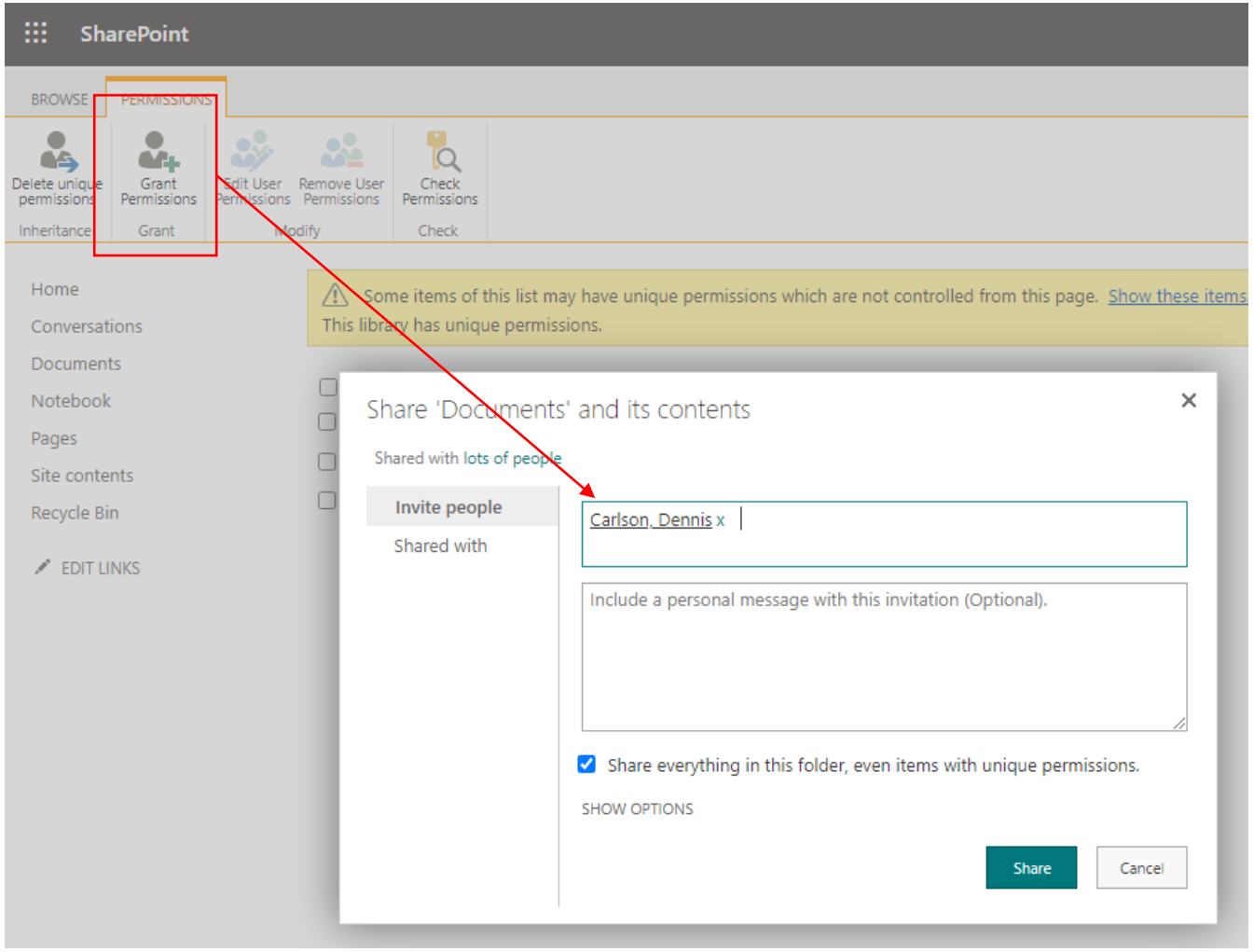
SCHRITT 5: DIREKT IN SHAREPOINT

- Der IT-Admin, Frank, hat den Auftrag erhalten, Dennis aus der Geschäftsführung Berechtigungen zu erteilen.
- Dazu navigiert er auf die entsprechende Dokumentenbibliothek in SharePoint und setzt die Rechte dort direkt



BERECHTIGUNGEN DIREKT IN SHAREPOINT

tenfold

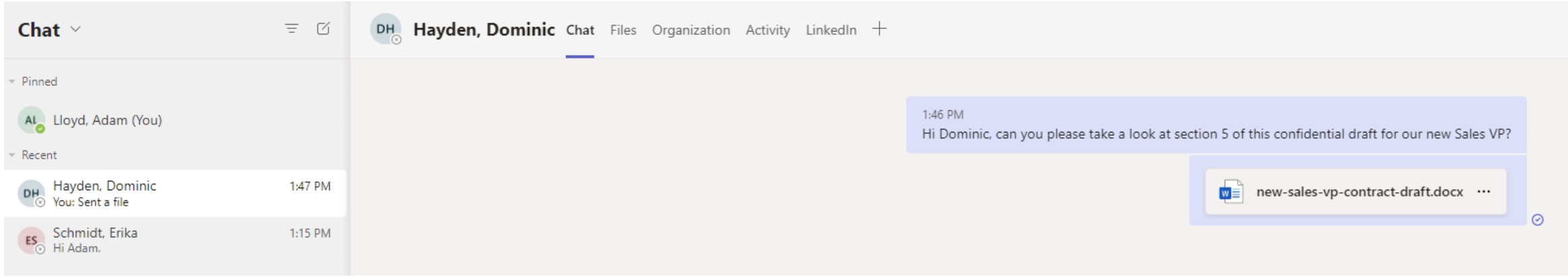


SCHRITT 6: ADAM TEILT DATEN IN EINEM CHAT

- Adam, zuständige für die Dienstverträge, hat rechtliche Fragen
- Eine wichtige Führungskraft soll kurzfristig ersetzt werden
- Er teilt einen Vertragsentwurf mit Dominic aus der Rechtsabteilung

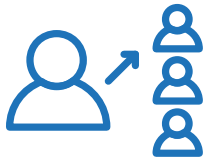
NEUE RECHTE PER DRAG & DROP

tenfold



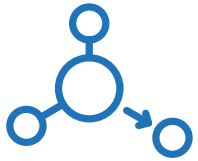
DIE 6 MÖGLICHKEITEN DES TEILENS

tenfold



Besitzer eines Teams können weitere Besitzer bestimmen

Diese können das Team dann ebenfalls vollständig steuern.



Mitglieder können neue Kanäle in Teams anlegen

Diese können öffentlich oder privat sein.

Externe Personen können als Gäste eingeladen werden

Sie erhalten damit ebenfalls Zugriff auf alle Daten, die im Team geteilt sind.

Daten können außerhalb des Teams geteilt werden

Über Sharing Links können Daten sowohl innerhalb des Unternehmens, als auch extern geteilt werden.

Direkte SharePoint-Berechtigungen

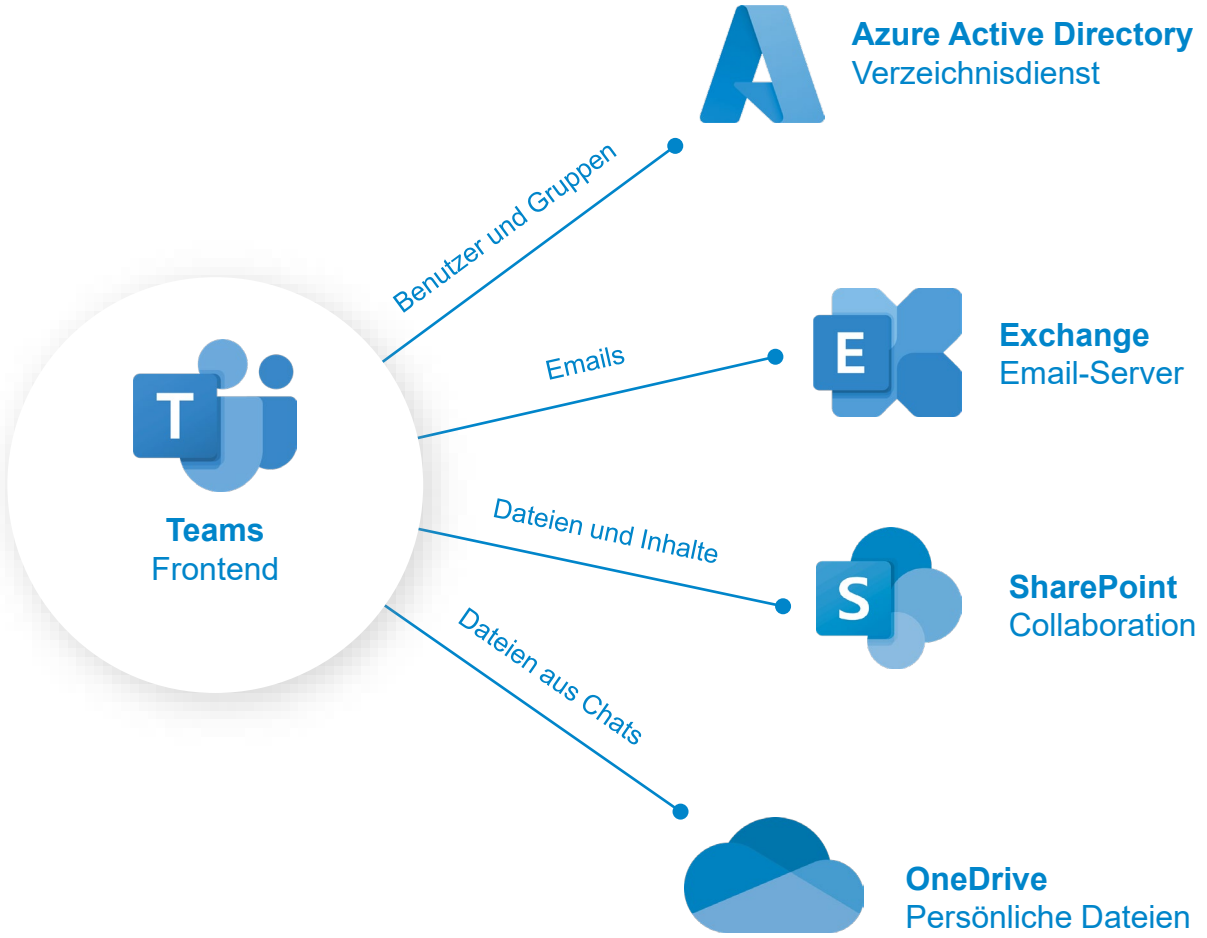
Berechtigungen können auch ohne Nutzung der Gruppen direkt in SharePoint auf der Dokumentenbibliothek vergeben werden

Benutzer können Daten in Chats teilen

Dass die Daten beim Löschen des Chats nach wie vor geteilt bleiben, ist (fast) keinem Benutzer bewusst.

WAS PASSIERT IM HINTERGRUND

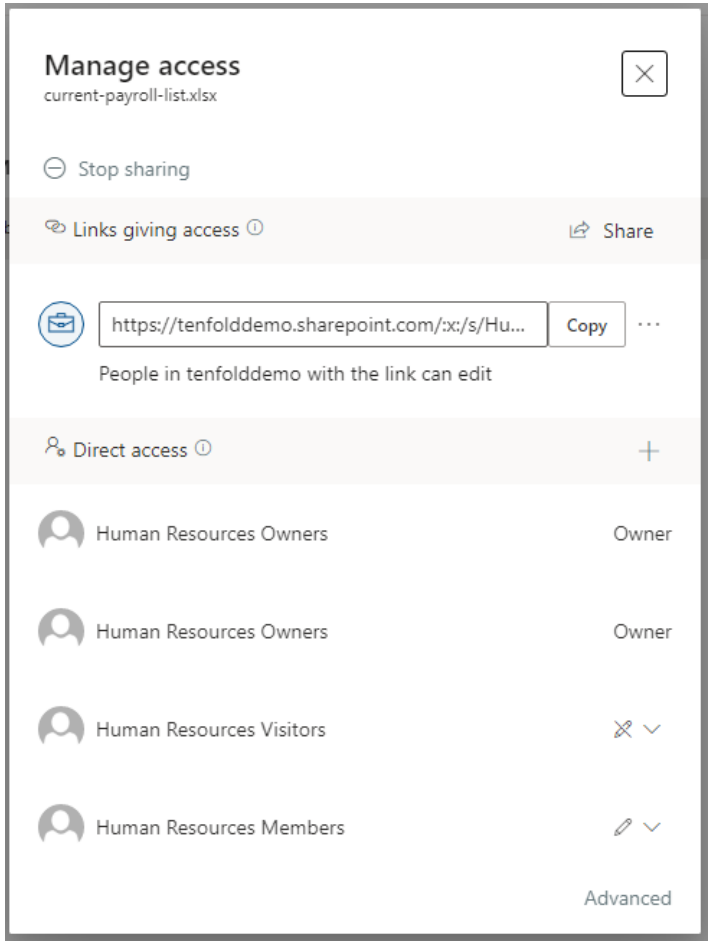
- Teams ist ein Frontend
- Erleichterung für Endanwender
- Daten kommen/landen anderswo:
  - Azure Active Directory
  - Exchange Online
  - SharePoint Online
  - OneDrive



WO SIND FREIGABEN UND BERECHTIGUNGEN ZU SEHEN?

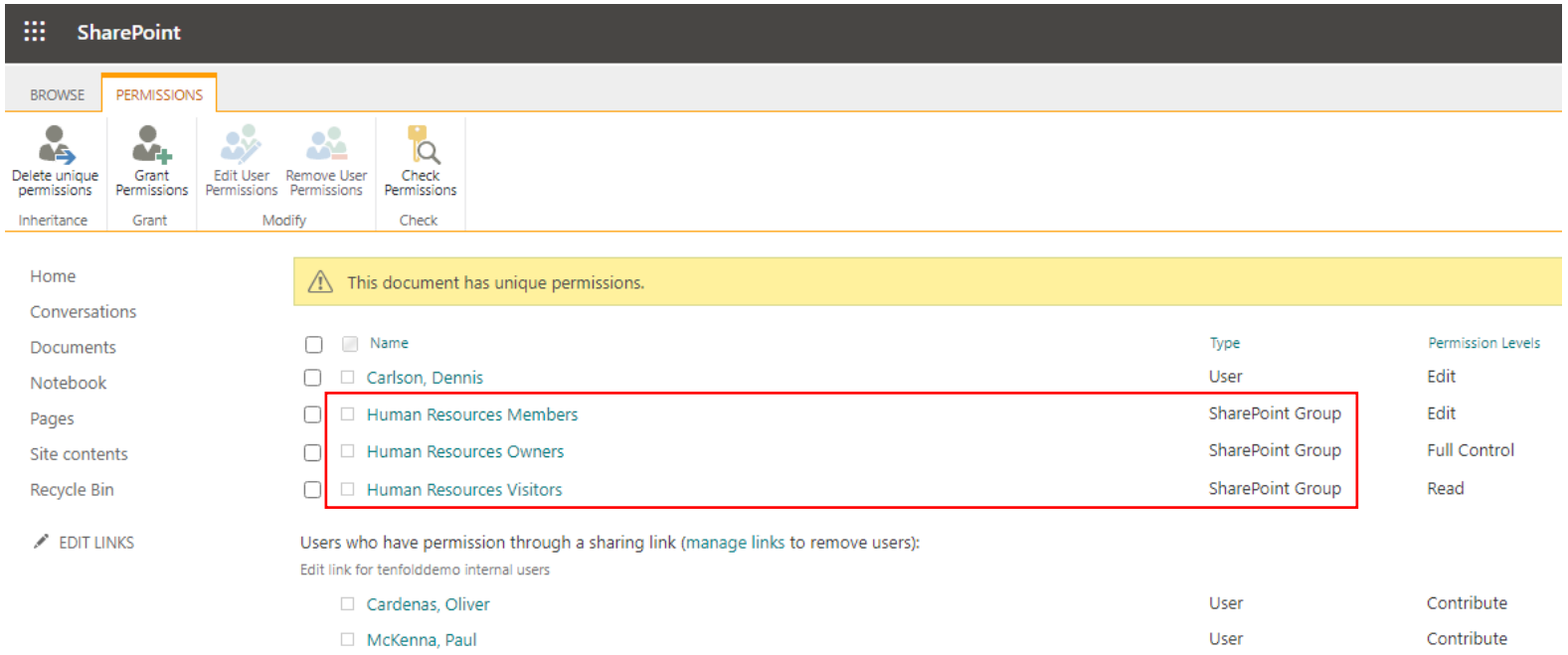
WO SIND FREIGABEN UND BERECHTIGUNGEN ZU SEHEN?

- In Teams und SharePoint kann man nur die berechtigten SharePoint-Gruppen sehen
- Es wird nicht angezeigt, welche Benutzer Mitglied der jeweiligen Gruppen sind (und damit Zugriffsrechte haben).



WO SIND FREIGABEN UND BERECHTIGUNGEN ZU SEHEN?

- Selbst im „Erweiterten Modus“ in SharePoint werden lediglich die Gruppen angezeigt.

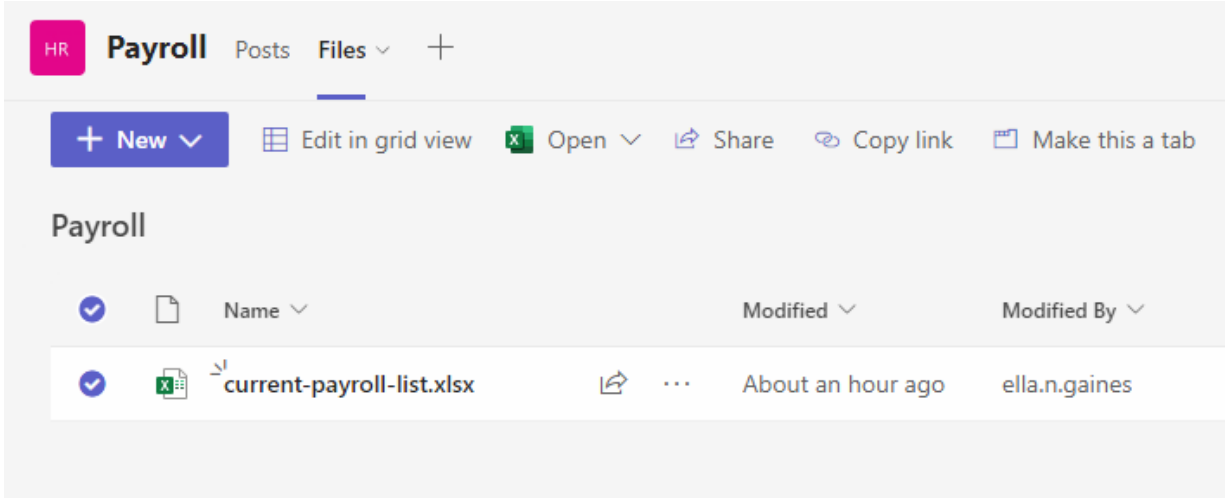


WO SIND FREIGABEN UND BERECHTIGUNGEN ZU SEHEN?

tenfold

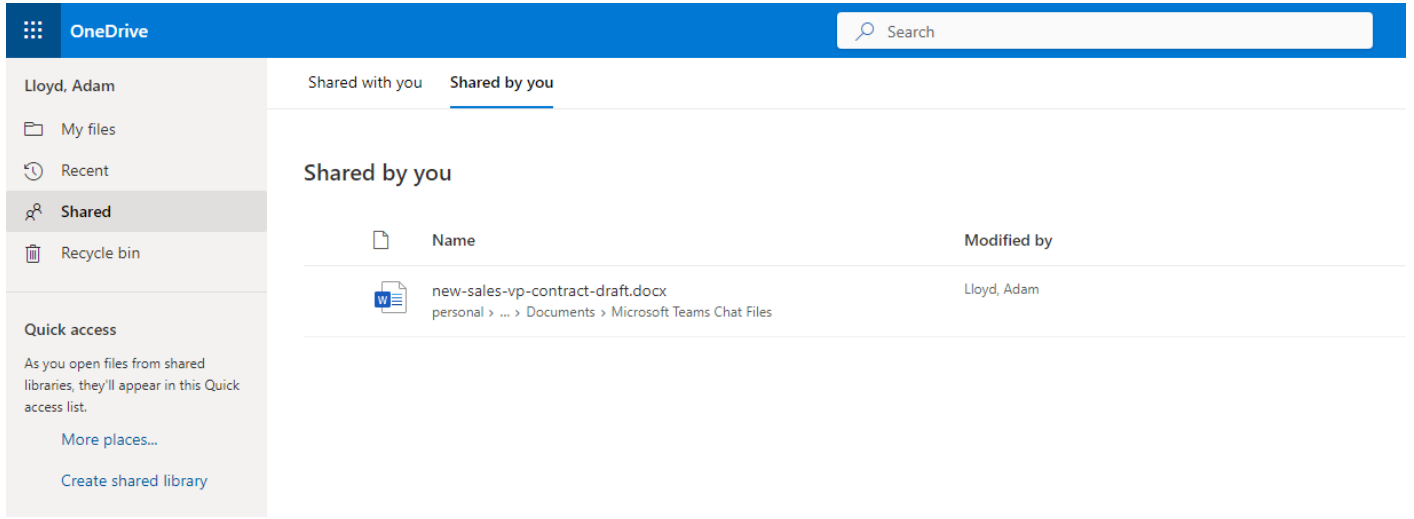
- Nutzt man manuell alle Datenquellen, kann man für einzelne Dateien herausfinden, wer Zugriff hat

- Es gibt allerdings keine Übersicht in Teams oder SharePoint, die alle erteilten Berechtigungen anzeigt.



WO SIND FREIGABEN UND BERECHTIGUNGEN ZU SEHEN?

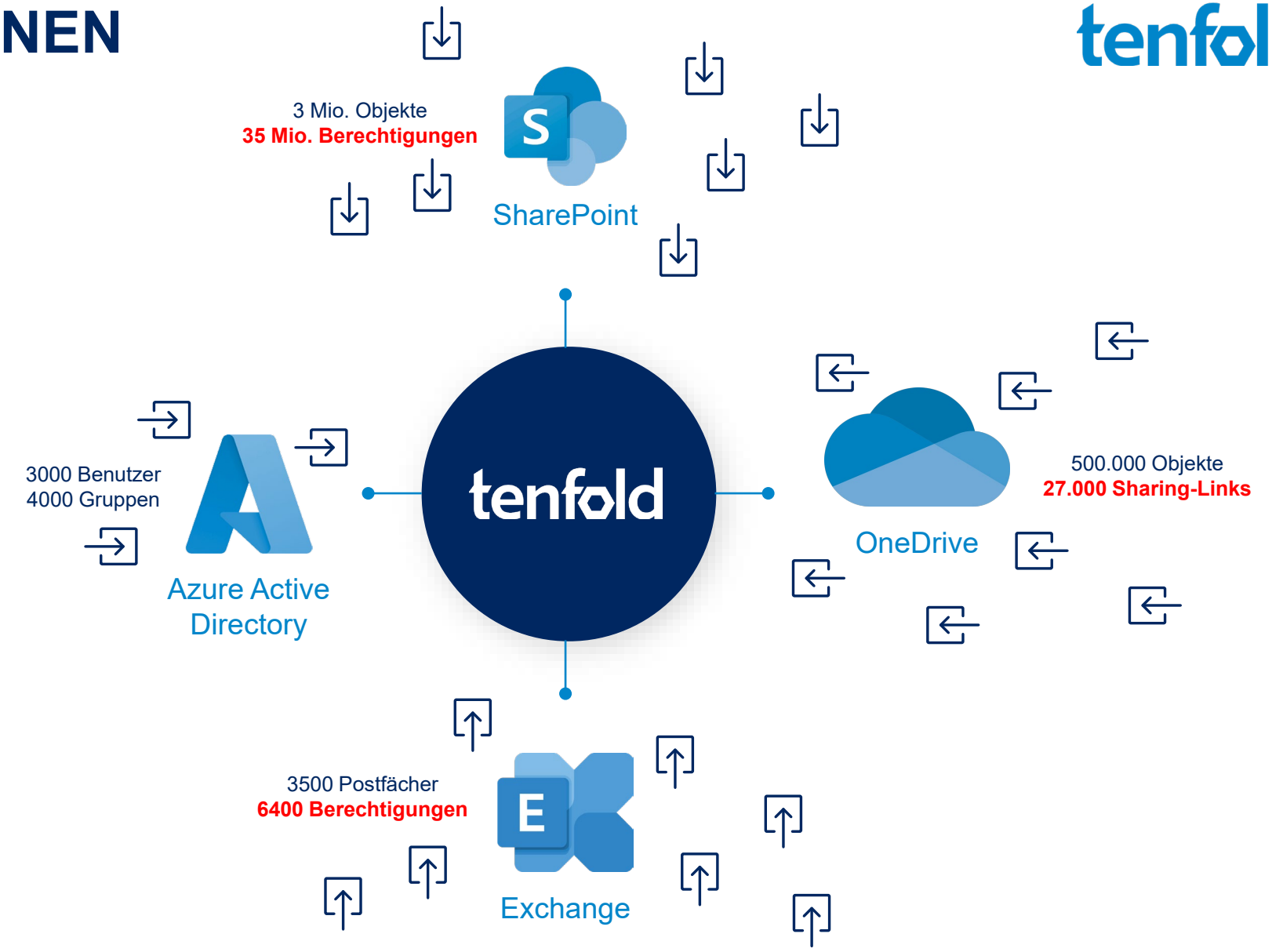
- Bei OneDrive kann nur jeder Benutzer selbst sehen, was er teilt.
- Die Funktion ist allerdings auf der Web-Oberfläche von OneDrive versteckt.



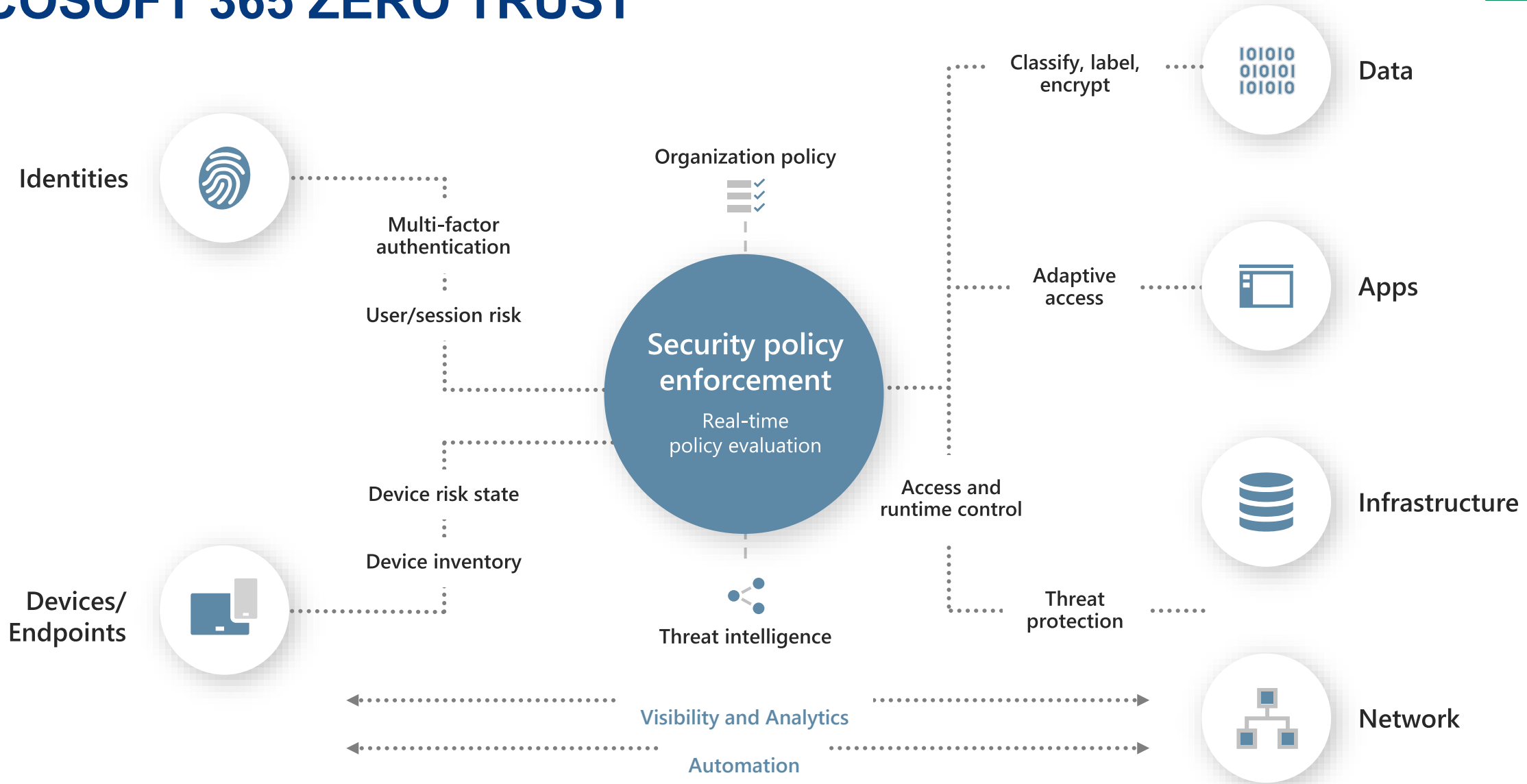
DIE RISIKEN ZUSAMMENGEFASST

GEFAHREN ERKENNEN

- Notwendige Daten werden aus allen Quellen synchronisiert:
  - Azure Active Directory
  - SharePoint Online
  - Exchange Online
  - OneDrive
- In tenfold können sie dann verständlich angezeigt werden



MIRCOSOFT 365 ZERO TRUST



FAZIT

tenfold

- Microsoft 365 ist im Internet exponiert und für jeden erreichbar
- Benutzer verwalten Berechtigungen auf sensible Daten selbst
- Die IT kann parallel selbstverständlich auch Berechtigungen setzen
- Dabei wird sowohl mit internen als auch mit externen Personen geteilt

- Die IT verliert dabei den Überblick über die Berechtigungen gänzlich
- Die Möglichkeit, bei ungewünschten Situationen einzugreifen, gibt es somit nicht
- Klar definierte Prozesse sind notwendig

TENFOLD LIVE DEMO

FEATURES

tenfold

Identity & Access Management

Verwaltung von Benutzerkonten und Berechtigungen auf Basis von Geschäftsrollen.

Self-Service & Workflows

Portal für Endbenutzer und Einrichtung von Genehmigungsworkflows für Fachbereiche.

User Access Reviews

Periodische Kontrolle der individuellen Zugriffsrechte durch die Dateneigentümer in den Fachbereichen.

Change Tracking

Dokumentation und Reporting aller über tenfold und extern angesteuerten Änderungen.

Microsoft, Cloud & Third-Party

Integration aller wichtigen Systeme, wie Active Directory, Fileserver, Microsoft 365 und Anwendungen wie SAP ERP.

Generic Connector

Integration von zusätzlichen Systemen über den Generic Connector und die REST API.

VORTEILE

tenfold

Höhere Security

Rollenbasierte Berechtigungsvergabe, Access Reviews, Workflows und umfangreiche Reports senken das Risiko für Diebstahl oder Missbrauch sensibler Daten.

Höhere Productivity

Wichtige und knappe IT-Ressourcen können durch automatische Provisionierung eingespart werden. Workflows sparen dem ganzen Unternehmen viel wertvolle Zeit.

Höhere Compliance

Regularien wie ISO 27001, PCI-DSS, KRITIS, TISAX oder BAIT erfordern ein nachvollziehbares und sicheres Kontrollsystem für Berechtigungen. Ohne Software ist das kaum zu bewerkstelligen.

Bechtle Austria – IAM-Team

Ernst Hanke
Team Lead IAM

Boris Kleibl
Technical Consultant

Markus Beier
System Engineer

Martin Antunovic
System Engineer

Alex Weil
System Engineer

Andreas Stachl
Senior System Engineer

Gabriela Swoboda
Service Administration

iam.at@bechtle.com

Zeit für Ihre Fragen.

Weitere Infos:
iam.at@bechtle.com