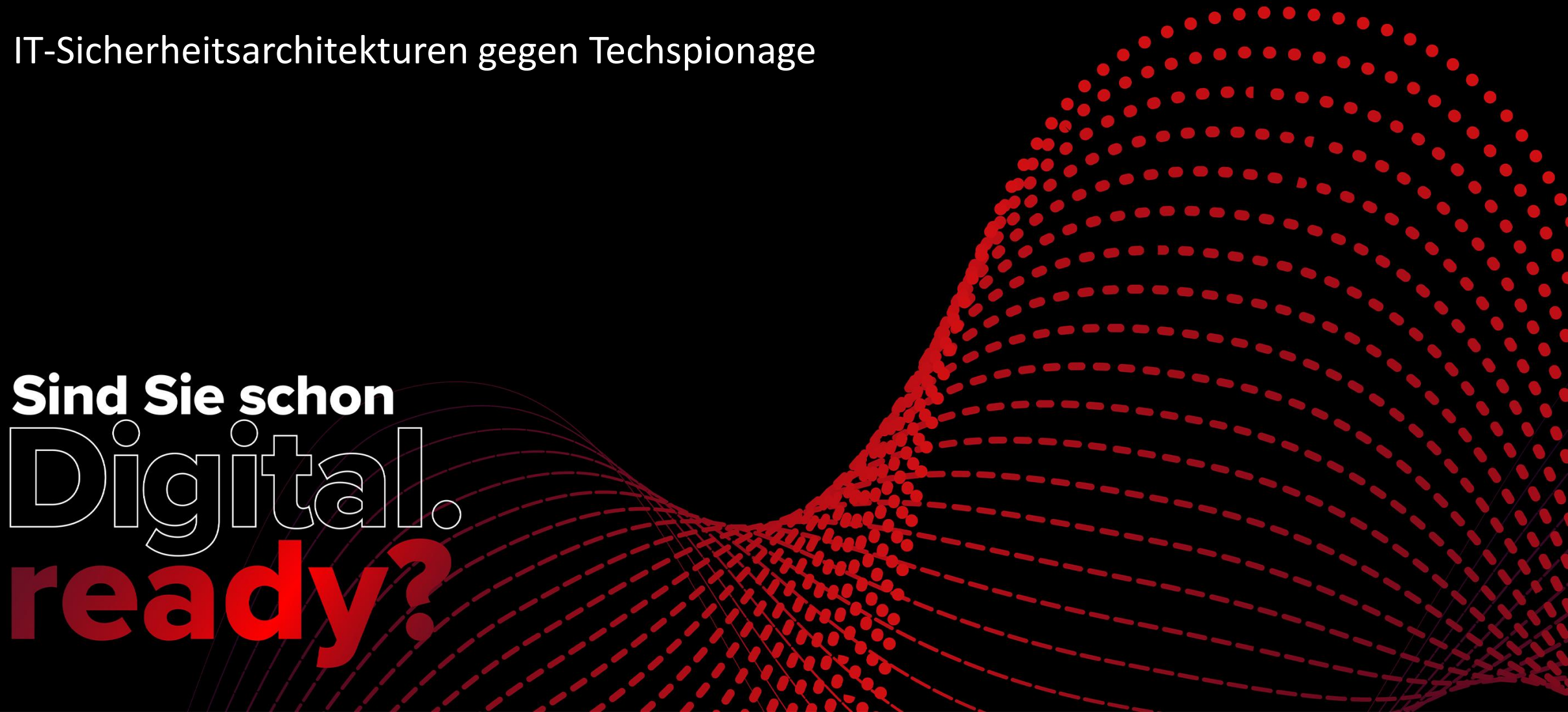
ProComp

// Zero Trust, DLP & Co.

IT-Sicherheitsarchitekturen gegen Techspionage



ProComp

// Andreas Ernstberger

Bereichsleiter IT-Infrastruktur & -Security

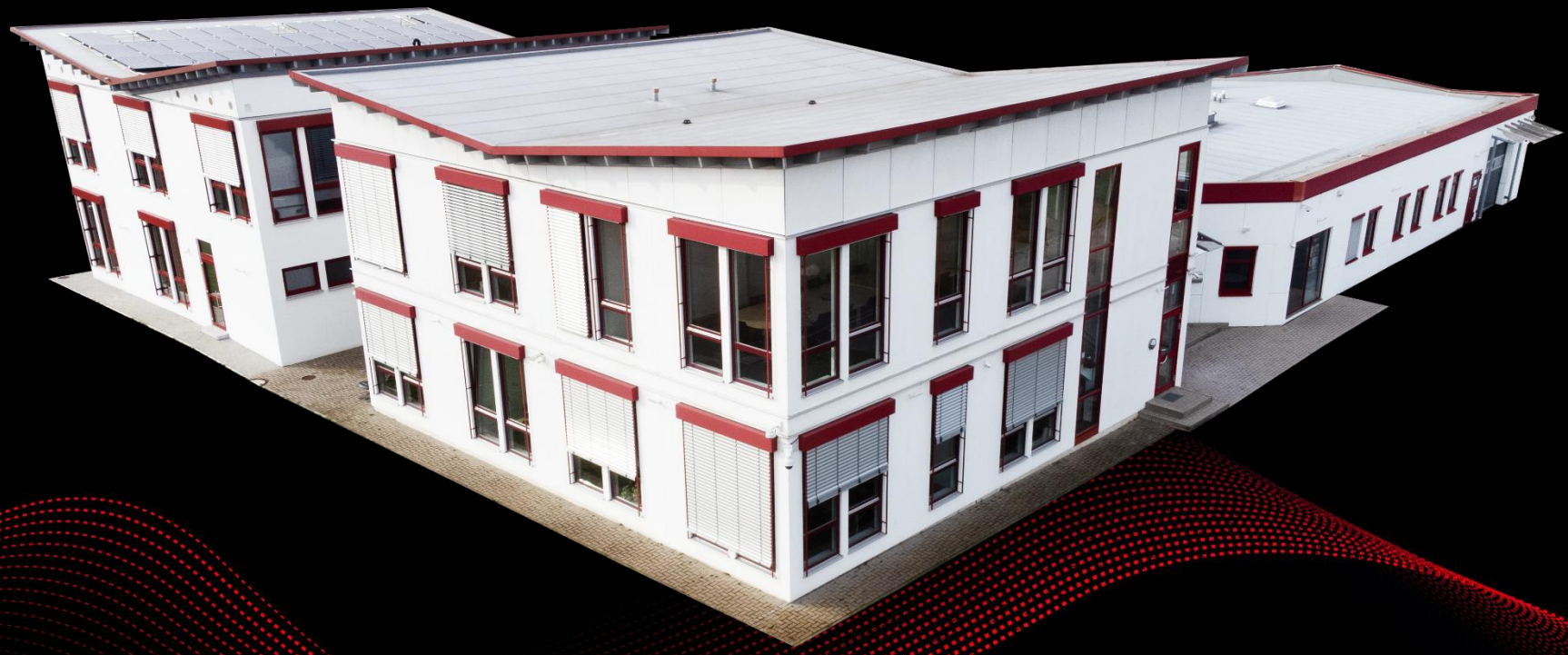
- Seit 2002 bei ProComp beschäftigt
- Seit 2015 Schwerpunkt IT-Sicherheit (Consulting & Vertrieb)

ProComp

ProComp Professional Computer GmbH

- Mitarbeiter: 60
- Gründung: 1990
- Standort: Marktredwitz

CERTIFIED ISO/IEC27001 Proks CERTIFICATION



ProComp

// Unsere Lösungen

Digitale Prozesse

IT-Infrastruktur

IT-Security

Video-/
Sicherheitstechnik

Webbasierte
Lösungen

ProComp

// Agenda

- Bedrohungslage
- Früher vs. heute
- Zero Trust – Vertrauen ist gut, Kontrolle ist besser
- Data Loss Prevention – Schutz sensibler Daten
- Organisatorische Maßnahmen
- Q & A

ProComp

// Bedrohungslage

Bitkom Wirtschaftsschutz-Studie 2025:

- 289 Mrd. € Schaden durch Datendiebstahl, Sabotage & Industriespionage 📈
- 9 von 10 Unternehmen berichten von Datendiebstahl
- Ransomware, Phishing, Einsatz von KI nehmen rasant zu
- Besonders betroffen: geistiges Eigentum, Zugangs- und Kundendaten

Quelle: https://www.bitkom.org/Bitkom/Publikationen/Studie-Wirtschaftsschutz

ProComp

// Bedrohungslage

Spiegel

Microsofts D… von Cybera…

Nur drei Staaten … Bundesrepublik…

vor 1 Woche

MDR

Hackerangr…

Nicht Flughäfen … Hackerangriffs.

vor 14 Stunden

Goslarsche.de

Hackerangriff … lahm

Vor 6 Tagen

SWR

Schwere Cyberattacke auf Gemeindeverwaltung: Nur noch das Telefon funktioniert

Vor 9 Tagen • Von Catharin Freudenberger

Quelle: Google

ProComp

// Wer steckt dahinter?

(Staatl. Unterstützte) Hackergruppen

Konkurrenzunternehmen

Insider

ProComp

Zero Trust

ProComp

// Früher vs. heute

- **Früher:**
  - Intern: gut
  - Extern: potenziell böse
  - Perimeter-Schutz (Firewall, VPN)

- **Heute:**
  - Hybride Infrastrukturen
  - Homeoffice
  - „Der eine“ Perimeter existiert nicht mehr

// Zero Trust

- **Was ist Zero Trust?**
  - Eine Sicherheitsstrategie, keine Lösung

- **Warum wichtig?**
  - Cloud-Nutzung und mobiles Arbeiten machten Netzwerkperimeter obsolet
  - Zunahme von Insider-Bedrohungen und komplexen Angriffen

- **Hauptziel:**
  - **Schutz vor unbefugtem Zugriff** auf Daten und Systeme, unabhängig davon, ob der Zugriff von innen oder außen erfolgt

// Prinzipien von Zero Trust

„never trust, always verify“

// Prinzipien von Zero Trust

// Prinzipien von Zero Trust

- Multifaktorauthentifizierung
- Kontinuierliche Überprüfung
- Daten-/Identitätszentrierung

// Prinzipien von Zero Trust

- Nur notwendige Rechte
- Zeitlich begrenzte Rechte
- Regelmäßige Überprüfung
- Rollenbasierte Vergabe

// Prinzipien von Zero Trust

- Mikrosegmentierung
- Kontinuierliches Monitoring & Anomalie-Erkennung
- Protokollierung und Forensik
- Incident Response & Notfallpläne
- Verschlüsselung
- Regelmäßige Pentests
- Zero Standing Privileges
- Automatisierte Reaktionen

// Wo lässt sich Zero Trust umsetzen?

- **Identität:**
  - Benutzeridentitäten: Starke Authentifizierung (z.B. MFA)
  - Geräteidentitäten: Zugriff nur für vertrauenswürdige Geräte

- **Endgeräte (Endpoints):**
  - Gerätezustand prüfen: Gepatcht? Verschlüsselt? Geschützt?
  - Endpoint Detection & Response (EDR): Echtzeitüberwachung / Reaktion
  - Mobile Device Management: Kontrolle über mobile Endgeräte

- **Netzwerk:**
  - Segmentierung: Mikrosegmentierung zur Begrenzung von Bewegungsfreiheit
  - Zugriffskontrolle: z.B. NAC, ZTNA

ProComp

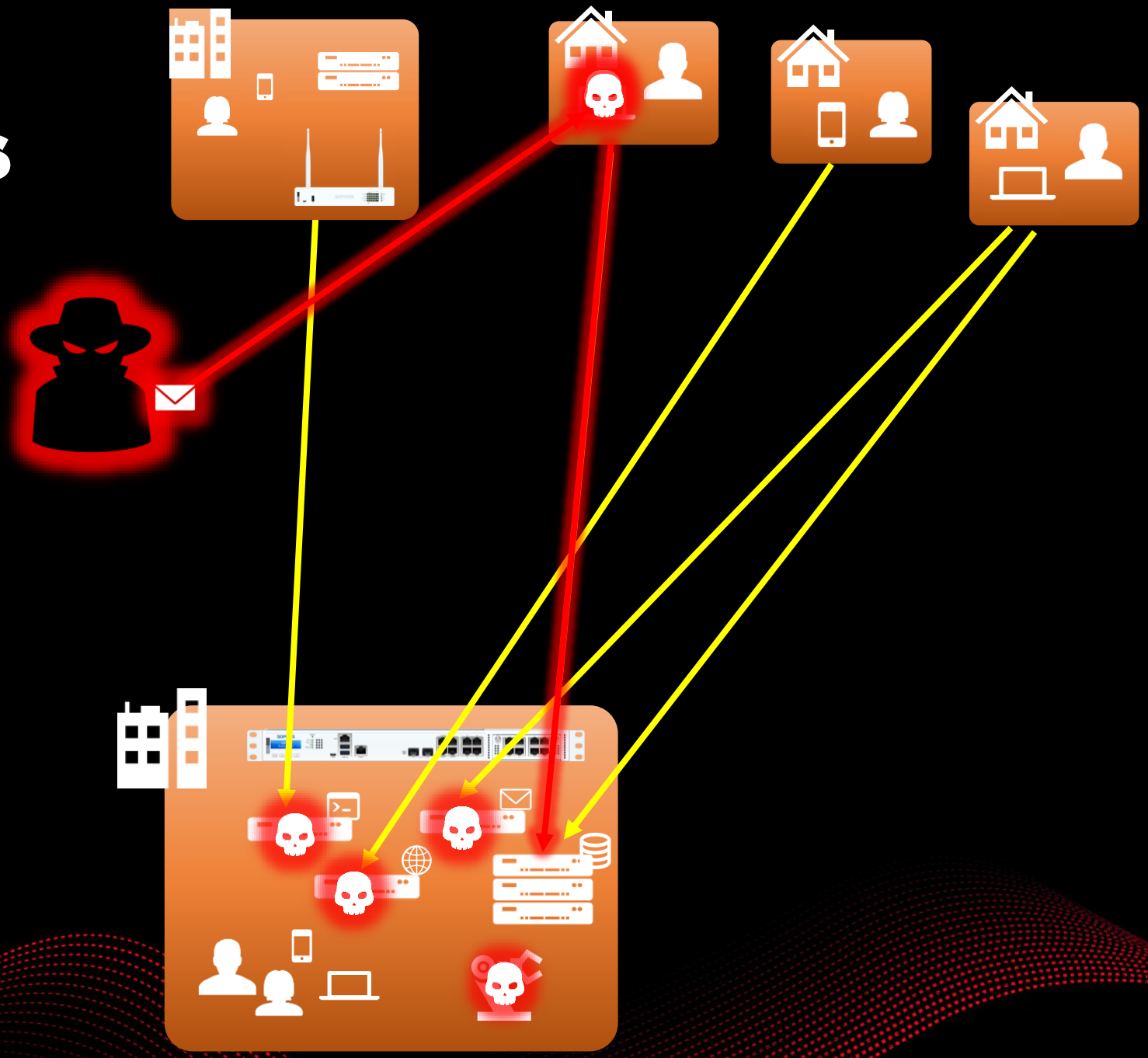
// Wo lässt sich Zero Trust umsetzen?

- **Cloud und SaaS-Anwendungen:**
  - Zugriffsrichtlinien: Conditional Access in M365, Google Workspace, etc.
  - App-Schutz: Cloud Access Security Broker zur Kontrolle von Schatten-IT
  - Datenklassifizierung: Schutz sensibler Daten durch Data Loss Prevention (DLP)
- **Daten:**
  - Verschlüsselung: Gespeicherte und übertragene Daten verschlüsseln
  - Zugriffsrechte: Zugriff nur nach Bedarf und Kontext
  - Monitoring: Protokollierung und Analyse von Datenzugriffen
- **Awareness und Prozesse:**
  - Schulungen: Sensibilisierung der MA für Zero Trust
  - Incident Response: Klare Prozesse zur Erkennung und Reaktion auf Vorfälle
  - Kontinuierliche Evaluierung: Zero Trust ist kein Zustand, sondern ein Prozess

ProComp

Zero Trust Network Access (ZTNA)

Klassisches VPN



Ransomware-Gruppen greifen gezielt VPN an

Netzwoche

Hacker nutz

Der US-amerikan
Sicherheitslücke i

10.01.2025

it- it-daily

SafePay-Ransomware legt IT-Systeme von Ingram Micro lahm

Der IT-Distributor
über VPN-Gatew

07.07.2025

Golem.de

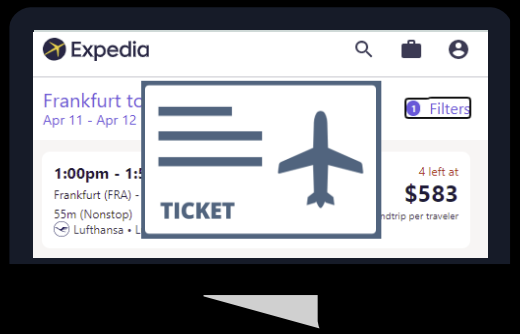
Ransomware: Akira umgeht MFA von Sonicwall-VPN-Konten

Die Google Threat Intelligence Group ordnete im Juli (öffnet im neuen Fenster) mehrere Einbrüche in Appliances von Sonicwalls SMA-100-Serie...

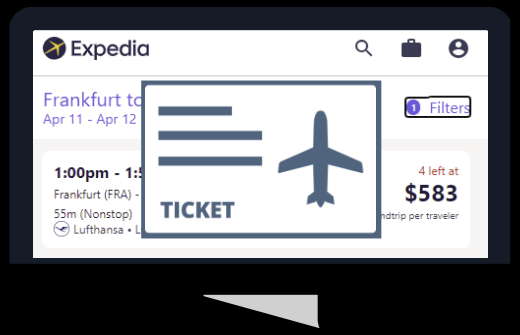
vor 1 Monat

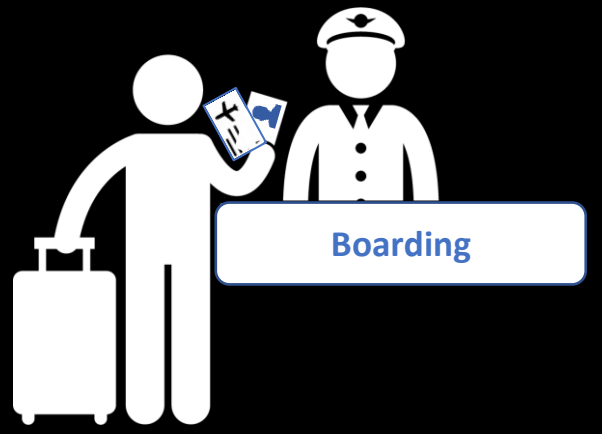
Quelle: Google

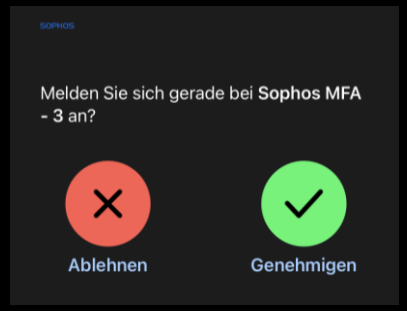
Flughafensicherheit heute

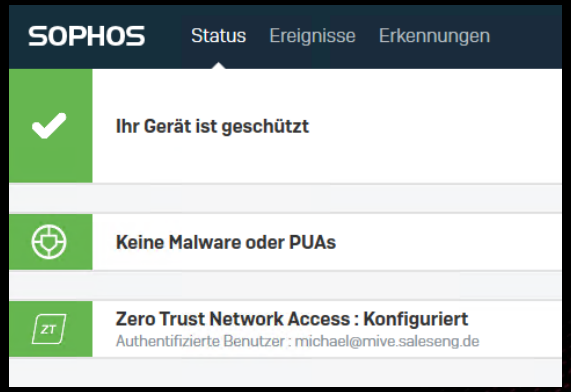


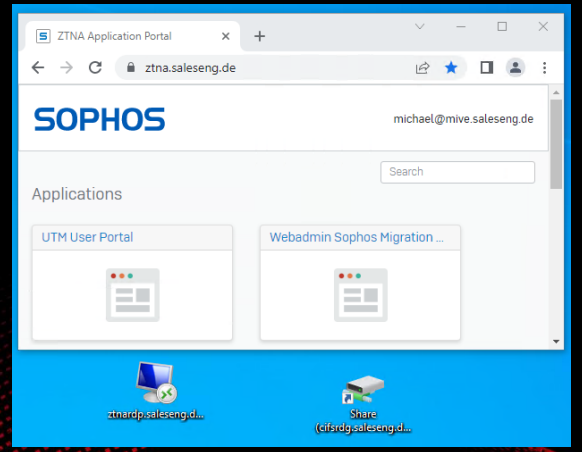
Flughafensicherheit heute





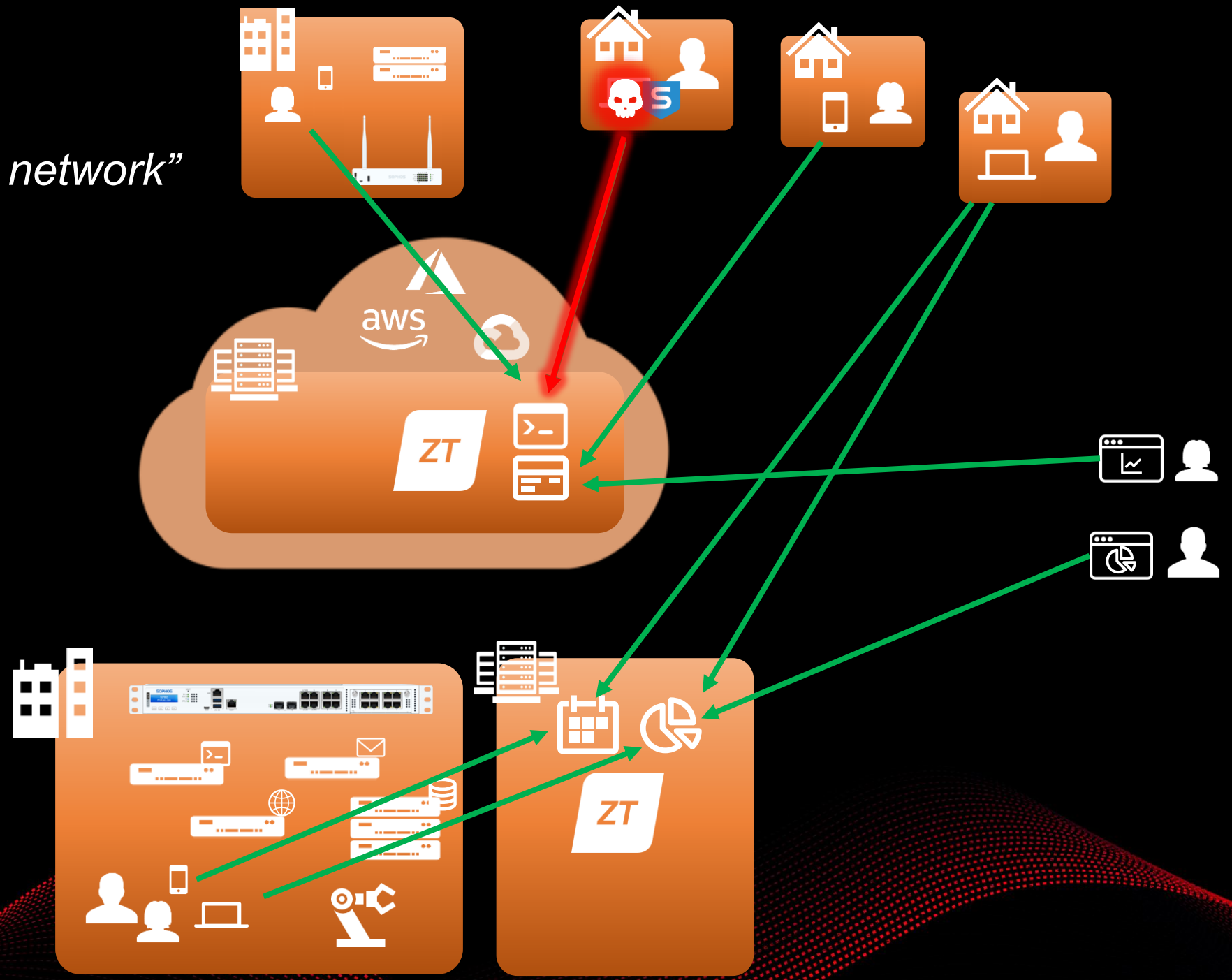






ZTNA

*"You're **NOT on** the network"*



(Live Demo ZTNA)

ProComp

Data Loss Prevention (DLP)

ProComp

// Data Loss Prevention (DLP)

- **Zweck:**
  - Verhindern, dass vertrauliche oder sensible Daten das Unternehmen unkontrolliert verlassen

- **Funktionsweise:**
  - Überwachung von Datenbewegungen
  - Erkennung von Mustern (z.B. Inhalte, Dateitypen, usw.)

- **Typische Einsatzbereiche:**
  - **E-Mail-DLP:** Verhindert das Versenden sensibler Daten an externe Empfänger
  - **Endpoint-DLP:** Schützt vor Datenabfluss über USB-Sticks / Software / Drucker
  - **Cloud-DLP:** Kontrolliert Daten in SaaS-Anwendungen (z.B. M365)

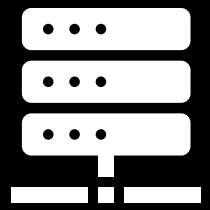
ProComp

// Data Loss Prevention (DLP)

- **Herausforderungen / ToDos:**
  - Unternehmen müssen wissen, **welche Daten sensibel sind**
  - Ohne klare Klassifizierung ist DLP ineffektiv
  - Komplexität wg. unterschiedlicher Speicherorte: On-Prem, Cloud, Endgeräte
  - Gute Kommunikation und Schulung der MA ist entscheidend
  - **DLP erkennt Muster, nicht Absichten**
  - Erfordert sowohl technisch- als auch organisatorisch durchdachte Planung

ProComp

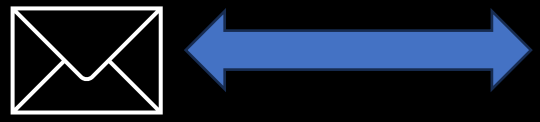
// E-Mail-DLP

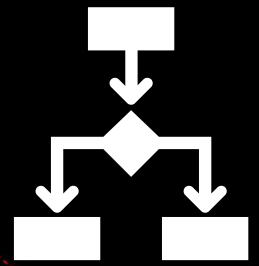


Mailserver on premises

oder

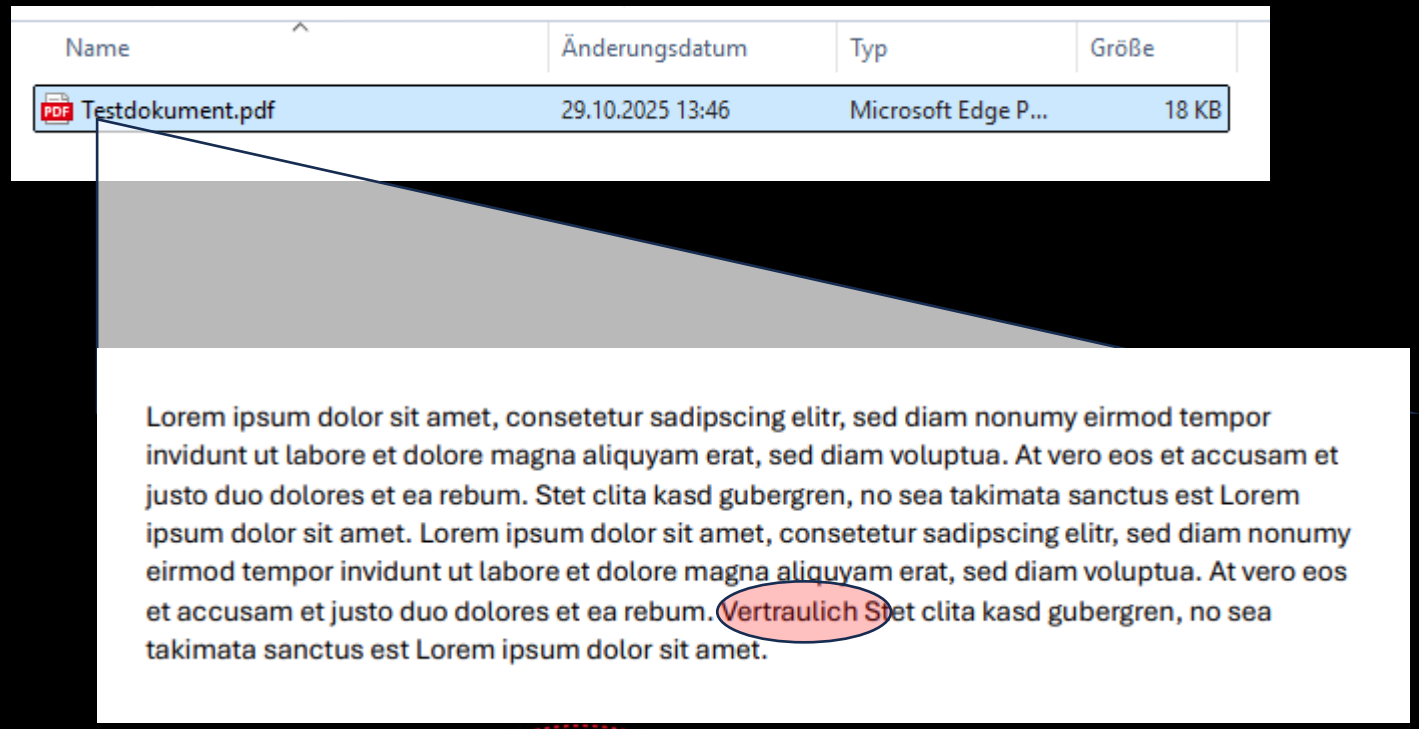
Microsoft 365



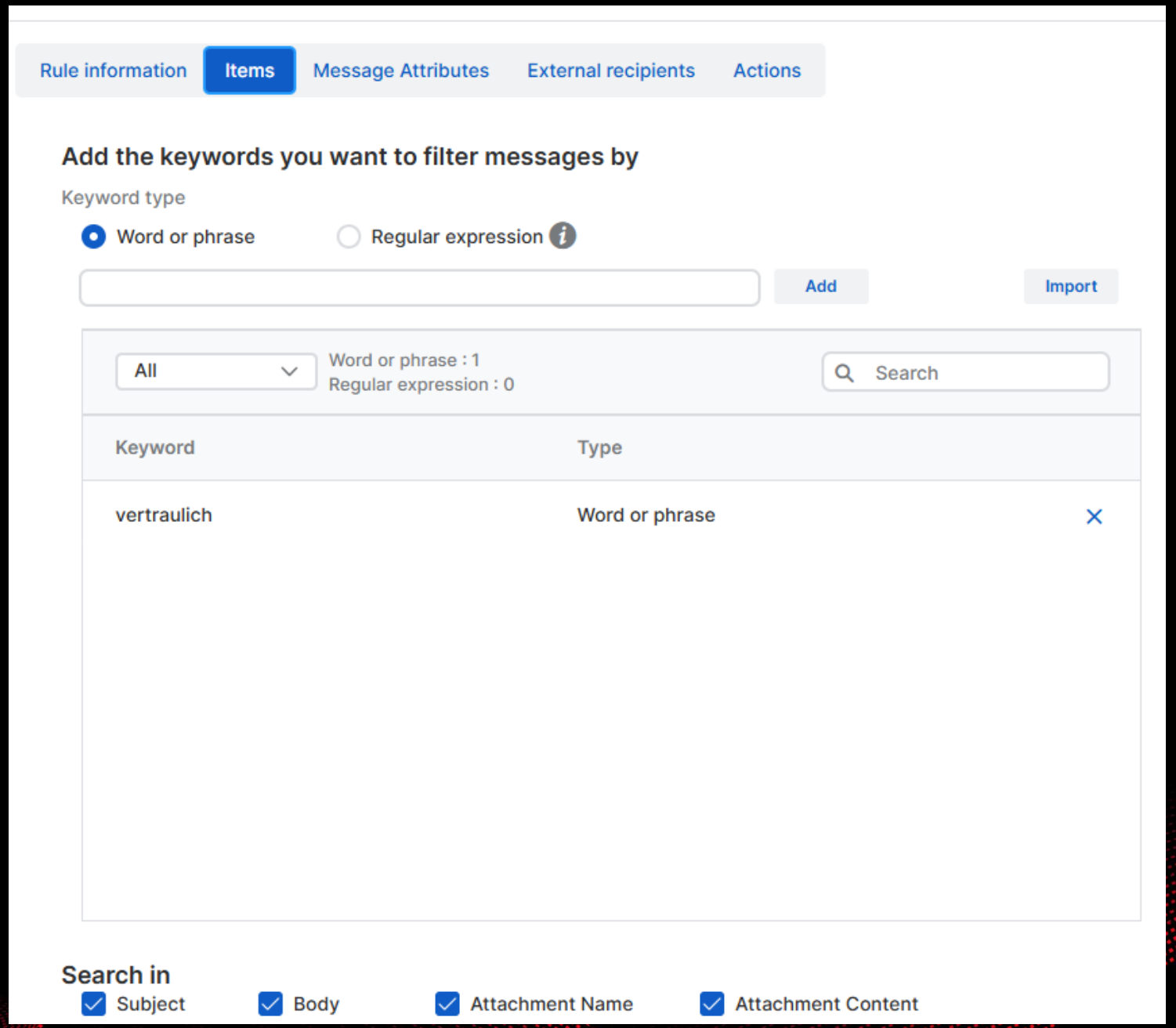


ProComp

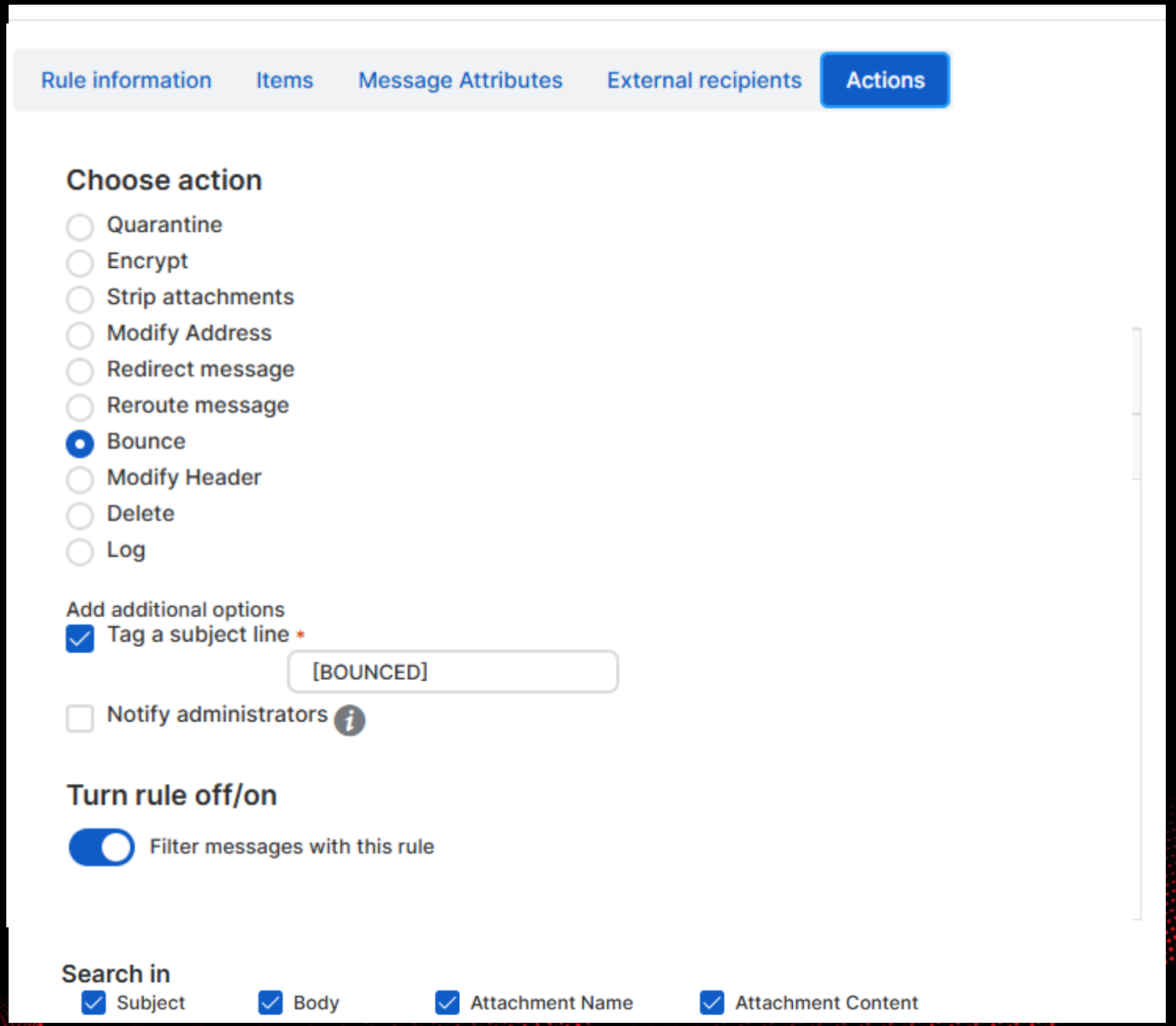
// E-Mail-DLP



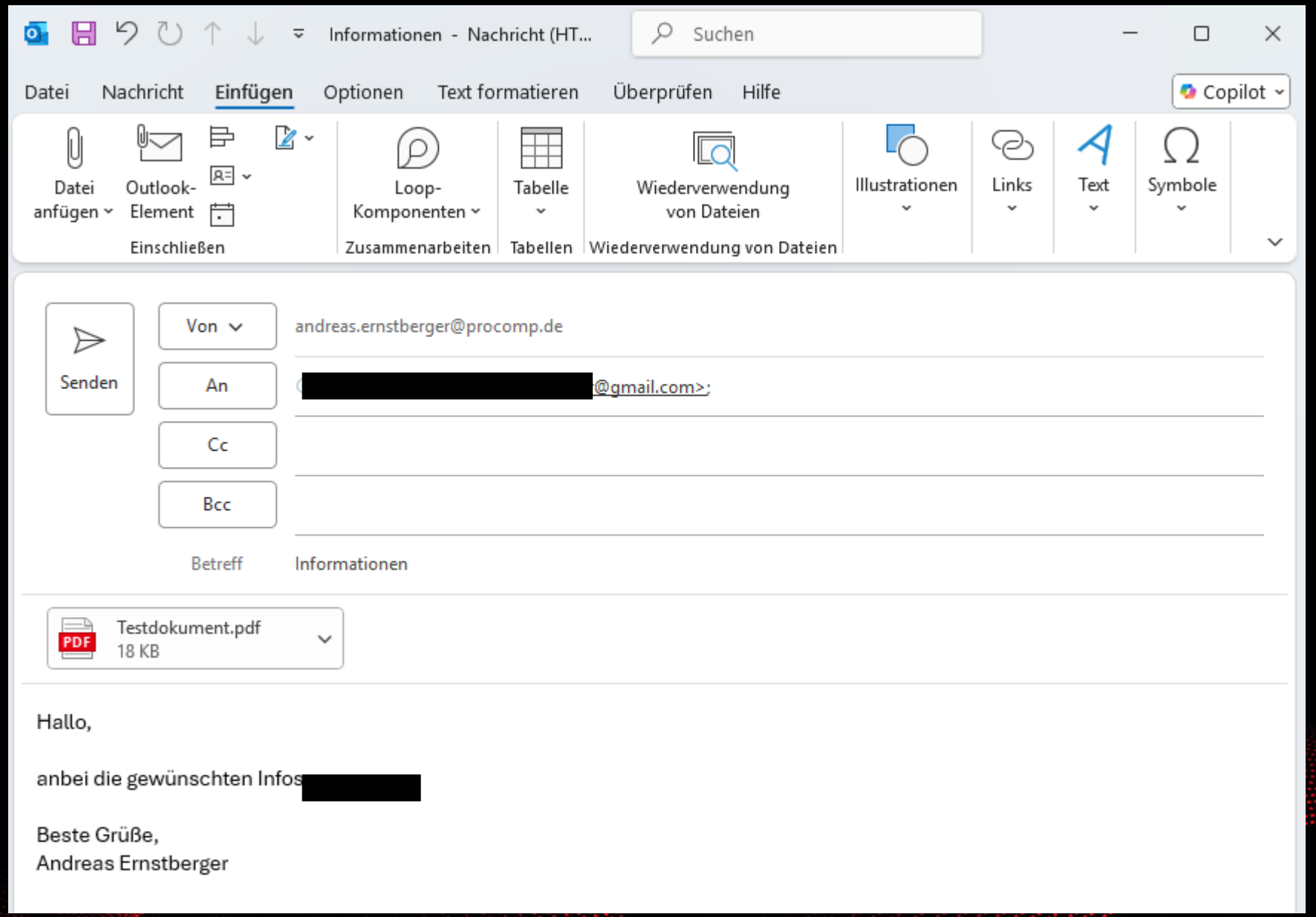
ProComp



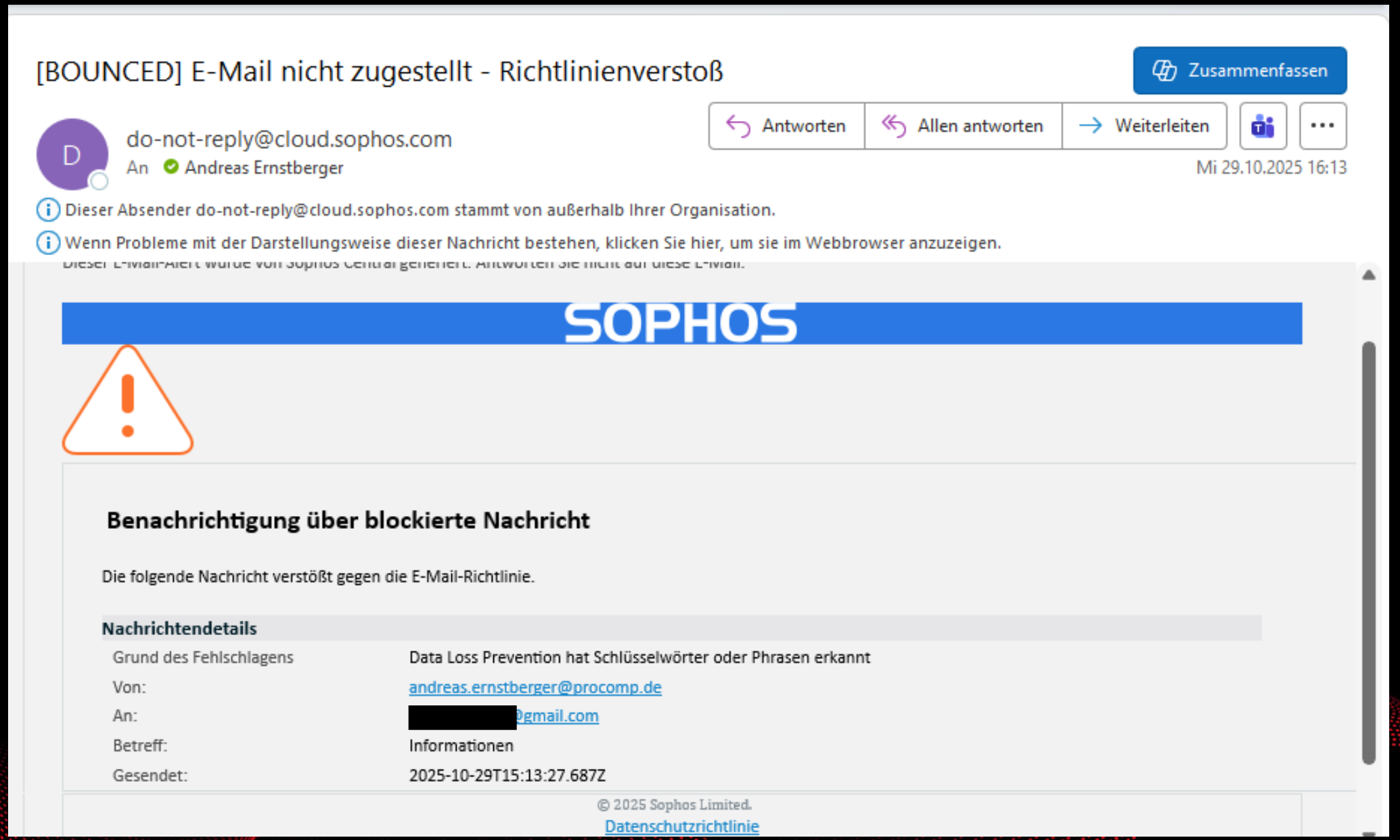
ProComp



ProComp

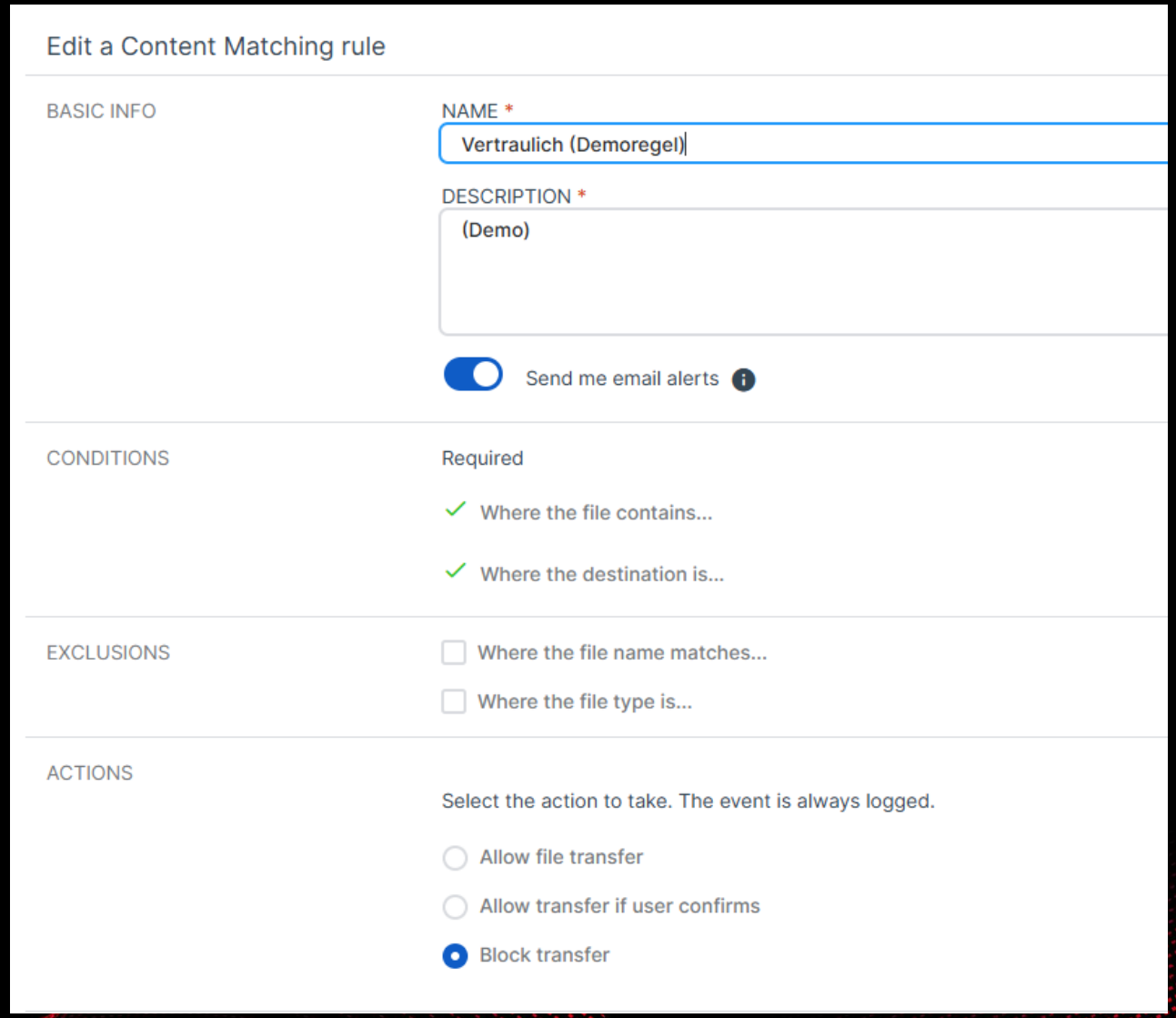


ProComp



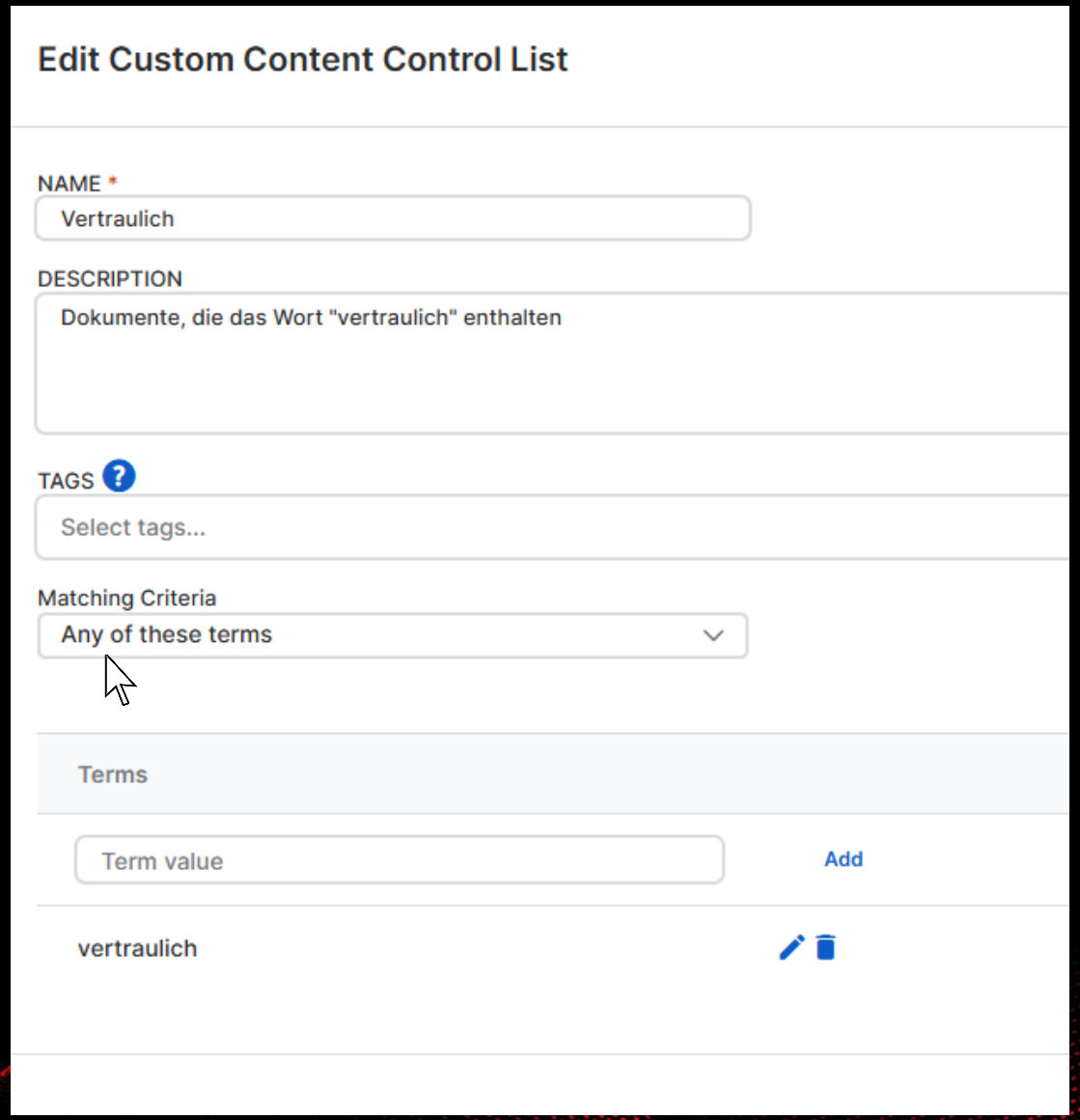
ProComp

// Endpoint-DLP



ProComp

// Endpoint-DLP



ProComp

// Endpoint-DLP

Destination is:

Internet browser

- CloudFactory WorkStream Browser
- Firefox (V7 and higher)
- Firefox 1
- Firefox 2
- Firefox 3
- Firefox 4
- Firefox 5
- Firefox 6
- Google Chrome
- Internet Explorer 10
- Internet Explorer 11
- Internet Explorer 5
- Internet Explorer 6
- Internet Explorer 7
- Internet Explorer 8
- Internet Explorer 9
- Microsoft Edge
- Opera Browser
- Vivaldi

• Internet browser

Email client

- Lotus Notes Client
- Microsoft HxOutlook
- Outlook
- Outlook Express
- Thunderbird
- Windows Mail

• Email client

ProComp

// Endpoint-DLP

Instant messaging

- Microsoft Lync
- Microsoft Office Communicator
- Microsoft Teams
- Skype for Business
- Slack
- WebEx Connect

Internet browser - external processes

- Adobe Flash file uploader
- Firefox Plugin Container

Voice over IP

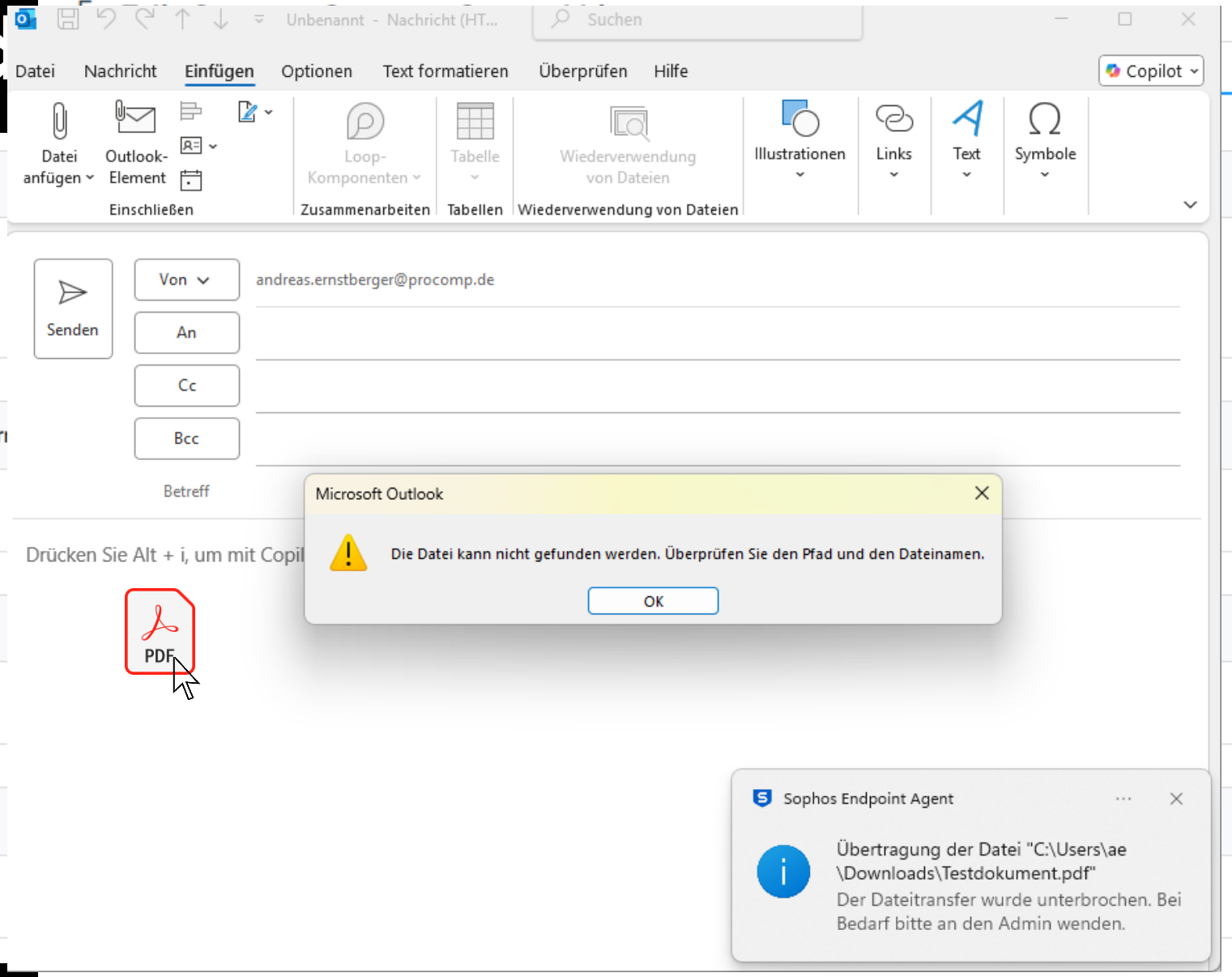
- Skype
- WhatsApp

Storage

- Floppy Drive
- Optical Drive
- Removable Storage

// End

ProComp



Instant messaging

Microsoft Lync

Slack

Skype for Business

Internet browser - exter

Adobe Flash file uploader

Voice over IP

Skype

Storage

Floppy Drive

ProComp

// Organisatorische Maßnahmen

- **Mitarbeiterschulungen & Awareness:**
  - Regelmäßige Schulungen zu Spionage-Risiken
  - Sensibilisierung für Social Engineering und Insider Threats
  - Meldeweg für verdächtige Vorfälle etablieren

- **Incident Response & Eskalationsprozesse:**
  - Notfallpläne bei Verdacht auf Spionage
  - Schnelle Eskalation und forensische Analyse
  - Dokumentation und Lessons Learned

ProComp

// Schlusswort

🔒 **Sicherheit beginnt nicht mit Firewalls – sie beginnt mit Bewusstsein.**

👥 **Jeder Mitarbeiter ist Teil der Verteidigungslinie.**

🔁 **Nur durch kontinuierliche Sensibilisierung, klare Prozesse und eine gelebte Sicherheitskultur können wir Spionage effektiv begegnen.**

ProComp

Vielen Dank für Ihre Aufmerksamkeit!

Andreas Ernstberger
Tel.: 09231/9970-31
E-Mail: andreas.ernstberger@procomp.de