

// Zero Trust, DLP & Co.

IT-Sicherheitsarchitekturen gegen Techspionage

Sind Sie schon
Digital.
ready?



// **Andreas Ernstberger**

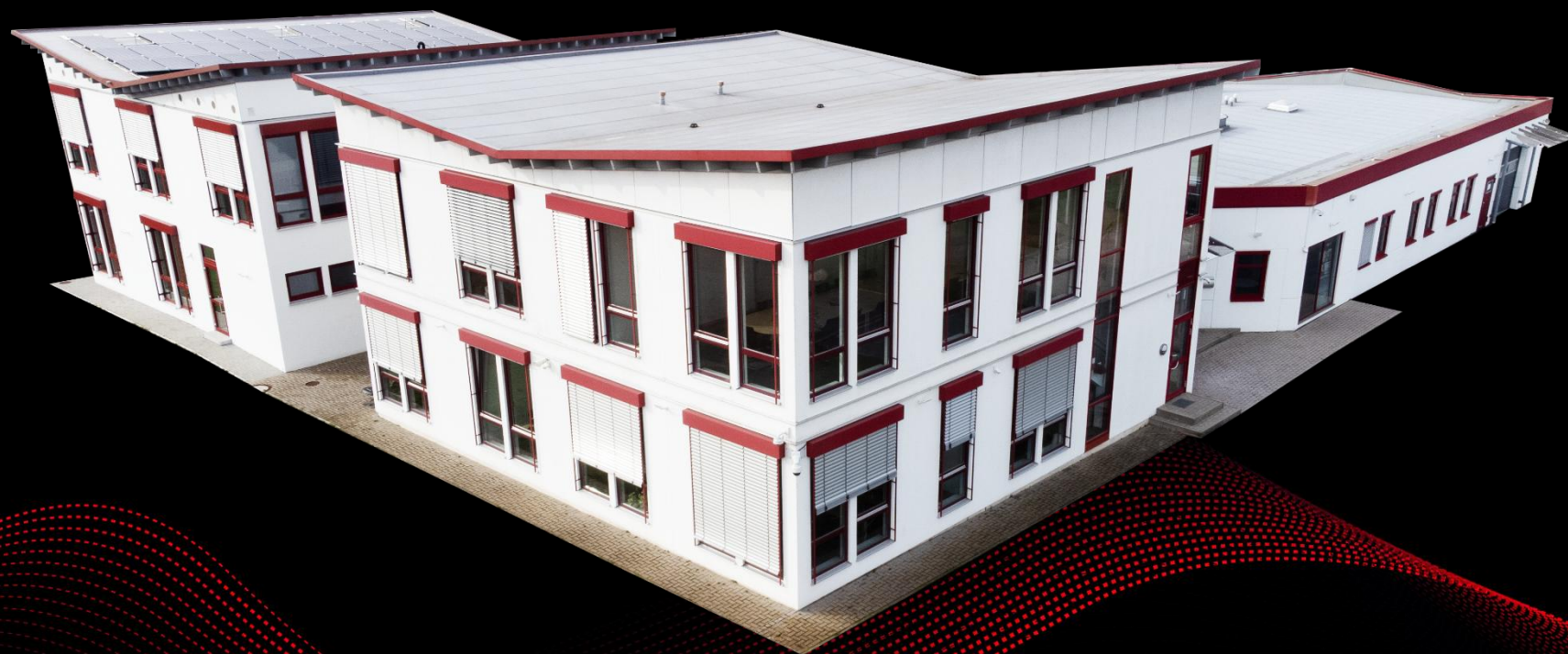
Bereichsleiter IT-Infrastruktur & -Security

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



ProComp Professional Computer GmbH

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



// Unsere Lösungen



Digitale Prozesse



IT-Infrastruktur



IT-Security



Video-/
Sicherheitstechnik



Webbasierte
Lösungen

// Agenda

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

// 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>

// Bedrohungslage



Quelle: Google

// Wer steckt dahinter?



(Staatl. Unterstützte)
Hackergruppen



Konkurrenzunternehmen



Insider

Zero Trust



// **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



**Explizit
verifizieren**



**Zugriff mit
minimalen
Rechten**



**Vom
Einbruch
ausgehen**

// Prinzipien von Zero Trust



**Explizit
verifizieren**

- Multifaktorauthentifizierung
- Kontinuierliche Überprüfung
- Daten-/Identitätszentrierung

// Prinzipien von Zero Trust



**Zugriff mit
minimalen
Rechten**

- **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

// 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

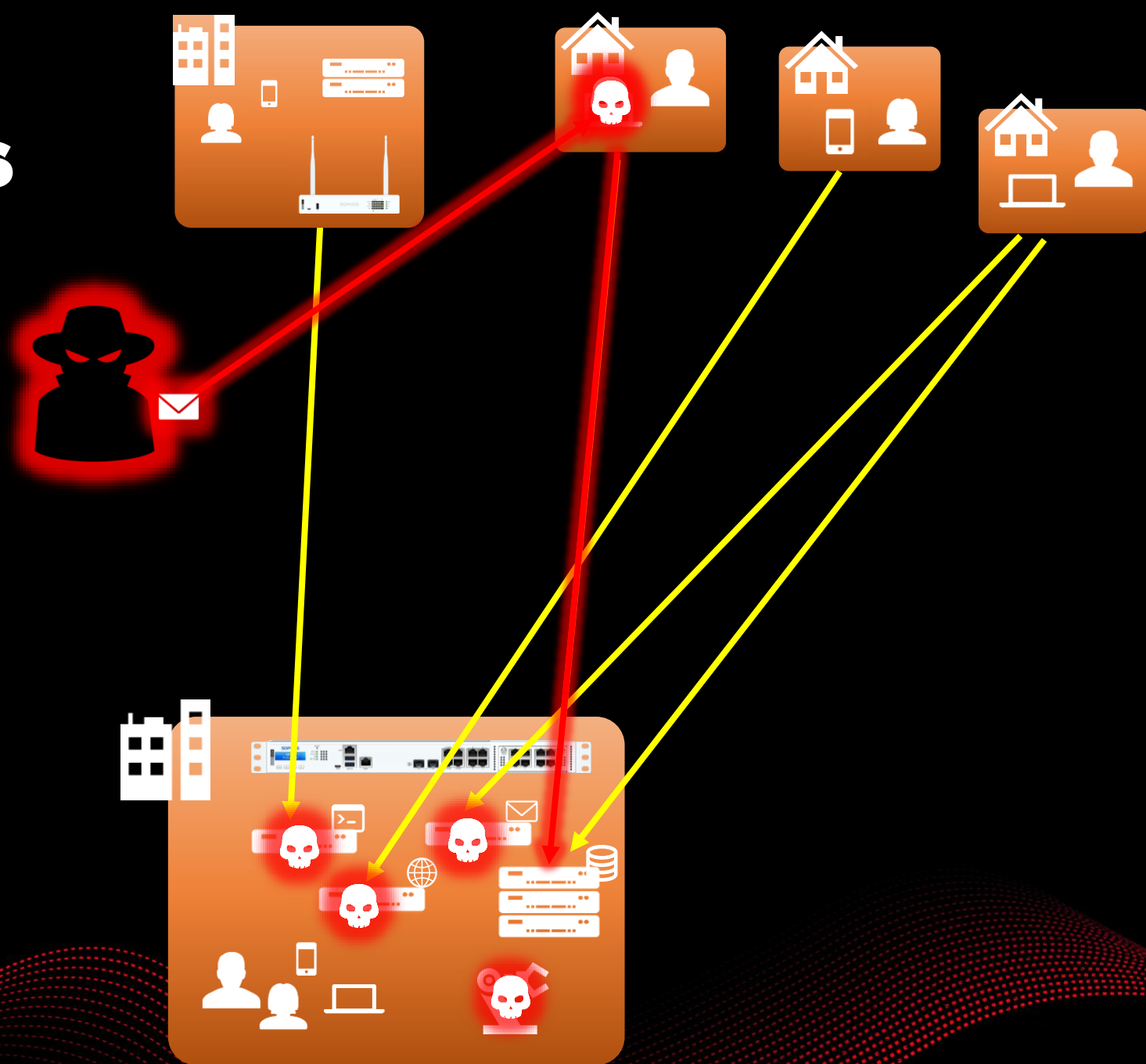
➤ Awareness und Prozesse:

- 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

Zero Trust Network Access (ZTNA)



Klassisches VPN

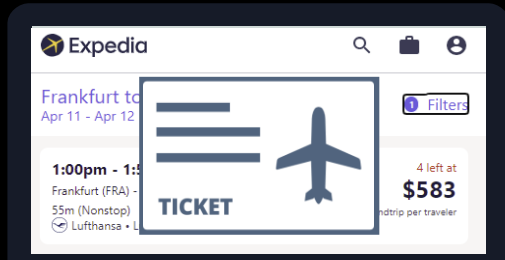


Ransomware-Gruppen greifen gezielt VPN an

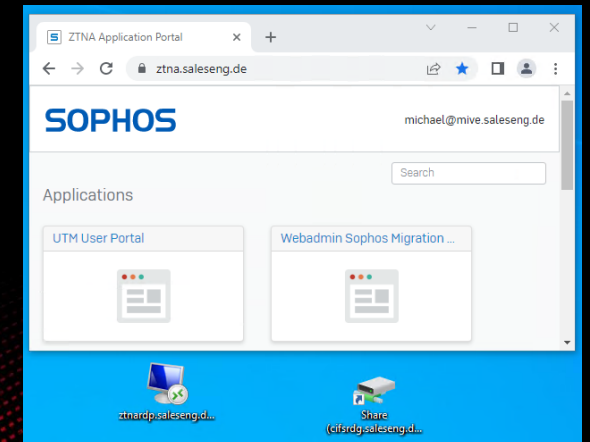
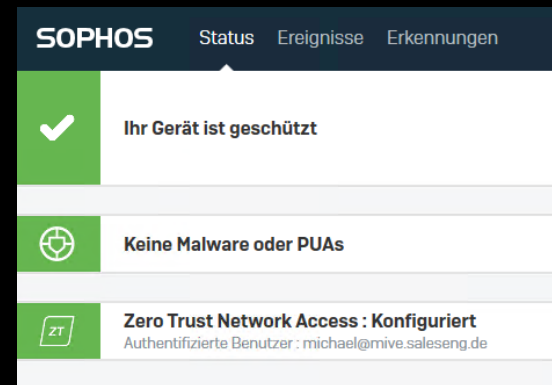
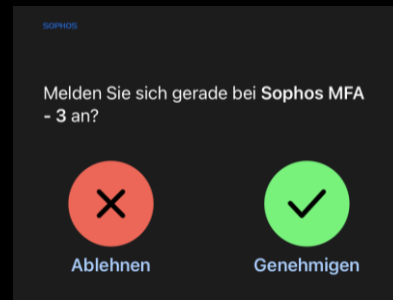
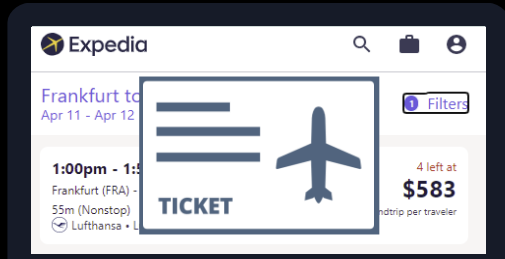


Quelle: Google

Flughafensicherheit heute

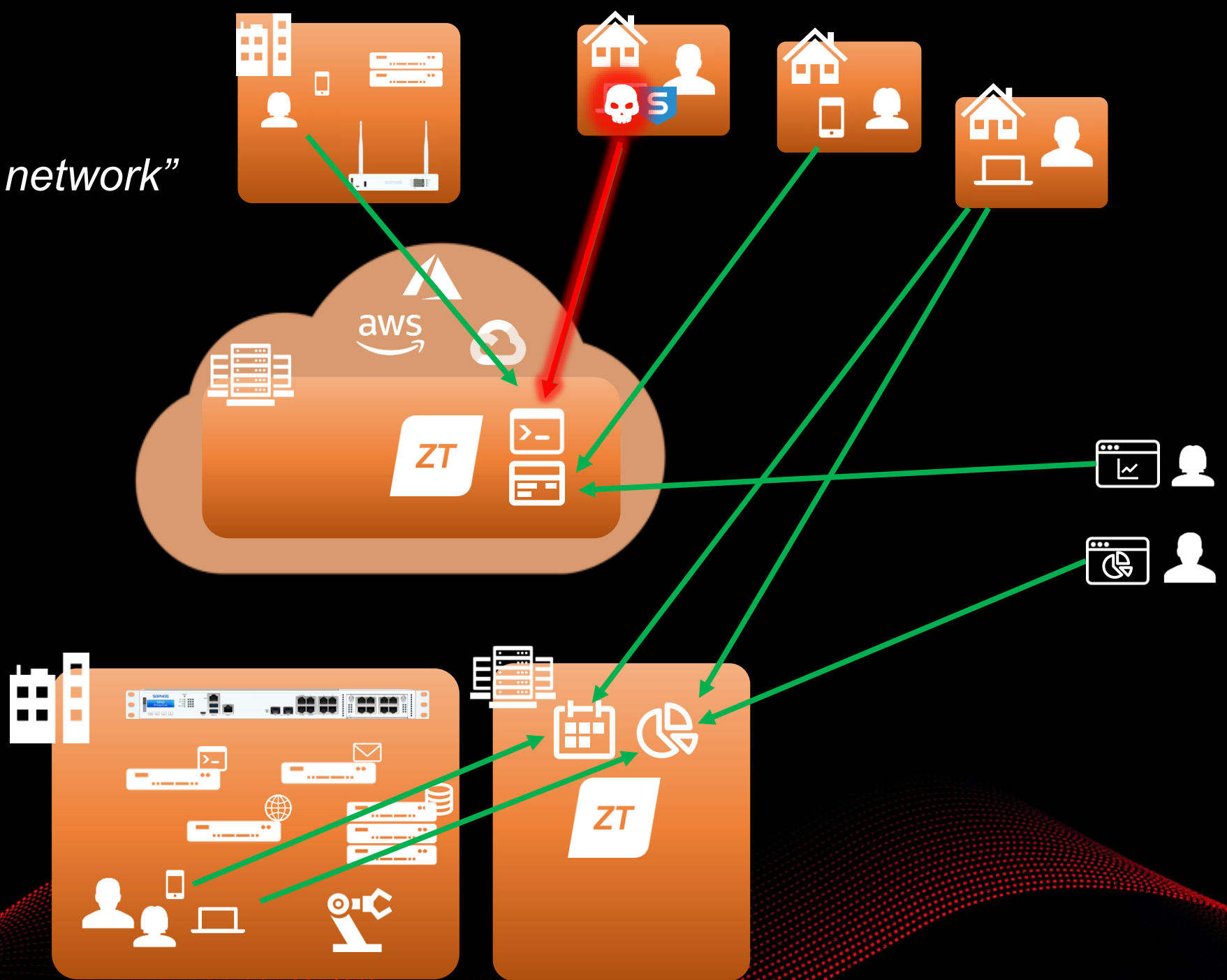


Flughafensicherheit heute



ZTNA

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



(Live Demo ZTNA)



Data Loss Prevention (DLP)



// 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:

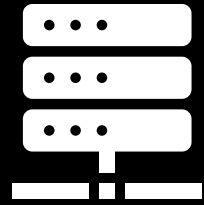
- **E-Mail-DLP:** Verhindert das Versenden sensibler Daten an externe Empfänger
- **Endpoint-DLP:** Schützt vor Datenabfluss über USB-Sticks / Software / Drucker
- **Cloud-DLP:** Kontrolliert Daten in SaaS-Anwendungen (z.B. M365)

// Data Loss Prevention (DLP)

➤ Herausforderungen / ToDos:

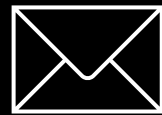
- Unternehmen müssen wissen, **welche Daten sensibel sind**
- Ohne klare Klassifizierung ist DLP ineffektiv
- Komplexität wg. unterschiedlicher Speicherorte: On-Prem, Cloud, Endgeräte
- Gute Kommunikation und Schulung der MA ist entscheidend
- **DLP erkennt Muster, nicht Absichten**
- Erfordert sowohl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

// E-Mail-DLP

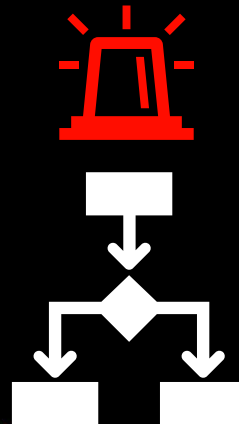


Mailserver on premises

oder



Microsoft 365



// E-Mail-DLP

Name	Änderungsdatum	Typ	Größe
 Testdokument.pdf	29.10.2025 13:46	Microsoft Edge P...	18 KB

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. **Vertraulich** Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

[Rule information](#) **Items** [Message Attributes](#) [External recipients](#) [Actions](#)

Add the keywords you want to filter messages by

Keyword type

☒ Word or phrase ☐ Regular expression *i*

Add

Import

All

Word or phrase : 1
Regular expression : 0

Search

Keyword	Type	
vertraulich	Word or phrase	

Search in
☒ Subject ☒ Body ☒ Attachment Name ☒ Attachment Content

Rule information

Items

Message Attributes

External recipients

Actions

Choose action

☐ Quarantine

☐ Encrypt

☐ Strip attachments

☐ Modify Address

☐ Redirect message

☐ Reroute message

☒ Bounce

☐ Modify Header

☐ Delete

☐ Log

Add additional options

☒ Tag a subject line *

[BOUNCED]

☐ Notify administrators i

Turn rule off/on

☒ Filter messages with this rule

Search in

☒ Subject

☒ Body

☒ Attachment Name

☒ Attachment Content

Informationen - Nachricht (HT...)

Suchen

Copilot

Datei anfügen

Outlook-Element

Einschließen

Loop-Komponenten

Zusammenarbeiten

Tabelle

Tabellen

Wiederverwendung von Dateien

Wiederverwendung von Dateien

Illustrationen

Links

Text

Symbole

Senden

Von andreas.ernstberger@procomp.de

An [REDACTED]@gmail.com

Cc

Bcc

Betreff

Informationen

Testdokument.pdf

18 KB

Hallo,

anbei die gewünschten Infos [REDACTED]

Beste Grüße,
Andreas Ernstberger

[BOUNCED] E-Mail nicht zugestellt - Richtlinienverstoß

 Zusammenfassen



do-not-reply@cloud.sophos.com

An  Andreas Ernstberger

 Antworten

 Allen antworten

 Weiterleiten



Mi 29.10.2025 16:13

 Dieser Absender do-not-reply@cloud.sophos.com stammt von außerhalb Ihrer Organisation.

 Wenn Probleme mit der Darstellungsweise dieser Nachricht bestehen, klicken Sie hier, um sie im Webbrowser anzuzeigen.

DIESER E-MAILEDIENST WURDE VON SOPHOS GEMISST. ANTWORTEN SIE NICHT AUF DIESE E-MAIL.

SOPHOS



Benachrichtigung über blockierte Nachricht

Die folgende Nachricht verstößt gegen die E-Mail-Richtlinie.

Nachrichtendetails

Grund des Fehlschlagens	Data Loss Prevention hat Schlüsselwörter oder Phrasen erkannt
Von:	andreas.ernstberger@procomp.de
An:	 @gmail.com
Betreff:	Informationen
Gesendet:	2025-10-29T15:13:27.687Z

© 2025 Sophos Limited.

[Datenschutzrichtlinie](#)

// Endpoint-DLP

Edit a Content Matching rule

BASIC INFO

NAME *

Vertraulich (Demoregel)

DESCRIPTION *

(Demo)

☒

 Send me email alerts ⓘ

CONDITIONS

Required

✓

 Where the file contains...

✓

 Where the destination is...

EXCLUSIONS

☐

 Where the file name matches...

☐

 Where the file type is...

ACTIONS

Select the action to take. The event is always logged.

☐ Allow file transfer

☐ Allow transfer if user confirms

☒ Block transfer

// Endpoint-DLP

Edit Custom Content Control List

NAME *

Vertraulich

DESCRIPTION

Dokumente, die das Wort "vertraulich" enthalten

TAGS ?

Select tags...

Matching Criteria

Any of these terms

Terms

Term value

Add

vertraulich



// Endpoint-DLP

▼ Destination is:

▼ ☒ Internet browser

☒ CloudFactory WorkStream Browser

☒ Firefox 3

☒ Google Chrome

☒ Internet Explorer 6

☒ Microsoft Edge

☒ Firefox (V7 and higher)

☒ Firefox 4

☒ Internet Explorer 10

☒ Internet Explorer 7

☒ Opera Browser

☒ Firefox 1

☒ Firefox 5

☒ Internet Explorer 11

☒ Internet Explorer 8

☒ Vivaldi

☒ Firefox 2

☒ Firefox 6

☒ Internet Explorer 5

☒ Internet Explorer 9

• Internet browser

▼ ☒ Email client

☒ Lotus Notes Client

☒ Thunderbird

☒ Microsoft HxOutlook

☒ Windows Mail

☒ Outlook

☒ Outlook Express

• Email client

// 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

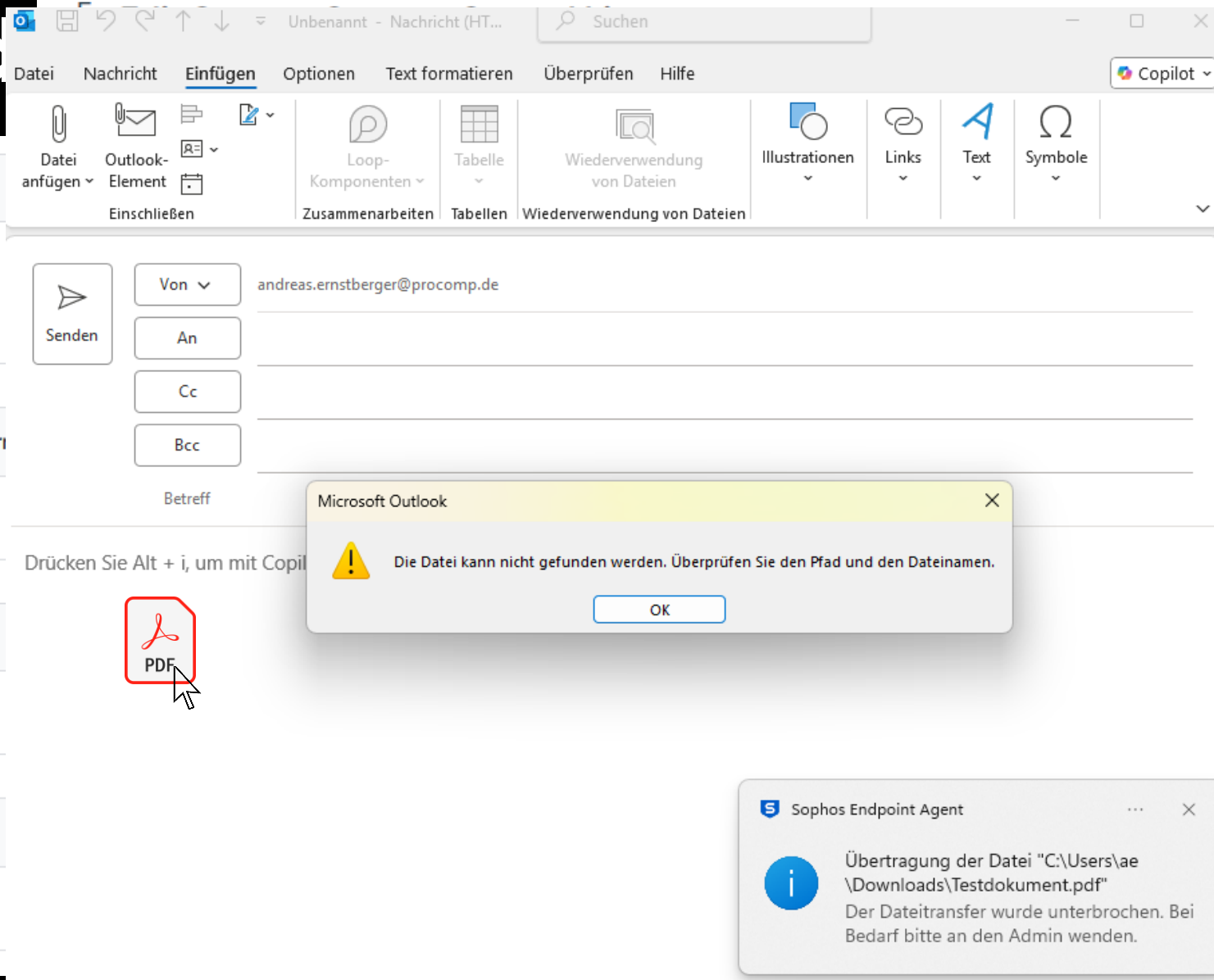
▼ ☐ Storage

☐ Floppy Drive

☐ Optical Drive

☐ Removable Storage

// End



// 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
- 

// **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.**

Vielen Dank für Ihre Aufmerksamkeit!

Andreas Ernstberger

Tel.: 09231/9970-31

E-Mail: andreas.ernstberger@procomp.de

