



Effektiver Schutz vor Phishing und Betrügern mit Sophos E-Mail Security

Falko Sperling
Senior Enterprise Account Executive

Martin Weiß
Senior Sales Engineer Public

SOPHOS

Oktober 1971

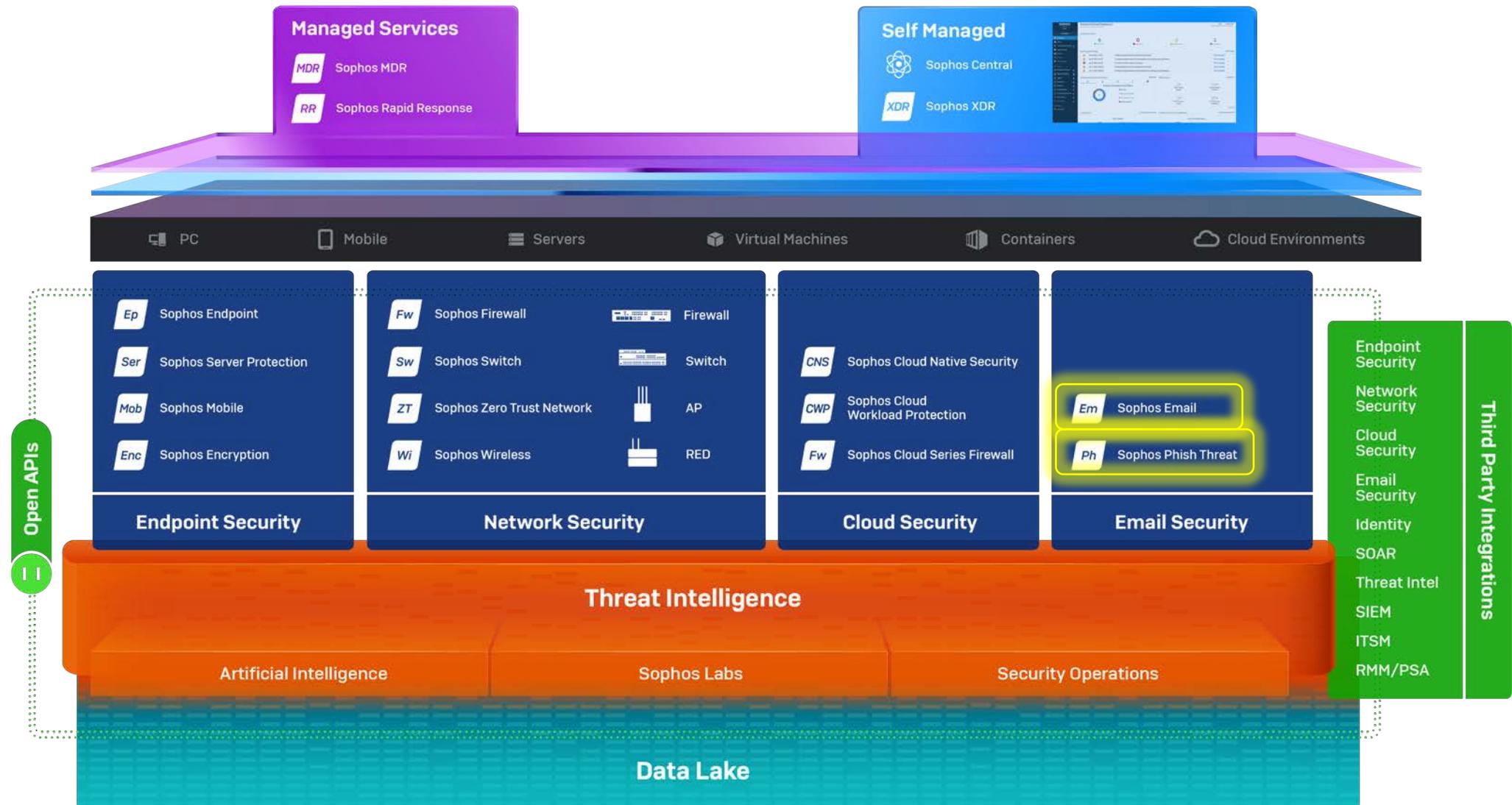
- Ray Tomlinson verschickt den ersten elektronischen Brief
- Er gilt als Erfinder der Email
- Heute werden ca. 319 Milliarden E-Mails täglich verschickt und empfangen.



3. August
1984 – Erste
E-Mail in
Deutschland
angekommen



Adaptive Cybersecurity Ecosystem



Central und Datenschutz



Cloud Computing Compliance Controls Catalogue (C5)

C5 und IT-Grundschrift führen zu einem vergleichbaren Sicherheitslevel. C5 bietet Kunden aber einen auf IT-Sicherheit und Datenschutz spezialisierten Nachweis eines detaillierten Audits der AWS Dienste, durchgeführt durch einen inländischen Auditor.

<https://aws.amazon.com/de/compliance/bsi-c5>

Sophos Central und Cloud-Dienste wie Sophos Sandstorm sind für EU-Kunden in deutschen Rechenzentren in Frankfurt am Main verfügbar

Sophos und die DSGVO

<https://www.sophos.com/de-de/legal/sophos-gdpr.aspx>

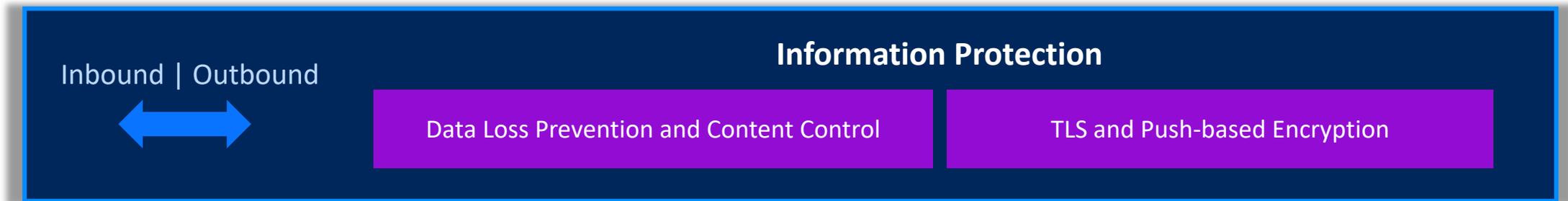
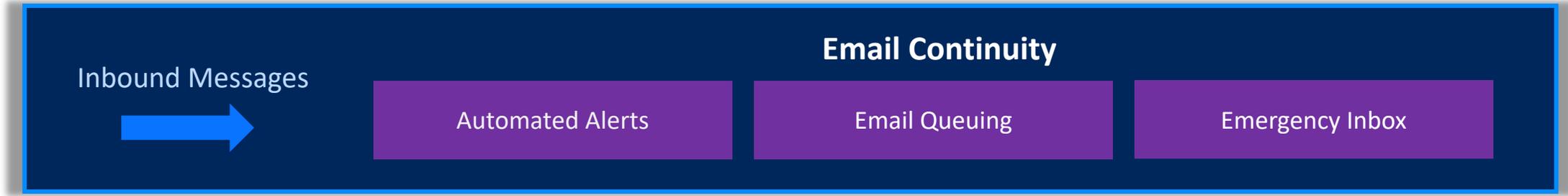
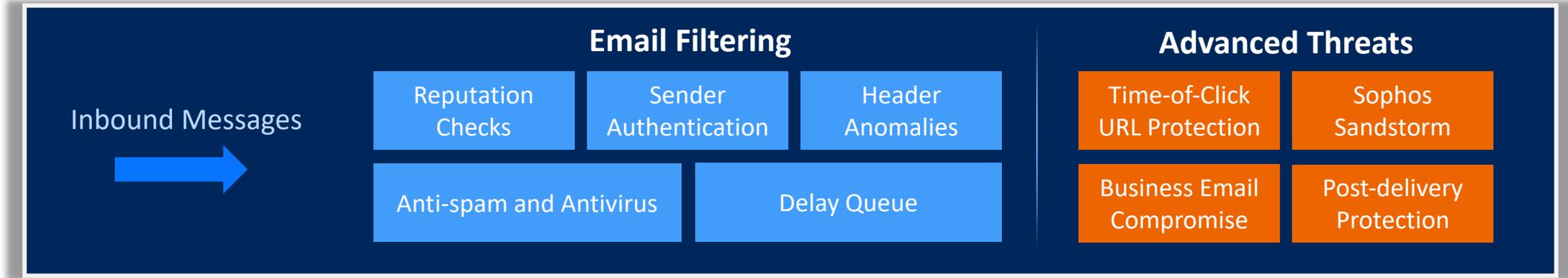
Ausführliche Beschreibung der Sicherheits-Architektur von Sophos Central

http://docs.sophos.com/central/Framework/security-framework/sc_security_framework.html

Sophos Central AVV

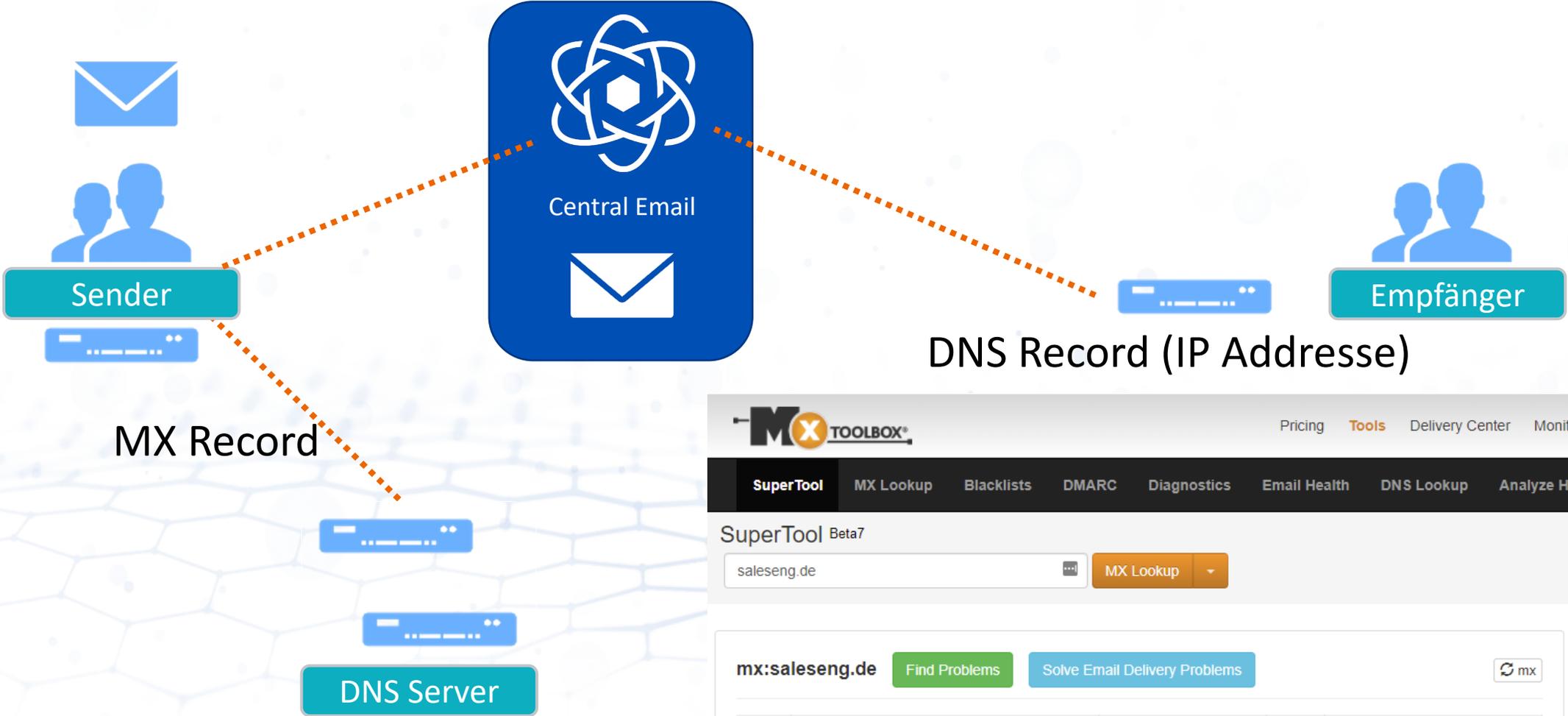
https://sophoslegal.na1.adobesign.com/public/esignWidget?wid=CBFCIBAA3AAABLblqZhD5B1GsoE2yr35Ef62AEweGNMRcn3ew6zTEAOofhgPIN_tHPXQ_ElytF8Y23XoMtyM*

Sophos Email – All in One Protection



Bereitstellung

Central Email Gateway Mode



MX TOOLBOX Pricing Tools Delivery Center Monitor

SuperTool MX Lookup Blacklists DMARC Diagnostics Email Health DNS Lookup Analyze H

SuperTool Beta7

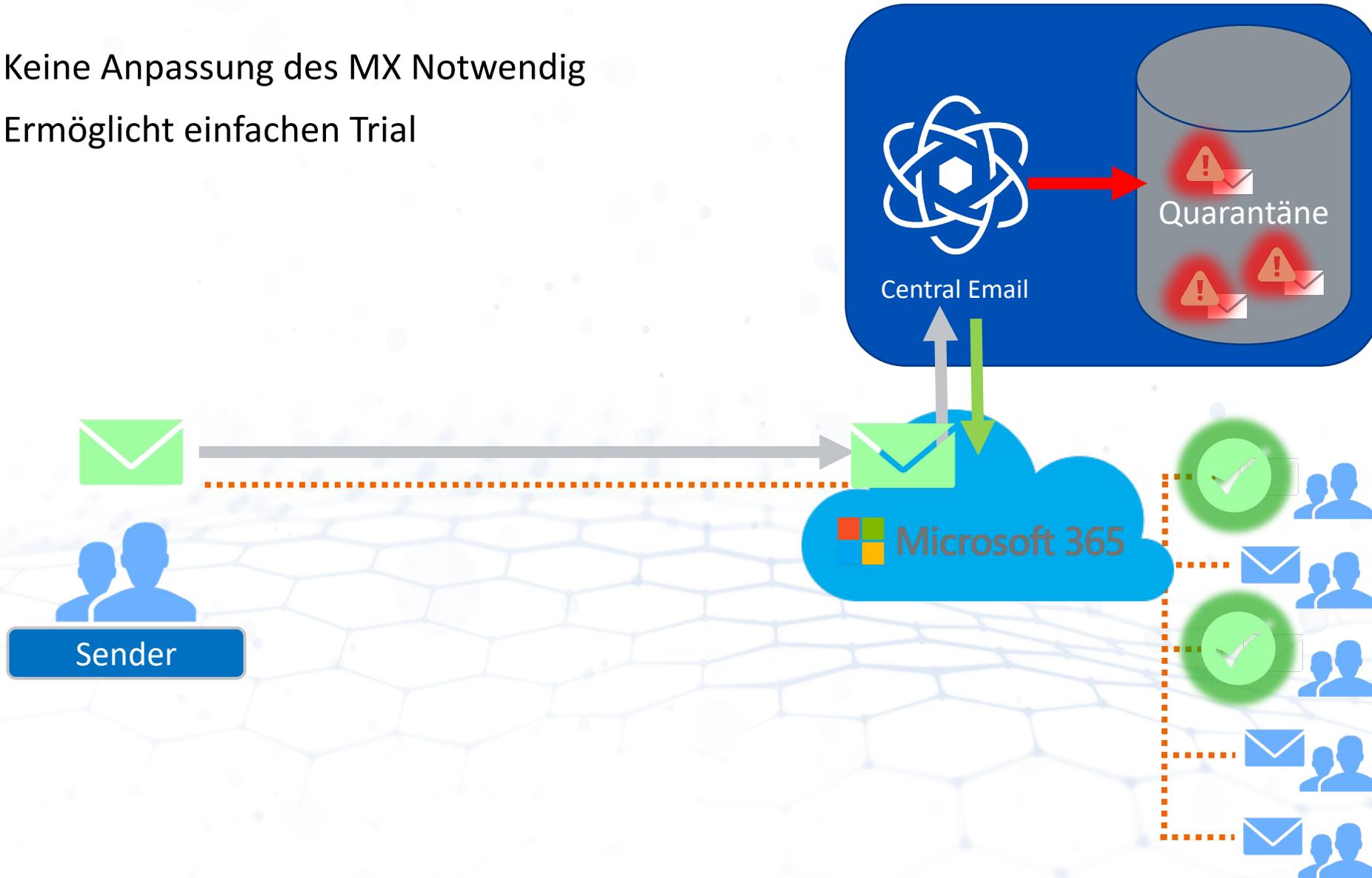
saleseng.de MX Lookup

mx:saleseng.de Find Problems Solve Email Delivery Problems mx

Pref	Hostname	IP Address	TTL		
5	mx-01-eu-central-1.prod.hydra.sophos.com	18.194.102.147 Amazon.com, Inc. (AS16509)	60 min	Blacklist Check	SMTP Test
32767	ms47579580.msv1.invalid	{No A Record}	60 min	Blacklist Check	SMTP Test

Mailflow Mode– M365

- Keine Anpassung des MX Notwendig
- Ermöglicht einfachen Trial



Identitätsübernahme

Identitätsübernahme

- Angreifer gibt sich als hochrangige Person aus
- Kommunikation sieht für das Opfer täuschend echt aus
- Angreifer überwacht und verändert Kommunikation



Geschäftsführer

Look-a-like Email-Adresse

The screenshot shows a website header for 'versicherungsmagazin' with a navigation menu including 'Abo', 'E-Magazin', 'Heftarchiv', 'Mediadaten', 'Newsletter', 'Kontakt', and 'Registrieren'. Below the header is a news article dated '28.08.2019' from the 'Branche' section, titled 'Millionenschäden durch Fake President & Co.'. The article text reads: 'Die Täuschungsdelikte „Fake President“, Besteller („Fake Identity“) und Zahlungsbetrug („Payment Diversion“) machen Unternehmen immer häufiger zu schaffen. Bei deutschen Firmen sowie deren ausländischen Töchtern verursachten diese seit 2014 Schäden von über 190 Millionen Euro. Dies ergaben Analysen des Kreditversicherers Euler Hermes.' Below the text is a graphic with the word 'HACKED' in large red letters on a blue digital background with terms like 'THEFT', 'PASSWORD', and 'CRACKER'. At the bottom of the graphic is the text '©sheelamohanachandran / Fotolia.com'.

t
mit dem GF

Deep Dive

- Envelope FROM
 - Wird in der SMTP-Übertragung (Email Server to Email Server) verwendet
 - Entspricht dem analogen Briefumschlag
- Header FROM
 - Wird in der Email im FROM oder auch Reply To: angezeigt
 - Kann einen Display-Namen beinhalten
 - Entspricht dem analogen Briefkopf



A diagram illustrating the structure of an email header, enclosed in a rectangular frame. The header fields are arranged as follows:

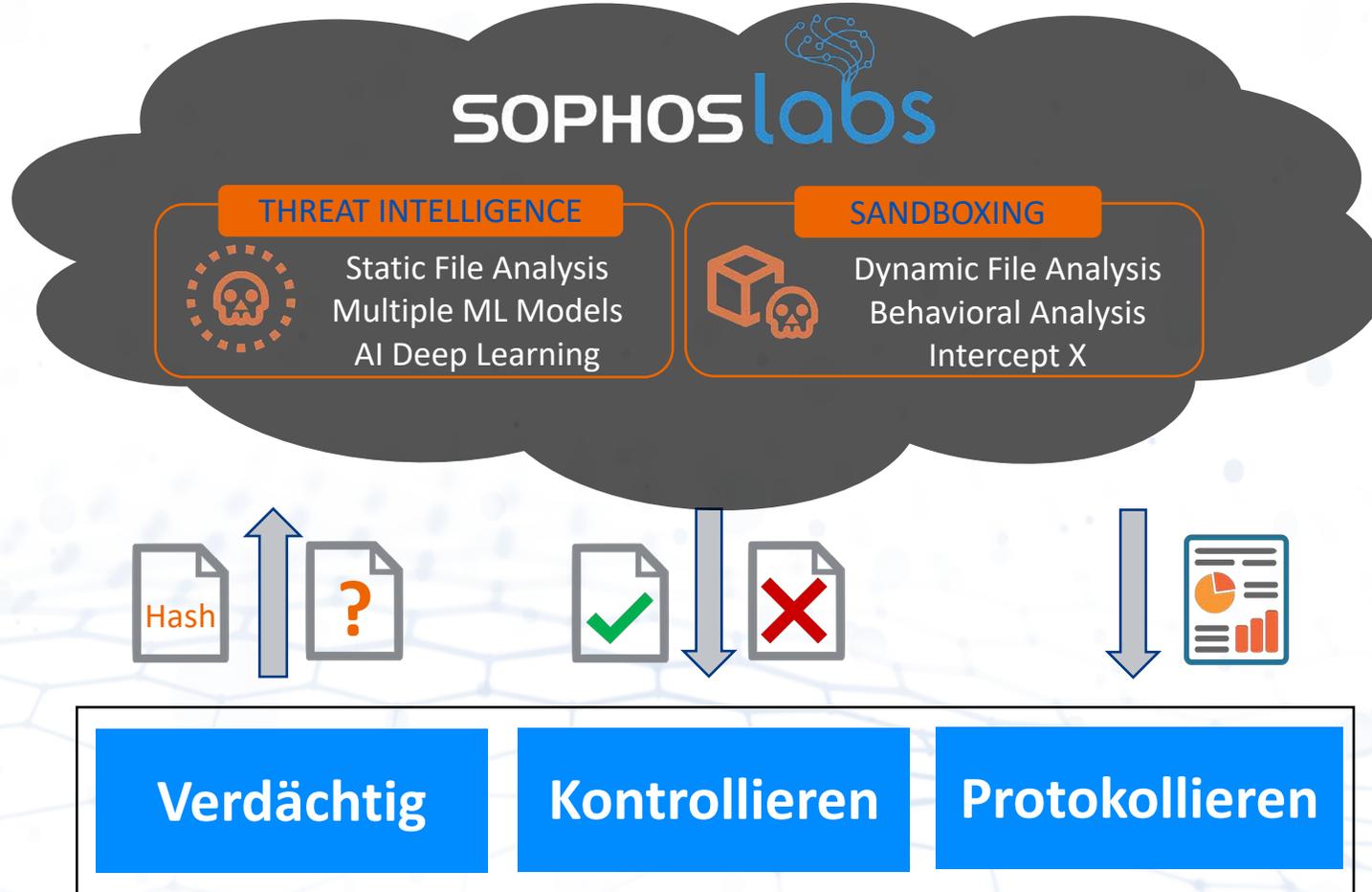
- Top right: A box containing the fields: Vorname Nachname, Telefonnummer, Mailadresse, Straße Hausnummer, PLZ ORT.
- Bottom left: The fields: Absender: Vorname Nachname • Straße • PLZ • Ort, followed by Vorname Nachname, Straße H-Nr., and PLZ Ort.
- Bottom right: The field: Ort, Datum.

Was können wir gegen Spoofing tun?

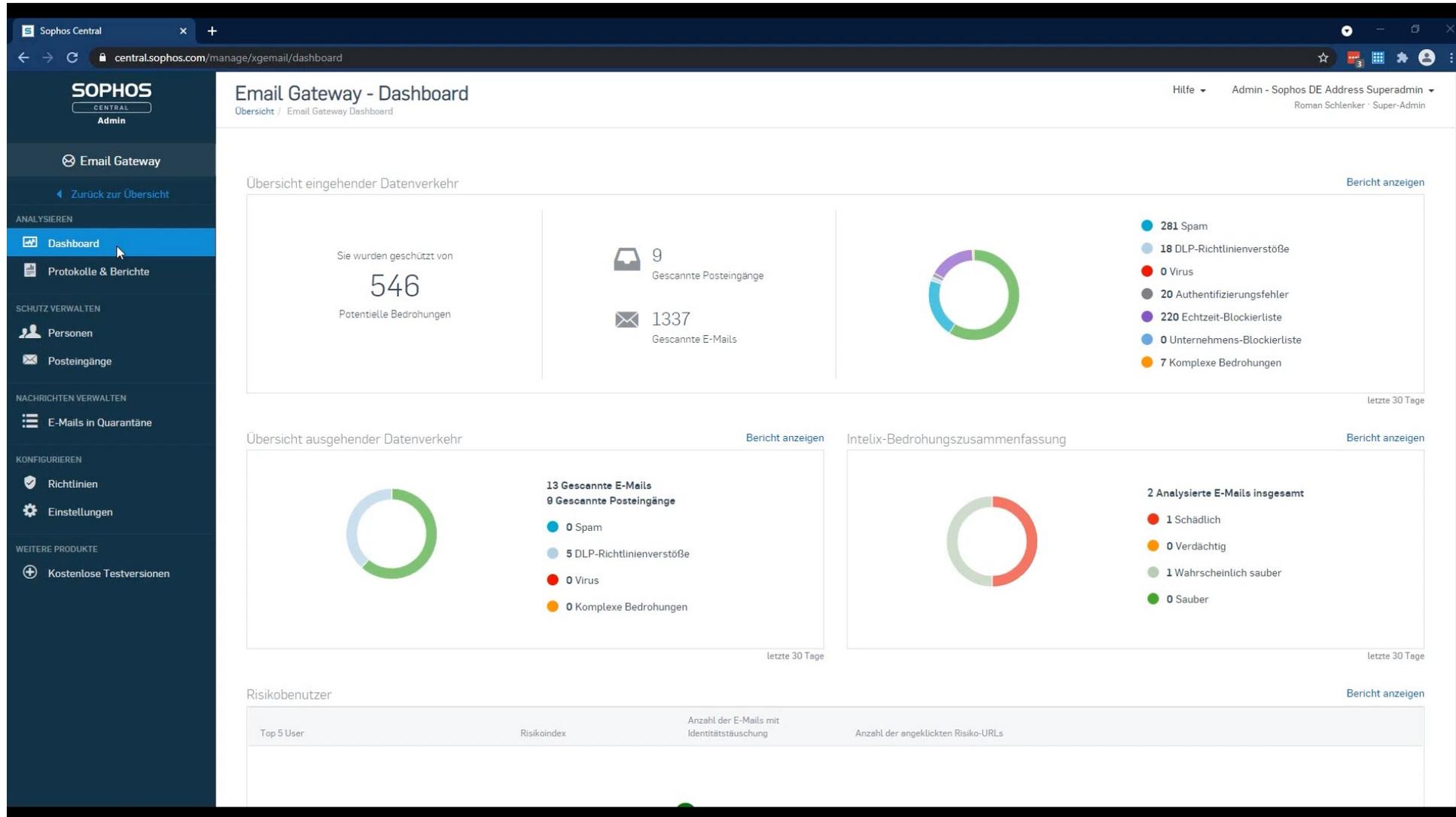
- Envelope FROM (Briefumschlag)
 - Sophos Labs - FQDN(DNS) Lookup
 - SPF (Sender Policy Framework)
 - DKIM (Domain Key Identified Mail)
- Header FROM (Briefkopf)
 - DMARC (Domain-based Message Authentication, Reporting and Conformance)
 - Impersonation Protection (Header Analyse)

Führt alle Tests durch:
DomainLookup
SPF
DMARC
DKIM
Impersonation Protection

Threat Intelligence



Threat Intelligence Report



Verschlüsselung

Arten der Email Verschlüsselung

- S/MIME
- SSL/TLS (Transport)
- Gesamte Email verschlüsseln als PDF (Content)
- Anhänge verschlüsseln als PDF (Content)
- Encryption Portal



Arten der Email Verschlüsselung

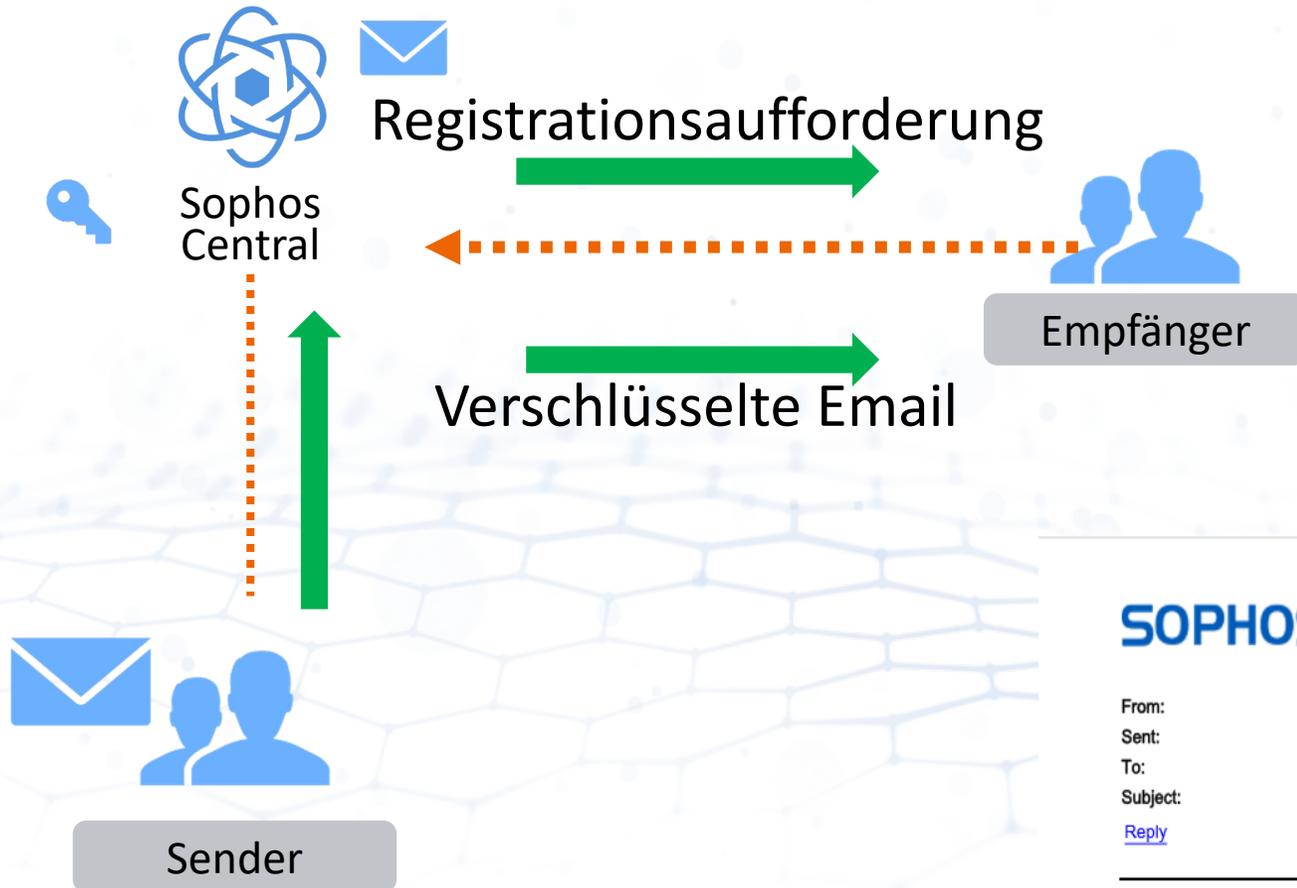
- SSL/TLS (Transport)
- Gesamte Email verschlüsseln als PDF (Content)
- Anhänge verschlüsseln als PDF (Content)
- Encryption Portal

Content Verschlüsselung



PDF Encryption

Password vorhanden?



Sophos Secure Message

SOPHOS

"acad acad" <bianca@acad.saleseng.de> has sent you an encrypted email. To view it, you need to set a Sophos Secure Message password. You'll then need to enter this password to view any email sent from the EU Central region.

You have 30 day(s) left to view this message before it expires.

- Subject : secure: Rechnung
- Sent : July 11, 2019 8:20:42 AM, GMT
- Importance: Normal
- Expires : August 10, 2019 8:20:51 AM, GMT

[Set Sophos](#) [ENCRYPTED] message.pdf 77 KB

Geben Sie ein Kennwort ein.

OK Abbrechen

- Öffnen Sie das an diese E-Mail angehängte PDF mit dem [Adobe Reader](#). Geben Sie bei entsprechender Aufforderung Ihr Kennwort ein.

SOPHOS

Sophos Secure Message

From: acad acad <bianca@acad.saleseng.de>
Sent: Thursday, 11 July 2019 08:20:42 GMT
To: Luca Christmann <Luca.Christmann@Sophos.de>
Subject: secure: Rechnung

[Reply](#)

Die Rechnung!

SOPHOS

Portal Encryption

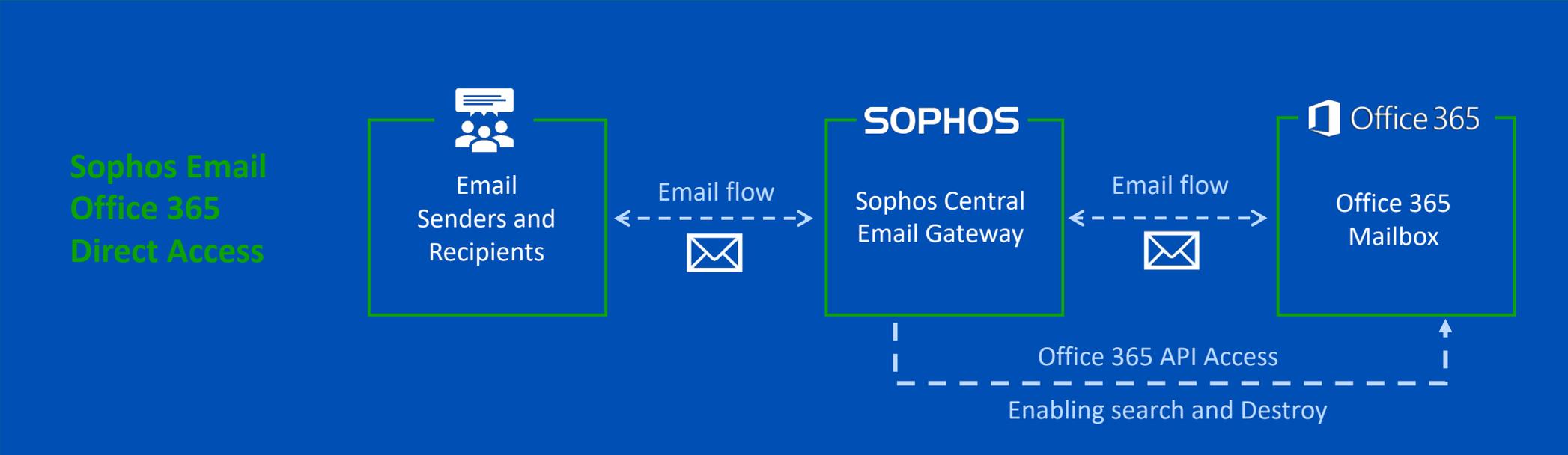
- Portal Encryption – auch als Pull-Verschlüsselung bekannt
- Verschlüsselte E-Mails über ein Web-Portal sicher zustellen
- Plattformunabhängig da komplett webbasiert
- Sehr schnelle und einfache Aktivierung

Portal Encryption Video

The screenshot displays the Sophos Central Email Gateway Dashboard. The interface is divided into several sections:

- Header:** Shows the user is logged in as 'Admin - Sophos DE Address Superadmin' with a sub-user 'Roman Schlenker - Super-Admin'.
- Left Sidebar:** Contains navigation options for 'Email Gateway', 'Zurück zur Übersicht', 'ANALYSIEREN' (Dashboard, Protokolle & Berichte), 'SCHUTZ VERWALTEN' (Personen, Posteingänge), 'NACHRICHTEN VERWALTEN' (E-Mails in Quarantäne), 'KONFIGURIEREN' (Richtlinien, Einstellungen), and 'WEITERE PRODUKTE' (Kostenlose Testversionen).
- Overview Incoming Data Traffic (Übersicht eingehender Datenverkehr):**
 - Shows 342 potential threats (Potentielle Bedrohungen).
 - 15 scanned mailboxes (Gescannte Posteingänge).
 - 1009 scanned emails (Gescannte E-Mails).
 - Donut chart showing threat distribution: 278 Spam, 18 DLP-Richtlinienverstöße, 0 Virus, 14 Authentifizierungsfehler, 21 Echtzeit-Blockierliste, 0 Unternehmens-Blockierliste, 11 Komplexe Bedrohungen.
- Overview Outgoing Data Traffic (Übersicht ausgehender Datenverkehr):**
 - 17 scanned emails (Gescannte E-Mails).
 - 15 scanned mailboxes (Gescannte Posteingänge).
 - Donut chart showing threat distribution: 0 Spam, 5 DLP-Richtlinienverstöße, 0 Virus, 0 Komplexe Bedrohungen.
- Intelix-Threat Summary (Intelix-Bedrohungszusammenfassung):**
 - 2 analyzed emails in total (2 Analysierte E-Mails insgesamt).
 - 1 Harmful (1 Schädlich), 0 Suspicious (0 Verdächtig), 1 Probably safe (1 Wahrscheinlich sauber), 0 Safe (0 Sauber).
- Risk Users (Risikobnutzer):** A table with columns for 'Top 5 User', 'Risikoindex', 'Anzahl der E-Mails mit Identitätstauschung', and 'Anzahl der angeklickten Risiko-URLs'.

Microsoft Office 365 Direct Access (Search and Destroy)



Nachrichtenverlauf

Reporting - Nachrichtenverlauf

The screenshot displays the Sophos Central Admin interface for the Email Gateway. The browser address bar shows `central.sophos.com/manage/xgmail/reports`. The page title is "Email Gateway - Protokolle & Berichte". The left sidebar contains navigation options: "Email Gateway", "Zurück zur Übersicht", "ANALYSIEREN" (Dashboard, Protokolle & Berichte), "SCHUTZ VERWALTEN" (Personen, Posteingänge), "NACHRICHTEN VERWALTEN" (E-Mails in Quarantäne), "KONFIGURIEREN" (Richtlinien, Einstellungen), and "WEITERE PRODUKTE" (Kostenlose Testversionen). The main content area is divided into two sections: "Protokolle" and "Berichte". Under "Protokolle", there is a link for "Email Security-Protokolle" with the sub-link "Nachrichtenverlauf" and a description: "Zeigt das Protokoll aller vom System verarbeiteten E-Mails an." Under "Berichte", there is a link for "Email Security" with the sub-link "Nachrichtenübersicht" and a description: "Hier wird eine Übersicht aller E-Mails angezeigt." Below this, several report types are listed: "Intelix-Bedrohungszusammenfassung" (Anzeige einer Zusammenfassung eingehender Nachrichten, die mittels statischer und dynamischer Analyse auf Bedrohungen untersucht wurden), "Time-of-Click-Zusammenfassung" (Zeigt eine Zusammenfassung der Time-of-Click-Aktivität), "Risikobnutzer" (Erkennen Sie die am meisten gefährdeten Benutzer in Ihrem Unternehmen), "Verstöße gegen die Data-Loss-Prevention-Richtlinien" (Anzeige eines Berichts der von Data-Loss-Prevention-Richtlinien protokollierten Nachrichten), and "Nach-der-Zustellung-Übersicht" (Zeigt eine Übersicht der nach der Zustellung entfernten Nachrichten).

Nachrichtenübersicht

Reporting - Nachrichtenübersicht

The screenshot displays the Sophos Central Email Gateway Dashboard. The interface is divided into several sections:

- Header:** Shows the user is logged in as 'Admin - Sophos DE Address Superadmin' (Roman Schlenker - Super-Admin).
- Left Sidebar:** Contains navigation options like 'Email Gateway', 'Zurück zur Übersicht', 'ANALYSIEREN' (with 'Dashboard' selected), 'SCHUTZ VERWALTEN' (Personen, Posteingänge), 'NACHRICHTEN VERWALTEN' (E-Mails in Quarantäne), 'KONFIGURIEREN' (Richtlinien, Einstellungen), and 'WEITERE PRODUKTE' (Kostenlose Testversionen).
- Dashboard Overview:**
 - Übersicht eingehender Datenverkehr:** Shows 611 potential threats, 8 incoming mailboxes, and 1385 incoming emails. A donut chart breaks down threats into: 274 Spam, 0 DLP-Richtlinienverstöße, 0 Virus, 17 Authentifizierungsfehler, 316 Echtzeit-Blockierliste, 0 Unternehmens-Blockierliste, and 4 Komplexe Bedrohungen.
 - Übersicht ausgehender Datenverkehr:** Shows 4 outgoing emails and 8 outgoing mailboxes. Legend: 0 Spam, 0 DLP-Richtlinienverstöße, 0 Virus, 0 Komplexe Bedrohungen.
 - Intelix-Bedrohungszusammenfassung:** Currently shows 'Aktuell keine erweiterte Bedrohungsübersicht anzuzeigen.'
- Risikobnutzer:** A table listing the top 5 users based on risk index, number of emails with identity spoofing, and number of clicked risk URLs.

Admin Quarantäne und User Quarantäne

Admin Quarantäne und User Quarantäne

SOPHOS CENTRAL Admin

Email Gateway - Dashboard
Übersicht / Email Gateway Dashboard

Hilfe Admin - Sophos DE Address Superadmin Roman Schlenker - Super-Admin

Übersicht eingehender Datenverkehr

Sie wurden geschützt von **625** Potentielle Bedrohungen

9 Gescannte Posteingänge

1415 Gescannte E-Mails

290 Spam
18 DLP-Richtlinienverstöße
0 Virus
20 Authentifizierungsfehler
294 Echtzeit-Blockierliste
0 Unternehmens-Blockierliste
3 Komplexe Bedrohungen

letzte 30 Tage

Übersicht ausgehender Datenverkehr

10 Gescannte E-Mails
9 Gescannte Posteingänge

0 Spam
4 DLP-Richtlinienverstöße
0 Virus
0 Komplexe Bedrohungen

letzte 30 Tage

Intelix-Bedrohungszusammenfassung

Aktuell keine erweiterte Bedrohungsübersicht anzuzeigen.

letzte 30 Tage

Risikobnutzer

Top 5 User	Risikoindex	Anzahl der E-Mails mit Identitätstauschung	Anzahl der angeklickten Risiko-URLs

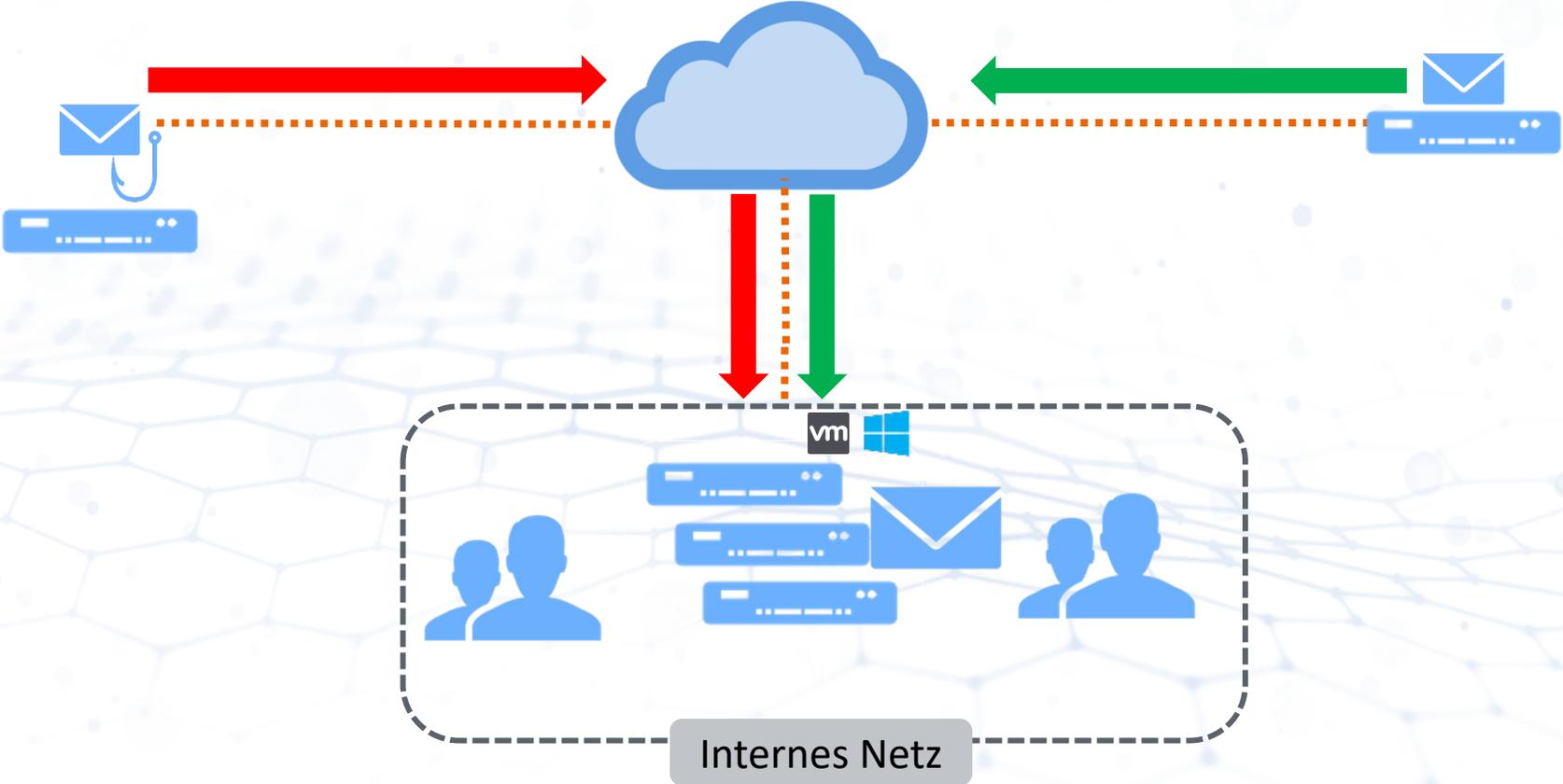
Post Delivery Protection

Post Delivery Protection

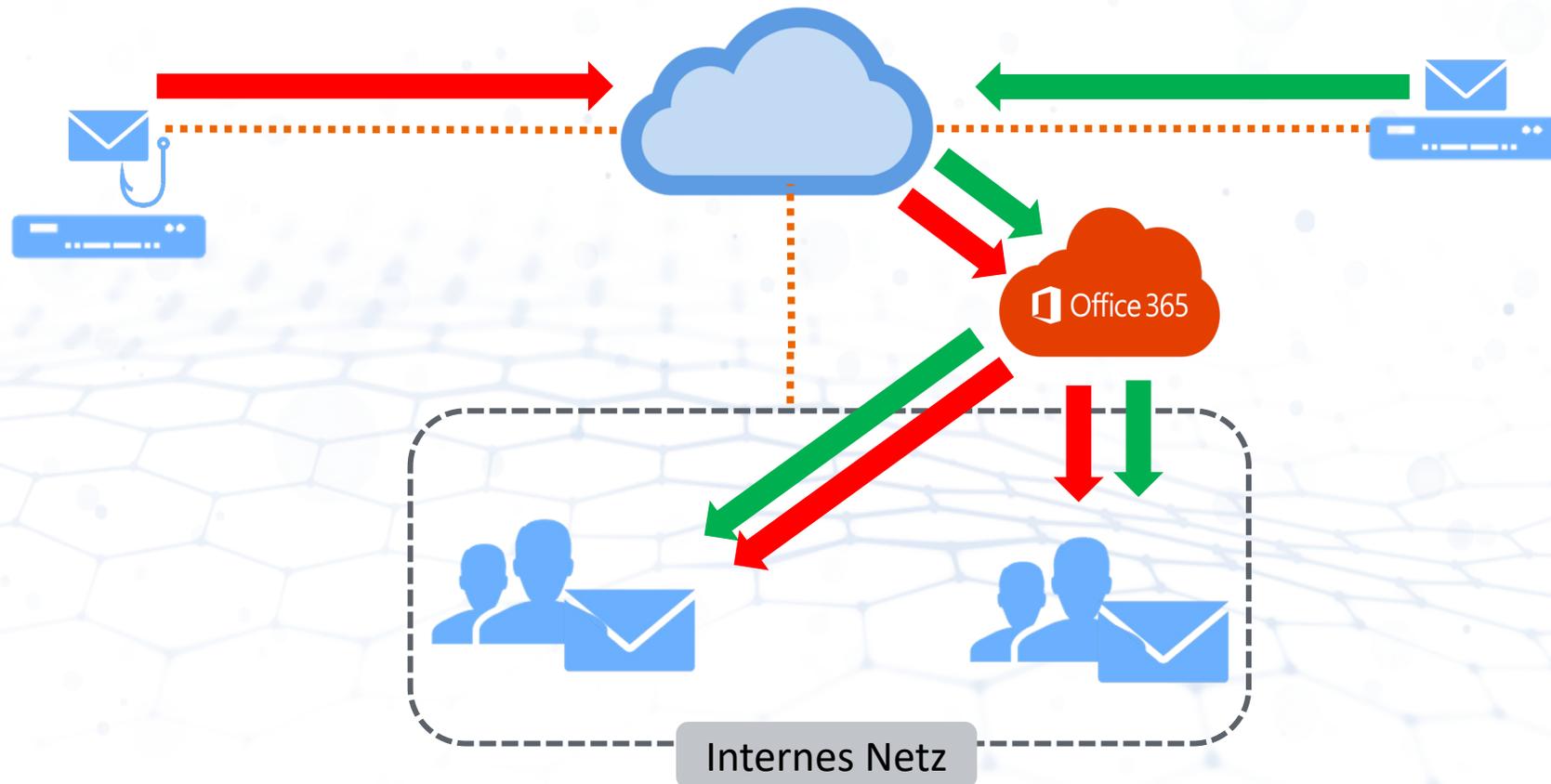
The image displays two screenshots of the Microsoft Outlook interface, illustrating the 'Post Delivery Protection' feature. The left screenshot shows the 'Posteingang' (Inbox) view with a 'Quarantäne-Übersicht' (Quarantine Overview) section. This section lists isolated emails with their status (e.g., [NIEDRIG] Alarm für Sophos Central) and provides a link to 'Isolierte E-Mails verwalten' (Manage isolated emails). The right screenshot shows the 'Isolierte E-Mails seit Mar 08, 2021 06:00 AM für roman.schlenker@sophos.com' (Isolated emails since Mar 08, 2021 06:00 AM for roman.schlenker@sophos.com) view. This view displays a list of isolated emails with columns for 'BETREFF' (Subject), 'VON' (From), 'EMPFANGEN' (Received), and 'MASSNAHME' (Action). The list includes emails from 'Spring', 'Louis', 'Vuitton', 'Handbags Special', 'Deal 80%', 'OFF!', 'johannes herda', and 'kaufen Sie Martini'. Each email entry includes the sender's name, email address, and the date and time it was received. The interface also shows standard Outlook navigation elements like 'Suchen' (Search), 'Neue Nachricht' (New Message), and various folder views.

Einrichtung und Verwaltung

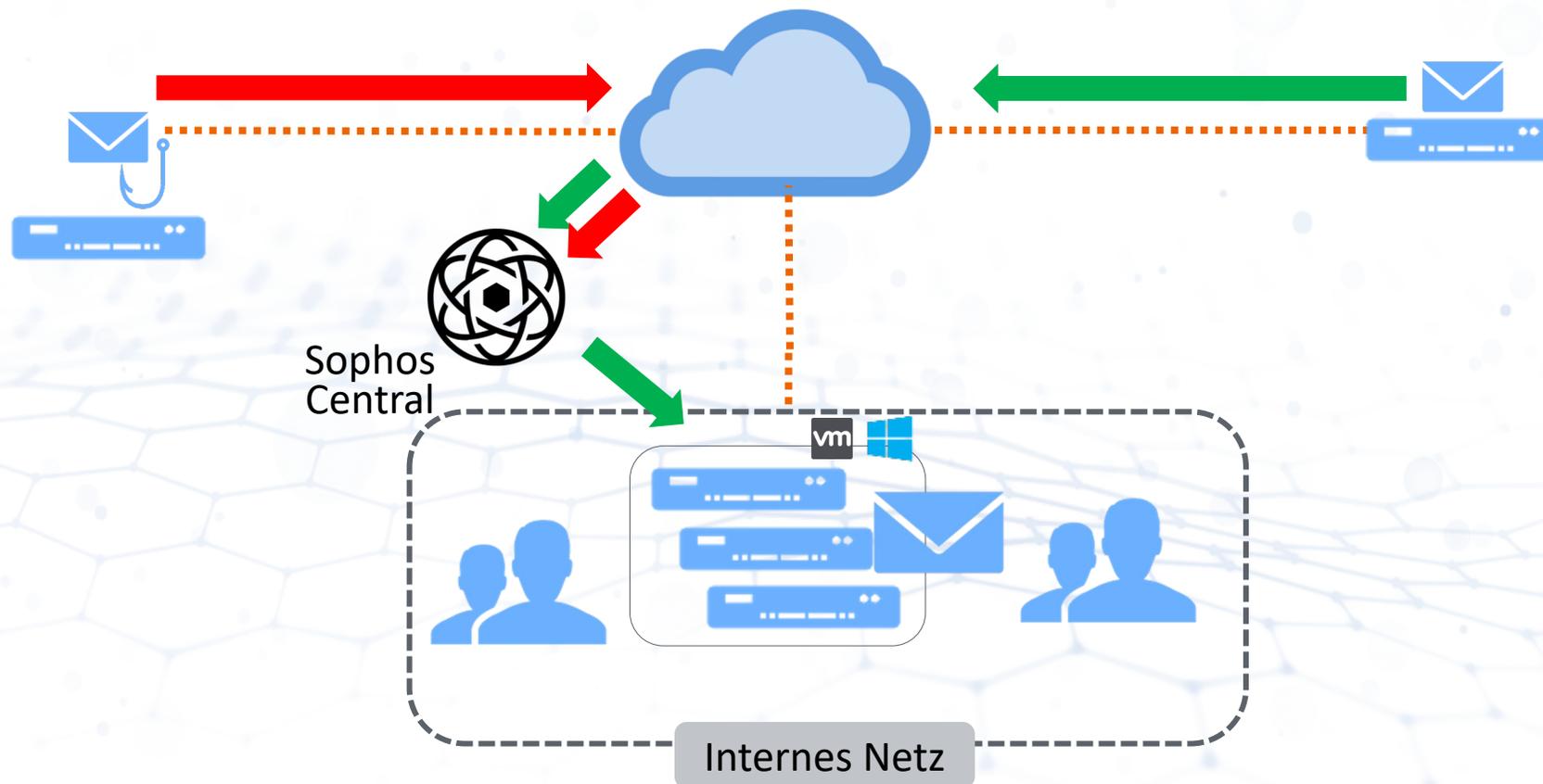
Email Umgebung – On Premise



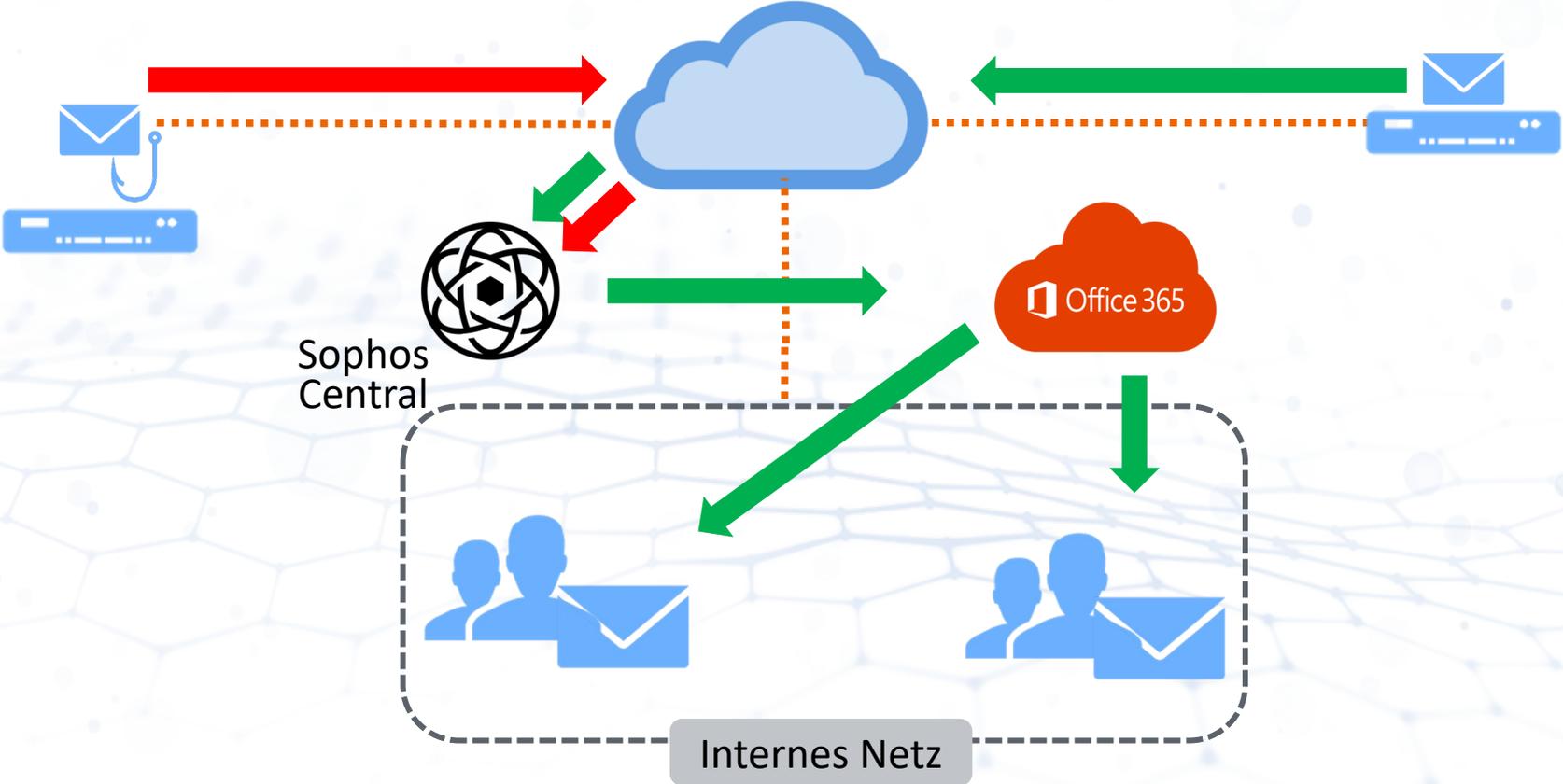
Email Umgebung – Office 365



Email Umgebung – On Premise



Email Umgebung – Office 365



Konfiguration

- Vorbereitung:
 - Hinzufügen eines DNS TXT Records zur Mail Domäne
 - Hinzufügen der Email Postfächer in Central
 - Mail Richtlinie konfigurieren
- Migration
 - Eigenen Mailserver / Online-Email-Dienst konfigurieren
 - MX Record umziehen
- Die Postfächer in Central Email können
 - synchronisiert werden via AD Sync oder Azure AD Sync
 - importiert werden via CSV Import
 - manuell angelegt werden

Postfächer

■ Postfachtyp:

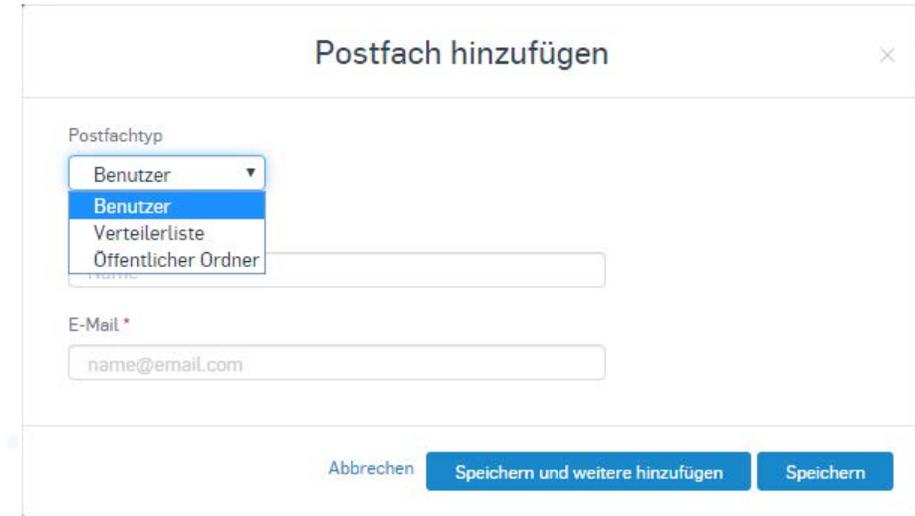
- Benutzer (User Mailbox)
- Verteilerliste (Distribution List)
- Öffentlicher Ordner (Public Folder)

■ Lizenzierung:

- Benutzer Postfächer (User Mailboxes) benötigen eine Lizenz
- Verteilerliste / Öffentliche Ordner benötigen keine Lizenz
- Shared Mailboxes (Microsoft) sind „Benutzer Postfächer“ und benötigen eine Lizenz

■ Shared Mailboxes

- „deaktivierte“ Benutzer im Microsoft AD
- Kein AD Sync aktuell möglich
- Müssen via CSV Import erstellt werden



Postfach hinzufügen

Postfachtyp

Benutzer

Benutzer

Verteilerliste

Öffentlicher Ordner

E-Mail *

name@email.com

Abbrechen Speichern und weitere hinzufügen Speichern

Domäneneinstellungen/Status

Email Gateway - Domäneinstellungen/Status

Übersicht / Email Gateway Dashboard / Systemeinstellungen / Email Security: Domäneinstellungen/Status

Hilfe ▾ Sophos Academy ▾

Sophos Central Academy 2019 - Superadmin



Domain bearbeiten



DOMAIN ÜBERPRÜFEN

E-MAIL-DOMÄNE*

acad.saleseng.de

DOMAIN KONFIGURIEREN

RICHTUNG*

Nur eingehend Eingehend und ausgehend

INBOUND-ZIEL*

E-Mail-Host

IP/FQDN*

saleseng.de

PORT*

25

OUTBOUND-GATEWAY*

Custom Gateway

IP/CIDR* (1)

IP/CIDR

Hinzufügen

51.144.76.249



[Vorgängigkeiten konfigurieren](#) | [Domäne hinzufügen](#)

URSPRUNG

Gateway



Abbrechen

Speichern

Domäneneinstellungen/Status

Domänenbesitz verifizieren



Um den Eigentümer der Domäne zu verifizieren, fügen Sie den nachfolgenden TXT-Eintrag zu Ihrem nach außen gerichteten DNS hinzu. Geben Sie Ihren E-Mail-Domännennamen als Name für den TXT-Eintrag ein. Je nach DNS-Anbieter können Sie das Feld entweder leer lassen oder @ für Root-Domänen eingeben. Geben Sie bei einer Subdomäne yoursubdomain.yourdomain.com als Name des TXT-Eintrags und den TXT-Wert ein.

Klicken Sie nach dem Hinzufügen des DNS TXT-Eintrags auf die Schaltfläche „Verifizieren“.

TXT-Wert	sophos-domain-verification=307575156b1289c63e1ba1055648ada8cedb6bf1
TTL	600

Hinweis: Das Hinzufügen und die Übernahme des Eintrags kann 5-10 Minuten dauern und hat keine Auswirkung auf Ihre E-Mail- oder sonstigen Dienste.

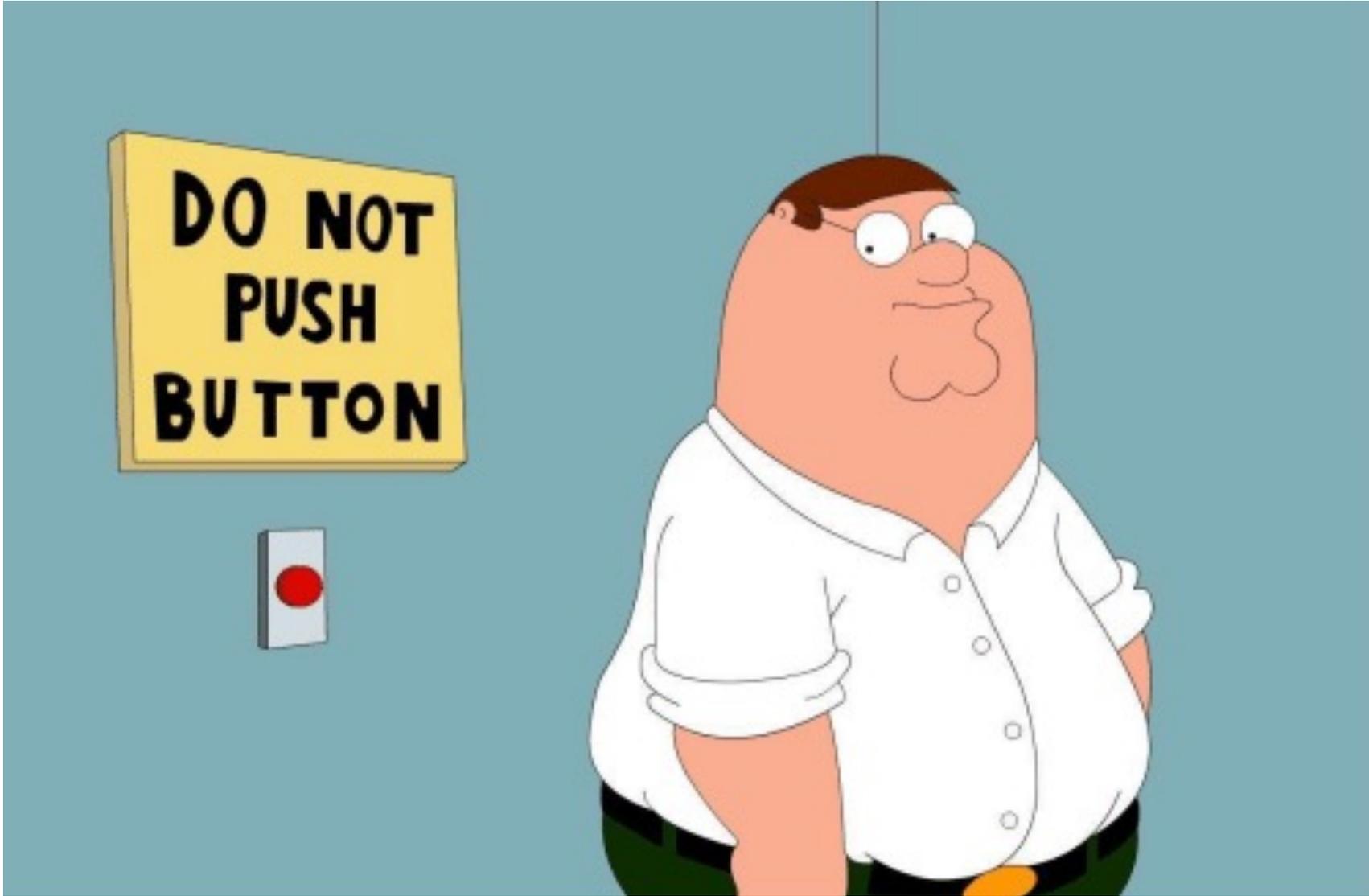
Überprüfen

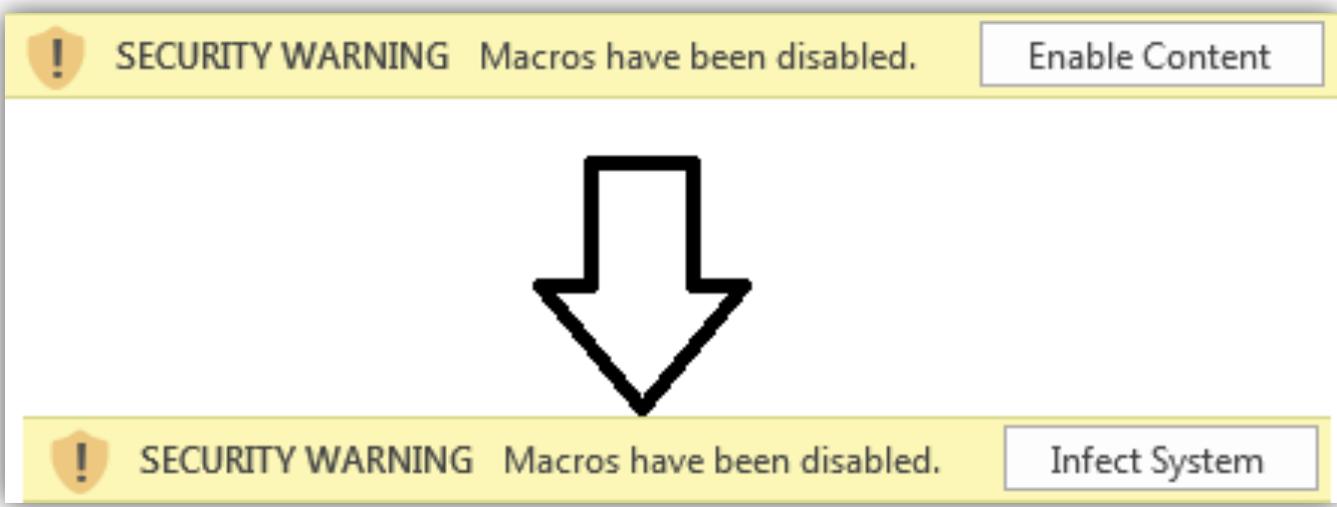
```
Microsoft Windows [Version 10.0.18362.239]
(c) 2019 Microsoft Corporation. Alle Rechte vorbehalten.
C:\Users\lucachristmann>nslookup -q=txt acad.saleseng.de
```

```
Nicht autorisierende Antwort:
acad.saleseng.de      text =
```

```
"sophos-domain-verification=307575156b1289c63e1ba1055648ada8cedb6bf1"
```

Phishing-Emails sind Einfallsweg #1 für Ransomware





Benutzer sind oft das
schwächste Glied
in der Abwehrkette





SPAM Quiz



eBay-Support <support@e.baycom.co>

Falko Sperling

29.06.2017

Congratulation! You Are The Winner Of a Discount Coupon For 90%



This message is from a trusted sender.



You Are The Winner Of a Discount Coupon For 90%!

Coupon ID : 695F6D356FI1

Dear Falko,

This is a random selection from ebay.com on the occasion of our 20th birthday we selected more than one million customers in first step then we have chosen just ten thousand other customers also randomly to be winner of discount coupon for **90%**.

This coupon is valid for all eBay product take it in the link below.

[Get Coupon Code](#)

Note:

- **The link of the coupon will expire within 24 hour from now.**
- **The coupon validity is 30 days.**

eBay, support team.
<http://www.ebay.com>



This email was intended for martin.weiss@sophos.de

SOPHOS



Hi Martin,

We are extremely pleased to inform you that as a part of great initiative to make our people happy and rejuvenating at work place, we are in process of launching SPA facility for our people and its **FREE**

We highly encourage you to register your interest to make this initiative a grand success. The details of How and when will be shared soon, so stay tuned!

Don't miss a chance to register!

Team Sophos.

Sign up today

Date: Friday, Dec 13, 2019

Location: Coming Soon!

Cost: Free!



Jan Vogel

23.06.2016 09:05

Bewerbung

An: kontakt@tb-medienproduktion.de



Bewerbung.zip
3.74 KB

Sehr geehrte Damen und Herren,

anbei erhalten Sie meine Bewerbung für Ihre bei meinestadt.de ausgeschriebene Stelle. Warum ich die Stelle optimal ausfüllen kann und Ihrem Unternehmen durch meine Erfahrung zahlreiche Vorteile biete, entnehmen Sie bitte meinen ausführlichen und angehängten Bewerbungsunterlagen.

Ich freue mich, wenn ich mich Ihnen noch einmal persönlich vorstellen kann.

Mit freundlichen Grüßen,

Jan Vogel



Alexandra-Danae Wassenhoven via XING <mailrobot@mail.xing.com>

Falko Sperling

12:26

Neuer Moderatorenbeitrag der Gruppe IT & Data - XING Ambassador Community: IT & Data März Highlights

 If there are problems with how this message is displayed, click here to view it in a web browser.

XING

Neuer Moderatorenbeitrag der Gruppe **IT & Data** - **XING Ambassador Community**

Moderator-Info



IT-Connection: Ideen, Vorschläge & Feedback ***Nur Diskussion keine Werbung /
Jobs 07.03.2018, 12:18

IT & Data März Highlights

Liebe IT & Data - XING Ambassador Community,
hier haben wir für Sie die aktuellen News aus der Gruppe zusammengefasst

Aus dem Forum:

Cyberisiken sind kaum noch abzuwehren

<https://www.xing.com/communities/posts/cyberisiken-sind-kaum-noch-abzuwehren-1014418153>



Sophos Healthcare <healthcare@s0phos.net>

Falko Sperling

27.07.2017

Revised Healthcare Policy



Dear Falko,

We have updated our healthcare policy provided to you on behalf of SOPHOS TECHNOLOGIES.

We request you to kindly login to our [Sophos HealthCare](#) portal and download your updated healthcare policy.

Warm Regards,
Sophos Management Team

"We care for your health"

M: (+91) 7881 340225

SOPHOS

Security made simple.



Network Protection



Enduser Protection



Server Protection

**Shareworks Notification - Invite for online account activation**

Dear Participant,

Welcome to the Sophos Share portal, a new digital tool that allows you to easily manage your share awards.

To access the portal, please first activate your account by clicking [here](#) where you will be asked to confirm your employee number.

Once your account has been activated, you can access the digital portal at any time.

For any related queries, please contact your HR.

Should you require assistance accessing the portal, please contact Global Service Desk. If you have a query about the functionality of the portal, contact Solium at:

Free Phone - United Kingdom	0800 088 5912 (8am to 6pm GMT)
Direct Dial - United Kingdom	020 3751 5668 (8am to 6pm GMT)
Free Phone - North America	1.877.380.7793 (8am to 8 pm EST)
Direct Dial - North America	1800.768.002 (9.30am to 4:30pm Australian EST)
International	1+ 403.515.3956 (8am to 8pm EST)
Email	help.emea@solium.com

Thank you,

The Solium Team



IT Helpdesk <it@sophos-helpdesk.com>

Falko Sperling

31.05.2017

Email Storage Warning



Dear Falko,

Your mailbox (falko.sperling@sophos.de) is almost full.



Please increase your mailbox size by clicking on [Mailbox Quota](#) and filling out the necessary mailbox requirement to increase your quota size.

IMPORTANT NOTE: You won't be able to receive email messages at 2020Mb.

IT Helpdesk Team
SOPHOS

SOPHOS

Phish Threat Kampagnen

- Trainings-Kampagnen
- Überprüfung durch Phishing-Test-E-mails

Sprache auswählen

Das ist die Sprache für Ihre E-Mails und Trainingsmaterialien

Deutsch ▼

- Deutsch
- English
- Español
- Français
- 日本語
- 繁體中文
- Italiano
- 한국어
- Nederlands
- Português (Brasil)
- Português (Portugal)

Kampagnentyp auswählen



Phishing

Benutzer dazu bringen, auf einen Link in einer E-Mail zu klicken



Diebstahl von Zugangsdaten

Benutzer dazu bringen, Zugangsdaten auf einer gefälschten Website einzugeben Hinweis: Es werden keine Kennwörter erfasst.



Anhang

Benutzer dazu bringen, einen Anhang in einer E-Mail zu öffnen



Was bieten unsere Trainings?

Benutzer für Pflichttraining basierend auf ausgewählten Trainingsmodulen anmelden

Viele aktuelle Vorlagen



Ihre E-Mail-Adresse für die Wiederherstellung wurde geändert

Guten Tag {FirstName},
Die E-Mail-Adresse für die Wiederherstellung für Ihr Konto {Email} wurde vor kurzem geändert.

Haben Sie das veranlasst?
Überprüfen Sie jetzt Ihre [kürzlich verwendeten Geräte](#).

Mit freundlichen Grüßen
Das Google Accounts Team

Diese E-Mail-Adresse kann keine Antworten empfangen. Nähere Informationen erhalten Sie im [Google Accounts Hilfecenter](#).

Sie haben diese vorgeschriebene E-Mail-Benachrichtigung erhalten, weil sie Informationen über wichtige Veränderungen im Zusammenhang mit Ihrem Google Produkt oder Konto enthält.

Google Inc., Mountain View, CA 94043 USA



Referenznummer: P-563D-1E36-4997-92D1



Aktualisierung des Kontostatus
Ändern Sie Ihr Passwort und die Sicherheitsfragen

Loggen sie sich so bald wie möglich in Ihr PayPal-Konto ein

Guten Tag {FirstName},

Wir haben in Ihrem PayPal-Konto ungewöhnliche Aktivitäten festgestellt. Loggen Sie sich bei PayPal ein, um Ihre Identität zu bestätigen und Ihr Passwort und die Sicherheitsfragen zu aktualisieren.

Zum Schutz Ihres Kontos kann niemand Geld senden oder Geld abbuchen. Außerdem kann niemand Geld auf Ihr Konto einzahlen, Kreditkarte hinzufügen, Bankkonto hinzufügen, Bankkonten entfernen, Kreditkarten entfernen, Rückzahlungen senden, oder Konto schließen.

Was ist los?

Hat jemand ohne Ihr Wissen Ihr PayPal-Konto verwendet? Wir haben in Ihrem PayPal-Konto ungewöhnliche Aktivitäten festgestellt.

Hi {FirstName},

Können Sie das heute noch einmal überprüfen? Bitte bewahren Sie es vertraulich auf.

Lida



Dieser Link funktioniert nur für die direkten Empfänger dieser Nachricht.



MitarbeiterLeistungsplan

Zuletzt geändert am 06:48:02



Microsoft respektiert Ihre Privatsphäre. Um mehr zu erfahren, lesen Sie bitte unsere [Datenschutzerklärung](#).
Microsoft Corporation, Redmond, WA 98052



Guten Tag {FirstName},

wir konnten Ihr/e Paket/e nicht zustellen!

Befolgen Sie bitte die Anweisungen in dem angehängten Beleg über die nicht zustellbare Lieferung, damit unsere Fahrer einen neuen Zustellversuch unternehmen können oder Sie Ihr Paket in Ihrer DHL-Niederlassung abholen können.

Hinweis:

Wir können Ihnen auch den Zustellvermerk zusenden, damit Sie ihn ausdrucken und bei Ihrer Postfiliale vorlegen können, wenn Sie Ihr Paket abholen.

DHL EXPRESS - Good for Business

© DHL International GmbH. Alle Rechte vorbehalten

Deutsche Post DHL Group



Hallo {FirstName},
ich möchte mich gerne auf LinkedIn mit Ihnen verbinden.

Renae Harris
Recruiting, Career & Salary Specialist

Annehmen

Profil anschauen

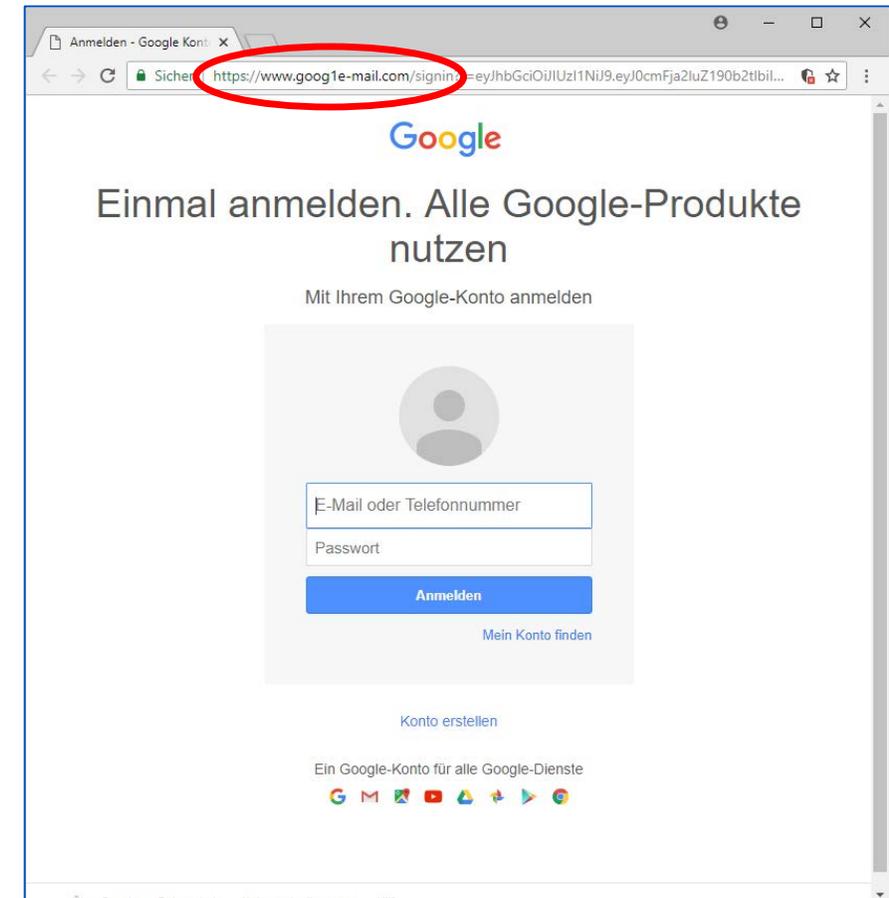
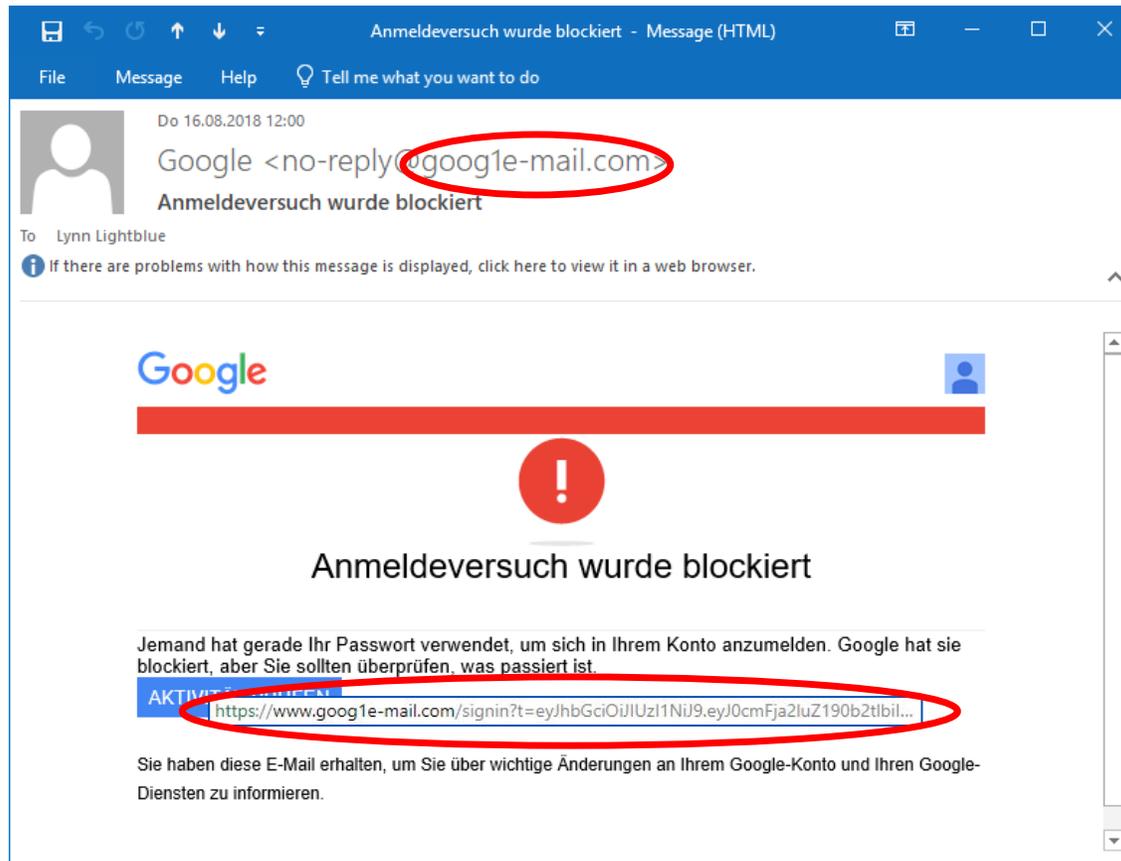
Sie erhalten Einladungs-E-Mails. [Abbestellen](#).

Diese E-Mail ist für {FirstName} {LastName} bestimmt. [Erfahren Sie, warum wir darauf hinweisen](#). © 2015, LinkedIn Corporation. 2029 Stierlin Ct. Mountain View, CA 94043, USA

Phish Threat Kampagnen - Zugangsdatendiebstahl

Es wird überprüft,

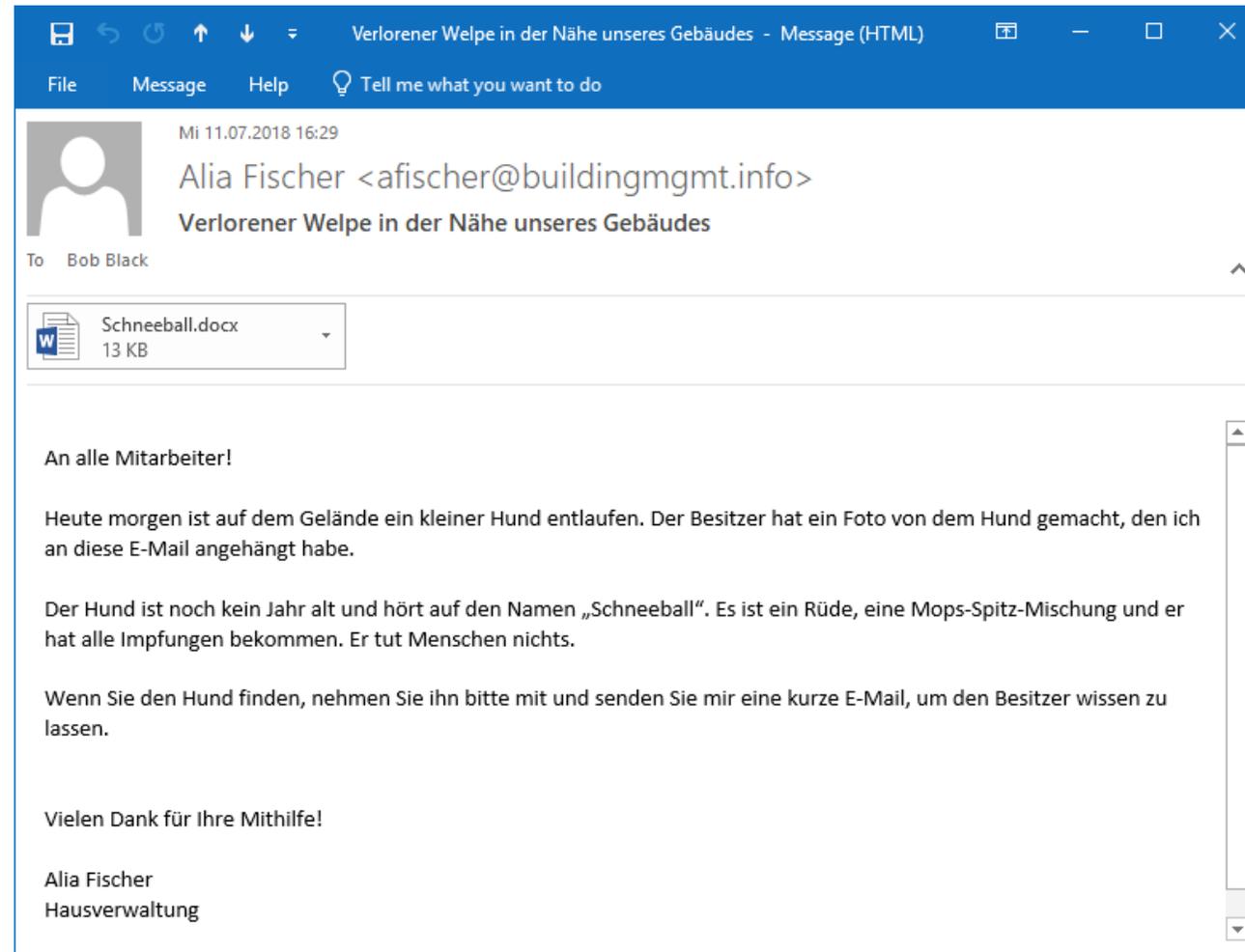
- ob der Benutzer auf den Link klickt
- ob Zugangsdaten eingegeben werden



Phish Threat Kampagnen – Office-Anhang

Es wird überprüft, ob der Benutzer einen MS-Office-Anhang

- herunterlädt
- öffnet



Phish Threat Trainings

Automatische Anmeldung zum Training bei Nicht-Bestehen eines Phishing-Tests



Das war kein wirklicher Angriff, aber es hätte sein können.

Willkommen bei Sophos Phish Threat. In Zusammenarbeit mit Ihrer Organisation führt Phish Threat simulierte Angriffe durch, um Mitarbeiter über die Gefahren von Phishing und Social Engineering aufzuklären.

Da Sie von diesem simulierten Angriff betrogen wurden, hat Ihr Administrator Sie für eine kurze Schulung angemeldet. Folgen Sie den Anweisungen unten, um das erforderliche Training abzuschließen.

[Gehe zum Training](#)

Vollständige Offenlegung: Der Schulungsfortschritt wird aufgezeichnet und an Ihren Administrator gemeldet. Sag nicht, dass wir dich nicht gewarnt haben!

P.S. BLEIB RUHIG FÜR DEN MOMENT. NICHT ALLE HABEN IHRE E-MAILS ÜBERPRÜFT, UND WIR MÖCHTEN NICHT, DASS SIE EINEN UNFAIREN VORTEIL HABEN.

Phishing-Awareness

2. Wortwahl



Überprüfen Sie die E-Mail auf Rechtschreibfehler, verdächtige Formulierungen oder dringende Handlungsaufforderungen. Liest sich die

Phishing-Awareness Quiz

[Prüfung zurücksetzen](#)

1 Wie können Sie überprüfen, ob der Absender wirklich die Person ist, die er vorgibt zu sein?

- Indem Sie eine E-Mail an ihn zurückschicken
- Indem Sie seine VOLLSTÄNDIGE E-Mail-Adresse überprüfen
- Indem Sie Anhänge überprüfen, die an Sie gesendet wurden
- Indem Sie auf Links klicken, die im Textteil der E-Mail stehen

Someone has added you to Project Darwin - Nachricht (HTML)

Datei Nachricht Hilfe Was möchten Sie tun?

Löschen Antworten QuickSteps Verschieben Markierungen Bearbeiten Rede Zoom An OneNote senden Insights Nachricht melden

Fr 30.10.2020 17:56

MT Microsoft Teams <notification@microsoftteams.com>

Someone has added you to Project Darwin

An Michael Veit

Microsoft Teams

A team member has added you to "Project Darwin"

Project Darwin - shared folder

<https://microsoftteams.com/?em=4c9dd999-e90a-4745-a09c-8&id=c3b41fdd-e2a7-41bb-c785->

Klicken oder tippen Sie, um dem Link zu folgen.

Teams Member - www.microsoftteams.com

Open Teams

© 2020 Microsoft Corporation
One Microsoft Way, Redmond, WA 98052-7329
[Privacy Policy](#)

Microsoft Teams

Nachricht melden

Verdächtige Nachricht melden?

Wenn Sie diese Nachricht melden, wird Ihr Sicherheitsteam auf einen möglichen Phishing- oder Spam-Versuch aufmerksam gemacht. Möchten Sie diesen Bericht wirklich senden?

Ja Nein

SOPHOS Cybersecurity evolved.

SOPHOS SECURITY OPERATIONS CENTER

Hi Michael.Veit@Sophos.de,

You caught a phish!

This was a simulated phishing email sent by our organization for training purposes. Had this been a real phishing attack, your report would have alerted the security team and helped to protect our organization.

Nice work!

Sophos Security Operations Center

2 von 6 aktiven Kampagnen

[Alle anzeigen](#)

academy2019

Beginnt: August 06, 2019
Endet: September 05, 2019



3 E-Mails gesendet



3 E-Mails geöffnet



0 gemeldete Bedrohungen



2 Benutzer ermittelt



0 haben die Schulung abgeschlossen

Academy 2019-2

Beginnt: August 07, 2019
Endet: September 06, 2019



4 E-Mails gesendet



1 E-Mails geöffnet



0 gemeldete Bedrohungen



1 Benutzer ermittelt



1 haben die Schulung abgeschlossen

Zusammenfassung (letzte 5 kampagnen)



Letzte 5 Kampagnen

Ertappte Benutzer

[Bericht anzeigen](#)

Name	Wie oft ertappt	Zuletzt ertappt
Mike M. Magenta	3	08.07.2019
Cindy C. Cyan	3	28.06.2019
Michael Saleseng	2	28.06.2019
Kris NextGen	1	28.06.2019

Vergangene 90 Tage

Bedrohungsmelder

[Bericht anzeigen](#)

Name	Bedrohungen gemeldet	Zuletzt gemeldet
Michael Veit	1	28.06.2019

Vergangene 90 Tage



Phish Threat - Vorteile

- Ganzheitliche Sicherheit – inklusive des menschlichen Faktors
- Steigert die Aufmerksamkeit der Mitarbeiter im Alltag
- Sensibilisierung der Budgetverantwortlichen für die Notwendigkeit von NextGen-Security
- Keine Installation notwendig, sofortiger Test möglich





Die nächsten Schritte



Solution Brief: IT-SiG 2.0

In diesem Solution Brief erfahren Sie, welche Anforderungen kritische Infrastrukturen bei der IT-Sicherheit erfüllen müssen, wie Sie die für KRITIS-Betreiber geforderten Sicherheitsvorkehrungen umsetzen uvm.

[Jetzt downloaden](#)



Podcast

Cybersecurity für kritische Infrastrukturen – was KRITIS-Unternehmen aus gesetzlicher Sicht beachten müssen mit Rechtsanwalt Andreas Daum, LL.M. (LSE) von Noerr Partnerschaftsgesellschaft mbB.

[Zum Podcast](#)



IT-Sicherheitsgesetz und Kritis

Das neue IT-Sicherheitsgesetz 2.0 betrifft nicht nur KRITIS-Betreiber in Deutschland, sondern auch deren Lieferanten in anderen Ländern. Weitere Informationen erhalten Sie auf unserer Webseite.

sophos.de/it-sicherheitsgesetz



Kontakt

Wenn Sie Fragen haben oder Unterstützung benötigen, ist Ihr Sophos-Ansprechpartner gerne für Sie da und hilft Ihnen weiter.

sophos.de/kontakt

SOPHOS
Cybersecurity as a Service