TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

"T.I.S.P. Community Meeting 2021"

Berlin, 03.-04.11.2021

Strategien und Verfahren zur sicheren E-Mail-Kommunikation

Steffen Zerbe, M&H IT-Security GmbH

Beratung

- ISMS-Einführung
- IS-Richtlinien

Schulungen

- TISP
- ISB

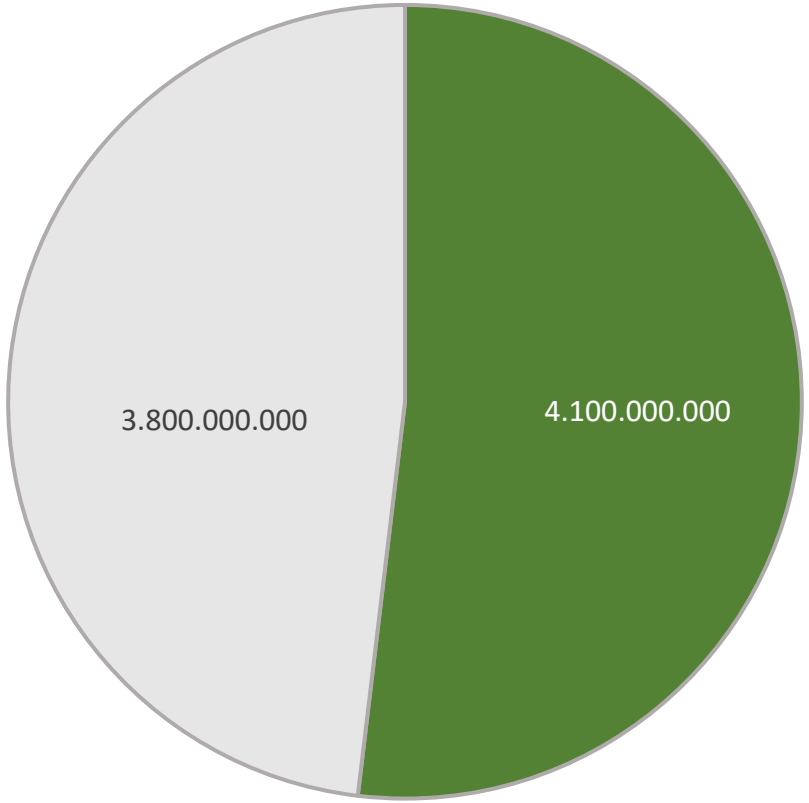
Klassifizierungslösung NovaPath

Fragerunde

- Wer verwendet E-Mail?
- Wer verwendet E-Mail, um (Geschäfts-) Geheimnisse auszutauschen?
- Wer verwendet Tools, um E-Mail abzusichern?

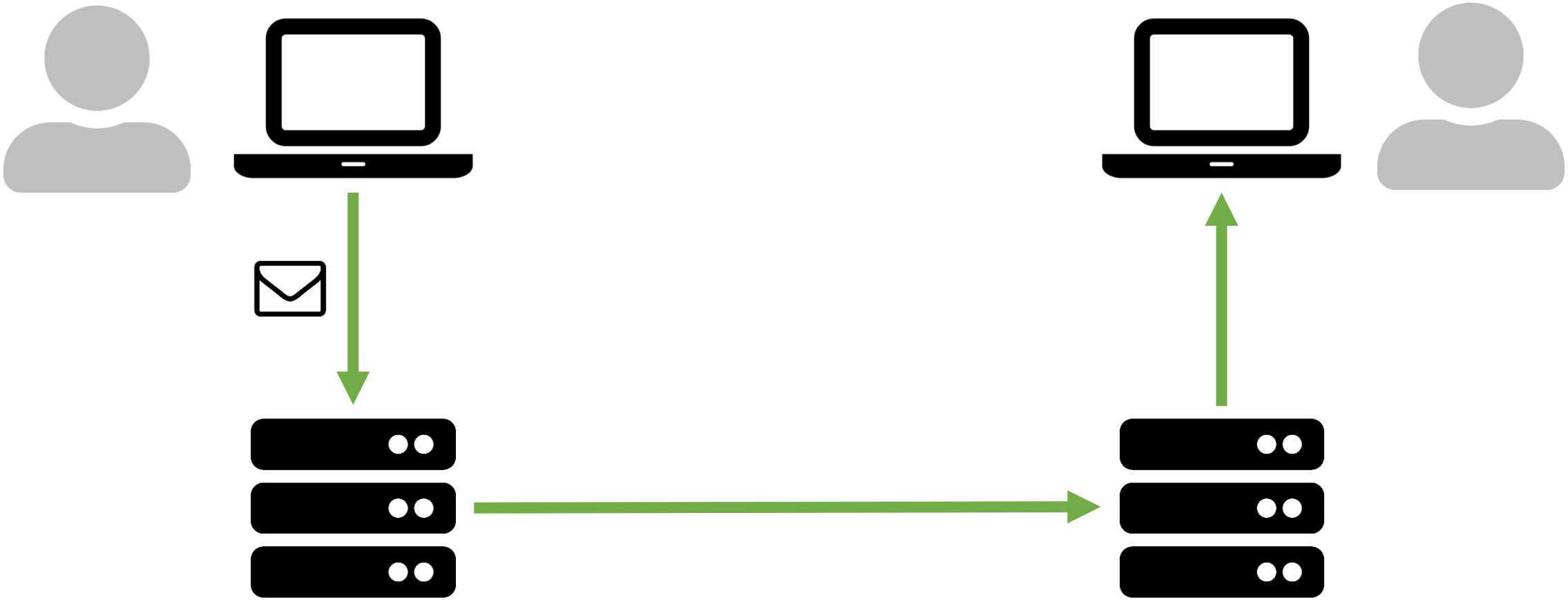
Wer verwendet E-Mail?

E-Mail-Nutzende im Vergleich zur Weltbevölkerung



The Radicati Group, Inc. „Email Statistics Report, 2019-2023“

Wie funktioniert E-Mail?

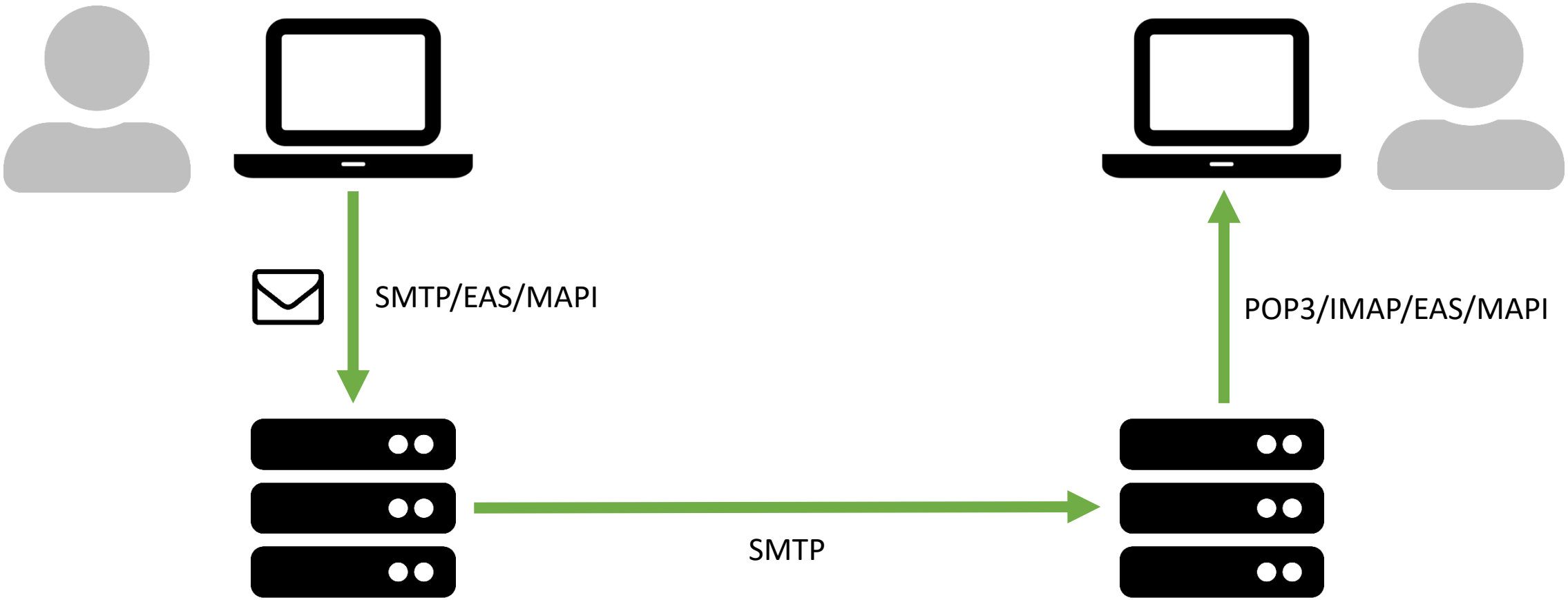


E-Mail ist dezentral

- Große Vielfalt an Anbietern
- Kann auch selbst gehostet werden
- Keine zentrale Instanz
- Große Vielfalt an Server- und Client-Software
- Hohe Interoperabilität

=> Aktuell: RFC 5322 ff (IETC)

Protokolle, Provider und Clients



~~Wie sicher ist E-Mail?~~

Falsche Frage!

- Konzeptionelle Analysetechnik zur Aufdeckung potentieller Schwachstellen
- Bietet einen Bezugsrahmen für die Sicherheitsbewertung

Variablen der Bedrohungsmodellierung

- Assets und ihr Schutzbedarf
- Angreifende mit ihren Zielen und Möglichkeiten
- Systeme mit ihren Sicherheitseigenschaften und Verwundbarkeiten

Sind meine Assets bei der Verwendung von E-Mail ausreichend vor potentiellen Angreifenden geschützt?

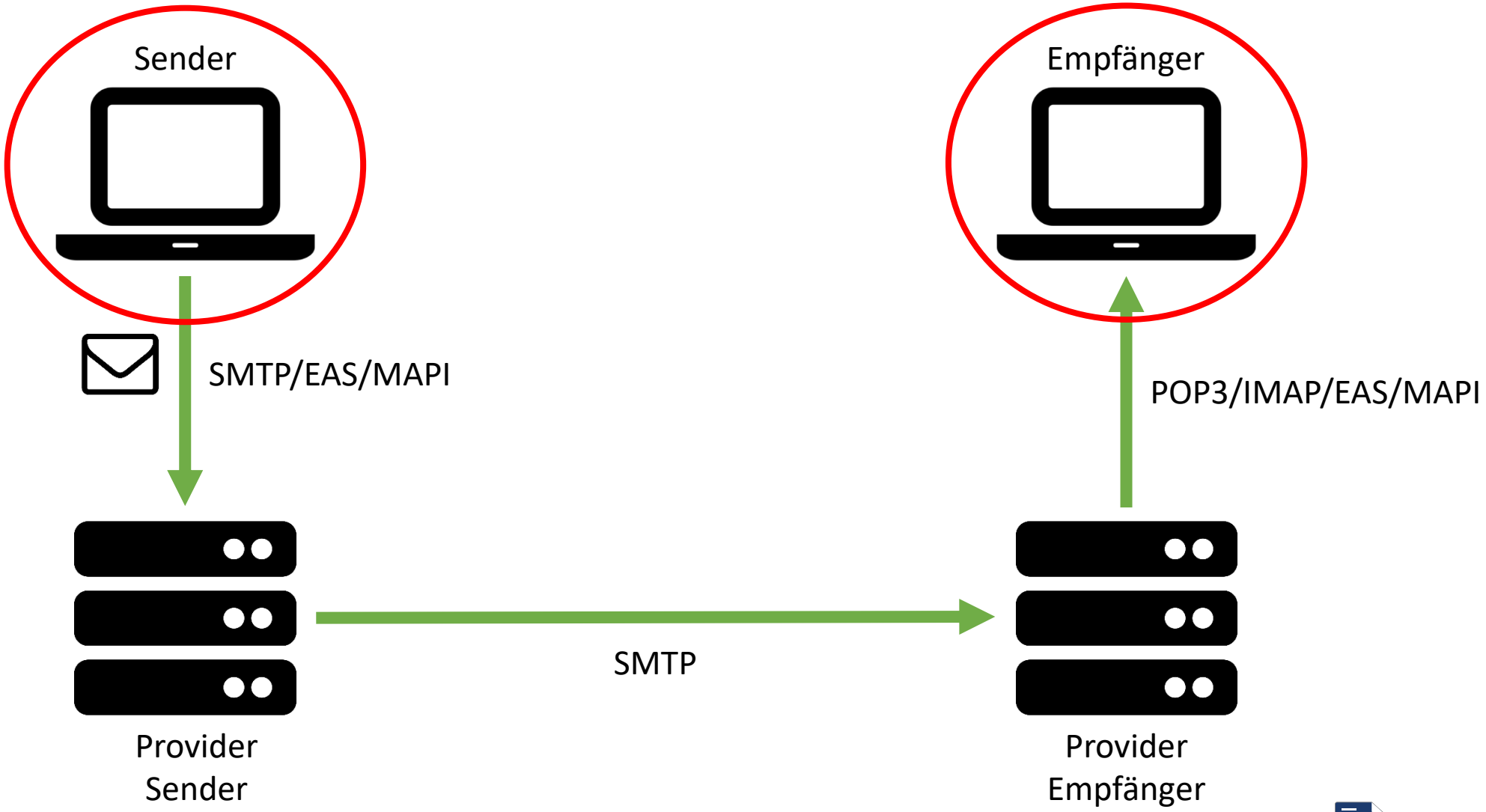
- **Was soll geschützt werden?**
  - Nachrichteninhalte
  - Anhänge
  - Metadaten
  - Kommunikationspartner
  - Kommunikationsverhalten
  - Aktivitätszeitraum

Angreifende mit ihren Zielen und Möglichkeiten

- **Vor wem sollen die Assets geschützt werden?**
  - Cyberkriminellen
  - Geheimdienste
  - E-Mail-Anbieter
  - Sonstige unberechtigte Dritte

Systeme mit ihren Sicherheitseigenschaften und Verwundbarkeiten

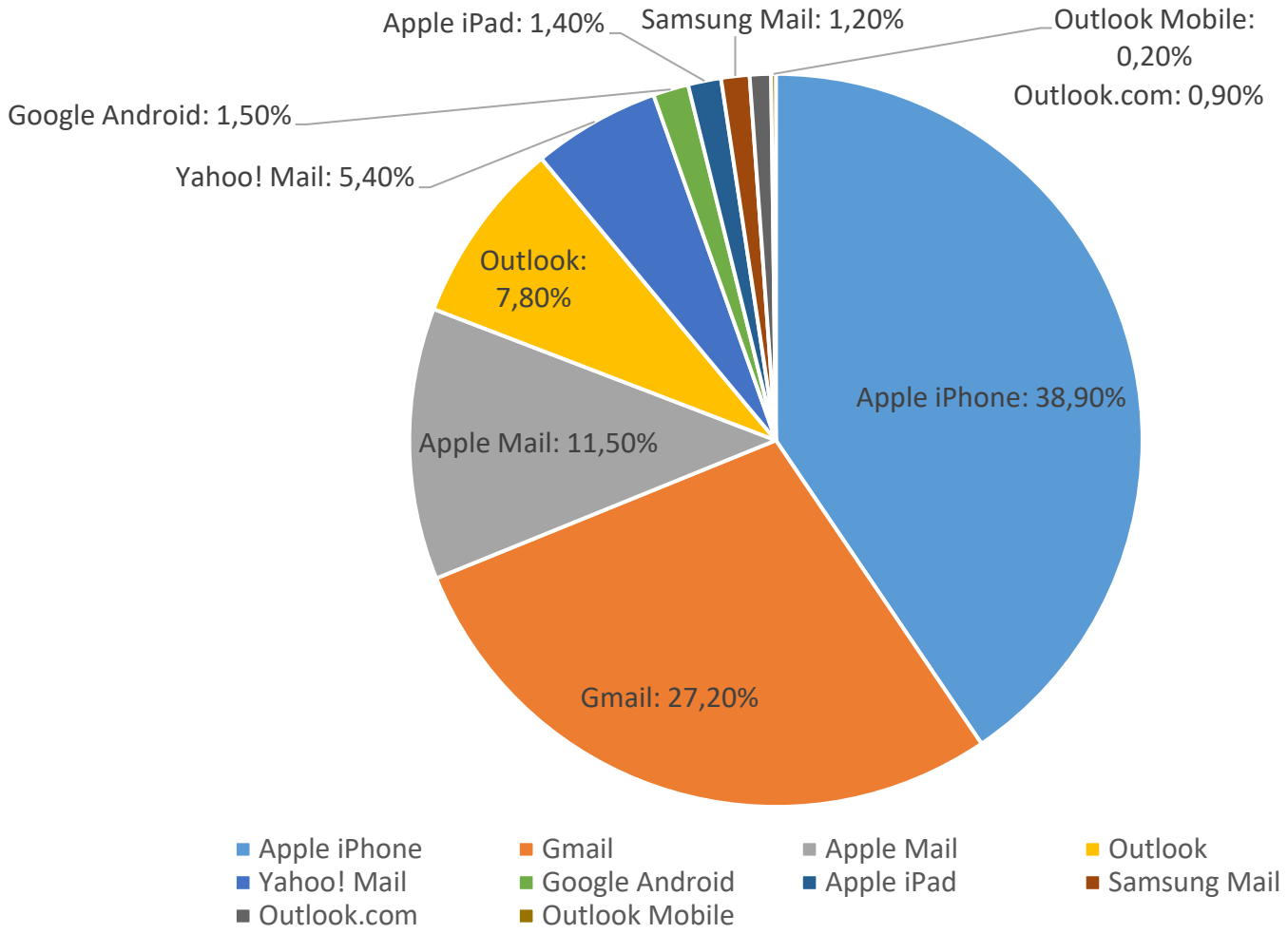
- **Modellierung: Wie sieht das System aus?**
  - Beteiligte Komponenten
  - Kommunikation zwischen Komponenten
  - => Data Flow Diagram (DFD)
- **Analyse der Sicherheitseigenschaften und Verwundbarkeiten**
  - Welche Sicherheitseigenschaften könnten verletzt sein?
    - Vertraulichkeit
    - Integrität
    - Verfügbarkeit
    - Authentizität
    - Autorisierung



- **Arbitrary Code Execution**
  - Ausnutzen von Schwachstellen zur Codeausführung (Buffer Overflow, Use After Free, Code Injection, Cross Site Scripting..)
  - Größte Angriffsoberfläche: Rendering-Engine
  - Gegenmaßnahmen:
    - Memory Safety
    - Privilege Separation
    - Sandboxing

- **Spoofing / Phishing**
  - Fälschung von E-Mails durch ähnlich aussehende Absenderadressen, offiziell wirkende Inhalte
  - Gegenmaßnahmen:
    - Signaturprüfung
    - Maschinengestützte Erkennung
    - Awareness-Maßnahmen

E-Mail Clients: Marktanteile 2021

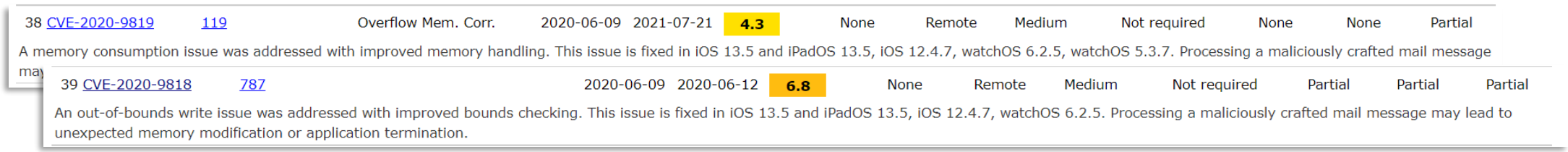


Litmus Software, Inc.: Email client market share in 2021: Trends from January to March

- **Überwiegend Outlook im geschäftlichen Umfeld**
  - Hochkomplexe Software
  - Alte Codebasis in C++
  - Nutzt WordHTML-Engine für HTML-Inhalte
  - Kein Sandboxing

15	CVE-2019-1200		Exec Code	2019-08-14 2020-08-24	9.3
A re					
6	CVE-2020-16947	125	Exec Code	2020-10-16 2020-10-22	9.3
A r					
1	CVE-2021-31949		Exec Code	2021-06-08 2021-06-15	6.8
Mic					
2	CVE-2021-31941		Exec Code	2021-06-08 2021-06-10	6.8
Microsoft Office Graphics Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31940.					

- **iOS Mail, Outlook Mobile, Gmail**
  - Oft reduzierter Funktionsumfang
  - Vergleichsweise moderne Codebasen
  - Nutzen System-Rendering-Engine
  - Plattformbedingt starkes Sandboxing



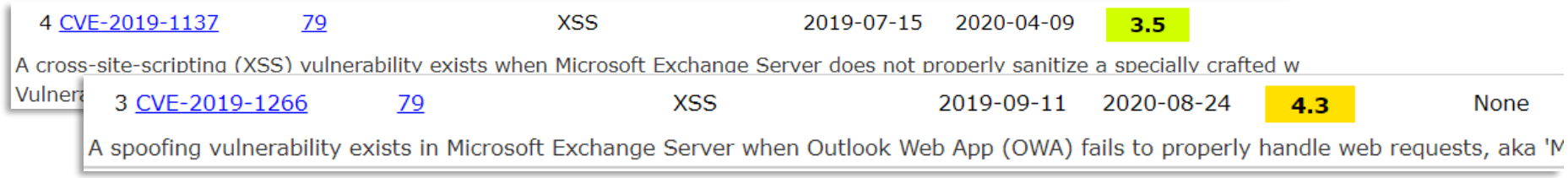
38	CVE-2020-9819	119	Overflow Mem. Corr.	2020-06-09	2021-07-21	4.3	None	Remote	Medium	Not required	None	None	Partial

A memory consumption issue was addressed with improved memory handling. This issue is fixed in iOS 13.5 and iPadOS 13.5, iOS 12.4.7, watchOS 6.2.5, watchOS 5.3.7. Processing a maliciously crafted mail message may

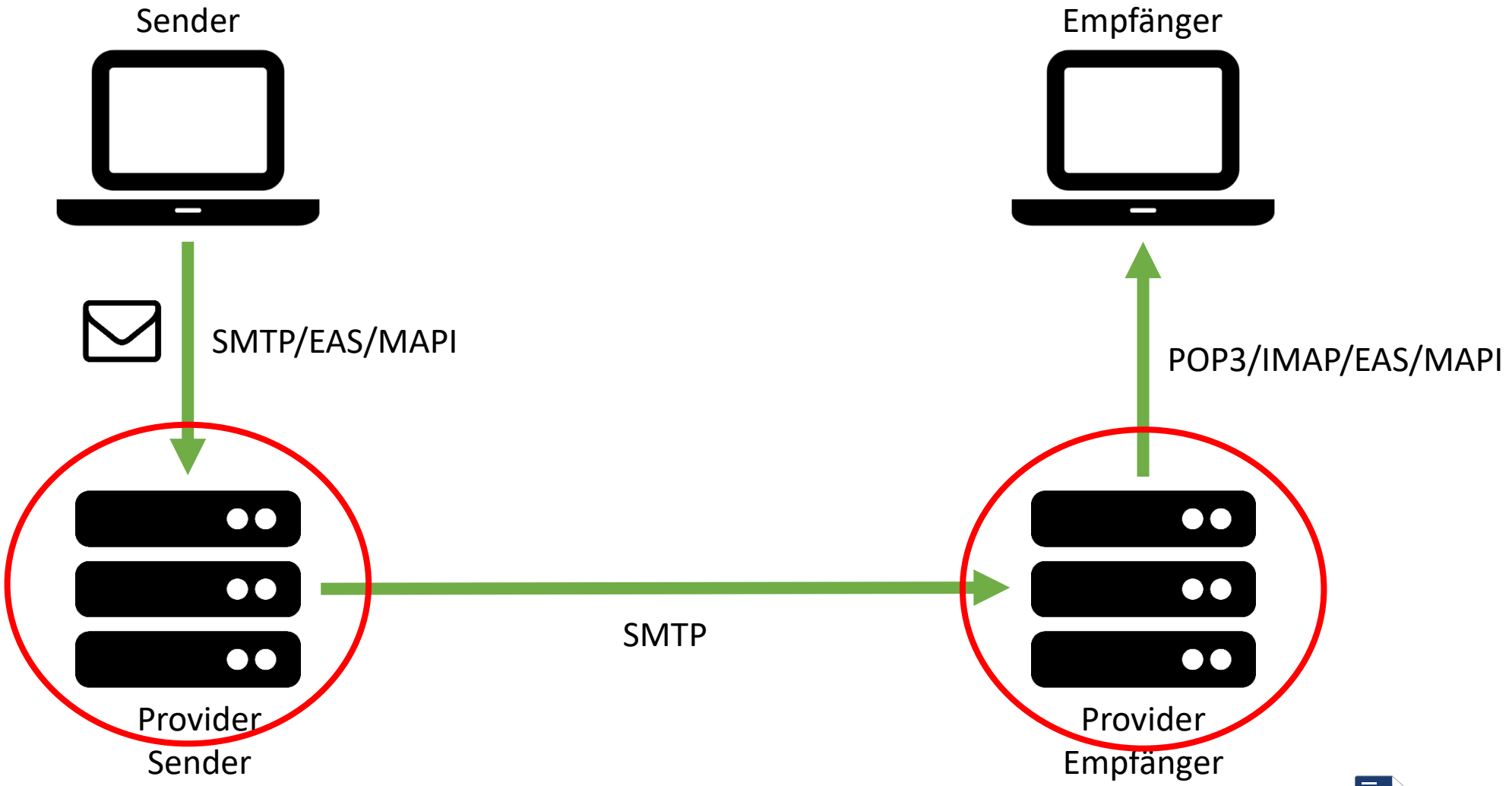
39	CVE-2020-9818	787		2020-06-09	2020-06-12	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial

An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 13.5 and iPadOS 13.5, iOS 12.4.7, watchOS 6.2.5. Processing a maliciously crafted mail message may lead to unexpected memory modification or application termination.

- **Outlook.com, OWA, Gmail**
  - Komplexe clientseitige Webanwendungen
  - In JavaScript implementiert
  - Verwenden HTML-Engine des Browsers
  - Starkes Sandboxing durch Browser
  - Plattformbedingte Gefährdungen: XSS, CSRF, ..



4	CVE-2019-1137	79	XSS	2019-07-15	2020-04-09	3.5	
A cross-site-scripting (XSS) vulnerability exists when Microsoft Exchange Server does not properly sanitize a specially crafted w							
Vulnera							
3	CVE-2019-1266	79	XSS	2019-09-11	2020-08-24	4.3	None
A spoofing vulnerability exists in Microsoft Exchange Server when Outlook Web App (OWA) fails to properly handle web requests, aka 'M							



- **Arbitrary Code Execution**
  - Ausnutzen von Schwachstellen zur Codeausführung (Buffer Overflow, Use After Free, Code Injection, Cross Site Scripting..)
- **Information Disclosure**
  - Zugriff auf fremde Postfächer
- **Privilege Escalation**
  - Zugriff auf fremde Nutzerkonten
- **Denial of Service**
  - Überlastung des Mailservers

- **On-Premises**
  - Microsoft Exchange
  - Open-Xchange
  - SOGo

- **Cloud**
  - Microsoft 365/Exchange Online
  - G Suite/Gmail
  - Andere Anbieter (IONOS, Strato, …)

On-Premises Exchange

2021 Microsoft Exchange Server

https://en.wikipedia.org/wiki/2021_Microsoft_Exchange_Server_data_breach

Not logged in Talk Contributions Create account Log in

Article Talk Read Edit View history Search Wikipedia

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Current events
Random article
About Wikipedia
Contact us
Donate

Contribute
Help
Learn to edit
Community portal
Recent changes
Upload file

Tools
What links here
Related changes
Special pages
Permanent link
Page information
Cite this page
Wikidata item

Print/export
Download as PDF

2021 Microsoft Exchange Server data breach

From Wikipedia, the free encyclopedia

A global wave of cyberattacks and data breaches began in January 2021 after four zero-day exploits were discovered in on-premises Microsoft Exchange Servers, giving attackers full access to user emails and passwords on affected servers, administrator privileges on the server, and access to connected devices on the same network. Attackers typically install a backdoor that allows the attacker full access to impacted servers even if the server is later updated to no longer be vulnerable to the original exploits. As of 9 March 2021, it was estimated that 250,000 servers fell victim to the attacks, including servers belonging to around 30,000 organizations in the United States, 7,000 servers in the United Kingdom,[8] as well as the European Banking Authority, the Norwegian Parliament, and Chile's Commission for the Financial Market (CMF).[9][10][11][12][13][14]

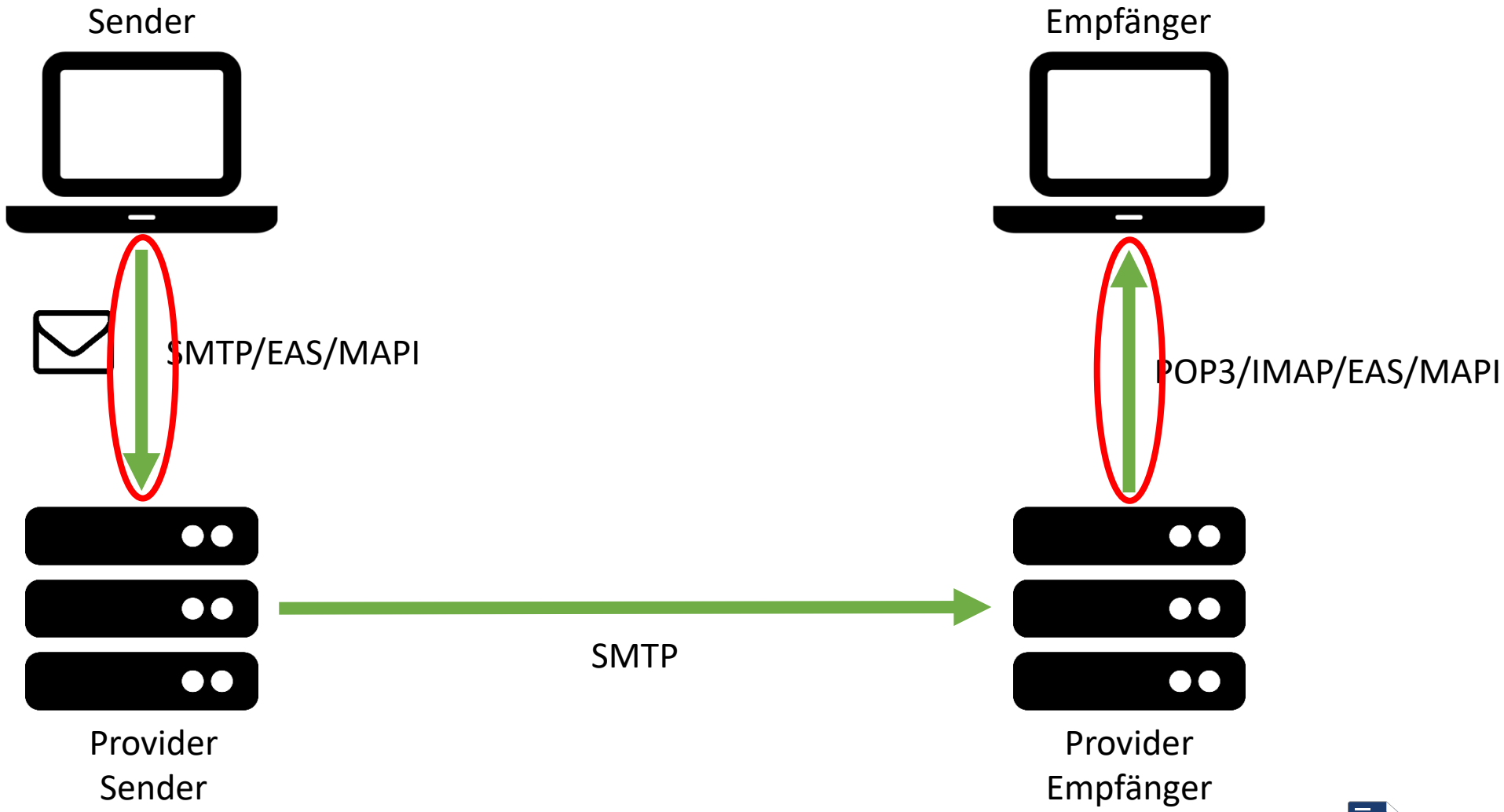
On 2 March 2021, Microsoft released updates for Microsoft Exchange Server 2010, 2013, 2016 and 2019 to patch the exploit; this does not retroactively undo damage or remove any backdoors installed by attackers. Small and medium businesses, local institutions, and local governments are known to be the primary victims of the attack, as they often have smaller budgets to secure against cyber threats and typically outsource IT services to local providers that do not have the expertise to deal with cyber attacks.[15]

On 12 March 2021, Microsoft announced the discovery of "a new family of ransomware" being deployed to servers initially infected, encrypting all files, making the server inoperable and demanding payment to reverse the damage.[16] On 22 March 2021, Microsoft announced that in 92% of Exchange servers the exploit has been either patched or mitigated.[17]

Contents [hide]
1 Background
2 Perpetrator
3 Methodology
4 Impact

2021 Microsoft Exchange Server data breach

Date	• 5 January 2021 (exploit first reported)[1] • 6 January 2021 (first breach observed)[1][2] • 2 March 2021 (breach acknowledged)[3]
Location	Global
Type	Cyberattack, data breach
Cause	Microsoft Exchange Server zero-day vulnerabilities[4]
First reporter	Microsoft (public disclosure)[3]
Suspects	Hafnium,[5][6] and at least nine others.[7]



Schwachstellen von Client/Server-Kommunikation

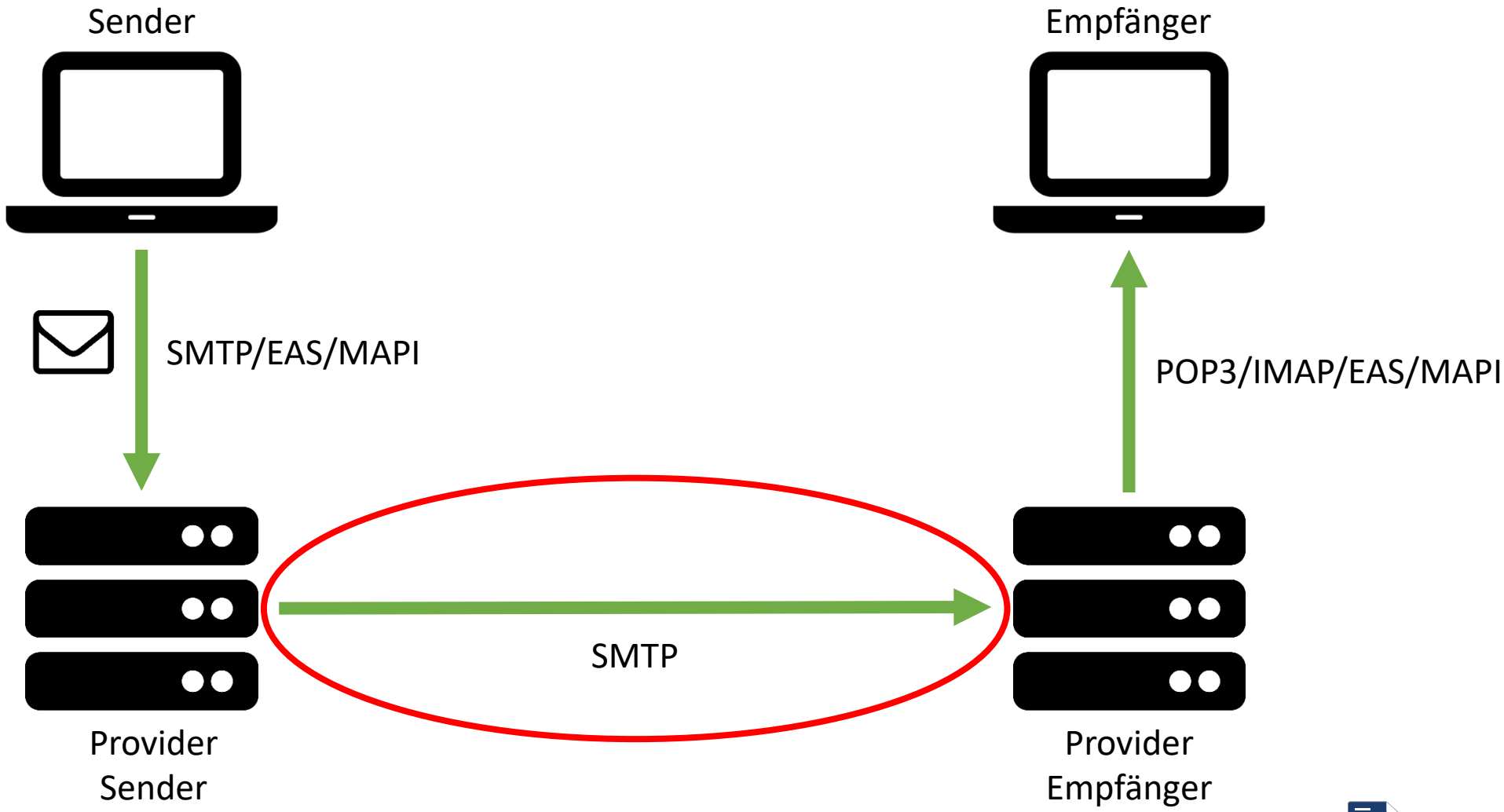
- **Sniffing**
  - Mitlesen des Datenverkehrs zwischen Client und Server
  - Gegenmaßnahme: Kryptographie
- **Spoofing**
  - Umleitung des Datenverkehrs an falsches Zielsystem
  - Gegenmaßnahme: Authentisierung
- **Elevation of Privilege**
  - Zugriff auf fremde Nutzeraccounts, bspw. per Bruteforce
  - Gegenmaßnahme: Zwei-Faktor-Authentisierung

- **Bietet:**
  - Integrität
  - Authentizität
  - Vertraulichkeit

- **Mittlerweile flächendeckend benutzbar:**
  - SMTPS (Port 465)
  - IMAPS (Port 993)
  - POP3S (Port 995)
  - EAS/MAPI über HTTPS (Exchange)

  - STARTTLS sollte nicht mehr verwendet werden

- **Zwei-Faktor-Authentisierung verwenden!**



- **Spoofing**
  - Vorgabe eines falschen Absenders
  - Gegenmaßnahme: Authentisierung
- **Denial of Service**
  - Überlastung des Zielsystems durch gezielte Anfragen
  - „Mail-Bombing“
  - Gegenmaßnahmen: Filter, ausreichender Uplink
- **Spam**
  - Ungewollte Massen-E-Mails
  - Gegenmaßnahme: Spam-Filter, Blacklisten

7.1. Mail Security and Spoofing

SMTP mail is inherently insecure in that it is feasible for even fairly casual users to negotiate directly with receiving and relaying SMTP servers and create messages that will trick a naive recipient into believing that they came from somewhere else. Constructing such a message so that the "spoofed" behavior cannot be detected by an expert is somewhat more difficult, but not sufficiently so as to be a deterrent to someone who is determined and knowledgeable.

RFC 5321: Simple Mail Transfer Protocol

```
From: John Doe <jdoe@machine.example>
To: Mary Smith <mary@example.net>
Subject: Saying Hello
Date: Fri, 21 Nov 1997 09:55:06 -0600
Message-ID: <1234@local.machine.example>

This is a message just to say hello.
So, "Hello".
```

- **SPF: Sender Policy Framework**
  - DNS-Eintrag mit IP-Adressen, die Mails für die Domain senden dürfen
  - Wird vom empfangenden Server geprüft

- **DKIM: DomainKeys Identified Mail**
  - Öffentlicher Schlüssel im DNS hinterlegt
  - Wird vom empfangenen Server zur Signaturprüfung verwendet

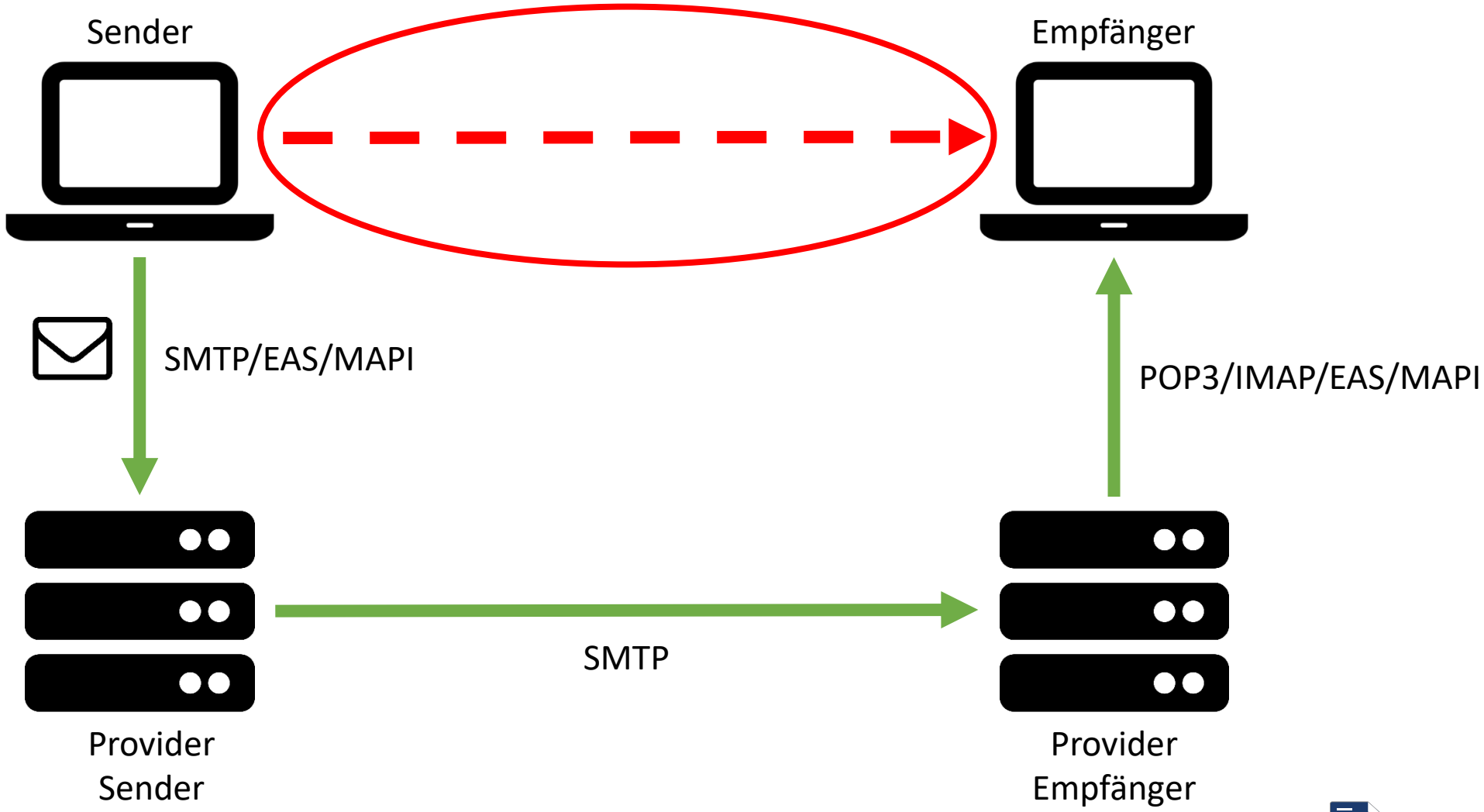
- **DMARC: Domain-based Message Authentication, Reporting and Conformance**
  - Kombiniert SPF und DKIM
  - Richtlinien für den Fehlerfall

- **DANE: DNS-based Authentication of Named Entities**
  - DNS-Eintrag mit vertrauenswürdigen CAs für diese Domain

- **60 bis 90 Prozent aller versendeten E-Mails sind Spam***
- **Beliebter Abwehrmechanismus: DNS-based Blackhole List (DNSBL)**
  - Listen von Mailservern, die in der Vergangenheit Spam versendet haben
  - Können von anderen Mailservern zur Spam-Abwehr verwendet werden
- **Delisting sehr zeitaufwendig oder gar unmöglich**
  - Große Hürde für kleinere Provider oder On-Premises Betrieb

*** https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/spam-emailmuell-im-internet-10757**

- **Betrieb der eigenen E-Mail-Infrastruktur wird zunehmend aufwendiger**
  - Sicherheitslücken in Mailservern
  - Konfiguration von Sicherheitsfeatures
  - Blacklisting



- **Vertraulichkeit**
  - Provider können Nachrichteninhalte lesen
  - Sowohl Provider des Senders als auch Provider des Empfängers
- **Integrität & Authentizität**
  - Provider können Nachrichteninhalte modifizieren
  - Sowohl Provider des Senders als auch Provider des Empfängers
- **Verfügbarkeit**
  - Sende- und Empfangsvorgang ist von beiden Providern abhängig

- **Zwei offene Standards für die E-Mail-Verschlüsselung/Signierung**
  - Verwenden asymmetrische Kryptographie (Public-Key-Verfahren)

- **S/MIME (1996)**
  - Zertifikatsbasiert
  - Zentrale Certificate Authorities (CA)
  - In viele E-Mail-Clients integriert

- **PGP (1991)**
  - Keine zentrale Zertifizierungsinstanz: „Web of Trust“
  - Plugins für viele Clients erhältlich
  - Freie Implementierung: GnuPG

Verschlüsselte E-Mails: Probleme

- **E-Mail ist standardmäßig unverschlüsselt**
  - Bedien- oder Softwarefehler führen zu Plaintext-Kommunikation
  - Meistens wird der Gesprächsverlauf noch unverschlüsselt mitgesendet
- **Keine Verschlüsselung von Metadaten**
  - Metadaten wie Sender, Empfänger, Header, Betreffszeile (!) können vom Provider eingesehen werden
- **PGP und S/MIME verwenden Langzeitschlüssel**
  - Kompromittierung eines Schlüssels legt vergangene und zukünftige Kommunikation offen
- **Manuelles Key-Management**
  - Wie bekommt der Empfänger meinen Schlüssel? Wie kommt mein Schlüssel auf alle meine Geräte? Wann und wie rotiere ich meinen Schlüssel?
- **PGP und S/MIME bieten kryptographische Agilität**
  - Welche Verfahren unterstützt werden, hängt stark von den verwendeten Clients ab
  - Alte Verfahren und Betriebsmodi (DES, RC4, AES-ECB) können durch fehlerhafte Anwendung oder Downgrade-Attacken verwendet werden

Vergleich mit modernen Messengern

- Moderne Messenger bieten verschlüsselte Kommunikation
  - Signal
  - Wire
  - WhatsApp
- Zentralisierte Infrastruktur
- Haben das explizite Ziel, das notwendige Vertrauen in den Betreiber zu reduzieren
- Keine unverschlüsselte Kommunikation möglich
- Automatischer Schlüsselaustausch und Schlüsselrotation

- Sicher: E2E-Vertraulichkeit, Authentizität und Integrität – verpflichtend und ausschließlich mit modernen Verfahren
- Dezentral: On-Premises oder durch Provider betreibbar
- Föderiert: Identität ist nicht an Provider gekoppelt
- Zuverlässig: Wirksamer und präziser Schutz vor Spam

Geht das mit E-Mail?

- Vermutlich nicht.
- Riesige Basis an Bestands-Clients und –Servern
  - Unterstützung durch alle Akteure und Komponenten erforderlich
- Kompatibilitätsbruch
  - E-Mail wäre nicht mehr E-Mail
- Inhärente Probleme des Protokolls
  - Wenn ein Kompatibilitätsbruch notwendig ist..
  - .. warum dann beim alten Protokoll bleiben?

Fazit

- E-Mail ist allgegenwärtig
- Wenn Sie E-Mail selbst betreiben *müssen*: Ausreichend Ressourcen allokieren!
- E-Mail-Clients können ein Einfallstor für Malware sein
- Authentizität von E-Mails stets hinterfragen
- Ob E-Mail sicher verwendbar ist, hängt vom eigenen Bedrohungsmodell ab
- Streng vertrauliche Kommunikation sollte nicht per E-Mail erfolgen

Fragen?

… gerne per E-Mail ☺

steffen.zerbe@m-und-h.de