# Linux am Dienstag

Was man als Hacker so macht,

wenn man Emailkonten geknackt hat

# Was Hacker so mit Mailkonten treiben

Ein Vortrag

von

Marius Schwarz

# Was Hacker so mit Mailkonten treiben

Die Monetarisierung auf Kosten des gehackten Benutzers

# Was Hacker so mit Mailkonten treiben

„Was könnte man bei mir schon holen?“

Tausende überraschter Opfer

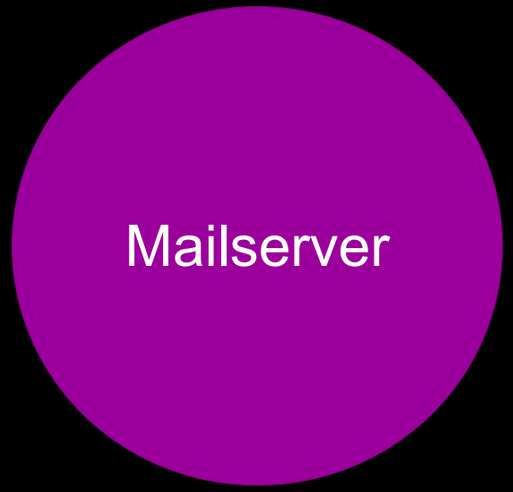
# Was Hacker so mit Mailkonten treiben

Diese Frage wollen wir heute beantworten

# Was Hacker so mit Mailkonten treiben

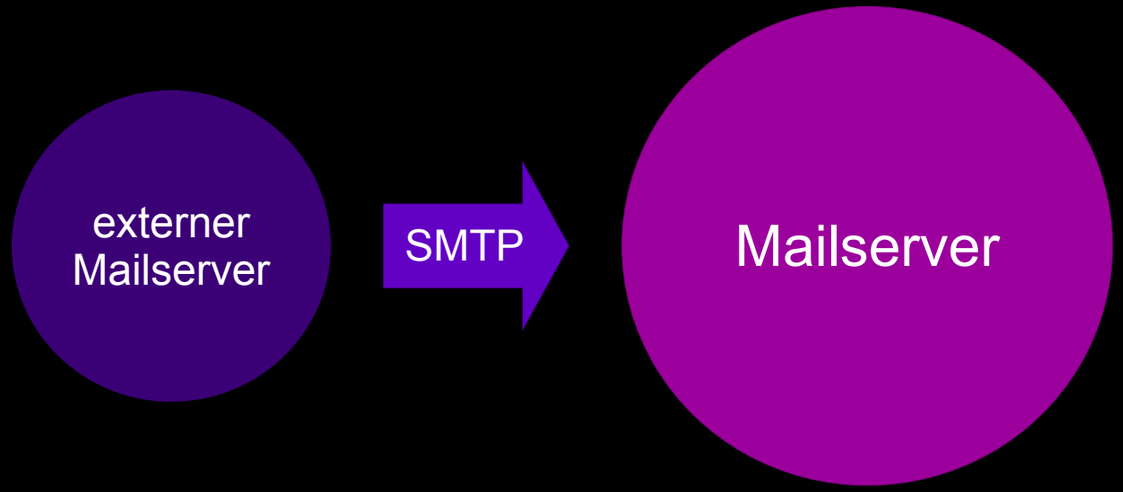
Wie bekommt man „normalerweise“ Emails?

# Was Hacker so mit Mailkonten treiben

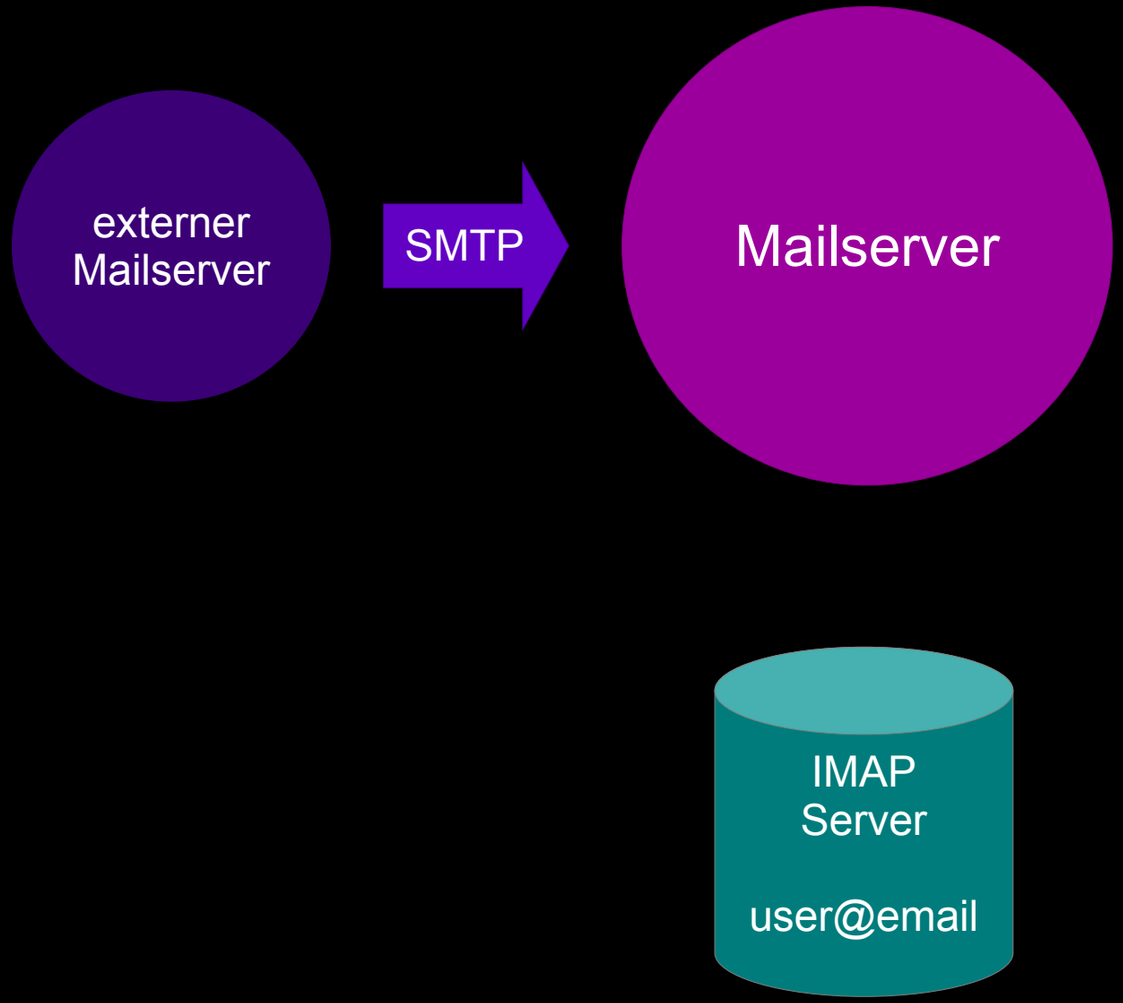


# Was Hacker so mit Mailkonten treiben

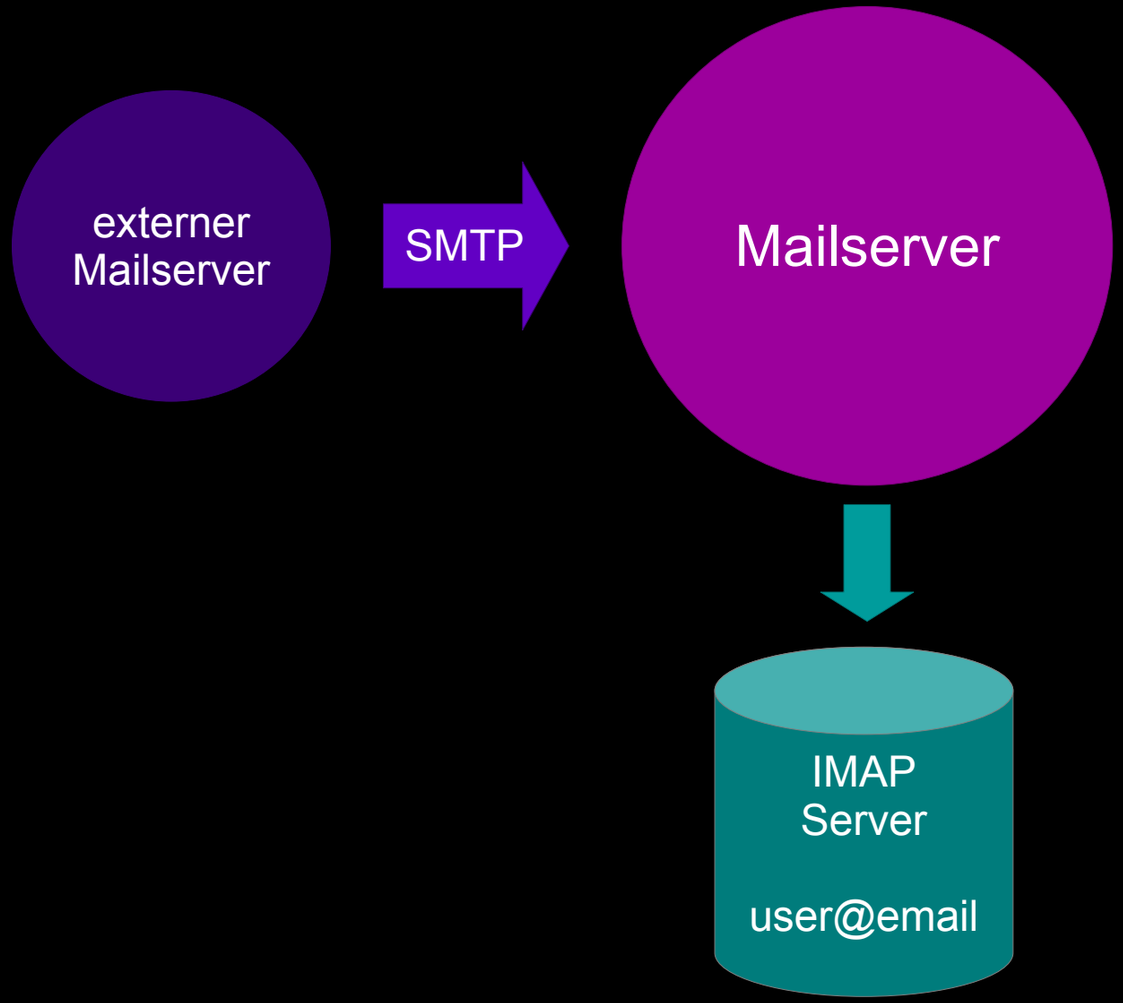
# Was Hacker so mit Mailkonten treiben



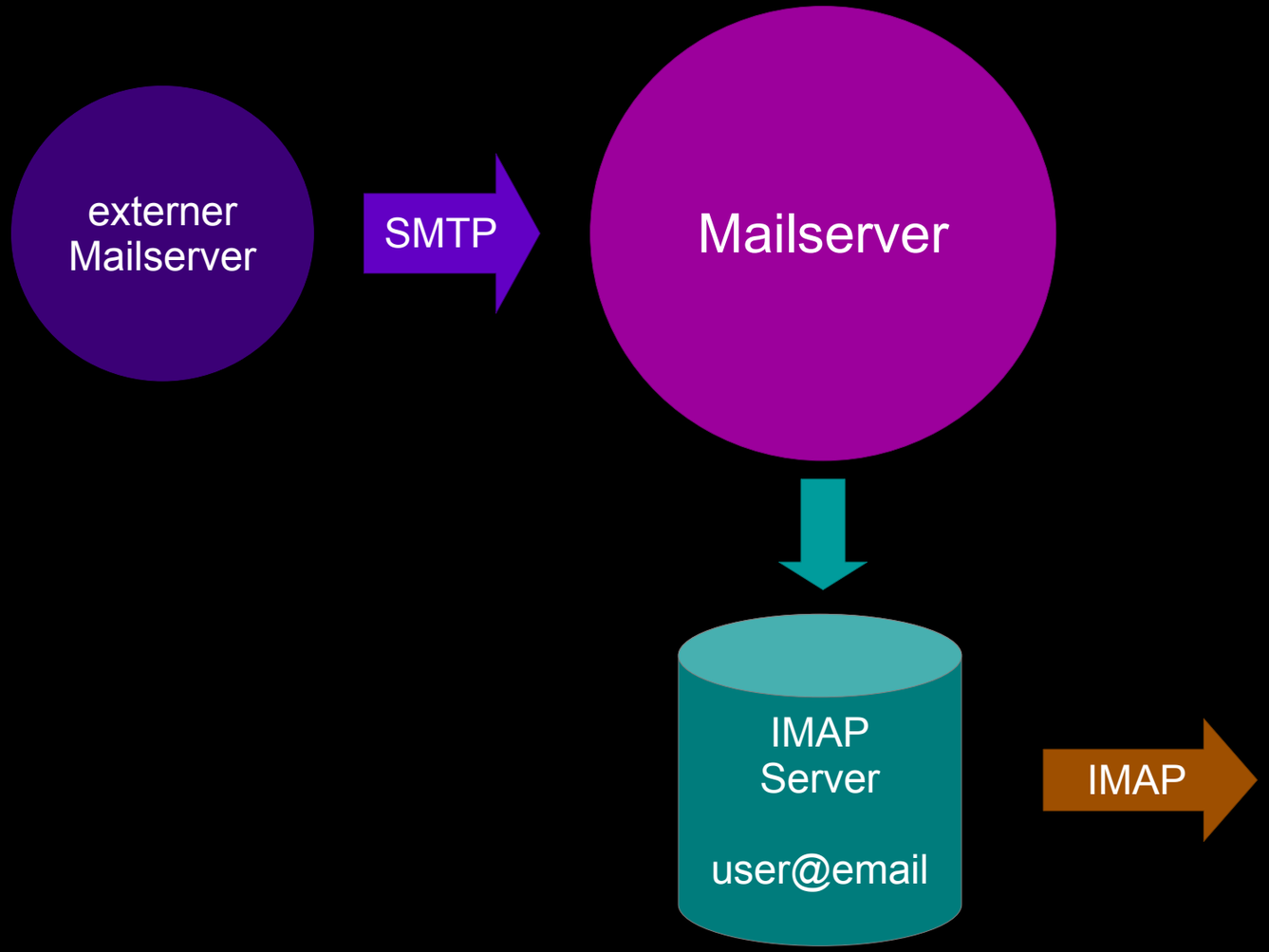
# Was Hacker so mit Mailkonten treiben



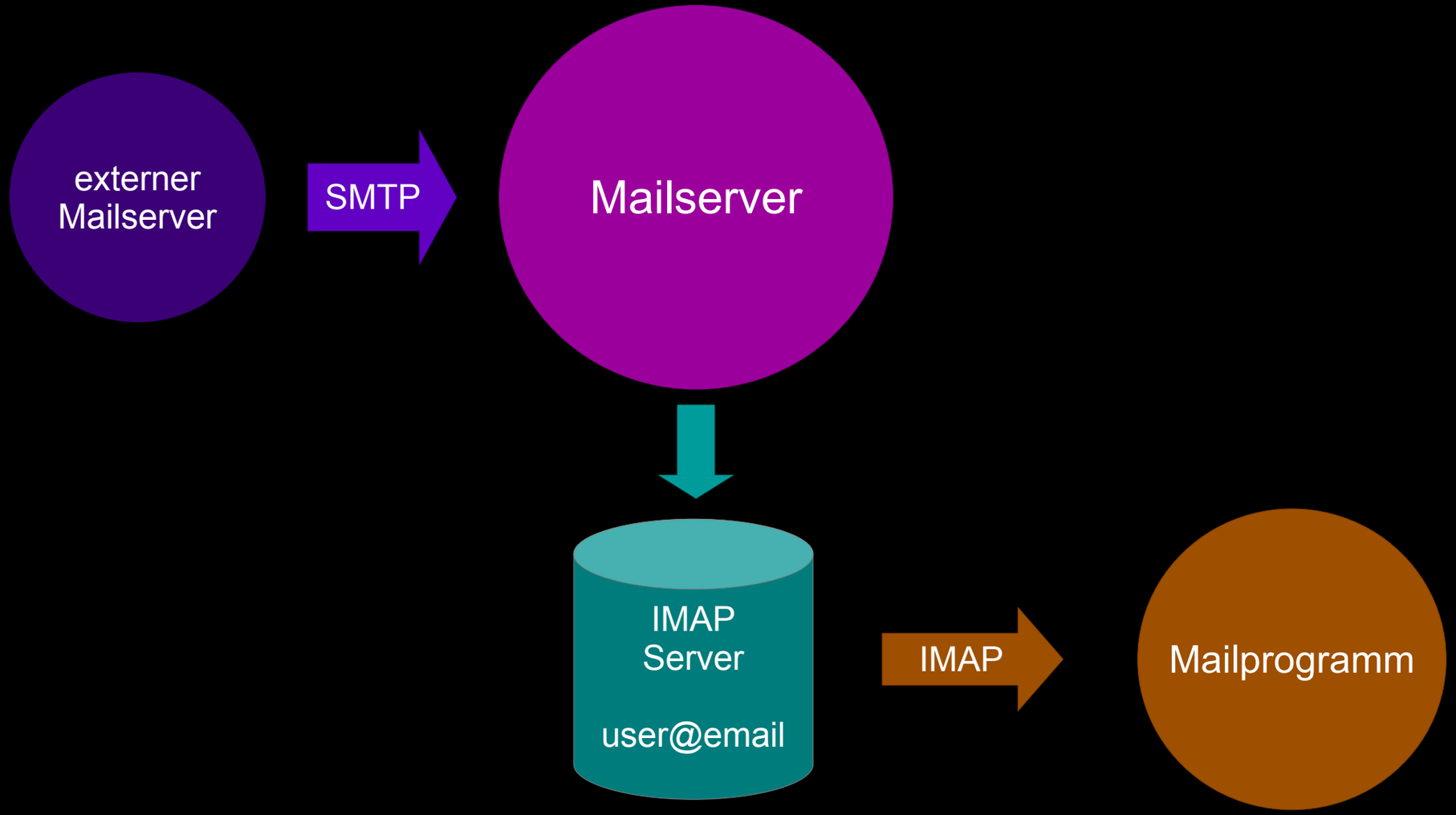
# Was Hacker so mit Mailkonten treiben



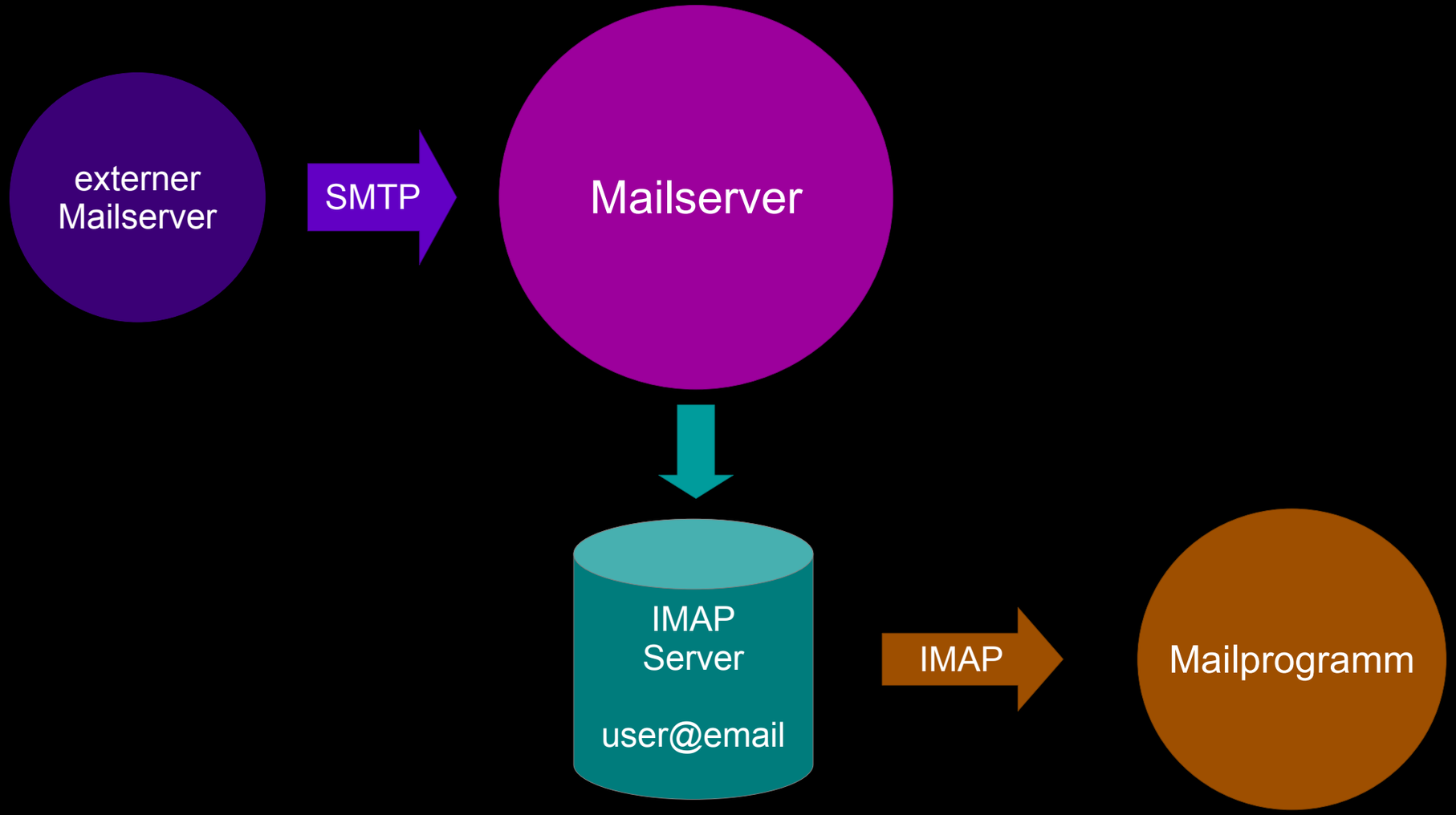
# Was Hacker so mit Mailkonten treiben



# Was Hacker so mit Mailkonten treiben



# Was Hacker so mit Mailkonten treiben



# Was Hacker so mit Mailkonten treiben

Wie sieht das in einer Email aus?

# Was Hacker so mit Mailkonten treiben

```
Return-path: <leant864@br594.hostgator.com.br>
Envelope-to: user@email
Delivery-date: Tue, 29 Mar 2022 08:29:25 +0200
Received: from gateway31.websitewelcome.com ([192.185.143.51])
    by resellerdesktop.de with esmtps  (TLS1.2) tls TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
    (Exim 4.94.2)
    (envelope-from <leant864@br594.hostgator.com.br>)
    id 1nZ5Lz-003t6D-8x
    for user@email; Tue, 29 Mar 2022 08:29:24 +0200
Received: from cm12.websitewelcome.com (cm12.websitewelcome.com [100.42.49.8])
    by gateway31.websitewelcome.com (Postfix) with ESMTP id BE38F5582E7
    for <user@email>; Tue, 29 Mar 2022 01:29:16 -0500 (CDT)
Received: from br594.hostgator.com.br ([108.179.253.185])
    by cmsmtp with SMTP
    id Z5LwnHZQw9AGSZ5Lwn43Up; Tue, 29 Mar 2022 01:29:16 -0500
Received: from leant864 by br594.hostgator.com.br with local (Exim 4.94.2)
    (envelope-from <leant864@br594.hostgator.com.br>)
    id 1nZ5Lw-002DGG-Bv
    for user@email; Tue, 29 Mar 2022 03:29:16 -0300
To: user@email
MIME-Version: 1.0
Content-Type: multipart/alternative;boundary=32df47d84333e91b632b0e408c95bbfb
From: Sparkasse Abteilung fÃ¼r Sicherheit <SparkasseAbteilungfÃ¼rSicherheit@mmlawyers.com.br>
Reply-To: SparkasseAbteilungfÃ¼rSicherheit@mmlawyers.com.br
Message-Id: <E1nZ5Lw-002DGG-Bv@br594.hostgator.com.br>
Date: Tue, 29 Mar 2022 03:29:16 -0300
Subject:  Wichtiger Hinweis zu Ihrem Konto
```

HTML entfernt um es lesbarer machen

# Was Hacker so mit Mailkonten treiben

Das geht auch anders

# Was Hacker so mit Mailkonten treiben

Das sieht dann so aus..

# Was Hacker so mit Mailkonten treiben

Hinweis:

Alle EMails sind echt

Alle Identifikationsmerkmale sind anonymisiert

# Was Hacker so mit Mailkonten treiben

```
From: user@email
Subject: ALERT! I'm hacked you and stolen you information
Date: Sun, 6 Mar 2022 12:35:48 PM +0000
To: user@email
Received: from domain.com (unknown [1.1.1.1])
        by imf08.b.hostedemail.com (Postfix) with ESMTP
        for <user@email>; Sun, 6 Mar 2022 12:35:48 PM +0000 (UTC)
X-Message-Flag: Flag for follow up

Hey user@email,
I have to share bad news with you.
Approximately few months ago I have gained access to your devices, which you use for internet browsing.
After that, I have started tracking your internet activities.
Some time ago I hacked you and got access to your email accounts user@email .
Obviously, I have easily hack to log in to your email.

Your password: XxxxxxxxXXXXXX

One week later, I have already installed Trojan virus to Operating Systems of all the devices that
you use to access your email.
```

HTML entfernt um es lesbarer machen

# Was Hacker so mit Mailkonten treiben

```
From: user@email
Subject: ALERT! I'm hacked you and stolen you information
Date: Thu, 31 Mar 2030 07:15:52 +0000
To: user@email
Received: from domain.com (unknown [1.1.1.1])
        by imf08.b.hostedemail.com (Postfix) with ESMTP
        for <user@email>; Thu, 31 Mar 2030 07:15:52 +0000 (UTC)
Content-Type: multipart/related; boundary="ab5218b44195b724f8fdb40266b2ca30f68k"
X-Message-Flag: Flag for follow up
X-Priority: 1 (Highest)
X-MSMail-Priority: High
Importance: High

Hey user@email,
I have to share bad news with you.
Approximately few months ago I have gained access to your devices, which you use for internet browsing.
After that, I have started tracking your internet activities.
Some time ago I hacked you and got access to your email accounts  user@email .
Obviously, I have easily hack to log in to your email.

Your password: XxxxxXXXXX

One week later, I have already installed Trojan virus to Operating Systems of all the devices that you use to
access your email.
```

HTML entfernt um es lesbarer machen

# Was Hacker so mit Mailkonten treiben

From: **user@email**
Subject: ALERT! I'm hacked your computer and stolen you information
Date: **Tue, 18 Oct 2022** 00:01:52 +0000
To: user@email
Received: from a13-109.smtp-out.amazonses.com ([54.240.13.109])
        by cmsmtp with ESMTP
        for <user@email>; **Tue, 18 Oct 2022** 00:01:52 +0000 (UTC)
Content-Type: multipart/related; boundary="1c7fe9672000730bacd67d48f509dd27a8b9"

Hey **user@email,**
Your computer was infected with my malware!
Your password for this mail: **XxxxxXXXXX**
I am a programmer and hacked your computer **3 months ago**. I kept saving information all the time, such as: browsing history, screen recordings, contacts, messages and much more.
I already wanted to forget you, but recently I saw something interesting on your desktop. I'm talking about the day you visited a porn site. I decided to record video from the webcam and desktop. Now I have a video of you masturbating yourself. You know what I mean
I connected to the webcam remotely, and turned off the indicator so that you would not notice anything.
I have already written down all your contacts from the address book. All contacts from friends, acquaintances, relatives. All this will be with me.

HTML entfernt um es lesbarer machen

# Was Hacker so mit Mailkonten treiben

Fangfrage:

Was stimmt damit nicht?

# Was Hacker so mit Mailkonten treiben

```
From: user@email
Subject: ALERT! I'm hacked you and stolen you information
Date: Thu, 31 Mar 2030 07:15:52 +0000
To: user@email
Received: from domain.com (unknown [1.1.1.1])
        by imf08.b.hostedemail.com (Postfix) with ESMTP
        for <user@email>; Thu, 31 Mar 2030 07:15:52 +0000 (UTC)
Content-Type: multipart/related; boundary="ab5218b44195b724f8fdb40266b2ca30f68k"
X-Message-Flag: Flag for follow up
X-Priority: 1 (Highest)
X-MSMail-Priority: High
Importance: High

Hey user@email,
I have to share bad news with you.
Approximately few months ago I have gained access to your devices, which you use for internet browsing.
After that, I have started tracking your internet activities.
Some time ago I hacked you and got access to your email accounts  user@email .
Obviously, I have easily hack to log in to your email.

Your password: XxxxxXXXXX

One week later, I have already installed Trojan virus to Operating Systems of all the devices that you use to
access your email.
```

HTML entfernt um es lesbarer machen

# Was Hacker so mit Mailkonten treiben

```
From: user@email
Subject: ALERT! I'm hacked you and stolen you information
Date: Thu, 31 Mar 2030 07:15:52 +0000
To: user@email
Received: from domain.com (unknown [1.1.1.1])
        by imf08.b.hostedemail.com (Postfix) with ESMTP
        for <user@email>; Thu, 31 Mar 2030 07:15:52 +0000 (UTC)
Content-Type: multipart/related; boundary="ab5218b44195b724f8fdb40266b2ca30f68k"
X-Message-Flag: Flag for follow up
X-Priority: 1 (Highest)
X-MSMail-Priority: High
Importance: High

Hey user@email,
I have to share bad news with you.
Approximately few months ago I have gained access to your devices, which you use for internet browsing.
After that, I have started tracking your internet activities.
Some time ago I hacked you and got access to your email accounts  user@email .
Obviously, I have easily hack to log in to your email.

Your password: XxxxxXXXXX

One week later, I have already installed Trojan virus to Operating Systems of all the devices that you use to
access your email.
```

**Na, was fehlt?!**

HTML entfernt um es lesbarer machen

# Was Hacker so mit Mailkonten treiben

- Kein Delivery-Date:

# Was Hacker so mit Mailkonten treiben

- Kein Delivery-Date:

- die Received-Header zeigen den Empfängerserver nicht

# Was Hacker so mit Mailkonten treiben

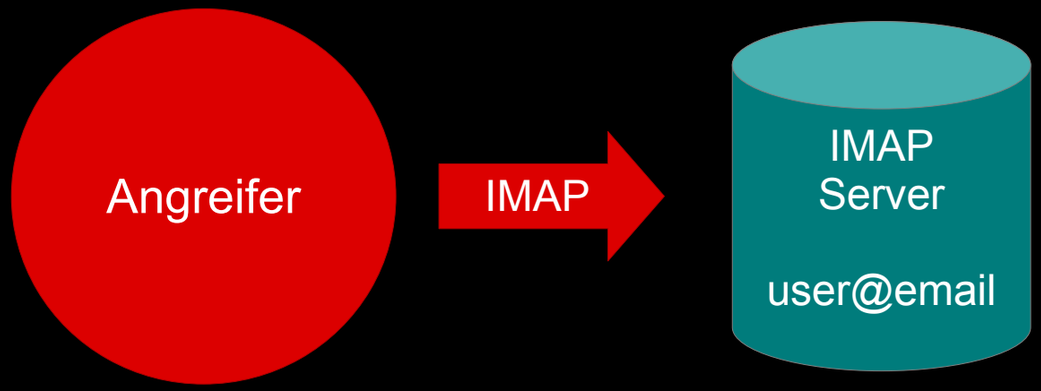
- Kein Delivery-Date:
- die Received-Header zeigen den Empfängerserver nicht
- es fehlen jede Menge „Sonstige“-Headerzeilen

# Was Hacker so mit Mailkonten treiben

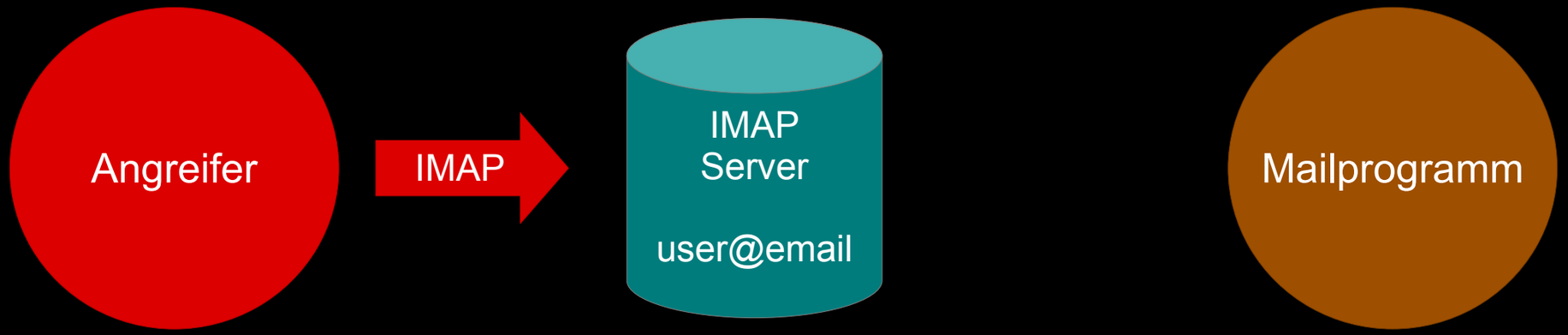
Und so läuft das ab...

# Was Hacker so mit Mailkonten treiben

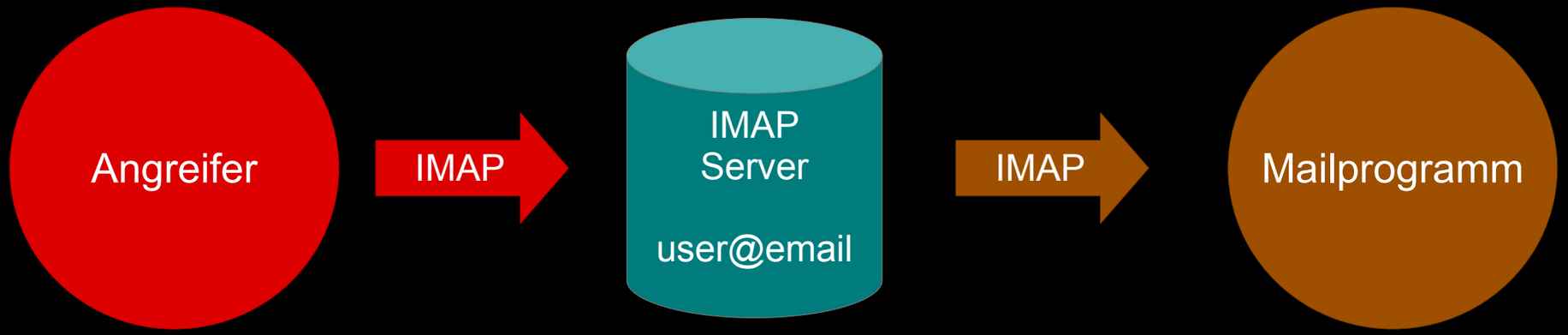
# Was Hacker so mit Mailkonten treiben



# Was Hacker so mit Mailkonten treiben



# Was Hacker so mit Mailkonten treiben



# Was Hacker so mit Mailkonten treiben

Was macht man jetzt mit so einem Konto?

# Was Hacker so mit Mailkonten treiben

Monetarisierung der Ressourcen

# Was Hacker so mit Mailkonten treiben

```
Return-path: <noreply@humblebundle.com>
Delivery-date: Mon, 28 Mar 2022 22:56:06 +0200
Date: Mon, 28 Mar 2022 20:55:39 +0000
From: "Humble Bundle" <noreply@humblebundle.com>
Reply-To: "Humble Bundle" <noreply@humblebundle.com>
To: <user@email>
```

**We received a request to resend your Humble Bundle orders.**

However, we do not have any orders on record for this email address. If you used a different email address to make your purchase, try entering it into our order resender page. Otherwise, please contact us at https://support.humblebundle.com/hc/requests/new, and our support staff will sort things out as soon as possible.

If you did not initiate this request, please disregard this message.

Sincerely,
Humble Bundle

HTML entfernt um es lesbarer machen

# Was Hacker so mit Mailkonten treiben

```
Date: Fri, 18 Mar 2022 08:07:09 +0000
From: Supercell <noreply@id.supercell.com>
To: <user@email>
Subject:  Supercell ID

Supercell ID

You attempted to log in with this email address, but there is no Supercell ID associated with it. If
you wish to create a new Supercell ID, go back to the game and tap "Register"

---

You received this email because someone requested to log in to Supercell ID. If you didn't request
to log in, you can safely ignore this email.

http://supercell.com/terms-of-service
Terms of Service

http://supercell.com/privacy-policy
Privacy Policy

Supercell ID = LEAGUE OF LEGENDS Entwickler
```

HTML entfernt um es lesbarer machen

# Was Hacker so mit Mailkonten treiben

Abgreifen der Emailadressen aller EMails

# Was Hacker so mit Mailkonten treiben

Zum Versenden von gezielter

Spam/Phising Mails

# Was Hacker so mit Mailkonten treiben

Bestellungen in Online-Shops

mit echten Daten.

# Was Hacker so mit Mailkonten treiben

INKASSO???

# Was Hacker so mit Mailkonten treiben

```
Return-path: <user@email>
Envelope-to: user@email
Delivery-date: Sun, 20 Mar 2022 23:05:45 +0100
Received: from [1.54.219.197]
        by <MAILSERVERNAME> with esmtp (Exim 4.94.2)
        (envelope-from <user@email>)
        id 1nW3gG-00AKd4-KL
        for user@email; Sun, 20 Mar 2022 23:05:45 +0100
Date: 21 Mar 2022 10:49:07 +0600
From: <user@email>
X-Priority: 3
Message-ID: <859210656.202203211106@XXXXXXXXXXXXXXXXXXXXXXX>
To: <user@email>
MIME-Version: 1.0
Content-Type: text/plain; charset="iso-8859-3"
Content-Transfer-Encoding: 8bit
Subject:  Pending for payment.

Greetings!
Have you seen lately my e-mail to you from an account of yours?
Yeah, that merely confirms that I have gained a complete access to device of yours.

Within the past several months, I was observing you.
Are you still surprised how could that happen? Frankly speaking, malware has infected your devices and it's coming
from an adult website, which you used to visit.
Although all this stuff may seem unfamiliar to you, but let me try to explain that to you.

With aid of Trojan Viruses, I managed to gain full access to any PC or other types of devices.
That merely means that I can watch you whenever I want via your screen just by activating your camera as well as
microphone, while you don't even know about that.
Moreover, I have also received access to entire contacts list as well as full correspondence of yours.
```

# Was Hacker so mit Mailkonten treiben

```
Whois 1.54.219.197


inetnum:        1.54.208.0 - 1.54.223.255
netname:        FPTDYNAMICIP-NET
country:        VN
descr:          FPT Telecom Company
descr:          2nd floor FPT Building, Pham Hung Road, Cau Giay District, Hanoi
admin-c:        LDP12-AP
tech-c:         NOC21-AP
status:         ASSIGNED NON-PORTABLE
remarks:        For spamming matters, mail to abuse@fpt.vn
mnt-by:         MAINT-VN-FPT
mnt-irt:        IRT-VNNIC-AP
last-modified:  2022-01-17T02:09:51Z
source:         APNIC
```

# Was Hacker so mit Mailkonten treiben

## Mailserver-Log dazu

```
2022-03-20 23:05:45 1nW3gG-00AKd4-KL H=([1.54.219.197]) [1.54.219.197] Warning: processing file ""
for "To: <user@email> -> From: <user@email> / R=<user@email>"
2022-03-20 23:05:45 1nW3gG-00AKd4-KL H=([1.54.219.197]) [1.54.219.197] Warning: send for
<user@email>
2022-03-20 23:05:45 1nW3gG-00AKd4-KL <= user@email H=([1.54.219.197]) [1.54.219.197] P=esmtp S=3223
id=859210656.2022032111106@soderstorf.de
2022-03-20 23:05:45 1nW3gG-00AKd4-KL => /mailacct/xxxxxxxxxxxxxxxxxx/Maildir/ (user@email)
<user@email> R=virtual_user T=address_directory
2022-03-20 23:05:45 1nW3gG-00AKd4-KL Completed
```

Also VON und AN die gleiche Adresse,
allerdings.. kein SMTP-AUTH, weil nicht nötig.

# Was Hacker so mit Mailkonten treiben

Konto nicht kompromitiert,

nur ein einfacher Betrugsversuch.

# Was Hacker so mit Mailkonten treiben

Fragen?