Password-Recovery für Cisco-Router

Der grundsätzliche Vorgang ist einfach: der Router wird dazu gebracht, seine Startup-Config zu ignorieren und in einen Initial-Zustand zu booten, der dem Benutzer die Möglichkeit bietet, ohne Passwort in den privilegierten Modus zu gelangen. Von dort aus kann entweder die alte Startup-Config in die Running-Config geschrieben werden, um bezüglich der Passwörter entsprechend angepasst zu werden, oder es wird eine komplett neue Konfiguration erstellt, die als Startup-Config gespeichert wird. Letzteres ist zwar einfacher aber eher selten, so dass in diesem Tutorial davon ausgegangen wird, dass die vorhandenen Startup-Config weiterhin genutzt werden soll, jedoch mit angepassten Passwörtern.
Die folgenden Schritte müssen vollzogen werden, um ein vollständiges Password-Recovery durchzuführen:

1. **Den Router in den ROM-Monitor-Modus booten:**
   Beim Starten des Routers Escape-Sequenz-Tastenkombination drücken (STRG+UNTBR bei PuTTY)
2. **Im ROM-Monitor-Modus das Config-Register so konfigurieren, dass die Startup-Config ignoriert wird:**
   `ROMMON1>confreg 0x2142`
3. **Anschließend muss der Router neu gestartet werden (z.B. durch Eingabe von `reset`)**
4. **Nach dem Neustart erscheint der Initial Configuration Dialog. Dieser sollte mit NO beendet werden.**
5. **Nun ist der Router ohne seine eigentliche Startup-Config aktiv. Somit kann der Benutzer mit `enable` aus dem User-Mode ohne Passworteingabe in den Privileged Mode wechseln und hat damit volle Admin-Rechte.**
6. **Mit dem folgenden Befehl kann die gespeicherte Originalkonfiguration geladen werden:**
   `R1#copy start run`
7. **Nun können mit entsprechenden Befehlen die gewünschten Passwörter geändert werden, z.B.**
   ```
   R1(config)#enable secret cisco
   R1(config)#username asterix privilege 15 secret cisco
   R1(config-line)#password cisco
   ```
   Werden diese Befehle eingegeben, überschreiben sie ggf. bereits entsprechende vorhandene Konfigurationszeilen.
8. **Anschließend muss die Running-Config in die Startup-Config geschrieben werden:**
   `R1#copy run start`
9. **Darüber hinaus muss das Config-Register wieder zurückgesetzt werden, damit der Router beim nächsten Reboot wieder auf seine Startup-Config zurückgreift:**
   `R1(config)#config-register 0x2102`
10. **Der aktuelle Status kann über den folgenden Befehl überprüft werden.**
    `R1#sh version`
    Die letzte Zeile enthält den aktuellen Wert des Config-Registers.

Im Anschluss enthält der Router in seiner Startup-Config die angepassten Passwörter.