
SBA
Research

COMET

Competence Centers for
Excellent Technologies

Resilient Web Application

How hard can it be?

Bundesministerium
Verkehr, Innovation
und Technologie

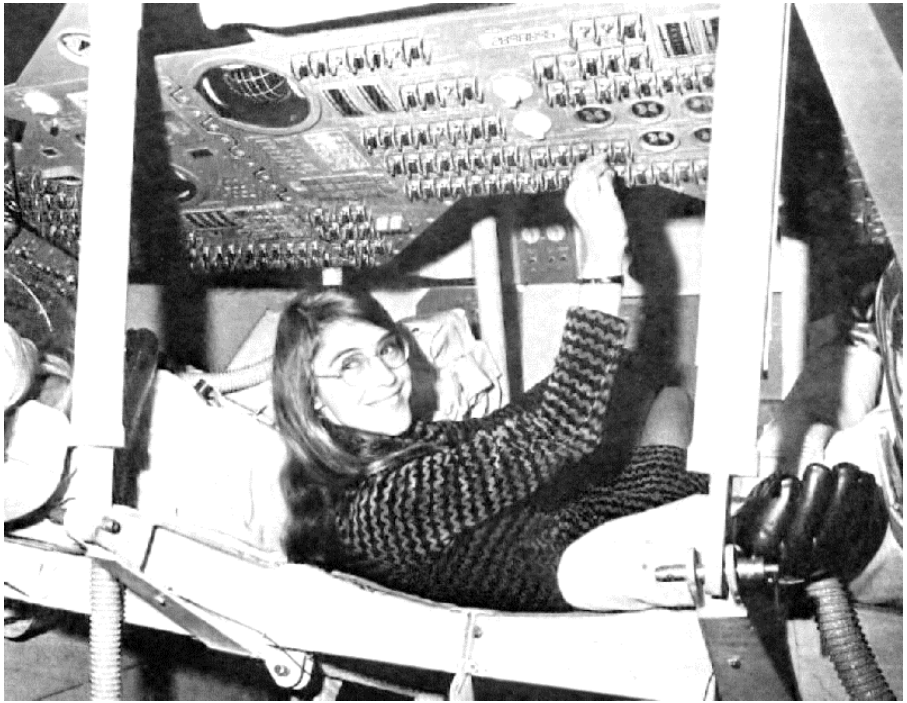
Bundesministerium
Digitalisierung und
Wirtschaftsstandort

FFG
Forschung wirkt.

wirtschafts
agentur
wien
Ein Fonds der
Stadt Wien

FWF
Der Wissenschaftsfonds.

netidee
OPEN INNOVATIONS



Margaret Hamilton,
NASA's First Software Engineer

Resilienz in Software

Build for Failure

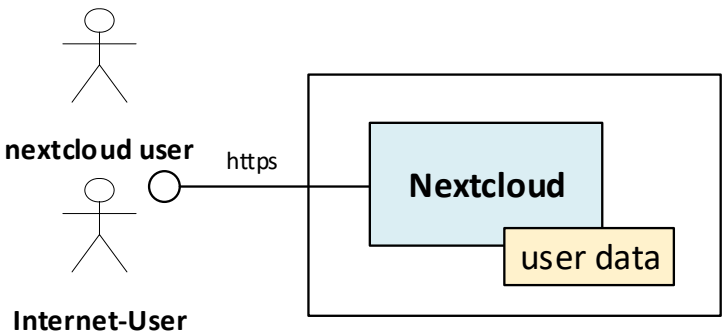
- ein Fehlverhalten wird erwartet
- wenn ein System nicht richtig funktioniert, dann schaltet es sich ab (z.B. Autopilot, Kompass)
- Redundante Systeme übernehmen den Job

Im Falle des Vorhandenseins von Schwachstellen, soll die Sicherheit der Daten gewährleistet werden.

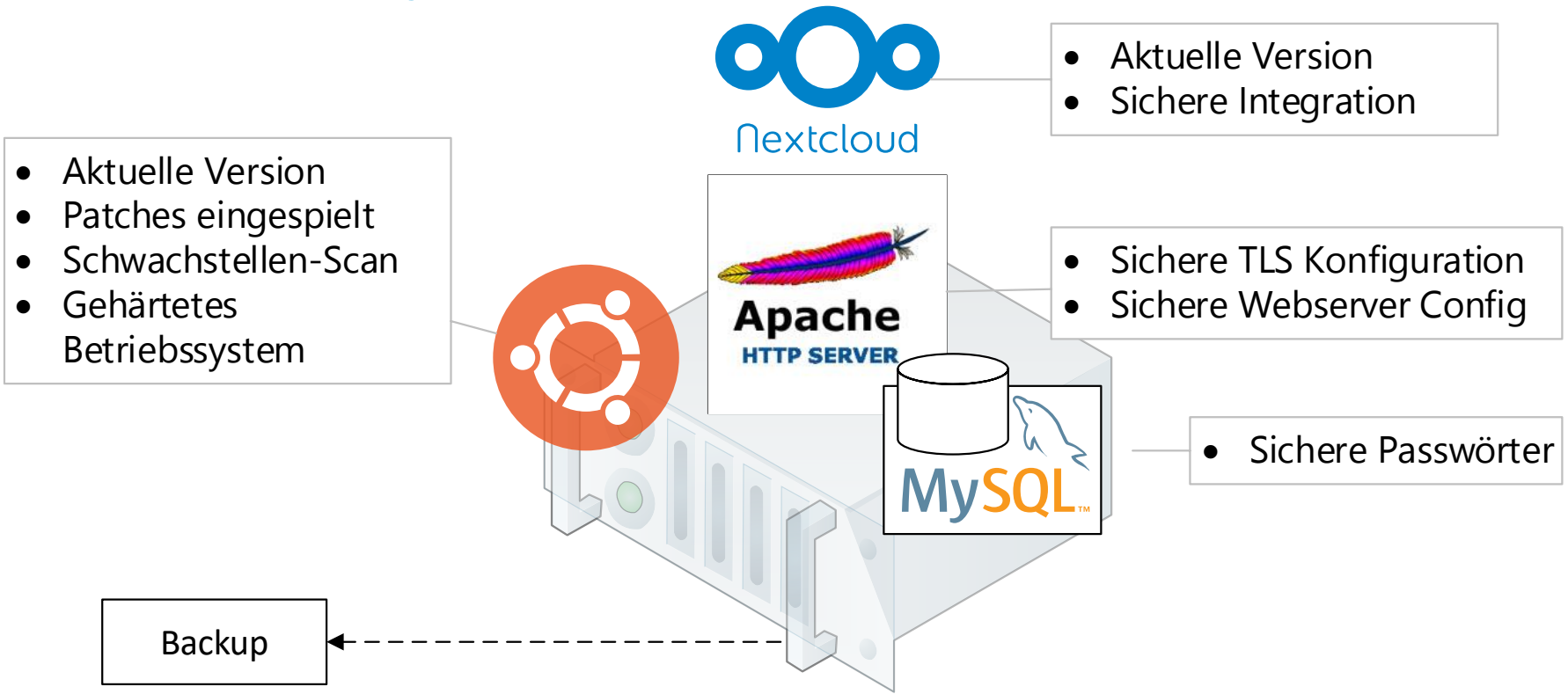

Nextcloud - Protecting your data
Building self-hosted products that allow you to be productive without losing control
Learn more

Einfaches Bedrohungsmodell

- Wer ist der Angreifer?
  - anonyme Internet-Benutzer (Bruteforce)
  - die Nextcloud-Benutzer (Phishing)
  - Schwachstellen in der Nextcloud/in den Apps
- Was sind die Assets?
  - die Benutzerdaten
  - der Server (CPU)



IT-Security Grundschutz



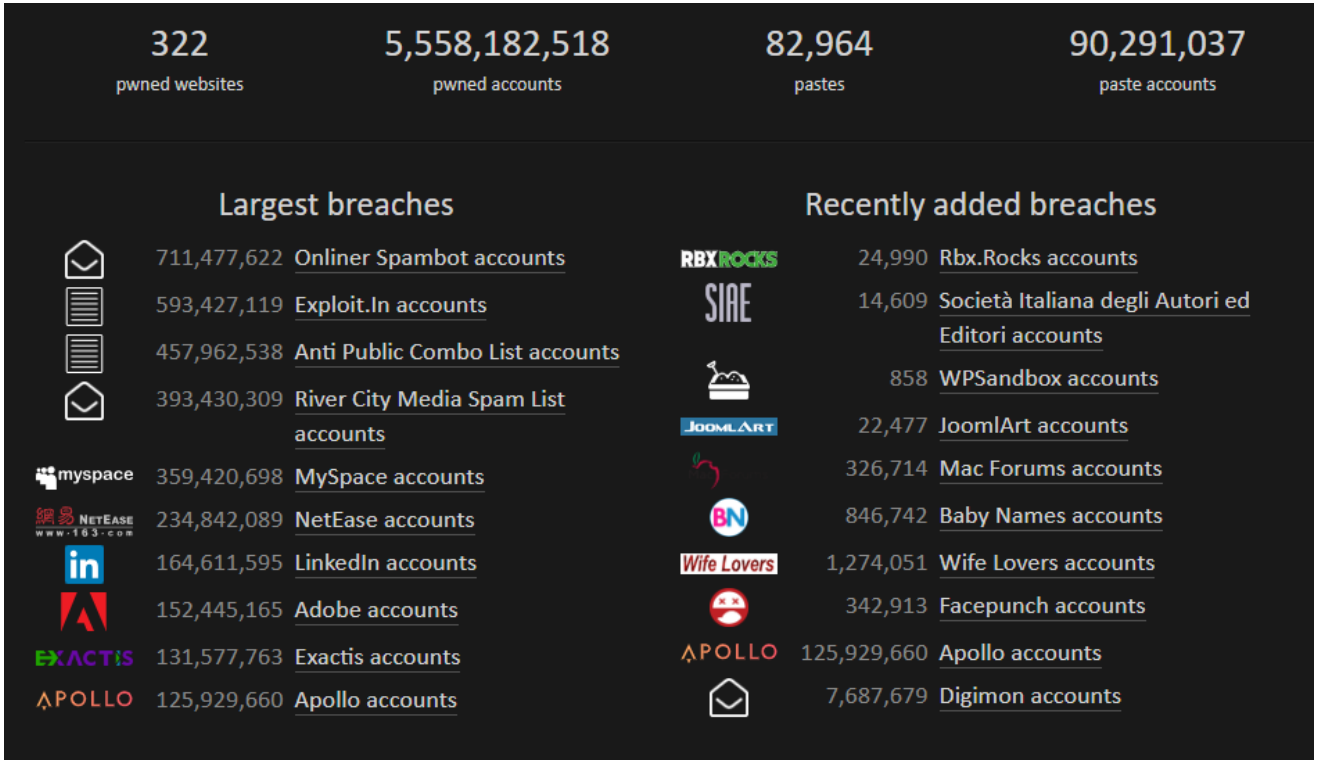
- Aktuelle Version
- Sichere Integration

- Aktuelle Version
- Patches eingespielt
- Schwachstellen-Scan
- Gehärtetes Betriebssystem

- Sichere TLS Konfiguration
- Sichere Webserver Config

- Sichere Passwörter

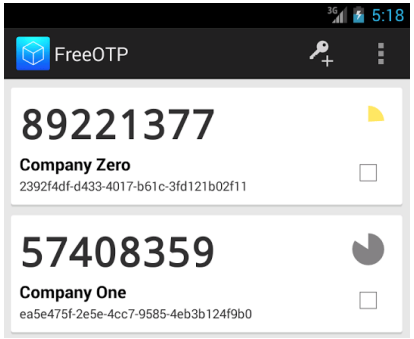
Passwort-Leaks / Data-Breach



https://haveibeenpwned.com/

2-Faktor Authentisierung

SMS

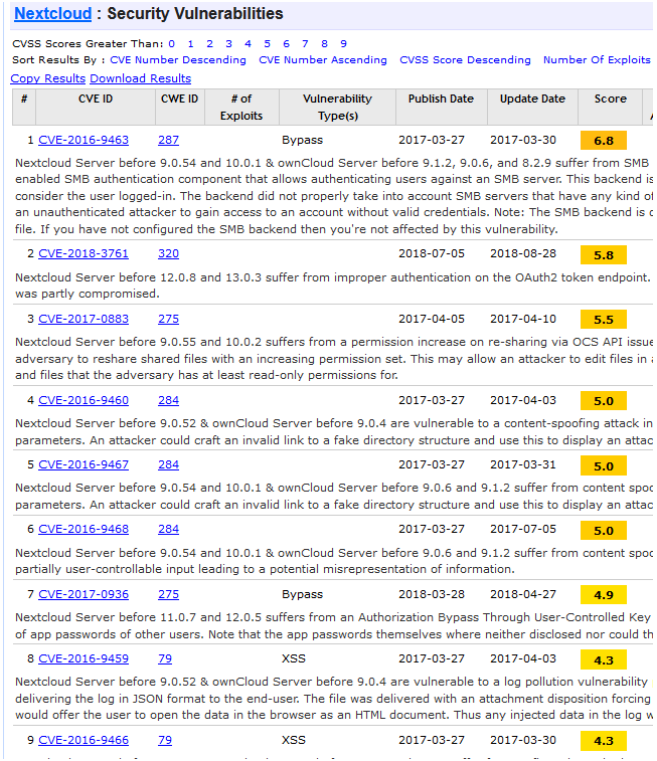


TOTP

U2F/FIDO2

Für Benutzer und Administratoren: **Nextcloud Weboberfläche**
Desktop – und Mobil-Clients und WebDAV? Kein 2-FA
Siehe auch NIST 800-63-3: Digital Identity Guidelines

Nextcloud - Schwachstellen



Nextcloud : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score
1	CVE-2016-9463	287		Bypass	2017-03-27	2017-03-30	6.8

Nextcloud Server before 9.0.54 and 10.0.1 & ownCloud Server before 9.1.2, 9.0.6, and 8.2.9 suffer from SMB enabled SMB authentication component that allows authenticating users against an SMB server. This backend is consider the user logged-in. The backend did not properly take into account SMB servers that have any kind of an unauthenticated attacker to gain access to an account without valid credentials. Note: The SMB backend is c file. If you have not configured the SMB backend then you're not affected by this vulnerability.

2	CVE-2018-3761	320			2018-07-05	2018-08-28	5.8

Nextcloud Server before 12.0.8 and 13.0.3 suffer from improper authentication on the OAuth2 token endpoint. was partly compromised.

3	CVE-2017-0883	275			2017-04-05	2017-04-10	5.5

Nextcloud Server before 9.0.55 and 10.0.2 suffers from a permission increase on re-sharing via OCS API issue adversary to reshare shared files with an increasing permission set. This may allow an attacker to edit files in and files that the adversary has at least read-only permissions for.

4	CVE-2016-9460	284			2017-03-27	2017-04-03	5.0

Nextcloud Server before 9.0.52 & ownCloud Server before 9.0.4 are vulnerable to a content-spoofing attack in parameters. An attacker could craft an invalid link to a fake directory structure and use this to display an attac

5	CVE-2016-9467	284			2017-03-27	2017-03-31	5.0

Nextcloud Server before 9.0.54 and 10.0.1 & ownCloud Server before 9.0.6 and 9.1.2 suffer from content spoo parameters. An attacker could craft an invalid link to a fake directory structure and use this to display an attac

6	CVE-2016-9468	284			2017-03-27	2017-07-05	5.0

Nextcloud Server before 9.0.54 and 10.0.1 & ownCloud Server before 9.0.6 and 9.1.2 suffer from content spoo partially user-controllable input leading to a potential misrepresentation of information.

7	CVE-2017-0936	275		Bypass	2018-03-28	2018-04-27	4.9

Nextcloud Server before 11.0.7 and 12.0.5 suffers from an Authorization Bypass Through User-Controlled Key of app passwords of other users. Note that the app passwords themselves where neither disclosed nor could th

8	CVE-2016-9459	79		XSS	2017-03-27	2017-04-03	4.3

Nextcloud Server before 9.0.52 & ownCloud Server before 9.0.4 are vulnerable to a log pollution vulnerability delivering the log in JSON format to the end-user. The file was delivered with an attachment disposition forcing would offer the user to open the data in the browser as an HTML document. Thus any injected data in the log w

9	CVE-2016-9466	79		XSS	2017-03-27	2017-03-30	4.3

https://cve.mitre.org/

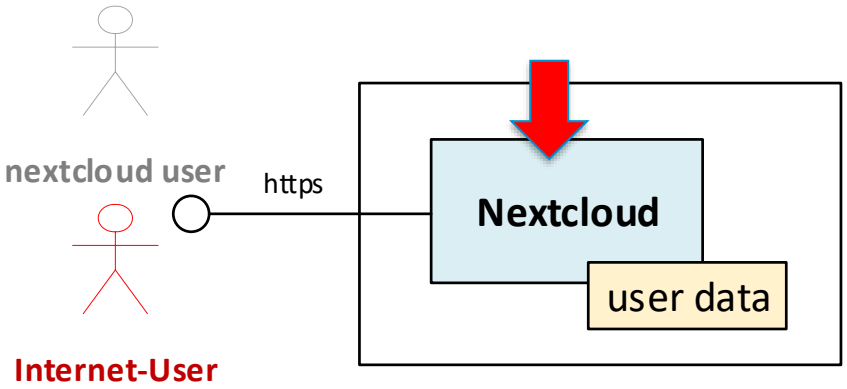
Example: Struts2 OGNL Injection

- Oct, 2006: Initial release
- Jul, 2017: CVE-2017-9791 Remote Code Execution

```
%{(#_='multipart/form-
data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memb
erAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.c
ontainer']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.
OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.ge
tExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#data=@org.ap
ache.struts2.ServletActionContext@getRequest().getHeader('X-
rXFG')).(#f=@java.io.File@createTempFile('CKMy','.exe')).(#f.setExecutable(t
rue)).(#f.deleteOnExit()).(#fos=new java.io.FileOutputStream(#f)).(#d=new
sun.misc.BASE64Decoder().decodeBuffer(#data)).(#fos.write(#d)).(#fos.close()
).(#p=new
java.lang.ProcessBuilder({#f.getAbsolutePath()})).(#p.start()).(#f.delete())
}
```

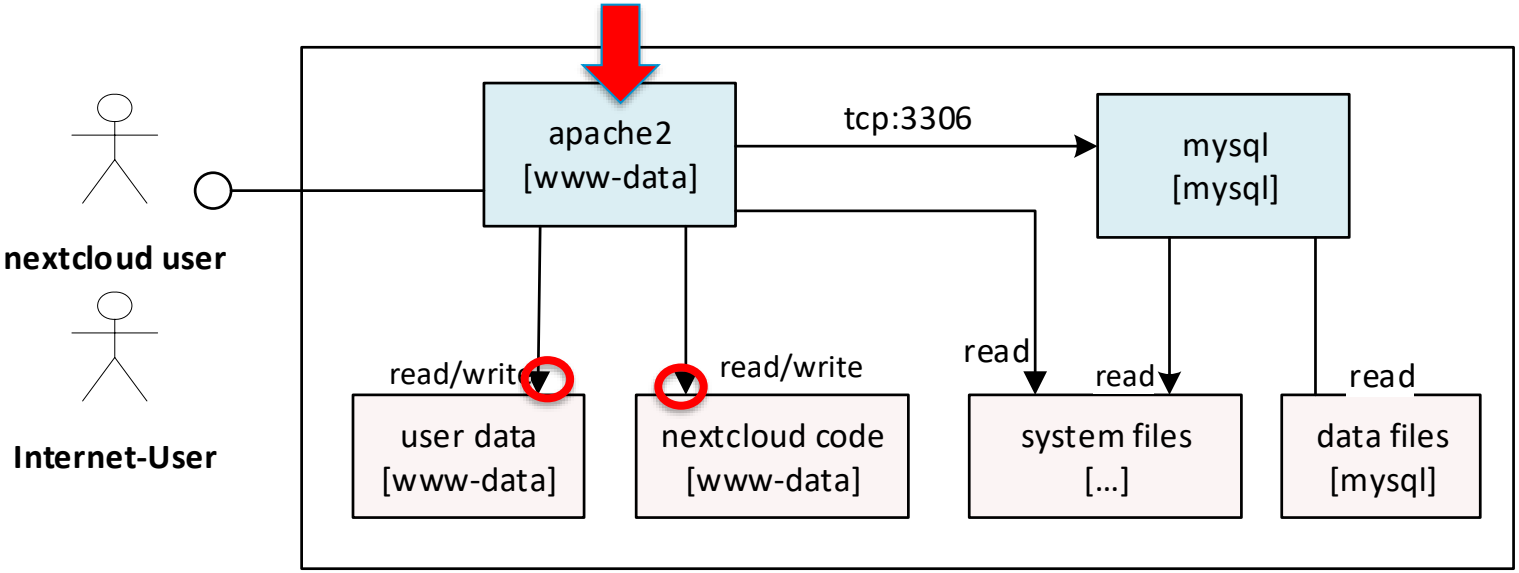
Risiko: RCE-Schwachstelle im System

- Beispiel: eine Remote-Code-Execution Schwachstelle in Nextcloud bzw. einer App
- Nun ist der Prozess selbst der Ausgangspunkt
- Die Daten sind das Ziel



Angriffsmuster verstehen

Threat Model: Out of the Box

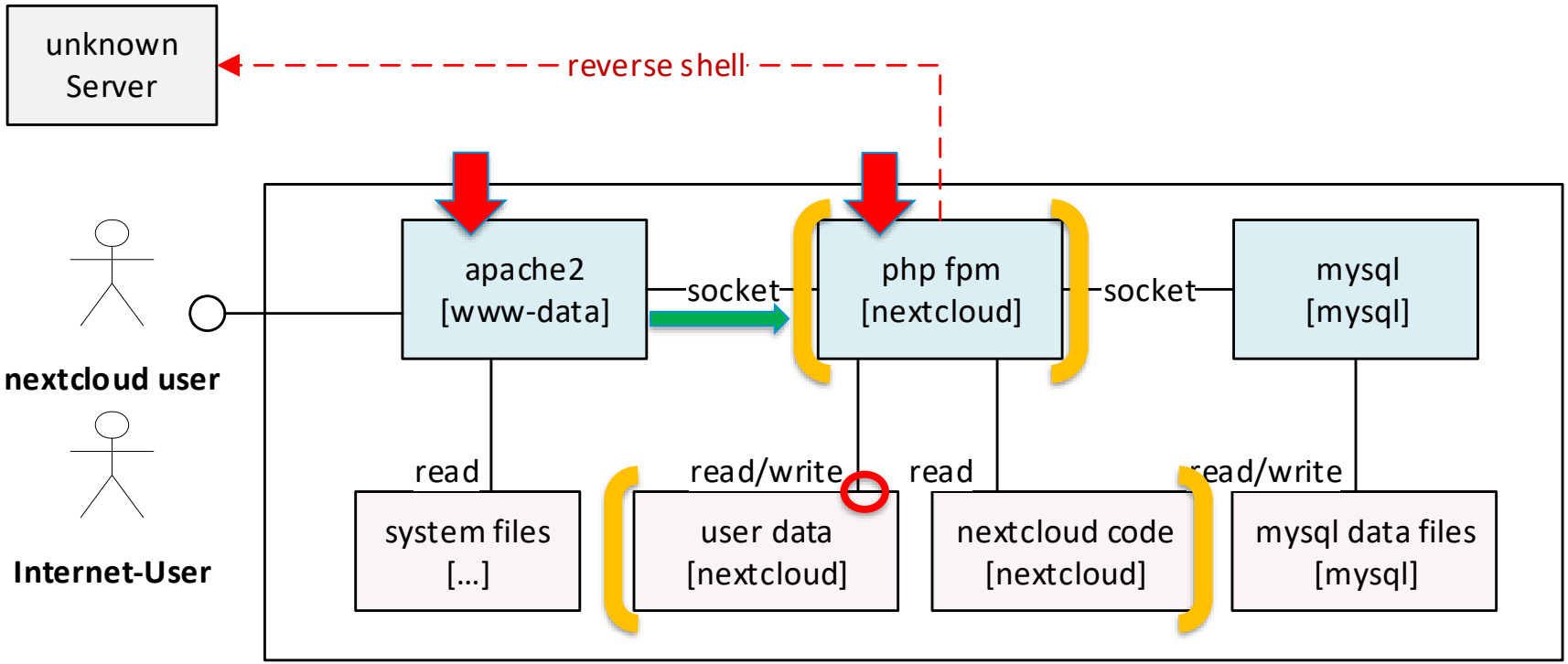



apache2
mysql
PHP

https://www.ebay.com/itm/Kenley-Mini-Sandbox-for-Desk-Miniature-Beach-Zen-Garden-Sand-Toys-Play-Kit-/253472884998

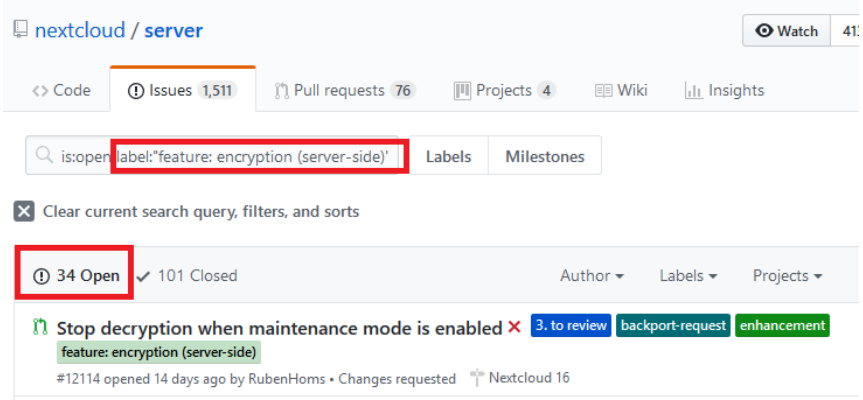
Prozesstrennung

Threat Model: Iteration 2



Verschlüsselung?

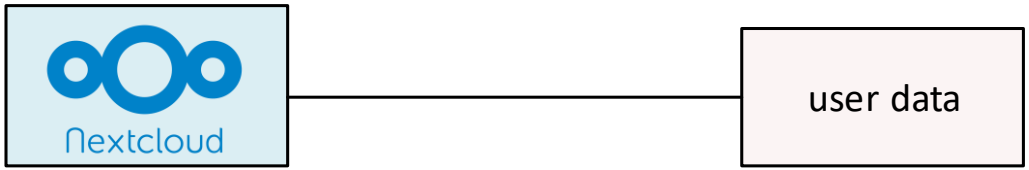
- Serverseitige Verschlüsselung erscheint nicht stabil:



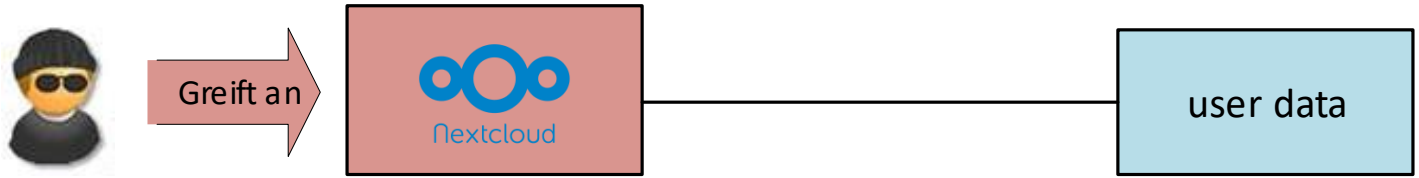
- Clientseitige Verschlüsselung
  - Einige Funktionseinschränkungen
  - Noch Alpha

Schutz der Benutzerdaten: Normalfall

- Direkter Zugriff auf die Benutzerdaten:

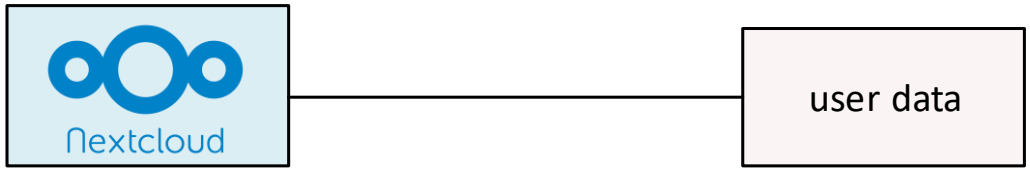


- Im Fall einer Kompromittierung:

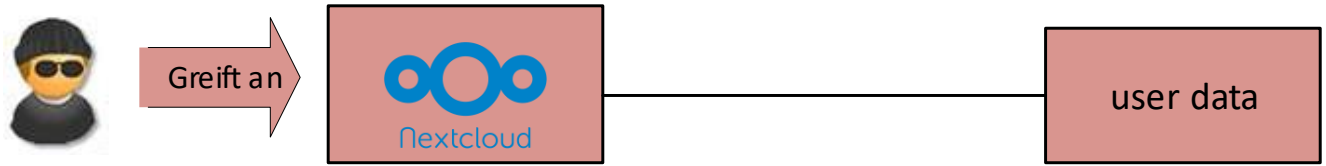


Schutz der Benutzerdaten: Normalfall

- Direkter Zugriff auf die Benutzerdaten:



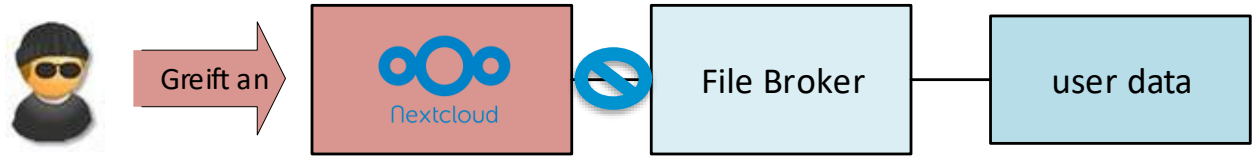
- Im Fall einer Kompromittierung:



Schutz der Benutzerdaten: Auftrennung

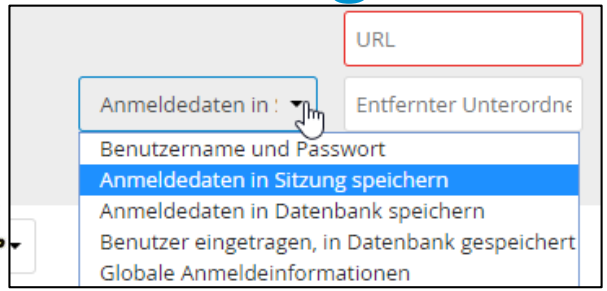
- Webservice authentisiert sich am File Broker als der jeweilige Benutzer
  - Angreifer benötigt auch das Benutzerpasswort

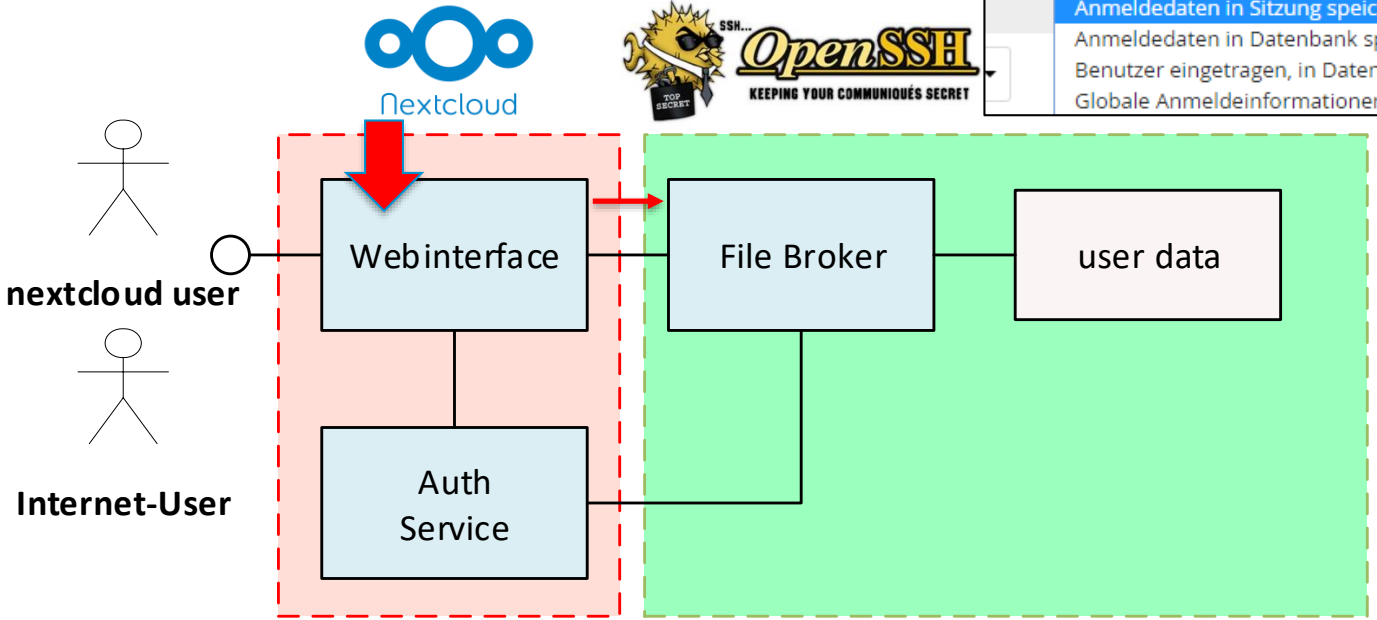
- Im Fall einer Kompromittierung:



Schutz der Benutzerdaten: External Storage

- Einbindung als *External Storage:*





Notwendige Nextcloud-Konfiguration

- Keine Schreibrechte auf Nextcloud – Code:
- Benötigt spezielle NC Konfiguration:

```
'config_is_read_only' => true,
'appstoreenabled' => false,
"apps_paths" => array (
    0 => array (
        "path"     => OC::$SERVERROOT."/apps",
        "url"      => "/apps",
        "writable" => false,
    )
)
```

- Beim Einbinden des externen SFTP
  - Option „Anmeldedaten in Sitzung speichern“
  - Verhindert Persistierung des Zugangs

Einschränkungen

- „Teilen“ mit anderen Benutzern nicht möglich
- Funktioniert für Dateien
  - Nicht für Kontakte, Kalender und andere Apps
- Administration für Nextcloud aufwändiger
  - Kein NC-Update via Webinterface
  - Keine Installation von Apps via Webinterface

Bewertung der Maßnahmen

- **2-Faktor Authentisierung** - kompensiert Passwort-Leaks
  - Nicht von allen Komponenten unterstützt -> feature loss
  - Erhöht Administrationsaufwand. Erhöht Sicherheit
- **Aufsplittung der Services**
  - Mehrere Schutzschichten
  - Zusammen mit **restriktiven Berechtigungen**
    - Erhöht den Integrationsaufwand
    - Update muss manuell gemacht werden
    - beschränkt Eskalationspfade
- => Resilientes Nextcloud-Server, das Schwachstellen kompensiert

COMET

Competence Centers for
Excellent Technologies

Ulrich Bayer

ubayer@sba-research.org

Reinhard Kugler

rkugler@sba-research.org

SBA Research gGmbH
Favoritenstraße 16
1040 Vienna
www.sba-research.org

sec4dev

sec4dev
25.-27. Feb 2019
CONFERENCE
+ BOOTCAMP