

Linux Security

Sven Höckel



Agenda



Agenda

- ▶ Geschichtliches zu Linux



Agenda

- ▶ Geschichtliches zu Linux
- ▶ Zugriffsrechte



Agenda

- ▶ Geschichtliches zu Linux
- ▶ Zugriffsrechte
- ▶ Kernelerweiterungen
 - ▶ LSM Framework
 - ▶ SELinux
 - ▶ AppArmor
 - ▶ RSBAC & Systrace



Geschichtliches (1)



Geschichtliches (1)

- ▶ 1991: Ankündigung auf Usenix



Geschichtliches (1)

- ▶ 1991: Ankündigung auf Usenix
- ▶ 1994: Version 1.0



Geschichtliches (1)

- ▶ 1991: Ankündigung auf Usenix
- ▶ 1994: Version 1.0
- ▶ 1996: Version 2.0



Geschichtliches (1)

- ▶ 1991: Ankündigung auf Usenix
- ▶ 1994: Version 1.0
- ▶ 1996: Version 2.0
- ▶ 1999: Version 2.2



Geschichtliches (1)

- ▶ 1991: Ankündigung auf Usenix
- ▶ 1994: Version 1.0
- ▶ 1996: Version 2.0
- ▶ 1999: Version 2.2
- ▶ 2001: Version 2.4



Geschichtliches (1)

- ▶ 1991: Ankündigung auf Usenix
- ▶ 1994: Version 1.0
- ▶ 1996: Version 2.0
- ▶ 1999: Version 2.2
- ▶ 2001: Version 2.4
- ▶ 2003: Version 2.6

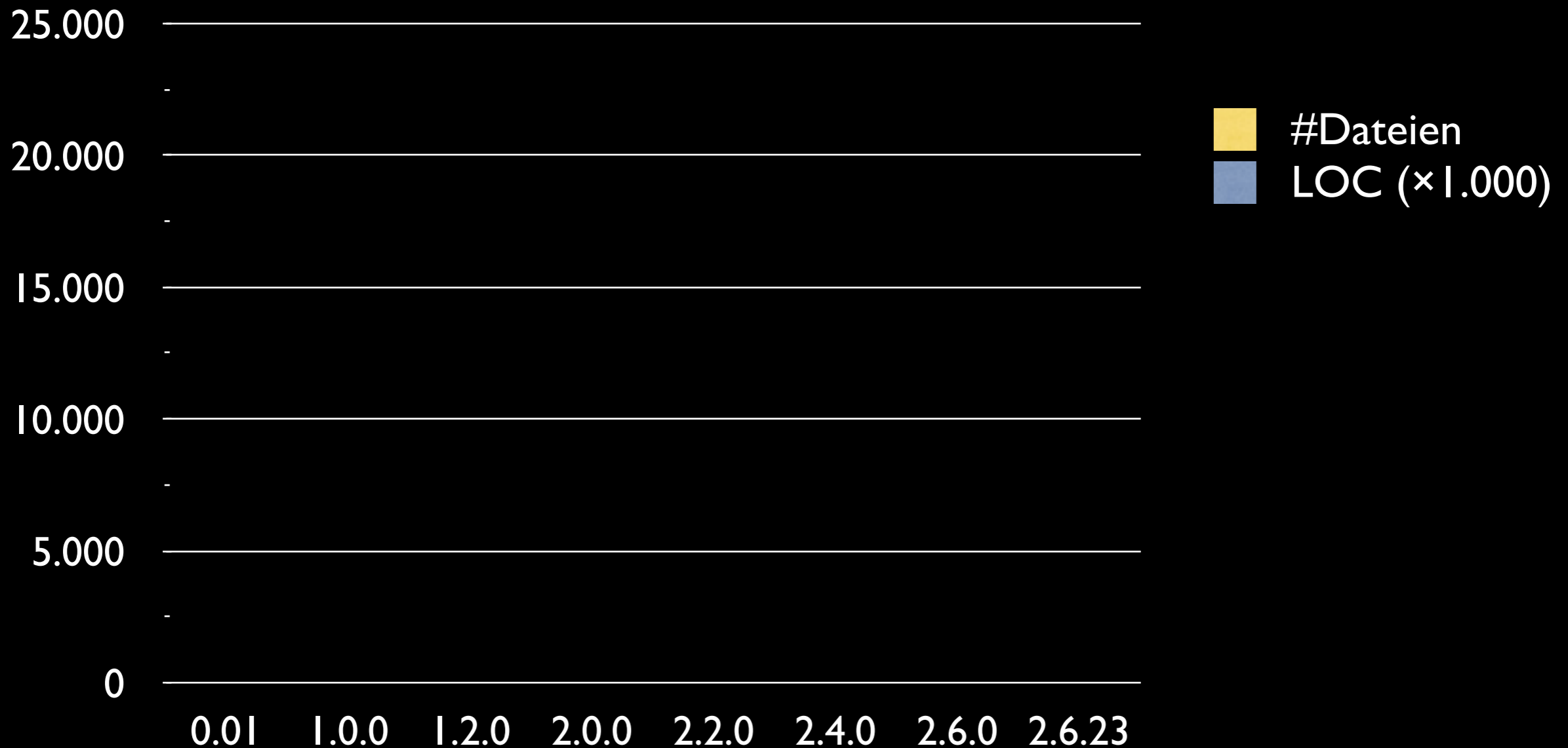


Geschichtliches (2)



Geschichtliches (2)

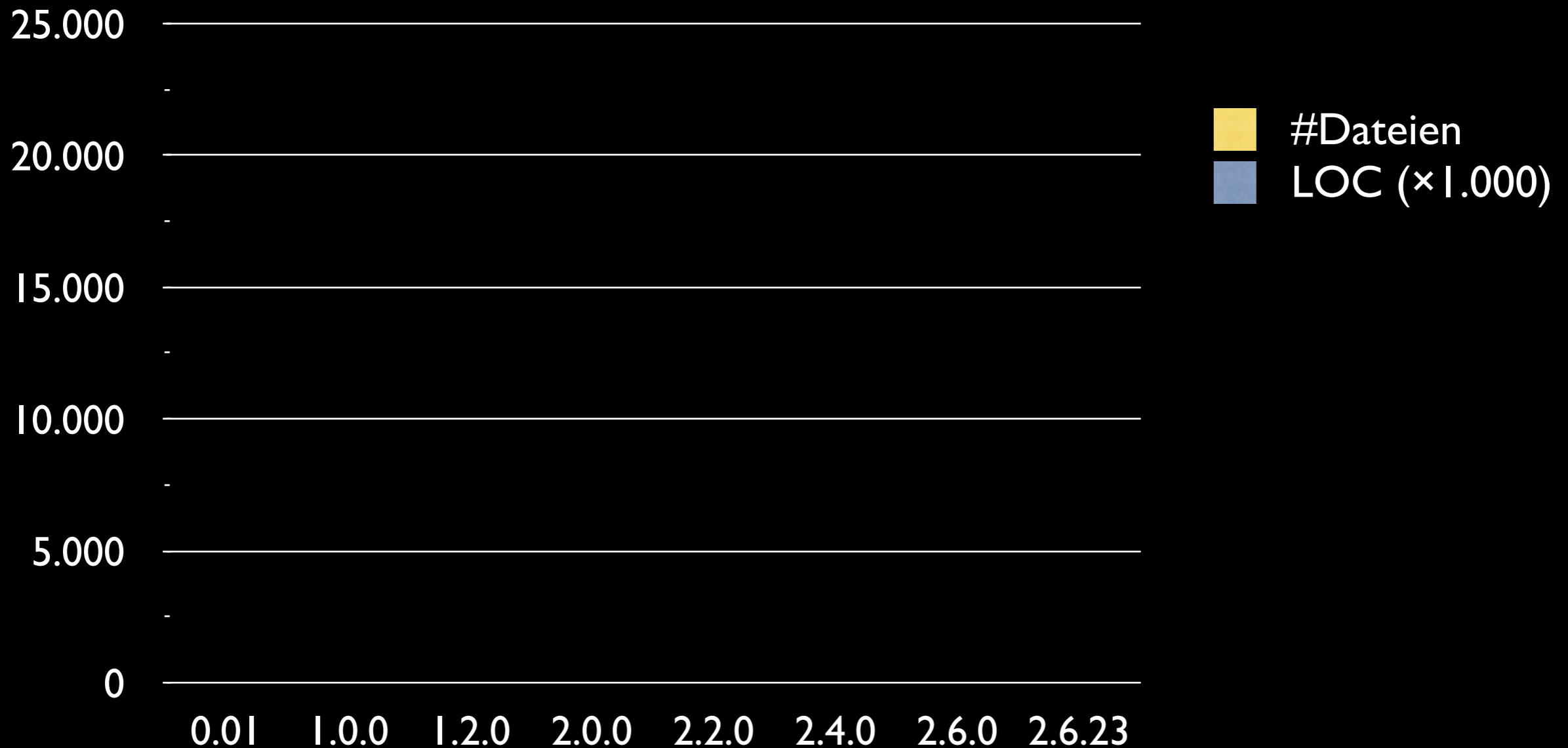
► Ein paar Zahlen:





Geschichtliches (2)

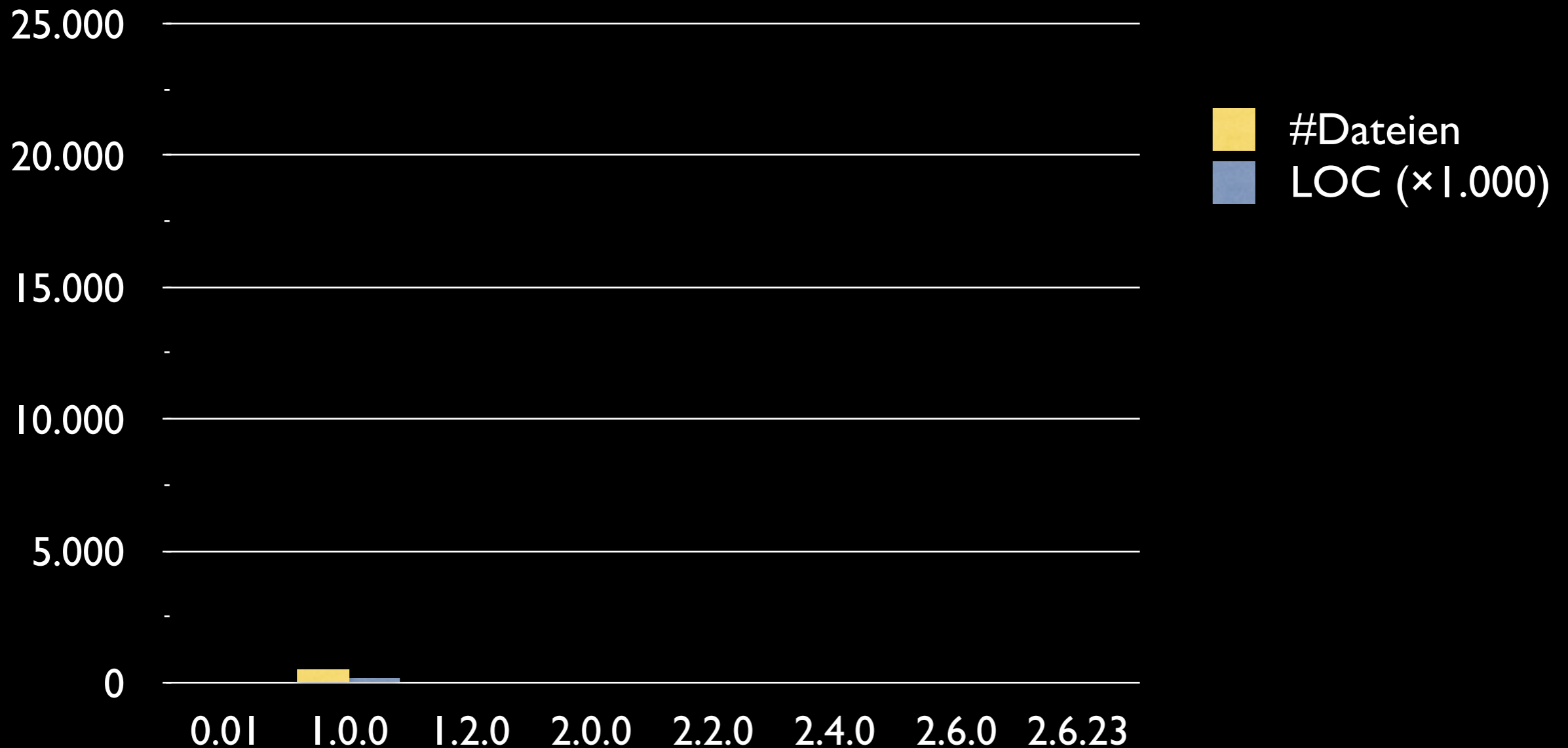
► Ein paar Zahlen:





Geschichtliches (2)

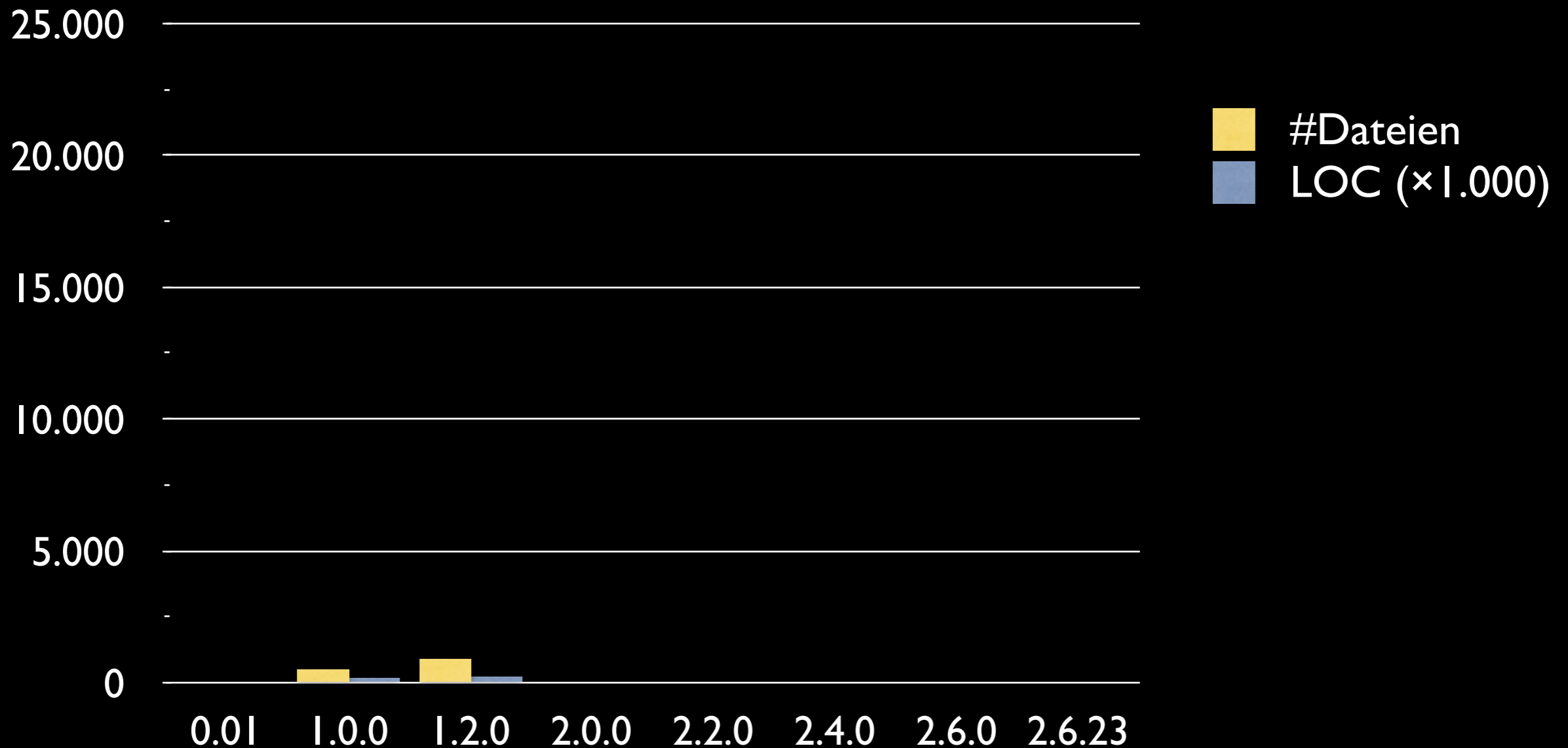
► Ein paar Zahlen:





Geschichtliches (2)

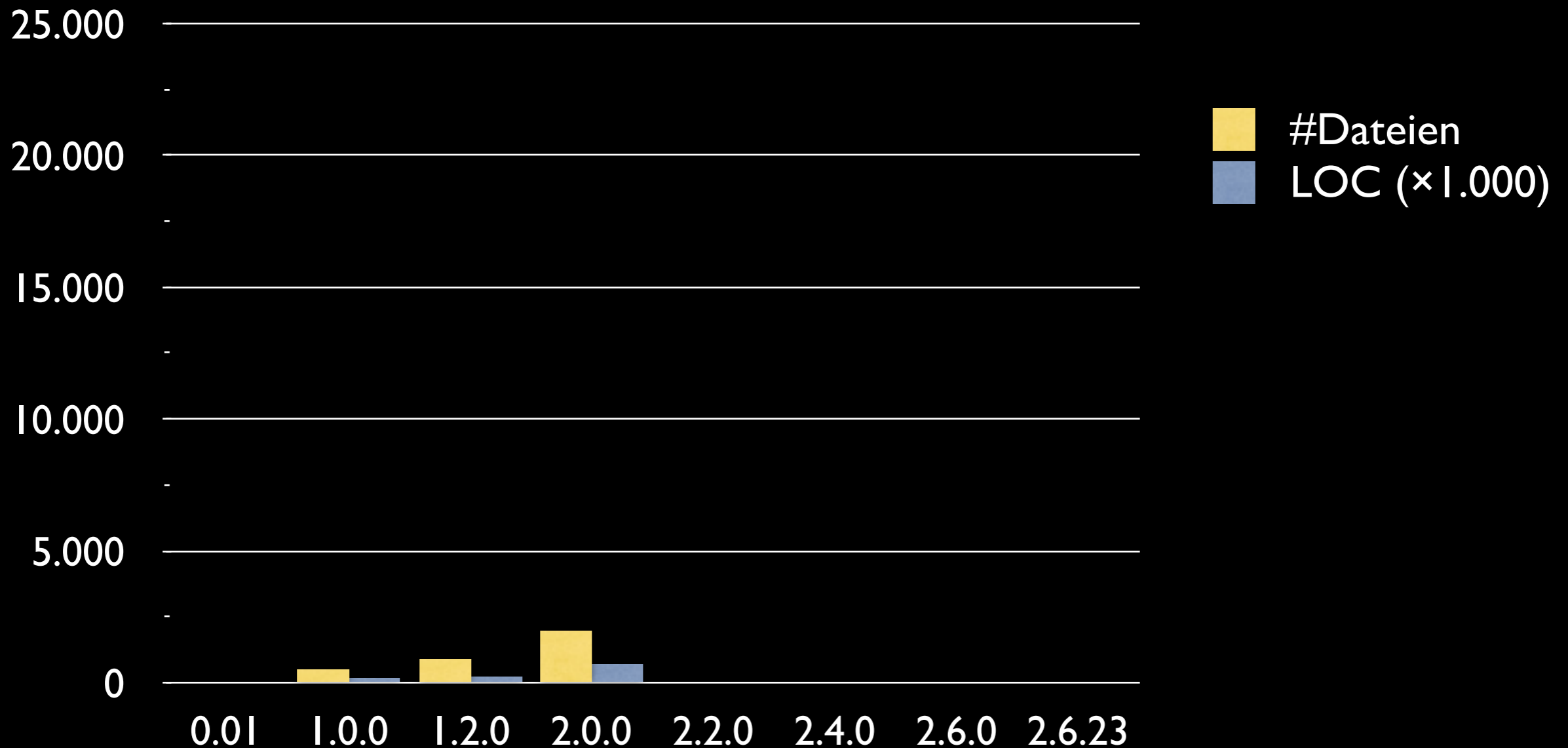
► Ein paar Zahlen:





Geschichtliches (2)

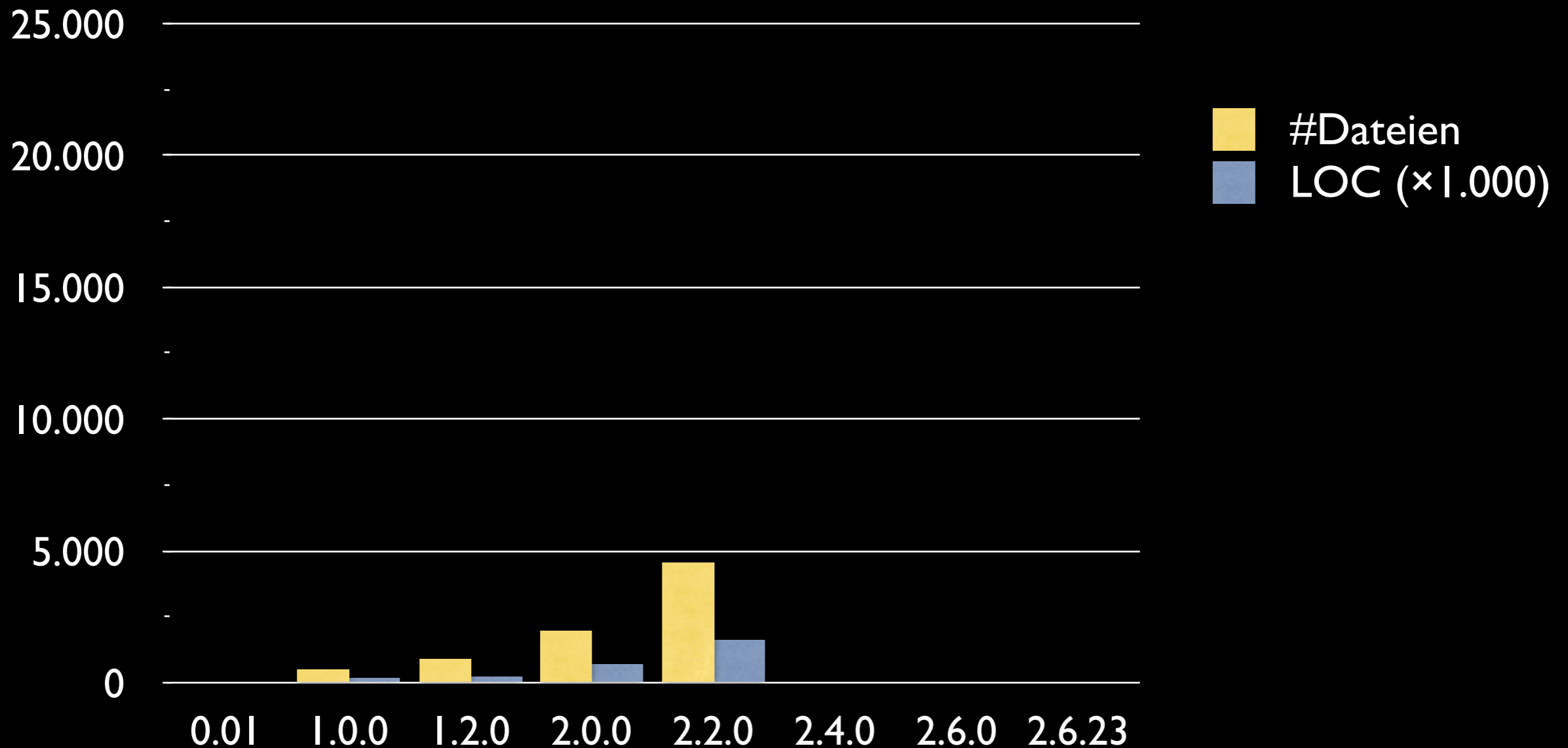
► Ein paar Zahlen:





Geschichtliches (2)

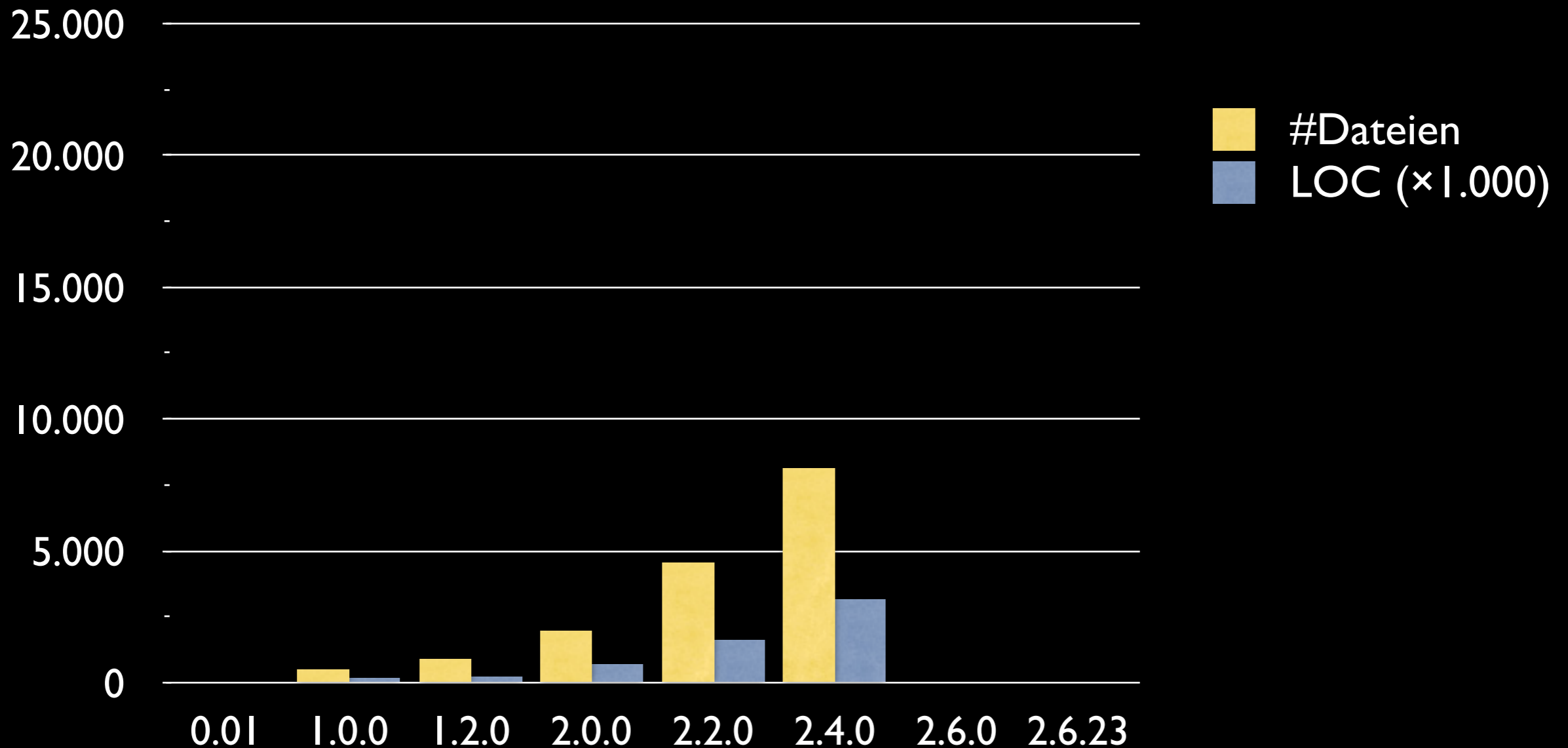
► Ein paar Zahlen:





Geschichtliches (2)

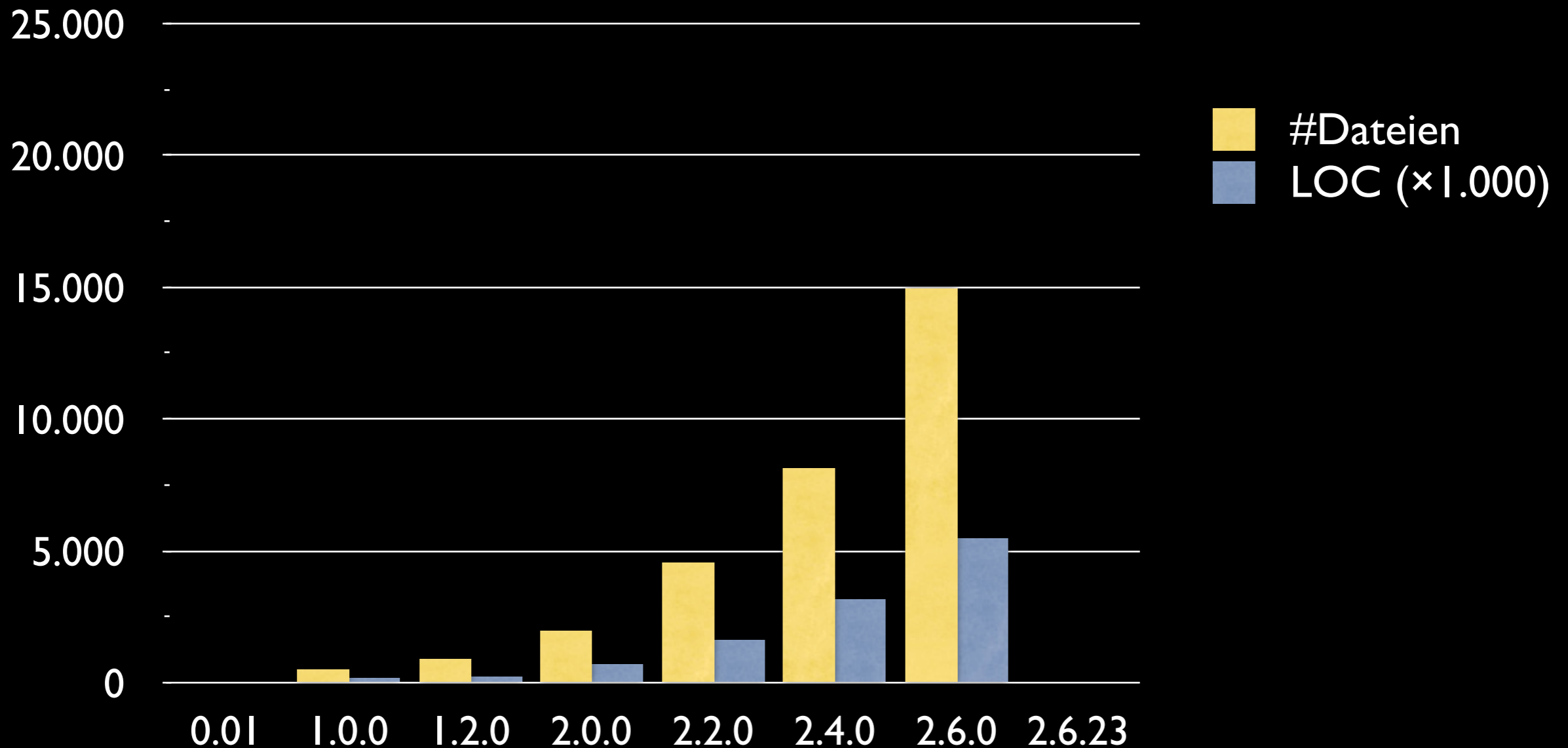
► Ein paar Zahlen:





Geschichtliches (2)

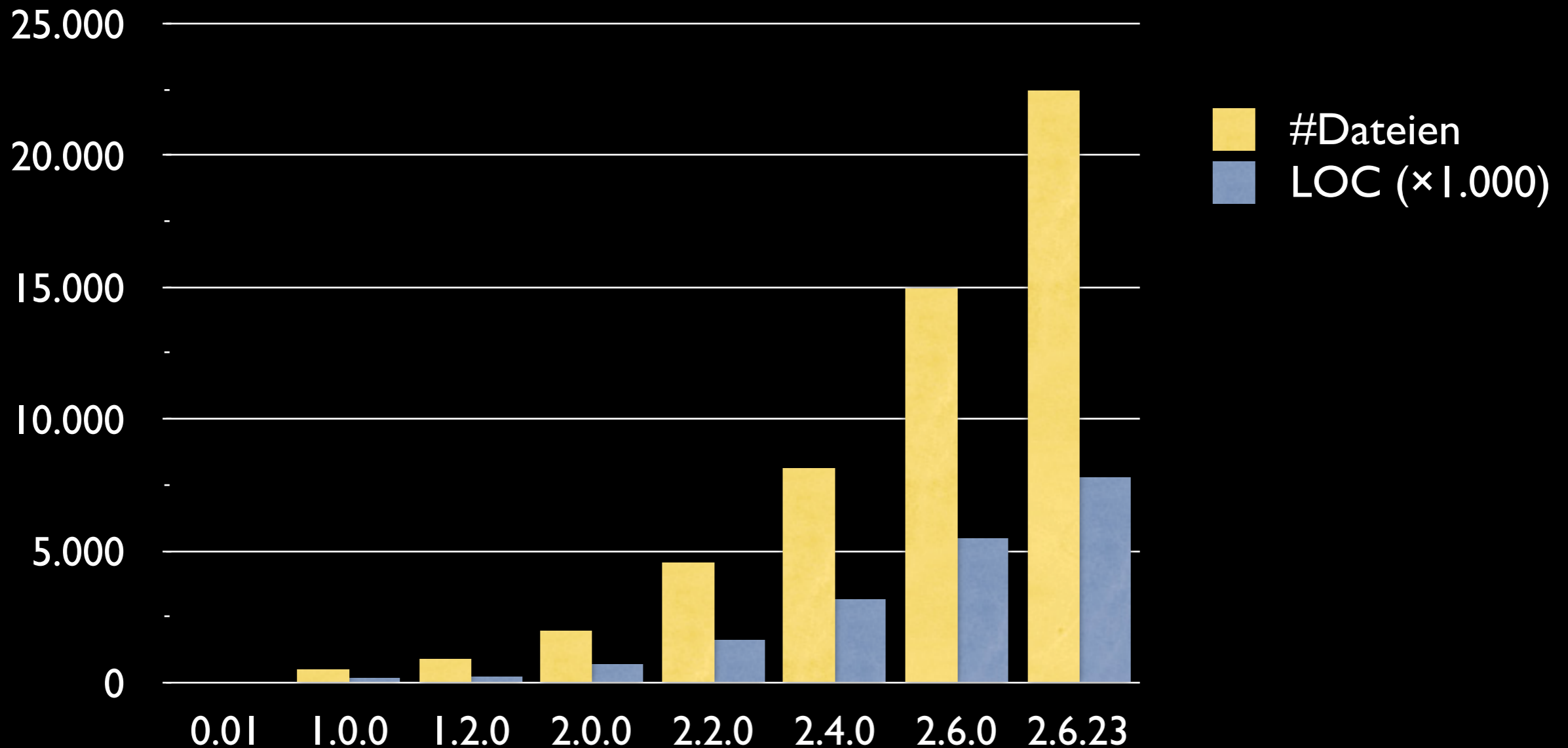
► Ein paar Zahlen:





Geschichtliches (2)

► Ein paar Zahlen:





Zugriffsrechte (1)



Zugriffsrechte (1)

- ▶ DAC: Discretionary Access Control



Zugriffsrechte (1)

- ▶ DAC: Discretionary Access Control



Zugriffsrechte (1)

- ▶ DAC: Discretionary Access Control
- ▶ 3 Arten:
 - ▶ Eigentümer
 - ▶ Gruppenmitglieder
 - ▶ Alle anderen



Zugriffsrechte (1)

- ▶ DAC: Discretionary Access Control
- ▶ 3 Arten:
 - ▶ Eigentümer
 - ▶ Gruppenmitglieder
 - ▶ Alle anderen
- ▶ Berechtigungen:
 - ▶ Lesen (r)
 - ▶ Schreiben (w)
 - ▶ Ausführen (x)



Zugriffsrechte (2)



Zugriffsrechte (2)

- ▶ Beispiel:

- ▶ `ls -l /home/tuser/`

- `-rw-r--r-- 1 tuser users 1234 14. Dez 16:00 Datei`
 - `drwxrwx--- 2 tuser users 240 10. Dez 11:11 Dir`
 - `-rwxr-x--- 1 tuser users 120 11. Dez 20:43 Exe`



Zugriffsrechte (2)

▶ Beispiel:

▶ `ls -l /home/tuser/`

```
-rw-r--r-- 1 tuser users 1234 14. Dez 16:00 Datei  
drwxrwx--- 2 tuser users 240 10. Dez 11:11 Dir  
-rwxr-x--- 1 tuser users 120 11. Dez 20:43 Exe
```

→ Typfeld:

- ▶ `-`: Normale Datei
- ▶ `d`: Verzeichnis
- ▶ `l`: Link



Zugriffsrechte (2)

▶ Beispiel:

▶ `ls -l /home/tuser/`

```
-rw-r--r-- 1 tuser users 1234 14. Dez 16:00 Datei  
drwxrwx--- 2 tuser users 240 10. Dez 11:11 Dir  
-rwxr-x--- 1 tuser users 120 11. Dez 20:43 Exe
```



Zugriffsrechte für den Eigentümer:

- ▶ r: Lesen
- ▶ w: Schreiben (Dateien anlegen)
- ▶ x: Ausführen (Verzeichniswechsel)



Zugriffsrechte (2)

▶ Beispiel:

▶ `ls -l /home/tuser/`

```
-rw-r--r-- 1 tuser users 1234 14. Dez 16:00 Datei  
drwxrwx--- 2 tuser users 240 10. Dez 11:11 Dir  
-rwxr-x--- 1 tuser users 120 11. Dez 20:43 Exe
```

→ Zugriffsrechte für die Gruppe



Zugriffsrechte (2)

▶ Beispiel:

▶ `ls -l /home/tuser/`

```
-rw-r--r-- 1 tuser users 1234 14. Dez 16:00 Datei  
drwxrwx--- 2 tuser users 240 10. Dez 11:11 Dir  
-rwxr-x--- 1 tuser users 120 11. Dez 20:43 Exe
```

→ Zugriffsrechte für alle anderen



Zugriffsrechte (3)



Zugriffsrechte (3)

- ▶ Problem: DAC reicht für bestimmte Aufgaben nicht aus
→ SUID bit



Zugriffsrechte (3)

- ▶ Problem: DAC reicht für bestimmte Aufgaben nicht aus
→ SUID bit
- ▶ Beispiel:
 - ▶ `ls -l /bin/passwd`
`-rws--x--x 1 root root 30052 5. Nov 17:28 /bin/passwd`



Zugriffsrechte (3)

- ▶ Problem: DAC reicht für bestimmte Aufgaben nicht aus
→ SUID bit
- ▶ Beispiel:
 - ▶ `ls -l /bin/passwd`
`-rws--x--x 1 root root 30052 5. Nov 17:28 /bin/passwd`



Zugriffsrechte (3)

- ▶ Problem: DAC reicht für bestimmte Aufgaben nicht aus
→ SUID bit
- ▶ Beispiel:
 - ▶ `ls -l /bin/passwd`
`-rws--x--x 1 root root 30052 5. Nov 17:28 /bin/passwd`
- ▶ Sicherheitslücken in SUID-Programmen kompromittieren Gesamtsystem



Kernelerweiterungen



Kernelerweiterungen

- ▶ 2 Arten von Kernelerweiterungen:



Kernelerweiterungen

- ▶ 2 Arten von Kernelerweiterungen:
 - ▶ Kernel Patches
(Systrace, RSBAC, ...)
 - ▶ Kernel Modul als LSM
(SELinux, AppArmor)



LSM (1)



LSM (1)

- ▶ Linux Security Modules (LSM)



LSM (1)

- ▶ Linux Security Modules (LSM)



LSM (1)

- ▶ Linux Security Modules (LSM)
- ▶ „Keine Festlegung auf ein Sicherheitsmodell“



LSM (1)

- ▶ Linux Security Modules (LSM)
- ▶ „Keine Festlegung auf ein Sicherheitsmodell“
- ▶ Ab Kernel 2.6 integraler Bestandteil



LSM (2)



LSM (2)

- ▶ Wie funktioniert es?
 - ▶ Hook-Funktionen an Stellen, wo Zugriffsberechtigung entschieden wird. Z.B. `mkdir()`



LSM (2)

- ▶ Wie funktioniert es?
 - ▶ Hook-Funktionen an Stellen, wo Zugriffsberechtigung entschieden wird. Z.B. `mkdir()`
- ▶ Pro/Kontra:
 - ▶ Einheitliche, stabile Schnittstelle
 - ▶ Eingeschränkte Funktionalität
 - ▶ Sicherheitsproblem



SELinux (1)



SELinux (1)

- ▶ NSA veröffentlicht FLASK-Architektur als Patch für Kernel 2.2



SELinux (1)

- ▶ NSA veröffentlicht FLASK-Architektur als Patch für Kernel 2.2
- ▶ ab 2001 Portierung auf LSM



SELinux (1)

- ▶ NSA veröffentlicht FLASK-Architektur als Patch für Kernel 2.2
- ▶ ab 2001 Portierung auf LSM
- ▶ Ab Kernel 2.6.0 integraler Bestandteil



SELinux (1)

- ▶ NSA veröffentlicht FLASK-Architektur als Patch für Kernel 2.2
- ▶ ab 2001 Portierung auf LSM
- ▶ Ab Kernel 2.6.0 integraler Bestandteil



SELinux (1)

- ▶ NSA veröffentlicht FLASK-Architektur als Patch für Kernel 2.2
- ▶ ab 2001 Portierung auf LSM
- ▶ Ab Kernel 2.6.0 integraler Bestandteil
- ▶ Unterstützte Modelle:
TE, RBAC und MLS/MCS



SELinux (2)



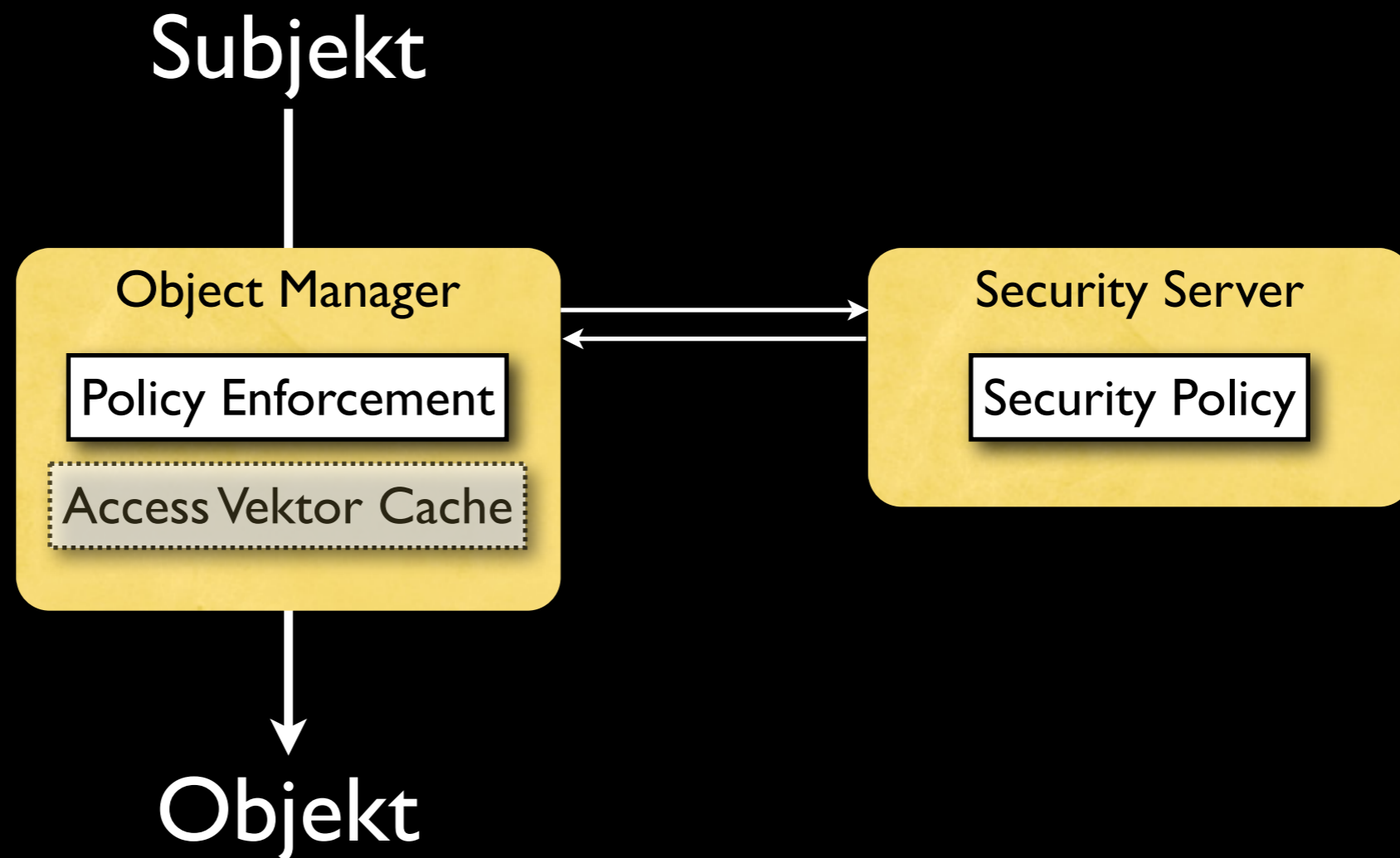
SELinux (2)

- ▶ Architektur



SELinux (2)

▶ Architektur





AppArmor



AppArmor

- ▶ 1998 Entwickelt unter dem Namen SubDomain



AppArmor

- ▶ 1998 Entwickelt unter dem Namen SubDomain
- ▶ 2004 Übernahme durch Novell, Integration in SuSE



AppArmor

- ▶ 1998 Entwickelt unter dem Namen SubDomain
- ▶ 2004 Übernahme durch Novell, Integration in SuSE
- ▶ 2005 in AppArmor umbenannt



AppArmor

- ▶ 1998 Entwickelt unter dem Namen SubDomain
- ▶ 2004 Übernahme durch Novell, Integration in SuSE
- ▶ 2005 in AppArmor umbenannt
- ▶ 2006 unter GPL freigegeben (OpenSuSE)



RSBAC (1)



RSBAC (1)

- ▶ Roleset Based Access Control



RSBAC (1)

- ▶ Roleset Based Access Control
- ▶ 1996: Beginn der Entwicklung als Diplomarbeit



RSBAC (1)

- ▶ Roleset Based Access Control
- ▶ 1996: Beginn der Entwicklung als Diplomarbeit
- ▶ Besteht aus Kernelpatch + Kommandozeilentools



RSBAC (1)

- ▶ Roleset Based Access Control
- ▶ 1996: Beginn der Entwicklung als Diplomarbeit
- ▶ Besteht aus Kernelpatch + Kommandozeilentools
- ▶ Framework für Sicherheitsmodule

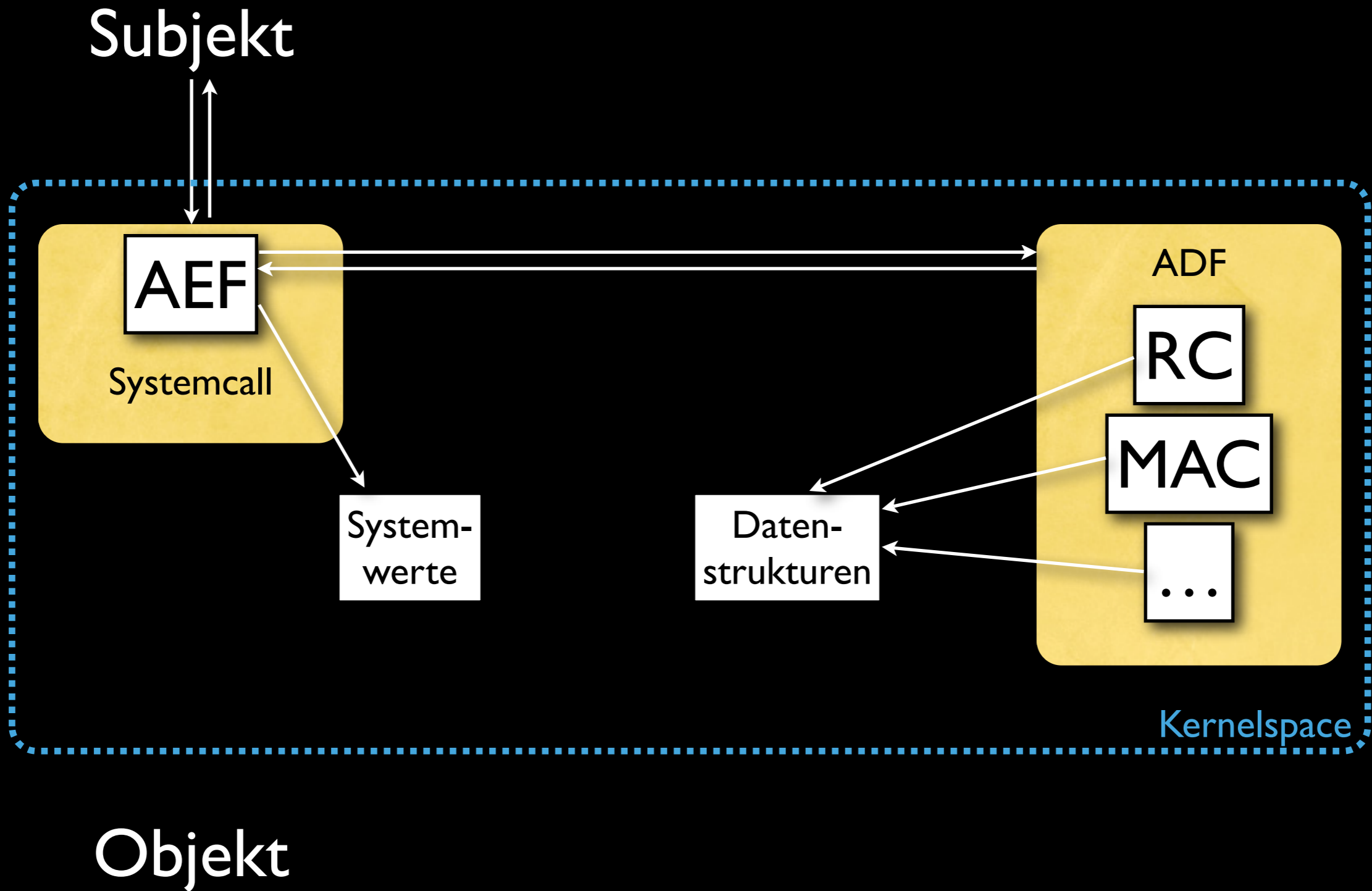


RSBAC (1)

- ▶ Roleset Based Access Control
- ▶ 1996: Beginn der Entwicklung als Diplomarbeit
- ▶ Besteht aus Kernelpatch + Kommandozeilentools
- ▶ Framework für Sicherheitsmodule
- ▶ Implementierte Module: MAC, RC, ACL, UM, DAZ, JAIL, ...

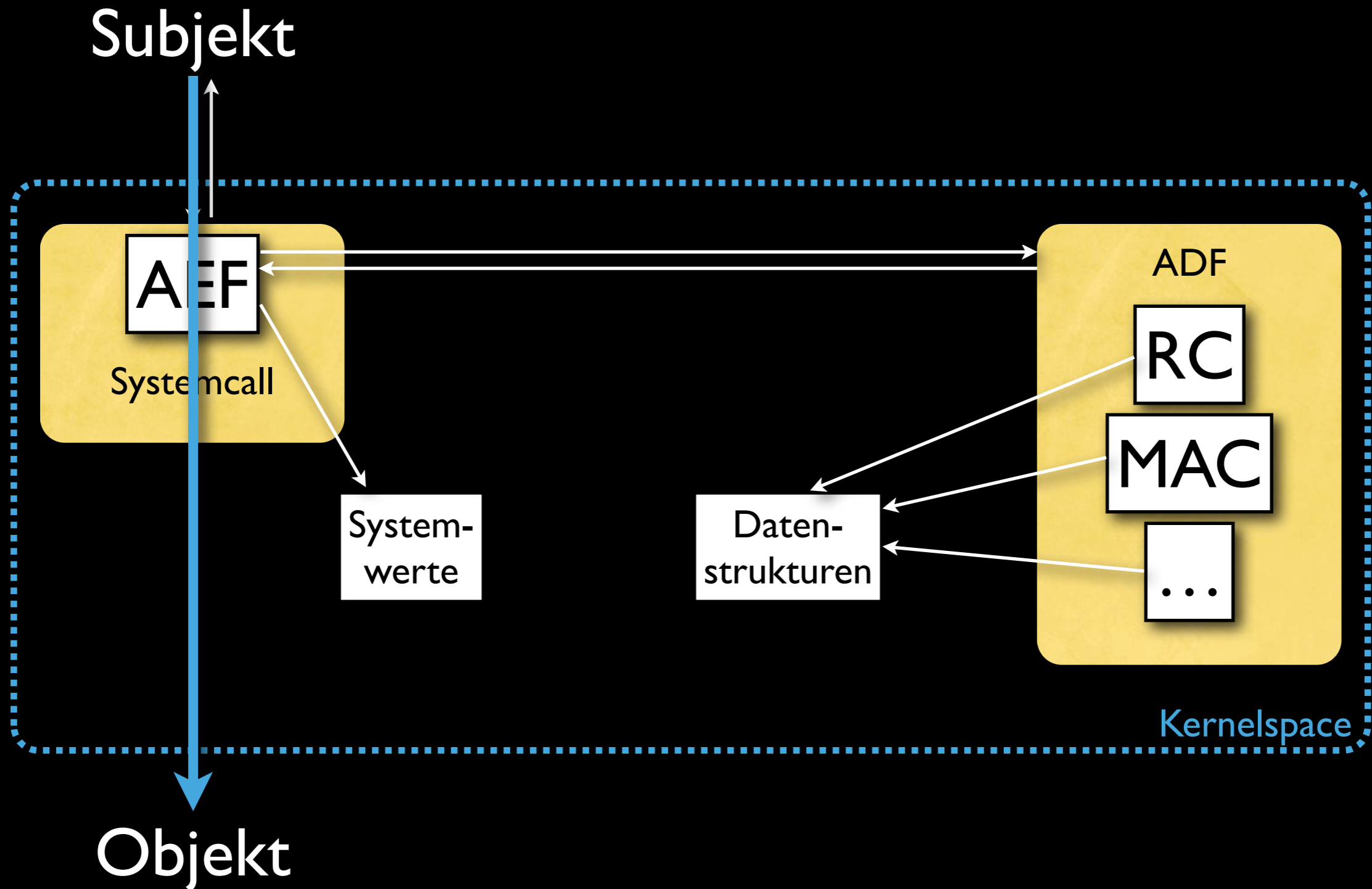


RSBAC (2)





RSBAC (2)





Systrace



Systrace

- ▶ Portierung von BSD Unix



Systrace

- ▶ Portierung von BSD Unix
- ▶ Kernel Patch



Systrace

- ▶ Portierung von BSD Unix
- ▶ Kernel Patch
- ▶ Merkmale:
 - ▶ Fragt Anwender nach Entscheidung (GUI)
 - ▶ Vermeidet time-of-check-to-time-of-use Probleme
 - ▶ Erhöhung der Berechtigung



Links



Links

- ▶ *SELinux und AppArmor*. Ralf Spenneberg. <http://www.os-t.de/HTML-SELinux/buch.html>



Links

- ▶ *SELinux und AppArmor*. Ralf Spenneberg. <http://www.os-t.de/HTML-SELinux/buch.html>
- ▶ *Access Control Comparison Table*. http://gentoo-wiki.com/Access_Control_Comparison_Table



Links

- ▶ *SELinux und AppArmor*. Ralf Spenneberg. <http://www.os-t.de/HTML-SELinux/buch.html>
- ▶ *Access Control Comparison Table*. http://gentoo-wiki.com/Access_Control_Comparison_Table



Links

- ▶ *SELinux und AppArmor*. Ralf Spenneberg. <http://www.os-t.de/HTML-SELinux/buch.html>
- ▶ *Access Control Comparison Table*. http://gentoo-wiki.com/Access_Control_Comparison_Table
- ▶ QEmu: <http://fabrice.bellard.free.fr/qemu/>



Links

- ▶ *SELinux und AppArmor*. Ralf Spenneberg. <http://www.os-t.de/HTML-SELinux/buch.html>
- ▶ *Access Control Comparison Table*. http://gentoo-wiki.com/Access_Control_Comparison_Table
- ▶ QEmu: <http://fabrice.bellard.free.fr/qemu/>



Links

- ▶ *SELinux und AppArmor*. Ralf Spenneberg. <http://www.os-t.de/HTML-SELinux/buch.html>
- ▶ *Access Control Comparison Table*. http://gentoo-wiki.com/Access_Control_Comparison_Table
- ▶ QEmu: <http://fabrice.bellard.free.fr/qemu/>
- ▶ <http://www.kernel.org>



Links

- ▶ *SELinux und AppArmor*. Ralf Spenneberg. <http://www.os-t.de/HTML-SELinux/buch.html>
- ▶ *Access Control Comparison Table*. http://gentoo-wiki.com/Access_Control_Comparison_Table
- ▶ QEmu: <http://fabrice.bellard.free.fr/qemu/>
- ▶ <http://www.kernel.org>
- ▶ <http://kernelnewbies.org>

**Danke für eure
Aufmerksamkeit!**

... und weiter zum 2. Teil...