MNM TEAM
Munich Network Management Team

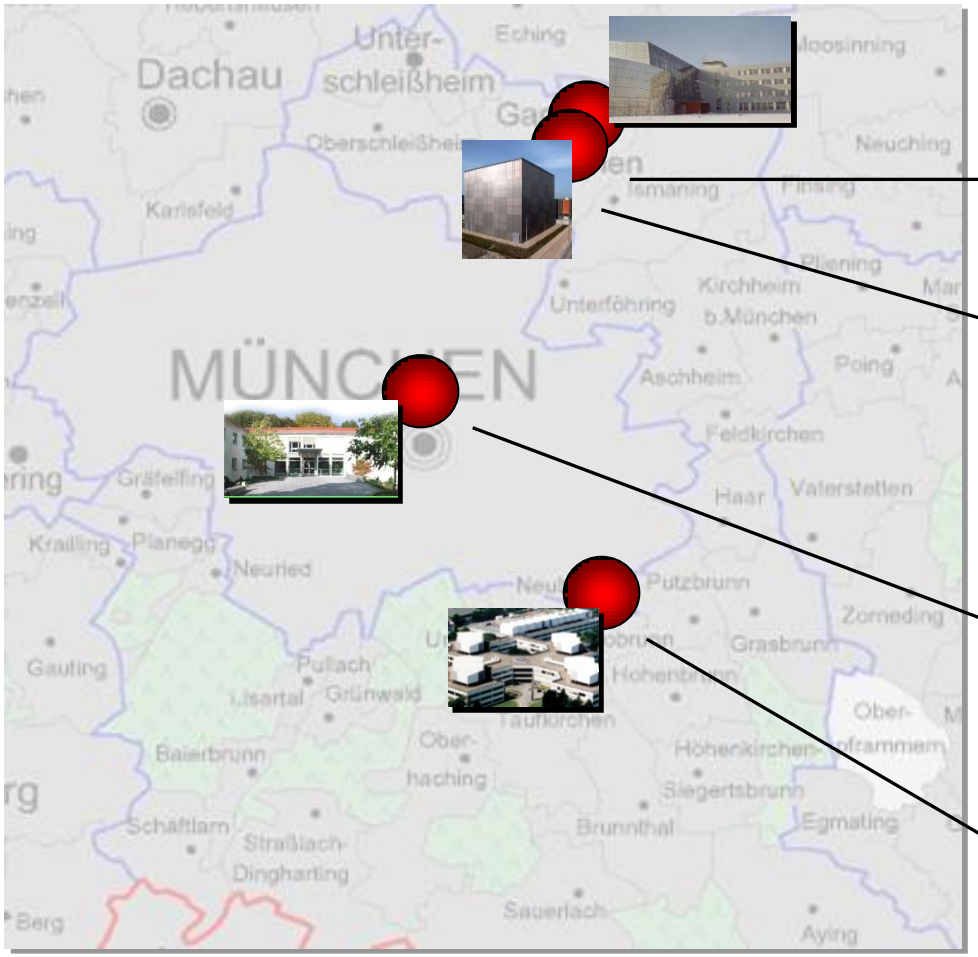
Felix von Eye, Stefan Metzger, Wolfgang Hommel

Innentäter in Hochschulrechenzentren

organisatorische und technische Maßnahmen zur Prävention und Detektion

MNM TEAM
Munich Network Management Team

Munich Network Management Team



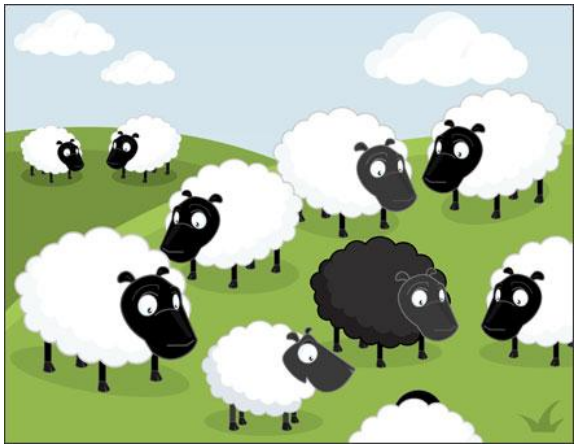
Technische Universität München

Leibniz-Rechenzentrum
der Bayerischen Akademie
der Wissenschaften

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

Universität der Bundeswehr München

Motivation



- **Beispiel: Ehemalige studentische Hilfskraft, die durch PHP-Schwachstelle Accounts erlangte.**
- **Warum Innentäter an Hochschulrechenzentren?**
  - Fluktuation?
  - Gelebte Prozesse?
- **Schutzmaßnahmen gegen Innentäter?**
  - Firewalls, IDS o.ä. helfen nicht!

Organisatorische Maßnahmen

- **Maßnahmenziele nach ISO/IEC 27001**
  - Gewährleistung personeller Sicherheit
  - Festlegung von Verantwortlichkeiten
  - Überwachung
  - Zugangskontrolle
- **Fazit an Hochschulrechenzentren**
  - Aufwand zu hoch
  - Arbeitsatmosphäre leidet

Technische Maßnahmen: Ziele

- **Rechtliche Bedingungen**
  - Beachtung von Datenschutz der Mitarbeiter
  - Wahrung der Persönlichkeitsrechte der Mitarbeiter
- **Ziele**
  - Erkennung von (neuen) ungewöhnlichen Login-Versuchen
    - Ungewöhnliche Uhrzeiten/Tage
    - Ungewöhnliche Herkunft/Ziele
  - Erkennung von Identitätsdiebstahl

Problemstellung

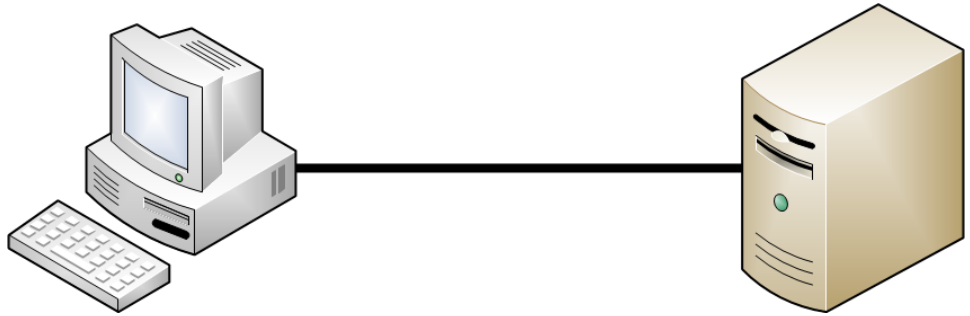
- **Logdaten werden kaum ausgewertet**
  - Zu wenig Zeit
  - Zu wenig Ressourcen
  - Unmotivierende Aufgabe
- **Was ist gewöhnliches Verhalten?**

Features von LoginIDS

- **Automatisierte Logdateiauswertung aktuell von**
  - sshd in /var/log/messages
  - Login-Events in Citrix Terminalserver
- **Langzeitspeicherung mit Beachtung des Datenschutzes**
  - Zuordnung (Quelle, Ziel)
  - Zuordnung (Tag, Stunde)
- **Erlernen des gewöhnlichen Verhaltens**
  - Erkennung ungewöhnlichen Verhaltens
  - Individuelle Lernphase

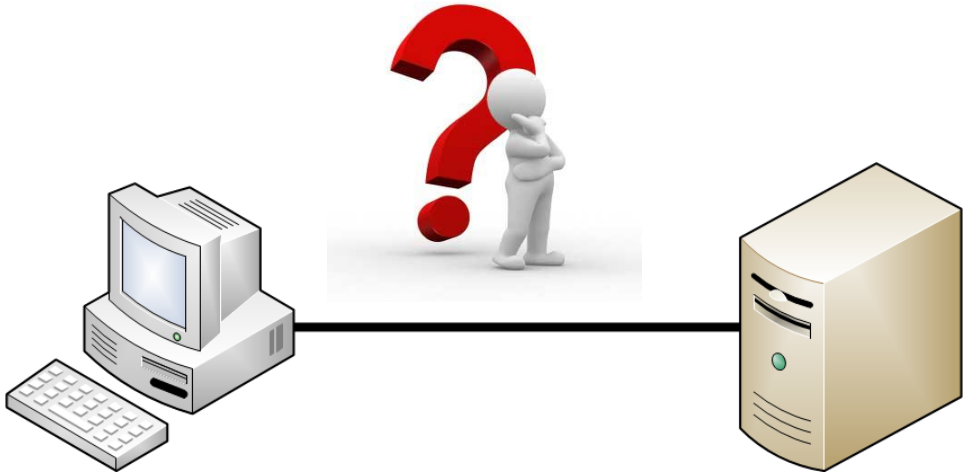
Vorgehen

- **Logdatei wird zeilenweise eingelesen**
- **Events werden geparst**
  - sshd-Login
  - Citrix-Login



NEW USER

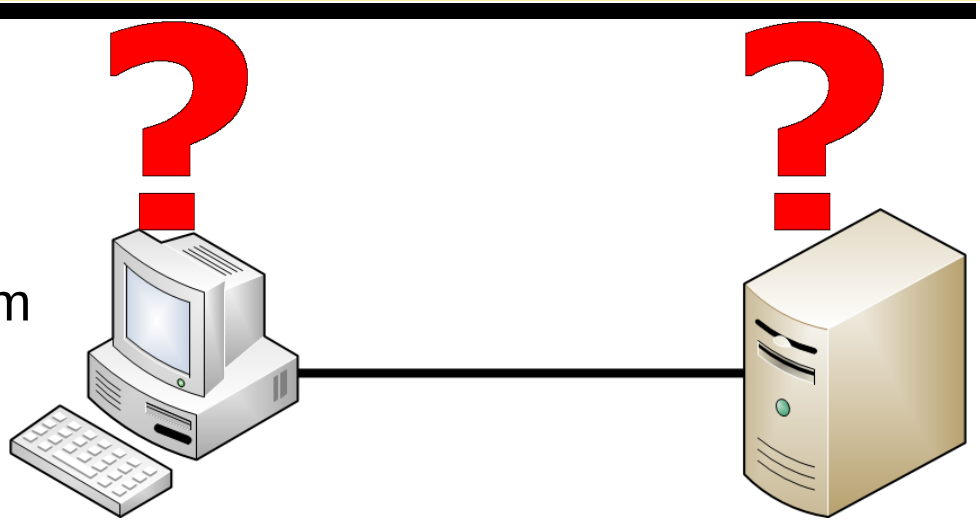
- **Unbekannter Nutzer**
  - Generiert „NEW USER“-Alarm
  - Lernphase für diesen Nutzer beginnt
  - Lernphase dauert in der Standardeinstellung 28 Tage (einstellbar).



- **Mögliche Kompromittierung**
  - Neue (lokale) Kennung

FIRST LOGIN

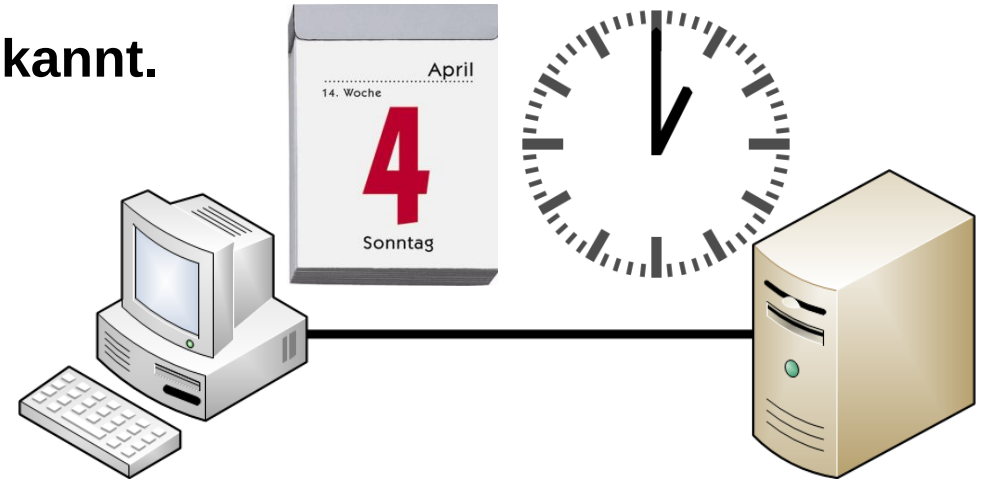
- **Das Tupel (Quelle, Ziel) ist unbekannt.**
  - Generiert „FIRST LOGIN“-Alarm
  - Quelle/Ziel möglicherweise schon bekannt



- **Mögliche Kompromittierung**
  - (Fremde) Kennung von einem anderen System aus
  - Berechtigungen auf einem bisher nicht genutzten System

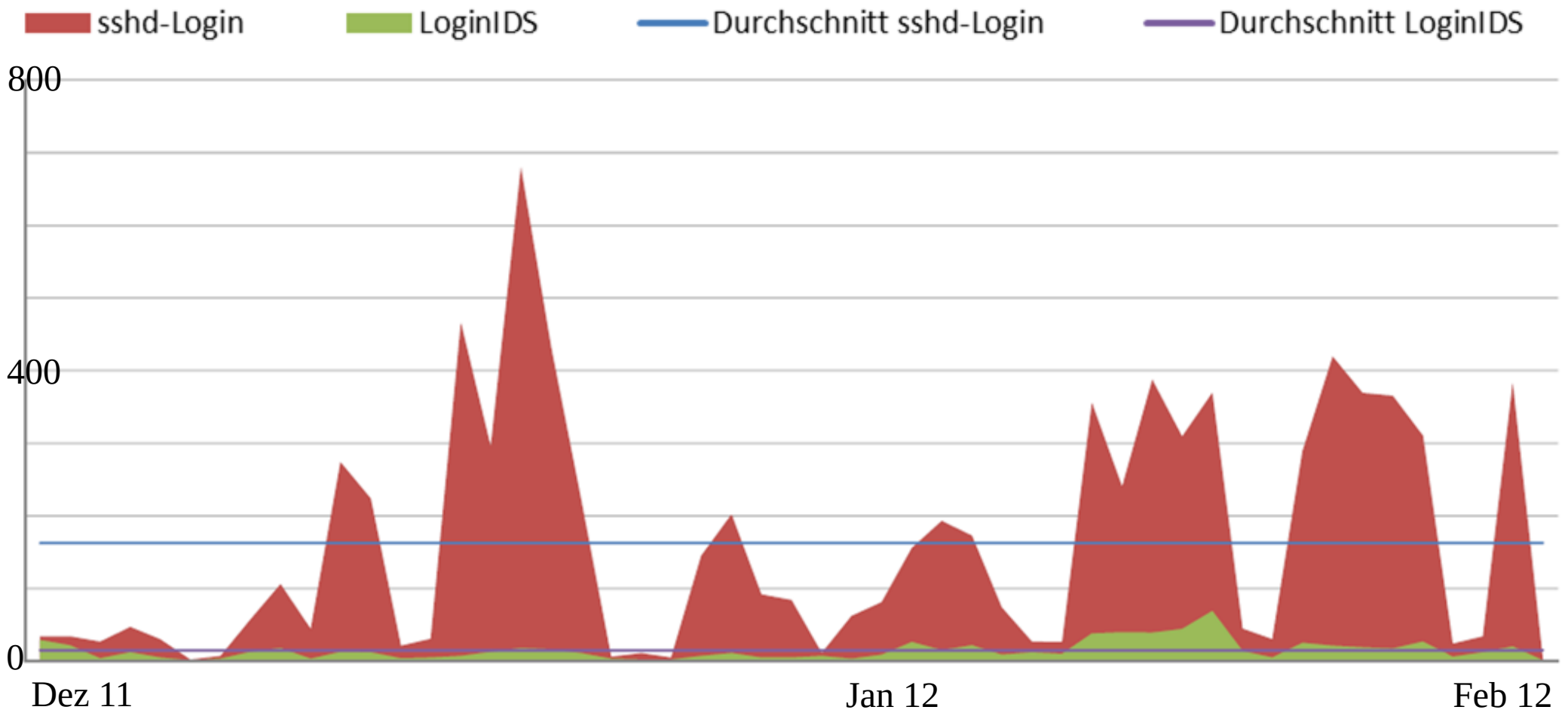
SUSPICIOUS LOGIN

- **Das Tupel (Tag, Stunde) ist unbekannt.**
  - Generiert „SUSPICIOUS LOGIN“-Alarm
  - Tag/Stunde möglicherweise schon bekannt
  - Granularität (z.B. Stundenintervalle) können eingestellt werden.

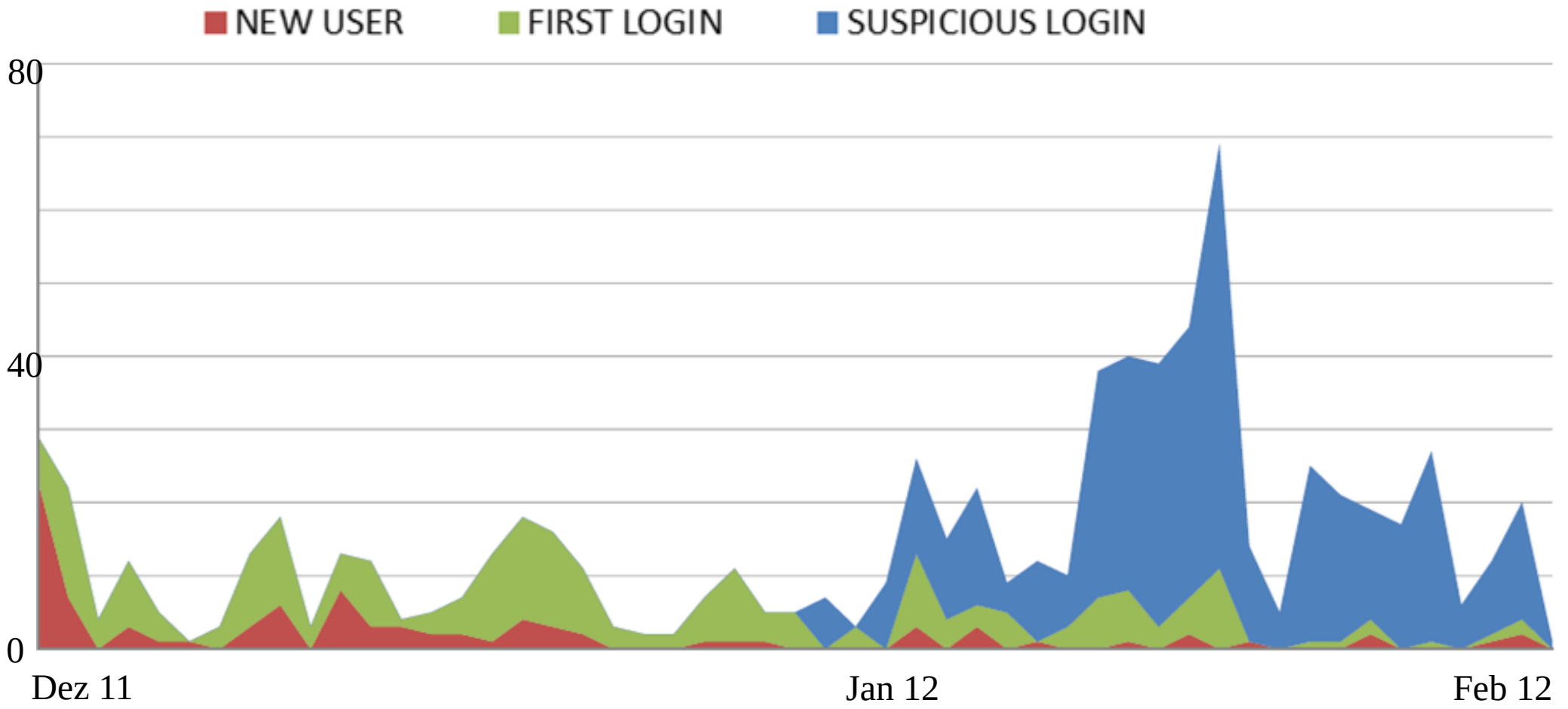


- **Mögliche Kompromittierung**
  - Zugriff soll durch ungewöhnliche Zeit verschleiert werden.

Ergebnisse


sshd-Login
LoginIDS
Durchschnitt sshd-Login
Durchschnitt LoginIDS
800
400
0
Dez 11
Jan 12
Feb 12

Ergebnisse


NEW USER
FIRST LOGIN
SUSPICIOUS LOGIN
80
40
0
Dez 11
Jan 12
Feb 12

Ergebnisse

In Zahlen (Dez/Jan):

- **sshd-Login: 8.310 Events**
- **LoginIDS: 754 Events**
  - NEW USER: 91 Events
  - FIRST LOGIN: 238 Events
  - SUSPICIOUS LOGIN: 425 Events

Nur noch 9% der ursprünglichen Events sind übrig!

Zukünftige Erweiterungen

- **Prototypische Implementierung**
  - Sourcecode unter: http://git.lrz.de/gitweb/?p=LoginIDS.git
  - Juristische Bewertung steht noch aus
- **Weiterentwicklung ist aktuell Bachelorarbeit**
  - Unterstützung für mehr Logdateiformate
  - Anbindung an Security Information and Event Management Systeme
  - Profilbildung eines Nutzers verbessern
  - Herausaltern von Einträgen
- **Konzept für Selfservice?**

Fragen?

Sourcecode unter:

http://git.lrz.de/gitweb/?p=LoginIDS.git

Kontakt:

Felix von Eye
voneye@lrz.de