Mehr schlecht als Recht

Fabian Franzen und Dominik Maier

Warum wir hier stehen

Disclaimer: Wir sind keine Rechtsanwälte!

Die “Antragsgegner”

Team “FAU” aus Erlangen

- 3: FAU Erlangen-Nürnberg
- Dominik: TU Berlin

Team “TUM” aus München

- Fabian + 3: TU München
- 1: TU Eindhoven
  ⇒ Wurde nicht involviert

Trauen keiner Lösung, die absolute Sicherheit bewirbt

Die “Antragstellerin”

- Anbieterin von Sicherheitslösungen
- Versprechen
  - “Gib mir deine Software, danach ist sie sicher”
  - “Auch bei Befall des Systems mit Malware”
- Hohe Verbreitung, vor allem im deutschen Markt

✓ Schützt vor
✓MALWARE ✓MAN-IN-THE-MIDDLE ✓CODE INJECTION ✓SPYWARE

Prequel

FAU: Last Christmas

- Meldung an Antragstellerin, mit der Presse als Mittelsmann
- Veröffentlichung der Details einige Wochen später

2017
2018
2019

Die fabelhafte Welt des Mobilebankings

Fazit

Ist App-Härtung überhaupt sinnvoll?

Ja, als *zusätzlicher* Schutz

Ist App-Härtung ein Ersatz für unabhängige Zwei-Faktor-Authentifizierung?

Nein

FAU: Happy Easter

Paper@DIMVA'18

Honey, I Shrunk Your App Security: The State of Android App Hardening*

Vincent Haupert[1](✉), Dominik Maier[2], Nicolas Schneider[1], Julian Kirsch[3], and Tilo Müller[1]

[1] Friedrich-Alexander University Erlangen-Nürnberg (FAU), Germany
vincent.haupert@cs.fau.de
[2] TU Berlin, Germany
dmaier@sect.tu-berlin.de
[3] TU Munich, Germany
kirschju@sec.in.tum.de

Abstract. The continued popularity of smartphones has led companies from all business sectors to use them for security-sensitive tasks like two-factor authentication. Android, however, suffers from a fragmented

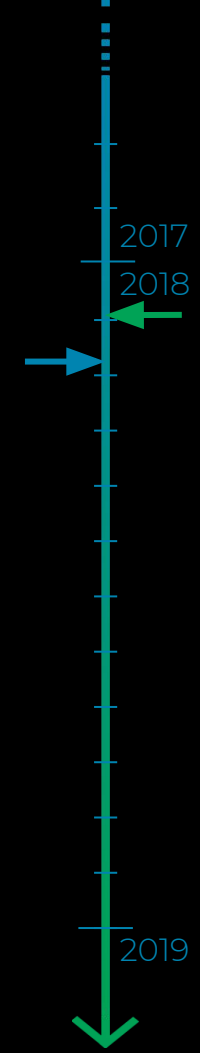
2017
2018
2019

Was gleichzeitig an der TUM geschah...

TUM: Breaking Whitebox Crypto

- Analyse der Elster-App
  - Erster Kontakt zum Team “FAU”
  - Teile fließen in das Paper für die DIMVA ein

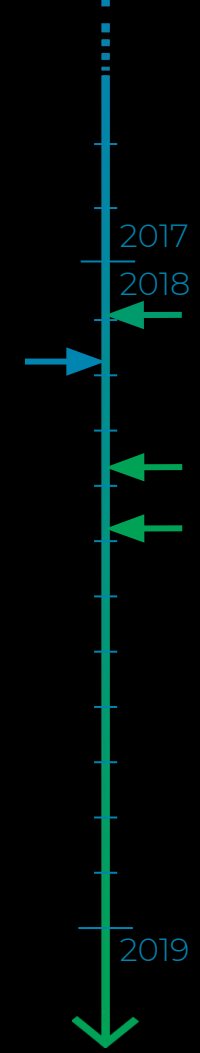
Elster Smart



TUM: Breaking Whitebox Crypto

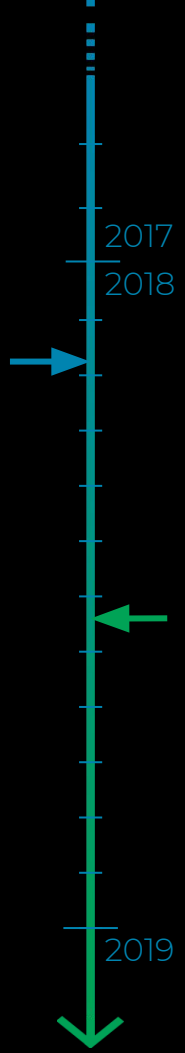
- Analyse der Elster-App
  - Erster Kontakt zum Team “FAU”
  - Teile fließen in das Paper für die DIMVA ein
- Whitebox Crypto ist ein Schutzbaustein
  - Analyseergebnisse zu diesem Aspekt werden als Paper “**Breaking a Real World AES Whitebox**” auf 12ten Usenix Workshop on Offensive Technologies (WOOT’18) eingereicht. (31.05.2018)
  - Conditionally Accepted (27.06.2018)

Elster Smart



TUM: Breaking Whitebox Crypto

- E-Mail von CTO der Antragstellerin an unsere Professoren
  - Betreff: “Responsible Disclosure Violation”
  - Mitteilung unserer Forschungsergebnisse und Vorabzug des Papers
- Diskussion über verschiedene Aspekte des Papers (10.07.-20.07.18)



Überraschung

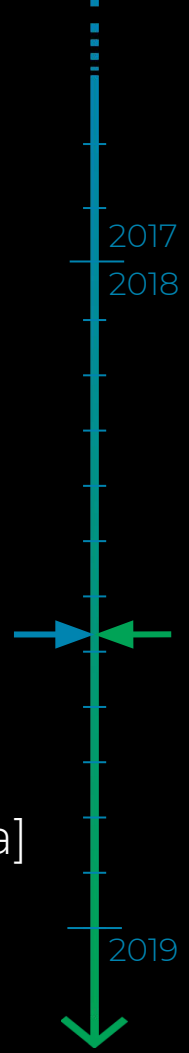
Sign Here Plz

2017
2018
2019

Sign Here Plz

20.07.18: E-Mail von Rechtsanwaltskanzlei mit Forderung der Abgabe einer strafbewehrten Unterlassungserklärung
(Frist: 24.07; nur zwei Werktage!)

- Verstoß gegen
  - §95a, §108b UrhG - Umgehung technisch wirksamer Schutzmaßnahmen [gilt nicht für Computerprogramme §69a]
  - §17 UWG - Zugänglichmachung von Betriebsgeheimnissen zum Zwecke des Wettbewerbs

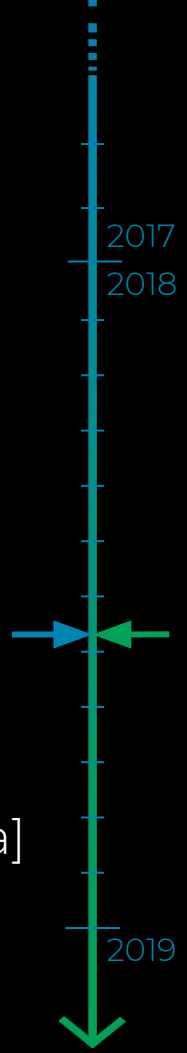


Sign Here Plz

20.07.18: E-Mail von Rechtsanwaltskanzlei mit Forderung der Abgabe einer strafbewehrten Unterlassungserklärung
(Frist: 24.07; nur zwei Werktage!)

- Verstoß gegen
  - §95a, §108b UrhG - Umgeh[illegible] wirksamer Schutzmaßnahm[illegible]t für Computerprogramme §69a]
  - §17 UWG - Zugänglichmachung von Betriebsgeheimnissen zum Zwecke des Wettbewerbs

Urheberrecht

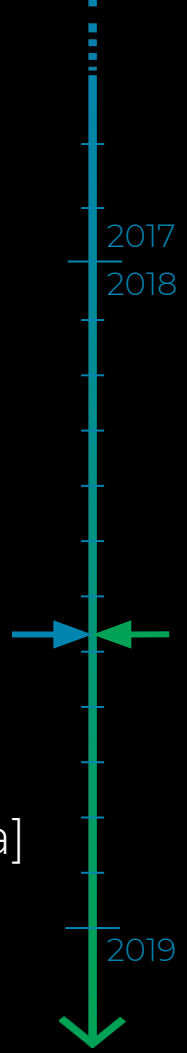


Sign Here Plz

20.07.18: E-Mail von Rechtsanwaltskanzlei mit Forderung der Abgabe einer strafbewehrten Unterlassungserklärung
(Frist: 24.07; nur zwei Werktage!)

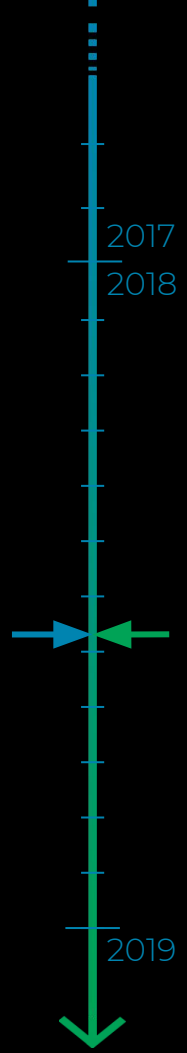
- Verstoß gegen
  - §95a, §108b [illegible] wirksamer Schutzmaßnah[illegible] Computerprogramme §69a]
  - §17 UWG - Zugär[illegible]bsgeheimnissen zum Zwecke des Wettbewerbs

Unlauterer Wettbewerb



Sign Here Plz

- Forderung:
  - a) Kein Reverse-Engineering der Software der Antragstellerin
  - b) Keine Umgehung technischer Schutzmaßnahmen
  - Keine Veröffentlichung/Mitwirkung von Handlungen nach a) und b)
  - Keine Weitergabe/Bewerben/Besitz von Software die a) & b) ermöglicht
  - Zeitlich unbefristet / gilt ein Leben lang
  - Strafe je Verstoß: 10.000 €
- Strafrechtliche Konsequenzen behält sich unser Gegner vor



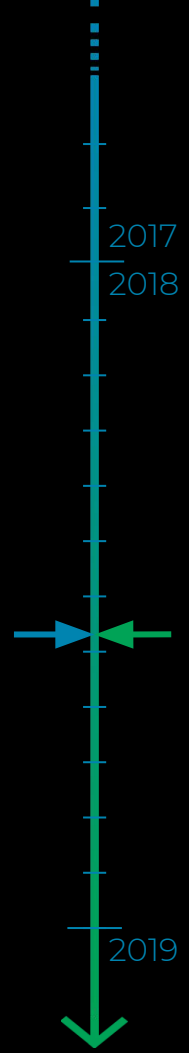
Dominik: Rechtsabteilung

Anruf bei Rechtsabteilung der TU Berlin:

- “Hallo? Ich habe ein Problem:” [Erkärt Situation]
- “Wir kümmern uns komplett um das Thema.”

Dominik klinkt sich aus dem Talk aus.

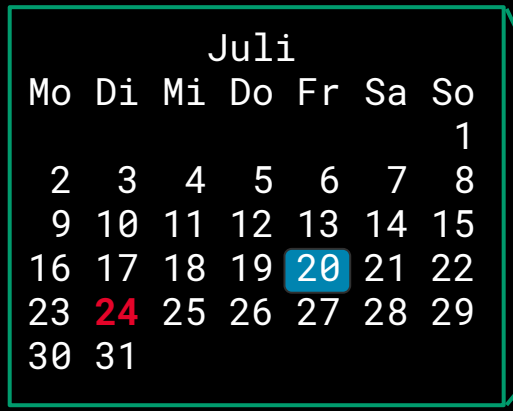
Vielen Dank für die Aufmerksamkeit.



Fabian: Rechtsabteilung TUM

Anruf bei Rechtsabteilung der TUM

- Meine Chefin ruft an… (am Freitag Nachmittag)
- “Der Herr … ist nicht mehr im Haus, ich gebe ihm das gleich am Montag”



Fabian: Rechtsabteilung TUM

- Rechtliche Bewertung schwierig
- 2 Tage Dauertelefonieren
- Rechtsabteilung schlägt Fristverlängerung vor

TUM: Wir beantragen Fristverlängerung...

Sehr geehrter Herr Rechtsanwalt Dr. [redacted],

Ihre Schreiben vom 20. Juli 2018 in o.g. Angelegenheit liegen der Rechtsabteilung der Technischen Universität München (TUM) seit gestern, Montag, den 23. Juli 2018, zur Bearbeitung vor.

Vorab darf ich betonen, dass die TUM ein großes Interesse an einer außergerichtlichen, einvernehmlichen Lösung hat. Aufgrund der Beteiligung mehrerer Betroffener (u.a. des Lehrstuhls für Sicherheit in der Informatik (I20) und des Lehrstuhls für Informatik (I8)) und der hierdurch erforderlichen Abstimmung, benötigen wir zur Klärung des Sachverhalts und zur rechtlichen Beurteilung Ihres Anliegens einen gewissen Zeitraum und bitten daher **um Fristverlängerung bis Dienstag, 31. Juli 2018 (18.00 Uhr).**

2017
2018
2019

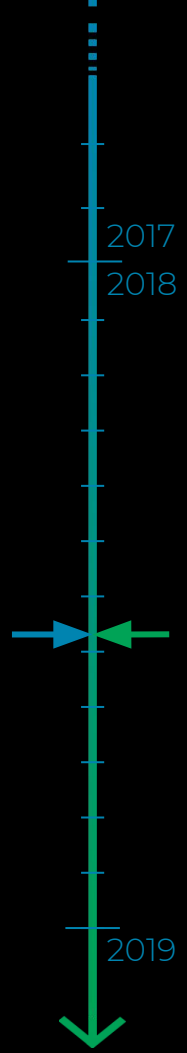
Fabian: Rechtsabteilung TUM

- Ergebnis: **1 Tag** Fristverlängerung!
- Telko am 25.07:
  - Rechtsabteilung: “Wir können das Antwortschreiben nur vorbereiten, aber nicht unterzeichnen”
  - [Stille]
  - Wir unterzeichnen das Schreiben am Ende selbst

Dominik: Rechtsabteilung (2)

Anruf bei Rechtsabteilung der TU Berlin (grob nacherzählt):

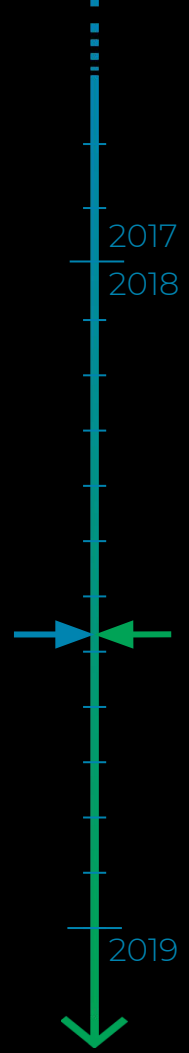
- “Hallo? Ich habe ein Problem:” [Erkärt Situation]
- “Wir kümmern uns…”



Dominik: Rechtsabteilung (2)

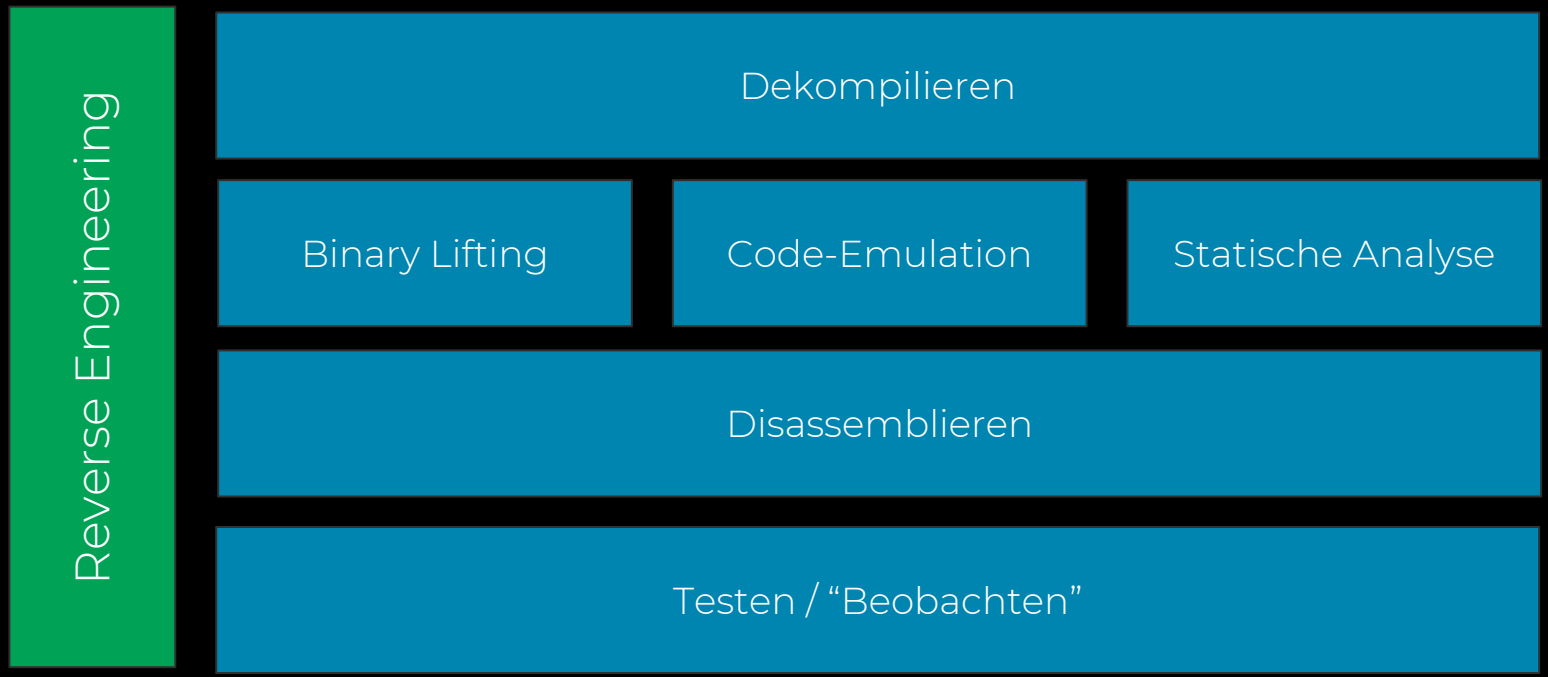
Anruf bei Rechtsabteilung der TU Berlin (grob nacherzählt):

- “Hallo? Ich habe ein Problem:” [Erkärt Situation]
- “~~Wir kümmern uns.~~.”
  “Es steht ihr Name drauf, dann dürfte ich Sie nicht mal vertreten, wenn sie Professor wären”
- [Sprachlos]
- “Sie sollten sich dringend einen Anwalt nehmen”

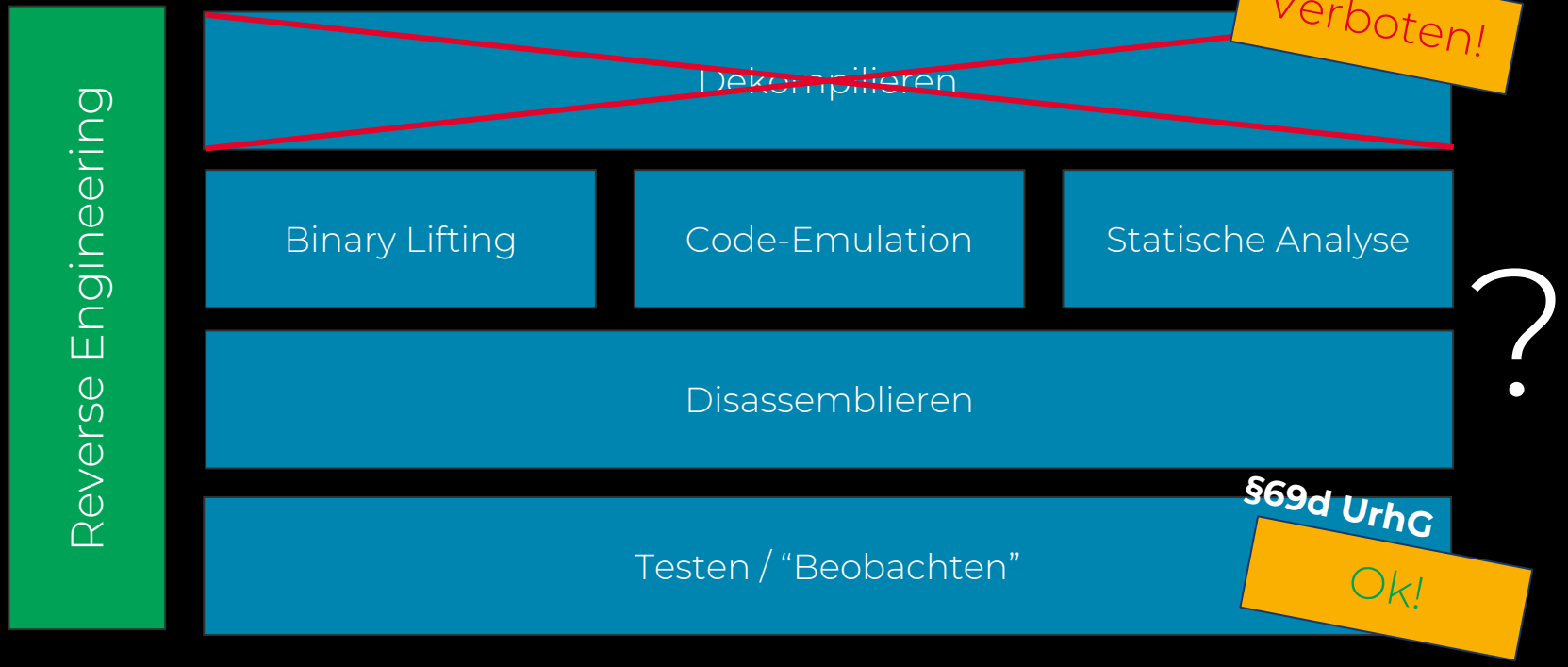


Rechtlicher Hintergrund

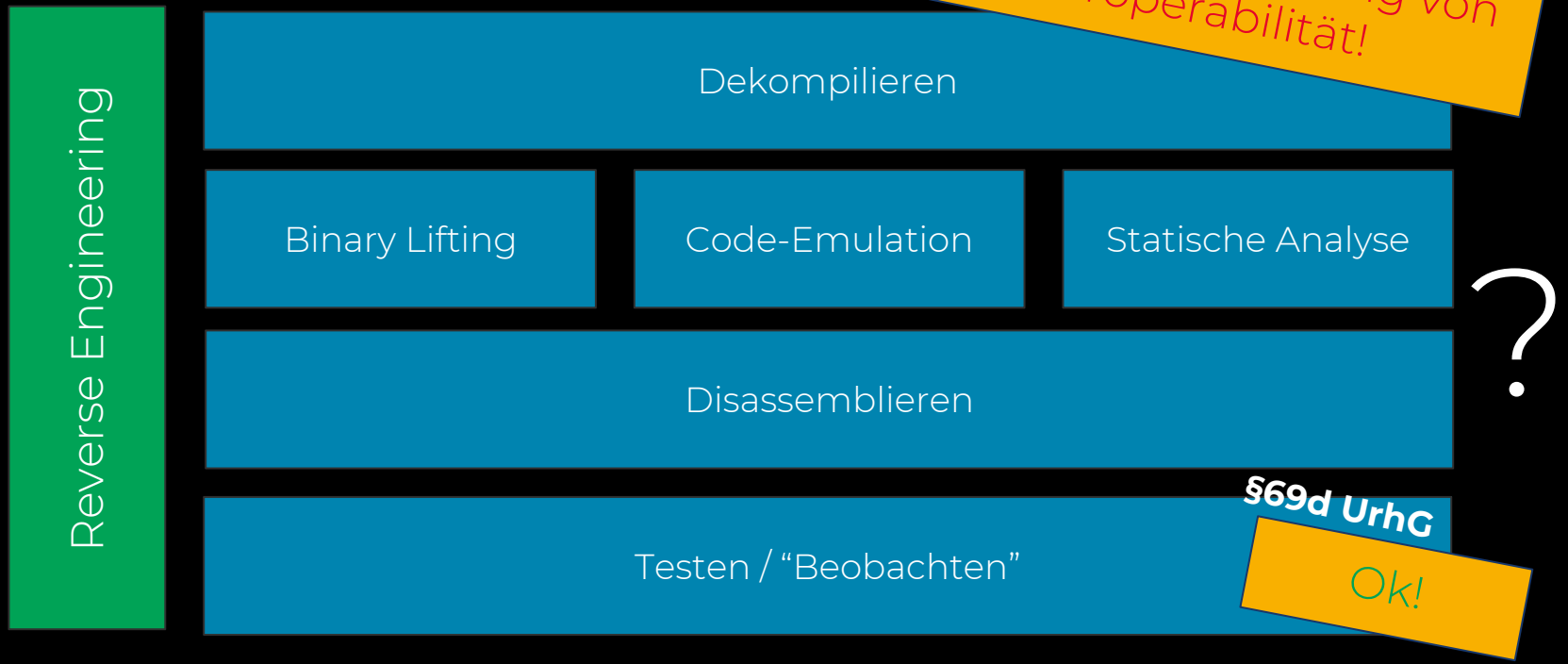
Reverse Engineering



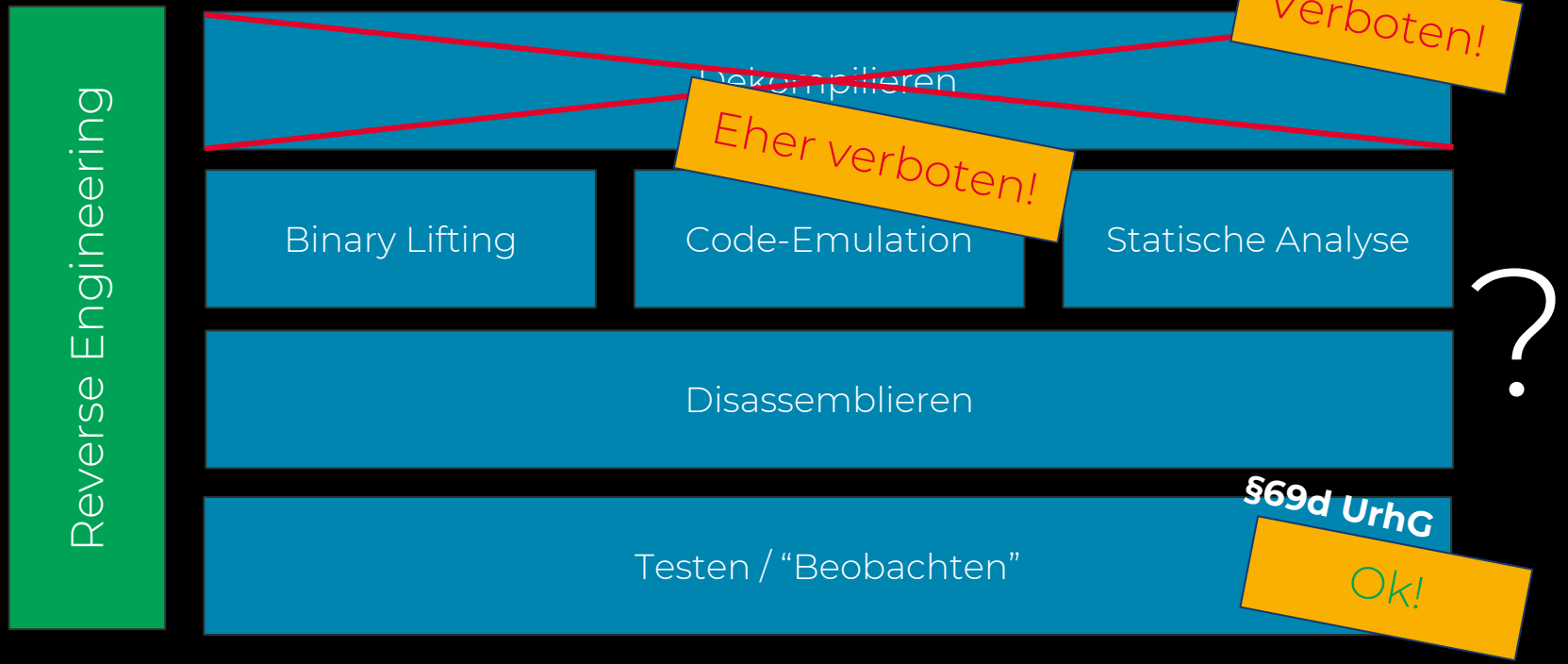
Reverse Engineering



Reverse Engineering



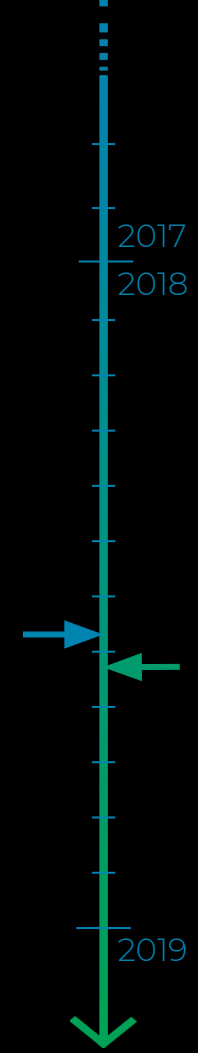
Reverse Engineering



TUM: Rückzug des Papers

Nach 1-2 Wochen intensiver Diskussion mit der Antragstellerin:

Paper zurückgezogen



Jetzt ist hoffentlich Ruhe...

... und einige fahren in den Urlaub

Überraschung (2)

Beschluss

Über den Antrag auf Erlass einer einstweiligen Verfügung gegen die Antragsgegner zu 3 bis 8 ist mündlich zu verhandeln. Es wird klargestellt, dass der Terminsverfügung vom 30.07.2018 in Richtung der Antragsgegner zu 1 und 2 ebenfalls ein - allerdings nur mündlich erlassener - Kammerbeschluss zugrunde liegt.

gez.

Dr. Dettenhofer
Vizepräsident
des Landgerichts

Liepold
Richterin
am Landgericht

Kroier
Richter
am Landgericht

BAYERN LANDGERICHT

Für die Richtigkeit der Abschrift
Nürnberg, 13.08.2018

Diller, JAng
Urkundsbeamtin der Geschäftsstelle

Durch maschinelle Bearbeitung beglaubigt
- ohne Unterschrift gültig

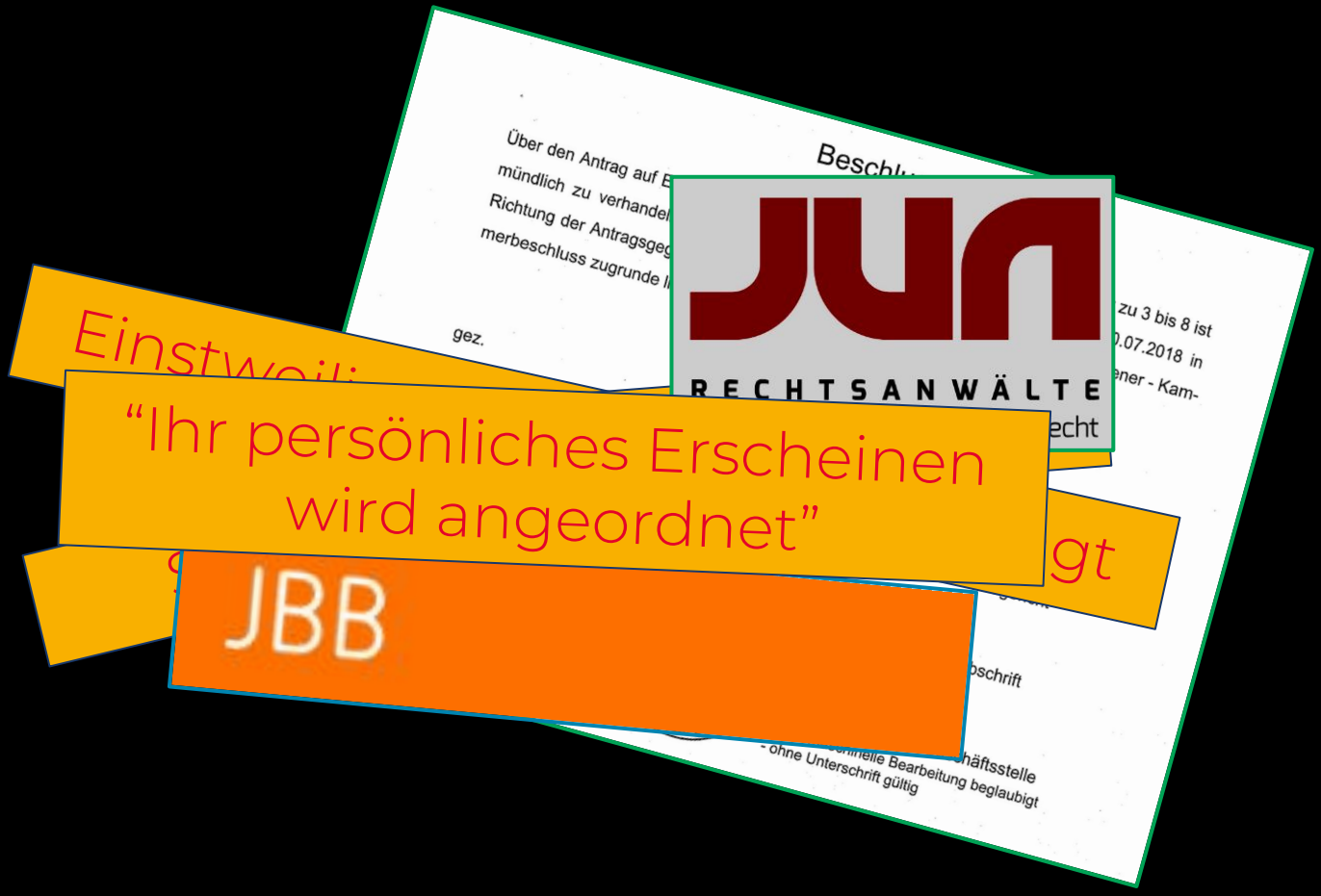
Einstweiliges Verfügung beantragt

2017
2018
2019

2017
2018
2019

2017
2018
2019

2017
2018
2019



2017
2018
2019

2017
2018
2019

Die mündliche Verhandlung

Sonstiges

2017
2018
2019

Ausgang

2017
2018
2019

Disclose Responsibly

7 Stunden später

2017
2018
2019

II. **Disclosure-Verfahren:**

Die Antragsgegner zu 1 - 8 und die Antragstellerin verpflichten sich jeder für sich ohne Anerkennung einer Rechtspflicht, gleichwohl rechtsverbindlich, für den Fall, dass die Antragsgegner IT-sicherheitsrelevante Schwachstellen an den Software-Produkten der Antragstellerin (insbesondere an der Software [redacted]) entdecken, folgendes Verfahren einzuhalten:

1. Die Antragsgegner werden die Antragstellerin vor einer Veröffentlichung ihrer Forschungsergebnisse zunächst von ihren Erkenntnissen unterrichten. Dazu werden die Antragsgegner sämtliche, aus ihrer Sicht zur Reproduzierung dieser Schwachstellen notwendigen Details ihrer Forschungsergebnisse mitteilen. Ferner werden die Antragsgegner einen aus ihrer Sicht angemessenen konkreten Zeitraum mitteilen, vor dessen Ablauf sie ihre Forschungsergebnisse nicht veröffentlichen oder auf andere Weise öffentlich machen werden.

   Die Parteien sind sich einig, dass eine Diskussion der Forschungsarbeit oder Forschungsergebnisse durch die Antragsgegner mit Kollegen noch keine Veröffentlichung darstellt, sofern dies nicht im Rahmen einer Publikation oder eines öffentlichen Vortrages erfolgt.

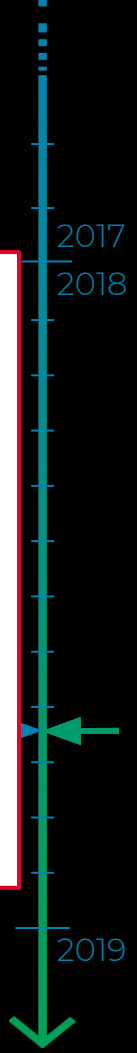
Disclose Responsibly (2)

2. Die Antragstellerin wird dem jeweiligen Antragsgegner nach Eingang der Mitteilung nach Ziffer 1 ihrerseits mitteilen, ob und gegebenenfalls welche weiteren Informationen sie aus ihrer Sicht benötigt; auch auf die Länge der Frist, die der jeweilige Antragsgegner stellt, ist dabei einzugehen.

3. Der jeweilige Antragsgegner wird diese Wünsche der Antragstellerin prüfen und der Antragstellerin entsprechende Mitteilungen machen.

4. Die Parteien sind sich darüber einig, dass die Vereinbarung mit Leben erfüllt werden muss und dass jede Partei bereit sein muss, auf die Interessen der Gegenseite angemessen Rücksicht zu nehmen.

Die Antragstellerin trägt die Kosten des Vergleichs



Nach dem Vergleich

2017
2018
2019

Nach dem Vergleich

2017
2018
2019

Nach dem Vergleich

Quelle: Heise (06.09.2018)

Offenlegung von Softwarelücken: Rechtsstreit endet mit Vergleich

Forscher mit der Urheberrechtskeule an der Veröffentlichung von Softwarelücken zu hindern, widerspreche gesundem Menschenverstand, befand ein Landgericht.

125

Von **Monika Ermert**

2017
2018
2019

Ziel erreicht?

Oder doch nicht?

Also ist doch alles gut?

- 8 Forscher wochenlang von ihrer Arbeit abgehalten
- Hoher psychischer Druck (bis hin zur Existenzangst)
- Rechtliche Unklarheiten unbeantwortet
- Paper der TUM zurückgehalten und bisher nicht veröffentlicht

Lessons Learned

Lessons Learned

- Don’t panic!
- Aber Ernst nehmen!
- Nicht blind Sachen unterschreiben…

Lessons Learned

- (Uni-)Juristen sind keine IT-Experten
  - Bleeding-Edge-Forschung schwer vermittelbar
  - Begriffsbestimmungen in Gesetzestexten sind oft ungenau!

Lessons Learned

- Nicht übertreiben in Publikationen
  - Science: “Es muss besonders cool sein, sonst wird es nicht akzeptiert”
  - Rechtlich: “Wenn Behauptungen nicht gerechtfertigt sind, dann droht im schlimmsten Fall Schadenersatzforderungen”

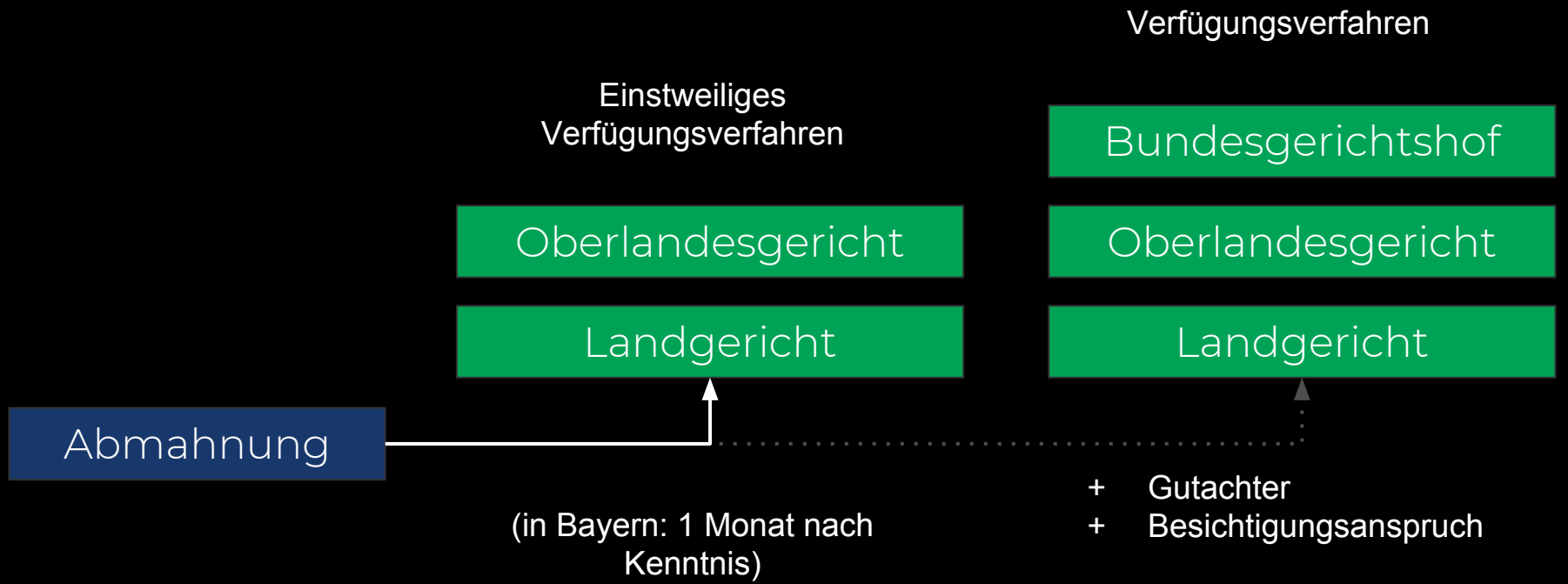
Lessons Learned

- 【NΣVΞR DΞCOMPILΞ】
  - Pragmatisch: Beweislast liegt beim Gegner
  - Problem: Besichtigungsanspruch

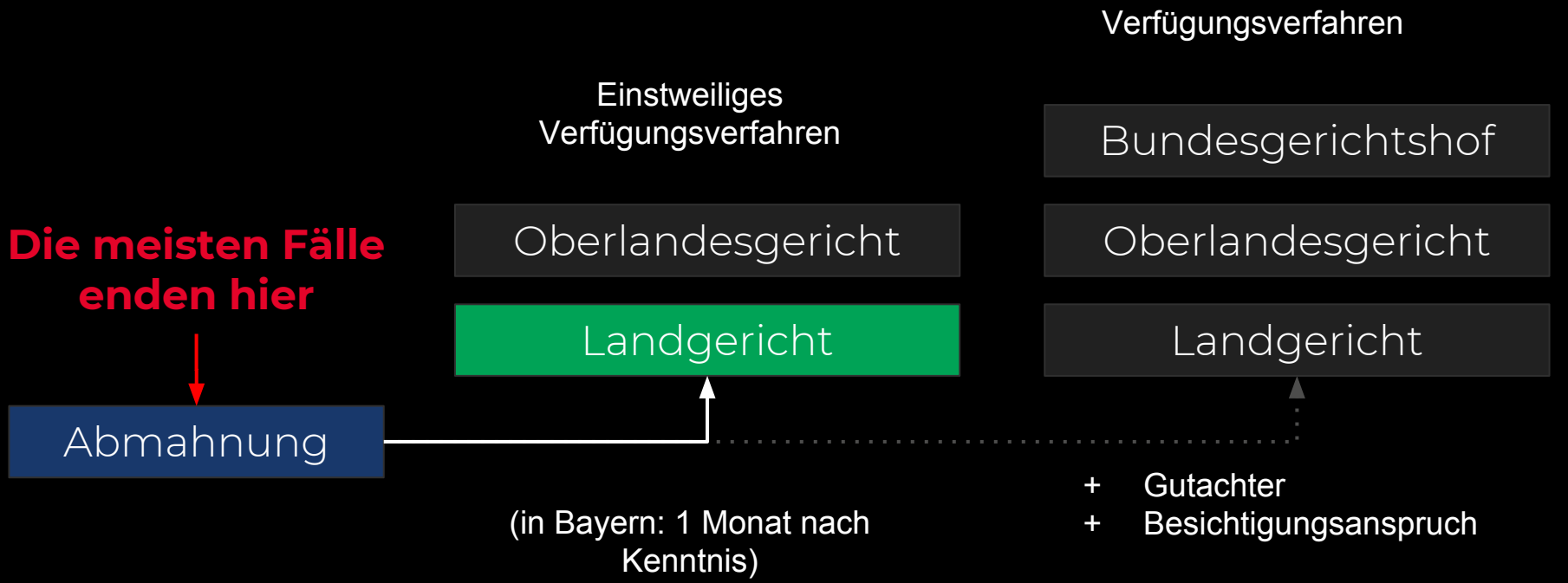
Fragen.

Hätte Gewinnen geholfen?

Instanzen: Einstweilige Verfügung



Instanzen: Einstweilige Verfügung

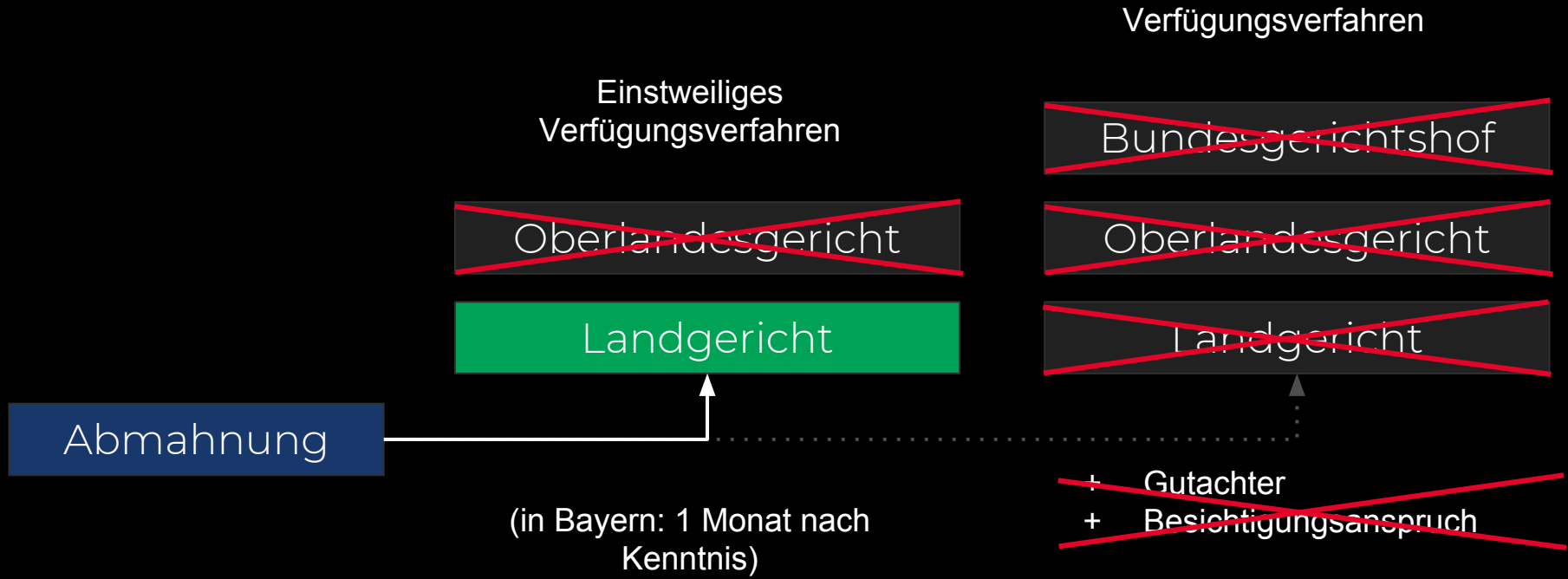


Hätte Gewinnen geholfen?

IV. **Abgeltung:**

Mit diesem Vergleich sind sämtliche Ansprüche der Antragstellerin gegen die Antragsgegner, gleich aus welchem Rechtsgrund, wegen des streitgegenständlichen Sachverhalts abgegolten und erledigt.

Instanzen: Einstweilige Verfügung



Kann man IT-Sicherheitsforscher durch rechtliche Schritte zum Schweigen bringen?

- Unsere Meinung: **Jein** ¯_(ツ)_/¯
- Können Firmen immer Gründe vorschieben, um Forscher mundtot zu machen?
- Unklare Rechtslage -> “man kann immer verklagt werden”
- Dadurch hoher psychischer Druck

Wer vertritt (Uni-)Sicherheitsforscher?

Wie geht man als Forscher mit Nebentätigkeiten um?

Forderungen

- “Hackerversicherung”?
- Unterstützung durch Forschungsinstitute
  - Klare Bekennung zu (externen) Forschern, Studenten, …
  - Rechtsschutz und Mithaftung
- Rechtliche Basis für Sicherheitsforschung
  - Ideal: Alle Analysen (einschließlich Dekompilieren erlaubt)
  - Bsp: Ausnahmeregelung im Digital Millennium Copyright Act (DMCA) für Sicherheitsforschung seit 2016

Fragen?

【NΣVΞR DΞCOMPILΞ】

Vielen Dank für die Aufmerksamkeit.