Log4Shell
Retrospektive aus verschiedenen Blickwinkeln

Matthias Altmann
secf00tprint.github.io/blog/
Mitorganisator IT-Security Meetup Kassel
// Webmontag 39 04.04.2022

Geschichte

One of the most serious I've seen in my entire career, if not the most serious (Jen Easterly Director CISA US)

The single biggest, most critical vulnerability ever (Tenable)

BSI Warnstufe Rot

Betroffen

100te Millionen Geräte

Überall wo Java im Spiel ist

93% aller Unternehmens-Cloud Umgebungen

Black Hat 2016 USA

Twitter 9.12.2021

Übersetzung

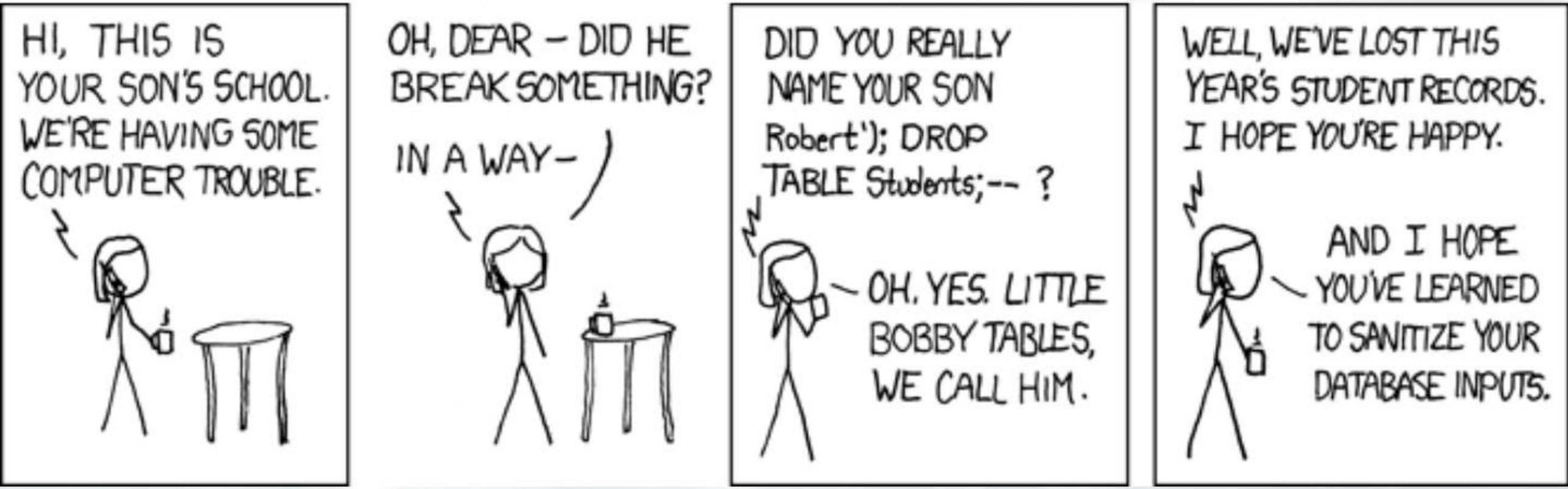
Chen Zhaojun

LunaSec

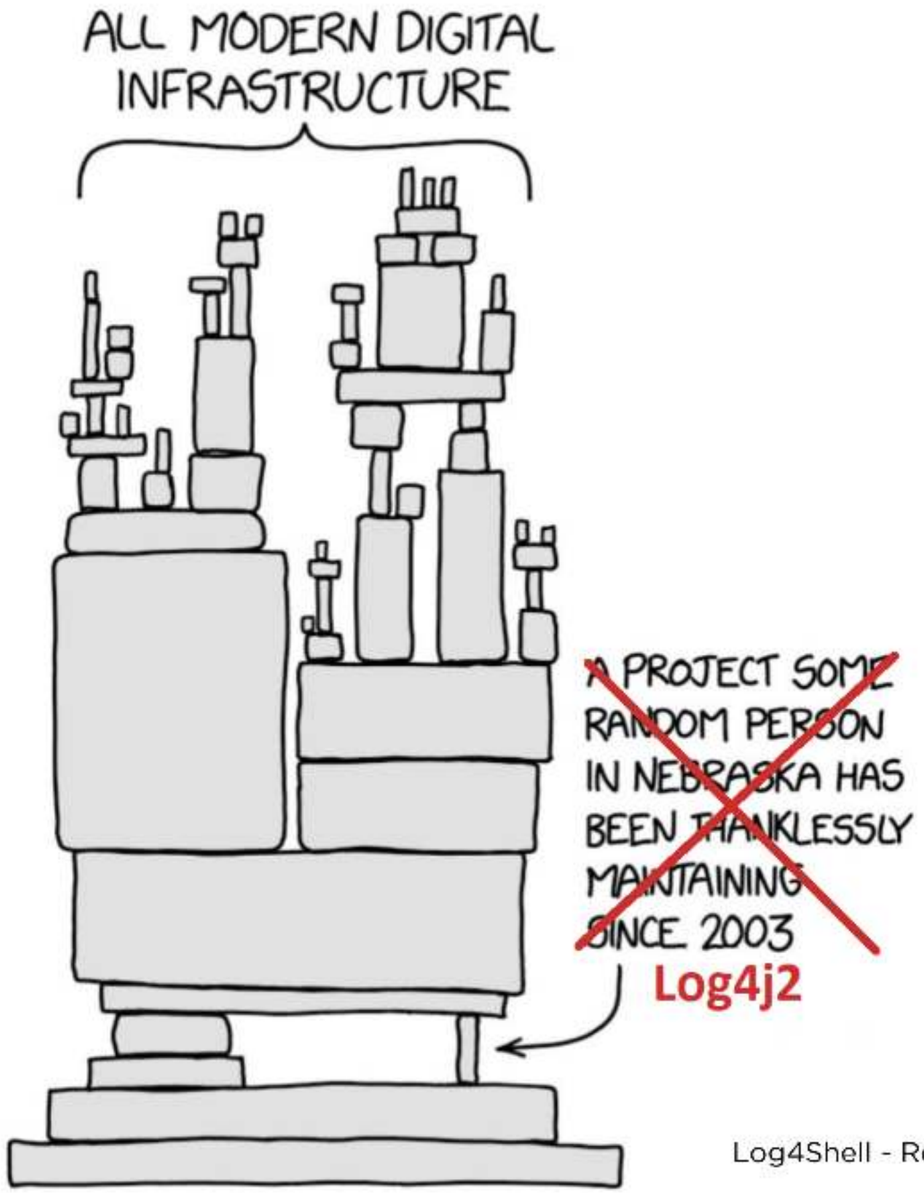
Technische Sicht

Overview

https://github.com/mbechler/marshalsec


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

Canaries als Hilfe


ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003
Log4j2

Listen zur Analyse

Log4j Seite

Red

CTF

Ergänzungen

Blue

CTF

Ergänzungen

Patchen vor anderen Lösungen

Scannen vor Listen

Scanner

Libraries - Google
URL - Fullhunt
Forensische Analyse
Vaccination