

# Enterprise IT

## Ein agiler Realitätsabgleich

Martin Leyrer

@leyrer@chaos.social

Christoph Stoettner

@stoeps@infosec.exchange

# Martin Leyrer (leyrer)



✉ [martin@leyrer.priv.at](mailto:martin@leyrer.priv.at)

📡 [martin.leyrer.priv.at](http://martin.leyrer.priv.at)

📧 [@leyrer@chaos.social](https://chaos.social/@leyrer)

- macht seit 40 Jahren was mit Computern
  - CP/M, Sinclair ZX Spectrum, C64
  - Amiga, OS/2, Lotus Notes
- verdient seit 30 Jahren Geld damit
- Palliative Systemadministration
- Linux seit ~ 1993
  - Linux Kernel < 1.0
  - 1995 thread support manuell in den Kernel gepatcht
- Windows nur gegen Schmerzensgeld
- vi, ich hab schon ein Betriebssystem
- Sucht immer noch einen NeXTcube

# Christoph Stoettner (stoeps)



✉ [christoph.stoettner@stoeps.de](mailto:christoph.stoettner@stoeps.de)

in [linkedin.com/in/christophstoettner](https://linkedin.com/in/christophstoettner)

📡 [stoeps.de](https://stoeps.de)

✉ [@stoeps@infosec.exchange](mailto:@stoeps@infosec.exchange)

- Macht seit 30 Jahren was mit Computern
  - Amiga, OS/2, Linux
  - Beruflich auch Windows (wenn es sein muss)
- Started with Linux / OSS around 1994/1995
  - Linux Kernel < 1.0
  - Slackware
- mag vi, vim, neovim
  - zu doof für emacs

# Jeder ist agil

- Ein paar Management Layer und Micromanagement
- Im Zweifelsfall ist die Verwendung von Jira agil genug
- "Ihr seid jetzt Ende zu Ende verantwortlich"
- Oder man benennt schon einmal die Teams in Tribes um
- "Standup" statt "Joure Fix", Scrum-Master statt Projektmanager



# Agile Manifesto

**Individuals and interactions** over processes and tools

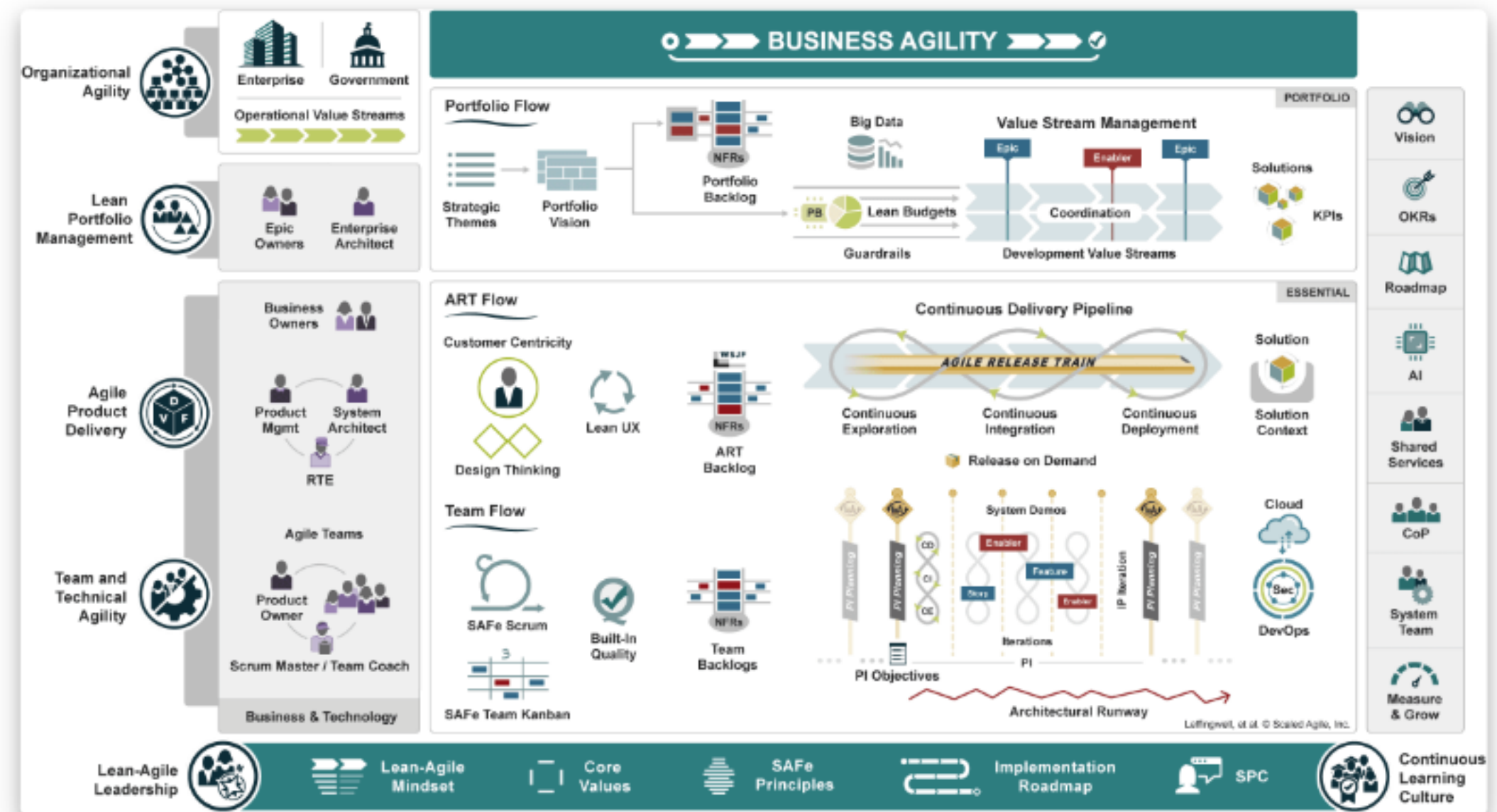
**Working software** over comprehensive documentation

**Customer collaboration** over contract negotiation

**Responding to change** over following a plan

# Enterprise Agile frameworks

- Kanban Maturity Model with Portfolio Kanban
- SAFe (Scaled Agile Framework)
- LeSS (Large Scale Scrum)
- Scrum@Scale (SaS)



# Agility

Sportart für Hunde, bei der ein Hund einen Parcours mit Hindernissen zu bewältigen hat, wobei der Besitzer nebenher mitläuft.



# Job Anzeigen und ihre Auswüchse

- IBM forderte 2022 12 Jahre Kubernetes Knowhow
  - Kubernetes wurde 2024 10 Jahre alt
- FastAPI Developer

 **The Cyber Security Hub™**  
1,155,230 followers

Required Technical and Professional Expertise

- **Minimum 12+ years' experience in Kubernetes administration and management**
- Hands-on experience on setting up Kubernetes platform, deploying microservices and other web applications, and managing secure secrets along with container orchestration using Kubernetes

 **Sebastián Ramírez**  
@tiangolo

I saw a job post the other day. 📌

It required 4+ years of experience in FastAPI. 🙄

I couldn't apply as I only have 1.5+ years of experience since I created that thing. 😂

Maybe it's time to re-evaluate that "years of experience = skill level". ♻️

1:40 PM · Jul 11, 2020



# AT: Diplomlehrgang Human Resource Management

- Zielgruppe
  - Personen ohne einschlägige HR-Qualifikation, die im HR-Bereich tätig sein wollen
  - Führungskräfte, die für Personalaufgaben verantwortlich sind bzw. diese in Zukunft übernehmen werden
  - MitarbeiterInnen aus der Personalverrechnung, die ihren Tätigkeitsbereich verbreitern möchten



# Job Benefits

- Obstkorb
- Kostenloses Wasser
- Freier Kaffee
- Dachterasse
- Tischkicker

# Der wöchentliche Obstkorb

- Ich bin nur selten in Büros
- Der Obstkorb sieht vieler Orts sehr zerplückt oder geplündert aus
  - Man sichert die besten Stücke im Schreibtisch

# Flache Hierarchien

- Der neue Obstkorb
- Die Suche nach jemand der Entscheidungen trifft wird schwieriger
- Trend geht m.M.n. zum 2. Manager
  - technisch/fachlicher Vorgesetzter
  - disziplinarische Vorgesetzte

# Die Extrameile gehen

- Anzeige:
  - hohe Belastbarkeit
  - hohe Einsatzbereitschaft
  - großes Engagement
- Bedeutung:
  - Neigung zur Selbstaussbeutung?



# Kicker





# Selbstverständlich (werden aber oft als Benefit aufgezählt)

- Ein positives Arbeitsklima
- Spannende und abwechslungsreiche Aufgaben
- Faires Gehalt
- Duz Kultur

# Es geht schlimmer

- mgm Job Anzeige für Redhat Administrator zum Neuaufbau des Netzwerks
- ca 100 Mio US \$ geringeres operatives Ergebnis Sept. 2023
- 10 Mio US \$ für IT Berater und Anwälte
- 25 Tage à 10 Std \* 100\$ = 25.000\$
  - IRS 1099 Stundensatz
  - Die Summe muss noch versteuert werden

Las Vegas, NV 89118

\$110 an hour

## Job details

Here's how the job details align with your job preferences.  
Manage job preferences anytime in your [profile](#).

### Pay

\$110 an hour

### Shift and Schedule

10 hour shift On call

Arganteal seeks an onsite Red Hat Linux System Admin "RHEL SysAdmin" in Las Vegas, Nevada for immediate work starting 9-21-2023. This role will be helping the MGM Grand Casino to build its net new IT environment after the recent ransomware hack.

**Candidates must be willing to work everyday until the new IT environment is fully stood up.**

**We are open to people who will only work a grand total of 7 days!**

**Higher Pay for those willing to stick it out until the job is done!**

**Expected Dates of Service** 9-21-2023 through 10-15-2023

**Hourly Rate:** \$100.00 per on 1099

**Location:** Onsite at MGM HQ in Las Vegas (absolutely no remote work)

**Visa Status:** Must be US Citizen (no Green Cards or H1b visa candidates will be accepted)

**Working Hours:** Expect to work 10 hours per day 7 days a week

# Reverse Job (600\$ / Woche)

## Data Analyst

- New York, NY

\$15 an hour

**Apply Now**

You will complete various applied research projects for data analysis. Strong critical thinking skills and some programming experience is a plus. Knowledge of machine learning techniques is a bonus!

Note, this is a reverse financed internship so you will pay \$15/hr to work here.

Job Type: Full-time

- Just posted - [save job](#) - [report job](#)

If you require alternative methods of application or screening, you must approach the employer directly to request this as Indeed is not responsible for the employer's application process.



**Personalführung ist die Kunst, den Mitarbeiter so schnell über den Tisch zu ziehen, daß er die Reibungshitze als Nestwärme empfindet.**

# Zurück ins Büro

- Video Konferenzen aus dem Büro statt Homeoffice
- Einige CEOs hoffen auf freiwillige Kündigungen (<https://www.techradar.com/pro/many-ceos-secretly-hoping-forcing-employees-back-to-the-office-will-make-them-quit>)



# Ordered back to the office, top tech talent left instead

Study by scholars from the University of Chicago and the University of Michigan:

- The RTO mandates at Apple, Microsoft, and SpaceX have led to a higher rate of employee turnover, particularly for senior-level personnel.
- Following Apple's RTO mandate, there was a 5% decline in the proportion of senior-level employees; a similar trend was evident at Microsoft.
- SpaceX's imposition of full-time RTO led to a 15% decrease in senior-level employees.
- The departure of senior-level workers may be related to the negative impact of RTO mandates on employee moral

<https://harris.uchicago.edu/sites/default/files/wright-return-to-office.pdf>

# Kosten des Personalverlusts

- High employee turnover can lower morale and make employees feel disconnected.
- A high rate of turnover can also impact productivity since your remaining employees may become overwhelmed with additional work.
- The financial impact of recruiting and training new employees to replace those who have left can be significant, with turnover costing thousands of dollars per employee.

# Ist HR wirklich so dumm?

3 out of 4 HR representatives say retaining those who don't want to return to work in the office is a problem, while 1 in 5 calls it a major problem.

When asked, "How big of a problem is it for your company to lose employees who want to stay remote but whom the company is not willing to let work remotely? 73% said it was a major or minor problem.

# Massenentlassungen im IT Bereich



Joe Fabisevich ✓

@mergesort@macaw.social

The layoffs will continue until shareholder value improves.

Dec 04, 2023, 18:01 · 🌐 · Ivory for Mac · ↻ 18 · ★ 37



# Shareholder Value

Das Shareholder Value-Konzept ist eine Unternehmensstrategie, bei der in einer börsennotierten Gesellschaft Maßnahmen im Vordergrund stehen, die dazu dienen, den Anteilseignernutzen zu erhöhen oder, konkreter, [...] das Aktionärsvermögen zu steigern.

Der Unternehmenswert ergibt sich dabei nicht aus dem Gewinn, sondern aus den künftigen Zahlungsströmen des Unternehmens.

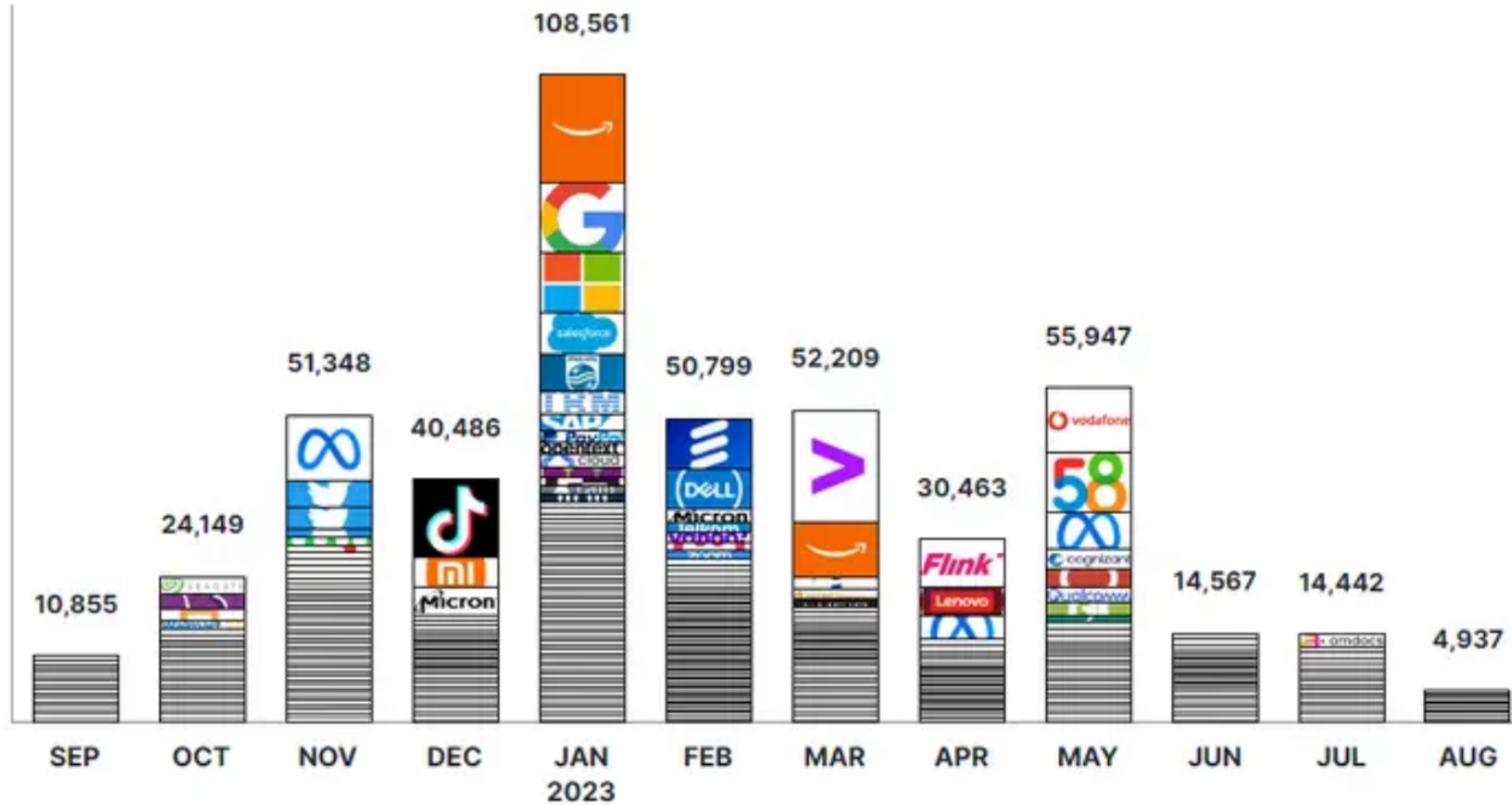
Quelle: <https://www.boerse-frankfurt.de/wissen/lexikon/shareholder-value>



# Massenentlassungen im IT Bereich

## # of Tech Employees Let Go

as of August 11, 2023



source: [trueup.io/layoffs](https://trueup.io/layoffs)

# Droht in Österreich eine große Kündigungswelle?

Tech-Riesen wie Amazon, Google und Microsoft setzten im Verlauf des Vorjahres zehntausende Angestellte vor die Türe.

Den Konzernen schadete das keineswegs. Im Gegenteil: Kletternde Aktienkurse und zufriedene Investoren waren die Folge der Massenentlassungen und anderer Sparmaßnahmen.

Quelle: <https://www.derstandard.at/story/3000000206187/droht-in-oesterreich-eine-grosse-kuendungswelle>

# Auswirkungen 1/4

Für besonders viel Erregung sorgten die Entlassungen bei X, vormals Twitter, wo nach der Übernahme durch den exzentrischen Milliardär Elon Musk seit Ende 2022 gar 80 Prozent der Belegschaft, teilweise ersatzlos, den Hut nehmen mussten – und dennoch funktioniert die Firma, entgegen vielen Befürchtungen, weiter.

Quelle: <https://www.derstandard.at/story/3000000206187/droht-in-oesterreich-eine-grosse-kuendigungswelle>



# Auswirkungen 2/4



SUBSCRIBE



SIGN IN

*SKELETON STAFF —*

## After Musk's mass layoffs, one engineer's mistake "broke the Twitter API"

Twitter's paid-API project had "only one site reliability engineer," report says.

JON BRODKIN - MAR 7, 2023 6:03 PM UTC

# Auswirkungen 3/4

## Did a DDoS Attack Hit the Musk-Trump Interview?

Emiliano De Cristofaro, professor of computer science and engineering at the [University of California, Riverside](#), told *Newsweek* that he highly doubted a DDoS was responsible.

"There is no evidence of any malicious activity happening but more importantly no other functionality was affected," he said.

"It is much more likely that the platform just couldn't handle a sudden big spike in the number of users trying to stream," the professor added.



# Auswirkungen 4/4



**Alp Toker** ✓  
@atoker

Follow



Any sufficiently overloaded server is indistinguishable from a DDoS



**NetBlocks** ✓ @netblocks · Aug 13

⚠ Note: X Spaces are currently experiencing international outages; the incident is understood to be due to server issues as the platform hosts a live interview between Elon Musk and US presidential candidate Donald Trump  
#TwitterDown



# Shareholder Value Über Alles



## Embracer confirms layoffs of nearly 1400 people were part of efforts to 'always maximize shareholder value'

By **Chris Neal** - February 16, 2024 10:30 AM 28



# Cory Doctorow

These layoffs have nothing to do with "trimming the fat" or correcting the hiring excesses of the lockdown. They're a project to transfer value from workers, customers and users to shareholders. Google's layoff of 12,000 workers followed fast on the heels of gargantuan stock buyback where the company pissed away enough money to pay those 12,000 salaries...for the next 27 years.

Quelle: <https://pluralistic.net/2023/03/21/tech-workers/#sharpen-your-blades-boys>



# Don't Panic !!!

Fachkräftemangel spitzt sich bis 2027 zu

Besonders hoch – und ungedeckt – entwickle sich die Nachfrage nach Experten (Master/Diplom) der Informatik. In der vorjährigen Fortschreibung gingen die Forscher noch von 15.052 fehlenden Fachkräften in 2026 aus. Nach dem aktuellen Report seien dies 2027 bereits 19.022.

Quelle: <https://www.heise.de/news/Studie-Fachkraeftemangel-spitzt-sich-bis-2027-zu-9830539.html>



# Kommunikation

# Antipattern

- Es werden blind Jira Tasks erstellt und zugewiesen
- Security Scan Ergebnisse (Qualys, Dive, etc.) als XLS/XLSX im Sharepoint
- Mailflut könnte weniger werden, aber Jira & Co senden x Mails pro Tag

# Security Scan Ergebnisse

- Keine CVE, ... Referenzen
- "Hingerotzt" bzw. lieblos mit Tools erstellt
- False Positives (SQL Injection bei NoSQL Datenbanken, ...)



# Prozesse die Excel beinhalten ...

	A	B	C	D		F	G	H	I
1	Plugin ID	CVE	CVSS	Risk	Host	Protoc	Port	Name	Synopsis
1601	90511			None	10.1.1.22	tcp	0	MS KB3152550: Update to Improve Wireless Mouse Input Filtering	The remote Windows host is missing an upd
1602	92365			None	10.1.1.22	tcp	0	Microsoft Windows Hosts File	Nessus was able to collect the hosts file fro
1603	92367			None	10.1.1.22	tcp	0	Microsoft Windows PowerShell Execution Policy	Nessus was able to collect and report the Po
1604	92371			None	10.1.1.22	tcp	0	Microsoft Windows DNS Cache	Nessus was able to collect and report DNS ca
1605	92421			None	10.1.1.22	tcp	0	Internet Explorer Typed URLs	Nessus was able to enumerate URLs that we
1606	92424			None	10.1.1.22	tcp	0	MUICache Program Execution History	Nessus was able to enumerate recently exec
1607	92428			None	10.1.1.22	tcp	0	Recent File History	Nessus was able to enumerate recently open
1608	92431			None	10.1.1.22	tcp	0	User Shell Folders Settings	Nessus was able to find the folder paths for
1609	92434			None	10.1.1.22	tcp	0	User Download Folder Files	Nessus was able to enumerate downloaded
1610	93962			None	10.1.1.22	tcp	445	Microsoft Security Rollup Enumeration	This plugin enumerates installed Microsoft
1611	96982			None	10.1.1.22	tcp	445	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	The remote Windows host supports the SMB
1612	97086			None	10.1.1.22	tcp	445	Server Message Block (SMB) Protocol Version 1 Enabled	The remote Windows host supports the SMB
1613	99364			None	10.1.1.22	tcp	445	Microsoft .NET Security Rollup Enumeration	This plugin enumerates installed Microsoft
1614	100871			None	10.1.1.22	tcp	445	Microsoft Windows SMB Versions Supported (remote check)	It was possible to obtain information about
1615	103569			High	10.1.1.22	tcp	445	Windows Defender Antimalware/Antivirus Signature Definition Check	Windows Defender AntiMalware / AntiVirus
1616	103871			None	10.1.1.22	tcp	445	Microsoft Windows Network Adapters	Identifies the network adapters installed on
1617	104743			None	10.1.1.22	tcp	3389	TLS Version 1.0 Protocol Detection	The remote service encrypts traffic using an
1618	10107			None	10.1.1.7	tcp	3000	HTTP Server Type and Version	A web server is running on the remote host.
1619	10114	CVE-1999-0524		None	10.1.1.7	icmp	0	ICMP Timestamp Request Remote Date Disclosure	It is possible to determine the exact time se
1620	10267			None	10.1.1.7	tcp	22	SSH Server Type and Version Information	An SSH server is listening on this port.
1621	10287			None	10.1.1.7	udp	0	Traceroute Information	It was possible to obtain traceroute informa
1622	10386			None	10.1.1.7	tcp	3000	Web Server No 404 Error Code Check	The remote web server does not return 404 e
1623	10881			None	10.1.1.7	tcp	22	SSH Protocol Versions Supported	A SSH server is running on the remote host.
1624	10884			None	10.1.1.7	udp	123	Network Time Protocol (NTP) Server Detection	An NTP server is listening on the remote hos
1625	11002			None	10.1.1.7	udp	53	DNS Server Detection	A DNS server is listening on the remote host.
1626	11002			None	10.1.1.7	tcp	53	DNS Server Detection	A DNS server is listening on the remote host.



# Wie kommuniziert man wichtige Dinge

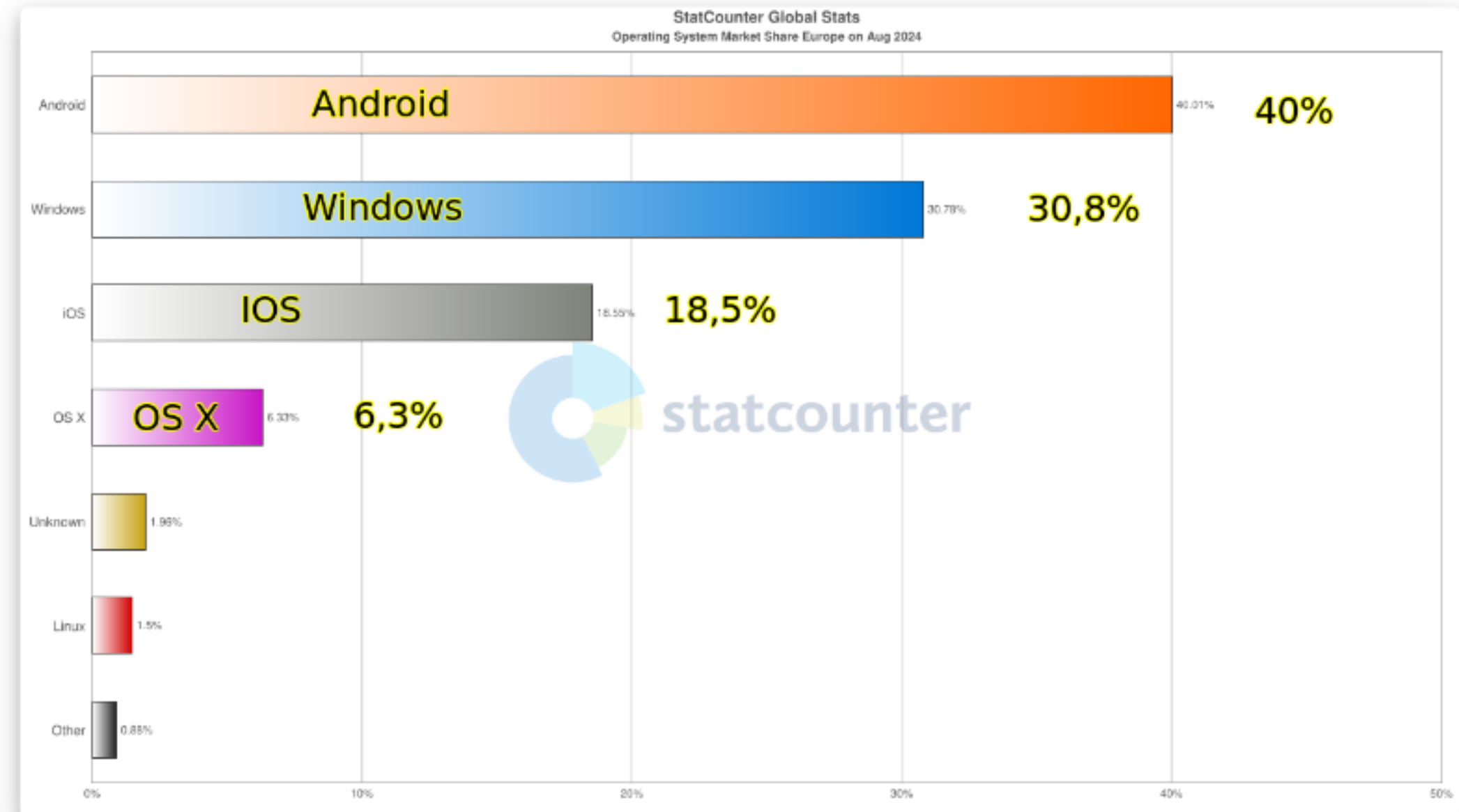
- Chats sind immer beliebter, aber oft automatisiert nach n Monaten gelöscht
- Warnungen an Produkt ManagerInnen, ProjektleiterInnen, Management sollten per Mail erfolgen (BCC an die eigene Adresse schadet auch nicht)

# Wo werden Mails gelesen?



<https://www.litmus.com/email-client-market-share>

- Apple Mail, Apple iPhone, Apple iPad, and Apple's Mail Privacy
- Gmail in a web browser, Gmail mobile app (Android), Gmail mobile app (iOS), all reported as via Gmail's image cache.



<https://gs.statcounter.com/os-market-share/all/europe/#monthly-202408-202408-bar>

- Mac OS / IOS: 25% OS Anteil

# Betreff

- Grossbuchstaben in Maititel
  - RISIKO (zieht eigentlich am Besten)
  - VERZÖGERUNG
  - WARNUNG

# Body

- Management Abstract / TL;DR / Call to Action zu Beginn, kurz und knackig (EIN (1) kurzer Absatz)
- @-Mention "TO" AdressatInnen
- Mailtext direkt und ohne Emotion
- Sollte in schönen Worten in etwa umschreiben:

“

*Kann man so machen, dann ist es halt Scheisse.*



# CYA - Cover your Ass

- Büro-Grabenkämpfe
- Verantwortungs Ping-Pong
- Told You So
- Dokumentation der eigenen Leistung

# CYA - Was

- Mündliche Beauftragung
  - "Wie soeben telefonisch besprochen ..."
- Meeting Ergebnisse
  - "Wie im heutigen Scrum-Standup beschlossen, lieferst Du bis ..."
- Warnungen verschriftlichen
  - "Wie im Jour Fix bereits erwähnt, rate ich von X ab, weil ..."
- Ressourcenkonflikte eskalieren
  - "Lieber Chef, da mich Dein Chef gerade beauftragt hat, X zu tun, bleibt Dein Projekt Y liegen ..."

*"If it is not written down, it does not exist!"*

# Enterprise IT

- an vielen Stellen beeinflusst vom BSI
  - Das BSI hat gesagt/verlangt, dass ...
  - Siehe Crowdstrike
- root ist böse und Admins vorbehalten
  - Jira Tickets für alle Tasks die root benötigen
    - Installation Pakete
    - Systemd
    - Troubleshooting

# Automatisierung

- Weboberfläche um z.B. lokale Firewallregeln für Linux zu beantragen
  - Laufzeit zwischen 30 min und 3 Tagen
  - keine Rechte um aktive Regeln sehen zu können
  - keine Möglichkeit um Aufträge zu kopieren
- Patches meistens automatisiert
  - v.a. auf den Clients mit Zwangsreboot (nachts, bzw. nach max 90 min – 3 Warnungen à 30 Min)
- Konfiguration im Git, aber main Branch geschützt (ohne 4 Augenprinzip kein Merge)
  - andere Branchnamen tun fehlerfrei



# Fehlende Automatisierung

- Server werden manuell vorbereitet (virtuelle Maschinen)
- unterschiedliche umask 077, 027, 022
- unterschiedliche UID Startnummern (1000, 2000, 2020, 3000)
- 6 VM benötigen 2-3 Tage
- Admins haben Angst sich selbst abzuschaffen
  - haben aber für wichtige Aufgaben keine Zeit

# Security ist v.a. geheim

- SIEM Regeln
- Arbeitsanweisung zu Zugriffsbegründung
  - Erinnerung tgl per Mail falls falsch

# Von der Wiege bis zur Bahre, Formulare, Formulare!

- TLS Zertifikatsrenewal: 3 Monate
- Änderungen an der Konfiguration nur mit Jira Ticket und nach Freigabe durch das Change-Board, das einmal die Woche zusammenkommt (Agil !!!)

# Everybody Lies !!!





# Schlusswort



ALWAYS LOOK  
*ON THE BRIGHT*  
SIDE OF LIFE

