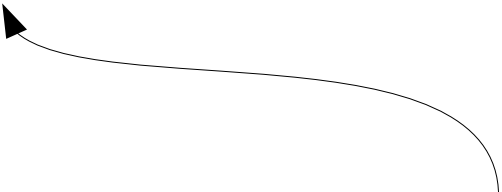


Two Years of Nothing

Closing Keynote **Swiss Cyber Storm 2021**

**A reflective retrospective
by Dr.-Ing. Mario Heiderich**

mario@cure53.de || Signal: +49 1520 8675782



Looking back at two years of
pandemic and the industry,
you, and me.

Our Dear Speaker



- **Dr.-Ing. Mario Heiderich**
 - **Ex-Researcher and now Lecturer, Ruhr-Uni Bochum**
 - PhD Thesis about Client Side Security and Defense
 - Runs the course “Web & Browser-Security” at RUB
 - **Founder & Director of Cure53**
 - Pentest- & Security-Firm located in Berlin
 - Security, Consulting, Workshops, Trainings
 - **The Best Company in the World, or even better**
 - **Published Author and Speaker**
 - Specialized on HTML5, DOM and SVG Security
 - JavaScript, XSS and Client Side Attacks
 - **Maintains DOMPurify**
 - A top notch JS-only Sanitizer, also, couple of other projects
 - **Anxiously considers this his worst talk so far**
 - **mario@cure53.de**
 - **+49 1520 8675782**

So, uhm, how long has it been?

Just yesterday?

A few months?

Just one year?

Two years or more?

I don't even remember?

When of when did you visit the last
actual conference?



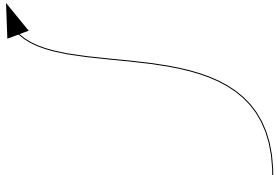
How to even...

Conference?

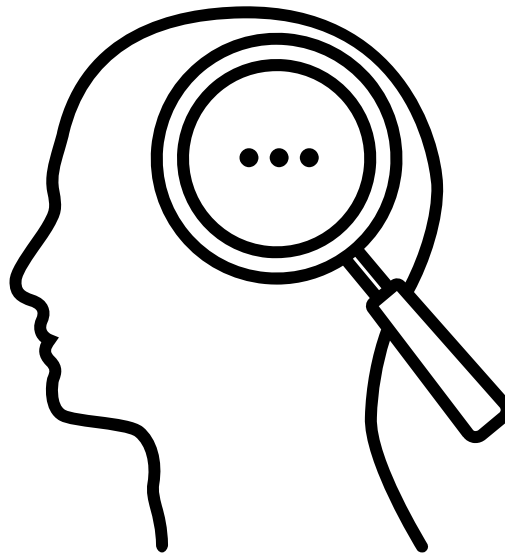
Do this whole travel thing?

Enter a Hotel room?

Order a drink at the bar?



My autopilot forgot everything, how
to pack a bag, how to leave the
house, oh my the anxiety



Or even just doing a talk, or a
keynote. How did that work again?
Well, let's see I guess...

Talk Structure

Act One: General Observations

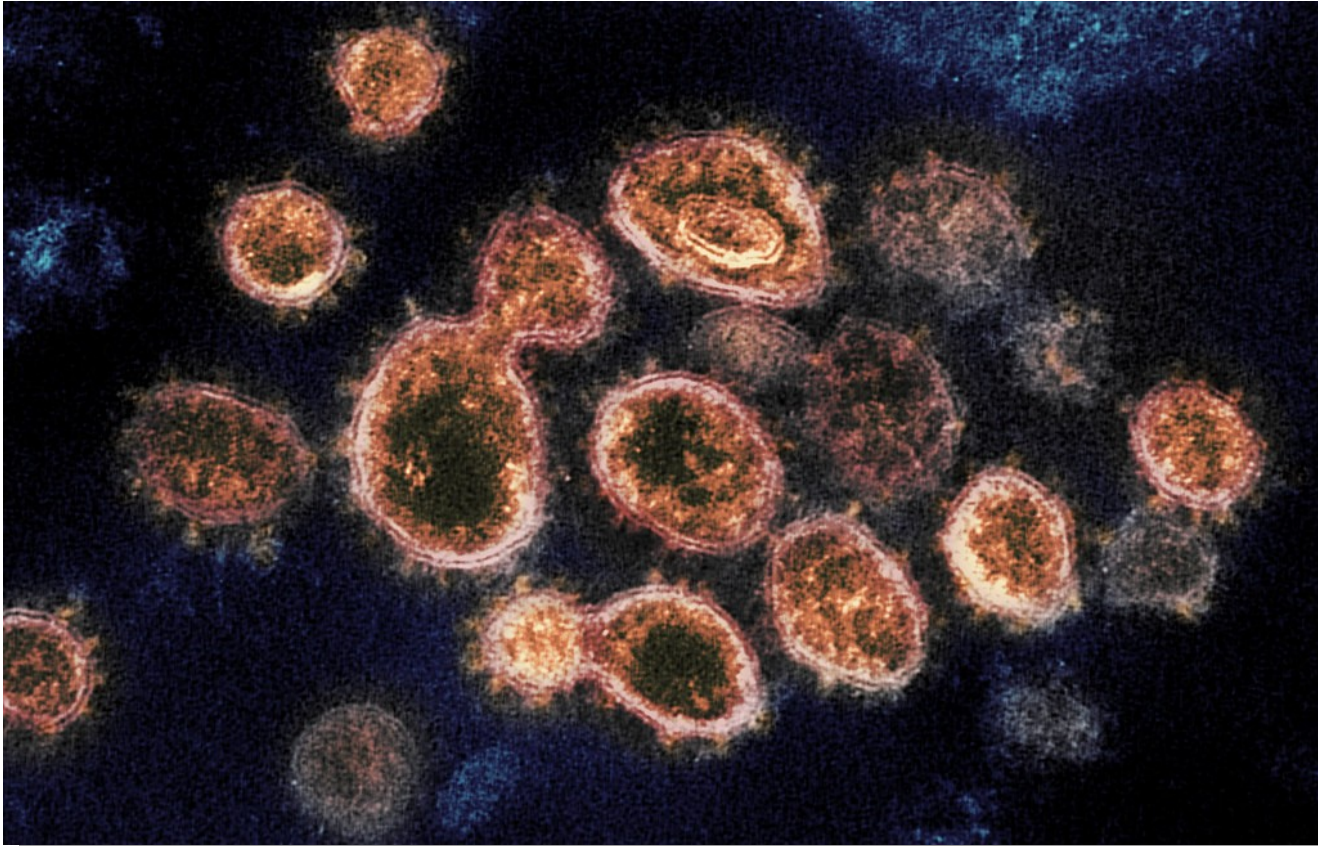
What happened in those last two years

Act Two: Professional Observations

How our industry felt the effects

Act Three: Personal Observations

What I personally noticed



Act One:

General Observations

Disclaimer: Not an expert, 99% of what I think is likely wrong.

Late 2019, and then...

- **This is when it all started for most of us.**
- **Most of us know the timeline quite well.**
 - From zero to hero in the news.
 - Well documented clusters.
 - Several waves were recorded.
 - Lots of terrifying consequences and losses.

The effects on us people

- **Lots of businesses going down**
 - Some industries and sectors more, others less.
 - In our industry, everyone who relied on **on-site work** suffered.
 - Trainers, Consultants, Event organizers, Community Managers, and many more...
- **Other business going through the roof**
 - Those however who specialized on remote work saw massive spikes in workload
 - Noticeable effects for Penetration Testers, Auditors, Online-Trainers, and others too...
- **Stark imbalances showed everywhere, and fear reigned supreme**

COVID-19 & Cybercrime

- **Corona-themed Malware on the rise starting day one**
 - Beyond the Virus: A First Look at Coronavirus-themed Mobile Malware
 - Liu Wang, Ren He, Haoyu Wang, Pengcheng Xia, Yuanchun Li, Lei Wu, Yajin Zhou, Xiapu Luo, Yulei Sui, Yao Guo, Guoai Xu, <https://arxiv.org/abs/2005.14619>
 - Malware Infections in the U.S. during the COVID-19 Pandemic: An Empirical Study
 - Sydney Gero, Sinchul Back, Jennifer LaPrade, Joonggon Kim, <https://vc.bridgew.edu/ijcic/vol4/iss2/3/>
 - Cyber Attacks in the Era of COVID-19 and Possible Solution Domains
 - Isaac Chin Eian, Lim Ka Yong, Majesty Yeap Xiao Li, Yeo Hui Qi, Fatima Z, <https://www.preprints.org/manuscript/202009.0630/v1>
- **Those and many more publications describe the spike in Malware targeting users' fears and worries**
 - Google Scholar tracks several thousand of publications meanwhile
- **Not even talking about COVID-related ransomware 🤖**
 - <https://www.europol.europa.eu/covid-19/covid-19-ransomware>

COVID-19 & Phishing

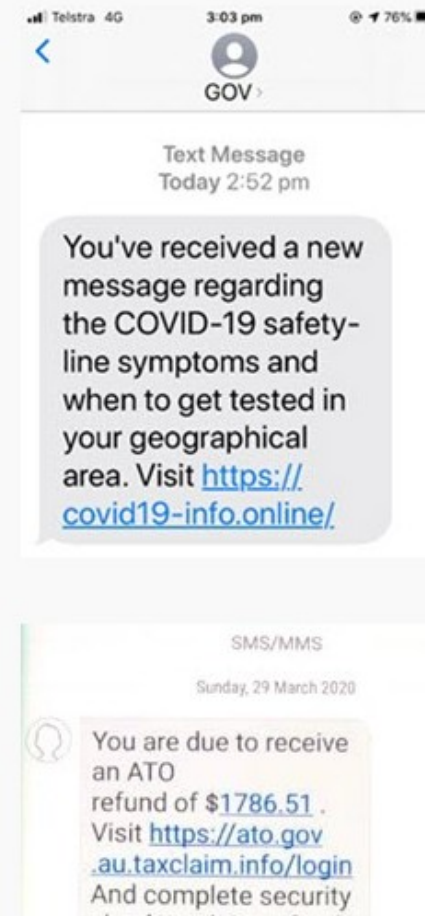
- **Phishers were early to react and abuse the pandemics, too**
 - “Google saw more than 18 million daily malware and phishing emails related to COVID-19 last week”
 - Kim Lyons, <https://bit.ly/3BrZMYB>
 - Several organizations reacted quickly as well and issued warnings
 - Often, showing screenshots of the various malware, fraud and phishing campaigns. Let’s see some of those.
 - <https://www.scamwatch.gov.au/types-of-scams/current-covid-19-coronavirus-scams>
 - <https://www.vadesecure.com/en/blog/hackers-exploit-coronavirus-pandemic-in-latest-event-based-email-attacks>
 - <https://www.hornetsecurity.com/en/security-informationen-en/coronavirus/>
 - And many more, google “Covid phishing”
- **Heck, we even did it too in several campaigns!**

Examples of phishing scams impersonating government agencies

Department of Health impersonation email



Fake myGov texts



From <https://www.scamwatch.gov.au/types-of-scams/current-covid-19-coronavirus-scams>

Examples of payment or financial assistance scams

Fake government subsidy phishing scam



Fake ATO tax credit scam



From <https://www.scamwatch.gov.au/types-of-scams/current-covid-19-coronavirus-scams>

Examples of other phishing scams

Fake bank phishing text



Fake insurance phishing text



Fake voucher phishing text

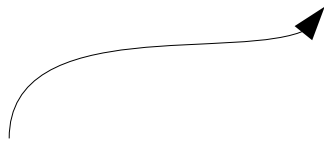


From <https://www.scamwatch.gov.au/types-of-scams/current-covid-19-coronavirus-scams>

Cybercrime? Party time!

For cyber criminals, the pandemics were a festival of **pure joy**.

Fear, uncertainty and doubt reigned supreme, worldwide, **everyone** was susceptible.



Vaccination scams, Mask scams, Government impersonation, Fake medication, Fake news and fake donation drives... everything!



Messing up Society

- The damage the virus did was **immense**, but some of us humans just kept adding on top of it
 - “Analysis of fake news disseminated during the COVID-19 pandemic in Brazil”
 - Barcelos et al., <https://bit.ly/3mM5gcB>
 - “Inoculating Against Fake News About COVID-19”
 - Sander van der Linden, Jon Roozenbeek, Josh Compton, <https://bit.ly/3kDHLQh>
 - “Fake news in COVID-19: A perspective”
 - Diego Carrion-Alvarez, Perla X. Tijerina-Salina, <https://bit.ly/2WwYVXZ>
- We feel the effects of those today, every day, well – at least in Berlin we do unfortunately.

SCIENCE

0

FOULS

0

BONUS



10:00

PERIOD

1



POSS



OH DEAR LORD

GUT
FEELING

3

FOULS

1

BONUS




Some Impressions



Some Impressions



 The Local Germany

Germany's spy agency to monitor 'Querdenker' Covid sceptics - The Local


Visit

Creator: Frank Rumpenhorst | Credit: picture alliance/dpa

Copyright: picture alliance/dpa

Want to know where this information comes from? [Learn more](#)

Some Impressions



Foreign Policy

The Querdenker—Lateral Thinker—Protests Against COVID-19 Measures Sweeping Germany's Cities Show Free Speech Is Alive and Well

Creator: picture alliance | Credit: dpa/picture alliance via Getty Images
Copyright: (c) Copyright 2020, dpa (www.dpa.de). Alle Rechte vorbehalten
Want to know where this information comes from? [Learn more](#)

Visit

Some Impressions



Some Impressions



Mask on, Mask off.

- While the pandemics forced many to wear a mask where they usually wouldn't...
 - It also unmasked lots of misery, wrongdoing, delusion and absurdity.
 - Some might say it even amplified a lot of things that went wrong before already.
 - Sometimes for good, often not so much.
- But where does this leave us, here, **in this room?**



Act Two:

Professional Observations

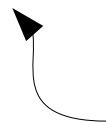
Please note, your mileage may vary.
Opinions and subjective stuff ahead

Daily Business changed...

- In the first months, **not much of a change** was to be observed, business as usual?
 - Predictions and prognoses were plenty, however...
 - Penetration tests and code-audits all continued as planned
 - Trainings were canceled of course, conferences and events were moved by some months
 - Things were seemingly under control
- But then, the lockdown effects hit. Hard.

Some Lockdown Effects

- “Working from home, a dream come true” - no? No? **NO?**
- Collaboration with almost everyone became **a nightmare**
 - People would sometimes disappear without notice :-)
 - Projects got canceled last second, all the time
 - People would be **extremely** thin-skinned and nervous
 - Global Home-Office showed to be a problem, bigger than estimated
 - Every solved task would give birth to at least three new ones
- And no surprise, the amount of work remained identical at least
 - But the means of getting stuff done changed dramatically



Home office, home schooling, home hardware, home everything. The effects were insane.

Apr 12, 2019, 06:28pm EDT | 25,608 views

Are Home Offices Fueling A Mental Health Crisis?



Laurel Farrer Contributor 

Careers

TWEET THIS



remote work has unprecedented opportunities to solve global crises... but it is also fueling a new one.



Remote workers often experience symptoms of anxiety and depression at a higher rate than people commuting into traditional office spaces.

Working from Home and Depression

[Depression vs. sadness](#) | [WFH and depression](#) | [5 to-dos](#) | [Coping resources](#) |
[About depression](#) | [Takeaway](#)



healthline

Health Conditions ▾

Discover ▾

Plan ▾

Connect ▾

MENTAL HEALTH

[Coping with Loneliness](#)

[Mental Health in Focus](#)

[Find a Therapist](#)

[Newsletter](#)



Nitpick Overkill

- Special Focus on Issues coming from insecure Integration of 3rd Party Service Providers
- Cure53 will enumerate B... attempt to locate vulnerable networks, leak sensitive employees, users or cus...
- **Additionally included Services**
 - Detailed royalty-free Pen...
 - Live-Reporting via Slack
 - Consulting and Advice, F...
 - Verification of installed F...

Could we say "at" instead of the French equivalent

Pricing:

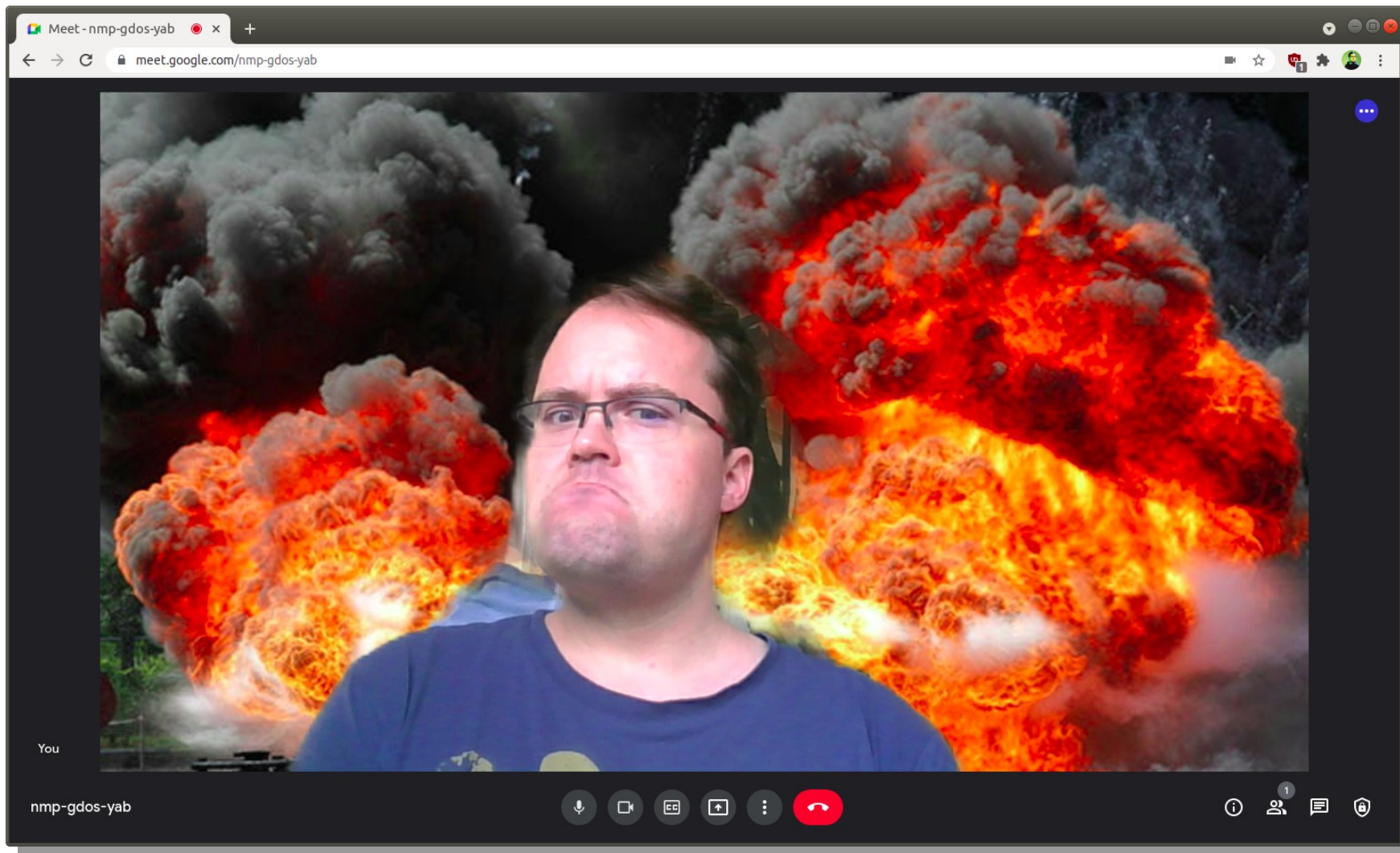
- Mentioned Services as stipulated in this Annexure's Summary and Description, accounted with (a maximum of) **26 daily rates** 1.150,00 EUR (no VAT applies)
- Maximum billable Amount: **€ 29.900,00 EUR** (no VAT applies, payment terms 30 days after invoice). The Terms of the MSA apply to this Annexure

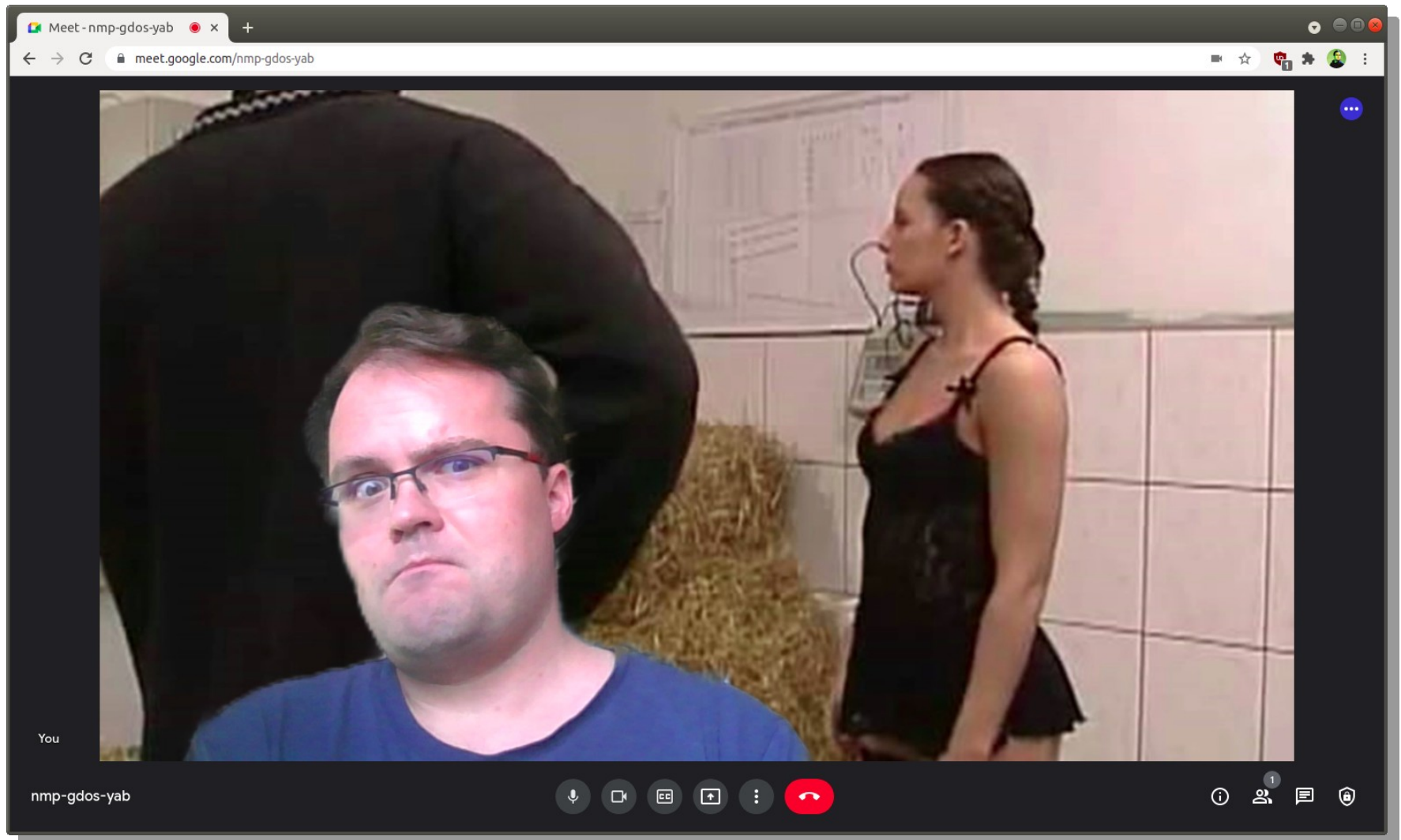
This should read "Subject", as that is the heading of the first paragraph.

Coordination & Communication
Send Security, API Tests and Server-side Security

Zoom Fails

- **This added some fun in-between, for sure.**
 - “Can you hear me?” “...” “No? No audio?”
 - Wow, what an amazing background!
 - Wow, what an amazing **animated** background!
 - Wow, animated background during screen-share... faints
 - My doorbell rings, someone else’s dog barks
 - Un-kept room hidden with well-kept room background





More Online Meeting Fun

- When someone else speaks, move your lips synchronously
- Play a very loud 10KHz sound in the background
 - You can find that here, on Youtube <https://www.youtube.com/v/TRKB5kWs7KE>
- Take your laptop, move it in circles focusing your face
 - If someone asks, pretend everything is fine
- Have an animated background with your self walking around
- Animated background with jump scares also work
- When speaking, move your face extremely close to the camera
- Aaaanyway... enough :D

But also, more Bugs!

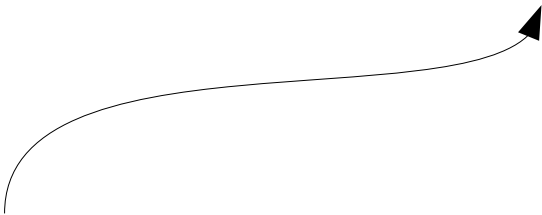
- We noticed over the course of the past months that the number of bugs went up.
- And not only the number, also the severity levels.
 - More critical severity issues in 2021 than ever before.
 - SQL Injections had a renaissance.
 - Platforms once secure now broken as heck.
 - Critical software showing cracks as well.
- But why? We can only guess. Home Office equals...
 - Far less focus on work?
 - Fewer hours to actually work?
 - No peer reviews and missing QA?
 - No more pair programming?



Bad Vibes, Bad Software

More overwhelmed developers means
more insecure software.

More insecure software means more cyber
attacks and **even more fallout.**



A vicious circle, one of the many
side effects of a global
catastrophe. And lots of long
lasting effects too.



Act Three:

Personal Observations

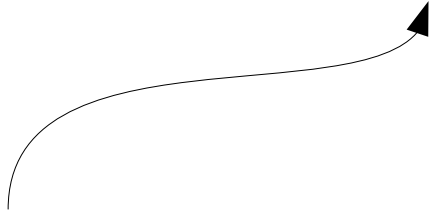
Personal Effects

- Initially, I believed myself to be a home-office exerts I “work” from home since 2007.
 - But it became clear that this doesn't matter too much
 - The chaos around me would drag things down no matter what
 - Early 2021, I was a thin skinned, semi-burnt-out, cabin-fever ridden mess, bad sleep, bad mood
 - Severe need to change processes, to be more mindful, to compensate for lack of social and traveling
 - Things could no go on like this, others around me faces the same challenges too

How to not go crazy

Restructure things from pre-pandemics
mode to fit the **new normal**.

Mindfulness and strictness. Eliminate bad
influences, **reinforce good ones**.



Take walks. Fire crazy clients. Cook more.
Eliminate bad habits. Read more books. Stop
doom-scrolling. Exercise more. Reduce the bad,
emphasize the good.



Final thoughts:

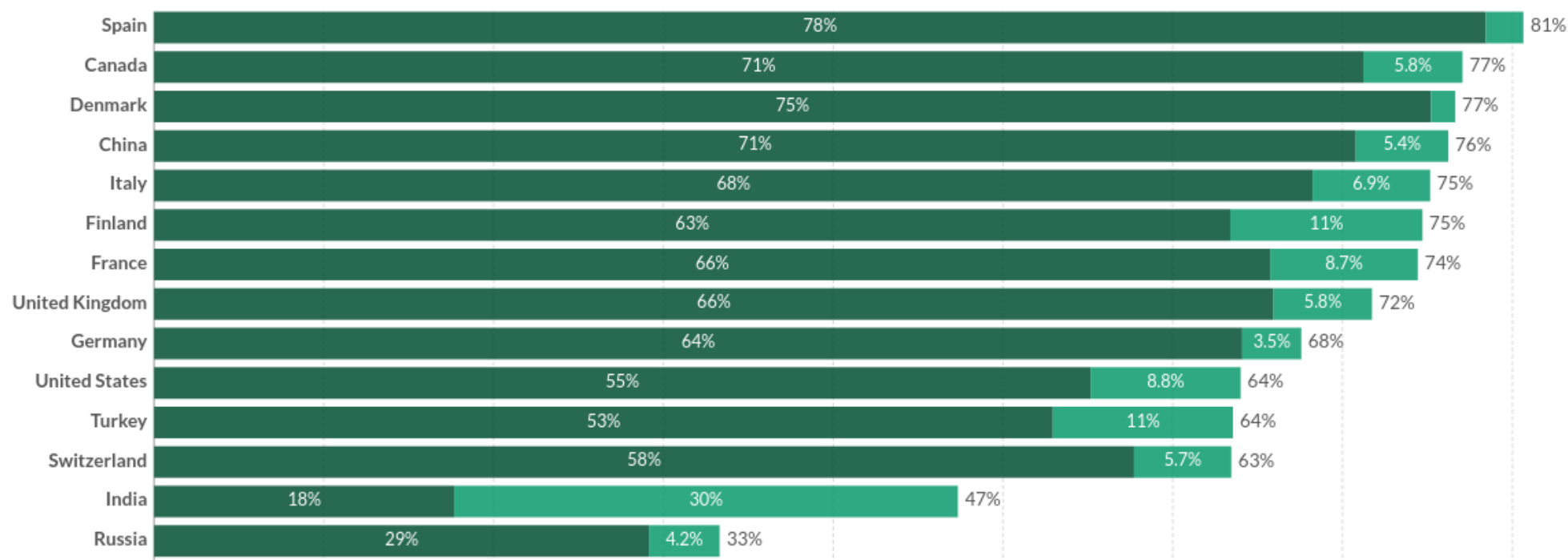
The Road Ahead

Share of people vaccinated against COVID-19, Oct 3, 2021

Alternative definitions of a full vaccination, e.g. having been infected with SARS-CoV-2 and having 1 dose of a 2-dose protocol, are ignored to maximize comparability between countries.

Our World
in Data

■ Share of people fully vaccinated against COVID-19 ■ Share of people only partly vaccinated against COVID-19



And now what?

- So, the pandemics ain't going away **anytime** soon
 - Vaccinations rates of around 60% are not gonna cut it
 - Mutations might happen, this things is here to stay
- Yet we are still here, in this room, **together**
 - Despite all this, thanks to amazing scientific achievements
 - And all of use here putting lots of trust into those achievements
 - And all of us really wanting to hang out again and meet



Back in 2019

2020

- A fight breaks out between the maintainers of CSP 4.0 and CSP.next
 - Two competing standards now, with Chrome supporting CSP.next and Mozilla CSP 4.0
 - Web servers now send at least ten different security headers per response, CSP, CSP.next, XFO, XCTO, HSTS, Super8, HDML, JayLo etc.
- Chrome sets the SameSite flag for all cookies by default
 - This forces millions of websites to change their code
 - After 2-3 months of complete Internet-wide panic, most of the WWW is sort of working again, no more CSRF
 - Developers find novel ways of re-implementing CSRF because without it "everything falls apart"
- All OWASP conferences are canceled until 2050
 - To see if the prophecies are accurate and not interfere with future events based on the knowledge gained in this talk.

CURE+53

Global AppSec
Amsterdam
by OWASP Foundation

without it "everything

re events based on the

An Infosec Timeline:
Noteworthy Events From 1970 To 2050

→ Mario Heiderich

49:05 / 1:01:41



CURE+53

Back in 2019



- All OWASP conferences are **canceled** until 2050
- To see if the prophecies are accurate and not interfere with future events based on the knowledge gained in this talk.

No more predictions from me. Ever.
Not if that is the actual outcome.
Sorry, shop's closed.

Now, in 2021 and beyond

- Let's **not work towards** canceling all conferences until 2050
 - But rather be mindful and enable more events like this one
 - And rather support meetups in reasonable ways, like here
 - Turn towards smaller, local events rather than fly across the ocean
- **We're all humans after all and we need social**
 - And we can still do it as (also) this conference has proven
- **Lets value every opportunity that is safe and reasonable**
- **Let's all wake up from the pandemics blues and do things**
 - Nicely, safely, reasonably, mindfully, ...

Let's close the gap of
two years of nothing
!

The End

- Question? Comments?
- **Thanks a lot! Like and subscribe.**
- **Shouts go out to**
 - The Conference Organizers..
 - Authors of Articles & Papers referenced..
 - Artists behind images stol.. **showcased..**
 - Everyone here for being here!
- **Ping me please if you have questions!**
 - **mario@cure53.de**