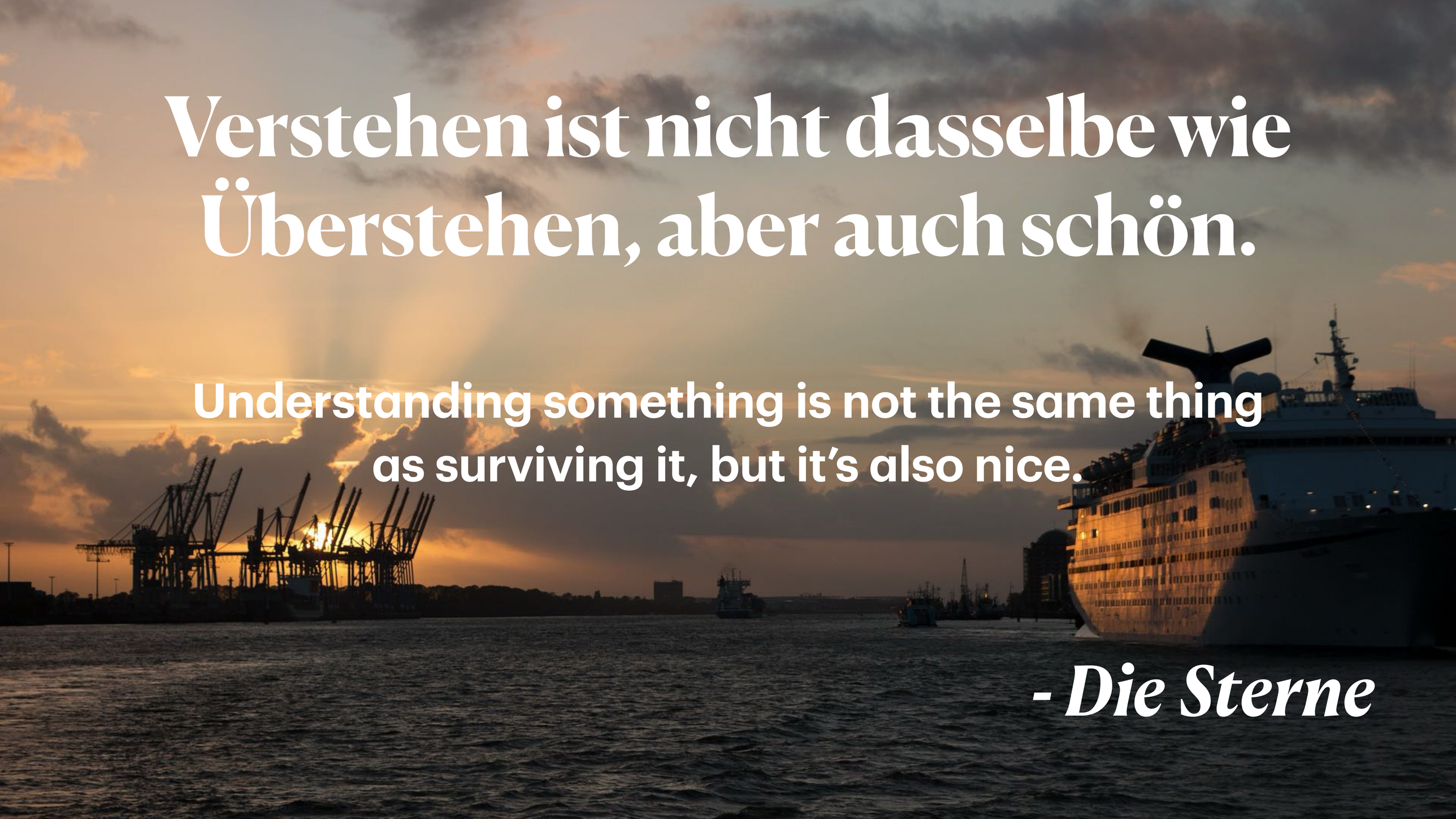
Far Beyond the Perimeter

Exploring External Attack Surfaces

khae 2024


Verstehen ist nicht dasselbe wie
Überstehen, aber auch schön.
Understanding something is not the same thing
as surviving it, but it’s also nice.
- Die Sterne

What this talk is about

About the perimeter...

Ignorance is bliss?

Exposing your private parts by putting your head
in the sand is not a viable strategy

Digital assets

Leaked Credentials (yawn)

Surprise!

Rogue websites

Vintage protocols

Code repositories

Partners and 3rd parties

Archives

ngur
3
App Store

Pastebins

RACCOLTA
CARTA
RACCOLTA
VETRO
RACCOLTA
PLASTICA
RACCOLTA
LATTINE

Wait, there's more!

Now what?

Your decision

If you aim for 100% - 99.999% is better than 99.99%

surely?

10% is better than 0%

Sinkholes

Keeping an eye on the Deep and Dark

Trust Issues

Are the “good” people really good people?

Using LLMs to test for side-channel attacks

Getting help

Attribution

Compliant doesn’t mean secure

Internal struggles

Conclusion

Links

Checking for leaked credentials:

haveibeenpwned.com

leakchecker.uni-bonn.de/de/index (German)

Rogue websites / newly registered domains:

letsencrypt.org/docs/ct-logs/

developers.facebook.com/tools/ct/ (needs facebook account)

dnslytics.com/domain-search/

Links

TLS version checker:

testssl.sh (it's a website)

Website hygiene:

www.immuniweb.com/cloud/

www.bitsight.com/

Sinkholes

www.shadowserver.org/

Links

Code repositories:

github.com

gitlab.com

bitbucket.org

Archives

archive.org

archive.io

Subdomain reconnaissance

github.com/aboul3la/Sublist3r

Canary Tokens:

www.canarytokens.org/nest/

Pastebins

pastebin.com

kleber.io

Links

Some unofficial app stores

pkpure.net
apkpure.com
aptoide.com
gratuitpourpc.com
apkgk.com
apkdownload.com
apk.support
luckymodapk.com
napkforpc.com
moddescargar.com

uptodown.com
aapks.com
steprimo.com
apkcombo.com
apkmonk.com
apkdll.com
apkfab.com
daroid.com
modapkdown.com
apkaio.com

softonic.com
9apps.com
appfurpc.com
apkonline.net
apksos.com
apkfun.com
apkfollow.com
...

Thank you for listening!

Questions?

You have questions, I have gifts...

I am also shameless.