FFHS
Fernfachhochschule Schweiz
Mitglied der SUPSI

Herzlich Willkommen

FFHS-BUSINESS BREAKFAST:

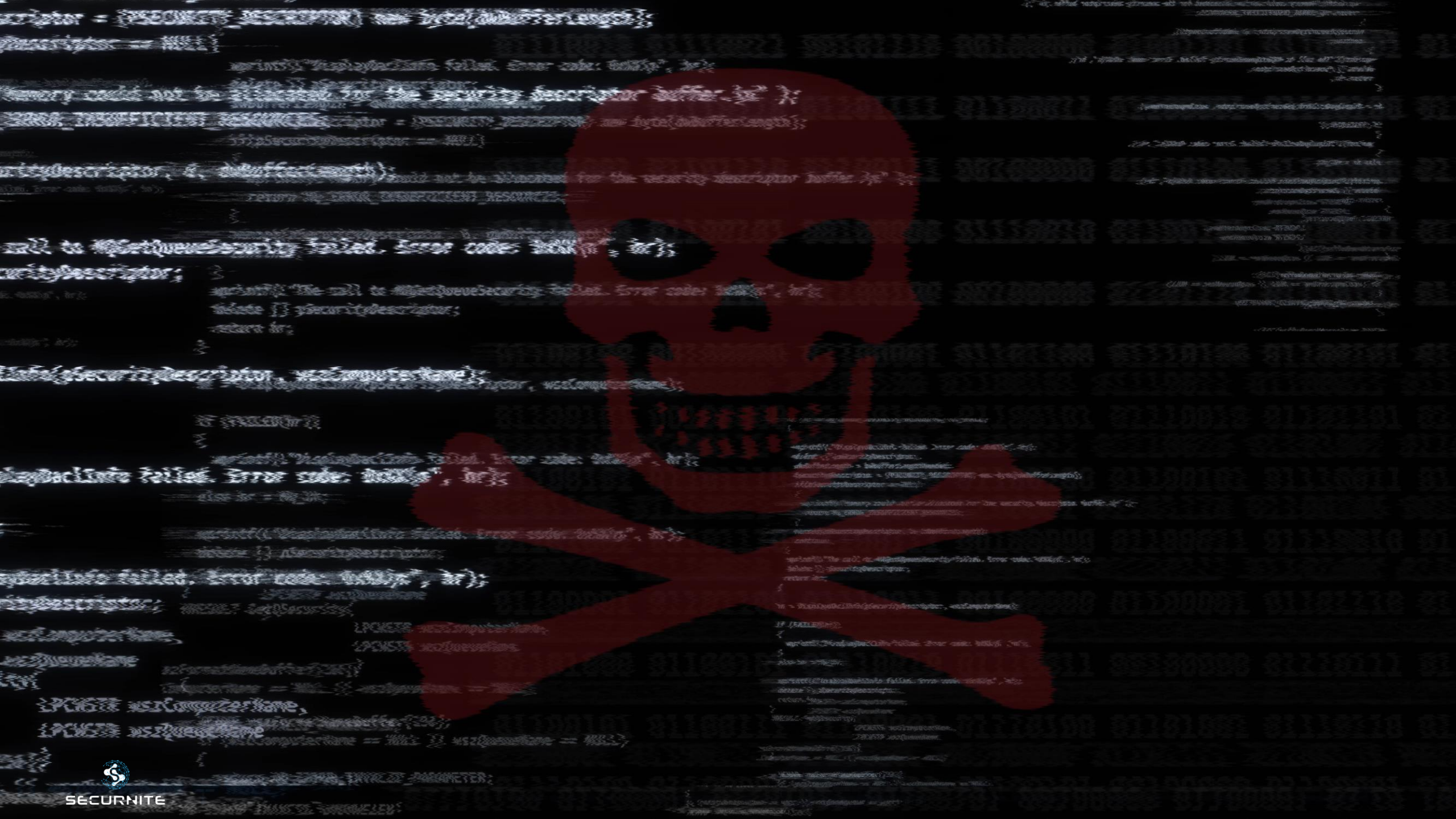
WHITE HAT-HACKERS – IST ANGRIFF DIE BESTE VERTEIDIGUNG?

Aktuelle IT-Gefahrenlagen und Lösungsansätze für Unternehmen

FFHS-Business Breakfast: White Hat-Hackers – Ist Angriff die beste Verteidigung?

Februar 2023

SECURNITE

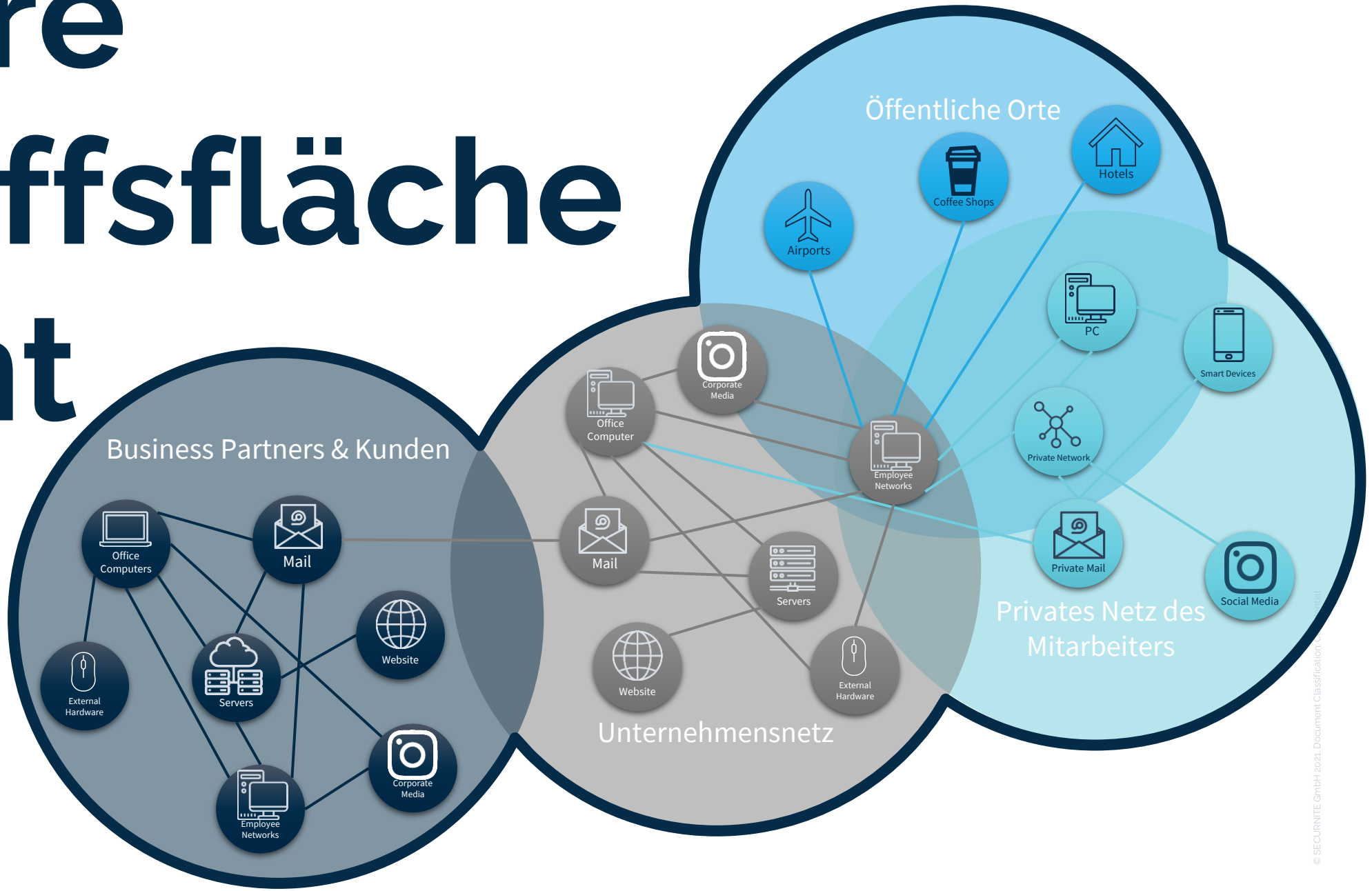


SECURNITE

Warum ist Cyber Security wichtig?

SECURNITE

Unsere Angriffsfläche nimmt zu



SECURNITE

E-Mail-Dienstleister: Angreifer haben erneut Kundendaten bei Mailchimp kopiert

Zum wiederholten Male gab es bei Mailchimp ein Datenleak, von dem Kunden aus dem Bereich der Kryptogeld-Plattformen betroffen sind.

19. Januar 2023, 13:47 Uhr

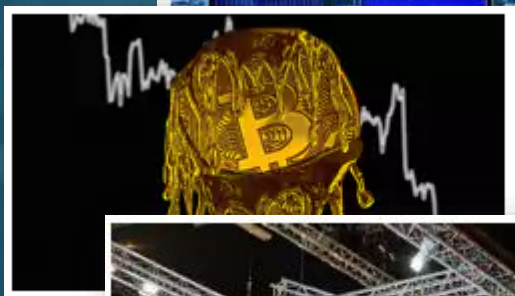
37 Millionen Kunden von Cyber-Angriff auf T-Mobile US betroffen

Die US-Tochter der deutschen Telekom ist Opfer einer weite-

Hackerin findet "No Fly List" der US-Regierung auf Testserver einer Fluglinie

Aus Langeweile habe sich "Maia Arson Crimew" einen ungesicherten Server von CommuteAir angeschaut. Dort fand sie eine Flugverbotsliste des FBI von 2019.

23. Januar 2023, 08:42 Uhr 235 UPDATE | heise online



Europol hebt Kryptobet viele deutsche Opfer

Europol hat eine Betrügerbande

League of Legends: Hacker dringen in Entwicklungsumgebung von Riot Games ein

Der Entwickler der erfolgreichen Videospiele League of Le-

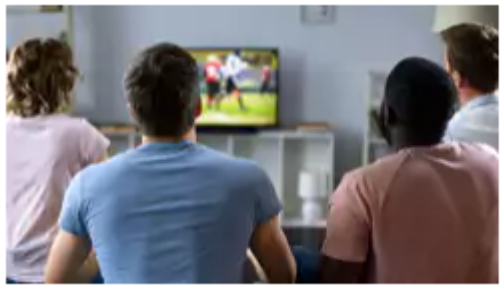
20. Januar 2023, 08:53 Uhr

Die Betreiber der Cloud-basier
Plattform CircleCI haben ihren
vorfall veröffentlicht.

Attacke auf Online-Apotheke DocMorris: 20.000 Kundenkonten betroffen

DocMorris zufolge kompromittierten Hacker 20.000 Konten aufgrund "mehrfach verwendeter Passwörter". Daraufhin wurden Konten vorsorglich gesperrt.

26. Januar 2023, 18:53 Uhr 54 UPDATE



"Cyberkriminelle" verschaffen sich Zugang zu Sky-Kundenkonten

Der Pay-TV-Anbieter Sky bestätigt, dass sich bösartige Akteure Zugriff zu Kundenkonten verschafft haben. Details gibt es noch nicht, der Schaden ist unklar.

23. Januar 2023, 14:00 Uhr 15 UPDATE

Cyber-Angriff: IT der TU Freiberg weitreichend lahmgelegt

Ein Cyber-Angriff auf die IT der TU Freiberg in Sachsen führt zu weitreichenden Einschränkungen. Zum Wochenende hat die Uni die Internetverbindungen gekappt.

24. Januar 2023, 21:43 Uhr 166

Kritische Sicherheitslücke b… Life-Router von Cisco

Der Netzwerkausrüster Cisco hat wic… dates für etwa verschiedene Router, … Webex veröffentlicht.

12. Januar 2023, 12:20 Uhr 2

Cyber-Attacken auf kritische Lücke in Control Web Panel

Cyberkriminelle greifen eine kritische Sicherheitslücke in CWP (Control Web Panel, ehemals CentOS Web Panel) an. Sie kompromittieren die verwundbaren Systeme.

13. Januar 2023, 13:55 Uhr 2

Webbrowser: Microsoft Edge-Update schließt hochriskante Lücken

Microsoft hat in einem Update des Webbrowsers Edge Si-

Jetzt patchen! Viele Cacti-Server öffentlich erreichbar und verwundbar

Sicherheitsforscher stoßen auf tausende über das Inter- … mit dem IT-Monitoring-Tool Cacti. … vurden noch nicht gepatcht.

2

Cisco: Hochriskantes Sicherheitsleck in Unified Communications Manager

In der Unified Communications Manager-Software von Cisco klafft eine Sicherheitslücke mit hohem Risiko. Der Hersteller stellt Updates zum Schließen bereit.

20. Januar 2023, 10:19 Uhr 9

Angreifer konnten ManageEngine-Produkte wie Access Manager Plus und Password Manager Pro mit Schadcode attackieren.

17. Januar 2023, 11:39 Uhr

…uter von InHand: Angreifer …e in der Cloud übernehmen

Es gibt wichtige Sicherheitsupdates für verschiedene In-Router-Modelle von InHand. Eine Lücke gilt als kritisch.

NortonLifeLock: Hersteller warnt vor potenziell geknackten Passwortmanagern

…greifer haben Nutzer-Passwort-Kombinationen durch-…testet und dabei Zugriff auf Norton-Konten erhalten. …s gefährdet Daten des Passwortmanagers.

…Januar 2023, 12:22 Uhr 35

Junos OS via DoS-Attacke …

MSI-Motherboards sollen trotz aktivem Secure Boot manipulierte Systeme starten

Ein Sicherheitsforscher hat herausgefunden, dass der Schutzmechanismus Secure Boot auf MSI-Motherboards zwar aktiv ist, aber trotzdem alles durchwinkt.

18. Januar 2023, 14:36 Uhr 69

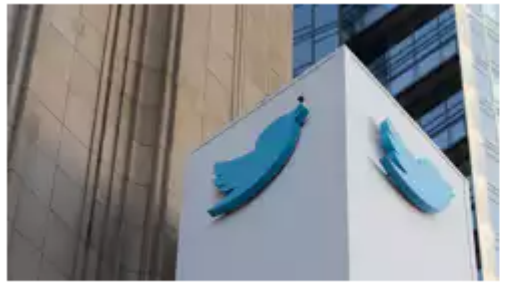
Wieso sollten Sie sich schützen?

SECURNITE

Fahrradhersteller: Prophete nach Cyber-Angriff in Insolvenz gerutscht

Der Insolvenzverwalter beim Fahrradhersteller Prophete hat als Ursache für die Insolvenz einen Cyber-Angriff ausgemacht, der einen Betriebsstillstand auslöste.

11. Januar 2023, 12:54



Twitter wegen Datenlecks auf fünf Millionen US-Dollar verklagt

Ein New Yorker verklagt Twitter auf 5 Millionen US-Dollar wegen eines Datenlecks, durch das die Daten von mehr als 235 Millionen Nutzern offengelegt wurden.

16. Januar 2023, 23:32 Uhr 10 | heise online

Die finanziellen Folgen können ruinös sein

SECURNITE

Der Reputations-verlust ist immens

SECURNITE

Was wird die Zukunft bringen?

SECURNITE

SECURNITE

Mehr Sicherheit durch ethische Hacker

GO BUGFREE

Februar 2023 | rolf.wagner@gobugfree.com

whoami

Wir setzen auf Experten in jedem Gebiet

Infosec Professionals seit 2003

Gründung im April 2021

> 900 Friendly Hacker

Unsere Mission

leveraging technology and the power, skills and creativity of our friendly hacker crowd

Other Stakeholders

Verwaltungsrat

Terry Fehlmann Founder / CEO placeB AG

Thierry Kneissler Co-Gründer TWINT

Partners

fidentity

BugBountyHunter

«A hacker to me is someone creative who does wonderful things.»

Tim Berners-Lee
(computer scientist best known as the inventor of the World Wide Web)

Fragen wir doch mal chatGPT…

Ein **Hacker** ist eine Person, die sich mit Computersicherheit und Netzwerken beschäftigt und **versucht, in Computer-Systeme und Netzwerke einzudringen, um sie zu untersuchen oder zu modifizieren**. Ein Hacker kann sowohl ethisch als auch unethisch sein. Ethische Hacker (auch "weiße Hut-Hacker" genannt) nutzen ihre Kenntnisse, um Schwachstellen in Computer-Systemen und Netzwerken aufzudecken und diese zu beheben, bevor sie von unethischen Hackern ausgenutzt werden können. Unethische Hacker (auch "schwarze Hut-Hacker" genannt), dagegen, nutzen ihre Kenntnisse, um in Computer-Systeme und Netzwerke einzudringen, um persönliche Informationen zu stehlen, Schaden anzurichten oder sogar Geld zu stehlen.

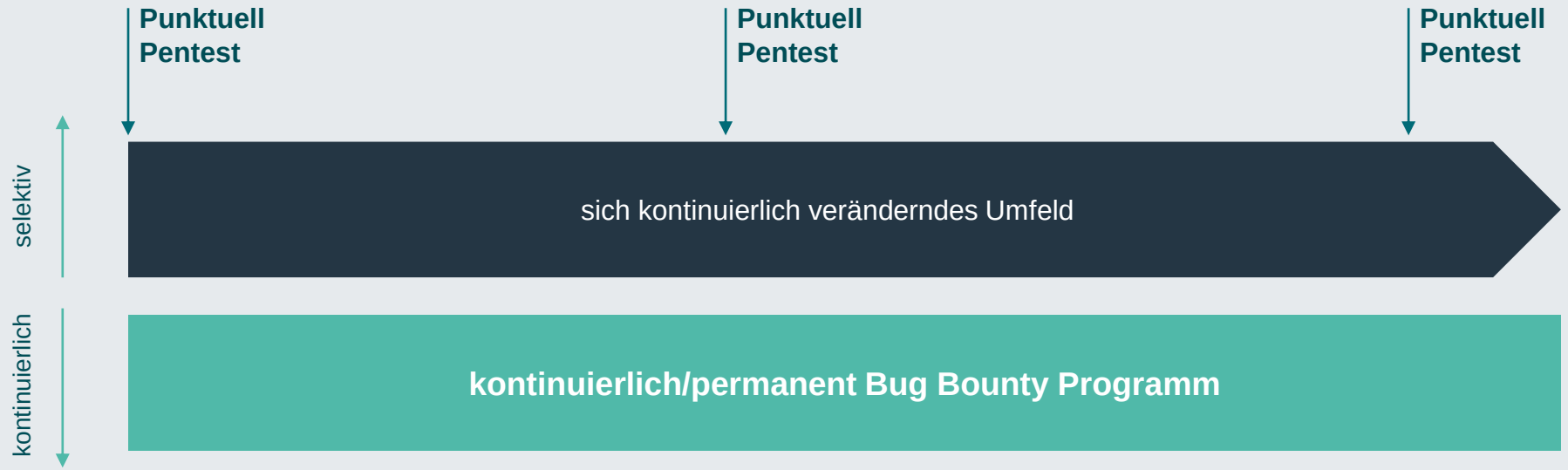
Wieso in Security investieren?
Stärkere Bremsen ermöglichen mehr Tempo!

- Security ist kein „Bremsklotz“ …
- … aber leistungsfähige und skalierbare Security-Massnahmen (Bremsen) verhindern auch bei höherer Geschwindigkeit Unfälle.

- Ethische Hacker – z.B. als Pentester oder Rahmen eines Bug Bounty Programmes sind ein wichtiges Puzzleteil im Sicherheitsdispositiv eines Unternehmens.

BUG-BOUNTY-PROGRAMME VS. PENTESTING

PENTESTING IST EIN PUNKTUELLER DEEP-DIVE

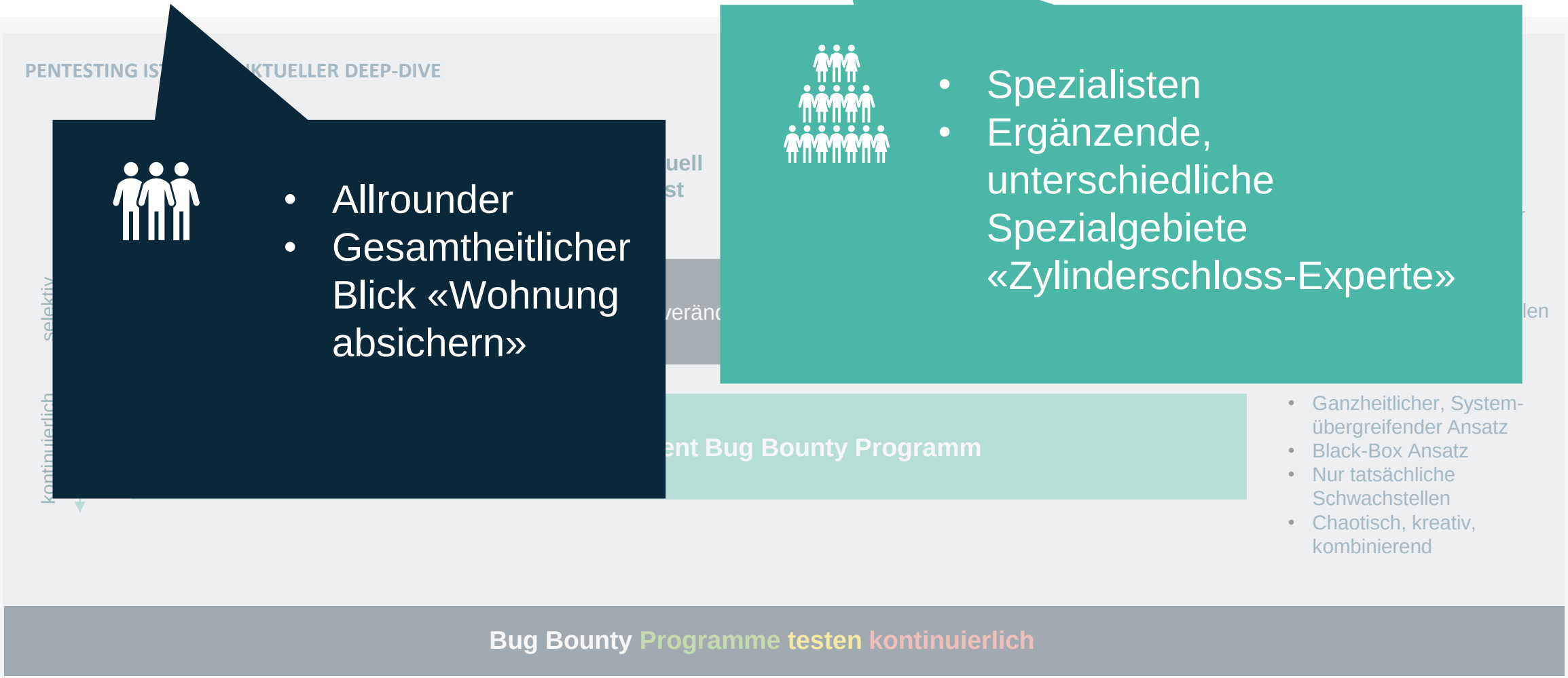


- Spezifischer Fokus auf Sourcecode, Architektur und Entwicklerprozesse
- White-Box Ansatz
- Auch theoretische (mögliche) Schwachstellen
- Meistens nach einem erprobten Schema

- Ganzheitlicher, System-übergreifender Ansatz
- Black-Box Ansatz
- Nur tatsächliche Schwachstellen
- Chaotisch, kreativ, kombinierend

Bug Bounty Programme testen kontinuierlich

BUG-BOUNTY-PROGRAMME VS. PENTESTING



- Allrounder
- Gesamtheitlicher Blick «Wohnung absichern»

- Spezialisten
- Ergänzende, unterschiedliche Spezialgebiete «Zylinderschloss-Experte»

Was motiviert Ethische Hacker?

- **Monetary rewards** Monetäre Entschädigung.
- **Learning** Lernen oder Verbessern von Fähigkeiten
- **Enjoyment** Spaß oder Herausforderung beim White-Hat-Hacking. Ruhmeshalle.
- **Legal** Schutz-Hacken, ohne dass rechtliche Schritte drohen, wenn man sich an die Regeln hält.
- **Flexibility** Flexibilität in Bezug auf Arbeitszeiten und -orte (im Vergleich zu herkömmlichen Arbeitsverhältnissen).
- **Career** Aufbau von Beziehungen zu Unternehmen für eine Anstellung und andere Möglichkeiten.
- **Community** Gemeinschaft Bug Bounty schafft eine Gemeinschaft von Hackern.
- **Altruism** Verbesserung der Cybersicherheit, um anderen zu helfen und das Internet zu sichern.
- **Reputation** Verdienen von Reputationspunkten auf der Plattform, Aufbau einer Fangemeinde usw.
- **Non-monetary:** Belohnungen nicht-monetäre Vergütung (z. B. SWAG, Hardware, Abonnements).

Source: https://arxiv.org/pdf/2301.04781.pdf

«You can never protect yourself 100%. What you do is protect yourself as much as possible.»

Kevin Mitnick
(computer security consultant, author, and convicted hacker)

WIESO BUG BOUNTY EINSETZEN?

Frühzeitige Erkennung von Sicherheitsschwachs tellen, bevor sie ausgenutzt werden.

Höheres Bewusstsein in den Entwicklungsteams, bei Einsatz eines Bug-Bounty Programms.

Kreativität der Crowd, Belohnung im Falle eines erfolgreichen Fundes und intrinsische Motivation der Friendly Hacker.

Kontinuierliche Überwachung der Systeme durch eine Gemeinschaft von Sicherheitsexperten mit unterschiedlichen Fähigkeiten.

Konsultation und Austausch mit verschiedenen GObugfree Sicherheitsexperten. Vermeiden Sie blinde Flecken.

Contact us:

Rolf Wagner
Chief Operations Officer & Co-Founder
+41 58 255 04 32
rolf.wagner@gobugfree.com
linkedin.com/in/rolf-wagner/

DREAMLAB
TECHNOLOGIES

FFHS-Business Breakfast

Hochpräzisions Cyber-Radarsystem für die Schweiz

Fernfachhochschule Schweiz FFHS| Zürich, 2. Februar 2023

Dreamlab Technologies

Introduction

Nick Mayencourt

Founder and CEO Dreamlab Technologies,
Board Member ISECOM
and Oneiroi

swiss cyber security DAYS

W3C® MEMBER

Bern University of Applied Sciences

University of Applied Sciences and Arts Northwestern Switzerland

UNIVERSITÄT BERN

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

OWASP
Open Web Application Security Project

CYBERSECURITY MADE IN EUROPE


Cyber Bedrohungslage

Globales Problem

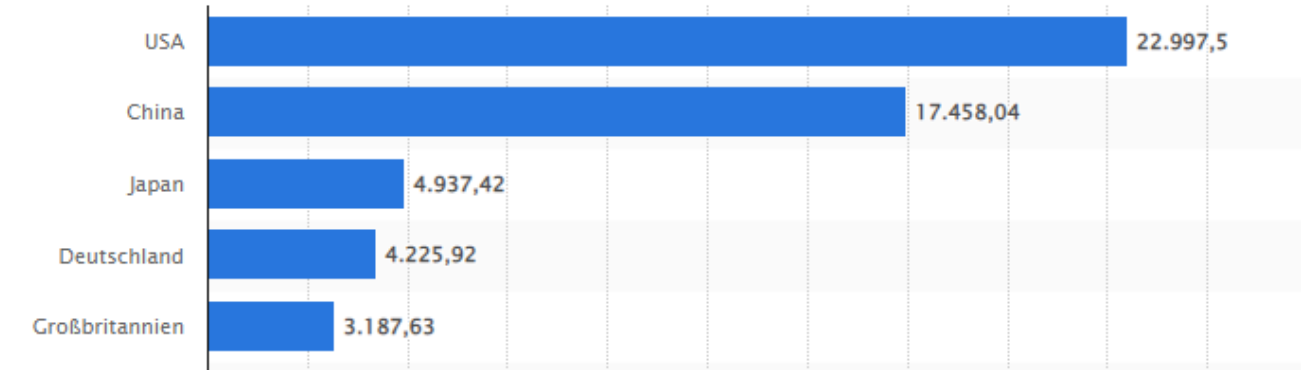
2021 betrugen die weltweiten Schäden durch Cyberangriffe über 5 Billionen Schweizer Franken.

Experten gehen davon aus, dass die Schäden 2025 bei 10 Billion und 2027 bei rund 23 Billionen Schweizer Franken liegen.

Solche Schadenssummen sind nicht mehr versicherbar.

Gemessen am BIP sind Schäden durch Cyberangriffe schon heute die drittgrösste Volkswirtschaft der Welt.

(*In Milliarden US Dollar*)



Cyberkriminalität betrifft auch uns

2021 war jedes Dritte Schweizer Unternehmen Opfer von Cyberkriminalität (gemeldete Fälle).

Verdopplung zu 2020, nur die Spitze des Eisbergs, da nur 25% der Fälle gemeldet werden.

Der durchschnittliche Schaden für ein KMU in der Schweiz beläuft sich auf zirka 6 Mio. CHF. Schwere Angriffe mit Datendiebstahl und -verschlüsselung können 50 bis 150 Mio. CHF kosten.

In der Schweiz verursachten die gemeldeten Cyberangriffe 2020 Schäden in Höhe von über 1 Milliarde Franken. 2021 waren es bereits über 2,5 Milliarden Franken – Tendenz weiter steigend.

Angriffe aus dem Cyberraum sind eine grössere Gefahr als Naturkatastrophen, Pandemien und Betriebsunterbrüche.

Physisch vs Digital

Sources: https://www.netzwoche.ch/news/2022-03-28/bfs-zaehlt-fast-83-digitale-straftaten-pro-tag / BfS (2022): Die Schweiz in 23 Infografiken: Gesellschaft, Wirtschaft, Raum und Umwelt, Neuenburg.

Top und Flop

Top ten innovative economies

#GlobalInnovationIndex

2021

Source: WIPO, 2021

1. Switzerland
2. Sweden
3. United States of America
4. United Kingdom
5. Republic of Korea
6. Netherlands
7. Finland
8. Singapore
9. Denmark
10. Germany

VS.

Table 3: GCI results: Global score and rank

Country Name	Score	Rank
United States of America**	100	1
United Kingdom	99.54	2
Saudi Arabia	99.54	2
Estonia	99.48	3
Korea (Rep. of)	98.52	4
Singapore	98.52	4
Spain	98.52	4
Russian Federation	98.06	5
United Arab Emirates	98.06	5
Malaysia	98.06	5
Lithuania	97.93	6
Japan	97.82	7
Canada**	97.67	8
France	97.6	9
India	97.5	10
Turkey	97.49	11
Australia	97.47	12
Luxembourg	97.41	13
Germany	97.41	13
Portugal	97.32	14
Latvia	97.28	15
Netherlands**	97.05	16
Norway**	96.89	17
Mauritius	96.89	17
Brazil	96.6	18
Belgium	96.25	19
Italy	96.13	20
Oman	96.04	21
Finland	95.78	22
Egypt	95.48	23

Country Name	Score	Rank
Indonesia	94.88	24
Viet Nam	94.59	25
Sweden	94.55	26
Qatar	94.5	27
Greece	93.98	28
Austria	93.89	29
Poland	93.86	30
Kazakhstan	93.15	31
Denmark	92.6	32
China	92.53	33
Croatia	92.53	33
Slovakia	92.36	34
Hungary	91.28	35
Israel**	90.93	36
Tanzania	90.58	37
North Macedonia	89.92	38
Serbia	89.8	39
Azerbaijan	89.31	40
Cyprus	88.82	41
Switzerland**	86.97	42
Ghana	86.69	43
Thailand	86.5	44
Tunisia	86.23	45
Ireland	85.86	46
Nigeria	84.76	47
New Zealand**	84.04	48
Malta	83.65	49
Morocco	82.41	50
Kenya	81.7	51
Mexico	81.68	52
Bangladesh	81.27	53

Grosse Gefahr für die Schweiz

Die Häufigkeit und Zahl von Cyberattacken explodieren, Angriffe werden heute professionell und hochgradig automatisiert ausgeführt.

Mit dieser Dynamik hält das Verhalten der Unternehmen in der Schweiz nicht Schritt. Viele sehen sich noch immer nicht als potenzielles Ziel oder haben das mögliche Ausmass verstanden.

Cyberangriffe sind nicht nur eine grosse Gefahr für die Wettbewerbsfähigkeit und Innovationskraft der Schweiz, Angriffe von staatlichen und hochprofessionalisierten nichtstaatlichen Hackergruppen bedrohen auch die nationale Sicherheit und unsere Demokratie.

Cyberangriffe sind heute fixer Bestandteil militärischer Kriegsführung, manipulieren die öffentliche Meinungsbildung oder beeinflussen Wahlen.

Fehlendes Verständnis & falsche Einordnung

Die digitale Vernetzung und Komplexität unserer globalisierten Welt wächst rasant und ist nicht mehr überschaubar.

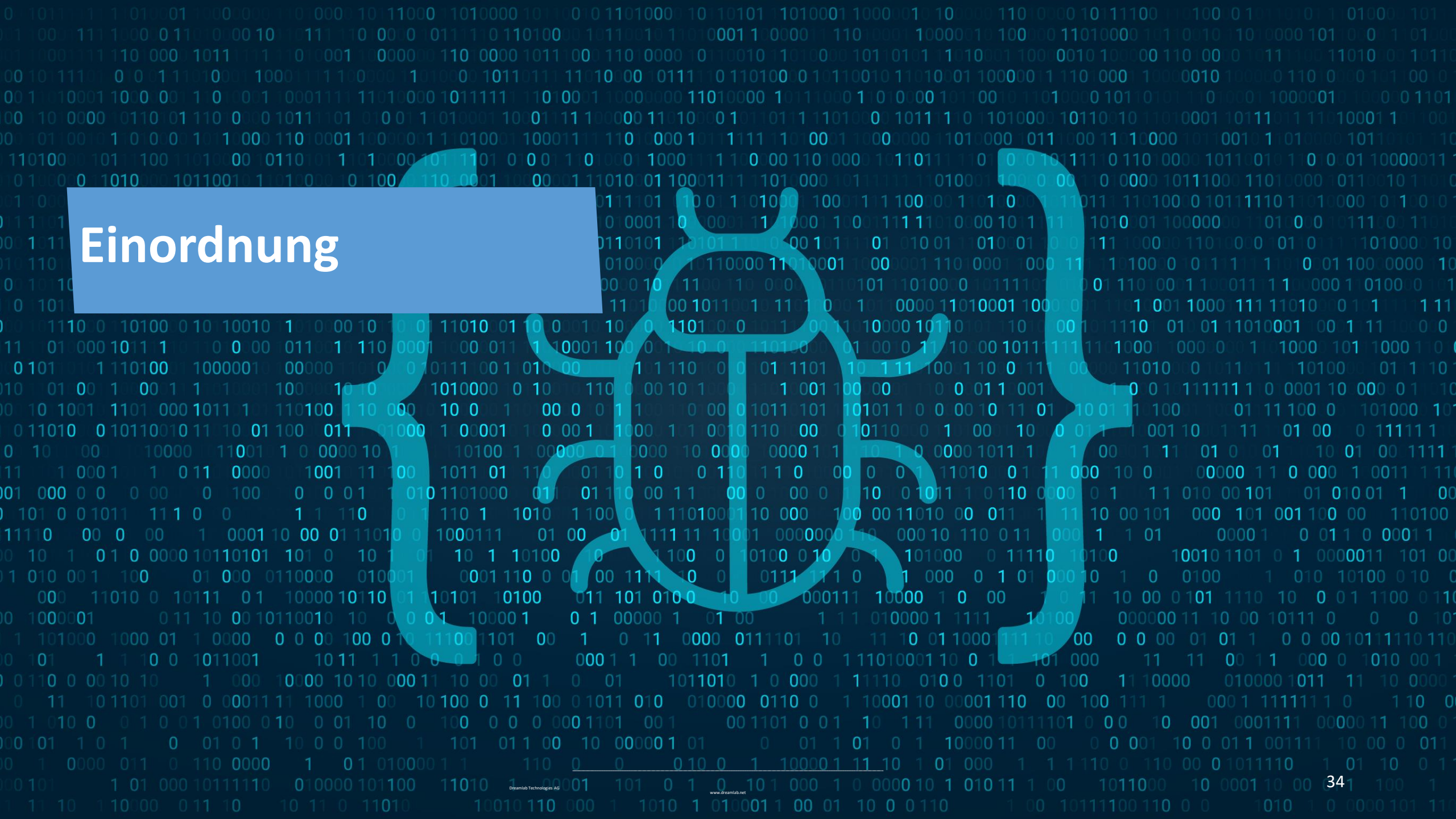
Es fehlt an Verständnis für die Abhängigkeiten, Wechselwirkungen und Funktionsweisen der technischen Systeme.

Das Thema ist längst in der Breite angekommen, die eigene Verwundbarkeit wird falsch eingeschätzt.

Kurz: Die Tragweite des Schadensausmasses wird falsch eingeschätzt, die eigene Verwundbarkeit unterschätzt und die dringend notwendigen Handlungen bleiben aus.

Warum ist das so?

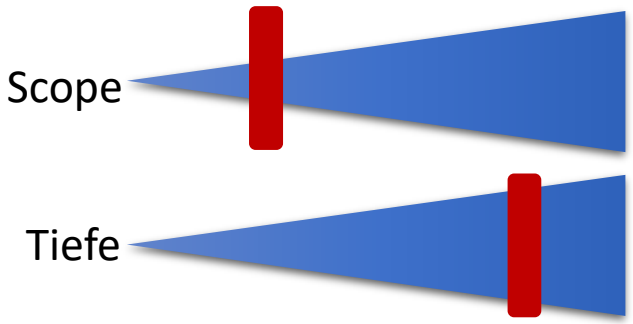
Einordnung



Pentest vs. Bug Bounty

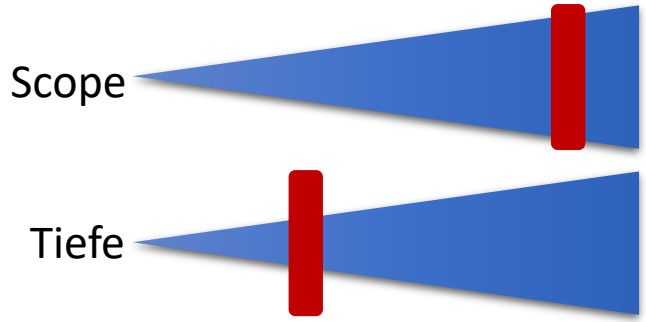
Nutzung herkömlicher und neuer Werkzeuge…

Pentest – Klassiker



→ Punktuelle Identifikation und Elimination von Schwachstellen
→ Analyse in der Tiefe

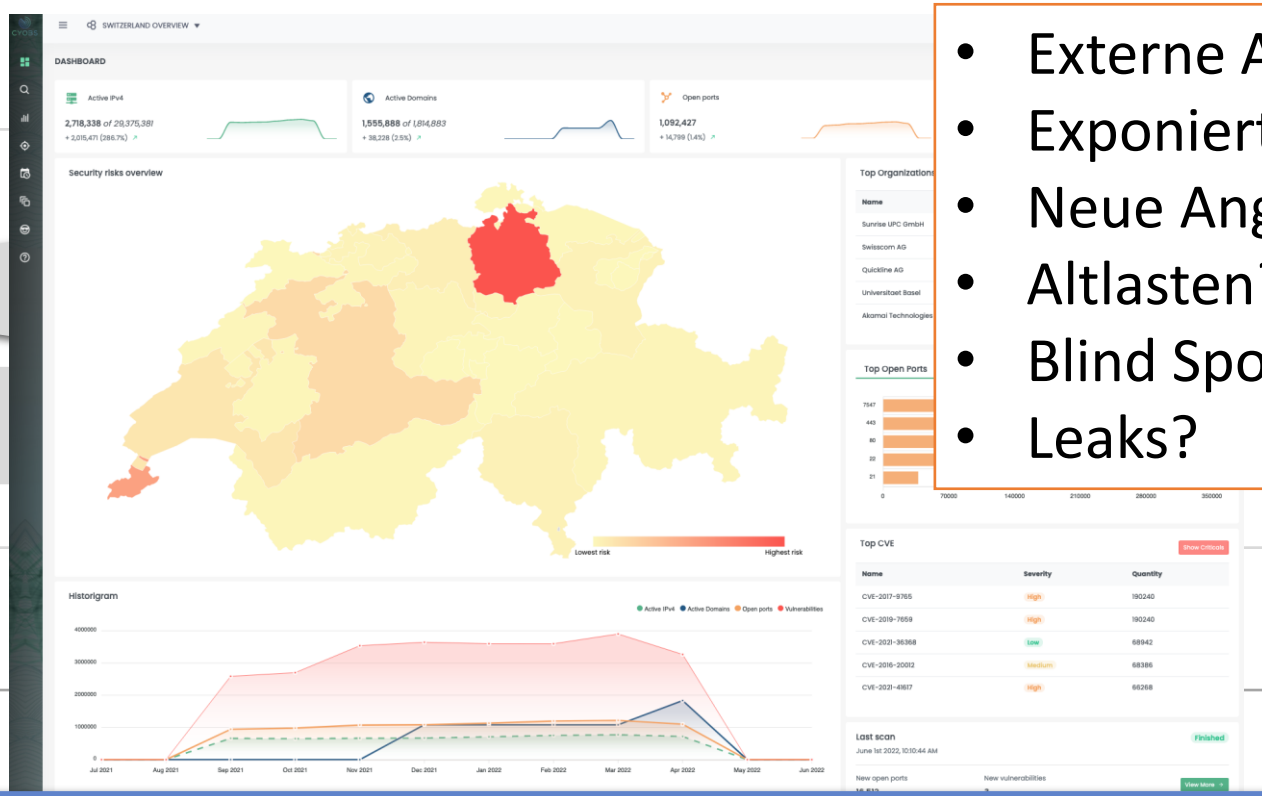
Bug Bounty – Zunehmende Adoption Rate



Kronjuwelen

- Trading Platform
- E-Banking
- Open APIs
- Core Banking
- Kundendaten

Bild vervollständigen: IT-Landscape-Gesamtsicht



Pentest – Klassiker

Scope

Tiefe

- Externe Angriffsfläche?
- Exponierte Assets?
- Neue Angriffspunkte?
- Altlasten?
- Blind Spots?
- Leaks?

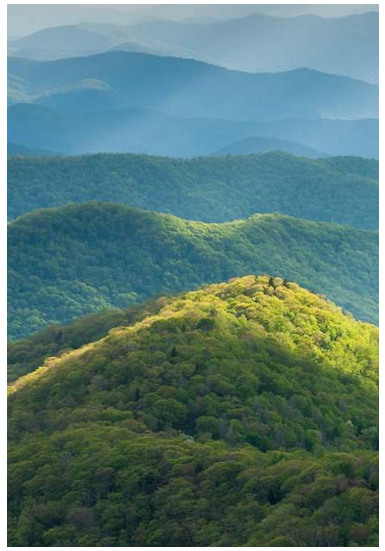
Trading P

e Banking

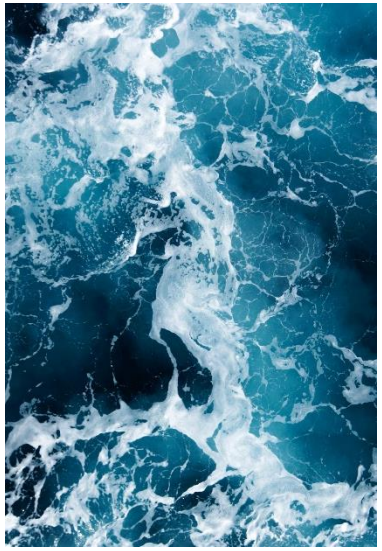
→ Es braucht eine **holistische Sicht** auf Cybersecurity

Vier Dimensionen

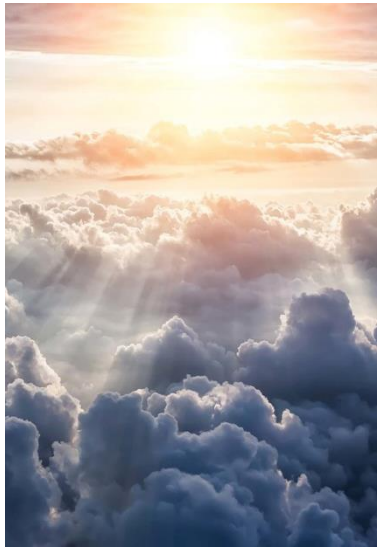
Land



Wasser



Luft



All

37

Cyber: Die alles durchdringende fünfte Dimension

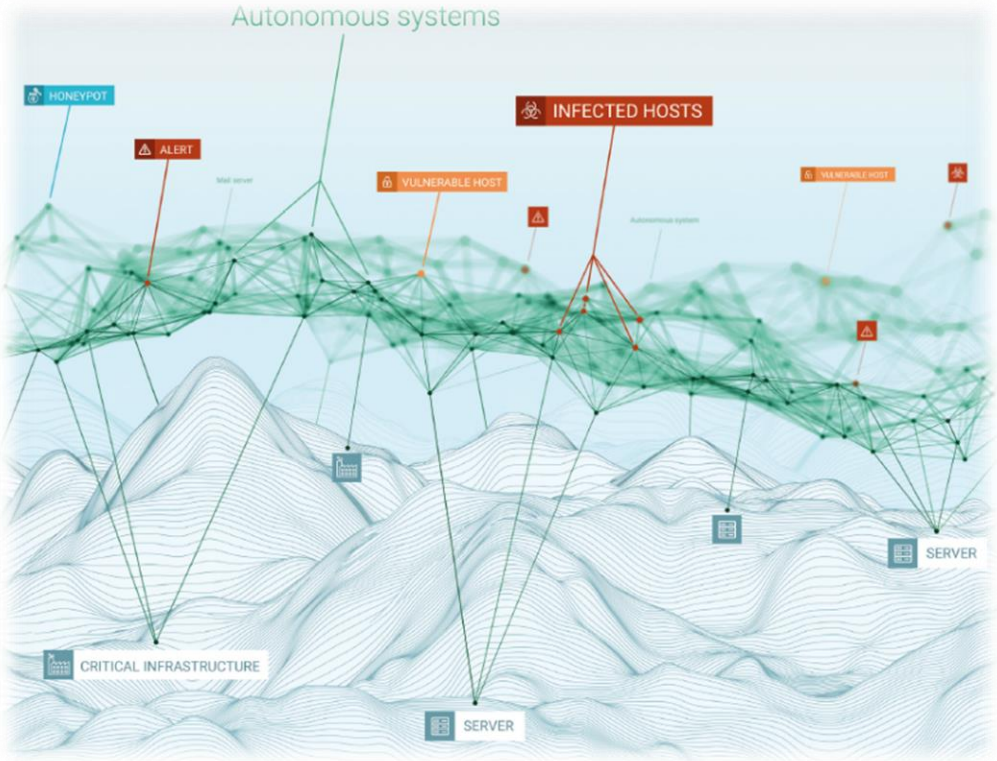
CyObs

CyObs

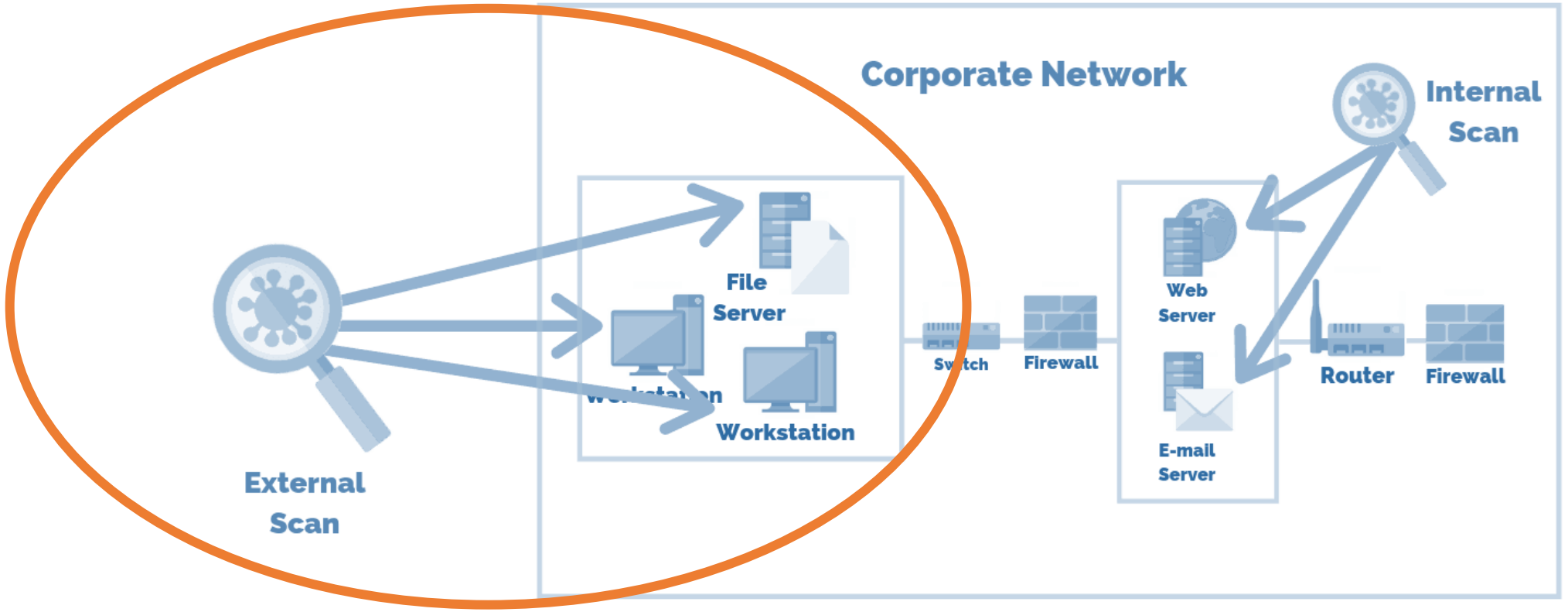
Von Dreamlab Technologies AG entwickelt.

Cyberspace-Radarsystem zur Kartierung, Analyse und Visualisierung des Cyberspace (regional, national und international)

CyObs identifiziert alle Cyberschwachstellen und die potenzielle Angriffsfläche eines Landes oder einer Organisation.

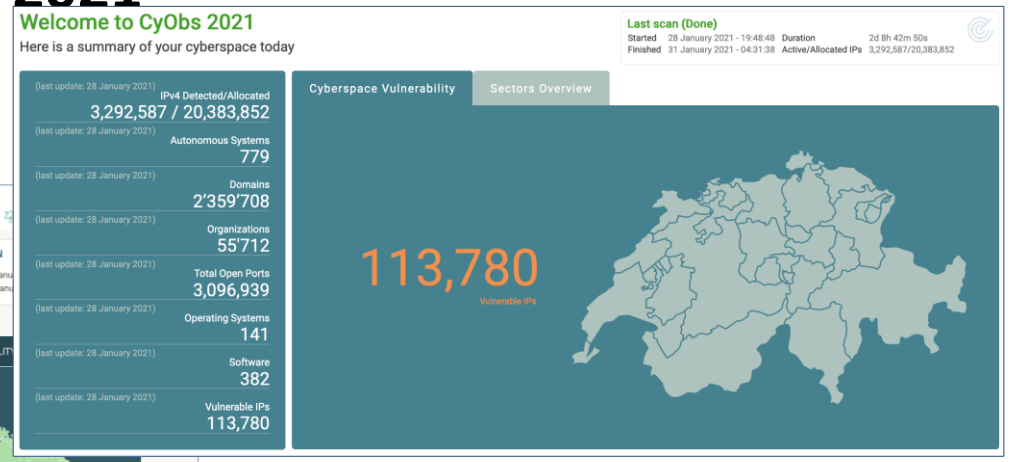


CyObs

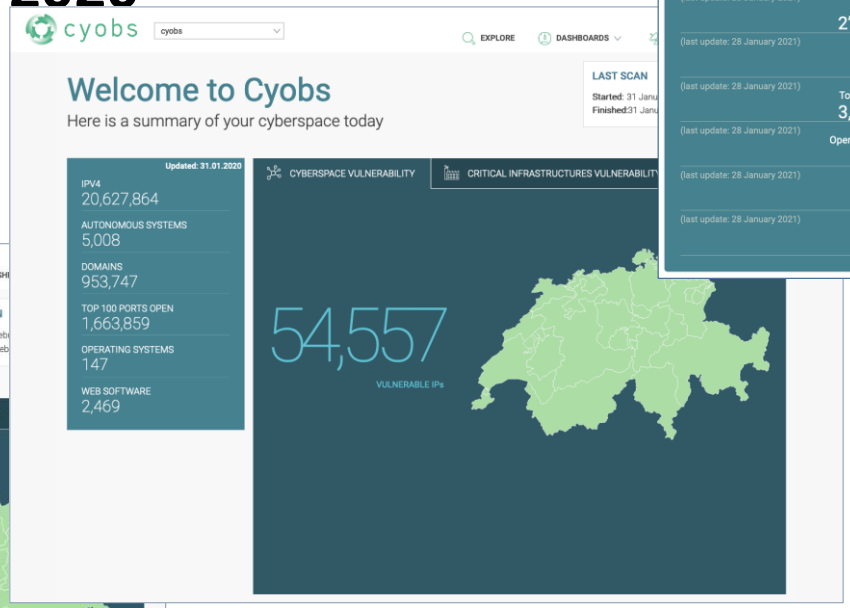

Corporate Network
Internal
Scan
File
Server
Workstation
Switch
Firewall
Web
Server
E-mail
Server
Router
Firewall
External
Scan

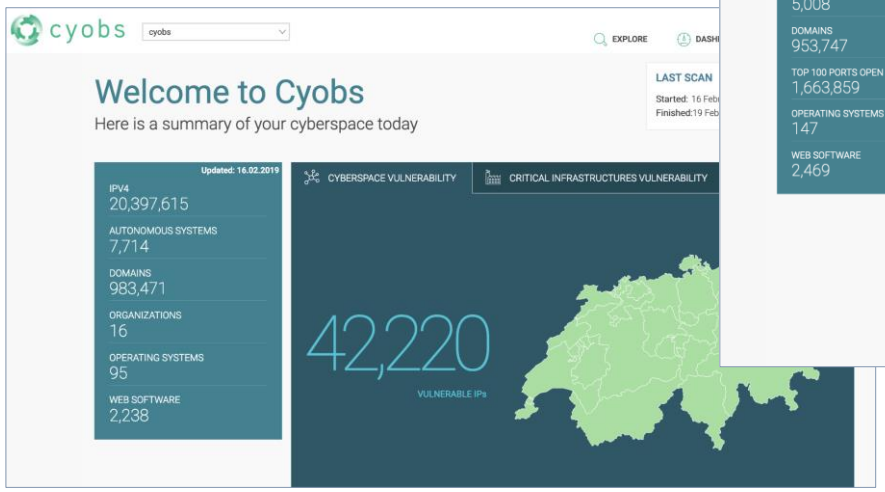
Der Schweizer Cyberspace 2019 bis 2021

2021



2020





Der Schweizer Cyberspace 2022: Stand 2. März

Welcome to CyObs

Here is a summary of your cyberspace today

IPv4 Allocated (last update: 02 February 2022)	24,472,676
Autonomous Systems (last update: 02 February 2022)	790
Domains (last update: 02 February 2022)	2'478'696
Sectors (last update: 02 February 2022)	9
Total Open Ports (last update: 02 February 2022)	2,453,447
Operating Systems (last update: 02 February 2022)	146
Software (last update: 02 February 2022)	1,081
Vulnerable IPs (last update: 02 February 2022)	106,577

Cyberspace Vulnerability | Sectors Overview

106,577

Vulnerable IPs

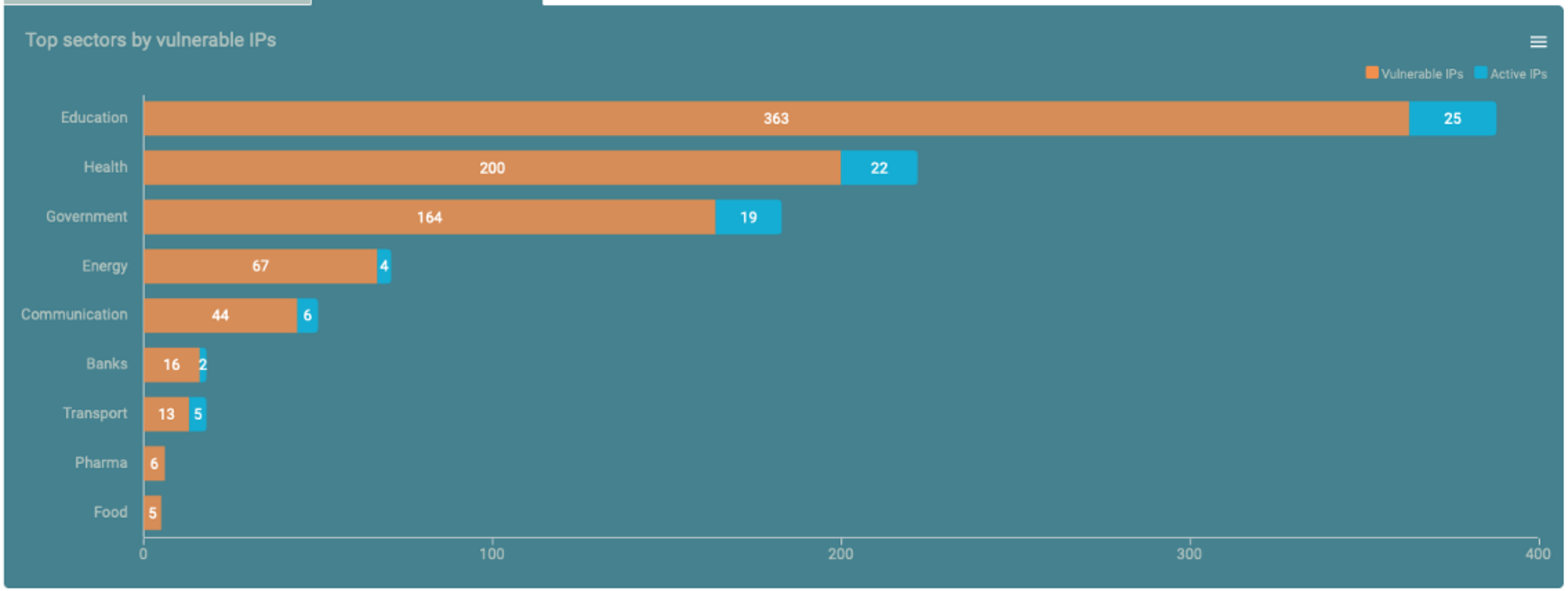
Der Schweizer Cyberspace 2022: Industrie und Sektor

Welcome to CyObs

Here is a summary of your cyberspace today

IPv4 Allocated (last update: 02 February 2022)	24,472,676
Autonomous Systems (last update: 02 February 2022)	790
Domains (last update: 02 February 2022)	2,478,696
Organizations (last update: 02 February 2022)	9
Total Open Ports (last update: 02 February 2022)	2,453,447
Operating Systems (last update: 02 February 2022)	146
Software (last update: 02 February 2022)	1,081
Vulnerable IPs (last update: 02 February 2022)	106,577

Cyberspace Vulnerability | Sectors Overview



Source: Dreamlab Technologies AG, CyObs & Audit Department, 2 March 2022

The Swiss Cyberspace 2022

Overview

Parameter	Results	Description
IPv4 allocated	**24,472,676**	CH IP range
IPv4 detected/active	**2,982,022**	ICMP response + port scan activity
Domains	**2,478,696**	#domains analysed
Domains using DNSSEC	**850,884**	#domains using DNSSEC
Autonomous Systems	**790**	Total active AS in CH
Total Open Ports	**2'453'447**	Cumulative number of open ports
Operating Systems	**146**	Distinct Operating Systems
Unique Software	**1081**	Distinct Software
Vulnerable IPs	**106,577**	Potentially vulnerable IPs

Source: Dreamlab Technologies AG, CyObs & Audit Department, 2 March 2022

The Swiss Cyberspace 2022

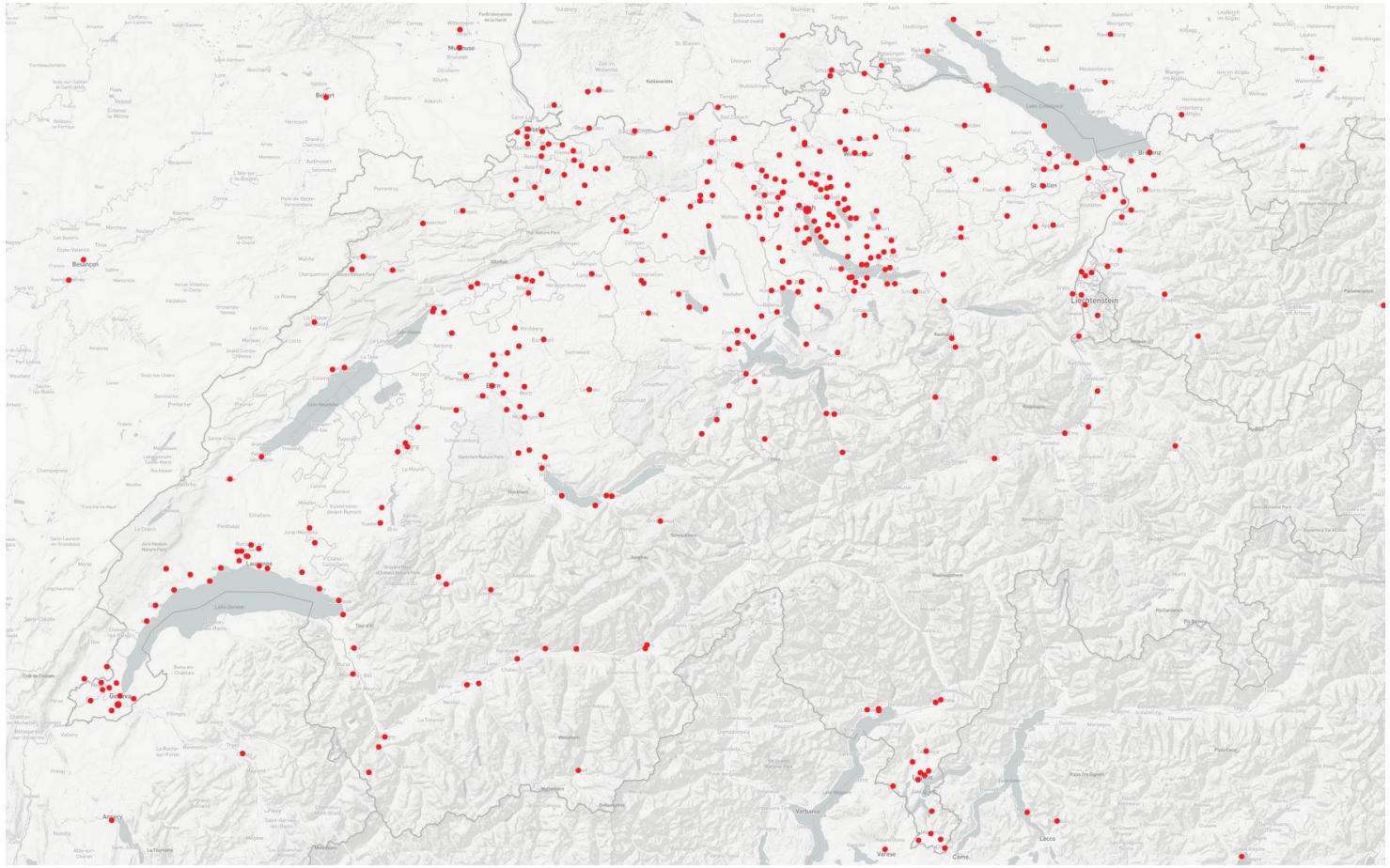
DNS & Mail Server Analysis

Scope	Results (Feb/March 2022)	Description
.ch	2,478,696	# domains analysed
.ch	850,884	# domains using DNSSEC
.ch	2,224,023	# domains with nameserver
.ch	62,493	# DNS server hostnames
.ch	38,134	# DNS server IPs
.ch	1,666,470	# domains with MX (mail servers)
.ch	738,007	# Mail server hostnames
.ch	66,762	# Mail server IPs

Source: Dreamlab Technologies AG, CyObs & Audit Department, 2 March 2022

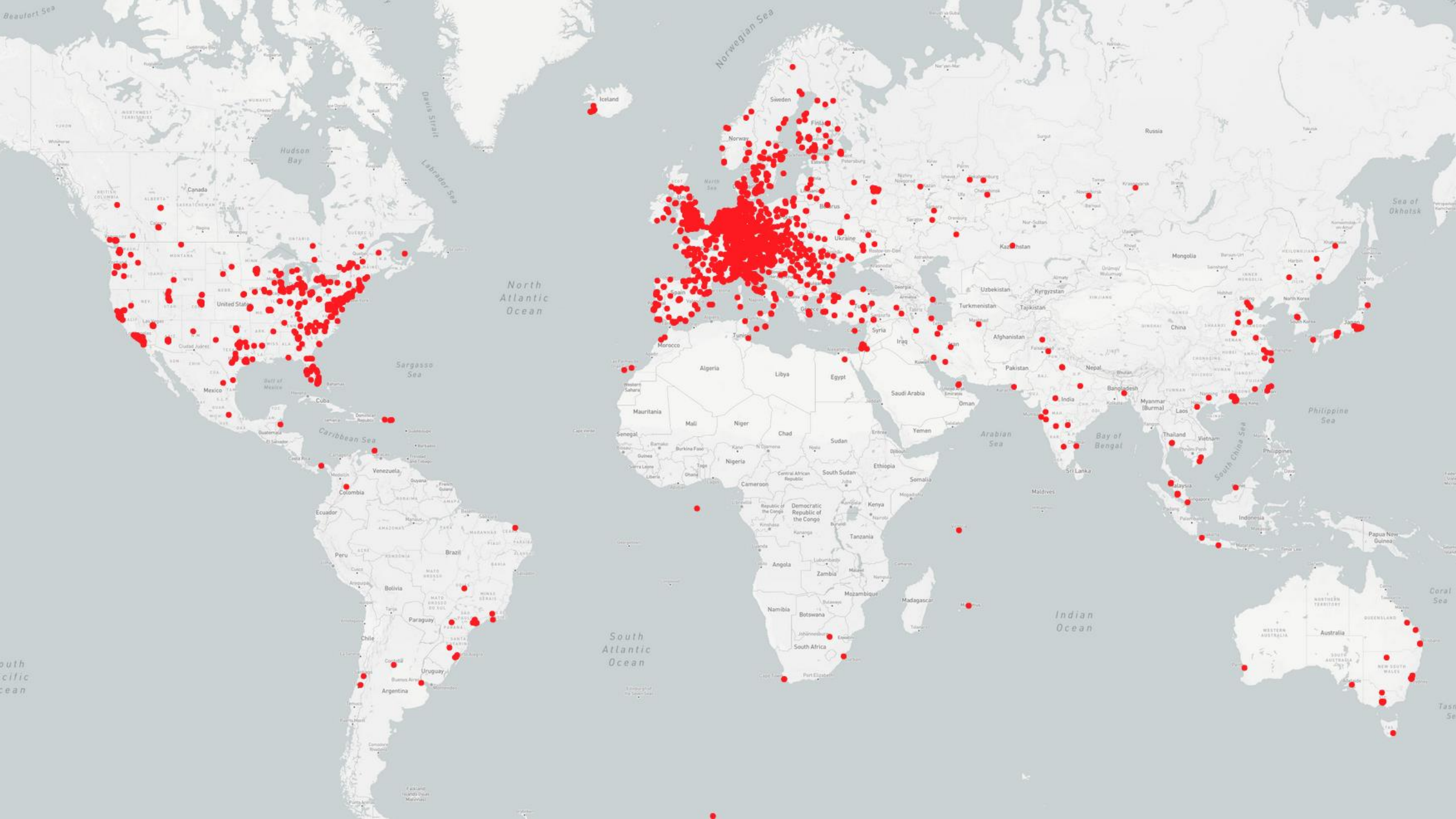
The Swiss Cyberspace 2022

.ch DNS Server Distribution



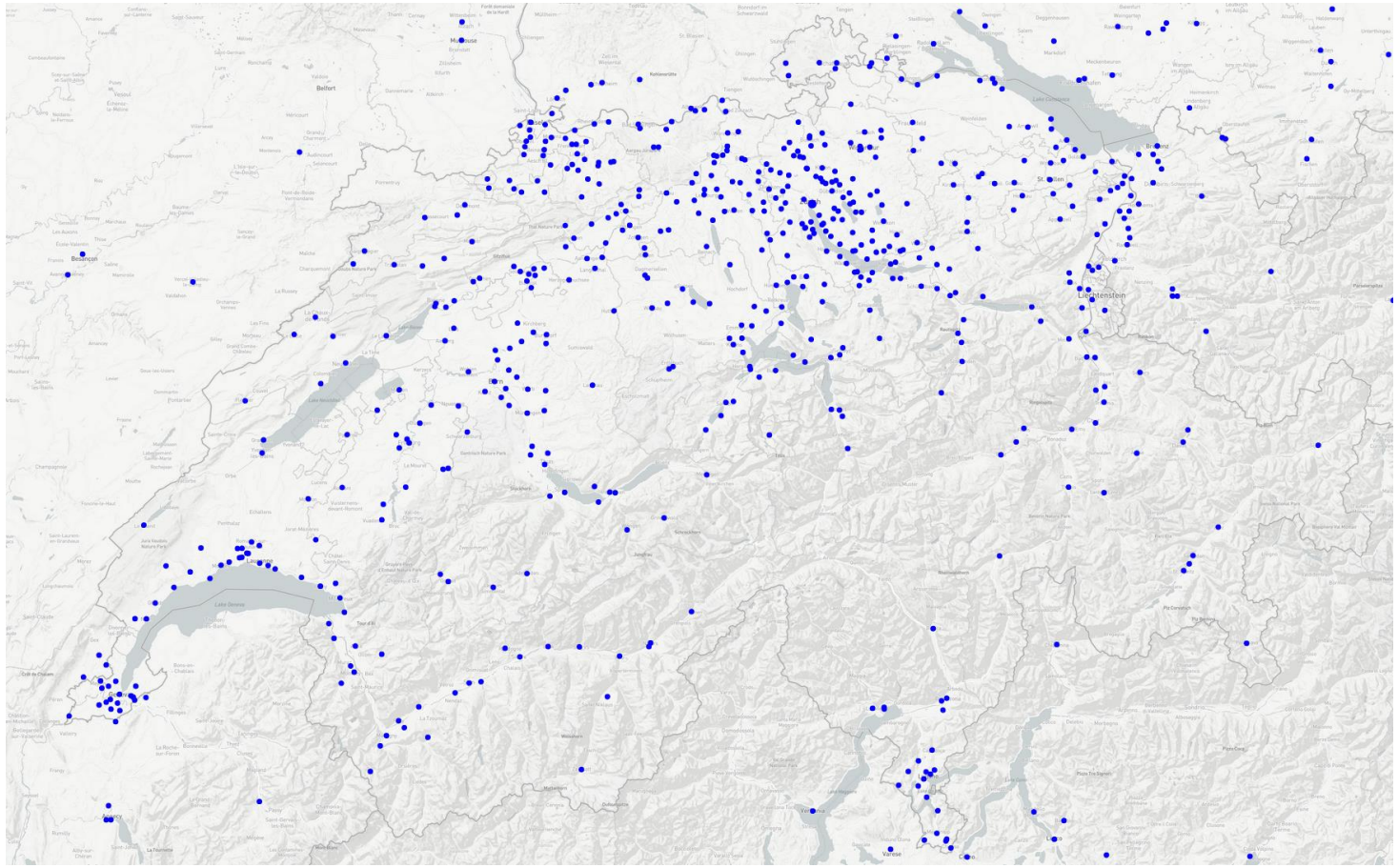
Source: Dreamlab Technologies AG, CyObs & Audit Department, 2 March 2022


North Sea
Baltic Sea
Denmark
Estonia
Latvia
Lithuania
Belarus
United Kingdom
Ireland
Irish Sea
English Channel
Poland
Germany
Czechia
Ukraine
France
Austria
Hungary
Moldova
Romania
Croatia
Bay of Biscay
Serbia
Bosnia and Herzegovina
Montenegro
Kosovo
Bulgaria
North Macedonia
Albania
Italy
Adriatic Sea
Black Sea
Spain
Andorra
Monaco
San Marino

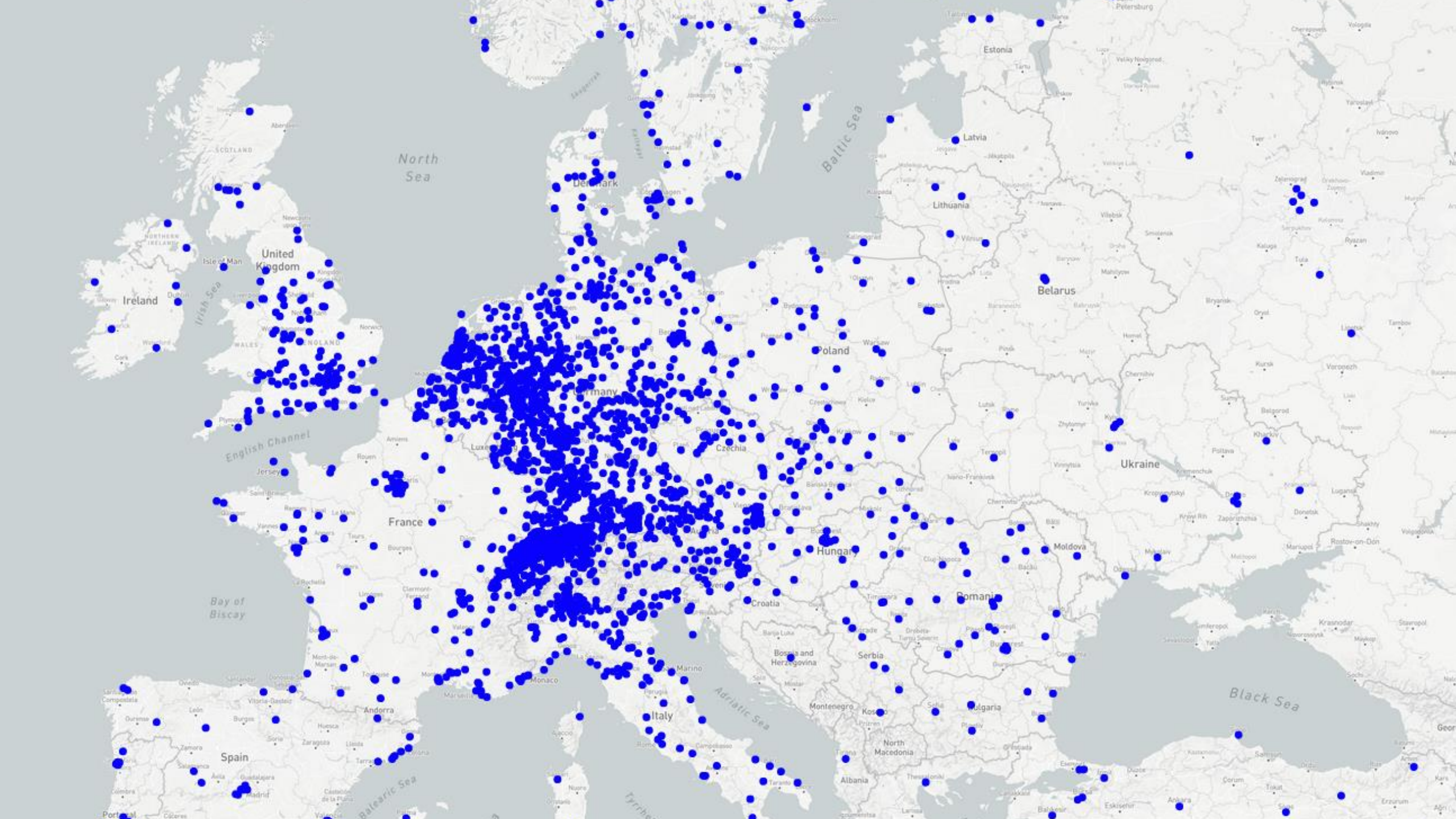

Beaufort Sea
Hudson Bay
Davis Strait
Labrador Sea
Norwegian Sea
Iceland
Sweden
Finland
Norway
Russia
Canada
United States
Mexico
North Atlantic Ocean
Sargasso Sea
Gulf of Mexico
Cuba
Caribbean Sea
Venezuela
Colombia
Ecuador
Peru
Brazil
Bolivia
Paraguay
Chile
Uruguay
Argentina
South Atlantic Ocean
Ireland
Spain
Morocco
Algeria
Libya
Egypt
Mauritania
Mali
Niger
Chad
Sudan
Nigeria
Cameroon
South Sudan
Ethiopia
Somalia
Kenya
Tanzania
Angola
Zambia
Mozambique
Namibia
Botswana
South Africa
Madagascar
Ukraine
Belarus
Kazakhstan
Uzbekistan
Turkmenistan
Kyrgyzstan
Tajikistan
Afghanistan
Pakistan
Iran
Iraq
Syria
Saudi Arabia
Yemen
Oman
India
Nepal
Bangladesh
Myanmar (Burma)
China
Mongolia
North Korea
South Korea
Japan
Sea of Okhotsk
Philippine Sea
Arabian Sea
Bay of Bengal
Sri Lanka
Maldives
Thailand
Laos
Vietnam
Philippines
South China Sea
Malaysia
Indonesia
Papua New Guinea
Coral Sea
Indian Ocean
Australia
Western Australia
Northern Territory
Queensland
South Australia
New South Wales

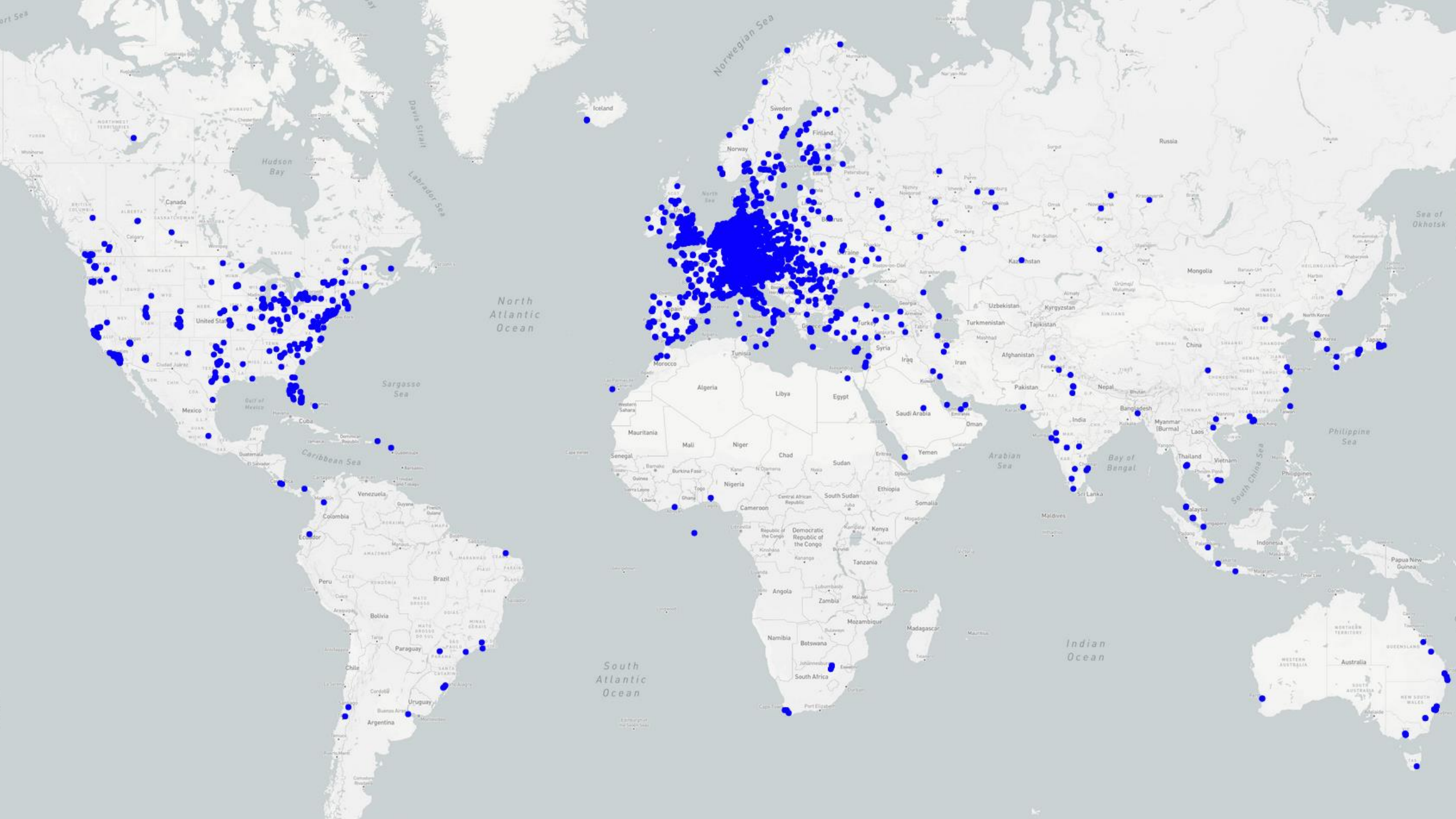
The Swiss Cyberspace 2022

.ch Mail Server Distribution



Source: Dreamlab Technologies AG, CyObs & Audit Department, 2 March 2022


North Sea
Baltic Sea
Ireland
United Kingdom
Irish Sea
English Channel
Bay of Biscay
France
Spain
Andorra
Monaco
Italy
Adriatic Sea
Balearic Sea
Tyrrhenian Sea
Germany
Czechia
Poland
Belarus
Ukraine
Moldova
Romania
Hungary
Croatia
Bosnia and Herzegovina
Serbia
Montenegro
North Macedonia
Albania
Bulgaria
Black Sea
Lithuania
Latvia
Estonia
Denmark


Norwegian Sea
Iceland
Sweden
Finland
Norway
Russia
Davis Strait
Labrador Sea
Hudson Bay
Canada
North Atlantic Ocean
Sea of Okhotsk
Mongolia
Kazakhstan
Uzbekistan
Kyrgyzstan
Tajikistan
Turkmenistan
Afghanistan
China
Pakistan
India
Nepal
Bangladesh
Myanmar (Burma)
Laos
Thailand
Vietnam
Philippines
Philippine Sea
South China Sea
Bay of Bengal
Arabian Sea
Sri Lanka
Maldives
Indonesia
Malaysia
Papua New Guinea
Australia
Indian Ocean
Sargasso Sea
Gulf of Mexico
Mexico
Cuba
Caribbean Sea
Venezuela
Colombia
Ecuador
Peru
Brazil
Bolivia
Paraguay
Chile
Uruguay
Argentina
South Atlantic Ocean
Morocco
Algeria
Tunisia
Libya
Egypt
Mauritania
Mali
Niger
Chad
Sudan
Nigeria
Cameroon
Ethiopia
Somalia
Kenya
South Sudan
Democratic Republic of the Congo
Tanzania
Angola
Zambia
Mozambique
Namibia
Botswana
South Africa
Madagascar
Saudi Arabia
Yemen
Oman
Iraq
Iran
Syria
Turkey
Belarus
Ukraine

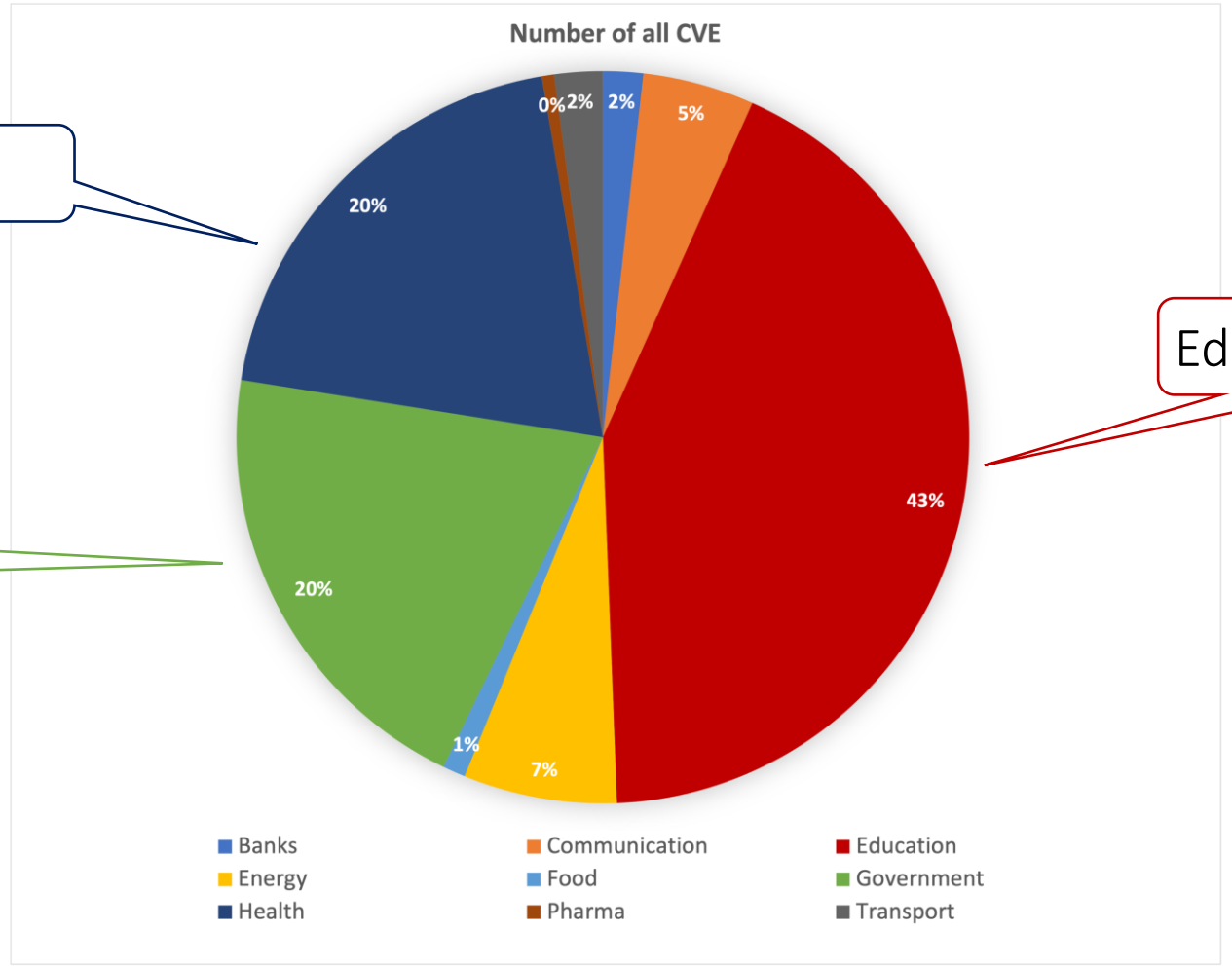
Der Schweizer Cyberspace 2022: Sicherheitslücken

Health

9,726

Government

9,979



Education

20,949

53

Source: Dreamlab Technologies AG, CyObs & Audit Department, 2 March 2022

Fachkräftemangel

Fachkräftemangel im ICT-Bereich

Drastische Folgen für die Schweizer Wirtschaft

Kumulierter wirtschaftliche Schaden durch den Fachkräftemangel allein bis 2025 rund 60 Milliarden Franken.

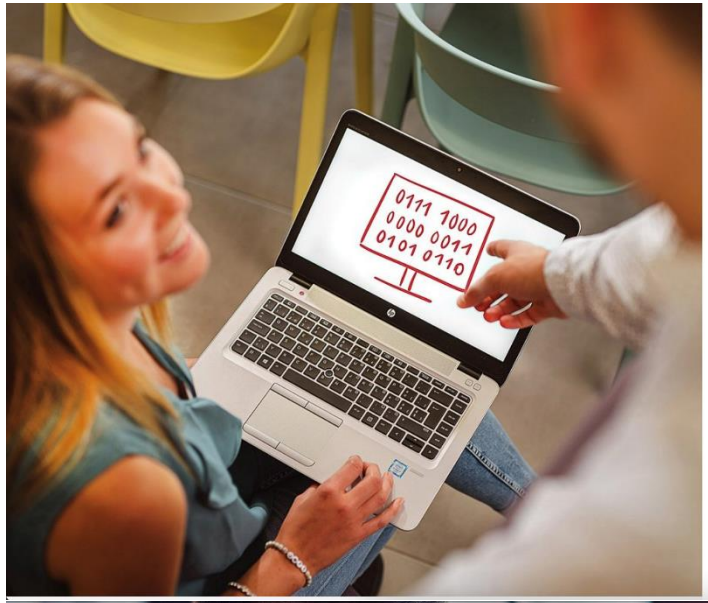
Informatikberufe auf Platz 2 im Fachkräftemangel-Index.

Besonders problematisch ist der Mangel in der Cybersecurity.

Bislang kaum Ausbildungsmöglichkeiten am Markt.

Der Schweiz fehlen im ICT-Bereich bis 2030 fast 40'000 Fachpersonen.

Endlich kommt Bewegung in den Markt



Neuer Bachelor Cyber Security

Der neue Bachelor Cyber Security vermittelt alle Grundlagen, um Programme, Netzwerke und Informationen sicher zu halten und vor Hacker-Angriffen zu schützen.

Mehr erfahren →

CAS Cyber Security

Ein umfassender Blick auf das Thema Cyber-Security auf technischer und auf organisatorischer Ebene ist heute unverzichtbar. Dieses CAS bietet einen soliden Einstieg in die Thematik, ohne tiefe technische Kenntnisse vorauszusetzen. Diese werden im Lauf des Kurses vermittelt und anhand von Fallbeispielen angewendet.

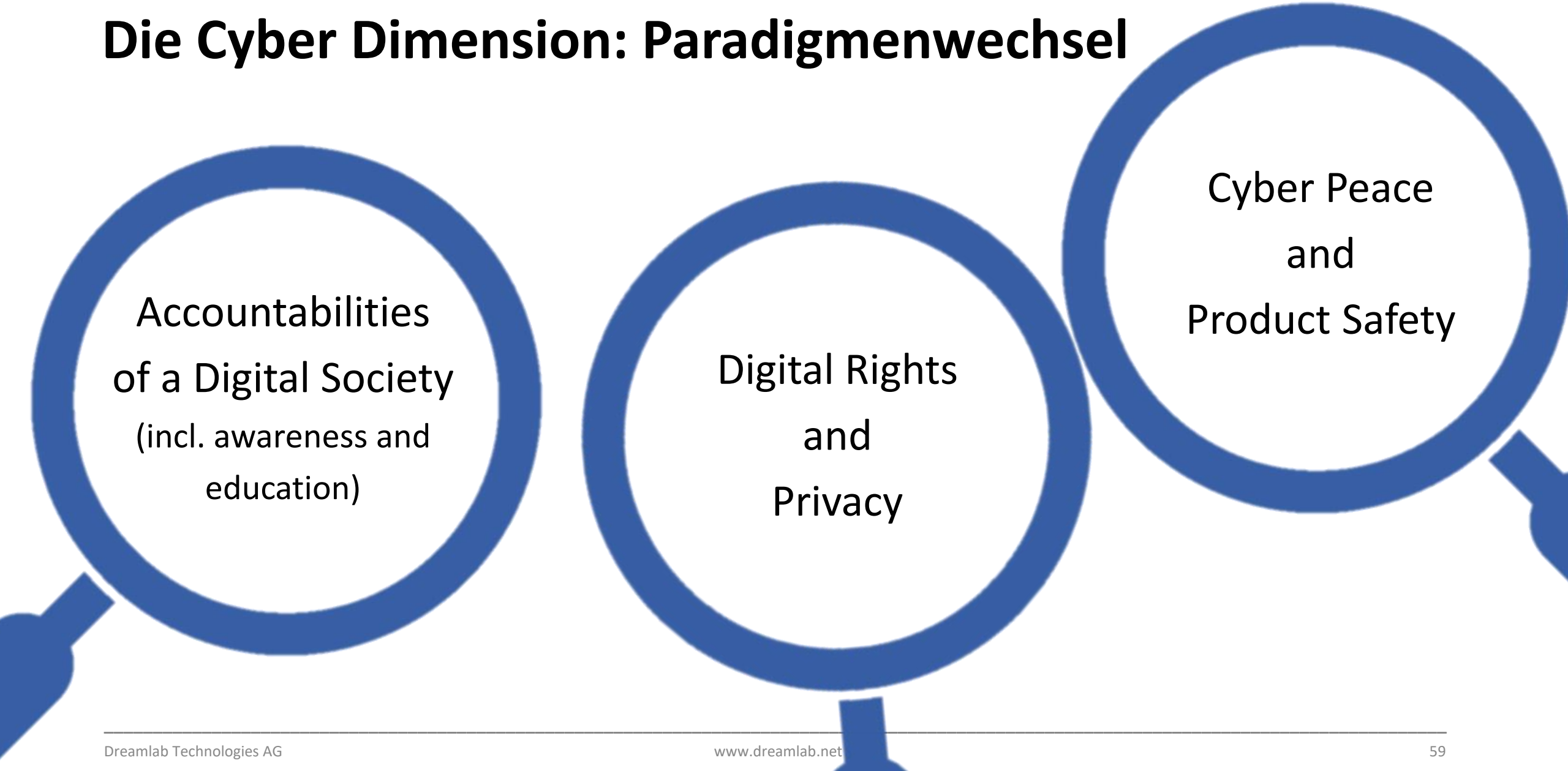
Cyber Security Specialist mit eidg. Fachausweis


STOP
DREAMLAB
TECHNOLOGIES
BEING
NAÏVE

“If you fail to prepare, you’re prepared to fail.”

Mark Spitz, 9-facher Olympiasieger

Die Cyber Dimension: Paradigmenwechsel



Für KMU und Interessierte

cybercheck.dreamlab.net

Beobachter & Dreamlab Cybercheck

Beobachter

DREAMLAB TECHNOLOGIES
Nicht glauben. Wissen.

Beobachter

IT-SICHERHEIT KMU-SELBSTTEST

Bericht: Auswertung und Handlungsempfehlungen

Besten Dank für das Ausfüllen des Cybersecurity-Selbsttests am 31.01.2022! Nachfolgend finden Sie Ihre Ergebnisse sowie die Möglichkeit umgehend weitere Schritte einzuleiten, um die IT-Sicherheit Ihres Unternehmens zu stärken.

Die Ergebnisse basieren ausschliesslich auf den von Ihnen während des Selbsttests getätigten Angaben. Dreamlab Technologies hat hierzu keine weiteren Analysen durchgeführt. Aufgezeigte Stärken und Schwächen Ihrer IT-Sicherheit sollten in jedem Fall fachmännisch nachgeprüft werden.

AUSWERTUNG UND ÜBERBLICK

Im folgenden Diagramm sind die Ergebnisse Ihrer Antworten zusammengefasst. Es zeigt auf, in welchen Bereichen Ihr Unternehmen gut aufgestellt ist und wo allenfalls Nachholbedarf besteht. Dabei gilt: Je weiter hinaus die jeweilige Dimension gefüllt ist, desto besser das Ergebnis.

HANDLUNGSEMPFEHLUNGEN FÜR IHR UNTERNEHMEN

Aufgrund Ihrer Antworten ergeben sich folgende zusätzliche Handlungsempfehlungen.

NETZWERKÜBERSICHT

Eine Netzwerkübersicht oder ein Zonenplan ist eine wichtige Grundlage, damit Ihre IT- Infrastruktur ausreichend geschützt ist. Deshalb sollten Sie eine solche Übersicht erstellen bzw. erstellen lassen und aktuell halten.

ANTIVIREN

Häufige und regelmässige Antivirenscans helfen, Schadsoftware zu erkennen und unschädlich zu machen. Es lohnt sich, mindestens wöchentliche Scans durchzuführen – auch der Server.

BACK-UP

Einer der Hauptzwecke von Back-ups ist die Wiederherstellung von Daten, zum Beispiel nach einem Befall durch Ransomware. Daher ist die Erstellung regelmässiger Back-ups essenziell. Entscheidend ist – gerade im Fall einer Ransomware –, dass Back-ups physisch vom Netzwerk getrennt aufbewahrt werden, da sie sonst möglicherweise ebenfalls befallen und somit unbrauchbar gemacht werden.

DURCHFÜHRUNG VON SENSIBILISIERUNGSMASSNAHMEN

Mitarbeitende sollen immer wieder über aktuelle Bedrohungen und Entwicklungen informiert und sensibilisiert werden. Je regelmässiger und professioneller dies geschieht, desto höher die Chance, dass Mitarbeitende im Ernstfall die richtigen Entscheidungen treffen und Schlimmeres verhindern können. Schulen Sie Ihre Mitarbeitenden mindestens einmal jährlich bezüglich IT-Sicherheit und gestalten Sie die Schulungen so, dass sie einen bleibenden Eindruck hinterlassen.

IMPLIKATIONEN DER NEUEN EU-DATENSCHUTZGRUNDVERORDNUNG

Am 25. Mai 2018 ist die Europäische Datenschutzgrundverordnung (DSGVO) in Kraft getreten. Diese sieht bei Versäumnissen, die zu Datenpannen führen, hohe Strafen vor. Sofern Sie Personendaten von EU-Bürgerinnen verarbeiten, unterstehen Sie automatisch der DSGVO. Obwohl die Durchsetzung in der Schweiz von Fall zu Fall sehr unterschiedlich geschieht, sollten Sie die Auswirkungen der DSGVO auf Ihr Unternehmen und den Handlungsbedarf rechtzeitig abklären. Dies umso mehr, da auch das Schweizer Datenschutzgesetz (DSG), das aktuell überarbeitet wird, sich voraussichtlich stark an die DSGVO anlehnen wird.

OFFENE FRAGEN

Hier sind alle Fragen aufgeli
ausgelassen oder nicht bea
haben. Es empfiehlt sich s
Fragen nachzugehen und
Informationen einzuholen
sind sicherheitsrelevant!

*Gibt es in Ihrem Unterneh
welche die Verwendung
Diensten (zum Beispiel
OneDrive) regeln?*

*Werden E-Mails Ihres U
einem Verschlüsselung
Beispiel PGP) versend*

VERHALTEN BEI SICHERHEITSRELEVANTEN VORKOMMNISSEN

Klare Wege und Ansprechpartner sind bei Sicherheitsvorkommnissen immens wichtig. Stellen Sie sicher, dass Ihre Mitarbeitenden jederzeit im Bild sind, an wen sie sich für IT-Sicherheitsfragen wenden sollen und wie sie dies konkret tun können.

SCHUTZBEDARFSANALYSE

Damit Sie sich vor Cyberbedrohungen schützen, im Ernstfall reagieren und einen kühlen Kopf bewahren können, müssen Sie wissen, welche Informationen und Systeme geschäftskritisch sind und noch stärker als andere geschützt werden müssen. Identifizieren Sie im Rahmen einer Schutzbedarfsanalyse, ausgehend von Ihren Geschäftsprozessen, die relevanten, besonders kritischen Informationen und Systeme und dokumentieren Sie diese.

UMGANG MIT IT-SICHERHEITSRISIKEN UND -BEDROHUNGEN

IT-Sicherheitsrisiken sind Geschäftsrisiken. Die Verantwortung für IT-Sicherheit im Unternehmen obliegt somit letztlich dem Management bzw. dem Verwaltungsrat, welcher nach Schweizer Obligationenrecht eine Sorgfaltspflicht wahrzunehmen hat. Integrieren Sie das Thema IT-Sicherheit bzw. die Risiken, die sich aus IT-Sicherheitsbedrohungen ergeben in geeigneter Form in Ihr Gesamt- Risikomanagement und behandeln Sie es gleichwertig wie andere essenzielle Risiken.

IT-SICHERHEIT ALS INTEGRALER BESTANDTEIL VON PROJEKTEN

IT- Sicherheitsrisiken können zu existenziellen Bedrohungen für Projekte werden. Es reicht weder aus, zu Projektbeginn ein Sicherheitskonzept zu erstellen und dann in der Schublade verschwinden zu lassen, noch am Projektende ein paar Sicherheitsmassnahmen zu definieren, welche nachträglich umgesetzt werden sollen, da zu diesem Zeitpunkt sowieso bereits alle wichtigen Entscheide gefällt wurden und gravierende Mängel nicht mehr behoben werden können.
Wir empfehlen, IT-Sicherheit zu einem integralen Projektbestandteil zu machen, welcher im Projektverlauf genau wie alle anderen Projekt- und Betriebsrisiken laufend bewirtschaftet und behandelt wird.

DREAMLAB TECHNOLOGIES
Nicht glauben. Wissen.

KONTAKTINFORMATIONEN

Für Rückfragen und weitere Auskünfte, kontaktieren Sie bitte Dreamlab Technologies unter 031 398 66 66 oder via E-Mail an cybercheck@dreamlab.net.

Der kostenlose Selbsttest zur Bestimmung der IT-Sicherheit – mit Handlungsempfehlungen – wurde vom Berner IT-Sicherheitsunternehmen Dreamlab Technologies entwickelt.

Weitere Informationen:
www.dreamlab.net
www.it-sicherheit.ch

Autoren:

Jacek Jonczy, Leiter IT-Sicherheitsaudits bei Dreamlab Technologies.
Nicolas Mayencourt, Gründer und CEO von Dreamlab Technologies.
Mischa Obrecht, Projektleiter und Berater bei Dreamlab Technologies.
Marc K. Peter, Prof.


thank
you

FFHS
Fernfachhochschule Schweiz
Mitglied der SUPSI

Diskussionsrunde

FFHS
Fernfachhochschule Schweiz
Mitglied der SUPSI

Vielen Dank für Ihre Mitwirkung.

Weiterführende Informationen und die passenden Bildungsangebote erhalten Sie bei unseren ExpertInnen vor Ort oder unter www.ffhs.ch

BSc Cyber Security

Wenden Sie Cyber-Angriffe ab, finden Sie Sicherheitslücken, versetzen Sie sich in die Angreifer hinein, um ihnen einen Schritt voraus zu sein. Werden Sie zum IT-Security-Profi!

Ethical Hacking, Schützen, Reagieren. Für Security Spezialisten.