muster.de

01.06.2021

Mustermann, Max

Note

cysmo® rates the security of a company's IT infrastructure that is visible from the outside. The publicly accessible online systems of the company are examined and rated. The rating is based on security criteria checked by cysmo®, which are derived from technical recommendations and industry standards such as the ones issued by the BSI or the VdS. The rating does not contain any organisational elements. The rating represents a snapshot of the current attack liability of the IT infrastructure. The attack situation and thus the attack liability can, however, change at any given moment. cysmo® does not pose a complete risk assessment of cyber attacks but it shows the attack liability of the IT from a cyber criminal's perspective. The performance of a cysmo® rating is thus to be considered one part of a comprehensive risk analysis that assesses the cyber risks of your company in their entirety.

Legend

Explanation of the symbols and abbreviations used

	**Timeout**	A timeout occurred during the data collection. As not all scores could be completed, there may be deviations in the rating result.
	**Risk highlighting**	Based on the answered risk questions, some scores have gained in relevance from a sales perspective and are, thus, highlighted.

Findings/rating-related messages:

	**Catastrophic**	An IT security incident could already have occurred.
	**Critical**	Deviations from standards or best practices detected - acute threat
	**Warning**	Deviations from standards or best practices detected - no acute threat
	**Positive**	No deviations from standards or best practices detected
	**Neutral**	Purely informative, no impact on the result

Abbreviations:

-NV-: Not available / No value could be determined.

SRV: Server

Management Summary

The Management Summary provides an overview of findings with the classification critical and warning. From an IT security perspective, these findings represent a potential threat. Each finding is described with easy-to-understand explanations, potential damage scenarios and recommendations. Detailed technical information can be found in the remaining report.

Attack Resilience

Internal Systems

Hostnames that indicate internal systems were found.

Technical explanation

Externally visible, potentially internal systems have been identified. They present an attractive target for attackers.

Potential risk

Depending on the services linked to the internal systems (e.g. e-mail clients, employee portals, development systems or test systems), attackers can gain access and cause damage. In addition, these systems are often much worse protected because they are assumed not to be visible to the outside world.

Recommended actions

If possible, the affected systems should not be visible externally.

Technical details

Technical details can be found in section "Attack Resilience - Internal Systems" in table "Internal Systems".

Darknet

Leak Age

At least one leak was found that occurred less than 1,000 days ago.

Technical explanation

E-mail addresses and possibly the corresponding passwords have been published on the darknet. The leaks are less than 1,000 days old.

Potential risk

E-mail addresses and corresponding passwords published on the darknet provide attackers with a basis for downstream attacks, e.g. spear phishing attacks or credential stuffing (attempting to login to other services using the data).

Recommended actions

It should be ensured that passwords are changed regularly and that employees are encouraged not to use their work e-mail address private contexts. Employees should also be advised to use a password manager.

Technical details

Technical details can be found in section "Darknet - Leak Age" in table "Leaks".

cysmo

cysmo® Technical Report

created on **01.06.2021**

Overview

Domains:

muster.de

B Rating 81%

To a large extent, the company meets the currently required minimum IT security criteria evaluated by cysmo® that are visible externally (online). No substantial security gaps were detected.

Risk questions

Do you store credit card data?

n/a

What is the share of your online turnover (e-commerce)?

n/a

How dependent is your business (turnover) on the online availability of your systems connected to the web presence (domain)?

n/a

How dependent is your operational business on the communication via e-mail?

n/a

1 Attack Resilience 97%

⚠ 1

1.1	Hostnames	100%
1.2	Internal Systems ⚠	30%
1.3	Open Ports	100%
1.4	Application Management	100%
1.5	Back-End Logins	100%
1.6	Malicious Activities	100%

2 DDoS Stability 45%

⚠ 2

2.1	DNS DDoS ⚠	35%
2.2	Mail DDoS	100%
2.3	Web DDoS ⚠	0%

3 DNS Config 88%

⚠ 1

3.1	Administrative Security ⚠	25%
3.2	Operational Security	100%
3.3	Best Practises	100%

4 Mail Config 85%

⚠ 1

4.1	Mail TLS	100%
4.2	Spoofing Protection ⚠	70%
4.3	Blacklist Reputation	100%

5 Privacy and Reputation 68%

⚠ 2

5.1	Web Server TLS	100%
5.2	Trackers ⚠	33%
5.3	User Security ⚠	55%
5.4	Web Server Reputation	100%
5.5	AS Reputation	100%
5.6	Domain Reputation	100%

6 Darknet 58%

⚠ 3

6.1	Leak Age ⚠	0%
6.2	Credential Stuffing	100%
6.3	Policy Violation ⚠	0%
6.4	Blackmail Threat	100%
6.5	Spear Phishing Threat ⚠	0%

1 Attack Resilience: 97%

The partial rating "Attack Resilience" rates the attack surface of the rated company that is visible externally. A high score is achieved if the number of systems that are visible externally and accessible is as low as possible. For the calculation of the score the criticality of the systems (mail server, web server, DNS server) and the criticality of the accessible services are rated. Non-critical elements are displayed and do not affect the rating. The scores listed here do not make assumptions on the security or configuration of the found systems but give information on the respective settings (e.g. firewall). Note: No active scans or penetrations are executed on the systems or system components.

Illustrative Story

A robbery gang wants to rob a casino and scouts it out in advance. The partial rating "Attack Resilience" focuses on everything that the robbers would be able to detect without even entering the casino.

1.1 Hostnames: 100% *

* This score has a purely informative value for the current rating.
The score does not affect the total rating.

This score shows the hostnames found for the domain(s). The systems associated with these hostnames are the basis for checking many other scores.

Illustrative Story

On the Internet, the robbery gang finds out that the casino also has a hotel, two restaurants and an underground car park. There is also a branch office in Atlanta.

117 hostnames were found.

Table 1.1 – muster.de – Hostnames

No.	Hostname	Role	Resolvable	Available
1	2fa-push.muster.de	SRV	Yes	Yes
2	2fa-test.muster.de	SRV	Yes	Yes
3	2fa.muster.de	SRV	Yes	Yes
4	abnahme-cssp.muster.de	SRV	Yes	Yes

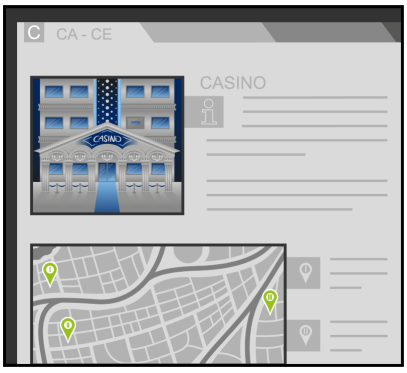
5	adhoc.muster.de	SRV	Yes	Yes
6	artifacts.muster.de	SRV	Yes	Yes
7	auth.muster.de	SRV	Yes	Yes
8	auth04.ns.de.uu.net	DNS	Yes	Yes
9	auth54.ns.de.uu.net	DNS	Yes	Yes
10	autodiscover.muster.de	SRV	Yes	Yes
11	bastian-01.muster.de	SRV	Yes	Yes
12	bastian-02.muster.de	SRV	Yes	Yes
13	bastian.muster.de	SRV	Yes	Yes
14	bd24-abnahme-cssp.muster.de	SRV	No	No
15	bego-rest-sst.muster.de	SRV	Yes	Yes
16	box.muster.de	SRV	Yes	Yes
17	change.muster.de	SRV	Yes	Yes
18	chat.muster.de	SRV	No	No
19	connections.muster.de	SRV	Yes	Yes
20	convo.muster.de	SRV	Yes	Yes
21	correlationmachine.muster.de	SRV	Yes	Yes
22	covid-abnahme.muster.de	SRV	Yes	Yes
23	cpe-dev-testdriver.cpe.muster.d	SRV	Yes	No
24	cpe-kafdrop.cpe.muster.de	SRV	Yes	No
25	cpe-ods.cpe.muster.de	SRV	Yes	No
26	cpe-pds-archive.cpe.muster.de	SRV	Yes	No
27	cpe-pds-collector.cpe.muster.de	SRV	Yes	No
28	cpe-pds-rest.cpe.muster.de	SRV	Yes	No
29	cpe-pds-tracker.cpe.muster.de	SRV	Yes	No
30	cpe.muster.de	SRV	Yes	No
31	crm.muster.de	SRV	Yes	Yes
32	crm2.muster.de	SRV	Yes	Yes
33	cssp-webas.muster.de	SRV	Yes	No
34	cssp.muster.de	SRV	Yes	Yes
35	demo.muster.de	SRV	Yes	Yes
36	deuba.muster.de	SRV	Yes	Yes
37	preview-backend.muster.de	SRV	No	No
38	preview-cockpit.muster.de	SRV	Yes	Yes
39	preview-keycloak.muster.de	SRV	No	No
40	ebics-testbank.muster.de	SRV	Yes	Yes
41	ebics-travic.muster.de	SRV	Yes	Yes
42	emm.muster.de	SRV	Yes	No
43	equus.muster.de	SRV	Yes	Yes
44	fox.muster.de	SRV	Yes	No
45	ftp.muster.de	SRV	Yes	Yes
46	gofit.muster.de	SRV	Yes	Yes
47	hcob.muster.de	SRV	Yes	Yes
48	herbert.muster.de	SRV	Yes	Yes
49	hhvcs-edge.muster.de	SRV	Yes	No
50	hmrv-abnahme-cssp.muster.de	SRV	Yes	Yes
51	inet.muster.de	SRV	Yes	No
52	insurance-experts.muster.de	SRV	Yes	No
53	intranet.muster.de	SRV	Yes	Yes
54	isotest.muster.de	SRV	Yes	Yes

55	jobs.muster.de	SRV	Yes	Yes
56	karriere-live10.muster.de	SRV	Yes	Yes
57	karriere-stage10.muster.de	SRV	Yes	Yes
58	karriere.muster.de	SRV	Yes	Yes
59	kasper.muster.de	SRV	Yes	Yes
60	kibana.cpe.muster.de	SRV	Yes	No
61	kpp.muster.de	SRV	No	No
62	lbr855.muster.de	SRV	Yes	Yes
63	mail.muster.de	SRV	No	No
64	mail1.muster.de	MAIL	Yes	Yes
65	mail2.muster.de	SRV	No	No
66	mail3.muster.de	SRV	No	No
67	mail4.muster.de	MAIL	Yes	Yes
68	mailarchiv.muster.de	SRV	Yes	Yes
69	minio.cpe.muster.de	SRV	Yes	No
70	monitor.muster.de	SRV	Yes	Yes
71	nirvana.muster.de	SRV	Yes	Yes
72	odo.muster.de	SRV	Yes	Yes
73	polarity.muster.de	SRV	Yes	Yes
74	port.muster.de	SRV	No	No
75	portal.muster.de	SRV	Yes	Yes
76	muster.de	SRV	Yes	Yes
77	ppitickets.muster.de	SRV	No	No
78	promato.muster.de	SRV	Yes	Yes
79	push.muster.de	SRV	Yes	Yes
80	secure.muster.de	SRV	Yes	No
81	servicedesk.muster.de	SRV	Yes	Yes
82	showcase-staging.muster.de	SRV	Yes	Yes
83	sisko.muster.de	SRV	Yes	Yes
84	smtp.muster.de	SRV	Yes	Yes
85	smtp2.muster.de	SRV	Yes	Yes
86	smtp3.muster.de	SRV	No	No
87	smtp4.muster.de	SRV	No	No
88	stage-karriere.muster.de	SRV	Yes	Yes
89	static.140.XX.69.XX.clients.your-server.de	SRV	Yes	Yes
90	static.XX.14.XX.144.clients.your-server.de	SRV	Yes	Yes
91	static.20.195.203.116.clients.your-server.de	SRV	Yes	No
92	static.XX.55.47.XXclients.your-server.de	SRV	Yes	Yes
93	static.55.XX.203.XX.clients.your-server.de	SRV	Yes	Yes
94	support.muster.de	SRV	Yes	Yes
95	testlink.muster.de	SRV	Yes	Yes
96	testlink1.muster.de	SRV	Yes	Yes
97	tools.muster.de	SRV	Yes	Yes
98	traveler.muster.de	SRV	Yes	No
99	travic-demo.muster.de	SRV	Yes	Yes
100	travic-dialog.muster.de	SRV	Yes	Yes

101	travic-france.muster.de	SRV	Yes	Yes
102	instant-payments.muster.de	SRV	Yes	Yes
103	travic-schweiz.muster.de	SRV	Yes	Yes
104	travic.muster.de	SRV	Yes	Yes
105	traviclink.muster.de	SRV	Yes	Yes
106	tucker.muster.de	SRV	Yes	No
107	tyr.muster.de	SRV	Yes	Yes
108	umfrage.muster.de	SRV	Yes	Yes
109	upload.muster.de	SRV	Yes	Yes
110	video.muster.de	SRV	Yes	No
111	webrepmonitor.muster.de	SRV	Yes	Yes
112	worf.muster.de	SRV	Yes	Yes
113	www-neu.muster.de	SRV	Yes	Yes
114	www-test.muster.de	SRV	Yes	Yes
115	www.karriere.muster.de	SRV	Yes	Yes
116	www.muster.de	WEB	Yes	Yes
117	zulip.muster.de	SRV	Yes	Yes

1.2 Internal Systems: 30%

This score rates whether there are externally visible, potentially internal systems. The detection is based on their names (e.g intranet, support or monitoring systems, internal servers, development and test systems). Additionally, it is checked whether the systems are online or offline. The fewer potentially internal systems are resolvable and visible externally, the higher the score.



Illustrative Story

In the business directory, the gang finds the addresses of a warehouse and an office building with the headquarters of the administration, registered to the name of the casino. Maybe those internal buildings are not as well secured as the actual casino?

Potential Risk

Depending on the services linked to the internal systems (e.g. e-mail clients, employee portals or development systems, see also the score "Critical Ports"), attackers can gain access and cause damage. In addition, these systems are often insecure because they are assumed not to be visible to the outside world.

Claim (example)

The provider Domain Factory was hacked because of an internal system that was visible and available from outside.

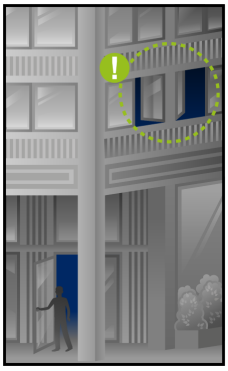
Hostnames that indicate internal systems were found.

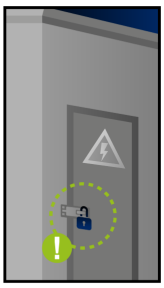
Table 2.1 – muster.de – Internal Systems

No.	Hostname	Role	Resolvable	Available
1	2fa-test.muster.de	SRV	Yes	Yes
2	abnahme-cssp.muster.de	SRV	Yes	Yes
3	autodiscover.muster.de	SRV	Yes	Yes
4	covid-abnahme.muster.de	SRV	Yes	Yes
5	intranet.muster.de	SRV	Yes	Yes
6	stage-karriere.muster.de	SRV	Yes	Yes
7	www-test.muster.de	SRV	Yes	Yes

1.3 Open Ports: 100%

This score rates the ports available from the outside and therefore, the accessible services provided by the found systems. Certain standard ports are indispensable for the use of various services, like external mail and web server communication, and do not affect the rating. Other services might be accidentally exposed to the Internet and might pose a security risk. As a rule, the following applies: the lower the number of these ports, the fewer opportunities there are for attackers and the better can the infrastructure be protected against attackers. Services that should never be accessible from the Internet (e.g. database and file servers) are more important for the assessment than, for example, maintenance accesses. In addition, services on systems that are critical to the operation of the infrastructure are penalised more severely while ports that are necessary for the operation are not taken into account for the assessment.





Illustrative Story

In the office building of the administration, the cleaning staff always leaves two windows slightly open after the work is done in order to air out. The door to the distribution substation, which supplies all casinos in the area with electricity, is also merely secured with a simple lock.

Potential Risk

Attacks on critical ports are frequent and usually fully automated, scoping out the entire Internet for potential targets. When successful, an attacker can cause damages starting with reputation and data loss and oftentimes the takeover of the entire systems.

Claim (example)

In November 2019, a medical practice in the Hannover area lost data of 20,000 patients due to a file server wrongly being accessible from the Internet.

cysmo

No open ports were found on critical systems or for critical services.

Table 3.1 – muster.de – Open Ports

No.	Hostnames	IP	Port	Service	Critical system	Classification	Last seen
1	auth04.ns.de.uu.net	192.XXX.144.17	53/UDP	domain	Yes		2021-05-18
2	auth54.ns.de.uu.net	194.XXX.171.100	53/UDP	domain	Yes		2021-05-15
3	mail4.muster.de, smtp2.muster.de	212.XX.0.113	25/TCP	smtp	Yes		2021-05-23
4	mail1.muster.de, smtp.muster.de	62.XXX.243.118	25/TCP	smtp	Yes		2021-05-28
5	jobs.muster.de, karriere-live10.muster.de, karriere-stage10.muster. de, karriere.muster.de, muster.de,	62.XXX.243.119	80/TCP	http	Yes		2021-05-13
6	jobs.muster.de, karriere-live10.muster.de, karriere-stage10.muster. de, karriere.muster.de, muster.de,	62.XXX.243.119	443/TCP	https	Yes		2021-06-01
7	deuba.muster.de, hcob.muster.de, static.XX.30.XXX.116. clients.your-	116.XXX.30.55	443/TCP	https	No		2021-05-14
8	deuba.muster.de, hcob.muster.de, static.55.30.203.116. clients.your-server.de	116.XXX.30.55	80/TCP	http	No		2021-05-14
9	abnahme-cssp.muster. de, covid-abnahme.muster. de, cssp.muster.de, hmrv-abnahme-cssp. muster.de, static.173.14.XX.144. clients.your-server.de	144.XX.14.173	80		No		2021-05-29
10	abnahme-cssp.muster. de, covid-abnahme.muster. de, cssp.muster.de, hmrv-abnahme-cssp. muster.de, static.173.14.XX.144. clients.your-server.de	144.XX.14.173	443	http	No		2021-05-25

11	static.140.197.XX.159.clients.your-server.de, travic-instant-payments.muster.de	159.XX.197.140	443/TCP	https	No		2021-05-25
12	static.140.197.XX.159.clients.your-server.de, travic-instant-payments.muster.de	159.XX.197.140	80/TCP	http	No		2021-05-13
13	autod.ha-autod.office.com, autod.ms-acdc-autod.office.com, autodiscover.outlook.com, autodiscover.muster.de	40.XX.138.24	80/TCP	http	No		2021-05-13
14	adhoc.muster.de	46.XX.2.57	1194/UDP	openvpn	No		2021-05-14
15	adhoc.muster.de	46.XX.2.57	443/TCP	https	No		2021-05-15
16	autod.ha-autod.office.com, autod.ms-acdc-autod.office.com, autodiscover.outlook.com, autodiscover.muster.de	52.XX.201.24	80/TCP	http	No		2021-05-16
17	autod.ha-autod.office.com, autod.ms-acdc-autod.office.com, autodiscover.outlook.com,	52.XX.152.168	80	http	No		2021-05-22
18	discover.muster.de bastian.muster.de	62.XXX.243.114	80/TCP	http	No		2021-05-24
19	bastian.muster.de	62.XXX.243.114	443/TCP	https	No		2021-05-26
20	bastian.muster.de	62.XXX.243.114	264/TCP	fw1-topology	No		2021-05-17
21	bastian.muster.de	62.XXX.243.114	500/UDP	isakmp	No		2021-05-14
22	bastian-01.muster.de	62.XXX.243.115	443/TCP	https	No		2021-05-26
23	bastian-01.muster.de	62.XXX.243.115	264/TCP	fw1-topology	No		2021-05-16
24	bastian-01.muster.de	62.XXX.243.115	80		No		2021-05-12
25	bastian-01.muster.de	62.XXX.243.115	18264	http (Check Point SVN foundation httpd)	No		2021-05-25
26	bastian-02.muster.de	62.XXX.243.116	443/TCP	https	No		2021-05-12
27	bastian-02.muster.de	62.XXX.243.116	80/TCP	http	No		2021-05-12
28	bastian-02.muster.de	62.XXX.243.116	264/TCP	fw1-topology	No		2021-05-10

29	artifacts.muster.de, crm.muster.de, crm2.muster.de, gofit.muster.de, mailarchiv.muster.de ,... 5 more	62.XXX.243.120	80/TCP	http	No		2021-05-16
30	artifacts.muster.de, crm.muster.de, crm2.muster.de, gofit.muster.de, mailarchiv.muster.de , ... 5 more	62.XXX.243.120	443/TCP	https	No		2021-05-26
31	artifacts.muster.de, crm.muster.de, crm2.muster.de, gofit.muster.de, mailarchiv.muster.de , ... 5 more	62.XXX.243.120	8099/TCP	http	No		2021-05-22
32	support.muster.de	62.XXX.243.121	443/TCP	https	No		2021-05-19
33	support.muster.de	62.XXX.243.121	80		No		2021-05-30
34	2fa-push.muster.de, 2fa-test.muster.de, 2fa.muster.de, change.muster.de, portal.muster.de, ... 3 more	62.XXX.243.122	80/TCP	http	No		2021-05-22
35	2fa-push.muster.de, 2fa-test.muster.de, 2fa.muster.de, change.muster.de, portal.muster.de, ... 3 more	62.XXX.243.122	443/TCP	https	No		2021-05-17
36	connections.muster.de, intranet.muster.de	62.XXX.243.123	443/TCP	https	No		2021-05-15
37	connections.muster.de intranet.muster.de	62.XXX.243.123	80/TCP	http	No		2021-05-30
38	bego-rest.muster.de, box.muster.de, convo.muster.de, correlationmachine. muster.de, demo.muster.de, ... 15 more	62.XXX.243.124	443/TCP	https	No		2021-05-26
39	zulip.muster.de	62.XXX.142.195	443/TCP	https	No		2021-05-30
40	zulip.muster.de	62.XXX.142.195	80/TCP	http	No		2021-05-30
41	kasper.muster.de	62.XXX.142.200	443/TCP	https	No		2021-05-30
42	ftp.muster.de, upload.muster.de, worf.muster.de	62.XXX.142.201	80/TCP	http	No		2021-05-31
43	ftp.muster.de, upload.muster.de, worf.muster.de	62.XXX.142.201	443/TCP	https	No		2021-05-18

44	herbert.muster.de, isotest.muster.de	62.XXX.142.202	443/TCP	https	No		2021-05-17
45	auth.muster.de	62.XXX.142.204	80/TCP	http	No		2021-05-31
46	auth.muster.de	62.XXX.142.204	443/TCP	https	No		2021-05-26
47	testlink.muster.de	62.XXX.142.205	443/TCP	https	No		2021-05-13
48	testlink.muster.de	62.XXX.142.205	80/TCP	http	No		2021-05-12
49	monitor.muster.de, static.248.55.XX.78. clients.your-server.de	78.XX.55.248	80/TCP	http	No		2021-05-14

1.4 Application Management: 100%

This score rates the software that is used on the externally visible systems. This is done by checking the executed software versions and their status regarding security updates. The highest possible score is achieved if the used software versions are up-to-date and supported by the manufacturer. It should be noted that an external view can identify, display and evaluate only parts of the software versions used. Currently cysmo® detects and evaluates the most popular server operating systems and content management systems.

Illustrative Story

By looking through the main entrance, the gang finds out that the inspection stamps on the slot machines are 10 years overdue. Maybe the old machines can be manipulated?

Potential Risk

Should a security gap for the version used become known in the future, the company will no longer be able to protect itself sufficiently against this security gap. The use of older software versions considerably increases the risk of becoming the victim of hacker attacks because this software is seen as an easy point of entry. The probability for a complete takeover of an outdated system (and with it consequences like loss of data, halting of production or blackmail) increases rapidly with each month the system is out of date.

Claim (example)

The botnet Smominru, for example, consists only of computers with the operating systems Windows XP, Windows 7, Windows 2003 or Windows 2008; these are all operating systems for which manufacturers no longer offer support to the broad mass of users.

cysmo

The used software versions are up-to-date and supported by the manufacturer.

Table 4.1 – muster.de – Software Versions Used

No.	Hostnames	IP	Port	Software	Version	Support-ed	Official end of support	Classifi-cation	Last seen
1	deuba.muster.de hcob.muster.de, static.55.XX. XXX.116.clients. your-server.de	116.XXX.30. 55	443/TCP	CentOS	7	Yes	2024-06-30	✓	2021-05-14
2	deuba.muster.de hcob.muster.de, static.55.30. XXX.116.clients. your-server.de	116.XXX.30. 55	80/TCP	CentOS	7	Yes	2024-06-30	✓	2021-05-14
3	static.140.197. XX.159.clients. your-server.de, travic-instant-XXX.muster.de	159.XX.XX. 140	443/TCP	CentOS	7	Yes	2024-06-30	✓	2021-05-25
4	static.XXX.197. 69.159.clients. your-server.de, travic-instant-XXX.muster.de	159.XX.197. 140	80/TCP	CentOS	7	Yes	2024-06-30	✓	2021-05-13
5	adhoc.muster .de	46.XX.2.57	443/TCP	CentOS	7	Yes	2024-06-30	✓	2021-05-15
6	XXX.muster.de, crm.muster.de, crm2.muster.de, gofit.muster.de, mail.muster. de, ... 5 more	62.XXX.243. 120	80/TCP	CentOS	7	Yes	2024-06-30	✓	2021-05-16
7	XXX.muster.de, crm.muster.de, crm2.muster.de, gofit.muster.de, mail.muster. de, ... 5 more	62.XXX.243. 120	443/TCP	CentOS	7	Yes	2024-06-30	✓	2021-05-26
8	XXX.muster.de, crm.muster.de, crm2.muster.de, gofit.muster.de, mail.muster. de, ... 5 more	62.XXX.243. 120	8099/TC-P	CentOS	7	Yes	2024-06-30	✓	2021-05-22
9	2fa.muster. de, test.muster.de, 2fa.muster.de, XXX.muster.de, portal.muster.de ... 3 more	62.XXX.243. 122	80/TCP	Canonical Ubuntu Linux 18.04 LTS Edition	18.04	Yes	2028-04-01	✓	2021-05-22

10	2fa-push.muster de, XXX.muster.de, 2fa.muster.de, XX.muster.de, portal.muster.de ... 3 more	62.XXX.243. 122	443/TCP	Canonical Ubuntu Linux 18.04 LTS Edition	18.04	Yes	2028-04-01		2021-05-17
11	bego-rest-sst. muster.de, box.muster.de, convo.muster.de correlationmac- hine.muster.de, demo.muster.de ... 15 more	62.XXX.243. 124	443/TCP	CentOS	7	Yes	2024-06-30		2021-05-26
12	zulip.muster.de	62.XXX.142. 195	443/TCP	Canonical Ubuntu Linux 18.04 LTS Edition	18.04	Yes	2028-04-01		2021-05-30
13	zulip.muster.de	62.XXX.142. 195	80/TCP	Canonical Ubuntu Linux 18.04 LTS Edition	18.04	Yes	2028-04-01		2021-05-30
14	ftp.muster.de, XXX.muster.de, worf.muster.de	62.XXX.142. 201	80/TCP	CentOS	7	Yes	2024-06-30		2021-05-31
15	ftp.muster.de, XX.muster.de, worf.muster.de	62.XXX.142. 201	443/TCP	CentOS	7	Yes	2024-06-30		2021-05-18
16	XX.muster.de, X.muster.de	62.XXX.142. 202	443/TCP	CentOS	7	Yes	2024-06-30		2021-05-17
17	auth.muster.de	62.XXX.142. 204	80/TCP	CentOS	7	Yes	2024-06-30		2021-05-31
18	muster.de, static.248.XX. X.78.clients. your-server.de	78.XX.X.248	80/TCP	Canonical Ubuntu Linux 18.04 LTS Edition	18.04	Yes	2028-04-01		2021-05-14
19	deu.muster.de, hcob.muster.de, static.XX.30. XXX.116.clients. your-server.de	116.XXX.30. XX	443/TCP	Apache	2.4.6	-NV-	-NV-		2021-05-14
20	deu.muster.de, hcob.muster.de, static.XX.30. XXX.116.clients. your-server.de	116.XXX.30. XX	443/TCP	OpenSSL	1.0.2k	-NV-	-NV-		2021-05-14
21	deu.muster.de, hcob.muster.de, static.XX.30. XXX.116.clients. your-server.de	116.XXX.30. XX	80/TCP	Apache	2.4.6	-NV-	-NV-		2021-05-14
22	deu.muster.de, hcob.muster.de, static.XX.30. XX.116.clients. your-server.de	116.XX.30. XX	80/TCP	OpenSSL	1.0.2k	-NV-	-NV-		2021-05-14

23	abnahme-XXX.muster.de, covid-abnahme.muster.de, XX.muster.de, hmrv-abnahme-XX.muster.de, static.XXX.14.76.XXX.clients.your-server.de	XXX.76.14.XXX	443	Apache	-NV-	-NV-	-NV-	2021-05-25
24	static.XXX.197.XX.159.clients.your-server.de, travic-instant-payments.muster.de	159.XX.197.XXX	443/TCP	Apache	2.4.6	-NV-	-NV-	2021-05-25
25	static.XXX.197.XX.159.clients.your-server.de, travic-instant-payments.muster.de	159.XX.197.XXX	443/TCP	OpenSSL	1.0.2k	-NV-	-NV-	2021-05-25
26	static.XXX.197.XX.159.clients.your-server.de, travic-instant-.muster.de	159.XX.197.XXX	80/TCP	Apache	2.4.6	-NV-	-NV-	2021-05-13
27	static.XXX.197.XX.159.clients.your-server.de, travic-instant-.muster.de	159.XXX.197.XXX	80/TCP	Bootstrap	-NV-	-NV-	-NV-	2021-05-13
28	static.XXX.197.XX.159.clients.your-server.de, travic-instant-.muster.de	159.XXX.197.XXX	80/TCP	OpenSSL	1.0.2k	-NV-	-NV-	2021-05-13
29	autod.ha-autod.office.com, autod.ms-acdc-autod.office.com, autodiscover.outlook.com, autodiscover.muster.de	40.XXX.138.24	80/TCP	Microsoft ASP.NET	-NV-	-NV-	-NV-	2021-05-13
30	autod.ha-autod.office.com, autod.ms-acdc-autod.office.com, autodiscover.outlook.com, autodiscover.muster.de	40.XXX.138.24	80/TCP	Microsoft Internet Information Services (IIS) 10.0	10.0	-NV-	-NV-	2021-05-13

31	autod.ha-autod.office.com, autod.ms-acdc-autod.office.com, autodiscover.outlook.com, autodiscover.muster.de	40.XXX.138.24	80/TCP	Microsoft Windows	-NV-	-NV-	-NV-		2021-05-13
32	adhoc.muster.de	46.XX.2.57	443/TCP	Apache	2.4.6	-NV-	-NV-		2021-05-15
33	adhoc.muster.de	46.XX.2.57	443/TCP	jQuery	1.8.2	-NV-	-NV-		2021-05-15
34	adhoc.muster.de	46.XX.2.57	443/TCP	jQuery UI	1.9.1	-NV-	-NV-		2021-05-15
35	adhoc.muster.de	46.XX.2.57	443/TCP	OpenSSL	1.0.2k	-NV-	-NV-		2021-05-15
36	autod.ha-autod.office.com, autod.ms-acdc-autod.office.com, autodiscover.outlook.com, autodiscover.muster.de	52.XX.201.24	80/TCP	Microsoft ASP.NET	-NV-	-NV-	-NV-		2021-05-16
37	autod.ha-autod.office.com, autod.ms-acdc-autod.office.com, autodiscover.outlook.com, autodiscover.muster.de	52.XX.201.24	80/TCP	Microsoft Internet Information Services (IIS) 10.0	10.0	-NV-	-NV-		2021-05-16
38	autod.ha-autod.office.com, autod.ms-acdc-autod.office.com, autodiscover.outlook.com, autodiscover.muster.de	52.XX.201.24	80/TCP	Microsoft Windows	-NV-	-NV-	-NV-		2021-05-16
39	autod.ha-autod.office.com, autod.ms-acdc-autod.office.com, autodiscover.outlook.com, autodiscover.muster.de	52.XX.152.168	80	Microsoft ASP.NET	-NV-	-NV-	-NV-		2021-05-22

40	autod.ha-autod.office.com, autod.ms-acdc-autod.office.com, autodiscover.outlook.com, autodiscover.muster.de	52.XX.152.168	80	Microsoft Internet Information Services (IIS) 10.0	10.0	-NV-	-NV-		2021-05-22
41	autod.ha-autod.office.com, autod.ms-acdc-autod.office.com, autodiscover.outlook.com, autodiscover.muster.de	52.XX.152.168	80	Microsoft Windows	-NV-	-NV-	-NV-		2021-05-22
42	bastian.muster.de	62.XXX.243.114	443/TCP	Checkpoint Connectra	-NV-	-NV-	-NV-		2021-05-26
43	bastian.muster.de	62.XXX.243.114	443/TCP	Check Point Mobile	-NV-	-NV-	-NV-		2021-05-26
44	bastian.muster.de	62.XXX.243.114	264/TCP	Checkpoint Firewall-1	-NV-	-NV-	-NV-		2021-05-17
45	bastian-01.muster.de	62.XXX.243.115	443/TCP	Checkpoint Connectra	-NV-	-NV-	-NV-		2021-05-26
46	bastian-01.muster.de	62.XXX.243.115	443/TCP	Check Point Mobile	-NV-	-NV-	-NV-		2021-05-26
47	bastian-02.muster.de	62.XXX.243.116	443/TCP	Checkpoint Connectra	-NV-	-NV-	-NV-		2021-05-12
48	bastian-02.muster.de	62.XXX.243.116	443/TCP	Check Point Mobile	-NV-	-NV-	-NV-		2021-05-12
49	bastian-02.muster.de	62.XXX.243.116	264/TCP	Checkpoint Firewall-1	-NV-	-NV-	-NV-		2021-05-10
50	jobs.muster.de, karriere-live10.muster.de, karriere-.muster.de, XXX.muster.de, muster.de, ... 6 more	62.XXX.243.119	80/TCP	Apache	-NV-	-NV-	-NV-		2021-05-13
51	jobs.muster.de, karriere-live10.muster.de, karriere-stage10.muster.de, XXX.muster.de, muster.de, ... 6 more	62.XXX.243.119	443/TCP	Apache	-NV-	-NV-	-NV-		2021-06-01

52	jobs.muster.de, karriere-live10.muster.de, karriere-XXX.muster.de, XXX.muster.de, muster.de, ... 6 more	62.XXX.243.119	443/TCP	Bootstrap	3.3.7	-NV-	-NV-		2021-06-01
53	jobs.muster.de, karriere-live10.muster.de, karriere-XXX.muster.de, XXX.muster.de, muster.de, ... 6 more	62.XXX.243.119	443/TCP	jQuery	1.11.1	-NV-	-NV-		2021-06-01
54	jobs.muster.de, karriere-live10.muster.de, karriere-XXX.muster.de XX.muster.de, muster.de, ... 6 more	62.XXX.243.119	443/TCP	TYPO3 CMS	-NV-	-NV-	-NV-		2021-06-01
55	XXX.muster.de, crm.muster.de, crm2.muster.de, gofit.muster.de, mail.muster.de, ... 5 more	62.XXX.243.120	80/TCP	Apache	2.4.6	-NV-	-NV-		2021-05-16
56	muster.de, crm.muster.de, crm2.muster.de, gofit.muster.de, mail.muster.de, ... 5 more	62.XXX.243.120	80/TCP	OpenSSL	1.0.2k	-NV-	-NV-		2021-05-16
57	muster.de, crm.muster.de, crm2.muster.de, gofit.muster.de, mail.muster.de, ... 5 more	62.XXX.243.120	80/TCP	PHP	5.6.40	-NV-	-NV-		2021-05-16
58	muster.de, crm.muster.de, crm2.muster.de, gofit.muster.de, mail.muster.de, ... 5 more	62.XXX.243.120	443/TCP	Apache	2.4.6	-NV-	-NV-		2021-05-26

59	muster.de, crm.muster.de, crm2.muster.de, gofit.muster.de, mail.muster.de, ... 5 more	62.XXX.243.120	443/TCP	OpenSSL	1.0.2k	-NV-	-NV-		2021-05-26
60	muster.de, crm.muster.de, crm2.muster.de, gofit.muster.de, mail.muster.de, ... 5 more	62.XXX.243.120	443/TCP	PHP	5.6.40	-NV-	-NV-		2021-05-26
61	muster.de, crm.muster.de, crm2.muster.de, gofit.muster.de, .muster.de, ... 5 more	62.XXX.243.120	8099/TCP	Apache	2.4.6	-NV-	-NV-		2021-05-22
62	muster.de, crm.muster.de, crm2.muster.de, gofit.muster.de, mail.muster.de, ... 5 more	62.XXX.243.120	8099/TCP	OpenSSL	1.0.2k	-NV-	-NV-		2021-05-22
63	muster.de, crm.muster.de, crm2.muster.de, gofit.muster.de, mail.muster.de, ... 5 more	62.XXX.243.120	8099/TCP	PHP	5.6.40	-NV-	-NV-		2021-05-22
64	support.muster.de	62.XXX.243.121	443/TCP	Lotus Domino	-NV-	-NV-	-NV-		2021-05-19
65	support.muster.de	62.XXX.243.121	443/TCP	IBM Lotus Domino Web Server	-NV-	-NV-	-NV-		2021-05-19
66	2fa-push.muster.de 2fa.muster.de, 2fa.muster.de, change.muster.de, ... 3 more	62.XXX.243.122	80/TCP	Apache	2.4.29	-NV-	-NV-		2021-05-22
67	2fa-push.muster.de 2fa.muster.de, 2fa.muster.de, .muster.de, portal.muster.de ... 3 more	62.XXX.243.122	443/TCP	Apache	2.4.29	-NV-	-NV-		2021-05-17

68	bego-rest-sst.muster.de, box.muster.de, convo.muster.de correlationmac-hine.muster.de, demo.muster.de ... 15 more	62.XXX.243.124	443/TCP	Apache	2.4.6	-NV-	-NV-		2021-05-26
69	bego-rest-sst.muster.de, box.muster.de, XX.muster.de, correlationmac-hine.muster.de, demo.muster.de ... 15 more	62.XXX.243.124	443/TCP	OpenSSL	1.0.2k	-NV-	-NV-		2021-05-26
70	zulip.muster.de	62.XXX.142.195	443/TCP	Nginx	1.14.0	-NV-	-NV-		2021-05-30
71	zulip.muster.de	62.XXX.142.195	80/TCP	Nginx	1.14.0	-NV-	-NV-		2021-05-30
72	kasper.muster.d	62.XXX.142.200	443/TCP	Microsoft Windows	-NV-	-NV-	-NV-		2021-05-30
73	ftp.muster.de, muster.de, worf.muster.de	62.XXX.142.201	80/TCP	Apache	2.4.6	-NV-	-NV-		2021-05-31
74	ftp.muster.de, muster.de, worf.muster.de	62.XXX.XXX201	80/TCP	OpenSSL	1.0.2k	-NV-	-NV-		2021-05-31
75	ftp.muster.de, muster.de, worf.muster.de	62.XXX.XXX.201	443/TCP	Apache	2.4.6	-NV-	-NV-		2021-05-18
76	ftp.muster.de, muster.de, worf.muster.de	62.XXX.XXX.201	443/TCP	OpenSSL	1.0.2k	-NV-	-NV-		2021-05-18
77	muster.de, iso.muster.de	62.XXX.XXX202	443/TCP	Apache	2.4.6	-NV-	-NV-		2021-05-17
78	muster.de, iso.muster.de	62.XXX.XXX.202	443/TCP	OpenSSL	1.0.2k	-NV-	-NV-		2021-05-17
79	auth.muster.de	62.XXX.XXX.204	80/TCP	Apache	2.4.6	-NV-	-NV-		2021-05-31
80	auth.muster.de	62.XXX.XXX.204	80/TCP	OpenSSL	1.0.2k	-NV-	-NV-		2021-05-31
81	testlink.muster.de	62.XXX.XXX.205	443/TCP	Apache	2.4.41	-NV-	-NV-		2021-05-13
82	testlink.muster.de	62.XXX.XXX.205	443/TCP	OpenSSL	1.1.0l	-NV-	-NV-		2021-05-13
83	testlink.muster.de	62.XXX.XXX.205	443/TCP	PHP	7.3.13	-NV-	-NV-		2021-05-13
84	testlink.muster.de	62.XXX.XXX.205	80/TCP	Apache	2.4.41	-NV-	-NV-		2021-05-12
85	testlink.muster.de	62.XXX.XXX.205	80/TCP	OpenSSL	1.1.0l	-NV-	-NV-		2021-05-12
86	testllink.muster.de	62.XXX.XXX.205	80/TCP	PHP	7.3.13	-NV-	-NV-		2021-05-12

87	muster.de, static.248.XX.XX.78.clients.your-server.de	78.XX.XX.248	80/TCP	Apache	2.4.29	-NV-	-NV-		2021-05-14

1.5 Back-End Logins: 100%

This score rates the number of logins available online, which indicates the access to a back-end system. These can, for example, be logins to back-ends of websites, terminal servers or databases (related to the web interface). Furthermore, it checks the CMS logins (content management system logins) that are available from the outside. For a perfect score none of these logins should be available from the outside.

Illustrative Story

In the casino area, you will also find a separate area "for staff only" with some lightly secured doors. If none of the security guards are looking, these doors should open quickly.

Potential Risk

Accessible back-end logins can result in major data losses (customer data, internal data). If the stored data is particularly sensitive, attackers might even resort to blackmail in order to extort money.

Claim (example)

47,000 sensitive data records of car manufacturers were found by a security researcher on a supplier company's externally visible backup server.

No accessible logins to back-end or content management systems were found.

5 VPN accesses have been found (this finding is only informative and does not affect the rating).

Table 5.1 – muster.de – Back-End Logins – VPN

No.	Hostnames	IP	Port	Type	Software
1	adhoc.muster.de	46.XX.2.57	1194/UDP	Virtual private network	-NV-
2	bastian.muster.de	XX.154.XXX.114	443/TCP	Virtual private network	Checkpoint Connectra, Check Point Mobile (VP-N)
3	bastian.muster.de	XX.154.XXX.114	500/UDP	Virtual private network	-NV-
4	bastian-01.muster.de	XX.154.XXX.115	443/TCP	Virtual private network	Checkpoint Connectra, Check Point Mobile (VP-N)

5	bastian-02.muster.de	XX.154.XXX.116	443/TCP	Virtual private network	Checkpoint Connectra, Check Point Mobile (VP-N)

1.6 Malicious Activities: 100%

For this score, the identified servers are examined regarding their participation in cyber attacks. This refers to both their participation as source and target of these attacks. Sources are servers with outgoing malicious traffic, for example when they act as part of a botnet or spread malware (mostly without the knowledge of their owner). This can result in further infections or in an exclusion from services (e.g. Google). Blacklists and honeypots are checked to identify these sources. Further servers are checked for an elevated risk of being targeted by attackers themselves. To this end, darknet sources listing rewarding, vulnerable or already infected targets are being checked.

Illustrative Story

There is a rumor on the street that the casino has already been broken into 2 weeks ago. The gang could find out what the burglars were up to in the local bars.

Potential Risk

The appearance of individual IPs in this score indicates that attackers have taken over parts of the infrastructure and will continue to abuse them in the future. The risk of further data loss is very high. Additionally, attackers might have installed backdoors in order to re-enter the systems at will and cause more damage.

Claim (example)

A small entertainment company was hacked and used to host malware. Google put a warning under the official website in its search results, indicating that "this website may have been hacked".

No signs of malicious activities were found.

2 DDoS Stability: 45%

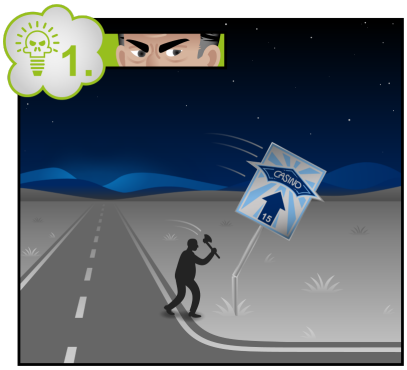
The partial rating "DDoS Stability" rates the resilience of the infrastructure regarding DDoS attacks (Distributed Denial of Service).

Illustrative Story

A robbery gang wants to rob a casino and scouts it out in advance. In addition to the gang of robbers, the operator of a casino in the neighbourhood is targeting the casino and is looking for ways to harm the unloved competitor. "DDoS Resilience" focuses on three different ways (DNS, Mail, Web) to reach this goal.

2.1 DNS DDoS: 35%

This score rates the resilience of the DNS infrastructure, i.e. of the servers that are responsible for the name resolution of the rated domain. A high score corresponds to a diversified and stable infrastructure that is more difficult for attackers to break down. The number of servers, their distribution across different network areas (CIDRs), the use of autonomous systems (AS) and the distribution across continents are checked and evaluated. In addition, it is checked whether they are cloud infrastructures or anycast structures which have a positive effect on scoring.



Illustrative Story

There is only one road to the casino. If a robber breaks the advertising sign at the last intersection to the street, most visitors will find not their way there.

Potential Risk

If the DNS servers are unavailable, there is a high risk that the website cannot be accessed and, in addition, mail traffic will be disrupted. This can quickly lead to a business interruption or damage to reputation.

Claim (example)

Several young people paralysed the infrastructure of an IT service provider of a German bank with a DDoS attack out of boredom.

The DNS infrastructure is not optimally protected against DDoS attacks.

Table 6.1 – muster.de – DNS Infrastructure Target-Actual

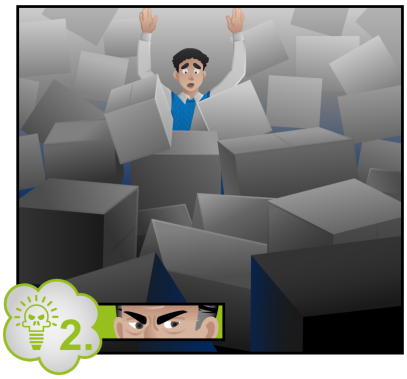
No.	Criteria	Actual	Target	Classification
1	Number of servers	2	5	
2	Number of CIDR	2	2	
3	Number of AS	1	2	
4	Number of continents	1	2	

Table 7.1 – muster.de – DNS Server

No.	Hostname	IP	Location	CIDR	ASN	AS name	Contin-ent	Cloud hosted	Anyca-st
1	auth04.ns.de.uu.net	XXXX:600:1c-0:e000::XX:9	Dortmund (Lütgendo-rtmund) (DE)	2001:600:1c-0::/XX	AS702	MCI Communications Services, Inc. d/b/a Verizon Business	EU	-NV-	-NV-
2	auth54.ns.de.uu.net	XXXX:600:1c-0:e001::XX:9	Dortmund (Lütgendo-rtmund) (DE)	XXXX:600:1c-0::/XX	AS702	MCI Communications Services, Inc. d/b/a Verizon Business	EU	-NV-	-NV-
3	auth54.ns.de.uu.net	194.128.XXX.100	London (GB)	194.128.XXX.96/XX	AS702	MCI Communications Services, Inc. d/b/a Verizon Business	EU	-NV-	-NV-
4	auth04.ns.de.uu.net	XXX.76.XXX.17	Dortmund (Lütgendo-rtmund) (DE)	XXX.76.XXX.0/24	AS702	MCI Communications Services, Inc. d/b/a Verizon Business	EU	-NV-	-NV-

2.2 Mail DDoS: 100%

This score rates the mail infrastructure's resilience against DDoS attacks. A high score corresponds to a diversified and stable infrastructure that is more difficult for attackers to break down. The number of servers, their distribution to different network areas (CIDRs) and the use of autonomous systems (AS) are assessed and rated. Additionally, it is checked whether they are cloud infrastructures or anycast structures which have a positive effect on scoring.



Illustrative Story

The doorman at the delivery entrance is already well occupied with daily operations. If the malicious competitor were to send a lot of parcel carriers with empty parcels, the entire delivery traffic would come to a complete standstill.

Potential Risk

Unavailability of the mail services could lead to an interruption of operations. Both outgoing e-mails (internal and external) and incoming e-mails, e.g. from customers or suppliers, would be disturbed.

Claim (example)

A group called "Turkish Hackers" attacked numerous hosting providers and their mail infrastructure in Italy and demanded bitcoins to stop the attacks.

The mail infrastructure is robust and protected against DDoS attacks.

Table 8.1 – muster.de – Mail Infrastructure Target-Actual

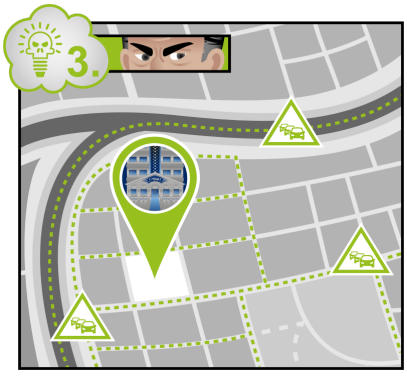
No.	Criteria	Actual	Target	Classification
1	Number of servers	2	3	
2	Number of CIDR	2	2	
3	Number of AS	2	2	

Table 9.1 – muster.de – Mail Server

No.	Hostname	IP	Location	CIDR	ASN	AS name	Contin-ent	Cloud hosted
1	mail1.muster.de	62.XXX.243.XXX	Frankfurt am Main (DE)	62.XXX.243.XXX/29	AS3320	Deutsche Telekom AG	EU	-NV-
2	mail4.muster.de	212.XXX.0.XXX	Kiel (Schreventeic-h - Hasseldieksd-amm) (DE)	212.XXX.0.XXX/28	AS25415	ADDIX Internet Services GmbH	EU	-NV-

2.3 Web DDoS: 0%

This score rates the web infrastructure's resilience against DDoS attacks. A high score can be achieved if the infrastructure is protected by protective measures against DDoS. The following protective measures influence the score: setting low time-to-live values (TTL) in the DNS server configurations, deploying a web application firewall software (WAF), deploying a strong concept for distributing network loads to different servers. A strong network load distribution concept involves the use of solutions from professional vendors (CDN providers) and load balancing across multiple, preferably globally distributed servers.



Illustrative Story

The operator of the competing casino wants to pay the local mafia to stop traffic to the casino and in the underground car park by creating a massive traffic jam with their vehicles.

Potential Risk

Unavailability of the web servers could lead to unavailability of the website. Customers, employees or others are no longer able to open the website.

Claim (example)

Hackers shut down the website of the University of Luxemburg with a DDoS attack. Fortunately, only the website was affected while the e-learning programme introduced to handle the impacts of COVID-19 remained operational.

Few or no measures were found to prevent DDoS attacks.

Table 10.1 – muster.de – DDoS Resilience (Web Servers)

No.	Hostname	IP	Location	CIDR	ASN	AS name	Contin-ent	Anyca-st	Scrubbing center
1	www.muster.de	62.XXX.243.XXX	Frankfurt am Main (DE)	62.XXX.243.XXX/29	AS3320	Deutsche Telekom AG	EU	-NV-	-NV-

Table 11.1 – muster.de – DDoS Resilience (Website)

No.	Hostname	Website	CDN	WAF	Location-based load balancing (CNAME)	Location-based load balancing (IP)	Round Robin via DNS	Low TTL
1	www.muster.de	https://www.muster.de	-NV-	-NV-	-NV-	-NV-	No	No

3 DNS Config: 88%

The partial rating "DNS Config" rates the configuration of the used DNS infrastructure (domain name system). This includes the servers that are responsible for the name resolution of the systems and the domain registrars involved. A high score corresponds to high resilience against attacks such as domain takeovers or man-in-the-middle attacks.

Illustrative Story

A robbery gang wants to rob a casino and scouts it out in advance. The partial rating "DNS Config" refers to what is comparable to the address of the casino, which makes it easier to find and navigate to the casino.

3.1 Administrative Security: 25%

This score rates the administrative security aspects regarding the configuration of the DNS infrastructure that might allow attackers to e.g. assume the used domains or pose as the DNS server in charge of the infrastructure.

Illustrative Story

The managers of the casino have forgotten to protect the name of the casino under trademark law. This increases the probability of imitators and swindlers.

Potential Risk

If certain administrative DNS settings are not made, hackers may take over the domains used.

Claim (example)

The website of the South African Transnet National Ports Authority (TNPA) was captured by hackers. They took over the domain and misused it to display information about gambling games in Indonesia. This led to reputational damage.

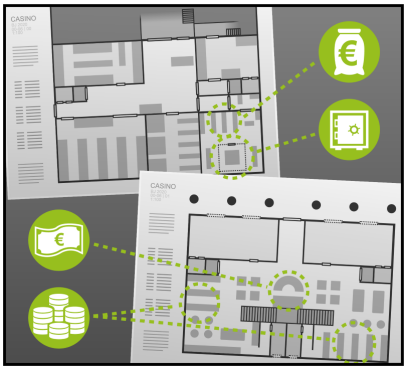
Problems were found in the configuration of the DNS infrastructure regarding the administrative security.

The domain registrar does not support the setting of the field "clientTransferProhibited". However, the registrar could still allow domains to be transferred to attackers.

DNSSEC is not used.

3.2 Operational Security: 100%

This score rates the operative security aspects regarding the configuration of the DNS infrastructure. Due to any problems found here attackers are able to spy out the infrastructure or abuse the DNS server for the launch of attacks.



Illustrative Story

At the local building authority, the robbers can find out the address of a casino whose building plans they can access, including sensitive areas such as the vault.

Potential Risk

Using the intercepted DNS data, attackers can easily gain knowledge on the company's internal infrastructure. They can then use this information to launch further attacks.

Claim (example)

A server of a subcontractor of the Global Media Group did not prohibit the use of a technique to copy all known internal and external server-addresses to another server without any authentication. One of these servers was an insecure and out-of-date monitoring server, which was set up to access other computers in the internal network and could therefore infect them with malware. The vulnerability was found by a security researcher, so luckily no harm was done.

No problems were found in the configuration of the DNS infrastructure regarding the operative security.

The DNS servers do not accept any zone transfer requests (AXFR). That way it becomes more difficult for attackers to spy out the infrastructure.

The DNS servers are not configured as open resolvers.

Table 12.1 – muster.de – Open Resolvers

No.	Hostname	IP	Open resolver	Classification
1	auth04.ns.de.uu.net	XXX.76.XXX.17	No	
2	auth54.ns.de.uu.net	XXX.128.XXX.100	No	

3	auth04.ns.de.uu.net	XXXX:600:1c0:XXXX::35:9	No	
4	auth54.ns.de.uu.net	XXXX:600:1c0:XXX::35:9	No	

No DNS entries with private or non-routable IP addresses were found.

All DNS entries have a regular time to live (TTL).

3.3 Best Practises: 100% *

* This score has a purely informative value for the current rating.
The score does not affect the total rating.

This score examines the use of best practices for the DNS configuration. These practices do not directly influence the security of the DNS infrastructure.

Illustrative Story

The casino's street address in the business directory and on the Internet was entered incorrectly. This leads to incorrect directions and makes it more difficult to find the casino.

Not all the best possible measures (best practices) that have already been tried and tested have been implemented.

An A record is located on the main domain(s). Visitors of the domain can directly access the company's website without the prefix "www." (e.g. "example.com" instead of "www.example.com").

No CAA record exists in the DNS system, which would limit the issuing of certificates for this/these domain(s) to certain issuers.

4 Mail Config: 85%

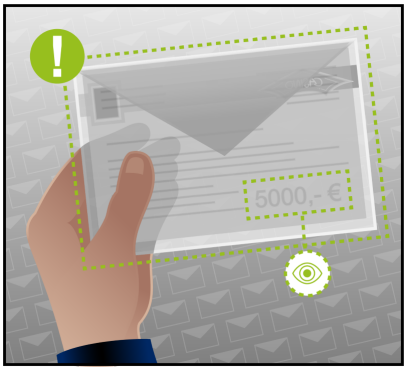
The partial rating "Mail Config" rates the configuration of the used mail servers. A high score is achieved by a configuration that complies with current standards, such as support of only secure encryption standards or authentication procedures that make social engineering attacks more difficult.

Illustrative Story

A robbery gang wants to rob a casino and scouts it out in advance. The partial rating "Mail Config" refers to what is comparable to the post department of the casino.

4.1 Mail TLS: 100%

This score evaluates the security of the transport encryption between mail servers. A high score is achieved if the mail servers communicate encrypted and only versions of the encryption protocol are used that are considered sufficiently secure (TLS 1.2 and higher). Note: Due to the introduction of the new TLS 1.3 encryption standard and the recommendation of the BSI, encryption via TLS 1.1 will no longer be classified as sufficiently secure.



Illustrative Story

The invoices sent by the casino are sent in transparent envelopes. This makes it easy to see the contents without even opening them.

Potential Risk

If mail traffic is not or only weakly encrypted or the TLS standard is outdated, attackers can intercept the e-mail traffic using various attacks. There is a very high risk of customer data or internal information (such as passwords) being intercepted.

Claim (example)

Internal documents of a notary were intercepted by hackers. Due to outdated mail encryption, hackers could crack the e-mail traffic within minutes and read it in plain text.

All found and reachable mail servers use TLS and are configured securely.

Table 13.1 – muster.de – Mail TLS Check

No.	Hostname	IP	Remark
1	mail1.muster.de	62.XXX.243.XXX	Connection to the mail server established successfully.
2	mail4.muster.de	XXX.51.0.XXX	Connection to the mail server established successfully.

The found mail servers only use secure TLS protocol versions.

Table 14.1 – muster.de – Mail TLS Versions

No.	Hostname	SSL v2	SSL v3	TLS v1.0	TLS 1.1	TLS 1.2	TLS 1.3
1	mail1.muster.de	No	No	No	No	Yes	Yes
2	mail4.muster.de	No	No	No	No	Yes	Yes

Table 15.1 – muster.de – Mail Certificates

No.	Hostname	Certification authority	Trusted	Valid for hostname	Expiration date	Extended validation title	Classification
1	mail1.muster.de	GlobalSign nv-sa	Yes	Yes	2021-12-19	-NV-	
2	mail4.muster.de	GlobalSign nv-sa	Yes	Yes	2021-12-19	-NV-	

4.2 Spoofing Protection: 70%

This score rates the use and effectiveness of common protection measures against forged mails (e-mail spoofing) and spam.

Illustrative Story

People are receiving fake invoices in the name of the casino.

Potential Risk

The so-called SPF (Sender Policy Framework) record is used to define specific network areas from which an e-mail sender address can originate. This enables the receiving e-mail servers to check whether the sender of the e-mail is genuine. This minimizes the risk of e.g. reputational damage or falling victim to a "CEO Fraud" attack.

Claim (example)

By means of a so called "CEO Fraud" attack, hackers were able to steal € 50,000 from a car dealership. The hackers pretended to be the managing director (CEO) and instructed the secretary to transfer the money as quickly as possible.

Not all evaluated security measures exist and/or are configured correctly.

No DANE entry (distribution and verification of public keys or TLS certificate) found.

Table 16.1 – muster.de – DANE

No.	Hostname	Uses DANE	Configuration error
1	mail4.muster.de	No	-NV-
2	mail1.muster.de	No	-NV-

No DMARC record has been found. The DMARC record would enforce the use of SPF and DKIM (DomainKeys Identified Mail) to successfully authenticate the sender of the e-mail.

The SPF (Sender Policy Framework) for the protection against falsified e-mails is used and effective.

Table 17.1 – muster.de – SPF

No.	Domain	SPF record	Permitted senders	Effective
1	muster.de	v=spf1 mx ip4:62.XXX.243.XXX ip4:78.XX.64.XXX ip4:212.51.0.113 ip4:XXX.51.0.XXX ip4:XX.4.XX.16 include:spf.mailjet.com ~all	XX.189.236.0/22, XX.211.XX.0/22, 185.XX.236.0/22, XX.51.0.XXX/32, XXX.51.0.XXX/32, ... 4 more	Yes

MTA-STS (Mail Transfer Agent Strict Transport Security) is not activated. An activation would enforce the use of encryption and certificate validation to protect against man-in-the-middle (MITM) attacks.

4.3 Blacklist Reputation: 100%

For this score the mail infrastructure is checked against various blacklists. A high score can be achieved if the mail infrastructure is not on any blacklist. A blacklist would indicate that the infrastructure sends spam mail. As a consequence the regular outgoing mails are displayed as spam for the recipient or cannot be opened.

Illustrative Story

The casino sends out bills and reminders with a very unreliable postman, which results in half of the letters never reaching the recipient.

Potential Risk

There is a risk that the company's e-mails do not reach the customer.

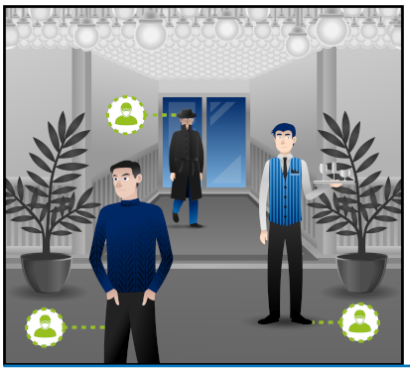
Claim (example)

In the past, customers of Deutsche Telekom's e-mail services were unable to send e-mails to Microsoft's e-mail infrastructure (e.g. Outlook, Hotmail) due to some of Deutsche Telekom's mail servers being on a blacklist.

No blacklist entries were found for the mail servers.

5 Privacy and Reputation: 68%

The partial rating "Privacy and Reputation" rates the treatment of website visitors and the "reputation" of the website(s). It evaluates, for example, the encryption, confidentiality and the transfer of information on the user behaviour (tracking) to third parties. In addition to the actual web server, the quality of the surrounding network is rated regarding events such as phishing, distribution of malware or botnet activities. Such activities can result in the exclusion of the respective network segment by other providers (e.g. in mail traffic, through security warnings in the Google index or content filters of security appliances). This can negatively influence the reputation of the company.



Illustrative Story

A robbery gang wants to rob a casino and scouts it out in advance. The partial rating "Privacy and Reputation" refers to what is comparable to a stay in the casino.

5.1 Web Server TLS: 100%

This score rates the quality of the transport encryption for the web servers (whether or not an encryption is used, and if so, which kind of protocol). A high score is achieved if data exchange is encrypted and versions of the encryption protocol are used that are deemed sufficiently secure (TLS 1.2 and higher). Note: Due to the introduction of the new TLS 1.3 encryption standard and the recommendation of the BSI, encryption via TLS 1.1 will no longer be classified as sufficiently secure.

Illustrative Story

During a game in the casino, it is possible to look at the cards of other players through a misplaced mirror.

Potential Risk

If web traffic is not or only weakly encrypted, attackers can read the traffic between users (including employees logging in to the company website externally) using various attacks. There is a very high risk of customer data or internal information (such as passwords) being intercepted.

Claim (example)

A doctor's practice has an online reception where patients can have their prescriptions issued directly by entering their patient data via the website. Since the website was not encrypted, attackers could intercept the patient data in plain text.

cysmo

The web server(s) use TLS and are configured securely.

Table 18.1 – muster.de – Web TLS Check

No.	Hostname	IP	Remark
1	www.muster.de	62.XXX.243.XXX	Connection to the web server established successfully.

The web server(s) accept secure TLS protocol versions only.

Table 19.1 – muster.de – Web TLS Versions

No.	Hostname	SSL v2	SSL v3	TLS v1.0	TLS 1.1	TLS 1.2	TLS 1.3
1	www.muster.de	No	No	No	No	Yes	No

Table 20.1 – muster.de – Web Certificate

No.	Hostname	Certification authority	Trusted	Valid for hostname	Expiration date	Extended validation title	Classification
1	www.muster.de	GlobalSign nv-sa	Yes	Yes	2021-08-04	-NV-	

5.2 Trackers: 33%

This score rates the respect for the privacy of website visitors. When integrating resources from third parties, personal data is transmitted to these external source. In some cases, this data is used to track, analyse and profile user behaviour (e.g. Mixpanel or Google Analytics). This score rates the third party resources with regard to extent of use, tracking capabilities and intent.

Illustrative Story

After visiting the casino, visitors receive advertising for other casinos by letter.

Potential Risk

By means of external references or trackers, the data of the website's users can be transmitted to third parties. There is a potential risk of violating the General Data Protection Regulation (GDPR).

Claim (example)

IKEA in Spain had to pay a € 10,000 fine for enabling cookies on website visitors' computers without the option to deactivate them.

The website loads data from third-party sources or trackers. This can affect the privacy of the website visitors.

Table 21.1 – https://www.muster.de/ – External References

No.	External reference	Category	Uses cookies	Tracker	IP anonymization	Classification
1	api.curator.io	-NV-	No	No	-NV-	
2	assets.pinterest.com	Analytics	No	Yes	-NV-	
3	c.leadlab.click	Analytics	No	Yes	-NV-	
4	cdn.curator.io	-NV-	No	No	-NV-	
5	consent.cookiebot.com	-NV-	No	No	-NV-	
6	consentcdn.cookiebot.com	-NV-	No	No	-NV-	
7	log.pinterest.com	Analytics	No	Yes	-NV-	
8	pbs.twimg.com	Analytics	No	Yes	-NV-	
9	px.ads.linkedin.com	Analytics	Yes	Yes	-NV-	
10	snap.licdn.com	Analytics	No	Yes	-NV-	
11	t.leadlab.click	Analytics	No	Yes	-NV-	
12	www.googletagmanager.com	-NV-	No	No	-NV-	

5.3 User Security: 55%

This score rates the protective measures that improve the security of the website visitors. These measures include, among others, forcing an encrypted connection and defining the permitted sources of scripts for the execution in the visitor's browser.

Illustrative Story

Some visitors were cheated out of their money by other visitors who pretended to be employees of the casino.

cysmo

Potential Risk

If the website can be manipulated due to insufficient user security, hackers can launch different attacks like clickjacking or cross-site scripting.

Claim (example)

The website of an online shop was hacked. Through clickjacking, customers did not order from the actual online shop, but from an online shop in China. By the time the cyber attack was discovered, the online shop had lost € 140,000 in sales.

Problems that reduce the security of the visitors were found for the website(s).

Table 22.1 – https://www.muster.de/ – User Security

No.	Feature	Remark	Technical details	Classification
1	By means of the Expect-CT header, the server signals conformity with the Certificate Transparency project (CT project). Browsers are instructed to verify the security certificates of the web server against the public log of the CT project and to report errors. This helps discover forged certificates.	Available and effective	"max-age=86400"	
2	The web server enforces the use of an encrypted connection by means of HTTP Strict Transport Security (HSTS).	Available and effective	"max-age=0; includeSubDomains"	
3	The domain is listed on the HSTS preload list. Domains on the HSTS preload list enforce an encrypted connection via HTTP Strict Transport Security (HSTS).	Unavailable or ineffective		
4	The web server loads its main contents in encrypted form (via TLS). Embedded contents (e.g. external scripts, images or external text) are, however, loaded in unencrypted form.	Available and effective		
5	By means of the X-Permitted-Cross-Domain-Policies header, the web server prohibits or restricts the embedding of the website in PDF files or Adobe Flash.	Available and effective	"same-origin"	
6	By means of the X-Content-Type-Options header, the server instructs the browser to only load scripts and style sheets with the correct MIME type. This makes cross-site scripting attacks more difficult as the attacker cannot embed any script contents or style sheets with an incorrect MIME type (e.g. images containing JavaScript code).	Available and effective	"nosniff"	
7	The web server does prevent the integration of the website into another via the X-Frame-Options header. This prevents attacks such as clickjacking.	Not available		

8	By means of the Referrer-Policy header, the server instructs the browser to only expect restricted information or no information at all on the origin address that referred the user to the website. This protects the privacy of the user.	Available and effective	"none"	✓
9	The web server instructs the browser not to deactivate the implemented cross-site scripting filter and to limit or prevent the loading of the page in case of detected cross-site scripting attacks.	Available and effective	"1; mode=block"	✓
10	The execution of scripts from untrustworthy sources is prevented by an effective Content-Security-Policy header (CSP header).	Not available		!

5.4 Web Server Reputation: 100%

This score rates the web servers regarding attacks originating from them. If the score is low, the IPs of the web servers are conspicuous by malicious traffic (e.g. participation in botnets or port scanning).

Illustrative Story

The robbers have secretly manipulated a coin changer machine, making it divert a small amount of money from each customer who uses it.

Potential Risk

A finding indicates that the server was taken over in the past. There is a risk that the server has become part of a botnet. From within a botnet, the attacker can use the computer for further attacks, potentially resulting in liability damage. In addition, the network may have been infiltrated during the takeover and sensitive data may have been intercepted.

Claim (example)

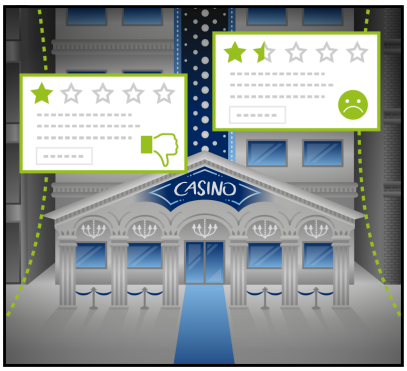
Hackers have disabled the IT infrastructure of a German machine builder (Pilz GmbH) for 4 weeks. The company specialising in automation lost € 19,000,000 in sales during this period.

✓ **The IPs of the web servers are not known for any events with bad outgoing traffic.**

5.5 AS Reputation: 100% *

* This score has a purely informative value for the current rating.
The score does not affect the total rating.

This score rates the traffic from within the autonomous system (AS) on which the identified web services are running. If the score is low, the host attracted attention due to a high level of malicious traffic (e.g. scan or exploit attempts). The rating of the specific IP of the web server is realised in the score "Web Server Reputation". No direct inference can be made to the specific IP of the rated company; there may, however, be a higher "risk of infection".



Illustrative Story

Visitors avoid the casino because there are many other casinos with a bad reputation in the same area.

Potential Risk

If there is a lot of suspicious web traffic in the data center, there is a potential risk that the whole data center becomes the subject of an attack.

Claim (example)

As a result of a lot of attacks coming from Amazon's data centers, they have been blacklisted on some mailing blacklists. As a result, some e-mail providers entirely refuse e-mails coming from Amazon Web Services instances.

For the autonomous systems on which web servers are located, no negative events are known.

5.6 Domain Reputation: 100% *

* This score has a purely informative value for the current rating.
The score does not affect the total rating.

This score rates the URLs of the identified web servers with regard to Safe Browsing, phishing and malware blacklists as well as against lists of known data breaches. Entries in these lists indicate that malware has already been successfully installed on the servers of the rated domain(s) or that attackers succeeded in stealing data of the company. Entries in these lists, for example, prevent the indexing in Google or block the call of the website by security appliances. Therefore, the website of the company can no longer be called up by the regular visitor or can only be called up after ignoring the warning messages.

Illustrative Story

The health department found cockroaches in one of the restaurants of the casino and the local press published an article about it.

Potential Risk

If a domain is on a blacklist, some web browsers (e.g. Chrome) completely block the page view of this site and display a red security warning. Although this security warning can be ignored by performing several steps, damage to the reputation remains. Customers will be deterred from visiting the website. Additionally, other e-mail servers might block e-mails coming from that server, leading to a total collapse of the mailing capabilities.

Claim (example)

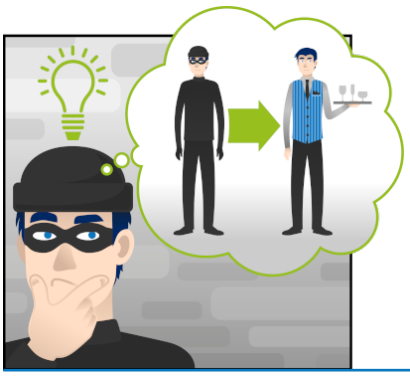
The domain of a mailing list provider for professional customers has been blacklisted by Google Safe Search. Customers trying to access their accounts only got a bright red screen trying to enter the website, and all e-mail traffic was blocked. Since the company was an e-mail provider, this meant business was completely interrupted for as long as the blacklist entry persisted.

- **The domain(s) display(s) no apparent abnormalities regarding breaches, leaks or blacklist entries.**
  - **No blacklist entries are known for the domain(s).**
  - **No breaches are known for the domain(s).**

6 Darknet: 58% *

* This score has a purely informative value for the current rating.
The score does not affect the total rating.

The partial rating "Darknet" rates the attack surface with regard to social engineering. The more finds there are for the rated company in current leaks, the lower the rating. It is checked whether personalised e-mail addresses of the company have been published in the Darknet and whether the corresponding passwords are available for these e-mail addresses. The findings are then checked and evaluated for timeliness, origin (i.e. which service is affected) and multiple use of the same passwords.



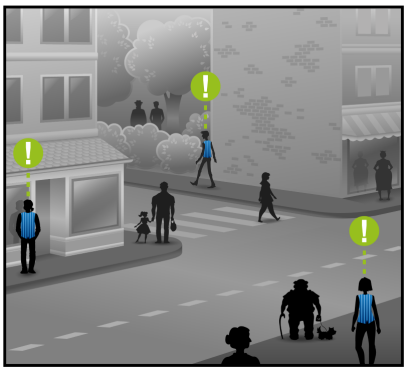
Illustrative Story

A robbery gang wants to rob a casino and scouts it out in advance. One of the robbers has the idea to gain access to the protected areas via the casino employees. The partial rating "Darknet" focuses on various ways to reach this goal.

6.1 Leak Age: 0% *

* This score has a purely informative value for the current rating.
The score does not affect the total rating.

This score rates how current all the leaks are (e-mail addresses without passwords). Since newer leaks are more valuable for social engineering attacks they result in a lower rating. Leaks that are younger than a year are punished maximally, i.e. the score is rated at 0 %.



Illustrative Story

The employees of the casino are very easy to recognise as they walk around in their casino uniforms after work. Therefore the robbery gang knows exactly who is a casino employee and a potential target.

Potential Risk

E-mail addresses and corresponding passwords published on the darknet provide attackers with a basis for social engineering e.g. spear phishing attacks or credential stuffing.

Claim (example)

Amidst the 2020 COVID-19 crisis, 500,000 Zoom accounts were hacked using a credential stuffing attack. The accounts of the online meeting plattform were sold in the darknet.

At least one leak was found that occurred less than 1,000 days ago.

Table 23.1 – muster.de – Leaks

No.	Name of leak	Affected service	Date of leak	# of passwords	# of addresses
1	cit0day	meltwaternews.com	2020-11-15	1	1
2	cit0day	newjob.de	2020-11-15	1	1
3	github_users	github.com	2020-05-05	0	1
4	canva_com	canva.com	2019-05-24	0	2
5	Collection #2 filtered	dfb.de	2019-05-12	1	1
6	Collection #2 filtered	seminar-shop.com	2019-05-12	1	1
7	Collection #2 filtered	udkik.dk	2019-05-12	1	1
8	Collection #2 filtered	www.linkedin.com	2019-05-12	3	3
9	Collection #1	-NV-	2019-01-14	7	7
10	Collection #1	dfb.de	2019-01-14	1	1
11	Collection #1	uplay.com	2019-01-14	1	1
12	Collection #1	www.udkik.dk	2019-01-14	1	1
13	appolo_v5	apollo.com	2018-07-23	0	21
14	myfitnesspal	myfitnesspal	2018-02-01	0	1
15	Anti-Public	-NV-	2016-12-01	6	6
16	Exploit.in	-NV-	2016-05-31	10	10
17	Myspace	myspace.com	2013-06-11	0	1
18	Adobe	www.adobe.com	2013-01-01	0	25
19	LinkedIn	www.linkedin.com	2012-06-05	0	7
20	Dropbox	www.dropbox.com	2012-01-01	0	9

The most current leak without passwords is 393 days old.

The most current leak with passwords is 199 days old.

6.2 Credential Stuffing: 100% *

* This score has a purely informative value for the current rating.
The score does not affect the total rating.

This score checks the probability of a successful credential stuffing attack. During such an attack, the attacker attempts to log in to company services using known combinations of user names or e-mail addresses and passwords (publicised in leaks). If users have identical passwords across several services, the probability is high that a login with these passwords will also be successful at services that did not suffer a data leak.

Illustrative Story

A casino employee has a very bad memory and uses the same PIN everywhere. He was observed using it to pay by card as well as to unlock his mobile phone. Maybe this PIN also works for the staff area of the casino.

Potential Risk
Employees might reuse credentials for personal services (such as social networks) and business matters. If one of these services suffers a breach, access to internal business systems could be gained from these leaks.

Claim (example)
Amidst the 2020 COVID-19 crisis, 500,000 Zoom accounts were hacked using a credential stuffing attack. Hackers used credentials they gained from other platforms to try to log in to the zoom accounts. These credentials were then sold on the darknet.

No e-mail addresses which use the same password for various services were found.

6.3 Policy Violation: 0% *

* This score has a purely informative value for the current rating.
The score does not affect the total rating.

This score rates the sources of the leaks. If employees have used their professional e-mail address to register for non-enterprise services, this indicates a violation of company policy and is rated negatively.

Illustrative Story
The casino has a regulation which prohibits wearing the uniforms on private occasions as the uniforms might get lost. Some employees have been observed violating this policy, giving the robbers an opportunity to steal them.

Potential Risk
E-mail addresses which are used in a non-business context have an increased chance of being stolen. Attackers could also obtain information that can be used to launch a cyber attack.

Claim (example)
A craft beer brewery fell victim to a cyber attack after hackers were able to gain access to internal systems using credentials published in the darknet. They were able to do so because an employee had registered with his company e-mail address at a game forum. Fortunately, the hackers could not access the production lines, so there were no delivery bottlenecks.

Leaked e-mail addresses were found that were used in a non-company-related context.

Table 24.1 – muster.de – Policy Violation

No.	Name of leak	Affected service	Date of leak	# of passwords	# of personal addresses	# of generic addresses
1	cit0day	meltwaternews.com	2020-11-15	1	1	0
2	cit0day	newjob.de	2020-11-15	1	1	0
3	github_users	github.com	2020-05-05	0	1	0
4	canva_com	canva.com	2019-05-24	0	2	0
5	Collection #2 filtered	dfb.de	2019-05-12	1	1	0
6	Collection #2 filtered	seminar-shop.com	2019-05-12	1	1	0
7	Collection #2 filtered	udkik.dk	2019-05-12	1	1	0
8	Collection #2 filtered	www.linkedin.com	2019-05-12	3	3	0
9	Collection #1	dfb.de	2019-01-14	1	1	0
10	Collection #1	uplay.com	2019-01-14	1	1	0
11	Collection #1	www.udkik.dk	2019-01-14	1	1	0
12	appolo_v5	apollo.com	2018-07-23	0	21	0
13	myfitnesspal	myfitnesspal	2018-02-01	0	1	0
14	Myspace	myspace.com	2013-06-11	0	1	0
15	Dropbox	www.dropbox.com	2012-01-01	0	9	0

6.4 Blackmail Threat: 100% *

* This score has a purely informative value for the current rating.
The score does not affect the total rating.

This score rates the sources of leaks with regard to their blackmail potential. If employees have used their professional e-mail address to register at private services whose use is usually not made public (e.g. dating or erotic portals), these employees are particularly exposed towards blackmail attempts.

Illustrative Story

A casino employee is often seen in a nearby brothel. Perhaps he can be blackmailed if a robber threatens to talk to his wife about his brothel visits.

Potential Risk

It is possible for an employee to be blackmailed and thus, for example, to transfer internal company data to the blackmailers.

Claim (example)

The aftermath of the "ashleymadison.com" leak brought a wave of extortion attacks against the individuals affected by the hack.

No leaked e-mail addresses were found that were used for services from which blackmail potential is derived.

6.5 Spear Phishing Threat: 0% *

* This score has a purely informative value for the current rating.
The score does not affect the total rating.

This score rates the number of personalised e-mail addresses of the company found (e.g. firstname.surname@company.de). Such e-mail addresses can be used by hackers for spear phishing attacks. Generic e-mail addresses (e.g. info@company.de) and e-mail addresses that were deliberately published (e.g. on the company's website) are not rated negatively even though they are also part of the attack surface.

Illustrative Story

A robber found out the names of some employees. Maybe the doorman at the supplier entrance can be outsmarted if the robber pretends to be a new employee and gives the dorrman the name of a real employee.

Potential Risk

If personalised e-mail addresses are found in the darknet, hackers can use the information to launch a social engineering attack, tricking employees and gaining access to internal systems.

Claim (example)

By means of a so called "CEO Fraud" attack, hackers were able to steal € 50,000 from a car dealership. The hackers pretended to be the managing director (CEO) and instructed the secretary to transfer the money as quickly as possible. The hackers had obtained all the necessary information to carry out this attack from the darknet. The money was transferred to an account abroad and was not retrievable.

101 personal e-mail addresses were found that were not deliberately publicised by the company.