your experts in IT

UNIQ consulting

Ihr Unternehmen durch den Blickwinkel des Johari-Fensters

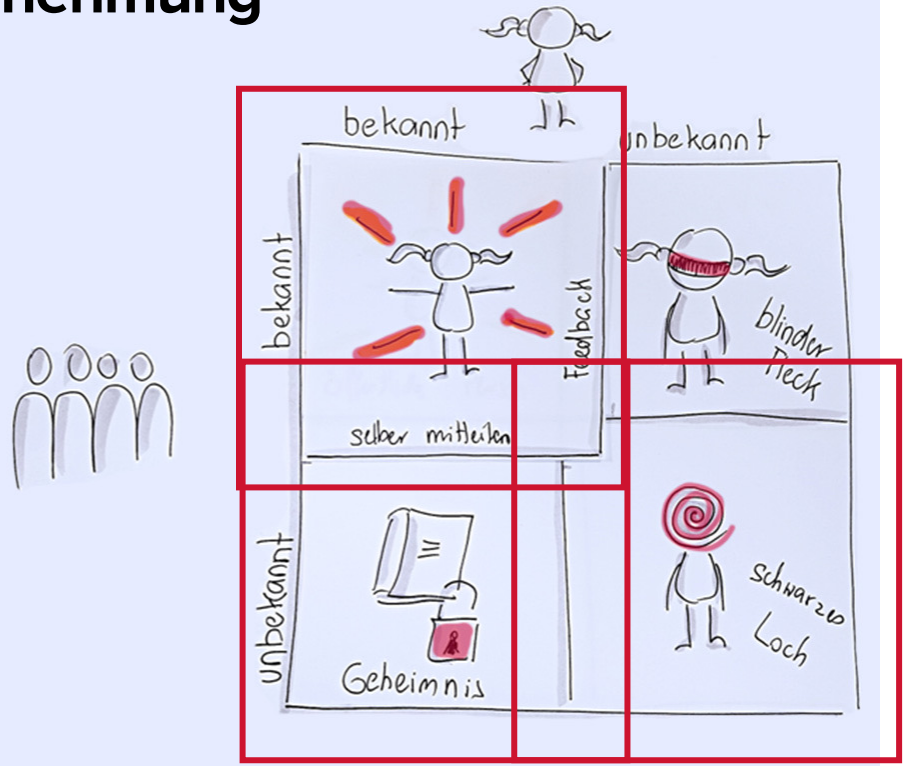
Was ist ein Johari-Fenster?

Das Johari-Fenster: Selbst- und Fremdwahrnehmung

Öffentlich – Daten die wir von unserem Unternehmen preisgeben und sichtbar machen.

Geheimnis – uns bekannte Daten, die nicht für die Aussenwelt bestimmt sind.

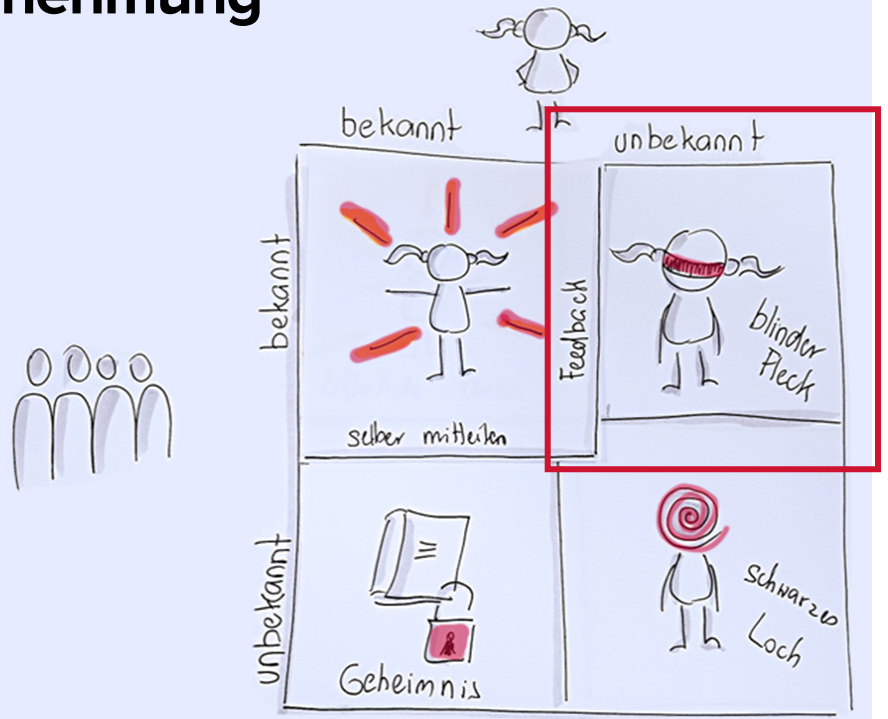
Schwarzes Loch – weder uns noch anderen bewusst oder bekannt.



Quelle: https://www.kargl.co.at/das-johari-fenster-in-der-beratung/

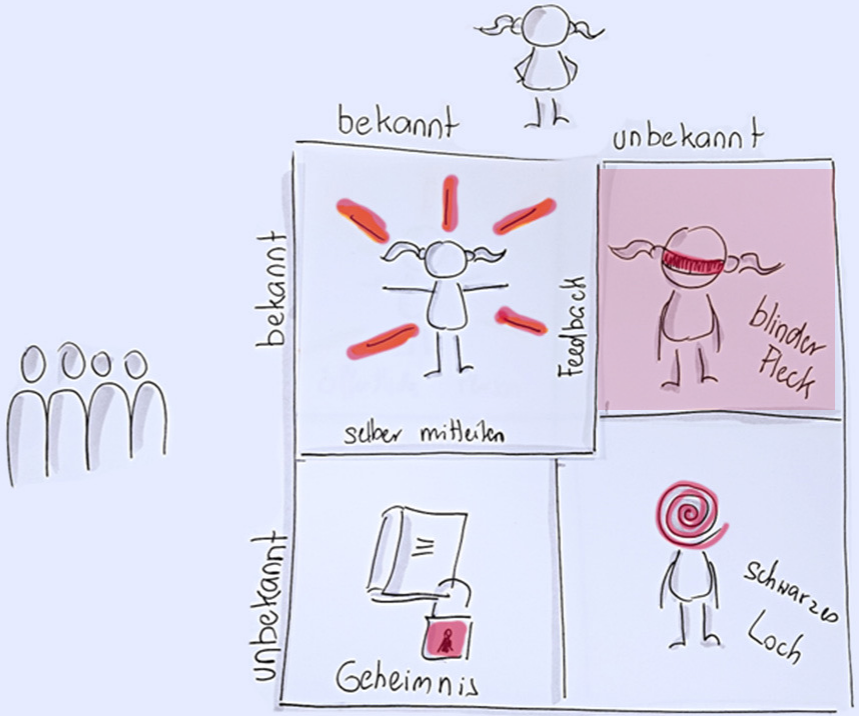
Das Johari-Fenster: Selbst- und Fremdwahrnehmung

Blinder Fleck – Kenntnisse, die andere von uns haben.
Wir jedoch nicht wissen, dass diese Kenntnisse bei Drittpersonen vorhanden sind.

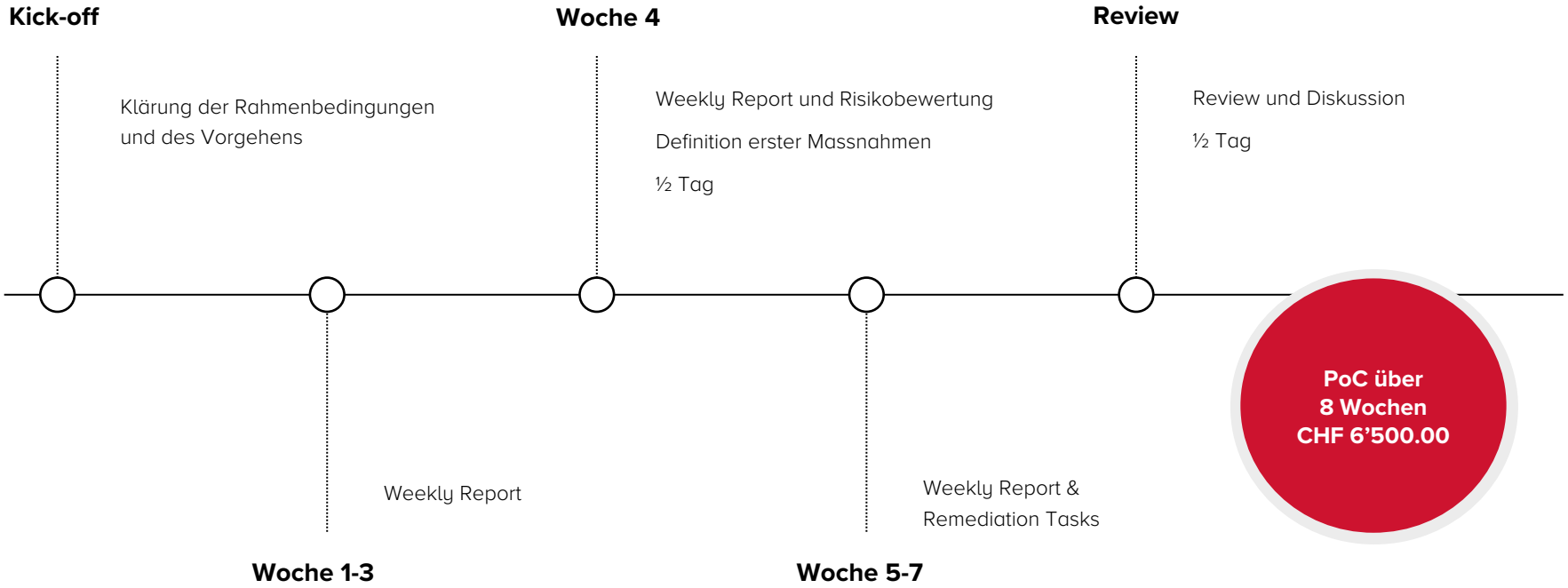


Quelle: https://www.kargl.co.at/das-johari-fenster-in-der-beratung/

Blinder Fleck bei Cyberangriffen: von Datendiebstahl bis zum Kollaps



Ablauf – Blinder Fleck



Unsere Aussicht – Ihre Risiken

Security Rating	Score	asset_title	title	description	evidence	proposed_action
e	78	https://[redacted].92	Vulnerable software found - nginx/1.14.1 (highest CVE score 7.8)	We discovered software with the following potential vulnerabilities.	headers[server] has nginx/1.14.1 CVE-2018-16845 CVE-2019-20372 CVE-2019-9511	Update the software listed in this risk, by contacting your provider or hosting party. Also, take note that this information should not be publicly accessible, as this might help the hacker in their attack preparation.
e	78	https://[redacted].82	Vulnerable software found - nginx/1.14.1 (highest CVE score 7.8)	We discovered software with the following potential vulnerabilities.	headers[server] has nginx/1.14.1 CVE-2018-16845 CVE-2019-20372 CVE-2019-9511	Update the software listed in this risk, by contacting your provider or hosting party. Also, take note that this information should not be publicly accessible, as this might help the hacker in their attack preparation.
d	50	https://[redacted].85	Open ports	Open ports found for one or several IP addresses hosting this application. Open ports can represent a risk if the services running on these ports are misconfigured or vulnerable. These can be exploited by threat actors to gain access into an internal network. More details can be found on the asset detail page of the related IP addresses.	Open ports for 212.25.2.85 - 25: smtp	Check with the administrator of the server if this open port is intentional or not
d	50	https://[redacted].92	Open ports		Open ports for 212.25.2.92 - 22: ssh	
d	50	https://[redacted].82	Open ports		Open ports for 212.25.2.82 - 4444, 2222	
d	50	https://[redacted].ch	Open ports		Open ports for 80.74.145.10 - 3306: mysql, 2121: iprop, 995: pop3s, 993: imaps, 587: submission, 465: submissions, 110: pop3, 53: domain, 25: smtp, 21: ftp	
d	50	https://[redacted].ch	Open ports		Open ports for 49.12.239.207 - 22: ssh	
d	50	https://[redacted].ch	Open ports		Open ports for 20.203.201.60 - 22: ssh	
d	50	https://[redacted].87	Open ports		Open ports for 212.25.2.87 - 10000: webmin, 22:	
d	50	https://[redacted].84	Open ports		Open ports for 212.25.2.84 - 10443	
d	50	https://[redacted].ch	Open ports		Open ports for 212.25.2.87 - 10000: webmin, 22:	
d	50	https://[redacted].ch	Open ports		Open ports for 212.25.2.84 - 10443	
d	50	https://[redacted].ch	Open ports		Open ports for 212.25.2.85 - 25: smtp	
d	50	https://[redacted].ch	Open ports		Open ports for 20.203.201.60 - 22: ssh	
d	50	https://[redacted].ch	Open ports		Open ports for 80.74.145.10 - 3306: mysql, 2121: iprop, 995: pop3s, 993: imaps, 465: submissions, 110: pop3, 53: domain, 25: smtp, 21: ftp	
c	32	https://[redacted].82	Vulnerable software found - php/7.2.24 (highest CVE score 6.4)	We discovered software with the following potential vulnerabilities.	headers[x-powered-by] has PHP/7.2.24 CVE-2019-11044 CVE-2019-11045	Update the software listed in this risk, by contacting your provider or hosting party. Also, take note that this information should not be publicly accessible, as this might help the hacker in their attack preparation.
c	21	https://[redacted].com	Vulnerable software found - jquery ui/1.12.0 (highest CVE score 4.3)		scripts has 1.12.0/jquery-ui.min.js, scripts has jquery-ui.min.js CVE-2021-41182	
b	19	https://[redacted].ch	Excessive cookie lifetime (> 1 year)	Cookies can be used to identify individuals. Long expiration periods allow for persistent visitor tracking and can pose a GDPR compliancy issue.	The following cookies have an incorrect lifetime: _ga - 11 Sep 2025 _ga_FGNZE1LMRT - 11 Sep 2025	Reduce the cookie expiration period by limiting the Max-Age setting in your website configuration
b	19	https://[redacted].ch	Cookies set without visitor consent	Setting cookies without obtaining consent from visitors first may pose a GDPR compliancy issue.	The following cookies are set without consent: JSESSIONID	Do not set cookies before obtaining consent from website visitors
b	10	https://[redacted].ch	X-Frame-Options header missing	The X-Frame-Options header protects websites against clickjacking attacks. Sometimes, this is not possible to implement. If that is the case, mark this risk as manually mitigated.	X-Frame-Options missing in headers. Headers found: Date, Etag, Server, Status, Content-Type, Accept-Ranges, Last-Modified, Content-Length, Www-Authenticate	Turn on the X-Frame-Options header in your web server software
b	10	https://[redacted].ch	HSTS header missing	The HSTS header enforces users to always visit your website through SSL, after their first visit.	No HSTS header present.	Turn on the HSTS header, read more on https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
b	10	[redacted].ch	E-mail spoofing possible (no SPF)	Your domain does not have an SPF record. This means other people can use your organization's email addresses in spoofing campaigns. This will most likely lead to abuse of your brand and reputation.	No SPF record found	Implement the SPF record within the DNS configuration for domain aov.uniqconsulting.ch
b	10	[redacted].com	E-mail spoofing possible (no SPF)		No SPF record found	Implement the SPF record within the DNS configuration for domain www.uniqconsulting.com

Unsere Aussicht – Ihre Risiken

e	78	https://[redacted].92	Vulnerable software found - nginx/1.14.1 (highest CVE score 7.8)	We discovered software with the following potential vulnerabilities.	headers[server] has nginx/1.14.1 CVE-2018-16845 CVE-2019-20372 CVE-2019-9511
d	50	https://[redacted].ch	Open ports	Open ports found for one or several IP addresses hosting this application. Open ports can represent a risk if the services running on these ports are misconfigured or vulnerable. These can be exploited by threat actors to gain access into an internal network. More details can be found on the asset detail page of the related IP addresses.	Open ports for 80.74.145.10 - 3306: mysql, 2121: iprop, 995: pop3s, 993: imaps, 587: submission, 465: submissions, 110: pop3, 53: domain, 25: smtp, 21: ftp
d	50	https://[redacted].ch	Open ports		Open ports for 49.12.239.207 - 22: ssh
d	50	https://[redacted].ch	Open ports		Open ports for 20.203.201.60 - 22: ssh
d	50	https://[redacted].87	Open ports		Open ports for 212.25.2.87 - 10000: webmin, 22:
d	50	https://[redacted].84	Open ports		Open ports for 212.25.2.84 - 10443
d	50	https://[redacted].ch	Open ports		Open ports for 212.25.2.87 - 10000: webmin, 22:
d	50	https://[redacted].ch	Open ports		Open ports for 212.25.2.84 - 10443
d	50	https://[redacted].ch	Open ports		Open ports for 212.25.2.85 - 25: smtp
c	32	https://[redacted].82	Vulnerable software found - php/7.2.24 (highest CVE score 6.4)	We discovered software with the following potential vulnerabilities.	headers[x-powered-by] has PHP/7.2.24 CVE-2019-11044
c	21	https://[redacted].com	Vulnerable software found - jquery ui/1.12.0 (highest CVE score 4.3)		scripts has 1.12.0/jquery-ui.min.js, scripts has jquery-ui.min.js
b	19	https://[redacted].ch	Excessive cookie lifetime (> 1 year)	Cookies can be used to identify individuals. Long expiration periods allow for persistent visitor tracking and can pose a GDPR compliancy issue.	The following cookies have an incorrect lifetime: _ga - 11 Sep 2025 _ga_FGNZE1LMRT - 11 Sep 2025
b	19	https://[redacted].ch	Cookies set without visitor consent	Setting cookies without obtaining consent from visitors first may pose a GDPR compliancy issue.	The following cookies are set without consent: JSESSIONID

Darknet Monitoring

Publish date	Domain	Email	Email Username	Email Domain	Password Type	Breach Title	Breach Acquisition Date
2023-04-14T00:00:00Z	[redacted]	[redacted]	[redacted]	[redacted]	plaintext	International Combolist	2017-03-01T00:00:00Z
2023-04-14T00:00:00Z	[redacted]	[redacted]	[redacted]	[redacted]	plaintext	International Combolist	2017-03-01T00:00:00Z
2021-04-08T00:00:00Z	[redacted]	[redacted]	[redacted]	[redacted]	plaintext	March 2021 Combolist	2021-03-12T00:00:00Z
2019-02-06T00:00:00Z	[redacted]	[redacted]	[redacted]	[redacted]	plaintext	Collection #4 Combo List	2019-01-17T00:00:00Z
2019-02-06T00:00:00Z	[redacted]	[redacted]	[redacted]	[redacted]	plaintext	Collection #5 Combo List	2019-01-17T00:00:00Z
2019-02-06T00:00:00Z	[redacted]	[redacted]	[redacted]	[redacted]	plaintext	2019 Antipublic Combo List	2019-01-17T00:00:00Z
2019-02-06T00:00:00Z	[redacted]	[redacted]	[redacted]	[redacted]	plaintext	2019 Antipublic Combo List	2019-01-17T00:00:00Z
2019-02-06T00:00:00Z	[redacted]	[redacted]	[redacted]	[redacted]	plaintext	Collection #4 Combo List	2019-01-17T00:00:00Z
2019-02-06T00:00:00Z	[redacted]	[redacted]	[redacted]	[redacted]	plaintext	AP MYR and Zabugor Combo List	2019-01-17T00:00:00Z
2019-01-29T00:00:00Z	[redacted]	[redacted]	[redacted]	[redacted]	plaintext	Collection #2 Combo List	2019-01-17T00:00:00Z
2019-01-29T00:00:00Z	[redacted]	[redacted]	[redacted]	[redacted]	plaintext	Collection #2 Combo List	2019-01-17T00:00:00Z
2019-01-25T00:00:00Z	[redacted]	[redacted]	[redacted]	[redacted]	plaintext	Collection #1 Combo List	2019-01-17T00:00:00Z
2018-12-20T00:00:00Z	[redacted]	[redacted]	[redacted]	[redacted]	plaintext	Sensitive Source	2018-11-30T00:00:00Z
2018-12-20T00:00:00Z	[redacted]	[redacted]	[redacted]	[redacted]	plaintext	Sensitive Source	2018-11-30T00:00:00Z
2018-12-20T00:00:00Z	[redacted]	[redacted]	[redacted]	[redacted]	plaintext	Sensitive Source	2018-11-30T00:00:00Z
2017-12-22T00:00:00Z	[redacted]	[redacted]	[redacted]	[redacted]	plaintext	Combolist of 1.4 Billion Credentials	2017-12-01T00:00:00Z

Herzlichen Dank für Ihre Aufmerksamkeit.

uniQconsulting ag
Grindelstrasse 9
CH-8303 Bassersdorf

044 838 64 64
info@uniQcosulting.ch
uniQconsulting.ch

uniQconsulting ag
Schützengraben 21
CH-4051 Basel

uniQconsulting ag
Haltelhusstrasse 1
CH-9402 Mörschwil