German American Chambers of Commerce
Deutsch-Amerikanische Handelskammern

TeleTrusT
Pioneers in IT security.
IT Security Association Germany

German-American IT Security Forum

IT Security Association Germany (TeleTrusT) in cooperation with GACC – German American Chamber of Commerce

San Francisco, 06.05.2024

Vendor Risk Management: Your Invisible Shield in the Digital Supply Chain

Lukas Baumann, Founder & CEO LocateRisk

Risks Only Exist for Others!

Risk assessment

less than 250 million turnover: 30% for yourself, 79% for others

0.250 to 3 billion turnover: 41% for yourself, 84% for others

more than 3 billion turnover: 34% for yourself, 84% for others

Self-assessment of the level of protection vs affectedness

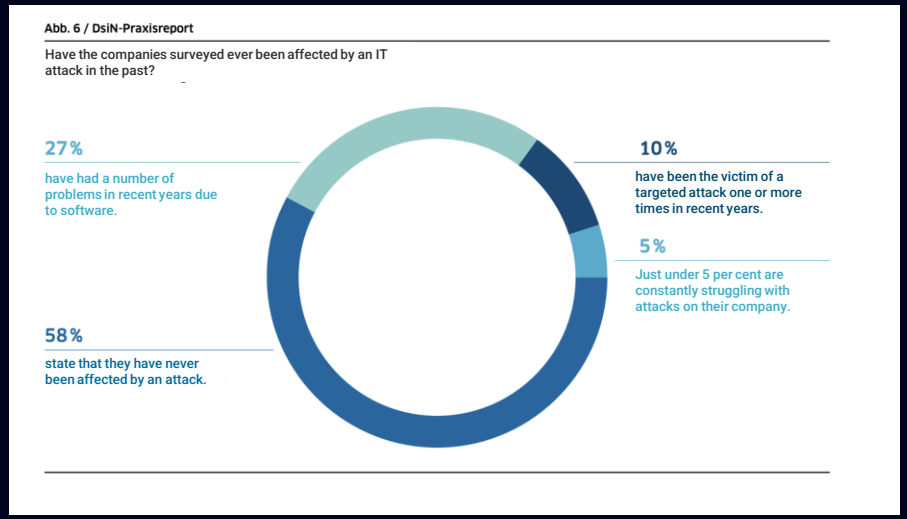
less than 250 million turnover: 89% level of protection, 30% affected

0.250 to 3 billion turnover: 92% protection level, 36% concern

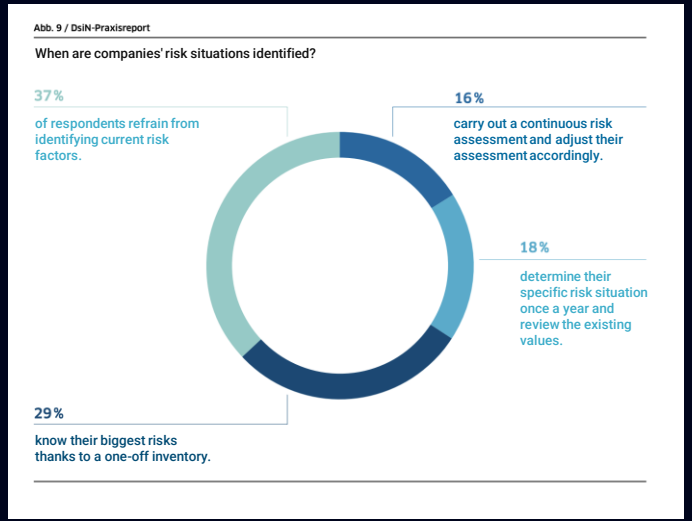
more than 3 billion turnover: 97% protection level, 45% concern

Source: KPMG study "White-collar crime in Germany 2023: Against every rule",
Survey of 1,001 representatively selected companies of various sectors and sizes in 2022

Discrepancy between Risk Situation and Risk Identification



42% of SMEs have experienced cyberattacks



only 16% carry out continuous risk assessment

→ Germany has a lot of catching up to do

Source: DsiN-Praxisreport 2021/22 SMEs @ IT security, Survey of 1,339 companies

The IT Security Status of 3.609 German Organisations Shows Significant Problems!

- Database systems found
- No database systems found

44%

Do not protect all their database systems adequately from cyber attacks

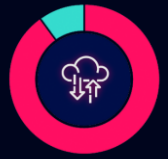
Facilitates the access to more systems and sensitive data

- Partly unprotected email dispatch
- Protected email dispatch

53%

Send emails partly unprotected

Enables spam and phishing attacks by fake mails



- Use of invalid encoding
- Use of up to date procedures

90%

Allow data transfer with outdated encoding

Facilitates data theft

- Have at least one application with an unpatched big security breach
- Do not have an application with an unpatched big security breach

43%

Use at least one application with a critical unpatched security breach

Opens the door for attackers

- Use tracking cookies without user permission
- Do not use cookies without user permission

35%

Use tracking cookies without user's consent

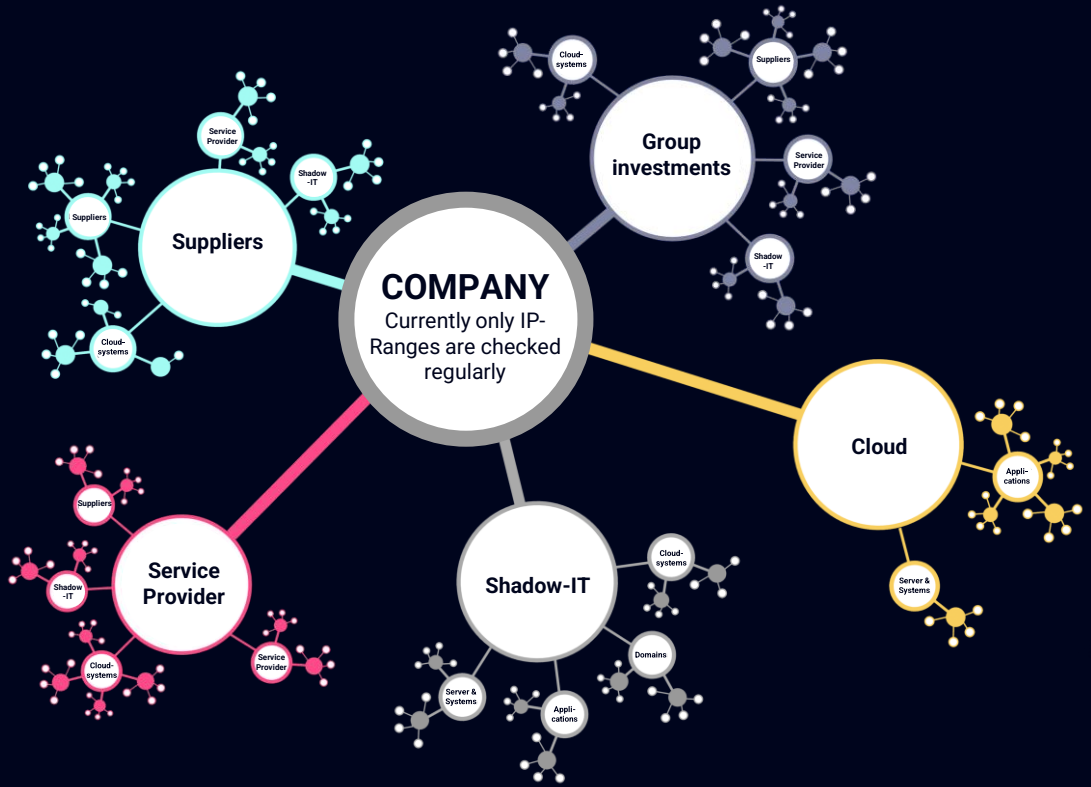
Risk of warning letters and fines

IT-Security is often treated superficially in everyday business.

Source: LocateRisk Data Report Cybersecurity 2021 - Review of more than 3,609 organisations - Survey Period: 2020/21

LocateRisk

The IT Attack Surface Becomes Unmanageable



Why Is No One Talking About the Problem?

Management and IT do not have a common basis for assessing the enterprise-wide cyber security posture.

LocateRisk

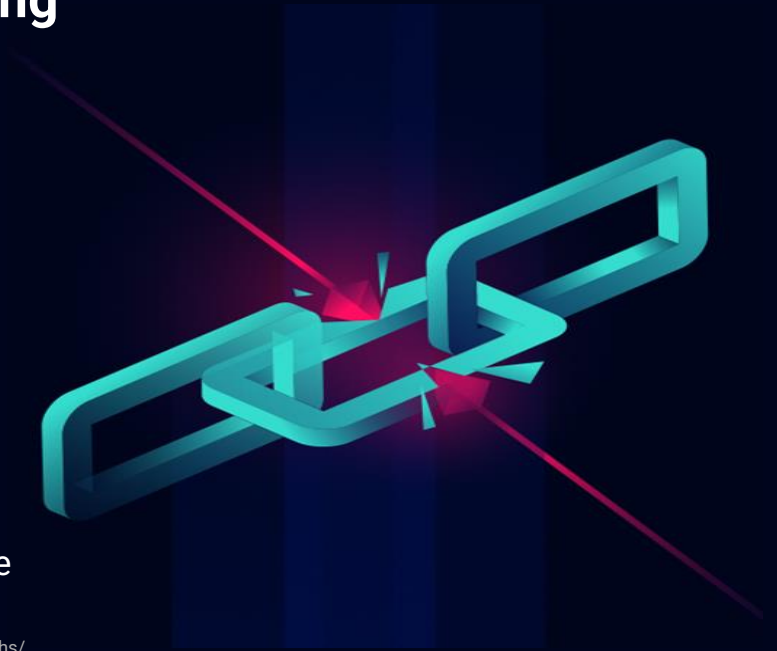
Suddenly, Supplier Hacks Changed Everything

OKTA (authentication service provider) affected 375 customers

SolarWinds affected 18,000

COUNT+CARE (Darmstadt, Entega)

→ Hack one, breach many



> 54% of organizations breached through third parties in the last 12 months
> https://venturebeat.com/security/report-54-of-organizations-breached-through-3rd-parties-in-last-12-months/

Within supply-chains the weakest link of the chain is crucial.

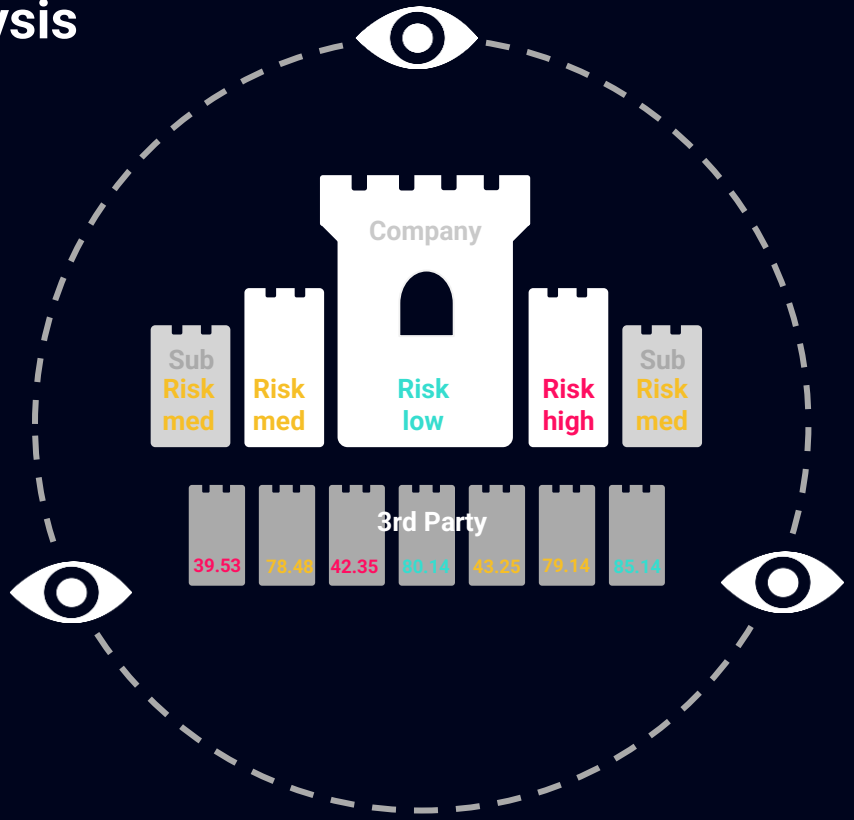
LocateRisk

Our Solution: Automated Analysis and Monitoring of the Attack Surface

We measure, evaluate and compare the security posture

of companies, their holdings and third-party companies

in an automated process to mitigate cyber risks.



What We Find ...

Charging station in municipal IT. No one knew where it came from, who owned it, where it was located.

Surveillance camera streaming prototype images from a sports car manufacturer's factory floor onto the web.

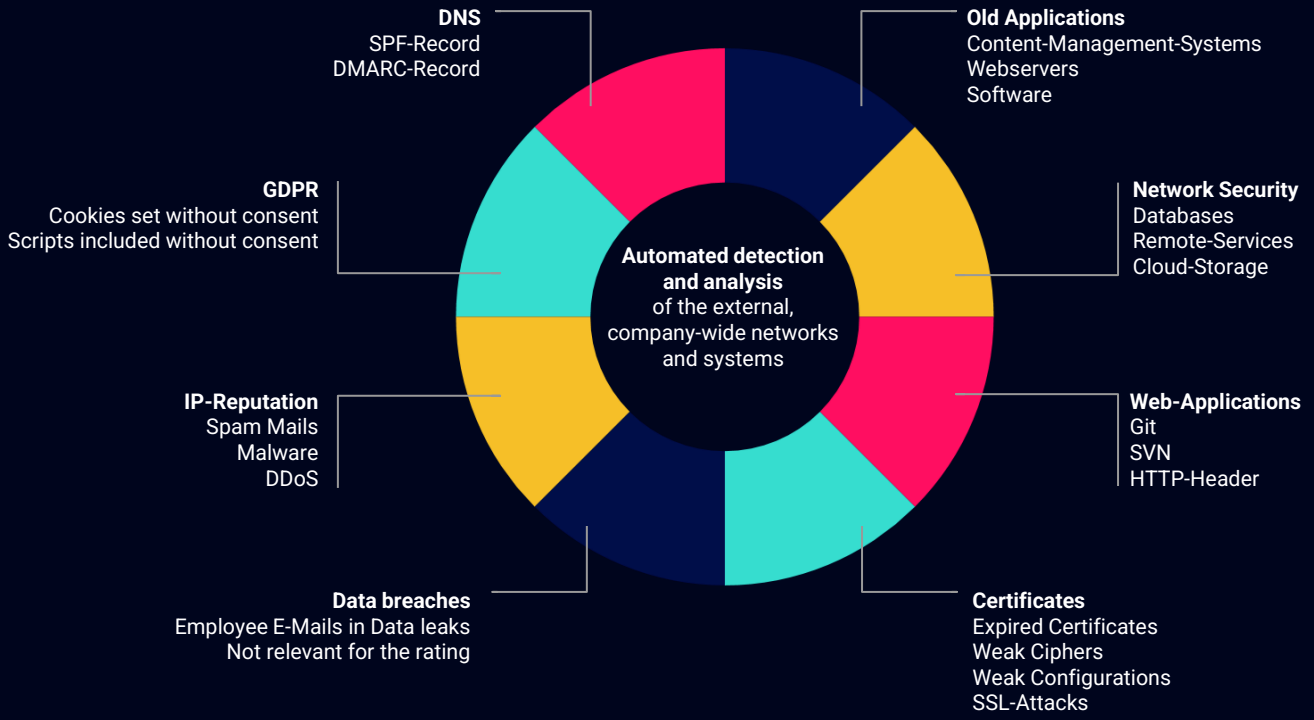
Webshop02.company.de with error message containing password for mail server.

GIT directories with passwords for anything.

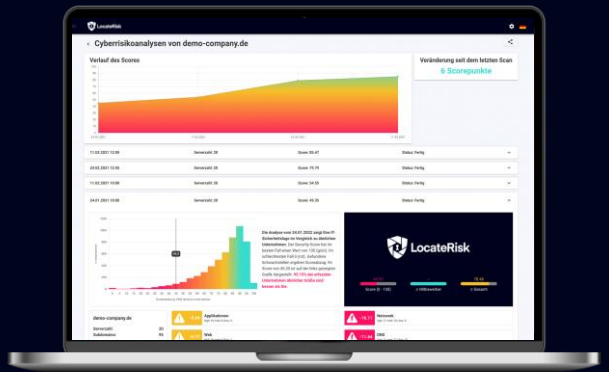
System backups for everyone to download.

The payment management system of an online shop could be viewed and manipulated throughout the internet.

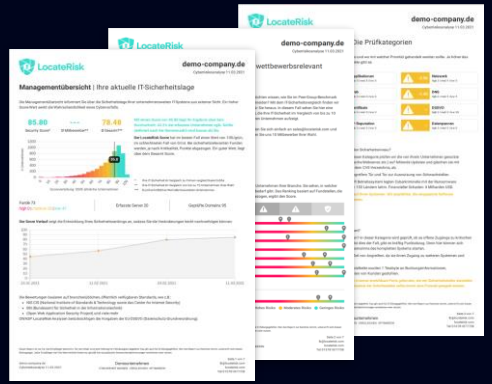
What Exactly Is Being Tested?



Result: Documented Security as Proof for Third Parties



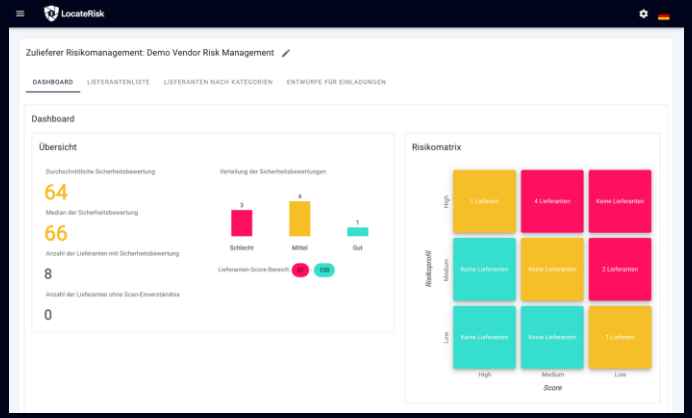
In-depth vulnerability list with recommendations for action, action plan and useful functions for IT managers. Configure. Filter. Delegate. Export.

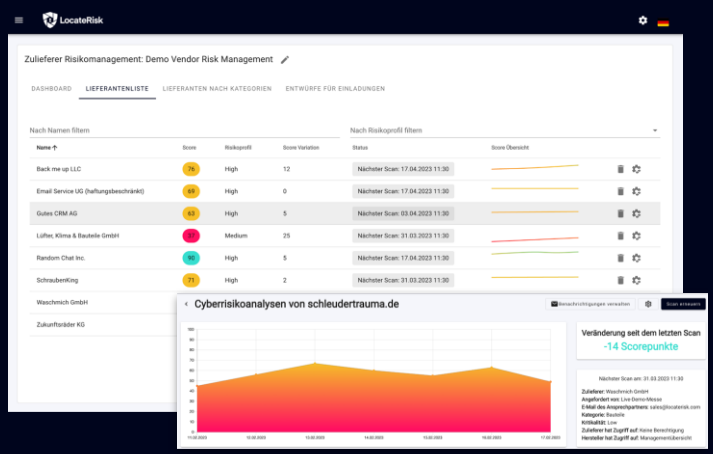


Exportable, condensed management report with clear graphics and understandable explanations.

Security proof vis-à-vis third parties.

Fully Automated Cyber Vendor Risk Management





Protect your business from potential risks by implementing an automated vendor risk management (VRM) solution that ensures all suppliers are within your risk tolerance level.

Capture all risk findings and alerts related to your third-party provider's security posture in a single reporting format and make better decisions based on objective facts.

Case Study: Direct Marketer of Electricity

Customer
One of the largest direct marketers of electricity from renewables in Germany. CRITIS operator – Has to ensure security of supply and grid stability.

Goal
Keep continuously determined, reliable security data ready for regular audit appointments.

Solution
Automated monthly monitoring of the attack surface replaces the previously manual identification of vulnerabilities.

Import internal scans for ALL IN ONE Vulnerability Management Dashboard.

Scan external Vendors for their security posture.

Result
Time savings & More resources for important things.

Progress of work is documented & Company is well prepared for audits.

Critical infrastructure requirements are met faster.

Benefits

Preventive instead of reactive/cyber hygiene

Minimise the attack surface continuously and efficiently, through automated analyses & monitoring.

Time saving

Automatic asset recognition
+
Functions that speed up the security process.

NIS2, DORA & TISAX ready

Measuring the effectiveness of information security
+
Automate supply chain auditing.

More Than 700 Customers

References

17 cities

8 counties

10 utility companies

More than 670 others

Mentioned in

FAZ

Süddeutsche

Zeit online

Heise online
and more

1st prize
Sparkassenversicherung Insurathon

3rd prize
Accelerator Programme for cyber- security start-ups ‘SpeedUpSecure’

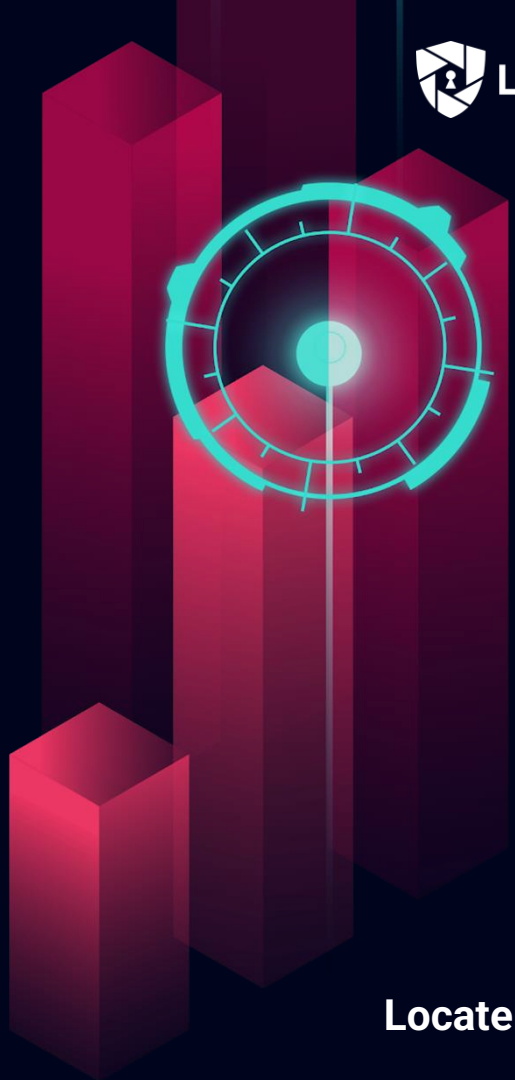
Nominated by the international expert organisation DEKRA

+ 100

LocateRisk

Feel free to check us out with a Live Demo!

Lukas Baumann
LB@LocateRisk.com
+49 6151 6290246



LocateRisk.com