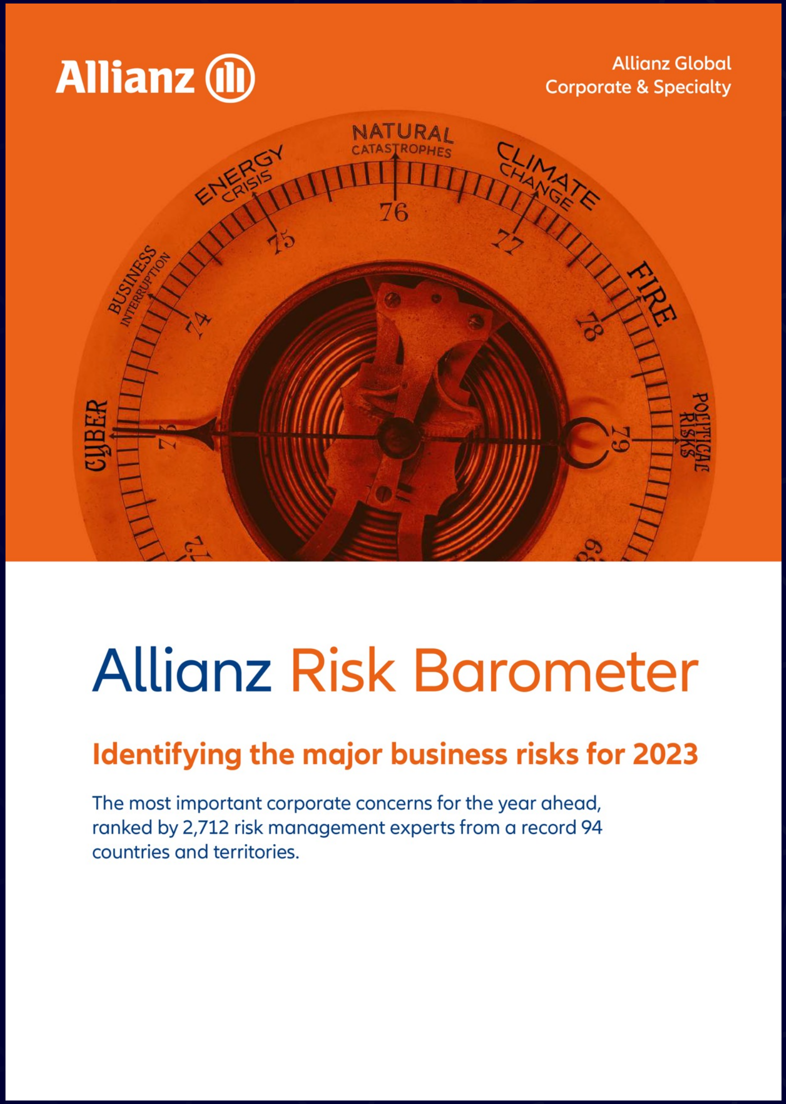
XM Cyber
A Schwarz Company

Cyberkriminalität – eine Gefahr für jeden

Mit den Augen des Angreifers Gefahren erkennen

Rolf Schumann
Vorstandsvorsitzender Schwarz Digital

12/05/2023



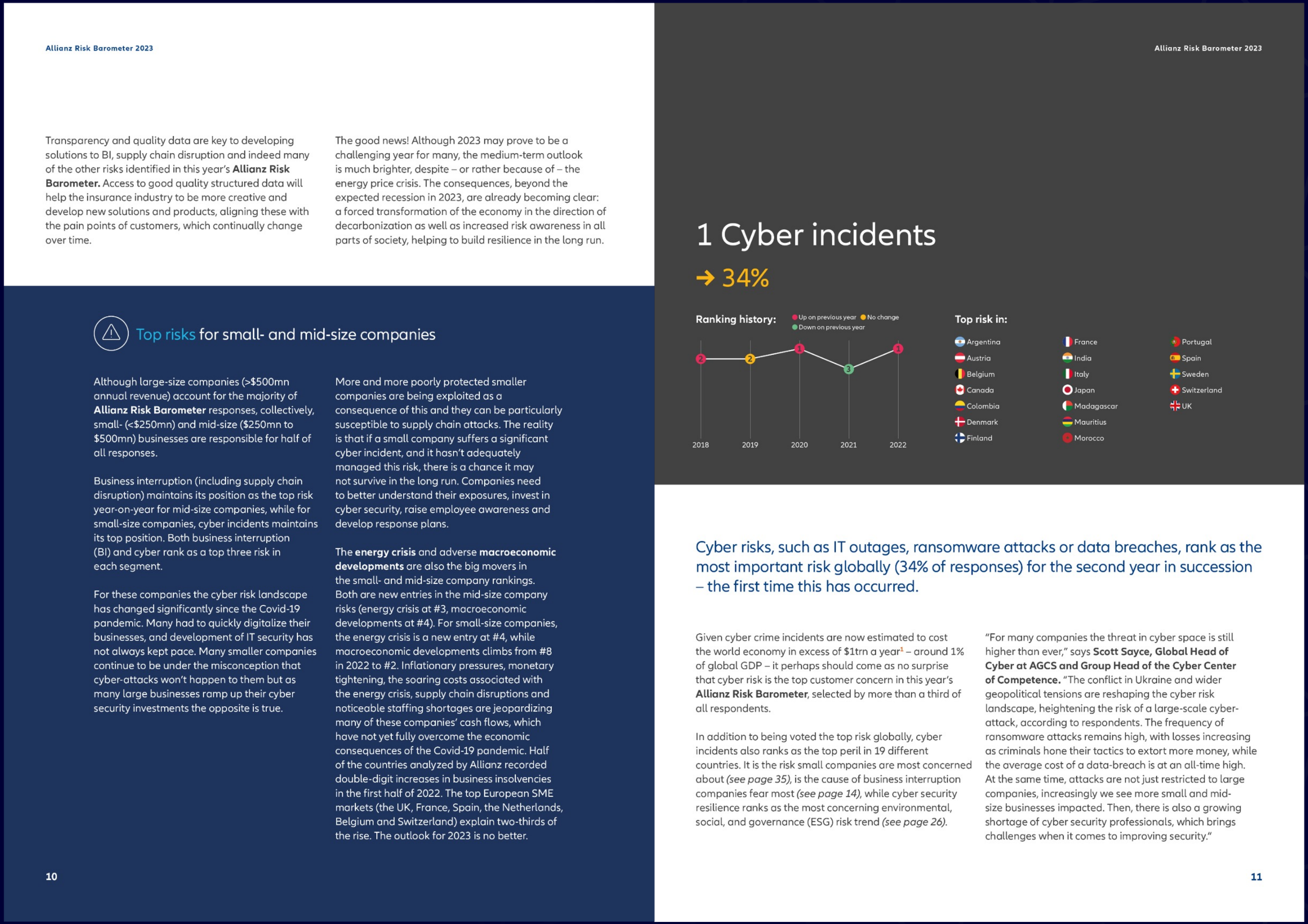
Allianz

Allianz Global Corporate & Specialty

Allianz Risk Barometer

Identifying the major business risks for 2023

The most important corporate concerns for the year ahead, ranked by 2,712 risk management experts from a record 94 countries and territories.



Transparency and quality data are key to developing solutions to BI, supply chain disruption and indeed many of the other risks identified in this year's **Allianz Risk Barometer.** Access to good quality structured data will help the insurance industry to be more creative and develop new solutions and products, aligning these with the pain points of customers, which continually change over time.

The good news! Although 2023 may prove to be a challenging year for many, the medium-term outlook is much brighter, despite – or rather because of – the energy price crisis. The consequences, beyond the expected recession in 2023, are already becoming clear: a forced transformation of the economy in the direction of decarbonization as well as increased risk awareness in all parts of society, helping to build resilience in the long run.

⚠ Top risks for small- and mid-size companies

Although large-size companies (>$500mn annual revenue) account for the majority of **Allianz Risk Barometer** responses, collectively, small- (<$250mn) and mid-size ($250mn to $500mn) businesses are responsible for half of all responses.

Business interruption (including supply chain disruption) maintains its position as the top risk year-on-year for mid-size companies, while for small-size companies, cyber incidents maintains its top position. Both business interruption (BI) and cyber rank as a top three risk in each segment.

For these companies the cyber risk landscape has changed significantly since the Covid-19 pandemic. Many had to quickly digitalize their businesses, and development of IT security has not always kept pace. Many smaller companies continue to be under the misconception that cyber-attacks won't happen to them but as many large businesses ramp up their cyber security investments the opposite is true.

More and more poorly protected smaller companies are being exploited as a consequence of this and they can be particularly susceptible to supply chain attacks. The reality is that if a small company suffers a significant cyber incident, and it hasn't adequately managed this risk, there is a chance it may not survive in the long run. Companies need to better understand their exposures, invest in cyber security, raise employee awareness and develop response plans.

The **energy crisis** and adverse **macroeconomic developments** are also the big movers in the small- and mid-size company rankings. Both are new entries in the mid-size company risks (energy crisis at #3, macroeconomic developments at #4). For small-size companies, the energy crisis is a new entry at #4, while macroeconomic developments climbs from #8 in 2022 to #2. Inflationary pressures, monetary tightening, the soaring costs associated with the energy crisis, supply chain disruptions and noticeable staffing shortages are jeopardizing many of these companies' cash flows, which have not yet fully overcome the economic consequences of the Covid-19 pandemic. Half of the countries analyzed by Allianz recorded double-digit increases in business insolvencies in the first half of 2022. The top European SME markets (the UK, France, Spain, the Netherlands, Belgium and Switzerland) explain two-thirds of the rise. The outlook for 2023 is no better.

1 Cyber incidents

→ 34%

Ranking history:

Top risk in:

Argentina
Austria
Belgium
Canada
Colombia
Denmark
Finland

France
India
Italy
Japan
Madagascar
Mauritius
Morocco

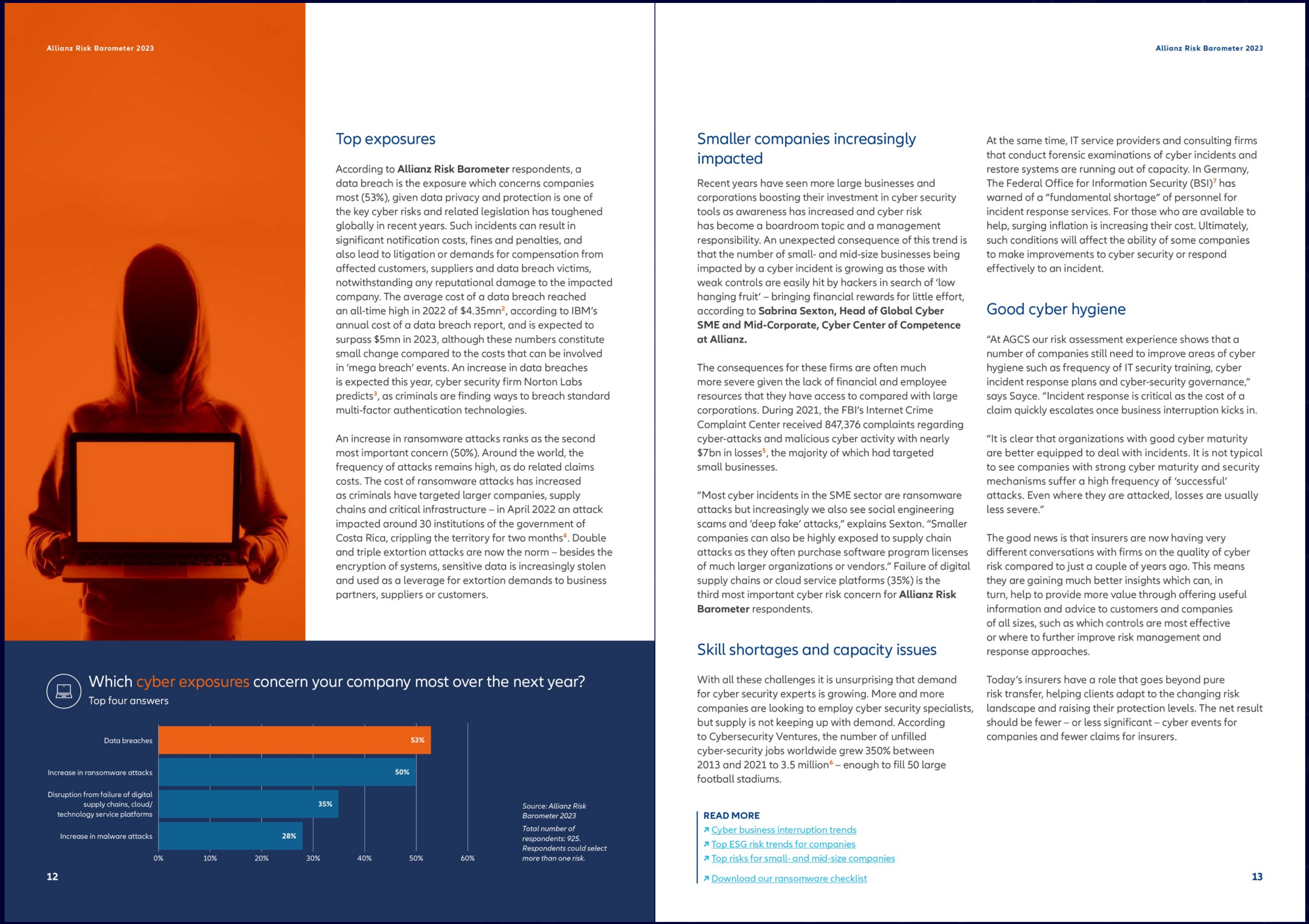
Portugal
Spain
Sweden
Switzerland
UK

Cyber risks, such as IT outages, ransomware attacks or data breaches, rank as the most important risk globally (34% of responses) for the second year in succession – the first time this has occurred.

Given cyber crime incidents are now estimated to cost the world economy in excess of $1trn a year[1] – around 1% of global GDP – it perhaps should come as no surprise that cyber risk is the top customer concern in this year's **Allianz Risk Barometer**, selected by more than a third of all respondents.

In addition to being voted the top risk globally, cyber incidents also ranks as the top peril in 19 different countries. It is the risk small companies are most concerned about *(see page 35)*, is the cause of business interruption companies fear most *(see page 14)*, while cyber security resilience ranks as the most concerning environmental, social, and governance (ESG) risk trend *(see page 26)*.

"For many companies the threat in cyber space is still higher than ever," says **Scott Sayce, Global Head of Cyber at AGCS and Group Head of the Cyber Center of Competence.** "The conflict in Ukraine and wider geopolitical tensions are reshaping the cyber risk landscape, heightening the risk of a large-scale cyber-attack, according to respondents. The frequency of ransomware attacks remains high, with losses increasing as criminals hone their tactics to extort more money, while the average cost of a data-breach is at an all-time high. At the same time, attacks are not just restricted to large companies, increasingly we see more small and mid-size businesses impacted. Then, there is also a growing shortage of cyber security professionals, which brings challenges when it comes to improving security."



Top exposures

According to **Allianz Risk Barometer** respondents, a data breach is the exposure which concerns companies most (53%), given data privacy and protection is one of the key cyber risks and related legislation has toughened globally in recent years. Such incidents can result in significant notification costs, fines and penalties, and also lead to litigation or demands for compensation from affected customers, suppliers and data breach victims, notwithstanding any reputational damage to the impacted company. The average cost of a data breach reached an all-time high in 2022 of $4.35mn[2], according to IBM's annual cost of a data breach report, and is expected to surpass $5mn in 2023, although these numbers constitute small change compared to the costs that can be involved in 'mega breach' events. An increase in data breaches is expected this year, cyber security firm Norton Labs predicts[3], as criminals are finding ways to breach standard multi-factor authentication technologies.

An increase in ransomware attacks ranks as the second most important concern (50%). Around the world, the frequency of attacks remains high, as do related claims costs. The cost of ransomware attacks has increased as criminals have targeted larger companies, supply chains and critical infrastructure – in April 2022 an attack impacted around 30 institutions of the government of Costa Rica, crippling the territory for two months[4]. Double and triple extortion attacks are now the norm – besides the encryption of systems, sensitive data is increasingly stolen and used as a leverage for extortion demands to business partners, suppliers or customers.

Which cyber exposures concern your company most over the next year?
Top four answers

Data breaches	53%
Increase in ransomware attacks	50%
Disruption from failure of digital supply chains, cloud/ technology service platforms	35%
Increase in malware attacks	28%

0% 10% 20% 30% 40% 50% 60%

Source: Allianz Risk Barometer 2023

Total number of respondents: 925. Respondents could select more than one risk.

Smaller companies increasingly impacted

Recent years have seen more large businesses and corporations boosting their investment in cyber security tools as awareness has increased and cyber risk has become a boardroom topic and a management responsibility. An unexpected consequence of this trend is that the number of small- and mid-size businesses being impacted by a cyber incident is growing as those with weak controls are easily hit by hackers in search of 'low hanging fruit' – bringing financial rewards for little effort, according to **Sabrina Sexton, Head of Global Cyber SME and Mid-Corporate, Cyber Center of Competence at Allianz.**

The consequences for these firms are often much more severe given the lack of financial and employee resources that they have access to compared with large corporations. During 2021, the FBI's Internet Crime Complaint Center received 847,376 complaints regarding cyber-attacks and malicious cyber activity with nearly $7bn in losses[5], the majority of which had targeted small businesses.

"Most cyber incidents in the SME sector are ransomware attacks but increasingly we also see social engineering scams and 'deep fake' attacks," explains Sexton. "Smaller companies can also be highly exposed to supply chain attacks as they often purchase software program licenses of much larger organizations or vendors." Failure of digital supply chains or cloud service platforms (35%) is the third most important cyber risk concern for **Allianz Risk Barometer** respondents.

Skill shortages and capacity issues

With all these challenges it is unsurprising that demand for cyber security experts is growing. More and more companies are looking to employ cyber security specialists, but supply is not keeping up with demand. According to Cybersecurity Ventures, the number of unfilled cyber-security jobs worldwide grew 350% between 2013 and 2021 to 3.5 million[6] – enough to fill 50 large football stadiums.

At the same time, IT service providers and consulting firms that conduct forensic examinations of cyber incidents and restore systems are running out of capacity. In Germany, The Federal Office for Information Security (BSI)[7] has warned of a "fundamental shortage" of personnel for incident response services. For those who are available to help, surging inflation is increasing their cost. Ultimately, such conditions will affect the ability of some companies to make improvements to cyber security or respond effectively to an incident.

Good cyber hygiene

"At AGCS our risk assessment experience shows that a number of companies still need to improve areas of cyber hygiene such as frequency of IT security training, cyber incident response plans and cyber-security governance," says Sayce. "Incident response is critical as the cost of a claim quickly escalates once business interruption kicks in.

"It is clear that organizations with good cyber maturity are better equipped to deal with incidents. It is not typical to see companies with strong cyber maturity and security mechanisms suffer a high frequency of 'successful' attacks. Even where they are attacked, losses are usually less severe."

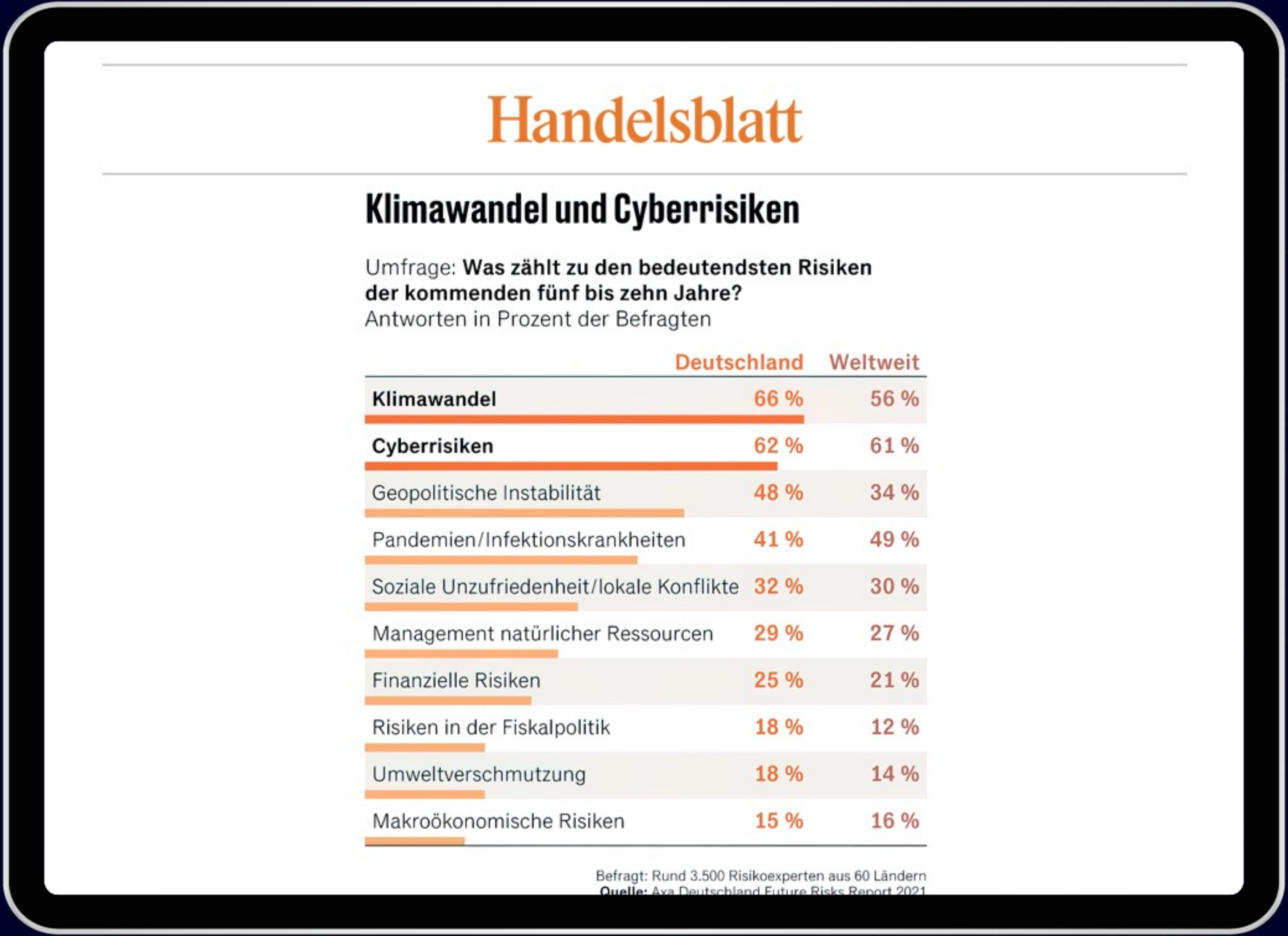
The good news is that insurers are now having very different conversations with firms on the quality of cyber risk compared to just a couple of years ago. This means they are gaining much better insights which can, in turn, help to provide more value through offering useful information and advice to customers and companies of all sizes, such as which controls are most effective or where to further improve risk management and response approaches.

Today's insurers have a role that goes beyond pure risk transfer, helping clients adapt to the changing risk landscape and raising their protection levels. The net result should be fewer – or less significant – cyber events for companies and fewer claims for insurers.

READ MORE
↗ Cyber business interruption trends
↗ Top ESG risk trends for companies
↗ Top risks for small- and mid-size companies

↗ Download our ransomware checklist

Nach der Krise ist vor der Krise – was bleibt?



Handelsblatt

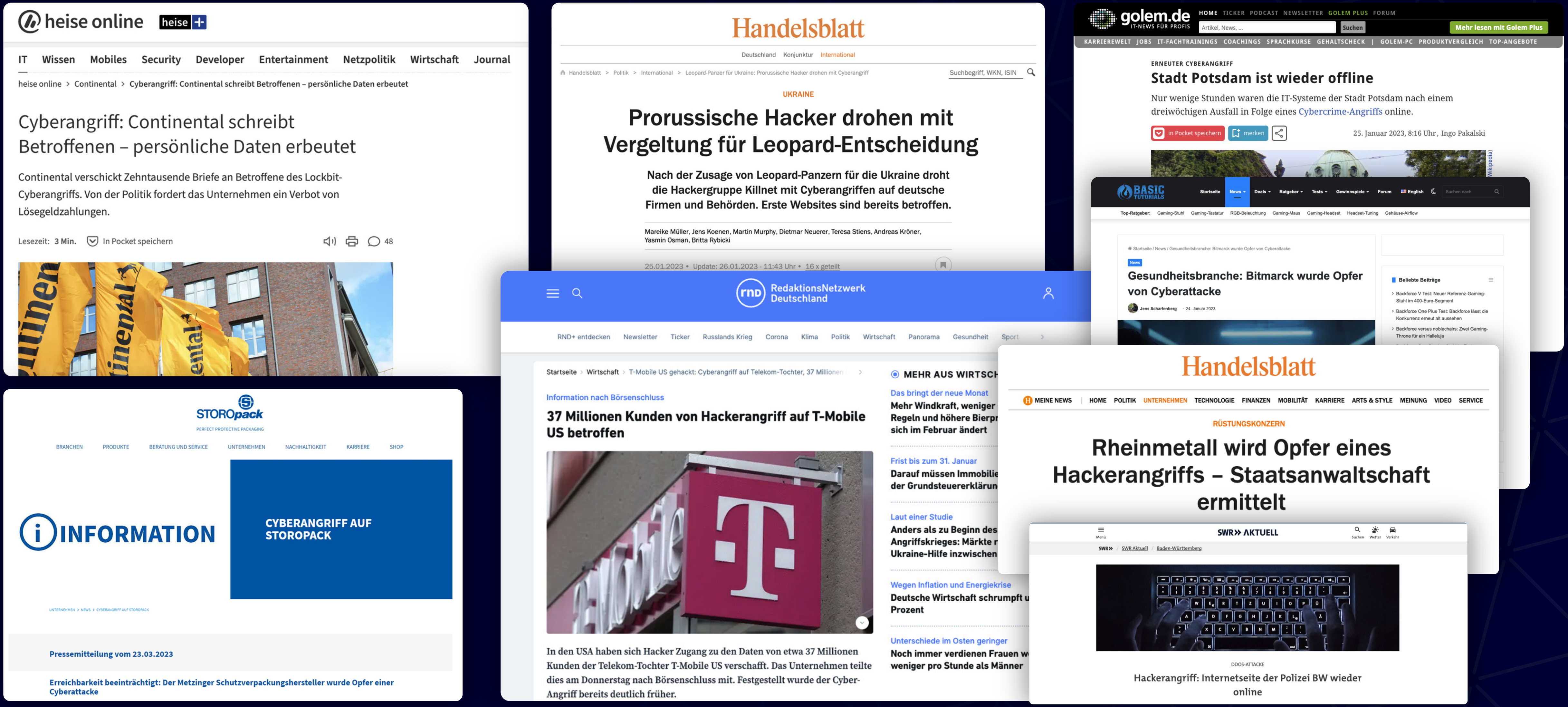
Klimawandel und Cyberrisiken

Umfrage: **Was zählt zu den bedeutendsten Risiken der kommenden fünf bis zehn Jahre?**
Antworten in Prozent der Befragten

	Deutschland	Weltweit
Klimawandel	66 %	56 %
Cyberrisiken	62 %	61 %
Geopolitische Instabilität	48 %	34 %
Pandemien/Infektionskrankheiten	41 %	49 %
Soziale Unzufriedenheit/lokale Konflikte	32 %	30 %
Management natürlicher Ressourcen	29 %	27 %
Finanzielle Risiken	25 %	21 %
Risiken in der Fiskalpolitik	18 %	12 %
Umweltverschmutzung	18 %	14 %
Makroökonomische Risiken	15 %	16 %

Befragt: Rund 3.500 Risikoexperten aus 60 Ländern
Quelle: Axa Deutschland Future Risks Report 2021

Cyber-Angriffe der letzten Wochen



heise online heise+

IT Wissen Mobiles Security Developer Entertainment Netzpolitik Wirtschaft Journal

heise online > Continental > Cyberangriff: Continental schreibt Betroffenen – persönliche Daten erbeutet

Cyberangriff: Continental schreibt Betroffenen – persönliche Daten erbeutet

Continental verschickt Zehntausende Briefe an Betroffene des Lockbit-Cyberangriffs. Von der Politik fordert das Unternehmen ein Verbot von Lösegeldzahlungen.

Lesezeit: 3 Min. In Pocket speichern 48

Handelsblatt

Deutschland Konjunktur International

Handelsblatt > Politik > International > Leopard-Panzer für Ukraine: Prorussische Hacker drohen mit Cyberangriff

Suchbegriff, WKN, ISIN

UKRAINE

Prorussische Hacker drohen mit Vergeltung für Leopard-Entscheidung

Nach der Zusage von Leopard-Panzern für die Ukraine droht die Hackergruppe Killnet mit Cyberangriffen auf deutsche Firmen und Behörden. Erste Websites sind bereits betroffen.

Mareike Müller, Jens Koenen, Martin Murphy, Dietmar Neuerer, Teresa Stiens, Andreas Kröner, Yasmin Osman, Britta Rybicki

25.01.2023 • Update: 26.01.2023 - 11:43 Uhr • 16 x geteilt

golem.de IT-NEWS FÜR PROFIS

HOME TICKER PODCAST NEWSLETTER GOLEM PLUS FORUM

Artikel, News, ... Suchen Mehr lesen mit Golem Plus

KARRIEREWELT JOBS IT-FACHTRAININGS COACHINGS SPRACHKURSE GEHALTSCHECK | GOLEM-PC PRODUKTVERGLEICH TOP-ANGEBOTE

ERNEUTER CYBERANGRIFF

Stadt Potsdam ist wieder offline

Nur wenige Stunden waren die IT-Systeme der Stadt Potsdam nach einem dreiwöchigen Ausfall in Folge eines Cybercrime-Angriffs online.

in Pocket speichern merken

25. Januar 2023, 8:16 Uhr, Ingo Pakalski

BASIC TUTORIALS

Startseite News Deals Ratgeber Tests Gewinnspiele Forum English Suchen nach

Top-Ratgeber: Gaming-Stuhl Gaming-Tastatur RGB-Beleuchtung Gaming-Maus Gaming-Headset Headset-Tuning Gehäuse-Airflow

Startseite / News / Gesundheitsbranche: Bitmarck wurde Opfer von Cyberattacke

News

Gesundheitsbranche: Bitmarck wurde Opfer von Cyberattacke

Jens Scharfenberg • 24. Januar 2023

Beliebte Beiträge

- Backforce V Test: Neuer Referenz-Gaming-Stuhl im 400-Euro-Segment
- Backforce One Plus Test: Backforce lässt die Konkurrenz erneut alt aussehen
- Backforce versus noblechairs: Zwei Gaming-Throne für ein Halleluja

RedaktionsNetzwerk Deutschland

RND+ entdecken Newsletter Ticker Russlands Krieg Corona Klima Politik Wirtschaft Panorama Gesundheit Sport

Startseite > Wirtschaft > T-Mobile US gehackt: Cyberangriff auf Telekom-Tochter, 37 Millionen

Information nach Börsenschluss

37 Millionen Kunden von Hackerangriff auf T-Mobile US betroffen

In den USA haben sich Hacker Zugang zu den Daten von etwa 37 Millionen Kunden der Telekom-Tochter T-Mobile US verschafft. Das Unternehmen teilte dies am Donnerstag nach Börsenschluss mit. Festgestellt wurde der Cyber-Angriff bereits deutlich früher.

MEHR AUS WIRTSCH

Das bringt der neue Monat

Mehr Windkraft, weniger Regeln und höhere Bierpr sich im Februar ändert

Frist bis zum 31. Januar

Darauf müssen Immobilie der Grundsteuererklärun

Laut einer Studie

Anders als zu Beginn des Angriffskrieges: Märkte r Ukraine-Hilfe inzwischen

Wegen Inflation und Energiekrise

Deutsche Wirtschaft schrumpft u Prozent

Unterschiede im Osten geringer

Noch immer verdienen Frauen w weniger pro Stunde als Männer

Handelsblatt

MEINE NEWS | HOME POLITIK UNTERNEHMEN TECHNOLOGIE FINANZEN MOBILITÄT KARRIERE ARTS & STYLE MEINUNG VIDEO SERVICE

RÜSTUNGSKONZERN

Rheinmetall wird Opfer eines Hackerangriffs – Staatsanwaltschaft ermittelt

SWR» AKTUELL

Menü Suchen Wetter Verkehr

SWR» / SWR Aktuell / Baden-Württemberg

DDOS-ATTACKE

Hackerangriff: Internetseite der Polizei BW wieder online

STOROpack PERFECT PROTECTIVE PACKAGING

BRANCHEN PRODUKTE BERATUNG UND SERVICE UNTERNEHMEN NACHHALTIGKEIT KARRIERE SHOP

INFORMATION

CYBERANGRIFF AUF STOROPACK

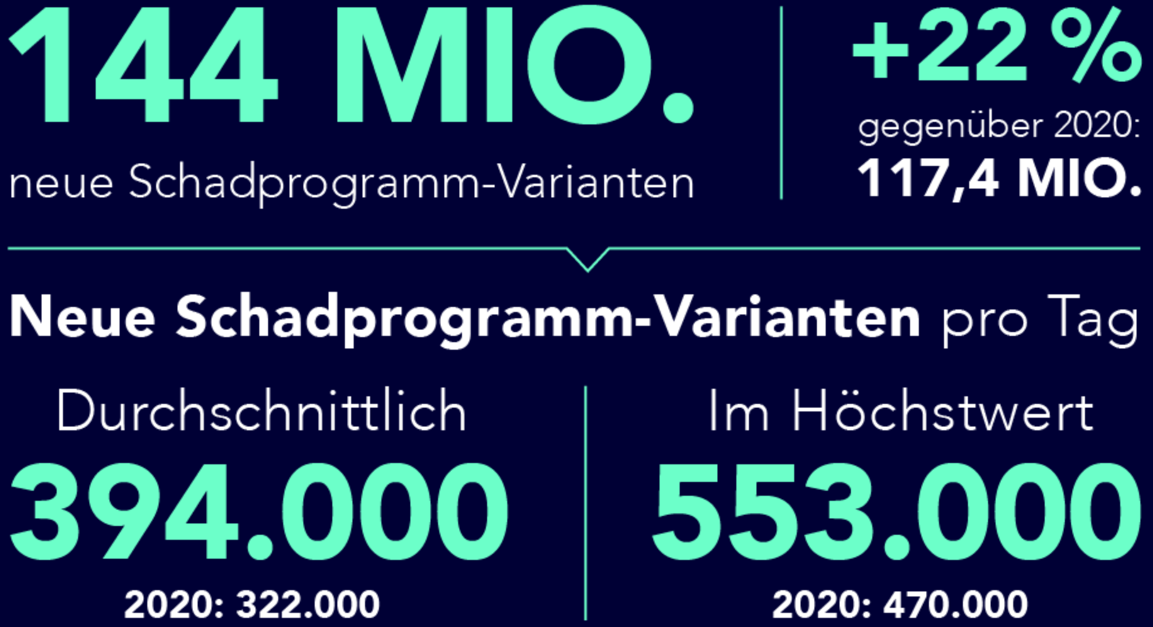
UNTERNEHMEN > NEWS > CYBERANGRIFF AUF STOROPACK

Pressemitteilung vom 23.03.2023

Erreichbarkeit beeinträchtigt: Der Metzinger Schutzverpackungshersteller wurde Opfer einer Cyberattacke

XM Cyber A Schwarz Company

Die Zahl und Intensität der Cyber-Angriffe nimmt stetig zu



144 MIO.
neue Schadprogramm-Varianten

+22 %
gegenüber 2020:
117,4 MIO.

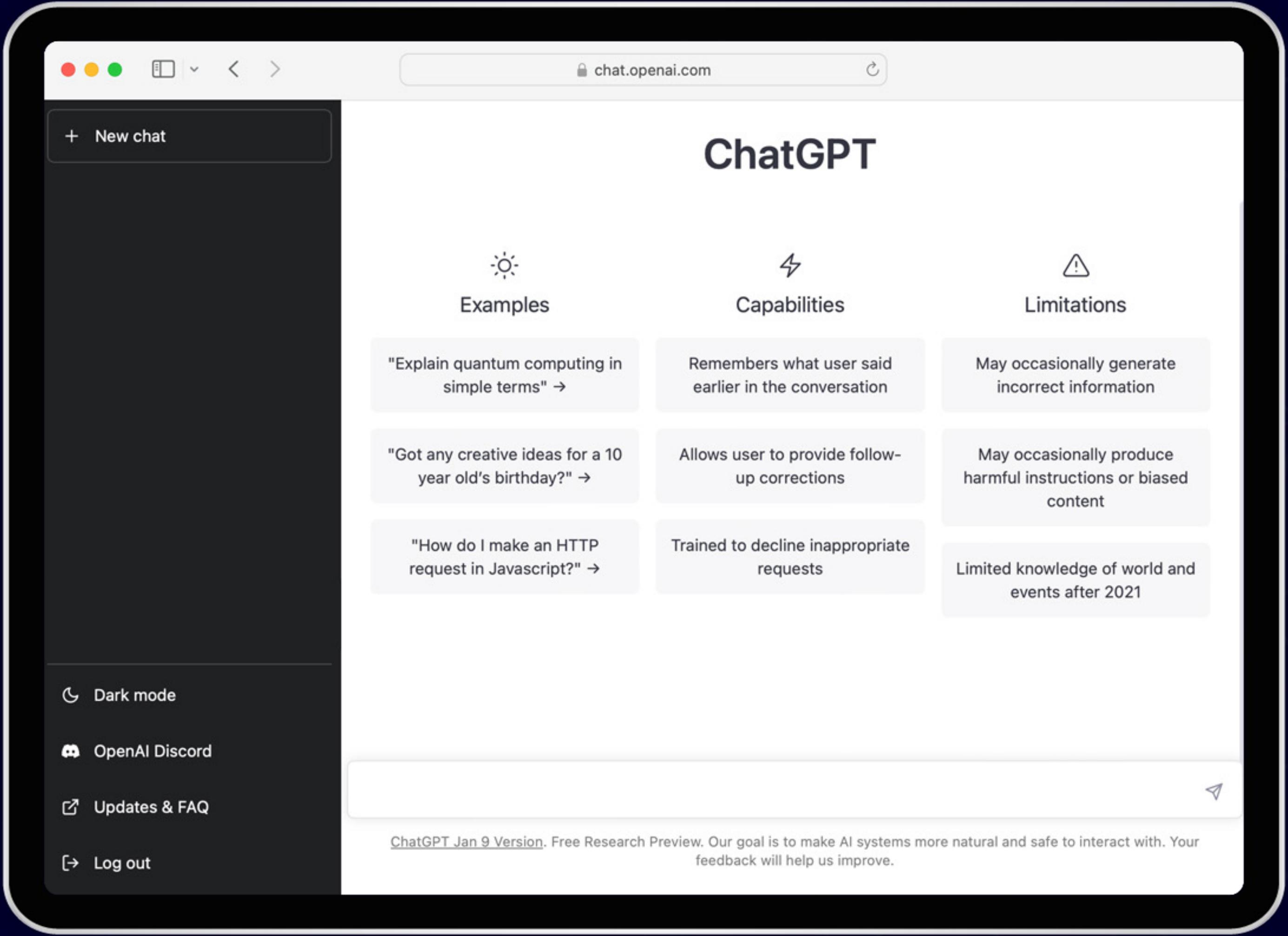
Neue Schadprogramm-Varianten pro Tag

Durchschnittlich
394.000
2020: 322.000

Im Höchstwert
553.000
2020: 470.000

Quelle: BSI „Deutschland. Digital. Sicher"

Es war nie einfacher Schadsoftware zu “entwickeln”



ChatGPT

Examples	Capabilities	Limitations
"Explain quantum computing in simple terms" →	Remembers what user said earlier in the conversation	May occasionally generate incorrect information
"Got any creative ideas for a 10 year old's birthday?" →	Allows user to provide follow-up corrections	May occasionally produce harmful instructions or biased content
"How do I make an HTTP request in Javascript?" →	Trained to decline inappropriate requests	Limited knowledge of world and events after 2021

ChatGPT Jan 9 Version. Free Research Preview. Our goal is to make AI systems more natural and safe to interact with. Your feedback will help us improve.

Das Problembewusstsein in der IT

91 %

sehen eine **potenzielle Gefährdung der Datensicherheit**

Das Problembewusstsein in der IT fehlt – es gibt eine Wahrnehmungskluft

91%

sehen eine **potenzielle Gefährdung der Datensicherheit**

94%

der kritischen Assets können innerhalb von **4 Schritten oder weniger** ab dem Einbruchspunkt kompromittiert werden

75%

der kritischen Assets eines Unternehmens können in **ihrem aktuellen Sicherheitszustand** gefährdet werden

73%

der wichtigsten Angriffstechniken umfassen **falsch verwaltete** oder **gestohlene Anmeldedaten**

XM Cyber
A Schwarz Company

Das Mindset als Herausforderung…

…zwischen „Cyber-Illusion“ und „Cyber-Dilemma“

Vergangenheit

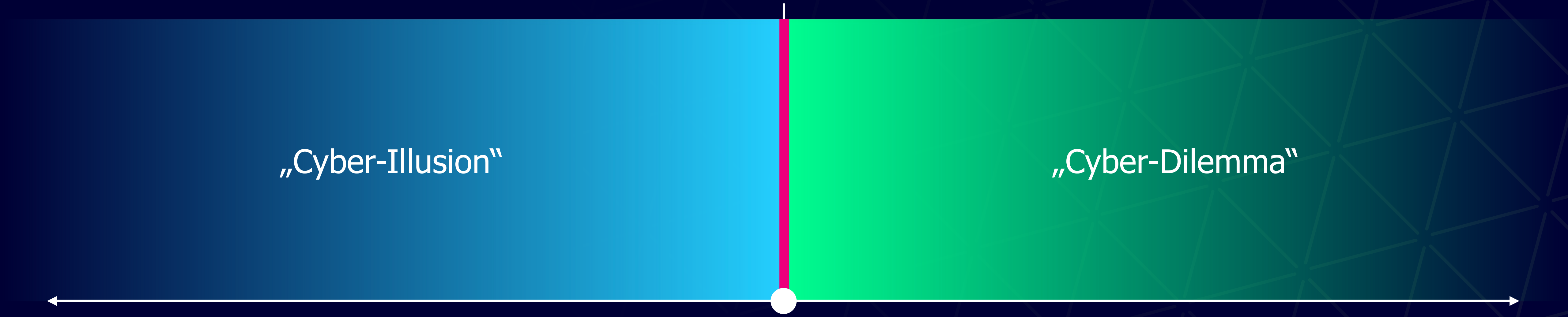
Gegenwart

Zukunft

…zwischen „Cyber-Illusion“ und „Cyber-Dilemma“

CIO / IT

CEO



„Cyber-Illusion“

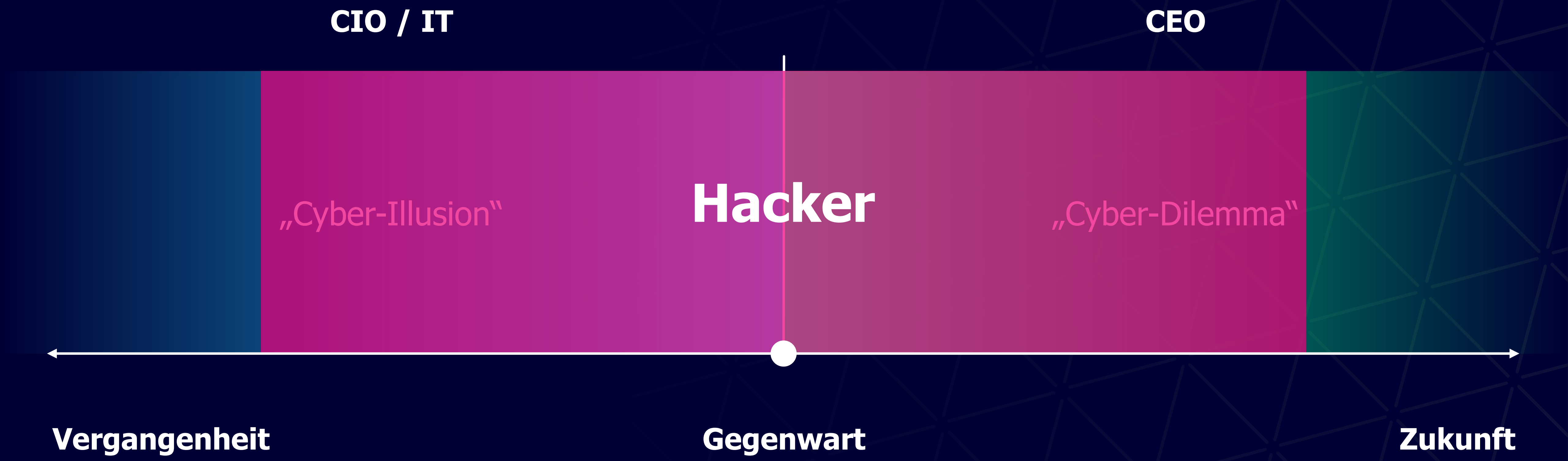
„Cyber-Dilemma“

Vergangenheit

Gegenwart

Zukunft

…zwischen „Cyber-Illusion“ und „Cyber-Dilemma“


CIO / IT

CEO

„Cyber-Illusion“

Hacker

„Cyber-Dilemma“

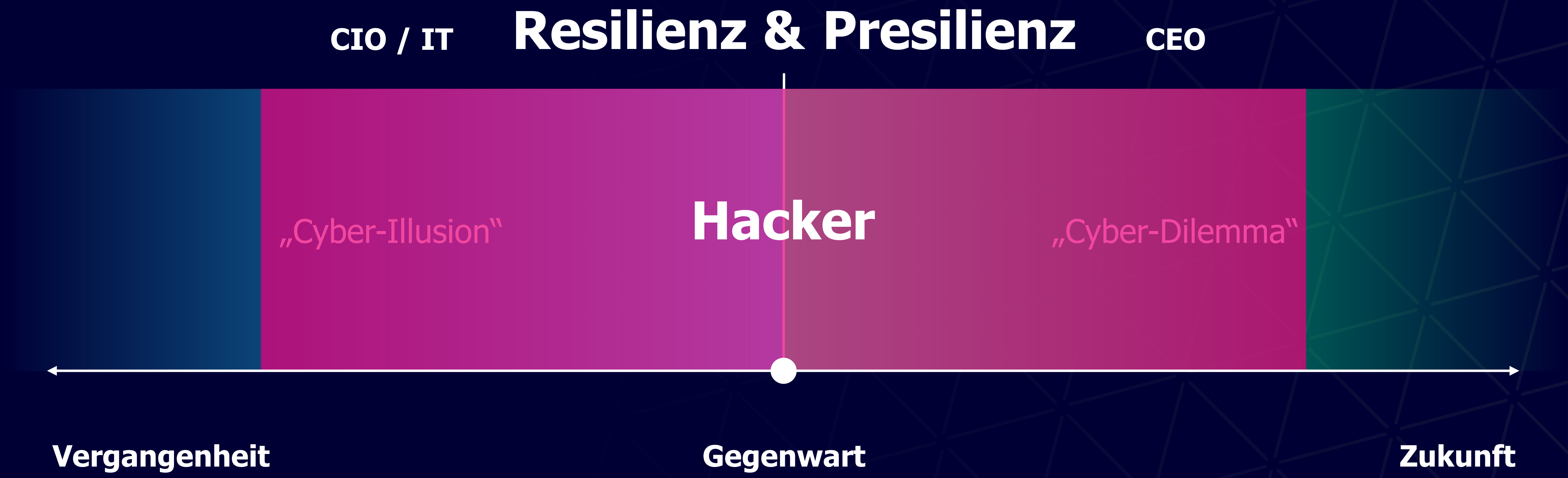
Vergangenheit

Gegenwart

Zukunft

XM Cyber
A Schwarz Company

…zwischen „Cyber-Illusion“ und „Cyber-Dilemma“



CIO / IT

Resilienz & Presilienz

CEO

„Cyber-Illusion“

Hacker

„Cyber-Dilemma“

Vergangenheit

Gegenwart

Zukunft

Was wäre, wenn Sie Folgendes wüssten?

Alle versteckten Angriffspfade, die zu Ihren kritischen Assets führen

Die kleinste Anzahl an Maßnahmen, die die größten Auswirkungen zur Risikominimierung haben

Wie man das Cyber-Risiko eines Unternehmens für das C-Level Management leicht quantifizieren kann

Alle Lücken in den Sicherheitskontrollen und wie diese geltenden Regulierungen und Bestimmungen entsprechen

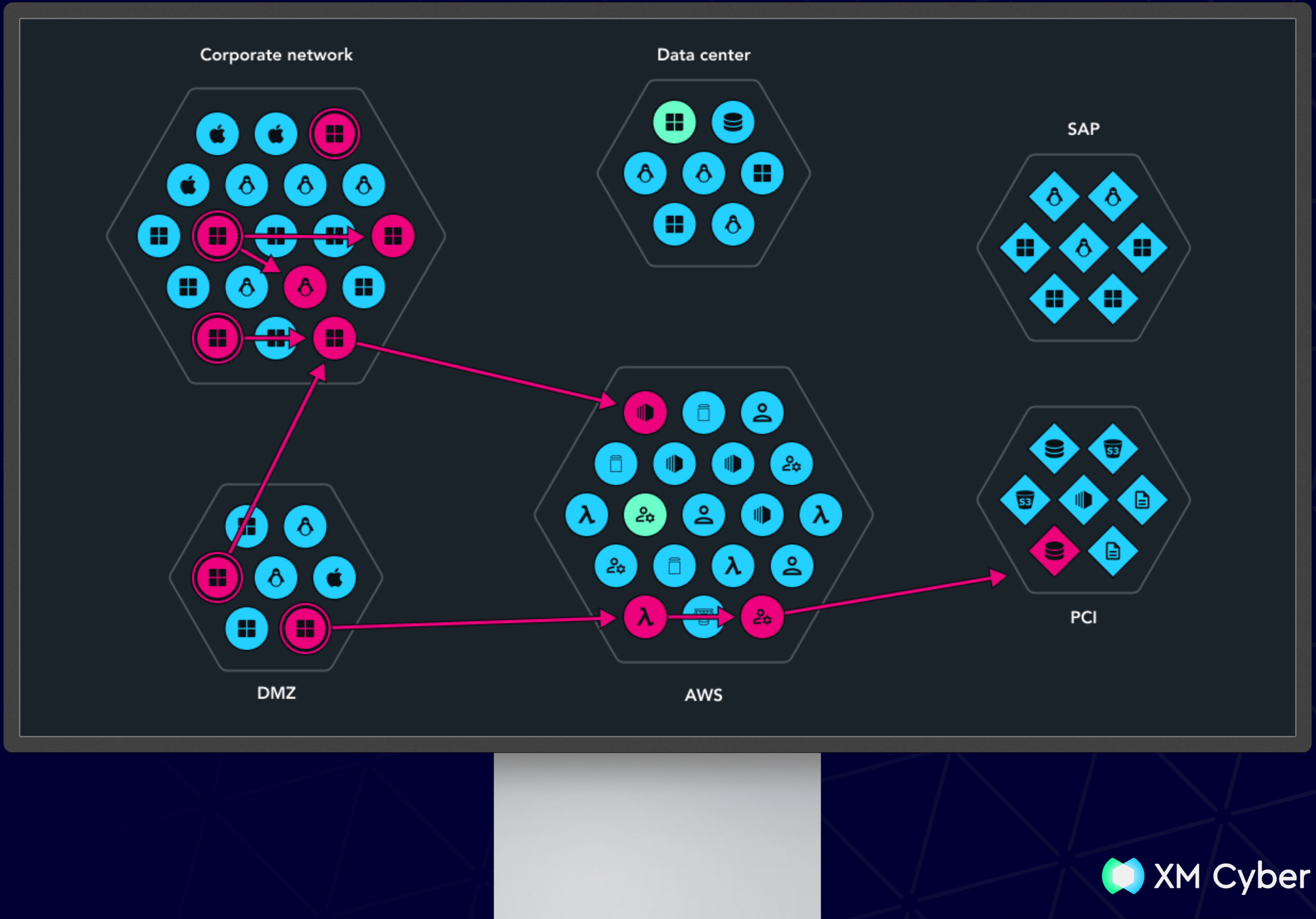
Sehen, was Angreifer sehen:
From Attack Paths to Attack Graph

Hybrid Cloud Security
SaaS Platform

Continuous & Safe Attack
Path Management across
On Prem & Cloud Assets

Cyber Risk Reporting

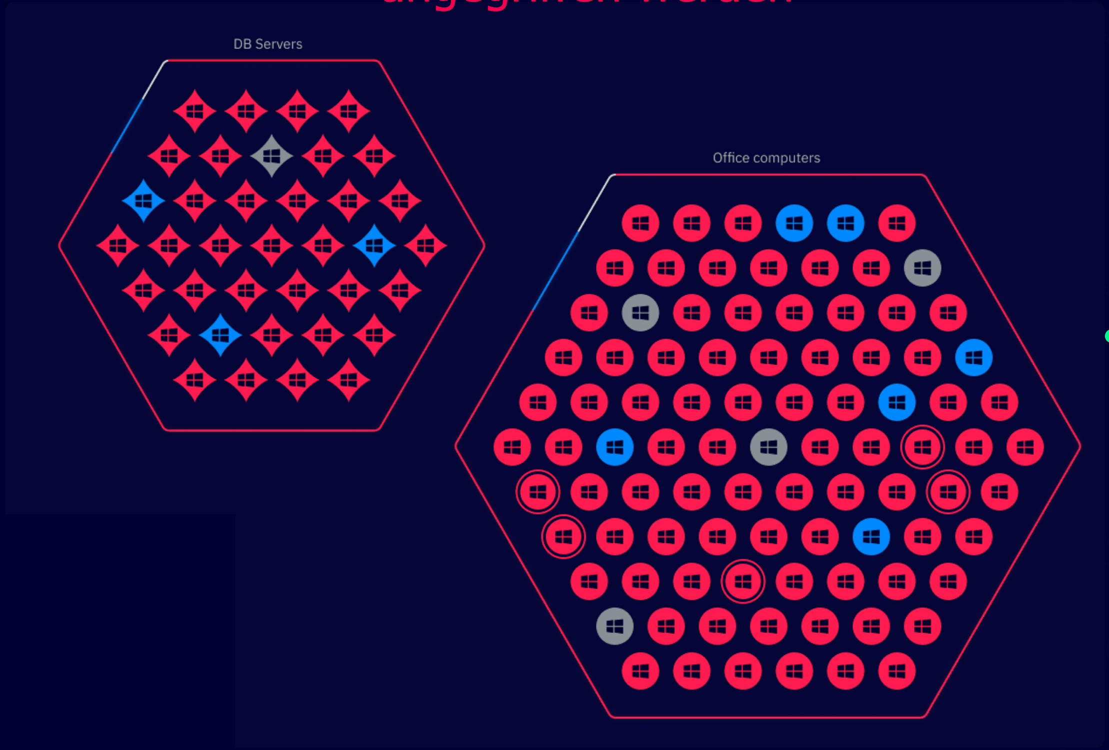
Prioritized Guided
Remediation



XM Cyber

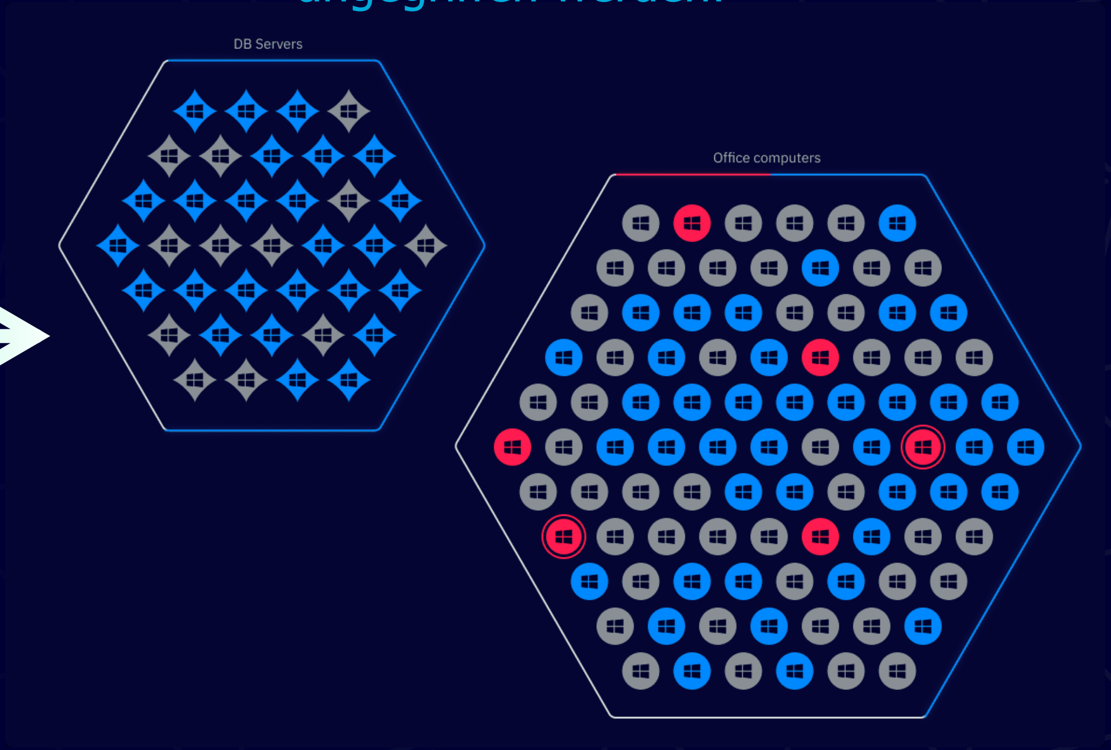
Jetzt können Sie sehen, ob Ihre Assets geschützt sind

93% der Assets können angegriffen werden



< 3 Monate

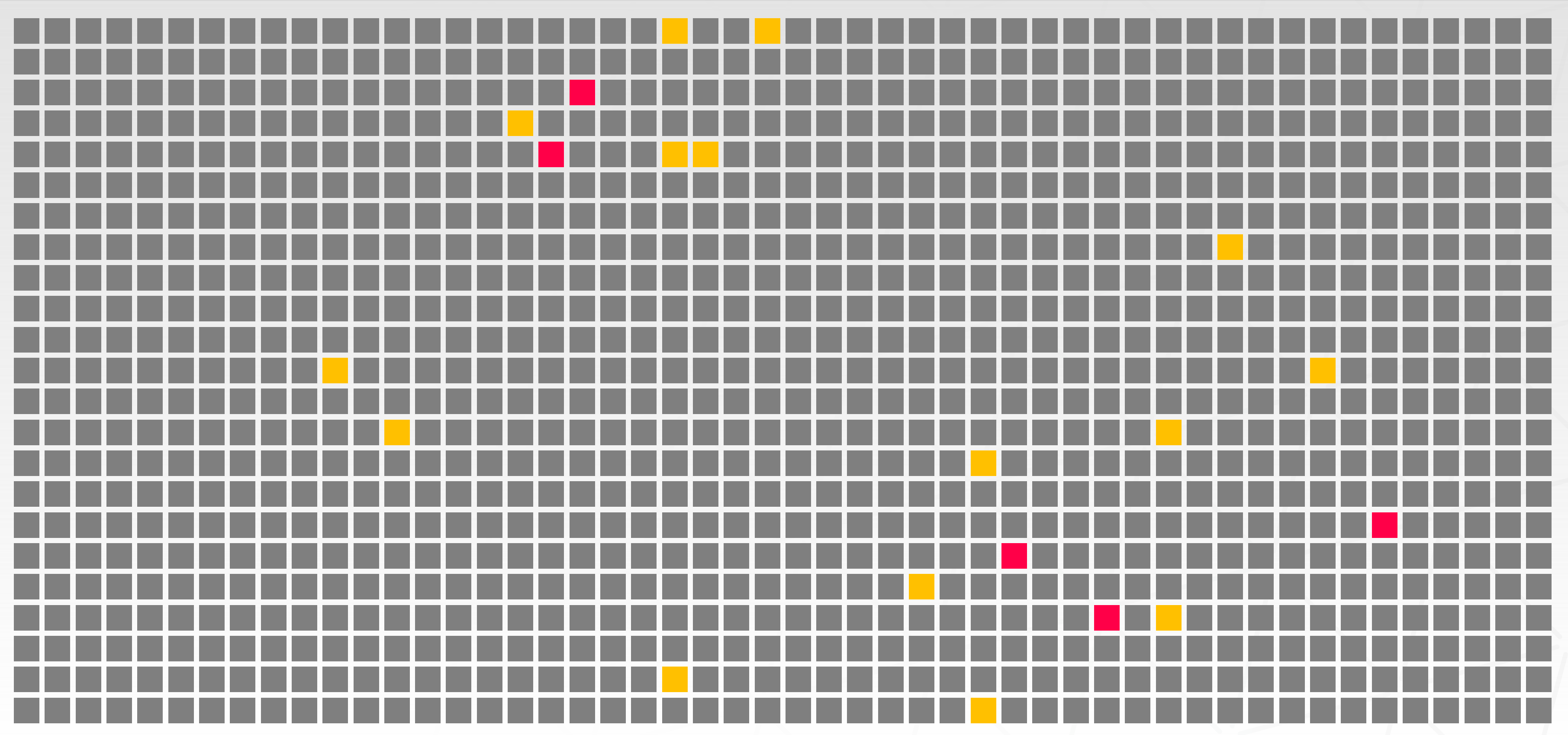
Nur 7% der Assets können angegriffen werden!



***Aktuelles Kundenumfeld**

Priorisierung entscheidet über wirksamen Schutz

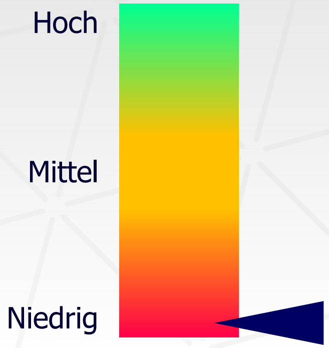
Typische Unternehmen haben durchschnittlich 11.000 Schwachstellen pro Monat



Legende:

- ■ 10 exposures (per square)
- 🟨 Choke Points
- 🟥 Critical Choke Points *)
- 🟩 Closed / fixed Exposure

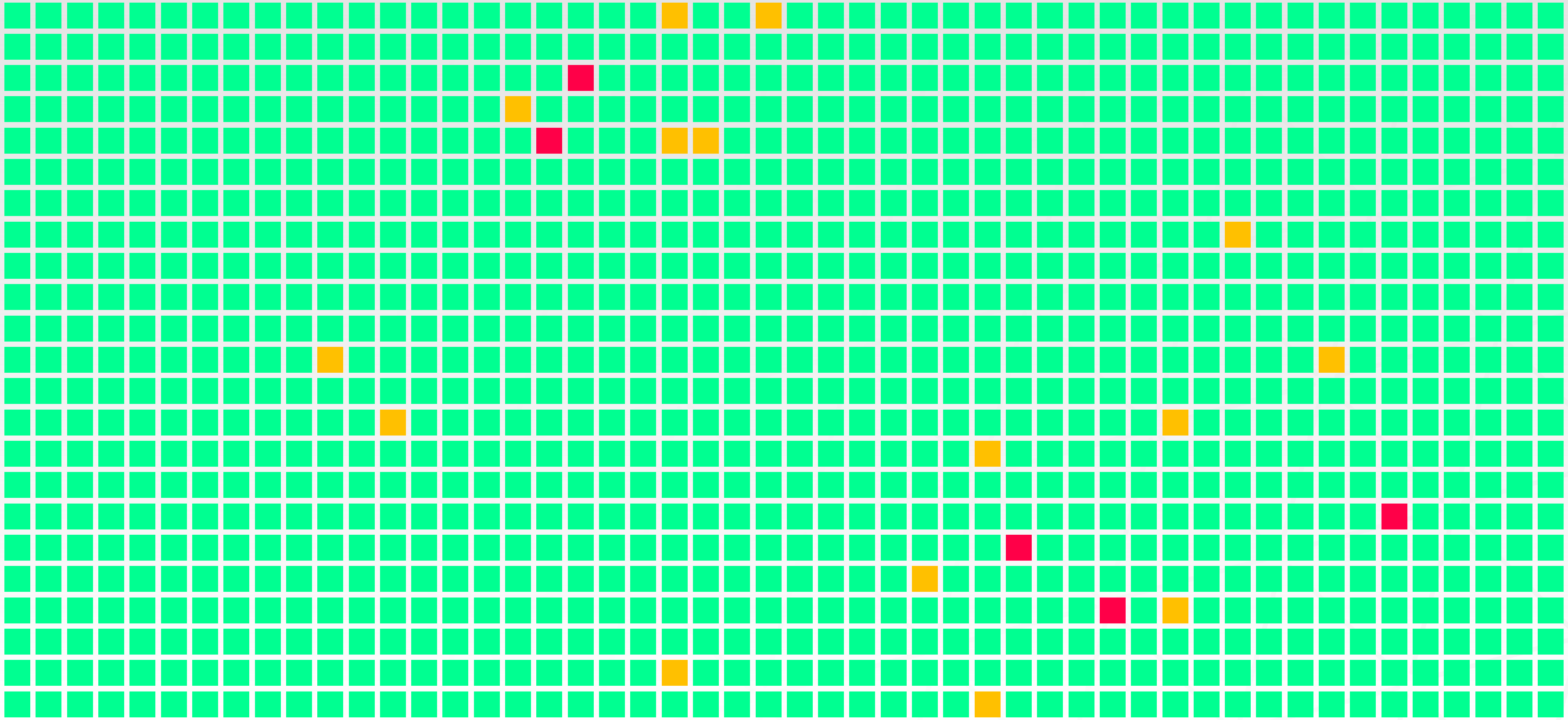
Sicherheitslevel:



*) Choke points that expose 10% or more of critical assets

Priorisierung entscheidet über wirksamen Schutz

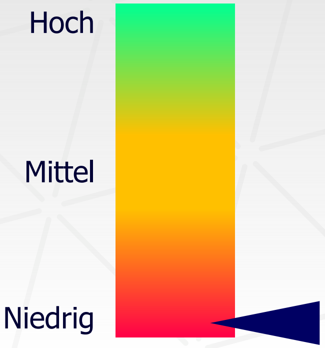
Schließen der falschen Schwachstellen ändert quasi nichts am Sicherheitsniveau



Legende:

- ⬛ 10 exposures (per square)
- 🟨 Choke Points
- 🟥 Critical Choke Points *)
- 🟩 Closed / fixed Exposure

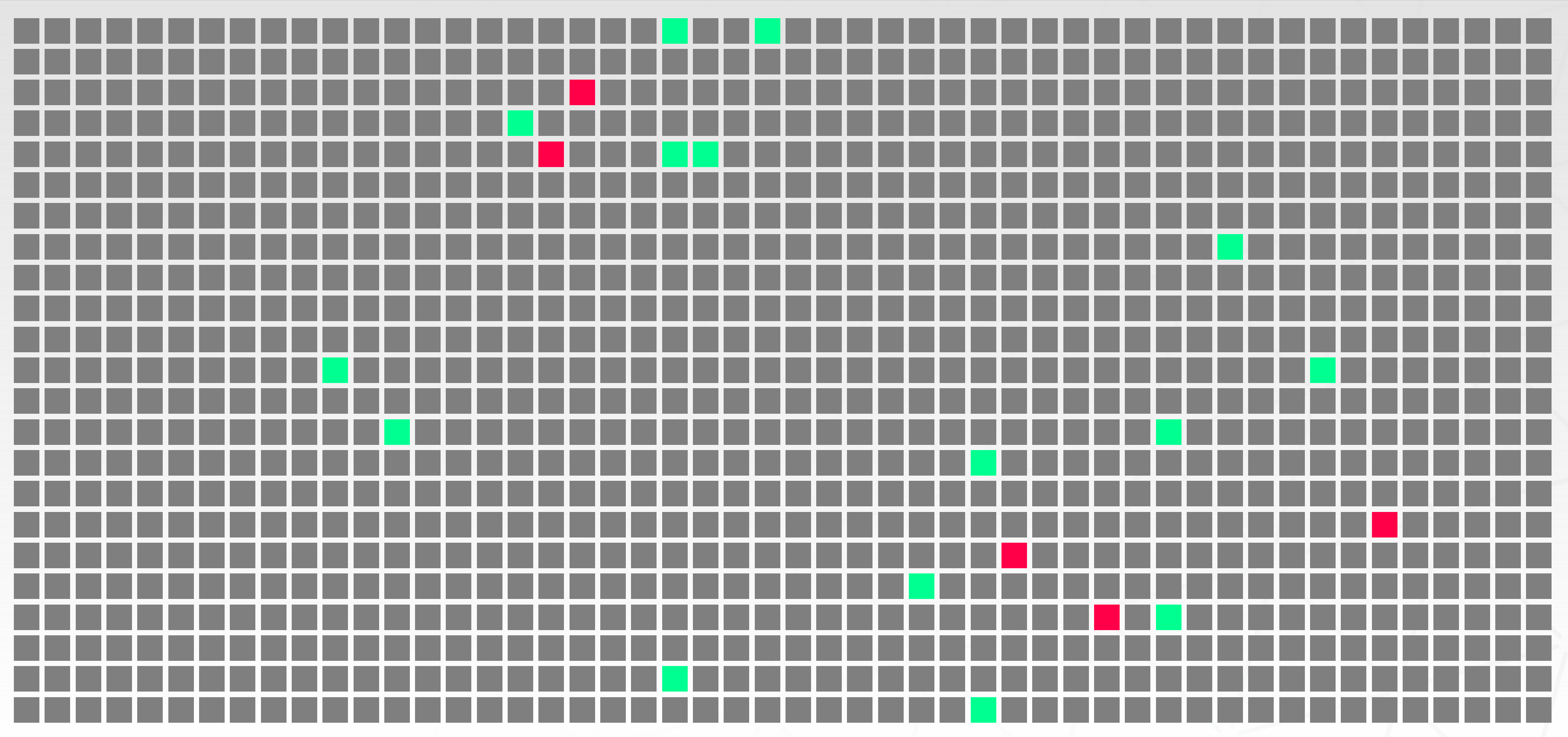
Sicherheitslevel:



*) Choke points that expose 10% or more of critical assets

Priorisierung entscheidet über wirksamen Schutz

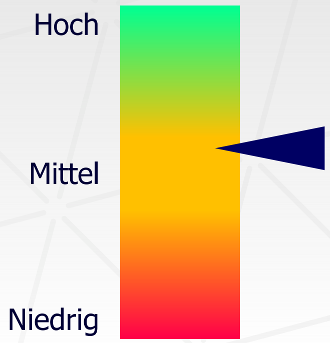
Schließen der Exposures an Choke Points macht den Unterschied



Legende:

- ⬛ 10 exposures (per square)
- 🟨 Choke Points
- 🟥 Critical Choke Points *)
- 🟩 Closed / fixed Exposure

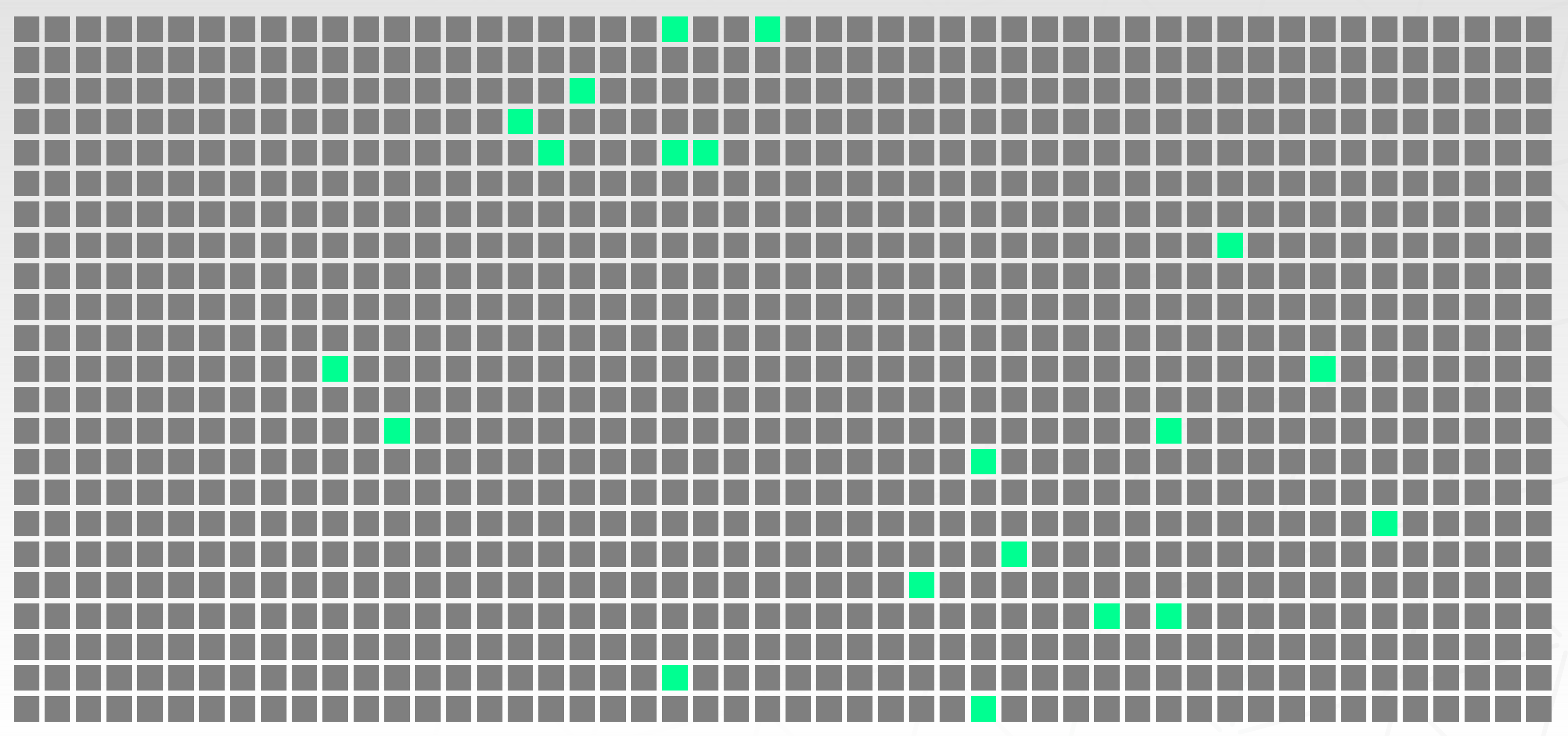
Sicherheitslevel:



*) Choke points that expose 10% or more of critical assets

Priorisierung entscheidet über wirksamen Schutz

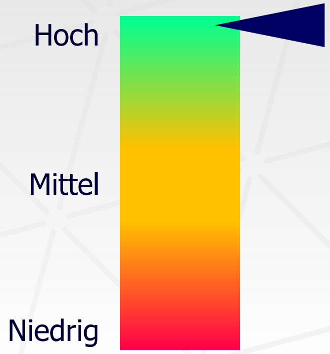
Schließen von 2% aller Exposures verhindert quasi sämtliche Angriffsmöglichkeiten



Legende:

- ⬛ 10 exposures (per square)
- 🟨 Choke Points
- 🟥 Critical Choke Points *)
- 🟩 Closed / fixed Exposure

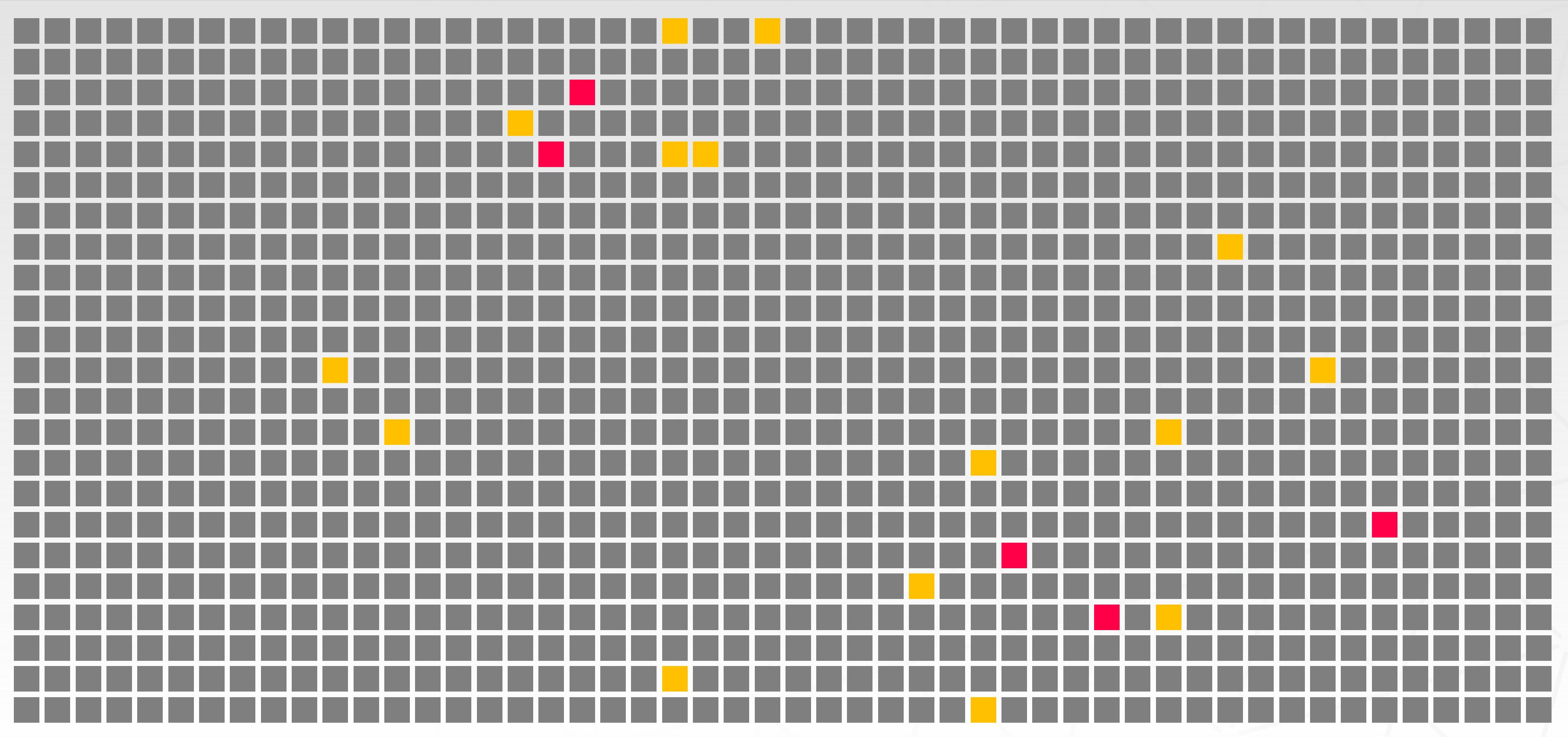
Sicherheitslevel:



*) Choke points that expose 10% or more of critical assets

Priorisierung entscheidet über wirksamen Schutz

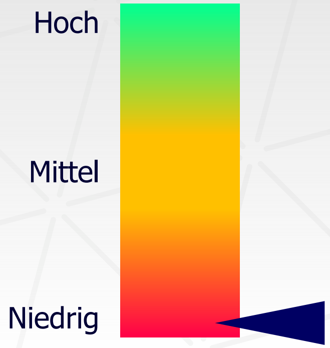
Die Sicherheitslage ist dynamisch – sie ändert sich stetig bei Systemänderungen



Legende:

- ■ 10 exposures (per square)
- 🟨 Choke Points
- 🟥 Critical Choke Points *)
- 🟩 Closed / fixed Exposure

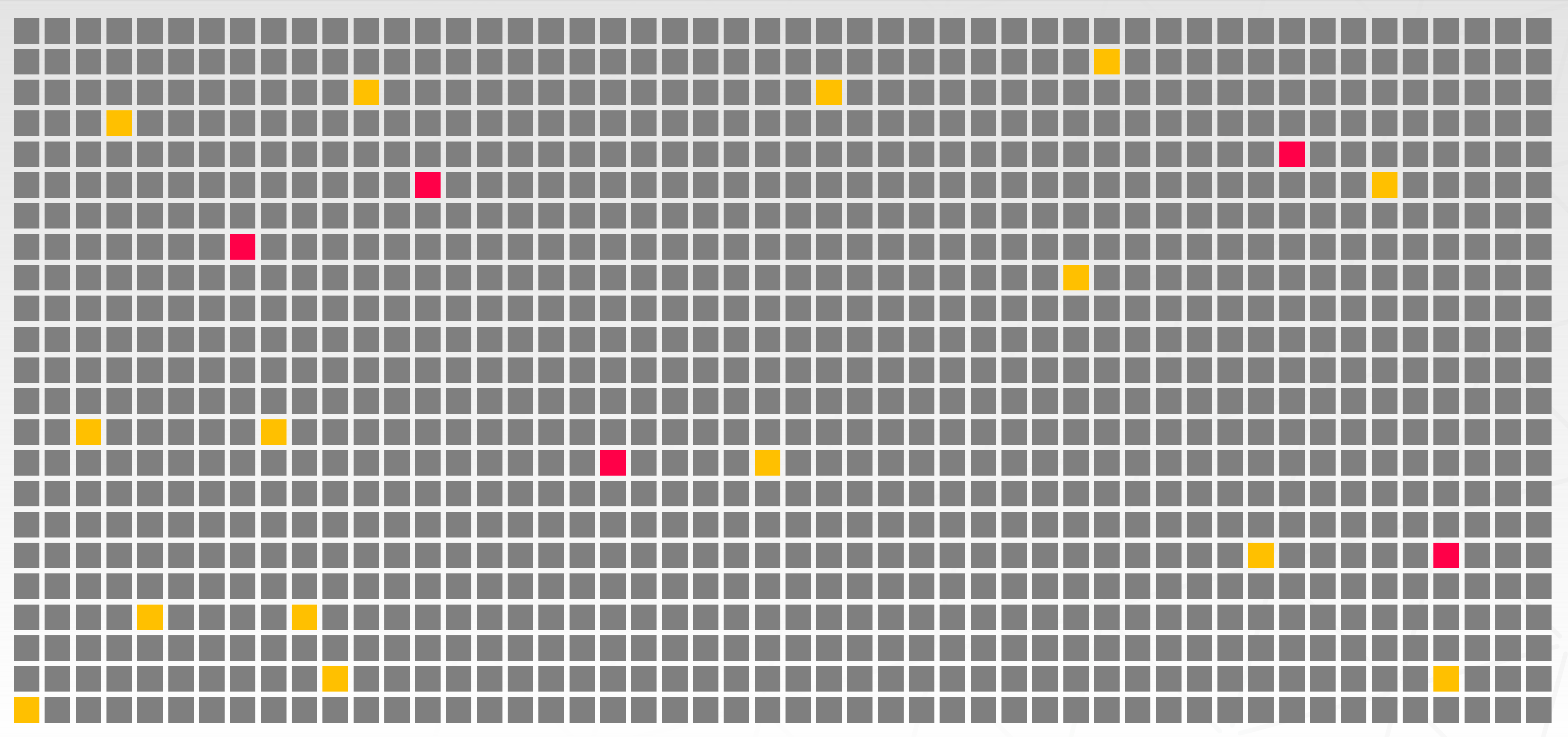
Sicherheitslevel:



*) Choke points that expose 10% or more of critical assets

Priorisierung entscheidet über wirksamen Schutz

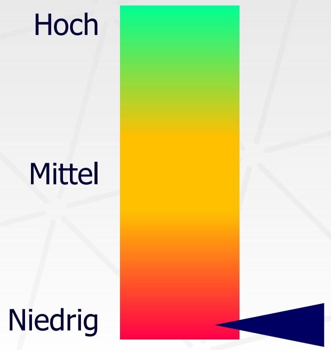
Die Sicherheitslage ist dynamisch – sie ändert sich stetig bei Systemänderungen



Legende:

- ⬛ 10 exposures (per square)
- 🟨 Choke Points
- 🟥 Critical Choke Points *)
- 🟩 Closed / fixed Exposure

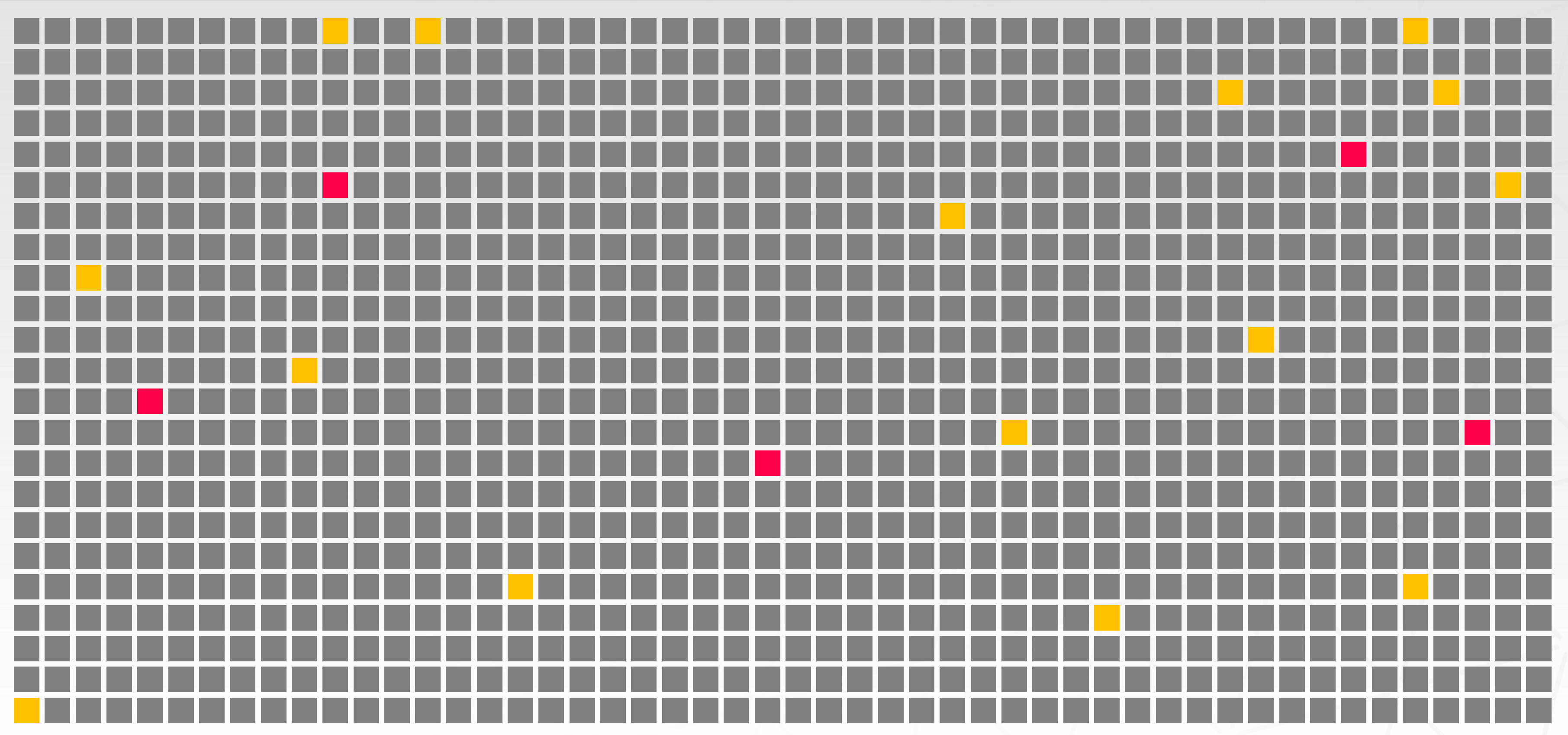
Sicherheitslevel:



*) Choke points that expose 10% or more of critical assets

Priorisierung entscheidet über wirksamen Schutz

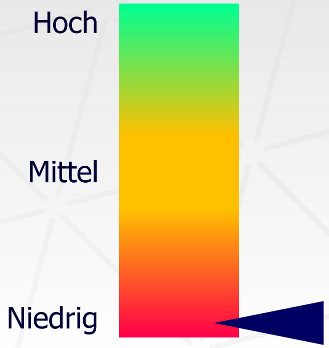
Die Sicherheitslage ist dynamisch – sie ändert sich stetig bei Systemänderungen



Legende:

- ■ 10 exposures (per square)
- 🟨 Choke Points
- 🟥 Critical Choke Points *)
- 🟩 Closed / fixed Exposure

Sicherheitslevel:



*) Choke points that expose 10% or more of critical assets

XM Cyber
A Schwarz Company

Cybersicherheit von XM Cyber.

Vorher wissen, was später passiert.

XM Cyber ist die einfache Antwort für Ihre Cybersicherheit. Die Software analysiert 24/7 die Schwachstellen Ihrer Infrastruktur aus Sicht der Angreifer – und priorisiert diese. Wir helfen Ihnen, die täglichen Sicherheitsanforderungen richtig einzuordnen, um Ihre wichtigsten Systeme und Daten effektiv zu schützen.

Mehr auf xmcyber.com

See All Ways™