ARMIS®

THE STATE OF
CYBERWARFARE

ARMIS STATE OF CYBERWARFARE AND TRENDS REPORT: 2022-2023

COUNTRY-BY-COUNTRY ANALYSIS

DACH
(AUSTRIA, SWITZERLAND, GERMANY)

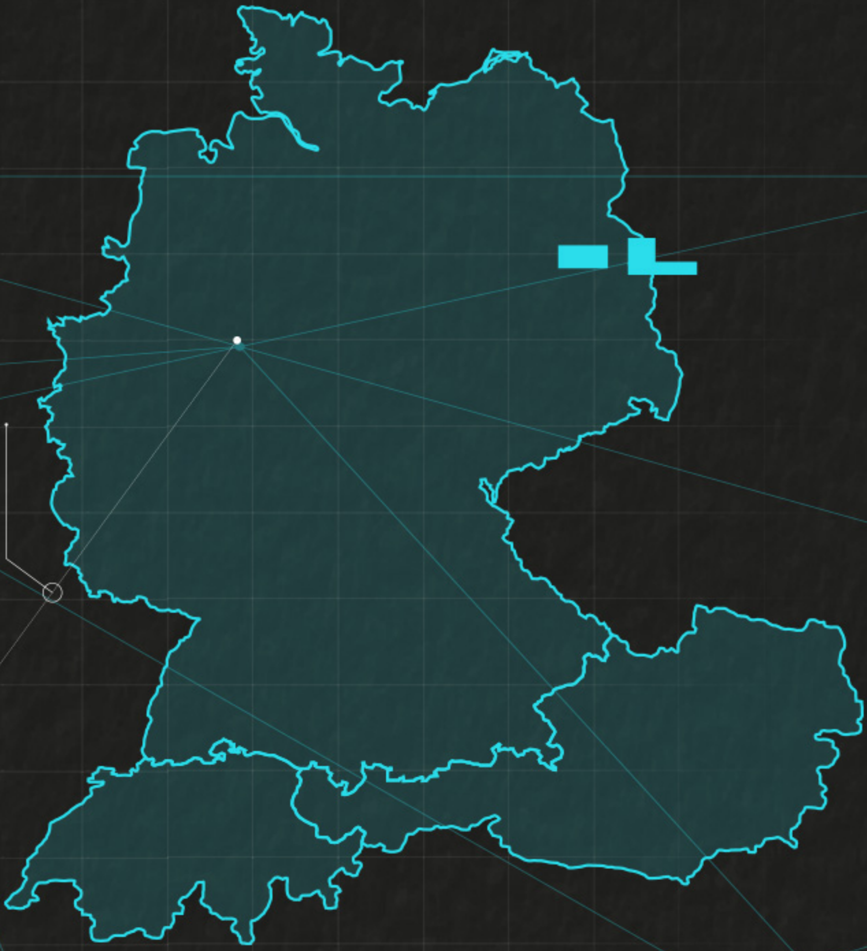


TABLE OF CONTENTS

INTRODUCTION

If you've reviewed the global Armis State of Cyberwarfare and Trends Report: 2022-2023, you know that it's critical for business and IT leaders to understand the evolving threat landscape surrounding cyberwarfare, so that they can improve their cybersecurity posture to defend against these attacks. To prepare this report, Armis commissioned a study surveying 6,021 IT and security professionals globally to determine worldwide trends as they relate to security professionals' sentiments on cyberwarfare, attack patterns, cyber spending, and more. Responses were gathered between September 22, 2022 and October 5, 2022.

Armis utilized data from its award-winning Asset Intelligence and Security Platform to verify the survey results against real-world data trends. Proprietary data from the Armis platform collected June 1, 2022 through November 30, 2022 confirmed that cyberattacks haven't slowed, only worsened. Threat activity against the global Armis customer base increased by 15% from September to November when compared to the three months prior. Further, Armis identified the largest percentage of threat activity against critical infrastructure organizations, with healthcare organizations the second most targeted when compared to various industries.

In addition to these global findings, Armis has prepared regional findings and country-by-country analysis to offer unique, localized insights which may be more impactful for individual readers depending on where they physically are based and the counties in which their business operates. **For this country-by-country analysis, we will zoom in on the findings pulled from the 651 respondents who shared insights for our survey that are based out of Germany (501), Austria (100) and Switzerland (50) and work across industries including healthcare, manufacturing, retail, financial services, and more.**

SUMMARY OF FINDINGS

Cyberwarfare was for a long time a subject that hasn't had any importance for organizations in DACH. Therefore, they could handle cyberattacks and threats in a business-as-usual way and protect themselves and their infrastructure. Since February 24th, 2022, this has changed completely, with groups like Conti, Killnet, and others declaring cyberwar on organizations within NATO states. Governments, security services, and related competent authorities in the EU continue to put greater emphasis on national and supranational legislation on the topic, which is a great start but has not proved to be enough. Recently the EU decided to strengthen cybersecurity across the Union, thus updating the bloc's requirements for enhanced cybersecurity by member states, while releasing its NIS2 initiative to give more guidance for organizations to look further into their SBOMs and secure their software supply chains. In DACH IT-Sicherheitsgesetz 2.0, or for the healthcare industry B3S, regulations are pushing companies to further adopt cybersecurity.

Overall, the findings show that only 40% of DACH organizations agree that they are prepared for cyberwar. Nearly the same number is somewhat concerned about their critical infrastructures which have been more challenged recently, as we've seen in cyberattacks on hospitals like Duisburg-Essen, various news agencies like DPA or APA in Austria, or media houses like the Heilbronner Stimme.

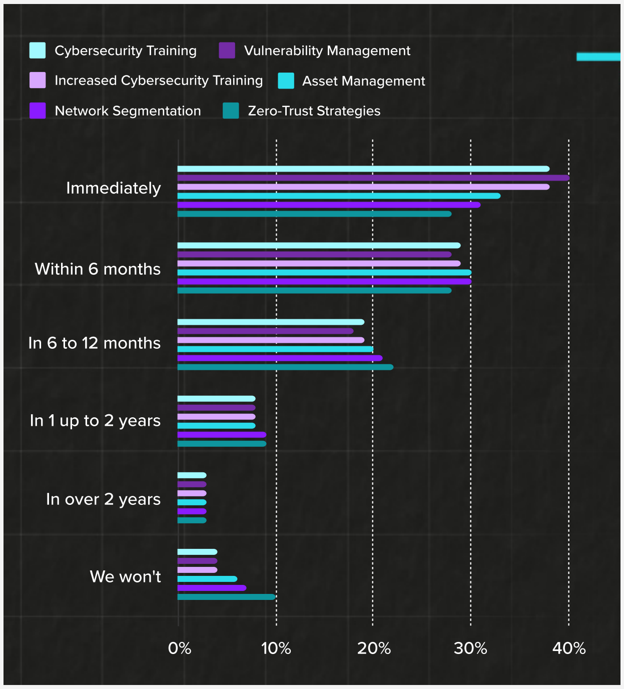
EMEA

Through the course of 2022, the EMEA region has been shocked by the invasion of the sovereign nation of Ukraine. With the geopolitical instability associated with physical warfare and cyberwarfare, shockwaves of consequences are arriving throughout the area. Unpredictability in the food supply, the infamous energy crisis, and a wave of cyberattacks focused against the most critical functions of society, are all contributing to changes in spending and priorities across numerous industries. The report confirms the rise in cyberattacks, bringing to light that almost 3 in 5 organisations (58%) experienced one or more cybersecurity breaches. And 25% of respondents confirmed that there has been an escalation in the number of threats to their organisation.

Measures are being taken to ensure protection, but to date, still less than half (44%) of IT and security professionals agree that their organisation has programs and practices in place to respond to cyberwarfare threats. Respondents depicted their company as ill-prepared as there are some relevant issues to be addressed:

- Only 46% of IT and security professionals in EMEA strongly agreed on knowing who to contact if they notice suspicious activity.
- Only 76% of IT and security professionals in EMEA said they collaborate with others in the industry when it comes to sharing information about threats, below the U.S. and APJ averages. Although being a high number, this indicates that there is still work to be done if all areas are to be shielded from cyberattacks.
- Only 33% of IT and security professionals in EMEA have reported an act of cyberwarfare to the authorities, below the US (63%) and APJ (61%) levels.
- Almost 2 in 10 (18%) of IT and security professionals in EMEA said their organisation does not have a contingency plan in place if cyberwarfare is detected.
- Only a third (33%) of IT and security professionals have a validated cyberwarfare plan with best practice frameworks, to be appropriate and proportionate.
- Moreover, less than half (49%) of companies are educating employees as a common practice, or restricting network admin rights (40%). Fewer still have cybersecurity practices implemented such as creating a security-focused work culture (37%), investing in cybersecurity insurance (31%), and implementing a Cyber Risk Framework (31%).

There is a disconnect between confidence levels of preparedness for cybersecurity attacks (84%) and reality, and investment is needed to close that gap, both for tools and services. When asked to select when they will invest in certain aspects, the following responses were given by IT professionals:



REGULATION IS PUSHING TOWARDS THE FUTURE

Governments, security services and related competent authorities continue to put great emphasis on the need for an improved cybersecurity posture, and the imperative necessity for a more cyber resilient strategy. The recent EU Cyber Resilience Act builds on the EU's existing Cybersecurity Directive of 2016, thus updating the bloc's requirements for enhanced cybersecurity by member states. Prior to this EU Cyber Resilience Act, much of the pressure when it came to cybersecurity was put on users of these products, both enterprises and individuals alike. Now, the manufacturer will share a larger part of this responsibility as well. Accountability can go a long way in helping to make improvements across the board. The EU also released NIS2, adding many more verticals into the spotlight and introducing fines, sanctions, and penalties, for not doing proper risk management, basic cyber hygiene, and taking undue delays in corrective action.

The emergence of regulations is a great conversation starter and will certainly help address that gap of investment in certain tools and prioritise their importance, but there is still a long way to go to secure the critical vulnerability gaps introduced by the exponential proliferation of connected assets. 37% of respondents agree that connected devices are a top priority in the event of a cyberwarfare attack.

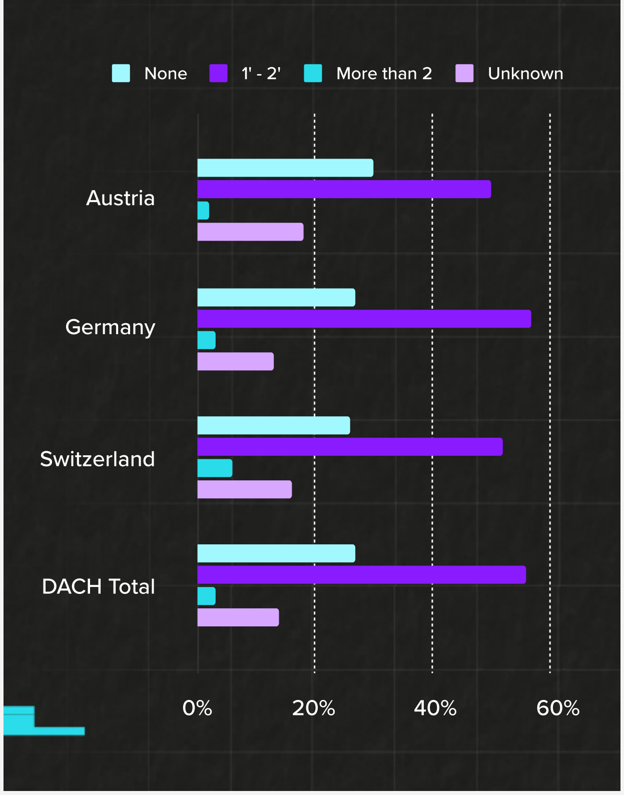
Beyond the internal efforts, it is believed amongst IT professionals that the European Union and its member states should also boost cooperation with other allies around the world. More than half (61%) stated that they would support conscription into a cyber defence league if their country were drawn into a cyberwar conflict.

DACH TRENDS FROM THE ARMIS STATE OF CYBERWARFARE AND TRENDS REPORT: 2022-2023

LACK OF CYBER RISK FRAMEWORK LEADS TO A LACK OF ASSET MANAGEMENT

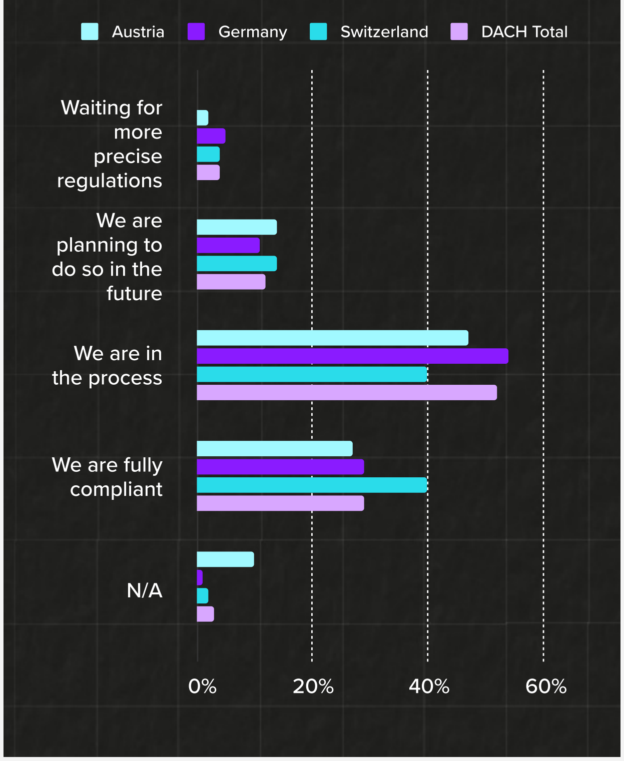
Results from the study show that 59% of DACH organizations have suffered one or more data breaches.

DATA BREACHES SUFFERED



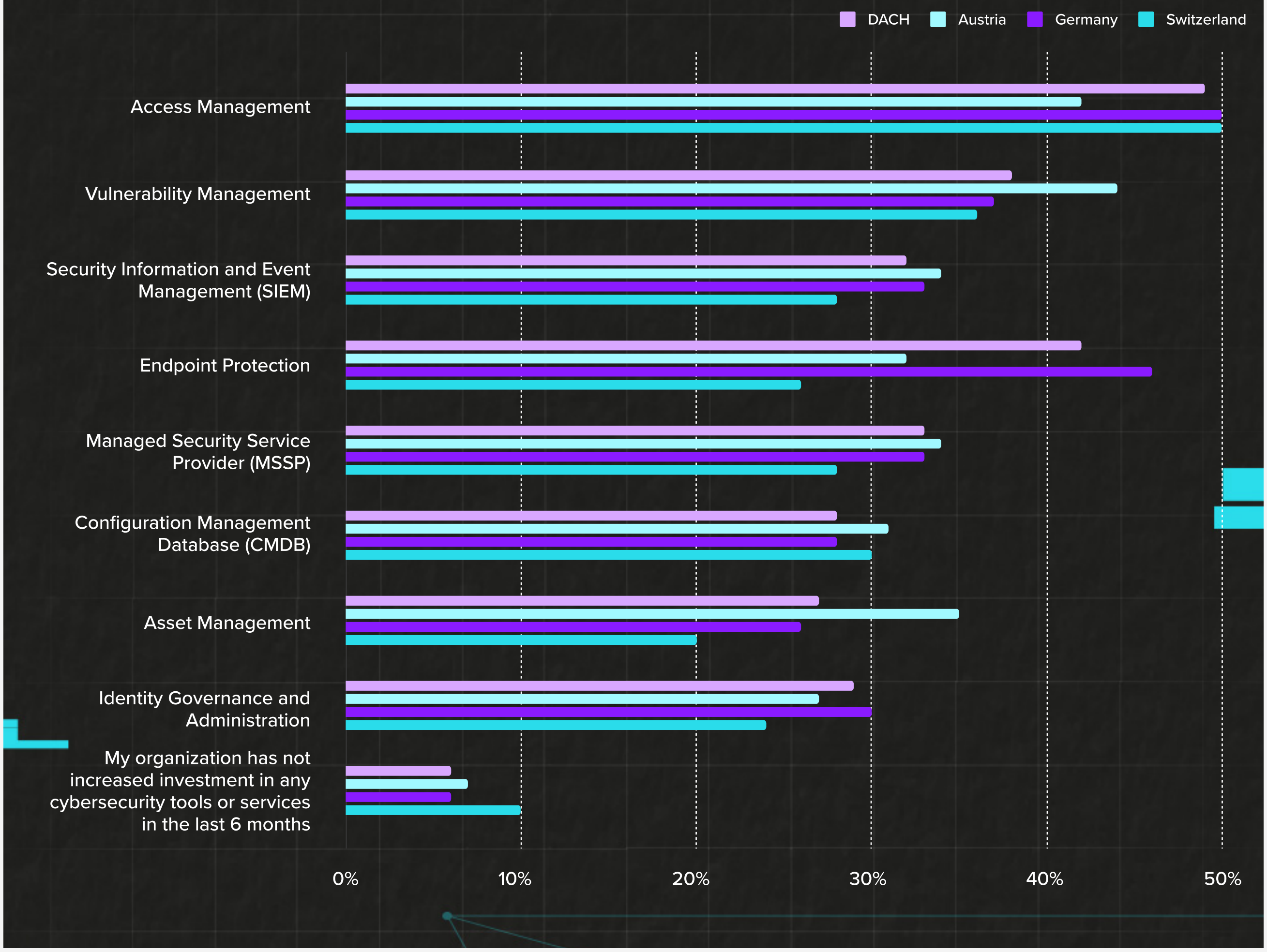
Despite this fact, 59% of IT professionals voted ‘backing data up’ as one of the most relevant strategies to protect their organization, and 61% stated data protection was their top priority in terms of cybersecurity. The stats showcase a clear gap in the security posture that competent authorities are trying to push through legislation. Unfortunately, 78% of respondents stated that cyber risk frameworks like those proposed by NIST, BSI, and others are not yet in place in their organizations.

WHICH OF THE FOLLOWING BEST DESCRIBES YOUR POSTURE TOWARDS COMPLIANCE TO B3S, IT-SEC 2.0 AND OTHERS?



A lack in identifying the right cyber risks, is also a lack of knowing what assets are in our inventory and what’s at risk. This research study brings to light that only 27% of respondents are investing in asset management, meaning 73% have not done so yet.

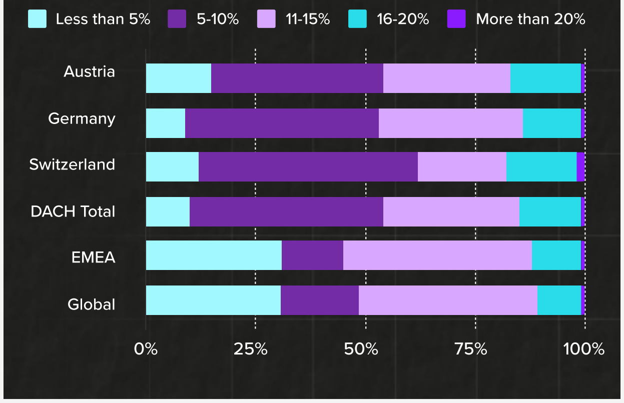
WHICH CYBERSECURITY TOOLS OR SERVICES, IF ANY, HAS YOUR ORGANIZATIONS INCREASED INVESTMENT IN WITHIN THE PAST SIX MONTHS?



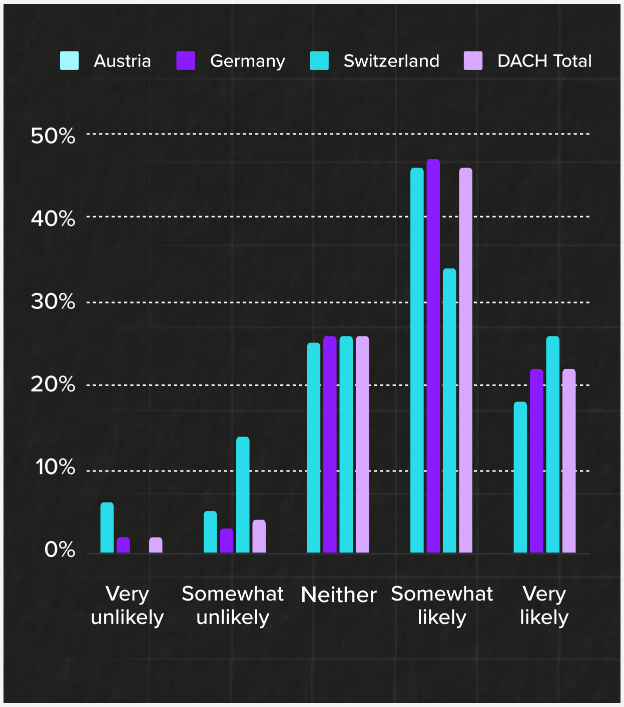
INVESTMENT IS ACCELERATING DUE TO CYBERWARFARE

Investment in cybersecurity for the DACH region is at lower levels than the rest of EMEA, with 44% of organizations only spending 5-10% of their IT budgets on security measures. When asked to select what percentage of their IT budget is spent on cybersecurity, the following response was received:

INVESTMENT IN CYBERSECURITY



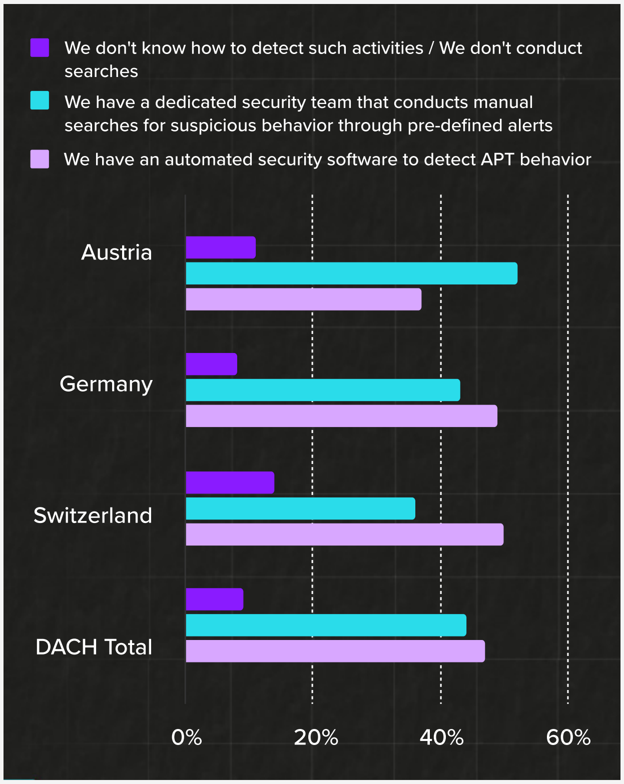
Despite this disparity in investment, most respondents (68%) stated the allocated amount will increase in the upcoming year, with 22% stating it is very likely due to the current multiple crises and 46% stating it is somewhat likely.



COMPLIANCE RULES FIRST, CYBERSECURITY SECOND

At the beginning of the year, the BSI warned that KRITIS will be targeted by specialized APT groups utilizing a variety of tactics, techniques, and procedures (TTPs). As predicted, in this past year we have seen critical infrastructure in danger with attacks on companies such as turbine manufacturer Enercon, oil utility companies, and even the German Chambers of Industry and Commerce. In an environment where the core parts of society are under attack, it is of utmost importance that companies focus on protecting themselves against those advanced persistent threat attacks.

The issue, in these cases, is detection. Results of the survey showcase that less than half (47%) of organizations have specialized software in place to target APT behavior and only 44% have the necessary dedicated security team to look for them in their networks.



Despite the risks of constant cyberattacks and multiple threats growing every day, many IT and OT security experts in DACH are controlling security tools manually to a certain degree. Results show that less than half (47%) of organizations have automated security software in place to detect APTs, which are identified as the most dangerous groups, and are often backed by nation-state actors. On the contrary, 44% of these organizations conduct manual searches for suspicious behavior through predefined alerts. The reason for this might be a lack of funding, but it looks strange that more than 66 % stated that their companies have cyber insurance and of those, only 51% have cyber insurance against incidents caused by threat actors that could be considered as cyberwarfare.

WHY DO THESE FINDINGS MATTER?

The need for automated security detection, which would decrease the time to respond to infiltrations and attacks, seems to be less important than having cyber insurance, which indicates that covering potential damage seems more important than preventing the damage in the first place. This conclusion fits, since the majority of the interviewed experts stated that they are currently in the process of implementing additional technical and organizational standards to be compliant with the latest regulations like IT-Sicherheitsgesetz 2.0, or for the healthcare industry B3S.

> *“Organizations in DACH need to invest more in relevant cyber risk and cyber security frameworks to be prepared for cyberwar attacks not only from hacktivist organizations like ransomware groups but by nation-state attackers,therefore, they need to focus more on asset management to be able to get more visibility into their IT environments, especially the OT that is part of their critical infrastructures. We have already seen attacks on windmills throughout Europe affecting remote control capabilities and leaving damage to the European Grid infrastructure, and we need to be ready to prepare for similar events on a large scale.“*
>
> **MIRKO BULLES**
> DIRECTOR TAM AT ARMIS

ARMIS
THREAT DETECTION & RESPONSE
ENSURE ASSETS ARE SECURED. ALWAYS. EVERYWHERE.
WATCH THE VIDEO

WHAT CAN ORGANIZATIONS DO TO PROTECT THEMSELVES?

Despite some bold statements about being ready for cyberwarfare events, most respondents think of their organizations as not prepared enough, and rightly so. There is an understanding that more budget into cybersecurity is needed in order to survive the storm once it happens. One field that they should look more into is asset management, as this is clearly underestimated so far. The recently released NIS2 will help address the gap. Article 18 prescribes a minimum set of compliant functions that an essential or important entity needs to adopt, and failure to adopt these minimum sets of requirements now also exposes the organization to fines of up to 10 million euros or 2 % of global revenue set out in Article 31. The first of the minimum set of requirements is to have adequate risk analysis. This alone, is a major issue for the majority of essential or important entities, because risk analysis is founded on an understanding of the critical assets that comprise the essential function, and for most organizations an up-to-date and accurate asset register is either non-existent, out of date, or partial at best. To validate cyber security expenditure, it will be vital for organizations to first prove their risk analysis is adequate and appropriate, and in line with NIS2 law.

Traditional inventory tools focus on visibility but do not provide cyber threat intelligence. They require organizations to implement multiple tools to inventory and assess risk in today's hybrid environments. Typically, organizations have an incomplete picture of their assets, don't understand the important context of risk, and leave open security gaps for cybercriminals to exploit. Therefore, security teams need a way to go beyond the static IT/OT inventory of assets to understand the security context.

ARMIS ASSET INTELLIGENCE PLATFORM

The **Armis Asset Intelligence Platform** provides unified asset visibility and security across all asset types, including information technology (IT), internet of things (IoT), operational technology (OT), internet of medical things (IoMT), cloud, and cellular-IoT — both managed and unmanaged. Delivered as an agentless software-as-a-service (SaaS) platform, Armis seamlessly integrates with existing

IT and security stacks to quickly deliver the contextual intelligence needed for improving an organization's security posture, without disrupting current operations or workflows. Armis helps customers protect against unseen operational and cyber risks, increase efficiencies, optimize the use of resources, and safely innovate with new technologies to grow their business – no matter the threat, cyberwarfare or other.

Register today for a Security Risk Assessment to learn which assets are most vulnerable to attack. Use these insights to prioritize your risk mitigation strategy and ensure full compliance with regulatory frameworks that require you to identify and prioritize all vulnerabilities.

To request a custom demo from Armis, please visit: armis.com/demo.

To dive deeper into the findings of the Armis State of Cyberwarfare and Trends Report: 2022-2023 on a global scale, please visit: **armis.com/cyberwarfare.**

THE STATE OF
CYBERWARFARE

ABOUT ARMIS

Armis, the leading asset visibility and security company, provides the industry's first unified asset intelligence platform designed to address the new extended attack surface that connected assets create. Fortune 100 companies trust our real-time and continuous protection to see with full context all managed, unmanaged assets across IT, cloud, IoT devices, medical devices (IoMT), operational technology (OT), industrial control systems (ICS), and 5G. Armis provides passive cyber asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in California.

armis.com

info@armis.com

20230110-1

ARMIS®