2023 Cyber-Incidents in Numbers

Period Covered by Report January 01st - December 31st, 2023

Date of the report: February 5th, 2024

SWISS IT SECURITY GROUP

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

In Focus –

AV-TEST Europe Cyber Incident Analysis for 2023.

Since 2023, our team has dedicatedly collected and analyzed data on cyber incidents across Europe, with a particular focus on Germany. This year's annual review highlights the evolving landscape of cyber threats, emphasizing Distributed Denial of Service (DDoS) and ransomware attacks due to their significant impact and high visibility. These types of cyber incidents have not only become more prevalent but also more sophisticated, presenting substantial challenges to cybersecurity defenses and necessitating a deeper understanding of their mechanisms and repercussions.

Cyber incidents reported by AV-TEST are derived from monitoring activities across both public and deep web sources. It is important to note that these findings may not fully represent the complete landscape of incidents that have occurred.

Europe

Top 20 Countries Attacked in 2023

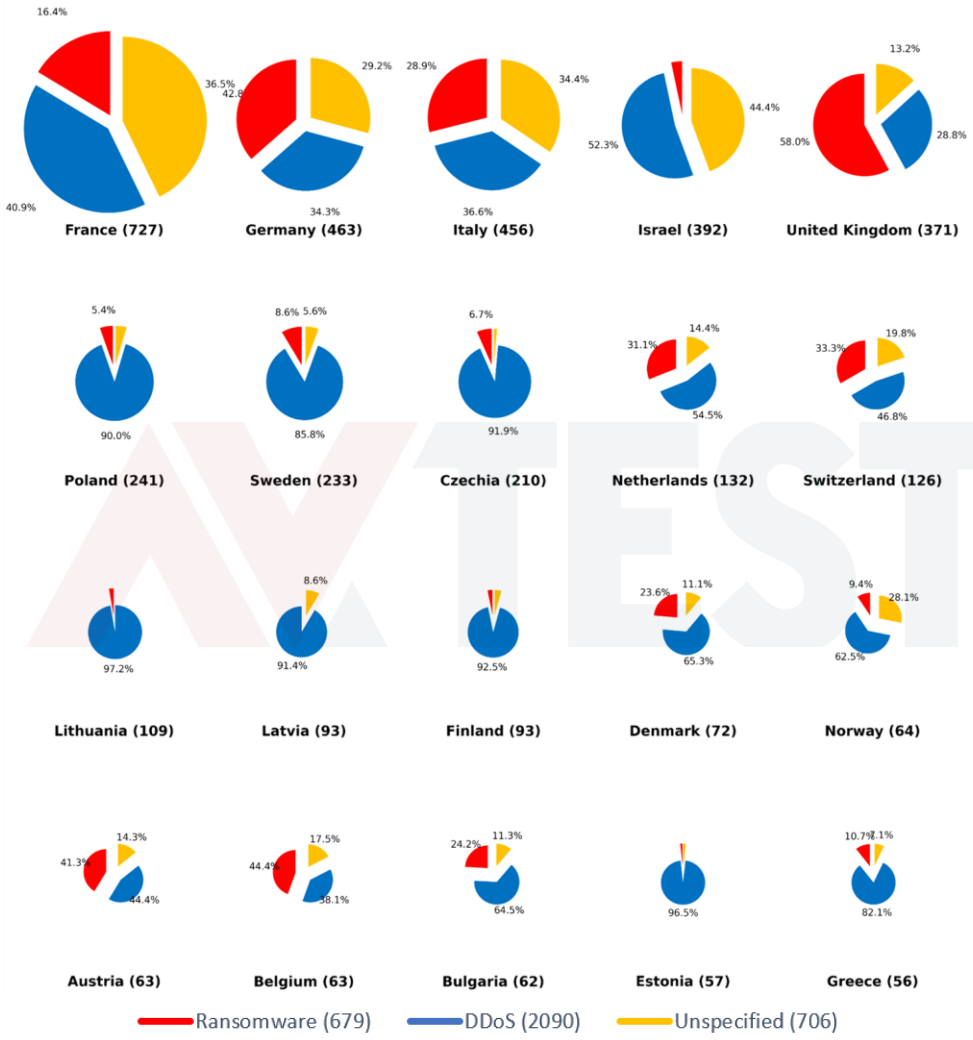

Figure 1: illustrates the distribution of cyber-attacks among the top 20 attacked European countries in 2023, with a breakdown of attack types—ransomware, DDoS, and unspecified—displayed in pie charts for each country. Total attack counts are noted beside the country names.

In 2023, AV-TEST observed a total of 4,618 cyber-attacks in Europe, with Distributed Denial of Service (DDoS) and Ransomware forming the bulk of these malicious activities. Specifically, there were 2,525 DDoS incidents and 1,066 Ransomware attacks, alongside 1,027 unspecified events that include a range of other malicious activities such as data theft for hacktivism or espionage. These figures underline the persistent threat posed by well-known attack vectors, as well as the prevalence of more covert operations.

Country	Ransomware	DDoS	Unspecified	All Attacks
France	119	297	311	727
Germany	169	159	135	463
Italy	132	167	157	456
Israel	13	205	174	392
United Kingdom	215	107	49	371
Poland	13	217	11	241
Sweden	20	200	13	233
Czechia	14	193	3	210
Netherlands	41	72	19	132
Switzerland	42	59	25	126
Lithuania	3	106	0	109
Latvia	0	85	8	93
Finland	3	86	4	93
Denmark	17	47	8	72
Norway	6	40	18	64
Austria	26	28	9	63
Belgium	28	24	11	63
Bulgaria	15	40	7	62
Estonia	1	55	1	57
Greece	6	46	4	56

Table 1: presents a tabulated summary of cyber-attacks in 20 European countries for the year 2023, categorized by type: ransomware, DDoS, unspecified, and the total number of attacks for each country.

Examining the Dynamics of Cyber Threats:
DDoS, Ransomware, and Emerging Attacks in the Second Half of 2023*.

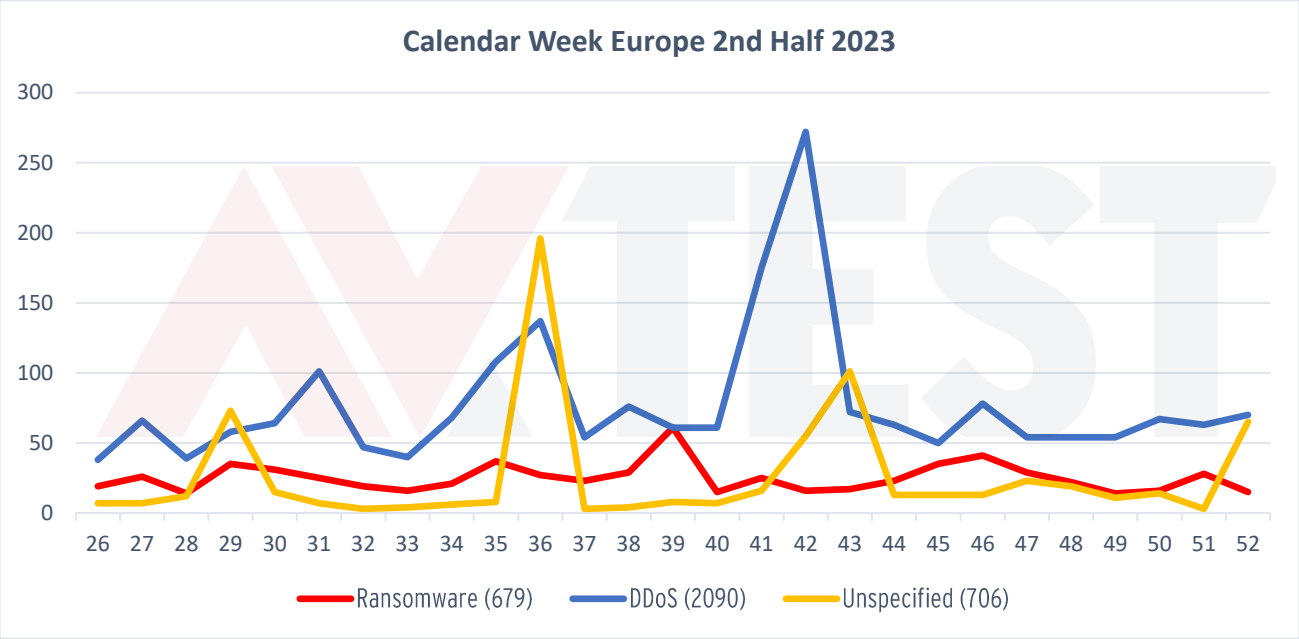

Figure 2: depicts a line graph tracking the weekly incidence of three types of cyber threats—DDoS, ransomware, and unspecified attacks—across European countries during the second half of 2023. Each line represents one threat type, with the total occurrences for the half-year provided in the legend.

The most targeted nations within Europe were France, Germany, Italy, Israel, and the United Kingdom, which faced 727, 463, 456, 392, and 371 attacks respectively. These numbers alone, however, do not tell the full story. Throughout the latter six months of the year, DDoS attacks predominated, likely signifying a surge in hacktivism-related activities. These incidents are characterized by their volatility, with notable peaks that coincide with specific campaigns by hacktivist groups. In contrast, Ransomware attacks displayed a relatively steady occurrence with occasional peaks, indicating a consistent threat presence that organizations faced during this period.

Unspecified attacks are also a constant in the landscape, though generally lower in frequency compared to the other types. However, there are instances of extreme spikes, which may correspond to multifaceted campaigns or underreported incidents that only surfaced upon detailed investigation.

Two significant outbreaks are worth highlighting. In calendar week 36, France experienced a concerted attack by the hacktivist group "Mysterious Team Bangladesh," which claimed to have targeted 188 companies. The group did not disclose the methods employed, leaving the nature of these incidents largely unknown. The second notable surge occurred in week 42, where France once again became the focal point of attacks. This time, the aggression was led by the collective efforts of "AnonGhost Indonesia" and "Anonymous Indonesia," who claimed responsibility for DDoS attacks against 173 French companies.

*The data presented herein covers only the second half of 2023 due to significant modifications in the sources and methodologies for collecting cyber incident information. These adjustments have led to inconsistencies in historical data, rendering it challenging to accurately depict a trend over an extended timeframe. As a result, to maintain the integrity and accuracy of our analysis, we have limited our scope to the period following these changes, ensuring the data reflects the most current and consistent reporting practices available.

Cyber-Attacks Europe 2023 by Population Top 20 Attacked Countries.

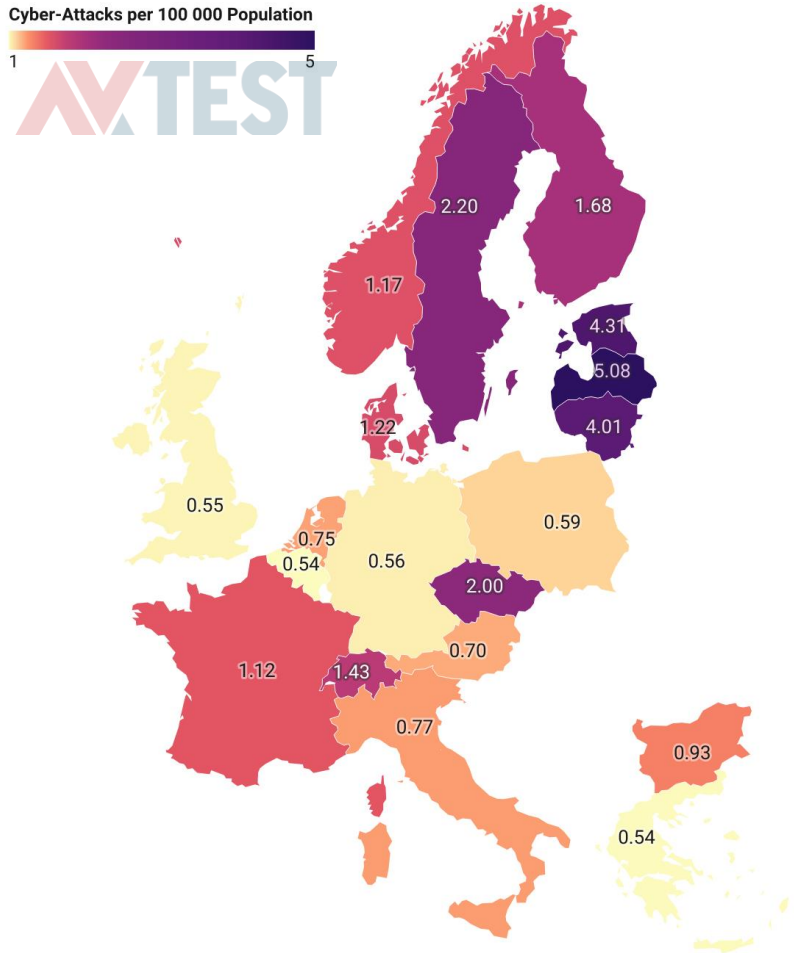

Figure 3: portrays a color-coded map of Europe, indicating the frequency of cyber-attacks per 100,000 population in various countries during 2023. Higher frequencies are shown in darker shades, with specific values annotated on the map.

Country	Attacks per 100 000 Population
Latvia	5,08
Estonia	4,31
Israel	4,19
Lithuania	4,01
Sweden	2,20
Czechia	2,00
Finland	1,68
Switzerland	1,43
Denmark	1,22
Norway	1,17
France	1,12
Bulgaria	0,93
Italy	0,77
Netherlands	0,75
Austria	0,70
Poland	0,59
Germany	0,56
United Kingdom	0,55
Greece	0,54
Belgium	0,54

Table 2: complements the map by listing European countries alongside the exact number of cyber-attacks per 100,000 population, with Latvia having the highest rate and Belgium the lowest.

When examining the density of attacks per capita, a different picture emerges. Smaller countries such as Latvia, Estonia, Israel, Lithuania, and Sweden experienced the highest rates of cyber incidents relative to their population size, with respective figures of 5.08, 4.31, 4.19, 4.01, and 2.20 incidents per 100,000 inhabitants. This suggests that the impact of cyber threats is not solely dependent on a nation's size but also on its cyber resilience and potential value as a target.

It's not only historical factors that make countries like Latvia, Estonia, Lithuania, and to a certain extent Sweden, frequent targets for Russian-based hacktivism, but also their stances regarding the ongoing conflict between Ukraine and Russia. These nations have expressed solidarity with Ukraine and have been vocal critics of Russian actions, which increases their profiles as targets for cyber operations that serve to intimidate or retaliate against political positions.

For Sweden, the situation is compounded by its recent application for NATO membership. This move represents a significant shift in regional security dynamics and is viewed unfavorably by Russia. As a result, Sweden may have become a more pronounced target for cyber-attacks aimed at undermining its NATO accession or simply as a means of expressing geopolitical dissent.

The cyber domain offers a relatively low-risk but high-impact means of exerting influence, gathering intelligence, and potentially destabilizing adversaries or those perceived as threats. For Russian hacktivist groups, whether state-sponsored or nationalist sympathizers, attacking these nations can be seen as an extension of Russia's broader strategic objectives. Cyber-attacks can disrupt critical infrastructure, sow confusion, and serve as a warning to other nations that might consider similar foreign policy stances or alliances.

In the case of the Baltic states, their cyber infrastructure could be seen as both a testbed for Russian cyber capabilities and a frontline of digital confrontation. These countries are not just dealing with the historical legacy of cyber threats but are actively engaged in a contemporary context where cyber operations are an ongoing concern tied to current international tensions.

Germany

The digital security landscape of Germany in 2023 has been meticulously charted in the following set of comprehensive maps, revealing the geographical distribution of cyber incidents across the nation's federal states. These visualizations are essential for understanding the localized impact of two predominant types of cyber threats.

Within Germany, the distribution of cyber-attacks highlights the focal points for malicious activities. North Rhine-Westphalia, Baden-Wurttemberg, Bavaria, Berlin, and Hesse were the most affected regions, with 94, 81, 80, 48, and 40 attacks respectively.

All Observed Cyber-Attacks Germany 2023.

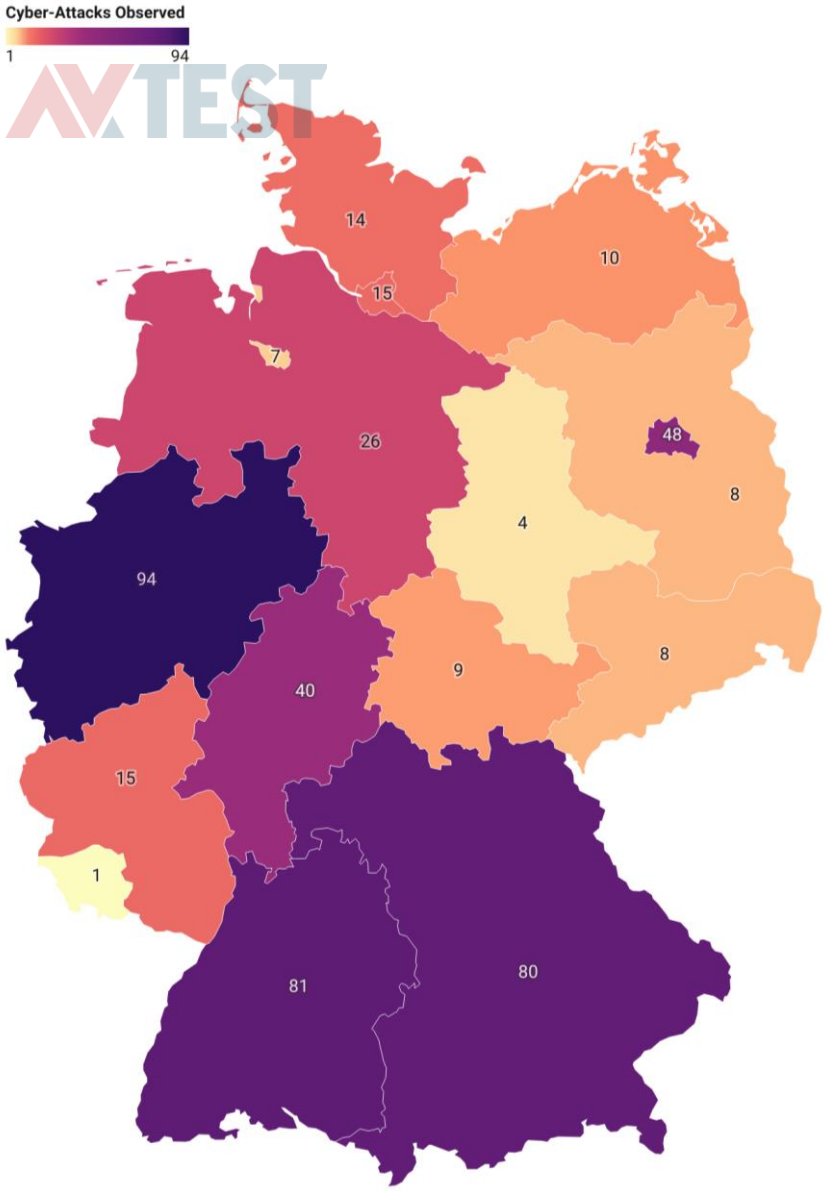

Figure 4: showcases a color-gradient map of Germany, detailing the total number of cyber-attacks observed in each federal state during 2023. Darker shades indicate higher numbers of attacks, with specific counts annotated on the map for notable regions.

Ransomware vs DDoS

For Ransomware and DDoS attacks, each of the following maps offers a granular look at the frequency of these incidents, providing insights into regional vulnerabilities and the resilience of cybersecurity measures across different areas.

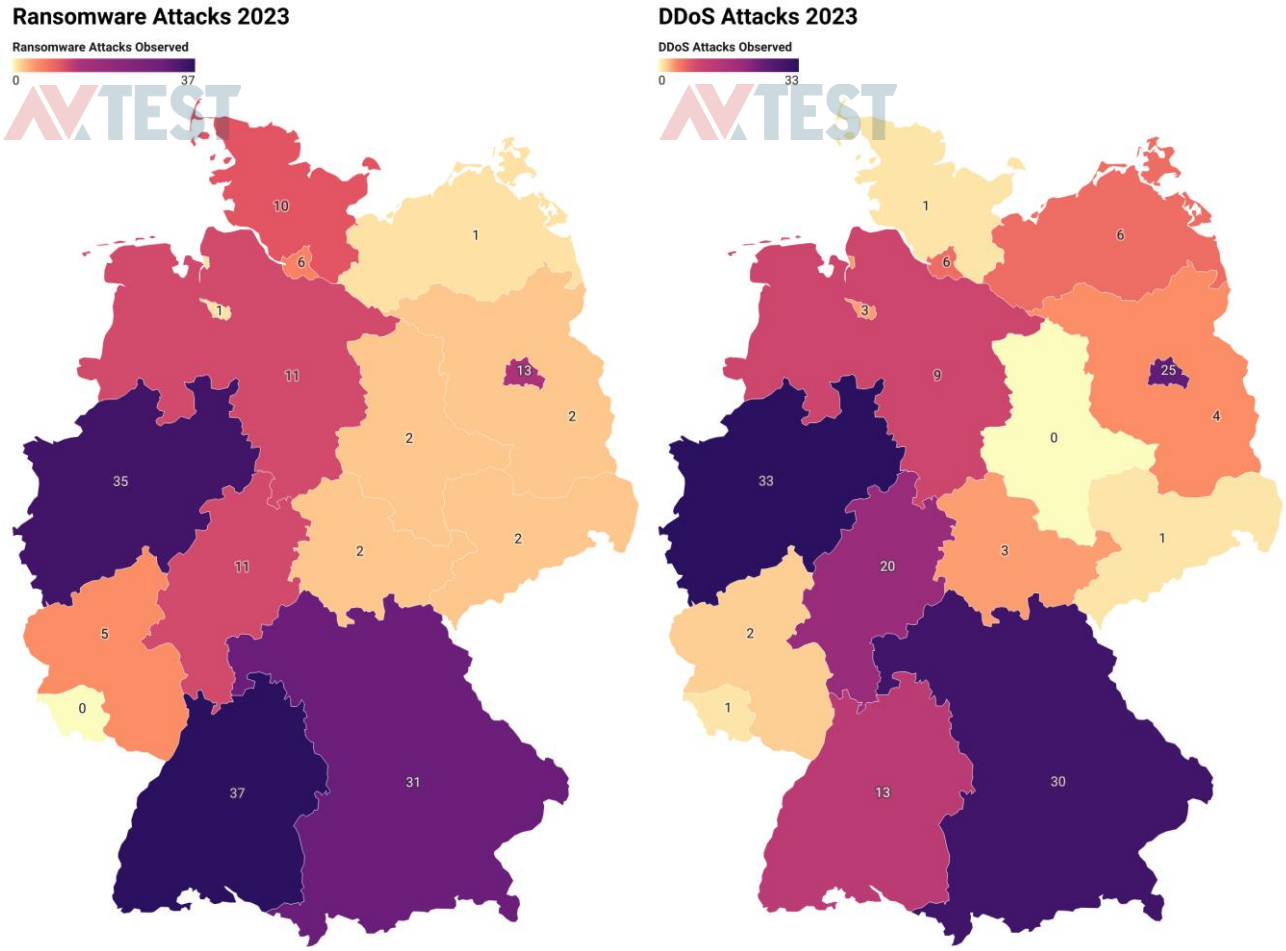

Figure 5: displays two separate color-gradient maps of Germany, each illustrating the regional distribution of two different types of cyber-attacks in 2023. The left map shows the incidence of ransomware attacks, while the right map depicts DDoS attack occurrences. Darker colors represent higher numbers of attacks in the respective states, with specific figures provided for each region.

The first map details Ransomware attacks, a form of malware that encrypts an organization's data and demands payment for its release. This map will highlight the extent to which each German state was affected by these disruptive threats, reflecting the penetration of this particular cybercrime across varied regions.

The second map focuses on DDoS attacks, which flood services with excessive web traffic to disrupt their normal functioning. The visualization will show the intensity of these attacks across the German states, indicating areas where such tactics were most frequently employed.

Together, these maps not only serve as a record of cyber adversities faced in 2023 but also as a tool for strategic planning and resource allocation for future cybersecurity defenses within Germany.

Cyber-Attacks by Population

Adjusting for population size, the highest attack rates per 100,000 inhabitants were observed in Berlin, Bremen, Hamburg, Baden-Wurttemberg, and Hesse, with rates of 1.28, 1.02, 0.79, 0.72, and 0.63 respectively.

Cyber-Attacks Germany 2023 by Population

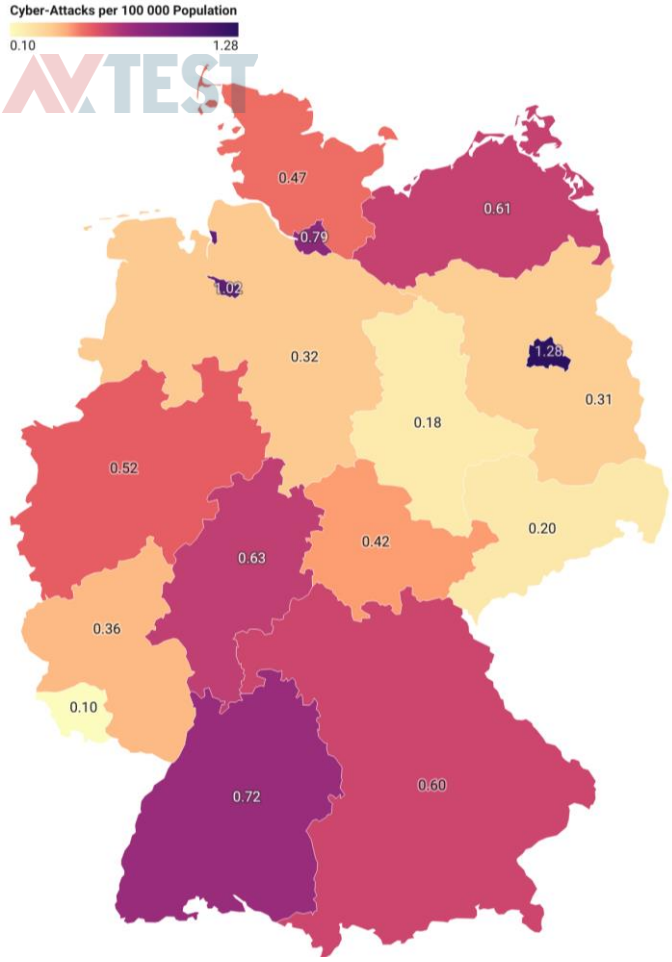

Figure 6: depicts a color-gradient map of Germany showing cyber-attacks per 100,000 population across its federal states in 2023. The intensity of the color indicates the frequency of attacks, with values marked on the map.

States	Attacks per 100 000 Population
Berlin	1,28
Bremen	1,02
Hamburg	0,79
Baden-Wurttemberg	0,72
Hesse	0,63
Mecklenburg-Vorpommern	0,61
Bavaria	0,60
North Rhine-Westphalia	0,52
Schleswig-Holstein	0,47
Thuringia	0,42
Rhineland-Palatinate	0,36
Lower Saxony	0,32
Brandenburg	0,31
Saxony	0,20
Saxony-Anhalt	0,18
Saarland	0,10

Table 3: lists the German federal states alongside the number of cyber-attacks per 100,000 population, detailing the specific attack density with Berlin recording the highest rate.

The data presented indicates a disproportionate concentration of cyber-attacks in Germany's city-states when adjusted for population size. The city-states of Berlin, Bremen, and Hamburg exhibit the highest rates of cyber-attacks per 100,000 inhabitants, suggesting that these densely populated urban areas are particularly attractive targets for cybercriminals.

Several factors likely contribute to this trend:

1. **High Connectivity**: City-states have a dense concentration of businesses and individuals who are highly connected to digital networks, providing a larger attack surface for cybercriminals.
2. **Concentration of Authorities in Berlin:** As the capital city of Germany, Berlin has a high concentration of federal agencies and governmental bodies. These entities are often the targets of Distributed Denial of Service (DDoS) attacks, which aim to disrupt services and access to information by overwhelming

systems with a flood of internet traffic. Such attacks can be politically motivated or may seek to cause disruption as a form of protest or statement.

3. **Economic Significance:** These city-states are economic powerhouses with significant commercial activity. Cyber-attacks, especially ransomware and DDoS, tend to target regions with thriving business sectors, aiming to disrupt operations and demand higher ransoms due to the higher stakes involved.
4. **Visibility and Impact:** Attacks on prominent cities often gain more media attention, which may be appealing for hacktivists seeking to publicize a cause or for cybercriminals wishing to demonstrate their capabilities.
5. **Resource Allocation:** The concentration of wealth and resources in city-states may lead to better cybersecurity infrastructure. However, this also means that successful attacks could yield more valuable data or cause more disruption, incentivizing more persistent and sophisticated attacks.
6. **Cybersecurity Challenges:** The complex infrastructure and diverse range of organizations in city-states may present unique challenges in terms of cybersecurity coordination and response, potentially leading to vulnerabilities that can be exploited.

Underrepresentation in the East: The data shows that eastern states like Saxony, Saxony-Anhalt, and Brandenburg have some of the lowest rates of cyber-attacks per capita. This could be due to several factors:

1. **Fewer High-Value Targets**: These areas may have fewer large corporations or high-value infrastructure targets, which tend to attract more sophisticated cyber threats.
2. **Economic Factors**: The economic profile of these regions might not be as attractive for certain types of economically motivated cybercrime.
3. **Visibility and Reporting**: There might also be differences in the visibility and reporting of cyber incidents. If cybersecurity measures or awareness are less developed, some attacks might go unreported.

The observed data reflects the heightened risk faced by urban centers in the cyber domain. While more populous states like North Rhine-Westphalia, Baden-Wurttemberg, and Bavaria experienced a higher number of attacks in absolute terms, the per capita rate in the city-states suggests a targeted pattern of cyber incidents. This could imply that cybercriminals are deploying strategic choices to focus on targets where potential gains are maximized or where defenses may be uneven, despite the concentration of resources.

Understanding the motives and methods behind these targeted attacks is crucial for developing effective cybersecurity strategies that can protect these critical urban centers, which play a vital role in Germany's economy and societal functions.

Collected and Curated by
David Walkiewicz, Director Test Research, AV-TEST GmbH
Jens Lichtenstein, Testing Engineer, AV-TEST GmbH
Maik Morgenstern, CTO, AV-TEST GmbH

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

About **AV-TEST**

AV-TEST GmbH is an independent supplier of services in the fields of IT Security and Antivirus Research, focusing on the detection and analysis of the latest malicious software and its use in comprehensive comparative testing of security products.

Due to the timeliness of the testing data, malware can instantly be analyzed and categorized, trends within virus development can be detected early, and IT-security solutions can be tested and certified. The AV-TEST Institute's results provide an exclusive basis of information helping vendors to optimize their products, special interest magazines to publish research data, and end users to make good product choices.

AV-TEST has operated out of Magdeburg (Germany) since 2004 and employs more than 30 team members, professionals with extensive practical experience.

The AV-TEST laboratories include 300 client and server systems, where more than 2,500 terabytes of independently-collected test data, containing both malicious and harmless sample information, are stored and processed.

For more information please visit our website at https://www.av-test.org .

Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web https://www.av-test.org