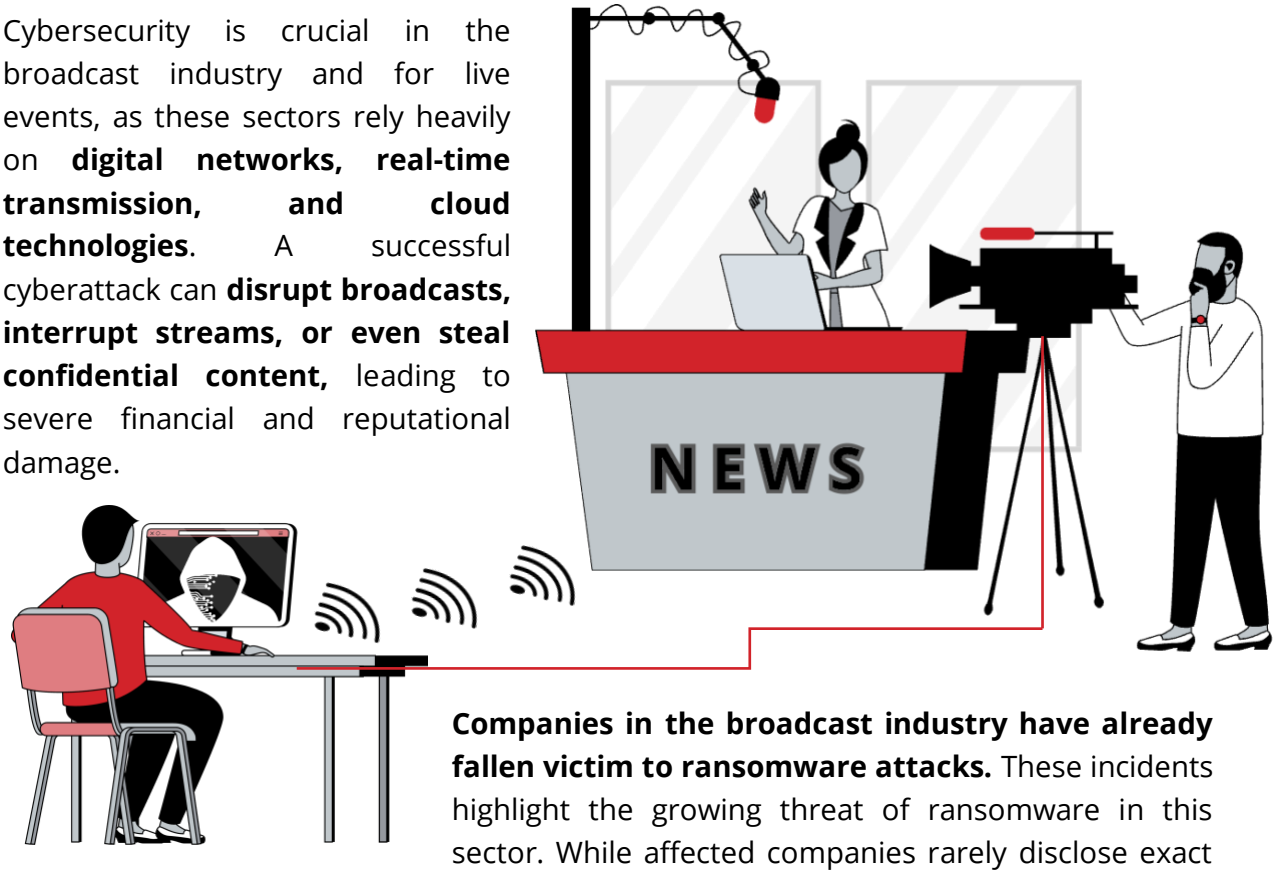
# CYBERSECURITY FOR BROADCAST & EVENTS

Cybersecurity is crucial in the broadcast industry and for live events, as these sectors rely heavily on **digital networks, real-time transmission, and cloud technologies**. A successful cyberattack can **disrupt broadcasts, interrupt streams, or even steal confidential content,** leading to severe financial and reputational damage.




**Companies in the broadcast industry have already fallen victim to ransomware attacks.** These incidents highlight the growing threat of ransomware in this sector. While affected companies rarely disclose exact financial losses, they are presumed to be substantial.

**Sinclair Broadcast Group (USA)**

In October 2021, Sinclair Broadcast Group, one of the largest TV networks in the U.S., was targeted by a ransomware attack. This incident disrupted numerous TV stations and caused significant interruptions to broadcasting operations.

**Pop TV (Slovenia)**

In 2021, Pop TV, Slovenia's leading television network, suffered a cyberattack, reportedly with extortion as the motive. The attack compromised the network's IT systems and disrupted the display of graphics during a news broadcast.

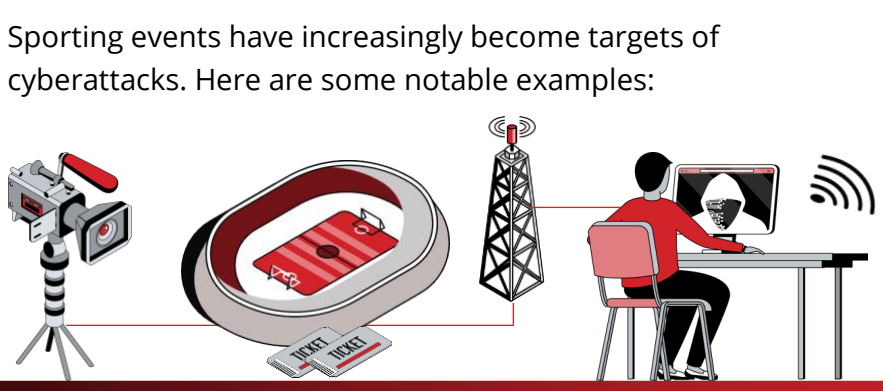
**Sky Deutschland (Germany)**

Reports suggest that in 2023, Sky Deutschland was affected by a cyberattack, though exact details and its full impact have not been disclosed.

## SPECIFIC THREATS TO THE BROADCAST AND EVENT SECTOR

| TV Broadcasters & OTT Providers<br>*(ARD, BBC, ESPN, Netflix, DAZN, Sky, etc.)* | Production Companies<br>*(IMG Studios, Game Creek Video, Sunset+Vine, NEP, etc.)* |
|---|---|
| • DDoS attacks → Streaming services or live TV broadcasts can be disrupted.<br><br>• Ransomware attacks → Critical production systems and broadcast signals can be encrypted.<br><br>• Signal hijacking → Hackers could inject illegal content or fake news.<br><br>• Data breaches → Customer data or subscription information could be stolen. | • Manipulation of video content → False or compromised broadcasts.<br><br>• Theft of copyrighted material → Premature release or resale.<br><br>• Attacks on remote production → IP-based workflows are particularly vulnerable. |

Sporting events have increasingly become targets of cyberattacks. Here are some notable examples:




### Olympic Games

• PyeongChang 2018: During the opening ceremony, a cyberattack disrupted the IT infrastructure of the Games, causing outages in internet and broadcast systems.

• Tokyo 2021: The Olympic Games saw a surge in cyberattacks, with a total of 4.4 billion registered incidents—20 times more than at the 2012 Games.

### Soccer Events

• Champions League Match PSG vs. FC Barcelona 2024: Two days before the quarterfinal first leg, Paris Saint-Germain's ticketing system was targeted in a cyberattack. While no data was stolen, additional security measures were implemented.

• French Football Federation 2024: A similar attack resulted in data exfiltration, highlighting the vulnerability of sports organizations.

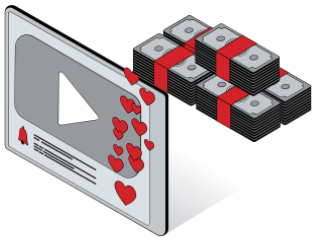
### Rugby

• French Rugby Federation (FFR) 2023: In June 2023, the FFR fell victim to a cyberattack, with threats to leak sensitive information—further emphasizing the growing cybersecurity risks for sports organizations.

## GENERAL THREAT LANDSCAPE

According to the United Kingdom's National Cyber Security Centre (NCSC), over 70% of surveyed sports organizations experience at least one cyberattack per year, highlighting the sector's vulnerability to digital threats.


**Attacks on digital infrastructure of stadiums & event organizers → Ticketing systems, LED screens, and stadium Wi-Fi networks are prime targets.**



**Live streaming piracy → Rights holders lose millions due to illegal streams.**

**Fake betting & data manipulation → Betting relies on real-time data, which can be targeted by cybercriminals.**

These incidents emphasize the need for sports organizations to implement robust cybersecurity measures to protect against the rising tide of digital threats. (See also: Infront Sports & Media.)

## WHY IS CYBERSECURITY PARTICULARLY IMPORTANT HERE?

**Live broadcasts & streaming are time-critical**

There's no second chance if a cyberattack occurs during an event.

**Digital Workflows & Remote Production**

Increased attack surfaces due to IP-based transmission.

**Valuable media assets & copyrights**

Content must be protected from theft and manipulation.

**Compliance with data protection regulations (GDPR, NIS2)**

Severe penalties for data breaches or service disruptions.

The broadcast and event industry must adopt modern security solutions such as **EDR/XDR, Zero Trust, SIEM, and DDoS protection** to defend against cyberattacks. **Specialized security services for media companies** are particularly crucial to safeguarding live streams, digital content, and production networks.

# RIEDEL NETWORKS FOR BROADCAST-CYBERSECURITY

RIEDEL Networks is not a traditional cybersecurity provider, but its highly secure network solutions and managed security services are particularly relevant to the broadcast industry. Especially for live sports events and critical media infrastructures, RIEDEL offers a strong security framework with its **RIEDEL Enterprise Defense [R.E.D.]** product suite.

## Specialization in Media & Broadcast Networks

- RIEDEL Networks operates dedicated, secure network infrastructures for media companies.
- Clients include TV broadcasters, production companies, and sports event organizers (e.g., Formula 1, UEFA, Eurovision).

## Security-Focused Network Services

- End-to-end encryption & protection for broadcast streams.
- DDoS mitigation & firewalls for media and live streaming applications.
- Redundant & latency-optimized networks for live transmissions.

## RIEDEL Enterprise Defense [R.E.D.] – Cybersecurity Solution

- Integrated EDR/XDR, SIEM & SOC services.
- Hosting & data protection compliant with EU standards (GDPR, NIS2).
- Customizable for media companies & streaming services.

**About RIEDEL Networks**

RIEDEL Networks is a privately owned, global network provider specializing in tailormade network solutions. Recognized as a Niche Player in the Gartner Magic Quadrant for Global WAN Services, RIEDEL focuses on mid-sized international enterprises as well as the media and event sectors.

With its own global backbone, RIEDEL Networks enables businesses to stay connected worldwide. Its services include internet connectivity, MPLS, SD-WAN, SASE, Cloud Connect, security, and more. Clients across various industries value quality, security, and reliability.

RIEDEL Networks is a 100% subsidiary of RIEDEL Communications Group in Wuppertal, Germany, and is fully privately owned by Thomas Riedel.

For more information, visit www.riedel-networks.net