CYBERSECURITY FÜR BROADCAST & EVENTS

Cybersecurity ist in der Broadcast-Branche und für Live-Events entscheidend, da diese Sektoren stark auf **digitale Netzwerke, Echtzeitübertragung und Cloud-Technologien** angewiesen sind. Ein erfolgreicher Cyberangriff kann **Sendungen stören, Streams unterbrechen** oder sogar **vertrauliche Inhalte stehlen,** was massive finanzielle und reputationsbezogene Schäden verursachen kann.

Unternehmen in der Broadcast-Branche wurden bereits Opfer von Ransomware-Angriffen. Diese Vorfälle verdeutlichen die wachsende Bedrohung durch Ransomware-Angriffe in der Broadcast-Branche. Konkrete Schadenssummen werden von den betroffenen Unternehmen oft nicht genannt, sind aber vermutet recht hoch.

Sinclair Broadcast Group (USA)

Im Oktober 2021 wurde die Sinclair Broadcast Group, eines der größten TV-Netzwerke in den USA, Ziel eines Ransomware-Angriffs. Dieser Vorfall beeinträchtigte zahlreiche TV-Stationen und führte zu erheblichen Störungen im Sendebetrieb.

Pop TV (Slowenien)

Im Jahr 2021 wurde Pop TV, der führende Fernsehsender in Slowenien, Opfer eines Cyberangriffs, der vermutlich auf Erpressung abzielte. Der Angriff beeinträchtigte das Computernetzwerk des Senders und störte die Ausstrahlung von Grafiken während der Nachrichtensendung.

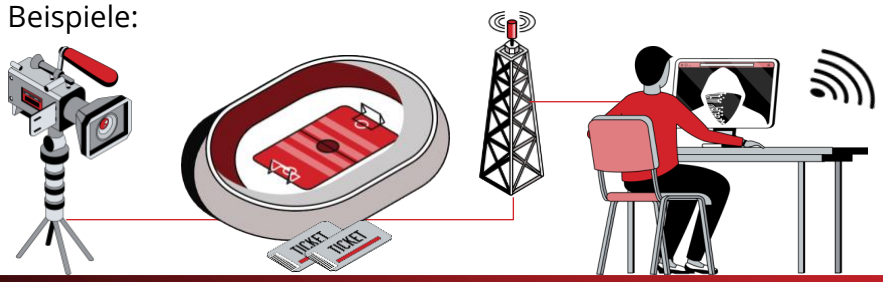
Sky Deutschland (Deutschland)

Berichten zufolge war Sky Deutschland im Jahr 2023 von einem Cyberangriff betroffen, wobei genaue Details und Auswirkungen nicht vollständig offengelegt wurden.

SPEZIFISCHE BEDROHUNGEN FÜR DIE BROADCAST- UND EVENT-BRANCHE

TV-Sender & OTT-Anbieter *(ARD, BBC, ESPN, Netflix, DAZN, Sky, etc.)*	Produktionsfirmen *(IMG Studios, Game Creek Video, Sunset+Vine, NEP, etc.)*
• DDoS-Angriffe → Streaming-Dienste oder Live-TV können ausfallen. • Ransomware-Angriffe → Kritische Produktionssysteme und Sendesignale werden verschlüsselt. • Signal-Hijacking → Hacker könnten illegale Inhalte oder Fake News einspeisen. • Datenlecks → Kundendaten oder Abonnementinformationen können gestohlen werden.	• Manipulation von Videoinhalten → Falsche oder kompromittierte Übertragungen. • Diebstahl von urheberrechtlich geschütztem Material → Vorabveröffentlichung oder Weiterverkauf. • Angriffe auf Remote-Produktion → IP-basierte Workflows sind besonders anfällig.

Auch Sportveranstaltungen sind zunehmend Ziel von Cyberattacken geworden. Hier einige bemerkenswerte Beispiele:



Olympische Spiele

• PyeongChang 2018: Während der Eröffnungszeremonie wurde die IT-Infrastruktur der Spiele durch einen Cyberangriff beeinträchtigt, was zu Ausfällen von Internet- und Broadcast-Systemen führte.

• Tokyo 2021: Die Olympischen Spiele verzeichneten einen Anstieg von Cyberattacken, mit insgesamt 4,4 Milliarden registrierten Angriffen, was eine zwanzigfache Steigerung im Vergleich zu den Spielen 2012 bedeutet.

Fußballveranstaltungen

• Champions-League-Spiel PSG vs. FC Barcelona 2024: Zwei Tage vor dem Viertelfinal-Hinspiel wurde das Ticketingsystem von Paris Saint-Germain Ziel eines Cyberangriffs. Obwohl keine Daten entwendet wurden, wurden zusätzliche Sicherheitsmaßnahmen implementiert.

• Französischer Fußballverband 2024: Ein ähnlicher Angriff ermöglichte die Exfiltration von Daten, was die Verwundbarkeit von Sportorganisationen unterstreicht.

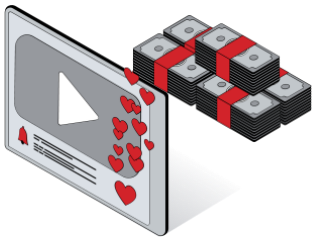
Rugby

• Französischer Rugby-Verband (FFR) 2023: Im Juni 2023 wurde der FFR Opfer eines Cyberangriffs mit der Drohung, Informationen offenzulegen, was die wachsende Bedrohung für Sportorganisationen verdeutlicht.

ALLGEMEINE BEDROHUNGSLAGE

Laut dem National Cyber Security Centre (NCSC) des Vereinigten Königreichs erleben über 70 % der befragten Sportorganisationen jährlich mindestens einen Cyberangriff, was die Anfälligkeit des Sektors für digitale Bedrohungen unterstreicht.

Angriffe auf digitale Infrastruktur von Stadien & Veranstaltern → Ticket-Systeme, LED-Wände, Stadion-WLANs.



Live-Streaming-Piraterie → Rechteinhaber verlieren Millionen durch illegale Streams.

Fake-Betting & Datenmanipulation → Wetten basieren auf Echtzeit-Daten, die Ziel von Angriffen sein können.

Diese Vorfälle verdeutlichen die Notwendigkeit für Sportorganisationen, robuste Cybersicherheitsmaßnahmen zu implementieren, um sich gegen die zunehmenden digitalen Bedrohungen zu schützen. Siehe auch Infront Sports & Media

WARUM IST CYBERSICHERHEIT HIER BESONDERS WICHTIG?

Live-Sendungen & Streaming sind zeitkritisch

Es gibt keine zweite Chance bei einem Hack während eines Events.

Digitale Workflows & Remote-Produktion

Mehr Angriffsflächen durch IP-basierte Übertragung.

Wertvolle Medien-Assets & Urheberrechte

Inhalte müssen vor Diebstahl & Manipulation geschützt werden.

Einhaltung von Datenschutzvor-gaben (DSGVO, NIS2)

Hohe Strafen bei Datenlecks oder Ausfällen.

Die Broadcast- und Eventbranche muss moderne Sicherheitslösungen wie **EDR/XDR, Zero Trust, SIEM & DDoS-Schutz** einsetzen, um sich gegen Cyberangriffe zu wappnen. Besonders wichtig sind **spezialisierte Security-Services für Medienunternehmen**, um Livestreams, digitale Inhalte und Produktionsnetzwerke zuverlässig zu schützen.

RIEDEL NETWORKS FÜR BROADCAST-CYBERSECURITY

Riedel Networks ist kein klassischer Cybersecurity-Anbieter, aber ihre hochgradig gesicherten Netzwerklösungen & Managed Security Services sind für die Broadcast-Branche besonders relevant. Vor allem für Live-Sport-Events & kritische Medieninfrastrukturen bietet Riedel mit der Product-Suite **RIEDEL Enterprise Defense** [**R.E.D.**] ein starkes Sicherheitskonzept. 🚀

Spezialisierung auf Medien- & Broadcast-Netzwerke

- Riedel Networks betreibt dedizierte, sichere Netzwerkinfrastrukturen für Medienunternehmen.
- Kunden sind TV-Sender, Produktionsfirmen & Sportevent-Veranstalter (z. B. Formel 1, UEFA, Eurovision).

Sicherheitsorientierte Netzwerkdienste

- End-to-End-Verschlüsselung & Schutz für Broadcast-Streams
- DDoS-Abwehr & Firewalls für Medien- und Live-Streaming-Anwendungen
- Redundante & latenzoptimierte Netze für Live-Übertragungen

RIEDEL Enterprise Defense [R.E.D.] – Cybersecurity-Lösung

- Integrierte EDR/XDR, SIEM & SOC-Services
- Hosting & Datenschutz nach EU-Standards (DSGVO, NIS2-konform)
- Anpassbar an Medienunternehmen & Streaming-Dienste

Über RIEDEL Networks

RIEDEL Networks ist ein in Privatbesitz befindlicher, globaler Netzwerkanbieter, der sich auf maßgeschneiderte Netzwerke konzentriert. Wir sind im Gartner Magic Quadrant für Global WAN Services als Nischenanbieter gelistet, der auf mittelständische internationale Unternehmen und den Medien- und Veranstaltungssektor spezialisiert ist. Mit unserem eigenen globalen Backbone unterstützen wir Unternehmen dabei, weltweit vernetzt zu sein. Unsere Dienstleistungen umfassen Internetverbindungen, MPLS, SD-WAN, SASE, Cloud Connect, Security und vieles mehr. Unsere Kunden stammen aus verschiedenen Branchen und schätzen Qualität, Sicherheit und Zuverlässigkeit. RIEDEL Networks ist ein 100%iges Unternehmen der RIEDEL Communications Gruppe in Wuppertal, Deutschland, und ist vollständig im Privatbesitz von Thomas Riedel.

Weitere Informationen über Riedel Networks unter www.riedel-networks.net