Foto: Gerd Pachauer

Ein modernes Stadion ist eine hochtechnisierte, digitalisierte und vernetzte Einrichtung

Vorbereitung und Cyber-Awareness

Sportveranstaltungen sind multimediale Ereignisse. Moderne Stadien sind hochtechnisierte, digitalisierte und vernetzte Einrichtungen. Neue Technologien bieten neue Angriffsflächen für Kriminelle. Für Organisationen, Verbände und Veranstalter ist es erforderlich, sich auf Cyber-Angriffe einzustellen.

Cyber-Sicherheit entwickelt sich von einem ursprünglich individuellen Problem hin zu einer sicherheitspolitischen Herausforderung mit gesamtgesellschaftlicher Dimension. Die Gründe dafür liegen in der steigenden Computer-Kriminalität, in der zunehmenden Verflechtung von Infrastruktur mit dem Internet sowie in einer wachsenden Abhängigkeit des Staates, der Wirtschaft und der Gesellschaft von einer funktionierenden IKT-Infrastruktur. Diese Entwicklung wirft ihre Schatten auch auf die Welt des Sports. Vergleicht man sportliche Großereignisse, wie Olympische Spiele, Welt- und Europameisterschaften oder internationale Endspiele von früher mit jenen von heute, könnten die Unterschiede nicht größer sein.

Heutige Sportveranstaltungen sind multimediale Events. Der sportliche Wettkampf ist nur mehr ein Element unter vielen. Mindestens von gleicher Bedeutung sind die mediale Aufbereitung, ein Rahmenprogramm, Werbe- und Sponsoringaktivitäten und begleitende Aktivitäten im Internet, insbesondere in den sozialen Medien. Die Sportstätten von einst sind mit den Arenen von heute nicht mehr vergleichbar. Ein modernes Stadion ist eine hochtechnisierte, digitalisierte und vernetzte Einrichtung. Elektronisch gesteuerte Flutlichtanlagen, Bewässerungssysteme oder Rasenheizungen, computerisierte Anzeigetafeln, Zutrittssysteme und Schließanlagen sind heute Standard. Diese technologischen Entwicklungen bieten Angriffsflächen für Kriminelle und Aktivisten.

Gefahren. In diesem Zusammenhang sind verschiedene Szenarien denkbar. Dabei kann es sich um harmlose Aktivitäten handeln, wie das nicht autorisierte Platzieren von aktivistischen Botschaften auf digitalen Werbeflächen. Schnell können aber auch Dimensionen mit erheblichem Schadenspotenzial erreicht werden. Eine durch einen gezielten Ausfall der Stadionbeleuchtung herbeigeführte Massenpanik – in Kombination mit einer Arretierung der Zutrittssysteme – kann leicht zu einer Situation führen, die mit der Katastrophe im Hillsborough Stadium im April 1989 mit 97 Toten und 766 Verletzten vergleichbar ist.

Motivlage. Oft wird das sportliche Ereignis dazu missbraucht, die Ziele der Täter zu erreichen, meist ist es Bereicherungsabsicht. Cyber-Kriminalität ist mittlerweile der umsatzstärkste Bereich der organisierten Kriminalität. Sportliche Events sind auch ein vielversprechendes Ziel für Erpressungsangriffe, insbesondere mit Ransomware. Dabei werden Daten des Veranstalters verschlüsselt – für die Entschlüsselung ist die Zahlung eines Lösegeldes erforderlich. Darüber hinaus darf nicht vergessen werden, dass Großveranstaltungen stets aufs Neue das Interesse eines Millionen- mitunter Milliardenpublikums erregen. Dies bietet Aktivisten eine Bühne, um ihre politischen, weltanschaulichen oder religiösen Überzeugungen darzustellen. Und letztlich ist

Ein Ausfall der Stadionbeleuchtung durch einen Cyber-Angriff kann zu einer Massenpanik führen

gerade in der gegenwärtigen Zeit das Thema Geopolitik ein starker Antrieb für Angreifer. Wird beispielsweise ein Staat von Spielen ausgeschlossen, können Rachebestrebungen eine starke Motivation sein, das Ereignis zu stören.

Angriffe. Das britische National Cyber Security Center veröffentlichte 2020 einen umfassenden Bericht zu Cyber-Bedrohungen für Organisationen im Sportbereich. Kernaussagen sind, dass etwa 70 Prozent der Organisationen sich bereits mit einem Cyber-Vorfall konfrontiert sahen, bei 30 Prozent waren es mehr als fünf solcher Vorfälle in den letzten 12 Monaten. 30 Prozent der Cyber-Vorfälle führten zu einem finanziellen Schaden über 10.000 Pfund. Der höchste bekannt gewordene Schaden eines einzelnen Vorfalls betrug vier Millionen Pfund.

Mediale Aufmerksamkeit erregten die Cyber-Angriffe auf die Olympischen Spiele 2018 in Pyeongchang, wo es infolge eines Angriffes mit der Schadsoftware „Olympic Destroyer" zu Problemen im Internet TV-System, im Medienzentrum und bei den Wettkampftickets kam, oder das Finale der Champions League 2018 in Kiew, wo Angreifer mehr als 500.000 Internet-of-Things-Geräte infizierten und es zu massiven Problemen bei WiFi und Web Broadcasting kam.

Soziale Medien. Kanäle in sozialen Medien stellen für die Organisationen eine wichtige Kommunikationsschnittstelle dar. Diese Kanäle haben eine hohe Reichweite und weisen eine hohe Seriosität auf. Werden solche Kanäle angegriffen, bietet sich für Täter die Chance, Falschinformationen an ein Millionenpublikum zu verbreiten.

Vorbereitung und Cyber-Awareness. Für Organisationen, Verbände und Veranstalter ist es erforderlich, sich auf Cyber-Angriffe einzustellen. Die wichtigste Maßnahme ist die Vorbereitung auf mehreren Ebenen.

Am Anfang der Überlegungen sollte eine Bewusstseinsbildung darüber stattfinden, welche Daten und Dienste für die jeweilige Organisation zentral sind. Was wird benötigt, um das Kerngeschäft aufrecht erhalten zu können? Wie könnten Schadensszenarien aussehen? Was wären die Konsequenzen?

Organisationen sollten vorab klären, wer im Angriffsfall helfen kann. Dabei kann es sich um spezialisierte Dienstleister, eigene Experten oder staatliche Stellen handeln. Gleichfalls sollte bekannt sein, welche Aufgaben den Einheiten zukommen und welche Garantien Dienstleister geben können.

Letztlich muss den Beteiligten klar sein, was in einem Angriffsfall zu tun ist. Dafür ist es erforderlich, detaillierte Krisenpläne auszuarbeiten, diese Pläne allen Beteiligten zu kommunizieren und die Pläne regelmäßig zu üben. Letzteres wird oft vernachlässigt und führt im Ernstfall zu einer ineffektiven Reaktion.

Cyber-Sicherheit Über all diesen Maßnahmen steht die Bewusstseinsbildung bei allen Beteiligten, die „Cyber-Awareness". Cyber-Sicherheit ruht auf drei Säulen: den technischen und organisatorischen Maßnahmen und vor allem den Menschen. Wenn sich alle Beteiligten der Gefahren der digitalisierten und vernetzten Welt bewusst sind und ihr Handeln daran orientieren, können viele Gefahren von vornherein ausgeschlossen werden. Nicht vergessen werden darf, dass auch komplexe Angriffe häufig mit dem unbedachten Öffnen einer E-Mail-Anlage oder dem Klick auf einen Hyperlink beginnen.

Philipp Blauensteiner/Martin Merka

FOTO: GERD PACHAUER