ANWENDERBERICHT
1. FSV MAINZ 05 e.V.

macmon intelligent einfach

Zuverlässig in der Abwehr dank macmon Network Access Control

macmon NAC sichert das Netzwerk in der Arena des 1. FSV Mainz 05 e.V. vor unberechtigten Zugriffen

Wenn in der Bundesliga der Ball rollt, konzentriert sich jeder Fan auf das Spiel seiner Mannschaft. Im Hintergrund läuft die IT-Abteilung auf Hochtouren, um „Eigentore" zu vermeiden.

Der Verein 1. FSV Mainz 05 e.V zählt inzwischen zu den etablierten Sportvereinen in der Bundesliga.
Die MEWA Arena bietet Platz für mehr als 33.000 Fans. Im Unterschied zu gängigen Büronetzen, sorgt der Spielbetrieb für besondere Anforderungen an die IT: So ist beispielsweise das Wi-Fi-Netz eines Stadions gekennzeichnet durch komplexe und anspruchsvolle Servicebereitstellung in Echtzeit.
In der IT-Infrastruktur eines Fußballvereins ist ein reibungslos funktionierendes Wi-Fi-6-Netz ein zentraler Faktor für die Besucherzufriedenheit, denn Zuschauer möchten das Live-Erlebnis via Smartphone filmen und beispielsweise in den sozialen Medien mit Freunden oder der Familie teilen. Journalisten und Fans verbinden sich zeitgleich mit dem Stadion-Netzwerk, haben jedoch getrennte Zugänge. Außerdem ist die Nutzung der Mainz-05-App ein wichtiger Faktor für die Fanbindung des Vereins und die Möglichkeit, in engem Kontakt mit seinen Fans zu bleiben. Im Wettbewerb mit TV-Angeboten, wird es immer wichtiger, das Erlebnis im Stadion multimedial zu gestalten. Die große Herausforderung besteht somit in der Bereitstellung eines ausreichenden Signals, aber vor allen Dingen der extrem hohen Benutzerdichte. So wurden an einem typischen Spieltag **1.472 autorisierte Verbindungen und 8.775 unautorisierte Verbindungen mit insgesamt 50 Gerätegruppen** genutzt.

Foto: 1. FSV Mainz 05 e.V.

Damit der Spielbetrieb in einem Bundesliga-Stadion reibungslos funktioniert, muss auch die IT-Abteilung in Top-Form sein.

Foto: 1. FSV Mainz 05 e.V.

Die **Mainz-05-App** ist ein wichtiger Faktor für die Fanbindung des Vereins

„Im Vergleich zu anderen am Markt verbreiteten Management- und Zugangssicherungssystemen der großen Hardware-Hersteller bietet uns macmon secure eine äußerst komfortabel zu bedienende Lösung."

Karsten Lippert, Leiter ICT & Digitalisierung 1. FSV Mainz 05 e.V.

Foto: 1. FSV Mainz 05 e.V.

Standorte	Kassensysteme	Endgeräte (59% mobil)	Office-Nutzer
5	210	467	460

Das Wi-Fi-Netz des 1. FSV Mainz 05 e.V. muss in der Lage sein, Benutzer zu erkennen, deren Netzwerkzugriff zu kontrollieren, differenzierte Services bereitzustellen und widerstandsfähig vor potenziellen Sicherheitsbedrohungen geschützt sein.

Stand: 06/2021

Foto: 1. FSV Mainz 05 e.V.

Mit der NAC-Lösung von macmon secure ist ein Überblick über alle Endgeräte im Netzwerk gesichert.

Hybride Kommunikations-Infrastruktur – hohe Anforderungen an die IT-Sicherheit

Neben den Kommunikationsanforderungen der Fans ist die IT-Abteilung des 1. FSV Mainz 05 e.V. mit einer Vielzahl von Themen beschäftigt. So stellt auch die Bürokommunikation der **1.095 Mitarbeiter**, darunter **460 Office-Nutzer**, höchste Herausforderungen an eine reibungslose und vor ungewollten Zugriffen geschützte IT. Zu den internen Nutzern, die sowohl stationär als auch mobil arbeiten, kommen nochmals regelmäßig rund 700 externe Nutzer der Kommunikationssysteme hinzu, die beispielsweise einen Netzwerkzugang für die Wartung der **210 Kassensysteme** benötigen. Die Administration von Gastzugängen muss sowohl einfach als auch sicher sein. Und nicht zuletzt besteht die gewachsene IT-Infrastruktur alleine aus **155 Netzwerkswitches, 380 Access Points und 7.500 Netzwerk-Ports** verschiedener Hersteller. Diese speziellen Anforderungen, insbesondere an die Netzwerksicherheit, veranlassten Karsten Lippert, Leiter ICT & Digitalisierung des Clubs, sich mit der Auswahl einer Lösung für Netzwerkzugangskontrolle, auch im Hinblick auf die Anforderungen der DSGVO, zu befassen.

Externe Nutzer	Angestellte	Provider	Sicherungssysteme
700	1095	3	3

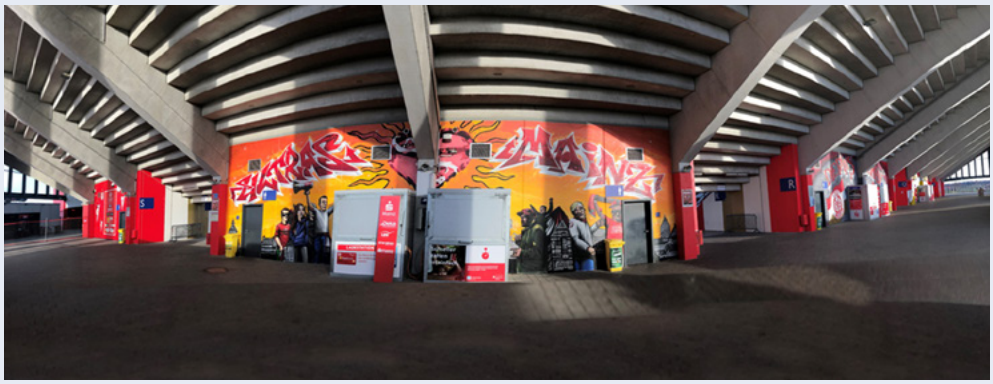

Foto: 1. FSV Mainz 05 e.V.

Genau wie bei der Netzwerkzugangskontrolle passiert auch in der MEWA ARENA vieles hinter den Kulissen.

Schnelle Übersicht, niedrige Komplexität und hohe Effizienz

„Vor Projektbeginn hatte ich die Befürchtung, dass durch die Einführung einer Netzwerksicherheitslösung unter Umständen vermehrt Störungen am Spieltag auftreten könnten. Auch schien mir eine möglicherweise lange Einführungsdauer kontraproduktiv, denn durch die vielen Anforderungen, beispielsweise im Hinblick auf Datenschutzthemen, ist unsere IT-Abteilung mehr als ausgelastet". In Zusammenarbeit mit einem lokalen IT-Systemhaus konnten die Experten der macmon secure GmbH die anfänglichen Befürchtungen schnell ausräumen. Das Projekt startete mit einer ausführlichen Risikoanalyse. In dieser Phase stellte sich unter anderem heraus, dass die Verbindung zwischen Switches und Access Points der kritischste abzusichernde Zugangspunkt in das Netzwerk ist, da auf den Anschlüssen der Access Points nahezu alle im Netz verwendeten VLANs anliegen und diese an „ungesicherten" Orten (zum Beispiel Außenwände, Laternenmasten, etc.) angebracht sind, so dass eine Demontage nicht ausgeschlossen werden kann. Exakt die Netzwerkgerät-zu-Netzwerkgerätverbindung kann jedoch durch klassisches 802.1x nicht abgedeckt werden und alternative Methoden wie macsec-Verschlüsselung

Foto: 1. FSV Mainz 05 e.V.

Während eines Fußballspiels können 65.000 Endgeräte im Einsatz sein – vom Smartphone über Rechner bis hin zu den elektronischen Kassen.

IT-KNOW-HOW | NAC-Expertenwissen

Access Points werden von **macmon NAC** anhand der MAC-Adresse und dem Fingerprint erkannt. Konforme Access Points kommunizieren über die tagged VLANs am Switch Port in ihre Netze. **macmon NAC** registriert innerhalb von einer Sekunde, wenn ein Access Point abgezogen wurde, der Port wird sofort heruntergefahren. Wird ein Access Point an einen neuen Port angeschlossen, setzt **macmon NAC** die tagged VLANs, damit die Service Set Identifier in die jeweiligen Netze kommunizieren können. Wenn der Access Point abgezogen wird, entfernt **macmon NAC** alle tagged VLANs, die zuvor für die WLAN-Kommunikation am Port gesetzt waren und schließt damit den tagged Zugang zu jeglichen Netzen am Port.

weiterführende Infos in unserem **Knowledgebase-Artikel** im **macmon Service Portal** **https://portal.macmon.eu**

werden von den meisten Edge-Switches und APs nicht unterstützt. Diese Herausforderung löste macmon NAC mit der SNMP-NAC-Funktionalität mit entsprechenden Event-Überwachungen und insgesamt nur drei Regeln. Zum einen werden am Spieltag zwei isolierte Netze für die Gast-Mannschaft und die Heim-Mannschaft in vorgegebenen Bereichen aktiv geschaltet. Zum anderen werden Access Point Ports gesondert behandelt, solange diese mit der Infrastruktur verbunden sind.

Zügige Implementierung und sofortige Übersicht im Netzwerk

„Wir erleben in der Praxis immer wieder, dass potenzielle Kunden sich aufgrund negativer Erfahrungen Sorgen bezüglich des Implementierungsaufwandes machen. Unsere NAC-Lösung ist jedoch einfach in der Implementierung und erzielt schnell einen Überblick über alle im Netzwerk befindlichen Endgeräte. Diese Visualisierung ist schon einmal ein schneller Gewinn. Die Nutzung der Lösung ist für einen IT-Administrator fast schon intuitiv und bietet vielfältige Mehrwerte." so Christian Bücker, Geschäftsführer der macmon secure GmbH. Ein wesentlicher Aspekt, der Betriebskosten senkt, ist der Wegfall der bisher manuellen, zeitaufwendigen Konfiguration von Netzwerkanschlüssen zu den verschiedenen Anlässen im Stadion. Zu den rund 20 Spielen pro Saison kommen auch circa 200 externe Veranstaltungen. Durch die Automatisierung der Konfigurationen wurde die Anzahl der Helpdesk Tickets minimiert und die ursprünglichen Netzwerkmanagementlösungen der Hardwarehersteller abgeschafft. Dabei nutzt der 1. FSV Mainz 05 e.V. drei Mechanismen für die Authentifizierung: SNMP-NAC basiert, mac-basiert über RADIUS und 802.1X. Abhängig vom Port und dem verwendeten Endgerät, wird der richtige Mechanismus angewandt. Dieser Prozess ist jedoch auf der macmon-GUI in einem Menü zusammengefasst und vereinfacht, so dass der Administrator lediglich die richtigen VLANs eintragen muss. macmon NAC regelt den Rest im Hintergrund, somit benötigt man keine protokollabhängigen Einstellungen.

Datenstandorte	logische Netze (VLANs)	Netzwerkswitches	Access Points
4	87	155	380

macmon NAC arbeitet mit allen marktüblichen Switches

Aufgrund des Einsatzes von macmon NAC mussten keine bestehenden Switch-Hersteller aussortiert und die bestehende Switch-Infrastruktur konnte nahtlos genutzt werden, eine Umstellung war nicht notwendig. Folgende verwaltete Systeme setzt der 1. FSV Mainz 05 e.V. ein, welche auch gegenüber

Schauen Sie sich die Use-Cases im gemeinsam durchgeführten Webinar **„Sicher durch die Saison mit macmon NAC“** an:
https://youtu.be/OcRy15KeHfQ

macmon NAC als Netzwerkgerät agieren: Aruba/HPE ehemalig Procurve Switches, Commscope/Ruckus Access Points (z.T. Hospitality- Ausführung mit LAN-Ports) und Microsens Microswitches (für den Kabelkanal). Darüber hinaus nutzen die Mainzer nicht-verwaltete PD-Switches von Netgear sowie Kabeltrommel-Switches von Pandacom, welche aus macmon-Sicht als Endgerät agieren.

Heterogene Netzwerke an verschiedenen Standorten – kein Problem. Seit der Einführung hat sich macmon NAC als zuverlässiger Helfer im Alltag und insbesondere am Spieltag bewährt. Für die Nutzung von macmon NAC braucht man zudem nicht zwangsläufig eine Appliance an jedem der drei Standorte. Die Außenstandorte können auch vom Hauptstandort bedient werden. Wichtig ist bei der Projektierung immer die Frage: Welche Sicherheit/welche Hochverfügbarkeit braucht man, wenn die Verbindung zum Außenstandort wegfällt und wie kritisch ist das Szenario in diesem Fall? Wenn am Außenstandort keine RADIUS-basierten Authentifizierungen gemacht werden, wäre ein Ausfall der Anbindung dorthin je nach Einsatzszenario möglicherweise vertretbar. Wenn ein Unternehmen aber auch dort die RADIUS-basierte Authentifizierung nutzen möchte, ist eine Appliance am Außenstandort sinnvoll. Im Fall des 1. FSV Mainz 05 e.V. sind die drei Standorte in Mainz mittels eines kanten- und knotendisjunkten Dark-fiber-Rings verbunden, so dass die redundanten macmon-Knoten in dem zentralen Rechenzentrum ausreichend sind.

Zentrale Herausforderungen während der Inbetriebnahme:

Geräte, welche von sich aus keinerlei Datenpakete an das Netzwerk senden, wodurch keine Authentifizierung stattfindet.

Drei sichere Tore für macmon:

1. **ÜBERSICHT** Mit macmon NAC gewann die IT-Abteilung des 1. FSV Mainz 05 e.V. innerhalb weniger Stunden bereits einen Überblick über das gesamte Netzwerk.
2. **KOMFORT** Das automatische und dynamische Regelwerk verringerte den Arbeitsaufwand für den IT-Administrator.
3. **SICHERHEIT** Unbekannte Geräte und Anomalien werden sofort erkannt und umgehend vom Spielfeld „isoliert“.

Beispiel: **Eintrittskartendrucker und EC-Terminals**
Lösung: **Umstellung der Geräte** von fester IP-Konfiguration auf DHCP, Konfiguration von „Nachhause“-Telefonie (Regelupdates) zur Aufrechterhaltung des Authentifizierungs-Timers sowie Einführung von mac-pinning.

Korrekte Zuordnung der Geräte, welche sowohl LAN- als auch WLAN-Schnittstellen haben.

Beispiel: **Notebooks**
Lösung: **Änderung der VLAN-Architektur** von der bisherigen Anbindungsartzuweisung (VLAN1=LAN, VLAN2=WLAN) zu Nutzergruppenzuweisung (VLAN11=Verwaltung, VLAN12=Lizenzspieler, ...)
Absicherung der Access-Point-Anbindung und gleichzeitige Gewährleistung der Hospitality-Funktionen (mit bis zu vier downlink-ports pro Access Point).
Lösung: **Definition der Access Points als Endgerät** und gleichzeitig als Netzwerkgerät.

Stand: 06/2021

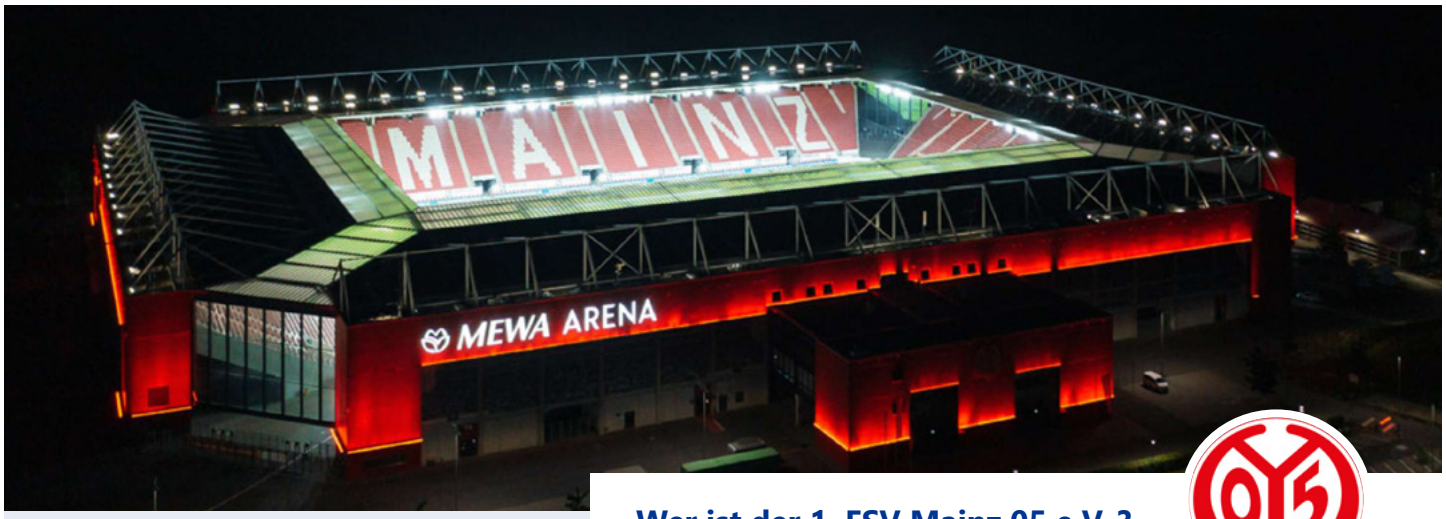

Foto: 1. FSV Mainz 05 e.V.

IT-Sicherheit hat auch im Fußballstadion des 1. FSV Mainz 05 e.V. höchste Priorität.

In einem zweiten Projektschritt stehen bei dem 1. FSV Mainz 05 e.V. Themen wie umfassendes Reporting der im Netzwerk ermittelten Messdaten und die Darstellung der Ereignisse im Netzwerk auf der Agenda. Dazu gehören beispielsweise Sicherheitsaspekte wie das Auftauchen bekannter Geräte zu ungewöhnlichen Zeiten oder das Aufzeigen von Angriffen wie ARP-Spoofing oder MAC-Spoofing. Dazu Karsten Lippert: „Neben den klassischen Vorteilen einer soliden und flexiblen Lösung für Netzwerkzugangskontrolle bieten sich hochflexible Anbindungsmöglichkeiten von Drittanbietern über die offene Schnittstelle REST-API für diverse Lösungen unserer Digitalisierungsprojekte. macmon secure arbeitet auch bereits an erweiterten Nutzungsmöglichkeiten um macmon NAC noch effektiver in der AWS-Cloud sowie in der Azure-Cloud zu betreiben. Somit wird unser Projekt sicher eine Referenzlösung für weitere Fußballvereine werden.

Wer ist der 1. FSV Mainz 05 e.V. ?

Der **1. FSV Mainz 05 e.V.** ist seit **1905** der Fußballverein in der **Landeshauptstadt von Rheinland-Pfalz** und meisterte Höhen und Tiefen. **Seit 1990** ist der Verein im Profifußball der **Bundesliga** präsent. Immer konnte sich der Verein auf den Rückhalt der Menschen und Institutionen der Stadt verlassen.
Der **besondere Geist** des Vereins entsteht durch bedingungslose und lautstarke Unterstützung im Stadion gegenüber dem eigenen Team, gepaart mit Toleranz, Respekt und Fairplay gegenüber den Gästen. Für den Verein ist es wichtig, diesen besonderen Geist trotz der zwangsläufigen Professionalisierung und Kommerzialisierung zu erhalten und in **das neue Stadion, die MEWA ARENA**, zu transportieren. Zu diesem professionellen Ansatz gehört ein **IT-Netzwerk der ersten Liga**.

FAZIT von Karsten Lippert:

Die Einführung von macmon bei uns im Verein war getrieben von der Steigerung der Netzwerkzugangskontrolle.

Erhalten haben wir darüberhinaus eine Lösung, welche aufgrund ihres hohen Automatisierungsgrads es uns erlaubt neue Services für Fans, Kunden und Partner anzubieten, ohne zusätzlich Personal bereitstellen zu müssen.

Kontakt macmon secure GmbH | Alte Jakobstraße 79-80 | 10179 Berlin | Tel.: +49 30 2325777-0 | nac@macmon.eu | www.macmon.eu

Stand: 06/2021