CASE STUDY

Memmingen Relies on Security for its Town Administration

State-of-the-art technologies for the citizens of a town steeped in tradition

Memmingen is an independent town in the Bavarian administrative region of Swabia. The former imperial town is the regional center as well as the school, administrative and commercial center in the Donau-Iller region.

With **43,837 inhabitants,** the **town in Upper Swabia is the fifth-largest town in the administrative region of Swabia.** The origins of Memmingen date back to Roman times. With its many squares, town houses and patrician houses, palaces and city fortifications, the old town is one of the best-preserved cities in southern Germany. Thanks to good transport connections by road, rail and air, it is also the transport hub of Upper Swabia, the Allgäu and Central Swabia.

207–day catastrophic event

The first digital disaster in Germany occurred in July 2021 in Saxony-Anhalt

Following a **ransomware attack**, parental benefits, unemployment and social benefits, registration of vehicles and other community-related services could not be provided in a district with 157,000 inhabitants for more than half a year.

The threat level in public administration is intensifying

The serious attack on a district administration in Saxony-Anhalt clearly shows that it's not just companies that are the target of ransomware attacks. For the first time, a cyber attack caused a **state of emergency** to be declared. Community-related services were unavailable or only partially available **for more than 207 days**.

The figures published in the **BSI status report** (Federal Office for Information Security) give a good insight into the risk situation at federal level. For example, around **44,000 e-mails containing malicious programs** were intercepted every month in the government networks by automated antivirus protection measures during the reporting period.

Comprehensive security concept to protect the citizens of Memmingen

Stefan Schönhals, Head of the Office for Information and Communication Technology of the town of Memmingen and Information Security Officer is only too aware of the threat situation: “The town administration of Memmingen employs around 750 people, working with sensitive and personal data. Our area of responsibility includes securing administrative processes for everywhere from old people’s homes to municipal utilities and municipal sewage treatment plants. Our extensive population data and critical infrastructure facilities are an enticing target for cybercriminals. Cyber attacks on municipalities are particularly effective in terms of publicity, directly affect the citizens, cause commotion and disrupt public services.”

The urgent need for comprehensive IT security in public administration has also been recognized at state and federal level: The creation of an information network for public administration—known as **IVÖV** for short—is the aim of the **Network Strategy 2030**. It was formulated at federal level as part of a conference of IT representatives with the aim of long-term further development of IT network infrastructures in public administration. It takes account of the increased demands in the area of communication capability for the entire public administration in Germany, new technical developments and the increased security requirements, including those caused by events such as the Ukraine war.

Key benefits of macmon NAC for the town administration of Memmingen:

- ✓ **Maximum security through** granular access control and precise network segmentation
- ✓ **Monitoring and control** of all devices in the network (live inventory management)
- ✓ **Ensuring the integrity of the network** by only granting network access to defined (owned and approved) devices
- ✓ **Protection of administrative IT** against attacks on sensitive, personal data
- ✓ **Support for the implementation of the German Data Protection Act (BDSG) and the State Data Protection Act (LDSG)** and the fulfillment of the requirements of the Basel Agreement Basel II/III

> *“Now we are informed when and where an unknown device is plugged in, and only devices approved by the IT department will be accepted.”*
>
> **Stefan Schönhals** | Information Security Officer, Memmingen

Elimination of potential dangers from unknown end devices in the network

The coronavirus pandemic has also led to accelerated digitalization in public administration in recent years. Not all administrative procedures can be digitally managed, however. Therefore, the movement of people in city administration is still an issue. Schönhals identified, for example, **open network ports as possible gateways** for connecting the administration network to infected unknown devices — not only through visitors to the municipal facilities, but also through employees. The IT team did not have an overview of the end devices in the network, such as private laptops. In addition, there was **no overview and control over third-party devices** added to the network by external service providers carrying out maintenance on city facilities. “Now we are informed when and where an unknown device is plugged in, and only devices approved by the IT department will be accepted.”

Comprehensive network protection provides a central line of defense

The topic of network security was discussed with the IT security consultant of **CyProtect AG**. The manufacturer-independent cybersecurity service provider has maintained a long-term partnership with **macmon secure GmbH**, which specializes in network security. When deciding in favor of macmon NAC, after a public tender, the good price-performance ratio of the Berlin-based macmon secure was also an important factor for Schönhals. “Now, the employees in the IT department couldn’t imagine life without macmon.” The macmon Network Bundle, an efficient tool for network protection, is being used to provide a comprehensive overview of all devices in the network, live inventory management, immediate alerts when unknown devices are connected and the initiation of automatic countermeasures.“ This not only increases security, but also reduces our administration work,” comments Schönhals. In addition to the use of software solutions, Memmingen is also focusing on prevention: “In order to improve our IT security, we implemented internal e-learning training courses, as many employees were not even aware of possible gateways for malware.”

“In order to improve our IT security, we implemented internal e-learning training courses, as many employees were not even aware of possible gateways for malware.”

Stefan Schönhals | Information Security Officer, Memmingen

As well as providing standard network access control, the IT expert believes one of the biggest advantages is the tool’s ability to automatically assign VLANs using group assignment. The VLAN Manager is an effective and time-saving management component for the simple introduction and automated operation of static and dynamic VLAN concepts. “The time saved by the automatic VLAN assignment when setting up and moving end devices is a major advantage. Previously, the VLANs had to be configured manually on the switch.”

“The time saved by the automatic VLAN assignment when setting up and moving end devices is a major advantage. Previously, the VLANs had to be configured manually on the switch.”

Stefan Schönhals | Information Security Officer, Memmingen

VLAN MANAGER

The **VLAN Manager** is included in the **Network Bundle** of **macmon NAC**.

The town hall of Memmingen

Date: 04/2023

The recent high-profile cyber attacks on administrations have shown just how important it is to protect the IT infrastructure of a municipality, and have led to a rethink among local politicians.

The increasing complexity of IT due to digitalization, the transfer of business processes to the Internet and new technologies create new vulnerabilities to cyber attacks. It is important to deal with these vulnerable areas quickly and comprehensively.
A digital administration needs not only a modern, but also a secure infrastructure.

SUMMARY Stefan Schönhals | Information Security Officer for the town of Memmingen

The macmon Network Bundle can be used as a central security solution to provide a quick and thorough overview of all end devices in the network. Unknown end devices are therefore a thing of the past and are no longer allowing malware to infiltrate the network. In addition to fulfilling numerous IT security targets, the solution also reduced the administrative effort — a welcome advantage given the ever increasing workload of Memmingen's IT team.

The handling and operation of the solution were also praised. macmon secure's in-house IT support team were on hand to answer all technical questions and met any requests promptly and professionally.

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