Reference Story: City of Baden-Baden

The City of Baden-Baden now enjoys comprehensive endpoint security by EgoSecure

"Baden-Baden – more pleasure and joy in life" – that's the motto of the famous spa town at the foot of the Black Forest. However, trying to implement an endpoint security solution was no pleasure and joy at all for the staff of the municipal information and communications department (IuK, "Informations- und Kommunikationstechnik"). After several attempts had failed, they have finally found a solution that provides all-round protection of the whole system landscape, is easy to administrate and to use – EgoSecure Data Protection.

A municipality with a wide range of responsibilities

In the IuK department in the town hall of Baden-Baden there is much activity going on – suggesting that a lot is managed and achieved in these rooms. The system plans on the computer screen or on print-outs on the walls show only parts of the complex IT landscape. As opposed to many "normal" municipalities, the City of Baden-Baden faces a larger scope of responsibilities: With 54,000 residents, Baden-Baden is the smallest independent town or urban municipality in the federal state of Baden-Württemberg, and this means that it also has to deal with tasks that are normally handled by the county administration office, which also comprises the road traffic authorities or the social welfare office. Also, Baden-Baden's cultural program is quite special, including the philharmonic orchestra or the theatre with its own tailor's workshop. "All these institutions and the 20 schools, plus many mobile devices such as those used by the public order authority or the forestry office, are part of our system landscape. Altogether, nearly 800 stationary and 110 mobile workplaces are exposed to attacks", explains Matthias Götz of the municipal IuK department.

Endpoint Security – a must for any district or municipal administration

In many organizations, including most district or municipal administrations, network security is limited to protecting networks against attacks from the Internet – with the help of widely-used solutions such as firewalls and antivirus software. Such measures are, however, by no means sufficient, since it is easy to steal data or infect the network via any kind of device, for instance simple devices such as USB sticks. Implementing an endpoint security solution is also an essential prerequisite for processing and administrating the residents' personal data. And so, the municipality of Baden-Baden made a strategic decision to implement such solution. "As we had anticipated when we tried to set up a short-list of products, the highly complex system landscape was a challenge for vendors with respective solutions" remembers Matthias Götz' colleague Stefan Hanmann. "There were great difficulties due to the large number of different applications. For instance, the land surveying office has a very effective solution, which is, however, quite old and therefore lacks compatibility. The inventory solution and the mobile handsets of the parks department and the municipal law enforcement office also presented major challenges."

Various solutions were examined and put to a first short test, but many tasks could not be mapped sufficiently with these products. "We decided to implement the solution which seemed to be best suited to address our requirements and conducted comprehensive tests in productive operations" reports Klaus Thomas, also a member of the IuK department. "However, as we found out, there were problems which not even the vendor's consultants were able to solve. At some point, we got stuck with this vendor." Hence, the City of Baden-Baden was forced to review the results of the first test

phase and to find another product. Finally, a new software was selected as the new favourite, based on the insights gained from the productive usage of the previous product. But again, this solution failed to address the requirements of the highly complex system landscape. "For weeks, we were busy with solving the problems of our users who complained about non-working applications and devices" remembers Matthias Götz. "The situation was unbearable; after all, the nine members of our team have to handle a multitude of other tasks. And we had certainly not planned to invest so much effort into endpoint security management."

The vendor's support team needed too much time for individual problems before a solution was provided – if such solution was found at all. Finally, the whole project was cancelled again. Was this the end of endpoint security for the City of Baden-Baden?

A solution was found in cooperation with TAP Desktop Solutions

The endpoint security issue came up during discussions with TAP Desktop Solutions. Surprisingly, TAP suggested a solution that had not been tested yet – EgoSecure Data Protection. This solution had not been included in the selection process, due to the vendor's low degree of market visibility in the past. But the basic product, which was launched in 2006, is leading-edge technology, a claim that is confirmed by EgoSecure's 1,100 satisfied customers. The company's name was changed into EgoSecure; the vendor developed a new marketing and sales strategy and also established the partnership with TAP Desktop Solutions. The previous failures with endpoint security implementation had put a strain on the IuK staff. No wonder that is was not easy to persuade the team to start yet another attempt. "During our discussions we realized that it would be very difficult to build understanding and trust among the responsible executives to gain their support for this new project; a creative solution was required, especially to address the commercial aspects", explains Michael Krause, Managing Director of TAP Desktop Solutions. "And we found such solution, in cooperation with EgoSecure." "We were very happy to have found an approach whose initial focus was on the successful implementation of the solution, with financial aspects playing a secondary role during this first phase of the project; this reduced our risks significantly, and we could present tangible results before we had to speak about internal budgets", says Matthias Götz about TAP 's commercial creativity. Soon, a decision was made: in favour of another jump into the "cold water".

Endpoint security is no magic and can be quite simple

The water was not that cold after all. Daniel Döring, head of EgoSecure's Professional Services department, performed the basic installation. The EgoSecure endpoint solution collected all required network information from Active Directory. The client component was rolled out with a software distribution solution – in this case, Empirum. 70% of clients run on Windows XP, 30% on Windows 7. EgoSecure Data Protection was already Windows-8-enabled. Basic protection was ensured directly after the basic installation. "We were very surprised about how fast Mr. Döring completed the basic installation – that was very different from what we had experienced with the other vendors" remembers Stefan Hanmann. "After the installation we just had to make some minor adjustments, a very easy task with the intuitive, centralized management console. Another great feature is the automatic update of clients." And Klaus Thomas adds: "Very soon it was obvious that many things really worked right from the start." EgoSecure Data Protection with its well-designed software architecture is highly compatible with other applications to provide real all-round protection. Competitive products often exclude some applications due to their lack of compatibility – this is by no means a comprehensive protection approach. The same is true for low acceptance rates among

users: If a security solution interrupts users' workflows, they will try to circumvent the solution, which again prevents comprehensive protection. And the criteria for assessing the degree of user acceptance? "Well", says Klaus Thomas, "I'd say, a new solution enjoys a high degree of acceptance when there are hardly any user reactions after the solution has been implemented – and that's how it was with EgoSecure Data Protection. While the solution works transparently and the users know what is going on, it does not interrupt their workflows." Stefan Hanmann is full of praise when he talks about the cooperation with the EgoSecure support team: "Of course we don't say that everything worked 100% perfect after the installation and configuration. With such a highly complex system landscape, such expectations would have been completely unrealistic. For instance, we had problems to scan the volume ID, but this is more a Microsoft issue. But as opposed to our previous attempts with other vendors, this and other minor problems were identified and solved within hours." And Matthias Götz adds: "That's how it should be, for endpoint security simply has to work, instead of consuming valuable IT resources." Future plans of the City of Baden-Baden envisage improved media encryption – good to know that EgoSecure also provides a solution for this issue.

About EgoSecure

With EgoSecure Data Protection, the German security specialist EgoSecure from Ettlingen has been the innovation leader in the field of comprehensive data protection solutions for more than 10 years. The innovation in the current product version is the further development of the "Insight" module. Insight provides an overview of the overall situation of data security in the network. Based on these facts, the protection requirements are determined individually for each company. EgoSecure is the first manufacturer in the world to combine analysis and protection modules in one solution. Both are closely linked in one solution through one management console, one database, one installation and administration concept. This guarantees a quick installation and easy administration. User training is usually not necessary, as most of the protection functions take place in the background. All true to the motto "we make the complicated things easy".