CASE STUDY LOCAL GOVERNMENT

Sylt Takes on Cybersecurity

INDUSTRY

Local governemnt

ENVIRONMENT

- 175 clients, 110 of which are virtual, 30 virtual servers on six physical servers, three of which are for the VMWare View environment

CHALLENGES

- Replace an existing antivirus system that was markedly tiresome to administer and constrained productivity during special administrative processes
- Find a solution that consumed fewer system resources
- Replace a traditional approach that did not meet current requirements in defending against threats

SOLUTION

- Implement CylancePROTECT® to defend against both known and unknown threats while reducing the impact on system resources

The Organization

Sylt is much more than just a vacation paradise, as you can read on the homepage of the municipality. Sylt is a lively place to live and enjoy with an outstanding infrastructure and a modern, service-oriented administration. The municipality of Sylt, with a full-time administration, runs the business of the collective municipality (Amt Landschaft) of Sylt with the municipalities of Hörnum (Sylt), Kampen (Sylt), List auf Sylt and Wenningstedt-Braderup (Sylt). The community administration follows a modern service-provider approach in every respect. It uses its Internet pages and the short message service Twitter to provide information in almost real time about important issues. The goal is to respond to questions about proposals, services and dealing with government authorities around-the-clock.

The Situation

The municipality of Sylt relies on electronically assisted administration and communication with its citizens for many issues. In government agencies, authorities, and the administration in general, there are a number of processes that differ from those used in the unregulated business world. This has an effect on both the methods and technologies used for IT security. One example was the existing antivirus solution used by the community of Sylt. Administration took a lot of time and effort, and the employees complained that the type and scope of the scans performed had a negative impact on their productivity.

Thomas Ranke, Central Services IT Administrator for the collective municipalities of Sylt's Office of Internal Affairs and Education, says, "Using the admin systems of our existing solution on a day-to-day basis was just torture. To express this a bit more tactfully, there was an urgent need for change in this area. Essentially, our list of requirements was not very complicated. We looked for reliable endpoint protection for our clients and servers that was simple to administer and came equipped with a toolbox containing the necessary tools that were quick to find when needed."

To secure their endpoints, Thomas's team relied on a traditional, signature-based, AV solution. Administration of the solution turned out to be decidedly complicated and to keep the solution up to date at all times required considerable personnel resources.

The current solution put a large load on CPUs. The traditional signature-based solution had a substantial negative impact on system performance. As a result, the end-user experience was negatively impacted and operations were slowed down.

Thomas says, "One example is the community budgeting, treasury, and accounting division, a centerpiece of public administration. Here, one user may have up to 300 files open at one time. These files are opened and closed again and again in quick succession corresponding to the tempo of the postings. Some of the scans necessary for the original antivirus solution had a tremendous effect on the processing speed. For this reason, we were compelled to exclude more than 10% of these files from the regular scans. This increased our attack surface considerably. Added to this, there was the time-consuming importing of the signature updates that was necessary on a constant basis."

"We use a total of 175 clients including 110 virtual ones and 30 virtual servers. Systems holding available data of the highest protection level. These data include resident registration data, personal data with some being marked with a ban on disclosure, real estate data, and much more. You can easily imagine what it would mean if these data were disclosed during a data privacy incident."

Official administration processes are being digitalized to an ever greater degree. Sylt's public administration team is facing a challenge that is not to be underestimated. It stems from the increasing number of data protection violations and cyberattacks. For the public administration to still be able to rely on appropriately stable and secure administration processes, they must integrate data privacy into a comprehensive IT security concept and must examine existing methods and technologies to that end. In addition, IT infrastructure is becoming more and more complex. Often, there is a local IT department, IT in the immediate governmental environment, central IT in the computer center, and perhaps external third parties as IT service providers. In these cases, besides a variety of directives that already apply, the EU basic data privacy regulation further increases the pressure. This affects the concrete requirements for protecting personally identifiable information and the overall handling of data and information within a government department.

The Process

"We were anything but happy with the existing situation. And, as chance dictates, we were contacted at precisely this time by Communication Systems GmbH, a system vendor partner. I must admit that, as a person interested in mathematics, I was impressed by the approach presented."

"However, we were skeptical at first because the terms of artificial intelligence, which has no standard definition, and machine learning were two buzzwords being tossed about with equal self-confidence. Then, it is rarely explained just how a product operates, which models of machine learning are used as a basis, how code analysis is performed, and so on. Fortunately, a customer provided as a reference by the company was able to completely disarm our concerns. We were appropriately impressed during the actual test by the quick implementation and the system performance. CylancePROTECT as an endpoint security solution is very compelling in its use of mathematical basics. The result of our tests: It works."

The Results

Thomas says, "We are using CylancePROTECT on a total of 175 clients, including 110 virtual ones, and 30 virtual servers. Of course, the solution complained about a few files during the initial phase. This was to be expected with 50 different technical procedures from the special segment of public administration. In the first days, I kept the portal open permanently to decide whether the files affected should be released or blocked or whether they should be put in quarantine. I only had to do this one time and it was handled quickly and simply. A file, once released, remains released unless it behaves differently than usual. Regarding the budgeting, treasury, and accounting division we already mentioned, the users no longer even notice that a top-shelf security solution is working without interruption in the background. Code analysis delivers a lot of benefits to the administration. Bandwidths today are no longer a hot topic, but still, you can save resources here. We have even reduced the amount of data traffic because we no longer have to import updates as regularly as before."

Conclusion

"I go home now much calmer when I think about protecting our clients," Thomas says. "The new solution consumes considerably less computing time and this, in turn, has a positive effect on the reaction times. It is easier to administer and runs in the background virtually without making a peep. CylancePROTECT is my first choice even when I think about administration in larger organizations."

+1-844-CYLANCE
sales@cylance.com
www.cylance.com
400 Spectrum Center Drive, Irvine, CA 92618

CYLANCE