CIO of Prinzhorn, Manfred Ofner.

“Growth is essential”

Manfred Ofner, CIO of packaging specialist Prinzhorn, talks to T-Systems Account Ececutive Christian Litschauer about the care of a security operations center, the ideal product life cycle as a perpetuum mobile and grab bags as a companion for strategic growth.

COPY —— Thomas van Zütphen

Mr. Ofner, Cloud solutions, SD-WAN and Cyber Security Services – why have you outsourced almost your entire ICT operations? And why T-Systems?

Because we are paving the way for the company’s further growth. That’s why management and shareholders decided six years ago to harmonize our IT landscape in all our locations. In our case, we’re talking about 15 countries, so it makes sense to look for a service provider that can deliver in all these countries.

With the growth that you mentioned, Prinzhorn is pursuing the strategic goal of achieving 100 percent growth by 2030. What does this mean for your IT?

In our European competitive situation, growth is essential. The doubling in the sense of 100 percent refers to sales by 2030, i.e. between five and ten points plus per year. This is clearly above average and underscores our market presence. The challenge for IT, in addition to the keyword ‘harmonization’ I just mentioned, is to integrate almost permanently new companies that are to be built or purchased by 2030. So we have a Green Field project every one or two years and at the same time we buy from the market if possible. This growth on two levels practically leads to a constant integration challenge for our IT.

Because at Brown Field you sometimes open a grab bag.

Exactly. Never before have we acquired a complete IT landscape that could have been seamlessly integrated into our infrastructure. This required a dedicated transition every time.

Governance has a key function for Prinzhorn, not least in such transitions. Why?

As we are internationally active in 14 languages, the introduction of IT systems and the harmonized IT infrastructure and subsequent support is a major challenge. Synergies from identical landscapes can only help. However, this requires a correspondingly high level of process governance in order to be able to ensure that, on the one hand, we are quick during implementation and, on the other hand, can actually provide good support. This is a task that logically encounters not only linguistic but also cultural challenges. In the background, it is also about transparency for us in our Group IT. That is why governance is a major issue for us, and one that we pay great attention to.

Photo: Oliver Krato

Who or what specifically provides you with this transparency?

At this point we are still in development and far from finished. Together with T-Systems, we have introduced the first tools with access to the central control and monitoring tools. This is transparency that we also pass on to the plants. This means that questions such as "What's currently going on in my network? – What is currently troublesome or not running as well" can be answered quickly. This is the only way you can coordinate and initiate countermeasures if necessary. In essence, it's always about optimization possibilities and – not to forget – the topic of security. Here, too, we have taken measures in order to be able to offer a better degree of security.

What does that mean in concrete terms? With which solutions do you try to achieve this higher level?

For example, by bringing T-Systems' Security Operations Center (SOC) on board. This is a step that we expect to bring more transparency back. For example, when it comes to possible viruses, malware, spam mails and the like. We actually experience such events on a daily basis and must then be able to get rid of them as quickly as possible. In this respect, the operational SOC we have been using since the fall of last year is a weapon we want to use to become more resistant to attacks throughout the Group. So today we see relatively quickly if there is a security threat. At the same time, we are constantly working with T-Systems on new use cases, which we process and refine in order to be able to cover new threat scenarios.

"The operational SOC is a weapon we want to use to become more resistant to attacks throughout the Group."

MANFRED OFNER,
CIO, Prinzhorn

What does 'quickly' mean?

It is fast if, for example, the monitoring systems report a virus attack to the SOC and automatically generate information for our security units from there. We are talking about minutes. The employees analyze the events and can react promptly. In the end, of course, it is always a person who has to take an action or measure. But according to our previous experience, both the recognition and the initiation of a measure takes place promptly.

Should the system not be able to automatically initiate necessary processes in order to keep damage as low as possible, or to ward off attacks before they cause any damage at all?

We don't have that level yet. But I have to say: We don't want that yet. I first need confidence in the software and the control options. That still has to grow before a system comes up with the idea, "I take a plant with a paper machine offline because a virus attack is reported there," and then the whole thing turns out to be a false alarm. It's okay in the first step for the system to point out and actively alert you: 'We have a problem here' and then take action. So it's up to us to react quickly. However, I expect this process to be automated in the long term with countermeasures that always run the same way.

At the moment you are in the phase of confidence-building measures.

Exactly. It has to run reliably. This is an evolutionary, step-by-step process, which we will of course refine further. It is the case that new insights emerge with monitoring. Unfortunately, security threats are very creative and of increasing diversity. Everyone must continue to grow and learn together: the system, the service, us as the customer and T-Systems as our partner.

Know-how is a good keyword and leads us to a completely different topic: What are the advantages of reorganizing your group-wide WAN landscape?

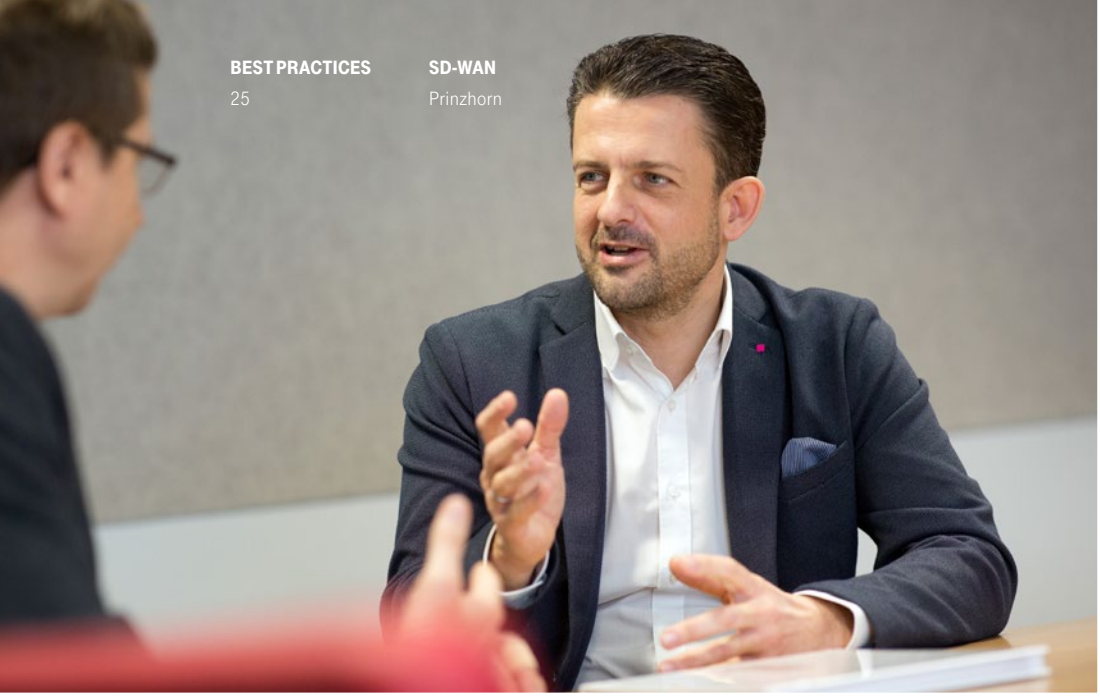
There are actually two reasons why we went in the direction of an intelligent SD-WAN. On the one hand, it is a fact that data traffic on our WAN lines has increased linearly. In this respect, it is in line with the usual trend of digitization to require more and more bandwidth. Because we used to have a very centrally built network and the locations had no Internet access of their own, but had to go centrally via the IT center, even the normal Internet load logically leads to a corresponding increase in bandwidth requirements. At the end of the day, the demand for throughput and speed is constantly increasing, the IT systems tend to be too slow, no matter how fast the bandwidth is expanded.

SD-WAN technology gives us the opportunity to combine two things. On the one hand, to enable local Internet breakout and still remain on the safe side in terms of security. And, of course, using Internet access instead of MPLS access for bandwidth expansion at the same time leads directly to savings. Our calculation is quite simply as follows: Cost reduction plus faster response time equals win-win. The first attempts – the transition is still ongoing – already seem to confirm this. The proof-of-concept will follow as soon as we have converted all outstations and plants to SD-WAN technology.

Cloud computing is another classic pillar of digitization. What is Prinzhorn's strategy?

For us, the private cloud is a familiar environment in which we can travel safely and on which we will continue to build in the near future. I don't see any need to deviate radically from this at the moment. The fact is, however, that there are more and more occasions or needs but also opportunities to use non-private cloud solutions. If these seem safe to us, we use them, have some solutions already in the implementation phase and run them parallel to our private cloud. I see this as a growth area for the next few years.

Photos: Oliver Krato



Christian Litschauer, Key Account Manager, T-Systems Austria, advises Prinzhorn-CIO Manfred Ofner on the testing of various cloud deployment models.

If you take another look into the future, what would be the next big thing in the IT context with regard to innovative competitive packaging solutions?

That's difficult to answer. But there is one general thing I am convinced of. The digitization share of the products will increase. That applies to everyone and it also applies to the packaging industry. This means that digitization will not only become more and more important in production, but will sooner or later also be incorporated into the product.

Could this, for example, concern the return of packaging products, i.e. equipping them with sensors? After all, your products already have a value in terms of raw materials and sustainable use.

The Prinzhorn Group with its three divisions is working intensively on the issue of increased internal value creation. We are starting with recycling. There we collect waste paper and waste cardboard to produce new raw materials. These are then processed into new corrugated base paper in the first step and then into corrugated packaging in the second step. A growing proportion of these are later returned to the container, the contents of which we recycle again, and the process starts all over again. Ideally a product life cycle as perpetuum mobile, if you like. If new technologies show that they can help us, we will use them. There is no question about that. For reasons of sustainability as well as for our customers and their customers.

Christian.Litschauer3@t-systems.com
www.prinzhorn-holding.com
www.t-systems.com/video/prinzhorn