AMPEG

KWS SAAT SE

70 Countries
at a Glance

A Security Lighthouse Case Study

70 Countries at a Glance

The more complex the technical and organisational structures of an IT landscape are, the more complex is also the assessment of the current security status of all systems. Until recently, KWS SAAT SE (KWS) solved this problem by manually comparing extensive tables originating from the most diverse sources around the globe. Now, Security Lighthouse by AMPEG collects and visualises the security-relevant data at the touch of a button. They are allotted according to the various roles and are made available nearly in real time to the KWS's own service centres and various IT service providers, which support the international KWS locations.

For 160 years now, KWS has been growing agricultural crops. Today, the company, with its headquarters in Einbeck in Germany, is one of the top international crop producers. KWS has more than 5,000 employees at locations in 70 countries on nearly all continents, which range from complete branch offices of various dimensions to small and very small representations, which sometimes only transmit measured data from test fields located in remote agricultural areas.

As a consequence of the company structure it is not possible to centralise the IT infrastructure with around 3500 client and 700 server systems completely. There are two important data centres at the headquarters, but the representations which are dispersed around the globe more or less work independently. As an example, some use their own Internet access because it is not possible to have a centralised communication due to possible transmission lags, and taking into account the consequences of the geo IP concept. Another reason is that KWS is not primarily active in the international metropolitan areas, but rather in rural areas where sometimes only a narrow-band Internet connection is available.

Visual check of sugar beet seedlings in a growth medium.
Source: KWS SAAT SE

Outsourced operative IT

KWS has placed substantial parts of its operative IT with service providers. Some of these service providers only take care for one region, others for several regions. Activities of the service providers, and the IT systems, are controlled by 5 KWS-owned service centres which are responsible for different regions: Germany, Western Europe, Eastern Europe, North America and South America.

This constellation requires a lot of organisational skills from the IT management and the security officers when it comes to checking the security status of the systems in the entire

70 Countries at a Glance

KWS network, to determining weak points and to rectifying them in a targeted way. KWS places a great deal of importance on a defined minimum security level for the IT because the results of its IT-based research and development are paramount for the market opportunities of this seeds supplier. In addition, global sales and the production control are closely interconnected with the IT systems, so confidentiality, integrity and availability of information and information technology have to meet high demands. *Currently, our IT systems do not have to comply with external compliance requirements*, Andreas Sternberg, IT Security Officer at KWS, says, explaining the significance of the security levels at the company, *but we define our own standards and have to find ways to enforce them internationally and to measure their success.*

Replacing a manual process

At staff level, KWS successfully employs staff members who are familiar with the regional culture and how best to explain the headquarters requirements to their fellow staff members and service providers at the various locations. However, there was no elaborate concept to solve the technical and organisational challenges of the global Security Level Management at the company. In particular, the process of the technical status determination of the IT security was to be organised in a much more efficient way. *We have been working with comprehensive Excel tables sent to us at regular intervals in order to have an overview of the existing IT systems and the installed software, but also of security tools, applied patches, virus patterns and other important data,* explains Sternberg, and he admits: *But this procedure did not offer us our desired direct access to the global status information.* The security team at KWS saw the risk that the gap between the actual security situation and the available data would widen with a growing company and its IT systems.

Working on an in vitro sugar beet culture under a microscope.
Source: KWS SAAT SE

Status information at the touch of a button on the dashboard

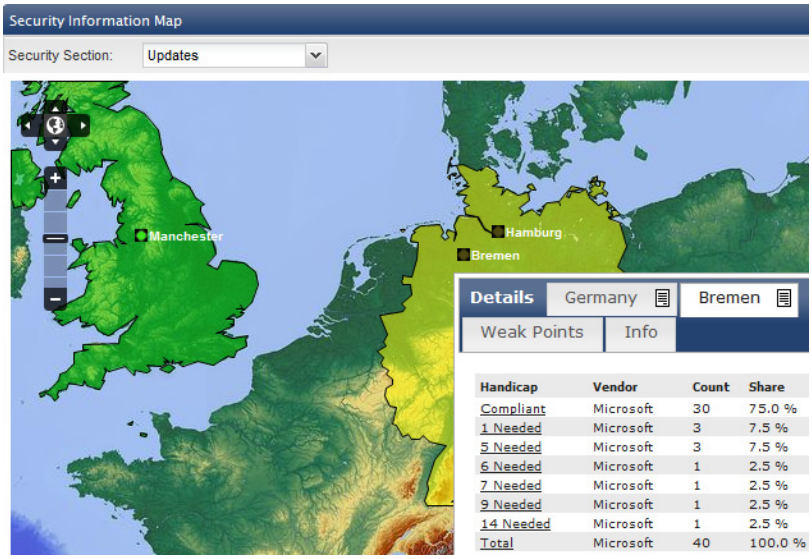
Against this background, KWS was looking for a solution to integrate the status of the security information from the system management and security tools into one dashboard, providing a current picture at any time - automatically, at the touch of a button and without any time lags, and independent of any data processing in the various time zones.

The security managers decided to install AMPEG Security Lighthouse as their monitoring system. The product is linked to the security systems in the network via “collectors”. It collects and correlates the collected data nearly in real-time and compares them to the company’s internal security requirements. The system processes the results in such a way that, among other things, they are visualised on a world map, representing the security level of the individual locations by traffic-light colours. In the event that there are some

70 Countries at a Glance

discrepancies or errors at one location - virus-pattern, which are not applied, missing software updates, omitted patches or delayed system feedback - the operator can investigate it in more detail by just one mouse click. At any time, s/he can request detailed information from a network segment down to the individual systems.

The more exact and up-to-date the data was, the easier it was for us to react in a target-oriented way, says Sternberg. If, e.g. the assessment of the tables previously used showed that a critical system had not contacted a certain system management tool for some time, and thus could not be up-to-date, the security team got in touch with the responsible service centre. The service centre in turn asked the relevant service provider to solve the problem. *Sometimes the result was that the system had been shut down in a controlled manner and had been replaced, or that in the meantime it had responded again*, says Matthias Helmke, Head of Infrastructure at KWS, when looking back. Such "false positives" caused unnecessary trouble, which Security Lighthouse now helps to avoid.



KWS looks closely at IT security as well. The Security Information Map in Security Lighthouse displays the current security status in near real-time.

At KWS a multitude of system management and IT security tools are connected to the AMPEG product: the virus protection, the patch and vulnerability management, the inventory, administration of the hard disk encryption, the active directory and other sources which allow evaluation of inconsistencies in the system tool messages by correlation. *Security Lighthouse allows all these security sections to be connected 'out of the box',* explains Michael Hänsel, project manager responsible at AMPEG, *and directly after the connection was established, all assessment results are available for analysing the security level.* Under these circumstances, the installation for the proof of concept phase at KWS took only 3 days. The security team was able to take over the configuration data directly from the PoC system when it came to the implementation of the productive solution, which went ahead without major effort.

In addition, AMPEG reacts quickly to requests of all kind and implements customer wishes very quickly, Sternberg adds, speaking about the positive experience of the introductory phase: *There are no long waiting times as we have known them from other service providers. Our supplier delivered missing analyses within two to three weeks.* In his

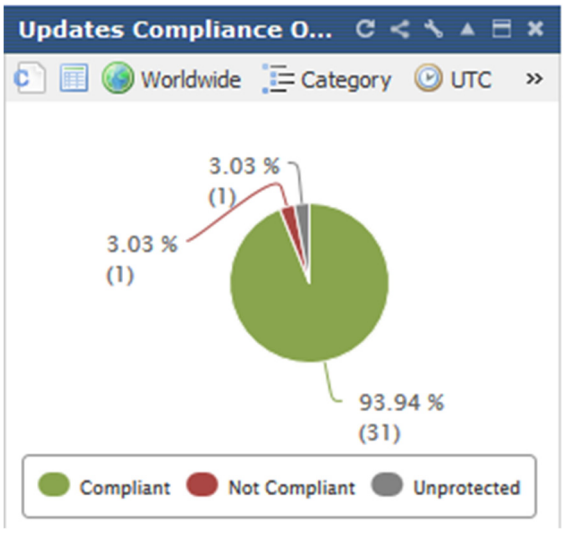
opinion, the high number of collectors on the one hand, and the excellent communication skills of AMPEG on the other hand are important also with regard to the flexibility of future investments: *For example, if we want to change our anti-virus system, we can be sure that Security Lighthouse will connect to the new product without problems and only little migratory effort.*

Required: role management

An important requirement for KWS was a sophisticated role management to access the status dashboards. This system specification was a result of the organisational special feature that possible defects in individual systems have to be solved at different KWS service centres and, in the end, with different service providers. Security Lighthouse offers a corresponding access control: *Based on the definition of their role, every service provider will see exactly the area they are responsible for, and we can be sure that they are effectively informed about the current tasks*, Sternberg describes the new situation.

AMPEG Security Lighthouse also plays a positive role in the communication with other departments of the company. Members of the management e.g. appreciate the well-designed visualisation of the security situation. Matthias Helmke points to another aspect: *If auditors want to have a look at our security level we are able to offer it immediately and in a remarkably vivid way. It is possible to generate reports quickly and tailored to the target groups. This makes audits considerably easier.*

We can see where we are, can go into detail immediately and can quickly find a solution, Andreas Sternberg summarises the result of the product introduction. Quality assurance in IT security is now timely and based on up-to-date information.



The global security level at a glance.

This solution was implemented at:

KWS SAAT SE
Grimsehlstrasse 31
37555 Einbeck, Germany
http://www.kws.com/

With support from:

AMPEG GmbH
Stavendamm 22
28195 Bremen, Germany
https://www.ampeg.de/