CASE STUDY

HANDL TYROL relies on Blocky for Veeam® ransomware backup protection from GRAU DATA

Security against targeted or mass attacks by cyber criminals is an issue that companies take seriously and therefore take appropriate protective measures. It is not just about the classic protection of clients, servers and network infrastructure. The steadily increasing danger from intelligently distributed ransomware requires a separate protective layer for the backups that are essential for survival. The family company HANDL TYROL has implemented the security of its backups with Veeam® in connection with the protection software Blocky for Veeam® from GRAU DATA.

HANDL TYROL is an Austrian family company based in Pians / Tyrol, which has specialized in the production of original Tyrolean bacon, ham, raw sausage and roast specialties since 1902. The medium-sized company, which is run in the fourth generation by Karl-Christian HANDL, employs 600 people and is a market leader as an ambassador for Tyrolean culinary delights and is known far beyond the borders.

The company is aware of the risk of being easily targeted by a ransomware attack. A scenario in which one would have to reckon with encryption of all business-relevant data is by no means acceptable for HANDL TYROL – not with regard to production and administration and certainly not with regard to a ransom demand from the cybercriminals to be paid.

“It was clear to us that protecting backups was the last line of defense against ransomware attacks. We therefore had to create suitable protection for our Veeam® data backups. For us, Blocky for Veeam® is the simplest and most effective solution to guarantee this security, ”explains Christian Nicolussi, IT manager at HANDL Tyrol Christian Nicolussi.

Backup for virtualized environment

By the end of 2019, the data load in the HANDL TYROL data center had become so high that a new data backup solution was required especially for the virtualized server environments. The previous data backup was no longer able to cope with the data growth, especially driven by photos, films and other media files. The new backup was implemented with a solution from Veeam®, which can meet the requirements for volume and performance not only today, but also for future expansion of the IT environment.

The IT team at HANDL TYROL was also impressed by the easy integration into the existing IT environment and the excellent handling of the backup solution. The new backup solution was installed and productive on a Dell platform under VMware at the beginning of 2020. Backups are written from EMC primary storage to QNAP storage systems on a daily basis. For geo-redundancy, the backups and their history are mirrored in another plant. HANDL TYROL thus has a total of 25 terabytes of backup data, distributed over two locations.

Security against ransomware

Even with the new and very satisfactory backup technology, the IT managers at HANDL TYROL had their concerns about the security of the backup data. Since the backup solution from Veeam® works with classic network shares, the data backups are visible in the internal network and thus in principle exposed to the risk of encryption by ransomware. In particular, new types of ransomware might be able to find their way not only to the primary storage, but also to the backup data.

“Encrypting our data on the production systems would be bad enough. But the additional encryption of our backups would be a catastrophe, because then we would no longer have the opportunity to restore our data without paying a ransom, ”confirms Christian Nicolussi.

This security problem was solved with special protection software for backups from GRAU DATA: Blocky for Veeam®. Veeam® makes this additional security layer available to its customers as an additional module to its data backup solutions – in this case together with its partner Cristie Data GmbH.

The IT managers at HANDL TYROL briefly considered a technical alternative. An additional Linux instance would have been integrated into the backup process to protect the backup data. However, this variant was much more complex and the decision was made very quickly for the lean solution with Blocky.

Ransomware protection through WORM technology

The technology behind Blocky for Veeam® comes from storage and archiving specialist GRAU DATA, who developed Blocky back in 2018. Blocky protects, based on the proven WORM (Write Only Read Many) technology from GRAU DATA. The WORM functionality prevents any changes to the data without explicit authorization.

Blocky uses the application fingerprint to identify only authorized Veeam® processes. This ensures that only Veeam® has full access to the valuable backup data. There is no way through this gateway for malware and the protection of the backup data from ransomware is guaranteed at all times.

The installation of the additional protection software Blocky for Veeam® took just over an hour via remote access. At the same time, the key employees in the seven-person IT department at HANDL TYROL got to know how the protection software works and the minimum amount of administrative work involved. The backup data of the virtual environment has also been protected since January 2020 and the company does not have to worry if ransomware should ever penetrate the traditional protective shields. Even in this case, the IT team would be able to restore the data quickly and reliably.

“It was important for us to ensure protection for our backup that can be quickly and easily integrated into our existing solution,” Christian Nicolussi sums up. “Blocky for Veeam® fits in seamlessly and is the ideal solution for us.”

For more information, contact sales@graudata.com