CASE STUDY

Maschinenringe Deutschland GmbH relies on backup with integrated WORM protection as the last line of defense against ransomware

Blocky for Veeam from GRAU DATA protects backups against encryption trojans using special WORM technology.

When organizations are attacked with ransomware by cybercriminals, it often comes out badly. Data is encrypted, including the backups, and the entire company runs into serious difficulties in getting IT and thus all work processes up and running again. As if the encryption had not already done enough damage, the criminals usually demand high ransoms for the decryption code - although it is never guaranteed that this actually and completely decrypts the data. To prevent such disaster scenarios, backups must always be available and must not be compromised by the ransomware. The agricultural association of machine rings has anticipated potential damage from ransomware and is protecting its internal data backups with the help of Blocky for Veeam from GRAU DATA. With this protection, which is seamlessly integrated into the backup software, machine rings can ensure that in the event of an attack, all data and systems are restored from the backups in the shortest possible time and that the blackmailers have no chance with their ransom demands.

The machine rings were founded in 1959 as an association and self-help organization for agriculture. In the association, for example, the participating farmers are provided with machines in a communal pool, spare parts and operating aids are offered or purchase and sales advantages are achieved for the community. In addition, the portfolio of services for the 192,000 member companies will also be expanded to include digital services. With the general advancement of digitalization, an organization like Maschinenringe Deutschland GmbH is also required to ensure the necessary steps for data security and IT security. Because the members rely on the constant availability of Maschinenringe.

The general danger situation gave cause for action

In January 2021, due to the increasingly frequent reports of ransomware attacks worldwide and in all industries, even more intensive protection was an issue for machine rings. Of course, at this point in time, the organization had good security solutions for servers, networks and endpoints. However, many examples of cyberattacks show that the

attackers repeatedly succeed in subverting this protection through massive criminal energy in order to encrypt all accessible data. Therefore, the importance of data and application backups has changed and is even more important. Backup solutions were originally used to ensure that in the event of a disaster - for example, a technical failure of servers, storage systems, a fire or a natural disaster - the data was saved as quickly as possible and, above all, with the smallest possible gap between the failure and the last Restore backup. Today the situation is very different today. Due to the increasing threat posed by ransomware, backups have become a kind of insurance that can save the company in the event of an attack. In an emergency, a restore of unencrypted data must be guaranteed in order to prevent downtimes and ransom payments.

The problem with classic backups, however, is that because of the large amounts of data, the enormous growth and the increasingly complex disaster / recovery and business continuity requirements, they are usually integrated into the network as a share and thus a potential and are achievable targets for ransomware. It is therefore important to isolate the backups in such a way that they are always and quickly available but still do not allow access by ransomware.

For those responsible at Maschinenringe Deutschland GmbH, it was clear from the start that the ransomware protection should be implemented while retaining the existing backup solutions. The backup solution from Veeam is used, which reliably backs up all servers and systems. In addition, there was a requirement that the IT team did not have to deal with any intensive additional administrative tasks. The protection system should be largely automated, have a clear and structured menu interface, provide detailed logs of access and be state-of-the-art, i.e. it should be able to be used over the long term.

The already trusted IT service provider Cristie Data had a suitable ransomware protection solution in its portfolio, which can be seamlessly integrated into the Veeam backup system. This is realized with the ransomware protection from GRAU DATA called Blocky for Veeam. After just one hour of presentation, the decision was made in April 2021 and the order for Blocky for Veeam was placed with Cristie Data.

“Attackers are now increasingly targeting secondary systems such as backups, as these have been neglected by many companies when it comes to protection. Fortunately, we have not had any ransomware incidents so far and it should stay that way. That's why we took preventive measures with the Blocky for Veeam solution to protect our systems, "says IT administrator Sascha Hein,

In the same month, the additional protection in the backup system was jointly installed by the IT specialists from Maschinenringe Deutschland GmbH and Cristie Data and put into operation after a test. The installation, including instruction, was completed in around 30 minutes.

Proven technology to protect against any ransomware

The technology behind Blocky for Veeam was developed by storage and archiving specialist GRAU DATA in 2018. Blocky protects backup data based on the proven WORM (Write Only Read Many) principle.

All backup sets are seamlessly transferred to a software WORM. The advantage: The WORM functionality inherently prevents any changes to data without explicit authorization, including encryption by ransomware. However, access to the data must be granted at exactly one point, namely during the backup process. For this, Blocky uses the unique

application fingerprint of the backup software. This ensures that only Veeam has full access to the valuable backup data. There is no way for malware to go through this gateway and the protection of the backup data from ransomware is always guaranteed.

“For us, three criteria were decisive. First, the additional security had to be seamlessly integrated into the existing systems. Second, it was important that the integration was quick and uncomplicated and that no further administration was required. Third, the cost of the software and the amount of work required were also important. Compared to other solutions, which usually would have required a complete overhaul and change of the backup structure, Blocky for Veeam is the most economical and at the same time the most secure solution. All three criteria are met by GRAU DATA Blocky for Veeam and we can be sure that in the event of an emergency, the data backups will be available without restriction and, above all, unencrypted”, Sascha Hein sums up.

For more information contact: sales@graudata.com