GRAU DATA

CASE STUDY

Die Maschinenringe Deutschland GmbH setzt als letzte Verteidigungslinie gegen Ransomware auf Backup mit integriertem WORM-Schutz

Blocky for Veeam® von GRAU DATA schützt Backups vor Verschlüsselungs-Trojanern durch spezielle WORM-Technologie.

Wenn Organisationen von Cyberkriminellen mit Ransomware angegriffen werden, kommt oft nichts Gutes dabei heraus. Daten werden inklusive der Backups verschlüsselt und die gesamte Unternehmung gerät in ernsthafte Schwierigkeiten, die IT und damit alle Arbeitsprozesse wieder ans Laufen zu bringen. Als wäre mit der Verschlüsselung nicht schon genug Schaden angerichtet, fordern die Kriminellen meist hohe Lösegelder für den Entschlüsselungs-Code – wobei niemals garantiert ist, dass dieser die Daten auch tatsächlich und komplett entschlüsselt. Um derartigen Katastrophenszenarien vorzubeugen, müssen Backups stets zur Verfügung stehen und dürfen von der Ransomware nicht kompromittiert werden. Einem potenziellen Schaden durch Ransomware hat die landwirtschaftliche Vereinigung der Maschinenringe vorgebaut und schützt seine internen Daten-Backups mit Hilfe von Blocky for Veeam® von GRAU DATA. Mit diesem nahtlos in die Backup Software integrierten Schutz kann Maschinenringe sicherstellen, dass bei einer Attacke alle Daten und Systeme in kürzester Zeit aus den Backups wiederhergestellt werden und die Erpresser keine Chance mit ihren Lösegeldforderungen haben.

Die Maschinenringe wurden 1959 als Verband und Selbsthilfeorganisation für die Landwirtschaft gegründet. In der Vereinigung werden den teilnehmenden Landwirten beispielsweise Maschinen in einem gemeinschaftlichen Pool zur Verfügung gestellt, Ersatzteile und Betriebshilfen angeboten oder Ein- und Verkaufsvorteile für die Gemeinschaft erzielt. Darüber hinaus wird das Portfolio an Dienstleistungen für die 192.000 Mitgliedsbetriebe auch auf digitale Services ausgeweitet. Mit der allgemein fortschreitenden Digitalisierung ist auch eine Organisation wie die Maschinenringe Deutschland GmbH gefragt, die nötigen Schritte für die Datensicherheit und IT-Security zu gewährleisten. Denn die Mitglieder verlassen sich auf die stetige Verfügbarkeit der Maschinenringe.

GRAU DATA GmbH
Marie-Curie-Str. 19
D - 73529 Schwäbisch Gmünd
Tel: 07171/187-0
Fax: 07171/187-250

E-Mail: info@graudata.com
www.graudata.com

Allgemeine Gefahrenlage gab Anlass zum Handeln

Im Januar 2021 war aufgrund der zunehmend häufigen Berichte über Ransomware-Attacken weltweit und in allen Branchen der noch intensivere Schutz ein Thema für Maschinenringe. Selbstverständlich verfügte die Organisation zu diesem Zeitpunkt über gute Security-Lösungen für Server, Netzwerk und Endpoints. Allerdings zeigen viele Beispiele von Cyberattacken, dass es den Angreifern durch massive kriminelle Energie immer wieder gelingt, diesen Schutz zu unterwandern, um alle erreichbaren Daten zu verschlüsseln.

Daher kommt der Bedeutung der Backups von Daten und Applikationen eine veränderte und noch wichtigere Rolle zu. Backup-Lösungen dienten ursprünglich dazu, bei einem Desaster – etwa einem technischen Ausfall von Servern, Storage-Systemen, einem Brand oder einer Naturkatastrophe – die Daten so schnell wie möglich und vor allem mit einer möglichst kleinen Lücke zwischen dem Ausfall und der letzten Sicherung wiederherzustellen. Heute ist die Lage heute eine ganz andere. Backups sind aufgrund der immer größeren Gefahrenlage durch Ransomware zu einer Art Versicherung avanciert, die im Falle eines Angriffs die Unternehmung retten können. Es muss im Ernstfall ein Restore von unverschlüsselten Daten gewährleistet sein, um Ausfallzeiten sowie Lösegeldzahlungen zu verhindern.

Das Problem von klassischen Backups ist allerdings, dass sie wegen der hohen Datenmengen, der enormen Zuwächse sowie aufgrund der zunehmend komplexen Desaster/Recovery- und Business-Continuity-Ansprüche meist als Share in das Netzwerk eingebunden und damit ein potenzielles und erreichbares Angriffsziel für Ransomware sind. Es gilt also, die Backups so abzuschotten, dass sie stets und schnell zur Verfügung stehen aber dennoch keinen Zugriff von Ransomware erlauben.

Für die Verantwortlichen der Maschinenringe Deutschland GmbH war von Anfang an klar, dass der Ransomware-Schutz unter Beibehaltung der existierenden Backup-Lösungen erfolgen sollte. Zum Einsatz kommt die Backup-Lösung von Veeam®, die zuverlässig die Datensicherung aller Server und Systeme durchführt. Zudem bestand die Anforderung, dass keine intensiven zusätzlichen administrativen Aufgaben auf das IT-Team zukommen. Das Schutzsystem sollte weitgehend automatisiert seinen Dienst verrichten, über eine übersichtliche und strukturierte Menüoberfläche verfügen, ausführliche Protokolle von Zugriffen liefern und State of the Art, also langfristig einsetzbar sein.
Der bereits vertraute IT-Dienstleister Cristie Data hatte eine passende Ransomware-Schutzlösung im Portfolio, die sich nahtlos in das Backup-System von Veeam® einfügt. Realisiert wird dies mit dem Ransomware-Schutz von GRAU DATA namens Blocky for Veeam®.
Nach nur einer Stunde Präsentation war im April 2021 die Entscheidung gefallen und der Auftrag für Blocky for Veeam® an Cristie Data erteilt.

„Angreifer haben es mittlerweile verstärkt auf Sekundärsysteme wie Backups abgesehen, da diese von vielen Unternehmen beim Schutz vernachlässigt wurden. Bisher gab es bei uns zum Glück keine Ransomware-Vorfälle und so soll es auch bleiben. Deshalb ergriffen wir mit der Lösung Blocky for Veeam präventive Maßnahmen, um unsere Systeme zu schützen", sagt IT-Administrator Sascha Hein,

Noch im selben Monat wurde der zusätzliche Schutz im Backup-System gemeinsam von den IT-Spezialisten der Maschinenringe Deutschland GmbH und Cristie Data installiert und nach einem Test in Betrieb genommen. Erledigt war die Installation inklusive Einweisung nach nur rund 30 Minuten.

Bewährte Technologie zum Schutz gegen jegliche Ransomware

Die Technologie hinter Blocky for Veeam® wurde vom Speicher- und Archivierungsspezialisten GRAU DATA im Jahr 2018 entwickelt. Blocky schützt Backup-Daten basierend auf dem bewährten WORM (Write Only Read Many)-Prinzip.

Dabei werden sämtliche Sicherungssätze nahtlos in ein Software-WORM überführt. Der Vorteil: Die WORM-Funktionalität verhindert systemimmanent jegliche Änderung von Daten ohne explizite Berechtigung, einschließlich einer Verschlüsselung durch Ransomware. Allerdings muss an genau einer Stelle der Zugriff auf die Daten gewährt werden, nämlich beim Backup-Prozess. Hierfür nutzt Blocky den einmaligen Anwendungsfingerabdruck der Backup-Software. Damit ist gewährleistet, dass ausschließlich Veeam® einen Vollzugriff auf die wertvollen Backup-Daten hat. Für Schadsoftware führt kein Weg durch dieses Tor und der Schutz der Backup-Daten vor Ransomware ist zu jederzeit gewährleistet.

„Für uns waren drei Kriterien entscheidend. Erstens musste sich die zusätzliche Sicherheit nahtlos in die bestehenden Systeme integrieren lassen. Zweitens war es wichtig, dass die Integration schnell und unkompliziert möglich ist und keine weitere Administration erfordert. Drittens waren auch die Kosten für die Software und der benötigte Arbeitsaufwand von Bedeutung. Im Vergleich zu anderen Lösungen, die meist eine komplette Überarbeitung und Änderung der Backup-Struktur erfordert hätten, ist Blocky for Veeam® die wirtschaftlichste und zugleich sicherste Lösung. Alle drei Kriterien werden von GRAU DATA Blocky for Veeam® erfüllt und wir haben die Sicherheit, dass im Ernstfall die Datensicherungen uneingeschränkt und vor allem unverschlüsselt zur Verfügung stehen", resümiert Sascha Hein.

GRAU DATA GmbH
Marie-Curie-Str. 19
D - 73529 Schwäbisch Gmünd
Tel: 07171/187-0
Fax: 07171/187-250

E-Mail: info@graudata.com
www.graudata.com