Case Study Universität zu Lübeck – Blocky for Veeam®

Kompromissloser Ransomware-Schutz für Backups

Prävention ist das A&O, damit Daten nicht kompromittiert oder gar durch Cyberkriminelle verschlüsselt werden. Diese Regel gilt für klassische Unternehmen gleichermaßen wie für die öffentliche Verwaltung oder Bildungseinrichtungen. Überall geht es darum, sensible Daten zu schützen und vor allem den Betrieb im Falle einer Cyber- oder Ransomware-Attacke so schnell wie möglich und ohne Datenverlust oder Lösegeldzahlungen weiterzuführen. Genauso sieht das auch **IT-Leiter Helge Illig** von der **Universität zu Lübeck**, wenn es um die teils wertvollen und jedenfalls schützenswerten Daten der Universität geht. Daher setzen er und seine Kollegen in der IT-Abteilung neben klassischen Security-Maßnahmen insbesondere auf ein Backup, das von Cyberkriminellen nicht verschlüsselt werden kann. Seit März 2023 werden die Backup-Daten der Universität zu Lübeck zusätzlich mit **Blocky for Veeam®** vor einem unautorisierten Zugriff und damit wirkungsvoll vor Ransomware geschützt.

Lage und Handlungsbedarf

Dem IT-Leiter und seinem Team war klar, dass das Gefahrenpotenzial insbesondere in Bezug auf Ransomware stetig zunimmt. Zwar musste die Universität zu Lübeck noch keinen Ransomware-Angriff bewältigen, allerdings gaben die jüngsten Berichte, die intensive Angriffswellen auf Bildungseinrichtungen bestätigen, Grund zur Vorsicht. Im November 2022 entschlossen sich die IT-Experten, einem potenziellen Schaden durch Ransomware vorzubeugen, indem sie ihre Backups gegen eine Verschlüsselung schützen. Es war das Ziel, jederzeit vollständige Backups zur Verfügung zu haben – auch im Fall eines Ransomware-Angriffs. Damit kann sichergestellt werden, dass Daten nicht dauerhaft verloren gehen und dass man sich den Erpressungsversuchen der Cyberkriminellen nicht beugen muss, um die Backups zu entschlüsseln.

UNIVERSITÄT ZU LÜBECK

Ransomware-Schutz soll einfach, unkompliziert und wirkungsvoll sein

Für die Lösung gab es seitens der IT-Experten ein paar wichtige Kriterien. Erstens muss die Datensicherheit auf jeden Fall garantiert sein. Zweitens sollte die Anwendung die Administratoren nicht mit zusätzlicher kontinuierlicher Arbeit belasten oder durch hohe Komplexität zu Fehlerrisiken in der Bedienung oder Konfiguration führen. Drittes Kriterium für die Lösung war, sich einfach und schnell in die existierende IT-Umgebung und ohne zusätzlich separate Hard- und Software-Infrastruktur zu integrieren. Last but not least war auch der Kostenfaktor ausschlaggebend. „Wir haben weder die Zeit noch die Ressourcen für eine komplizierte und kostspielige Lösung. Das System muss nach der Installation einfach und zuverlässig laufen, damit wir uns im Notfall hundertprozentig darauf verlassen können“, erklärt Helge Illig.

itiso GmbH	Anschrift:	Bankverbindung:	Registergericht:	Geschäftsführung
Telefon: 040-53299 410	Flughafenstr. 52a	Volksbank Sprockhövel	Hamburg	Mukesh Unadcath
Telefax: 040-53299 100	22335 Hamburg	IBAN DE40452615470108493900	HRB 96090	Ronald Martens
E-Mail: info@itiso.de		BIC GENODEM1SPO		

Die Entscheidung fiel schnell, nicht zuletzt auch aufgrund des langjährig vertrauten IT-Systempartners itiso. Da itiso seit 2011 die Universität im Bereich Storage und damit auch beim Backup unterstützt, hatte das Systemhaus mit Blocky for Veeam® von GRAU DATA eine pragmatische und vor allem zuverlässige Lösung parat, die sich unmittelbar in das existierende Backup von Veeam integrieren lässt. Die Software für den Ransomware-Schutz funktioniert nahtlos mit der Backup-Software von Veeam, was eine reibungslose und unkomplizierte Interaktion der beiden Software-Lösungen garantiert.

Das elegante daran: Neben dem sicheren Repository, in dem das Veeam® Backup die Daten mit Hilfe von Blocky for Veeam® vor Ransomware geschützt speichert, sind die IT-Experten davon überzeugt, dass eine zusätzliche Sicherheit erreicht wird, wenn die Software-Lösungen von unterschiedlichen Herstellern stammen. „Somit haben wir ohne zusätzlichen Aufwand eine zusätzliche Plattform für unser geschütztes Backup. Das macht unserer Meinung nach den Gesamtschutz noch resilienter“, erklärt Illig.

Bewährte Technologie, optimaler Schutz

Der Ransomware-Schutz Blocky for Veeam® baut auf einer Technologie auf, die GRAU DATA bereits vor vielen Jahren entwickelt, kontinuierlich verfeinert und speziell für diese Anwendung mit einigen Besonderheiten angepasst hat: die bewährte GRAU DATA WORM-Technologie.
Aus Sicht des Anwenders erlaubt das Software-WORM einmaliges Schreiben und unbegrenztes Lesen, jedoch keinerlei Veränderung einer Datei. In einer dedizierten Softwareschicht, welche im Betriebssystemkern implementiert ist, wird das Schreiben von Daten auf der Festplatte kontrolliert und überwacht. Ein Filter zwischen Dateisystem und physischer Festplatte steuert alle schreibenden Zugriffe auf das Dateisystem. Zugelassen sind lediglich Schreibvorgänge für neue Dateien und das Lesen existierender Daten. Ein nachträgliches Verändern vorhandener Daten wird über den Filter verhindert. Und genau diese Technologie hilft auch Backupdaten zu schützen, indem das Schreiben und damit auch das Verschlüsseln von Daten durch Ransomware wirksam unterbunden wird.
Allerdings müssen Backuplösungen wie Veeam® die Daten nicht nur schreiben, sondern auch verändern können. Schließlich müssen sich die Änderungen am originalen Datenbestand auch im Backup niederschlagen. Zudem muss die Möglichkeit bestehen, Altbestände nach Ablauf der Aufbewahrungspflicht zu löschen. Hierfür hat GRAU DATA die Türe des Software-WORM in Blocky for Veeam® ein kleines Stückchen geöffnet, damit ausschließlich der Backuplösung das Verändern der Daten gestattet wird. Die Backupanwendung muss sich mit ihrem sicheren digitalen Fingerabdruck gegenüber der Filterschicht ausweisen. Nur wenn der Fingerabdruck mit einer zuvor hinterlegten Referenz übereinstimmt, lässt die Filterschicht den schreibenden Zugriff der Backupanwendung auf die Daten zu. Alle anderen Anwendungen, insbesondere Schadsoftware, können sich nicht mit einem Fingerabdruck ausweisen und werden somit durch den Filter blockiert. Die Ransomware trifft somit auf WORM-geschützte Backupdaten und hat keine Chance.

„Mit dieser von itiso vorgeschlagenen Lösung wurden alle von uns aufgestellten Anforderungen erfüllt. Wir haben einen wirkungsvollen Schutz gegen die Verschlüsselung durch Ransomware, der zusätzlich unautorisierte Zugriffsversuche dokumentiert, und wir können uns im Worst Case auf ein unverschlüsseltes, funktionierendes Backup verlassen. Noch besser, die Lösung passt sehr gut in unser Budget“, freut sich IT-Leiter Illig.

Kompletter Backup-Schutz nach nur 3 Stunden

Die Installation des Ransomware-Schutzes wurde in Zusammenarbeit mit dem IT-Team der Universität, itiso und einem Spezialisten von GRAU DATA großteils remote durchgeführt. Sie dauerte inklusive Einrichtung, Administration und minimalem Schulungsaufwand nicht mehr als drei Stunden. Illig dazu: „Anpassungen an unserem existierenden System mussten weder im Voraus noch bei der Installation vorgenommen werden. Blocky for Veeam® wurde installiert und auf dem zu schützenden Laufwerk aktiviert. Seit diesem Zeitpunkt ist der Schutz vor unautorisierten Zugriffsversuchen aktiv.“

Der vielleicht größte Vorteil für die Universität zu Lübeck: Mit einem vergleichsweise kleinen technischen Aufwand konnte die Sicherheit und Cyber-Resilienz des Backups entscheidend erhöht werden. Sollten laufende Systeme der Universität verschlüsselt werden, sind die IT-Profis in der Lage, die Systeme schnell und vollständig wiederherzustellen, ohne „auf der grünen Wiese“ neu beginnen zu müssen. Seit März 2023 ist Blocky for Veeam® von GRAU DATA bei ihnen aktiv und ohne zusätzlichen Aufwand für die Administratoren im Einsatz. Gelegentlich werden Daten als Test und ohne jegliche Beanstandung aus dem Backup-Repository zurückgespielt. „Seit wir den Ransomware-Schutz für unsere Backups einsetzen, sind wir gut vorbereitet. Auch wenn wir natürlich hoffen, dass wir nie in diese Lage kommen, ist die Gefahr eines Ransomware-Angriffs relativ hoch.

Unserer Meinung nach ist besser, für einen guten Schutz zu sorgen, anstatt sich im Ernstfall auf das kostspielige und zeitintensive Spiel der Cyberkriminellen einzulassen, bei dem man den Ausgang nicht kennt“, resümiert Helge Illig.

Über die Universität zu Lübeck
Die Universität zu Lübeck (UzL) ging 1973 als Medizinische Hochschule Lübeck aus der 1964 errichteten zweiten Medizinischen Fakultät der Christian-Albrechts-Universität (CAU) hervor. Stand 2022 sind an der UzL 5.142 Studierende eingeschrieben. Seit 2015 befindet sie sich in der Trägerschaft einer öffentlich-rechtlichen Stiftung. Sie ist damit die einzige Stiftungsuniversität in Schleswig-Holstein. Die UzL versteht sich als Life-Science-Universität und ist in die drei Sektionen Medizin, Naturwissenschaften und Informatik/Technik gegliedert.

Über GRAU DATA
GRAU DATA ist der Spezialist für Datenarchivierung, Data Protection & Metadata-Mining. GRAU DATA ist ein mittelständisches Unternehmen mit Sitz in Schwäbisch Gmünd bei Stuttgart. Eine starke Entwicklungsmannschaft sorgt für innovative Software-Lösungen. GRAU DATA verkauft ihre Produkte indirekt über Vertriebspartner wie Systemhäuser, Integratoren und Hardwarelieferanten in Deutschland, Europa und den USA.

Über die itiso GmbH:
„Bei itiso stehen die speziellen Anforderungen und Herausforderungen Ihres Unternehmens immer im Fokus. So verhelfen wir Ihnen zu Lösungen, die Ihr Datenmanagement optimieren und Sie für die Zukunft wappnen. Unser Ansatz zahlt sich aus: Wir dürfen immer mehr namhafte mittelständische und international agierende Firmen unterstützen. Sie alle vertrauen auf unsere Expertise rund um Datenanalyse, Virtualisierungs-, Backup- und Recovery-, Disaster-Recovery sowie digitale Archivierungsfragen. Von der Bestandsaufnahme über den Vergleich von Konzepten und Angeboten bis hin zu Ausschreibungen und schließlich der Entwicklung und Implementierung – die erfahrenen Spezialisten und Projektmanagement-Veteranen von itiso stellen sicher, dass Ihre IT Ihr Unternehmenswachstum fördert, nicht hemmt.

itiso GmbH	Anschrift:	Bankverbindung:	Registergericht:	Geschäftsführung
Telefon: 040-53299 410	Flughafenstr. 52a	Volksbank Sprockhövel	Hamburg	Mukesh Unadcath
Telefax: 040-53299 100	22335 Hamburg	IBAN DE40452615470108493900	HRB 96090	Ronald Martens
E-Mail: info@itiso.de		BIC GENODEM1SPO		