„Das Thema Cyber Security hat bei unserer Geschäftsführung einen relativ hohen Stellenwert - man war und ist sich der Tatsache bewusst, dass man etwas tun muss.“

Marcus Thiel,
Teamleiter IT bei AUG. PRIEN

REFERENZBERICHT

PowerProtect Data Domain und Cyber Recovery bei AUG. PRIEN Bauunternehmung (GmbH & Co. KG)

DAS UNTERNEHMEN

Seit knapp 150 Jahren erbringt die AUG. PRIEN Bauunternehmung (GmbH & Co. KG) mit Sitz in Hamburg Bauleistungen für den Hoch- und Industriebau in Norddeutschland, sowie im Rhein-Main-Gebiet und Nordrhein-Westfalen. Dabei setzt das Unternehmen vom ersten bis zum letzten Tag auf individuelle und persönliche Betreuung, um die Projekte zur vollsten Zufriedenheit ihrer Auftraggeber umzusetzen. Die Kunden, welche vom Generalunternehmer bis hin zum privaten Bauherren reichen, profitieren von einem breiten Leistungsportfolio und fachübergreifendem Wissen. So steht AUG. PRIEN seit seiner Gründung 1873 für Kompetenz, Qualität und Zuverlässigkeit in allen Geschäftsbereichen und verbindet handwerkliche Tradition mit modernster Technik.

DIE HERAUSFORDERUNG

Die Anzahl der Cyber-Attacken steigt dramatisch und das Strickmuster von Ransomware-Angriffen ist dabei sehr unterschiedlich. Oftmals werden die betroffenen Unternehmen zunächst im Backup verschlüsselt und dann geht der Angreifer systematisch auf die Primärsysteme über. „Das Thema Cyber Security hat bei unserer Geschäftsführung einen relativ hohen Stellenwert - man ist sich der Tatsache bewusst, dass man etwas tun muss“, berichtet Marcus Thiel, Teamleiter IT bei AUG. PRIEN. Das Unternehmen wollte eine zusätzliche Barriere und Sicherheit schaffen. Sollte das Backup im produktiven Netzwerk ebenfalls von dem Angriff betroffen sein, müssen die Daten vor Verlust geschützt sein.

AUG. PRIEN hatte bereits eine redundante Data Domain-Lösung von Dell EMC im Einsatz und die Sicherung der Daten erfolgte auf einem primären und zusätzlich auf einem sekundären Backup-System. Beide Infrastrukturen agierten zu diesem Zeitpunkt jedoch mehr als ein einziges System, da auf der sekundären Einheit ausschließlich Klone erzeugt wurden, um logische Fehler oder ähnliches auszuschließen. Sie diente also hauptsächlich der Ausfallsicherheit und umfasste außerdem die Archive.

DIE LÖSUNG

AUG. PRIEN entschied sich dafür, das existierende Sicherheitskonzept zu erweitern und die Schutz-Software „Cyber Recovery“ von Dell EMC einzusetzen. Diese ist eine Art letzte Verteidigungslinie gegen Malware-Angriffe und schafft eine zusätzliche Sicherheitsstufe, um die Systeme oder besser gesagt die Backup-Daten dahinter noch effektiver zu schützen.

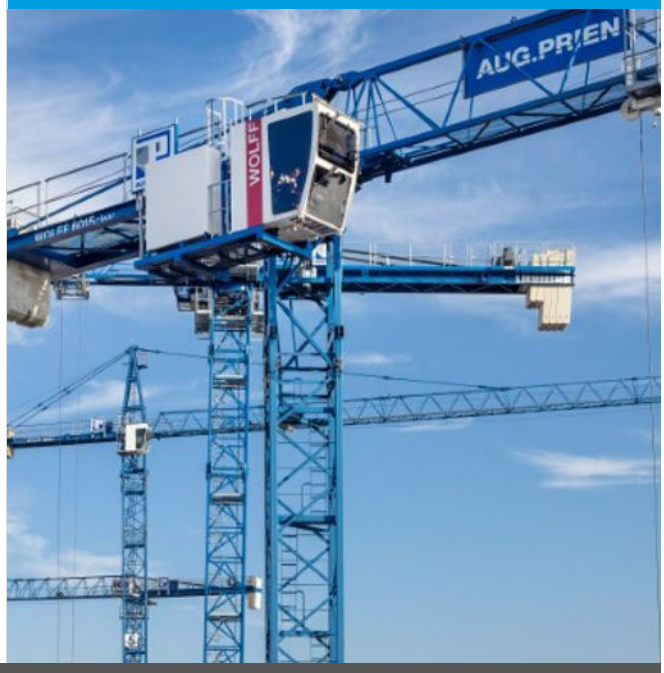
Konkret hatte das zur Folge, dass die zweite Data Domain Appliance aus dem bereits bestehenden Backup-Konzept in einem sogenannten „Cyber Vault“ untergebracht wurde, welcher hinter einer weiteren Firewall steht und nur über ein Air Gap* zu erreichen ist. Der Kommunikationsweg kann dann nur von der Cyber Vault Data Domain geöffnet werden. Des Weiteren wird die Funktion „Retention Lock“ als Governance- oder Compliance-Modus angewendet und für den in der Aufbewahrungssperre festgelegten Zeitraum können diese Daten nicht geändert, überschrieben oder gelöscht werden. Der Retention-Lock-Modus wird für strenge regulatorische Standards des Unternehmens verwendet und sichert das Data Domain-System über einen Security Officer gegen innere und äußere Angriffe ab. Wenn der Security Officer einmal angelegt ist, haben alle weiteren Benutzer nur noch operative Rechte und können weder Benutzer ausschließen, Daten löschen, verändern oder verschlüsseln. Ein Zugriff ist nur physisch, direkt am System möglich. Das beim Kunden eingesetzte BOOST-Protokoll ist vor Angriffen geschützt und macht eine Verschlüsselung der Systeme unmöglich, da diese nicht im Netzwerk sichtbar sind. Die Archive laufen weiterhin auf dem Sekundär-System - jetzt jedoch innerhalb der Cyber Recovery-Lösung und abgetrennt von dem Standard-Netzwerk.

Begonnen haben die Arbeiten an dem Projekt im Oktober 2020. Zum Projektteam gehörten drei bzw. kurzzeitig vier Mitarbeiter auf der Seite von AUG. PRIEN und beim Partner GID waren drei weitere Personen beteiligt. Aktuell gilt das Projekt als erfolgreich beendet und Marcus Thiel erklärt: „Die Lösung als solche ist umgesetzt - und auch genau so, wie wir uns das vorgestellt haben. Es ist eine präventive Maßnahme und keine Reaktion auf einen bereits erfolgten Angriff.“ AUG. PRIEN ist ein sehr gutes Beispiel dafür, wie wichtig die Vorausplanung im Bereich IT-Security ist. Der IT-Leiter betont noch einmal: „Meine klare Empfehlung ist die, sich frühzeitig Gedanken darüber zu machen, wie man das System aufsetzen möchte, und alle

* **Air Gap** (englisch für „Luftspalt“) meint einen Prozess, der zwei IT-Systeme physisch und logisch voneinander trennt, aber dennoch die Übertragung von Daten zulässt.

„Das System ist vollständig einsatzbereit und tut, was es (derzeit) tun soll - wir hoffen natürlich, dass wir diese letzte Instanz nie benötigen werden.“

Marcus Thiel,
Teamleiter IT bei AUG. PRIEN



Aspekte zu beleuchten. Das Ganze geht auch einher mit einem fundierten Backup-Konzept und man muss meiner Meinung nach auch erst mal etwas Aufwand investieren und verstehen, wie dieses System an sich funktioniert. Die Technologie dahinter ist komplex und umfangreich. Man ist gut beraten, vorneweg über Konzepte und Grundlagen nachzudenken und darüber, wie die Lösung am Ende implementiert und betrieben werden soll - das sollte man einmal wirklich ernsthaft tun."

DER PARTNER – GID GmbH

Die Global Information Distribution GmbH (GID) ist ein deutschlandweit agierendes Systemhaus mit Hauptsitz in Köln. GID als Systemintegrator berät und bietet Lösungen in den Bereichen Infrastruktur, HCI, Storage, Backup, E-Mail-/File-Management, Deduplizierung, Server, Clients und Virtualisierung an. In den vergangenen Jahren haben sich interessante Entwicklungen im Bereich HCI (Hyperconverged Infrastructure) ergeben, mit denen GID sehr erfolgreich ist. Gemeinsam mit Dell Technologies trifft GID nun Vorsorgemaßnahmen für seine Kunden gegen Ransomware als Angstgegner Nummer 1 mit Hilfe der Schutz-Software „Cyber Recovery". Langjährige Erfahrung und bei namhaften Partnern zertifizierte Spezialisten in Vertrieb und Technik setzen die Projekte um und halten so die IT ihrer Kunden auf Erfolgskurs. Weitere Informationen zu den Produkten und Services der GID GmbH finden Sie unter https://www.gid-it.de oder folgen Sie uns auf LinkedIn, XING und Facebook.

Global Information Distribution GmbH.
Wissen bewahren - Zukunft sichern.

GLOBAL INFORMATION
DISTRIBUTION GMBH

DELL Technologies
PLATINUM PARTNER

Global Information Distribution GmbH
Hauptsitz, Vertrieb und Service
Brügelmannstr. 5
50679 Köln

Telefon: +49 (0) 221 837902-0
Telefax: +49 (0) 221 837902-30
E-Mail: info@gid-it.de
Web: https://www.gid-it.de

GID in Ihrer Nähe
Niederlassung Augsburg
Morellstr. 33, 86159 Augsburg
Telefon: +49 (0) 821 25849-0
E-Mail: augsburg@gid-it.de

Weitere Vertriebsstandorte
Frankfurt frankfurt@gid-it.de
Stuttgart stuttgart@gid-it.de
Berlin berlin@gid-it.de