★★★★★

Mehrstufige Datensicherung von ExaGrid

Schnellste Datensicherungen.

Schnellste Datenwiederherstellungen.

Unerreichtes, preiswertes Scale-out.

ExaGrid

Retention Time-Lock – vorübergehende Sperrung von Datensicherungen zum Schutz gegen Erpressersoftware (Ransomware)

Ransomware-Angriffe sind auf dem Vormarsch und werden für Unternehmen immer störender und potenziell sehr kostspielig. Egal wie akribisch ein Unternehmen die empfohlenen Vorgehensweisen zum Schutz wertvoller Daten befolgt, die Angreifer scheinen immer einen Schritt voraus zu sein. Sie verschlüsseln böswillig die Primärdaten, übernehmen die Kontrolle über die Datensicherungsanwendung und löschen die gesicherten Daten.

Der Schutz vor Epressersoftware (Ransomware) steht heute bei den Unternehmen im Vordergrund. ExaGrid bietet einen einzigartigen Ansatz, um sicherzustellen, dass Angreifer die gesicherten Daten nicht beeinträchtigen können.

Die Herausforderung besteht darin, die gesicherten Daten vor dem Löschen zu schützen. Gleichzeitig soll auch ermöglicht werden, dass Datensicherungen bereinigt werden, wenn Retentionspunkte erreicht sind. Wenn Sie alle Daten eines Speicherorts sperren, können Sie die Retentionspunkte nicht löschen und die Speicherkosten werden untragbar. Wenn Sie das Löschen von Retentionspunkten zulassen, um Speicherplatz zu sparen, bleibt das System für Hacker angreifbar, und alle Daten können gelöscht werden.

Der einzigartige Ansatz von ExaGrid heißt „Retention Time-Lock". Es verhindert, dass Hacker die Datensicherungen löschen, und ermöglicht das Bereinigen von Retentionspunkten. Das Ergebnis ist eine starke Datensicherungs- und Wiederherstellungslösung mit sehr geringem Speicheraufwand.

ExaGrid ist eine mehrstufige Datenspeicherung auf Basis einer Landezone mit Frontend-Festplatten-Cache und einer separaten Wiederherstellungsebene, die alle gespeicherten Daten enthält. Die Daten werden direkt in die „dem Netzwerk zugewandte" Landezone im Festplatten-Cache geschrieben. Anschließend werden diese Daten an einen „nicht dem Netzwerk zugewandten" Langzeitspeicherort verlegt, wo sie als deduplizierte Datenobjekte gespeichert werden, um die Kosten der Speicherung für die Langzeitvorhaltung vorgesehener Daten zu senken. Bei der Einordnung der Daten in die Retentionsebene werden sie dedupliziert und in einer Reihe von Objekten und Metadatensätzen gespeichert. Genau wie bei anderen Objektspeichersystemen verändern sich die Objekte und Metadatensätze von ExaGrid niemals. Hieraus folgt, dass ausschließlich das Erstellen neuer Objekte und das Löschen alter Objekte zulässig sind, wenn die Retention erreicht wurde.

Die Methode von ExaGrid im Kampf gegen Ransomware ermöglicht es Unternehmen und anderen Einrichtungen, einen Time Lock festzulegen, der für das Abarbeiten von Löschaufträgen in der Retentionssebene maßgebend ist, da diese Ebene dem Netzwerk nicht zugewandt und für Hacker nicht zugänglich ist. Die Kombination aus einer nicht dem Netzwerk zugewandten Ebene, einer verzögerten Löschung über einen bestimmten Zeitraum und Objekten, die sich nie ändern, sind die Teile der Retentions-Time-Lock-Lösung von ExaGrid. Wenn beispielsweise der Time Lock der Retentionsebene auf 10 Tage eingestellt wird, dann werden, sobald Löschanfragen von einer schadhaften Datensicherungsanwendung oder einem gehackten CIFS oder anderen Datenaustauschprotokollen an das ExaGrid-System gesendet werden, die in der Retentionsebene vorhandenen Daten bis zu 10 Tage gegen jede Art von Löschung gesperrt. Die Daten in der Landezone werden gelöscht oder verschlüsselt. Die Daten in der Retentionsebene werden jedoch bei einer externen Anfrage für den konfigurierten Zeitraum nicht gelöscht. Wenn ein Ransomware-Angriff registriert wird, können Sie Ihr ExaGrid-System einfach in einen neuen Modus für die Datenwiederherstellung schalten und anschließend alle gesicherten Daten wieder am primären Speicherort herstellen. Die Länge des Time Locks ist separat und ein Zusatz zu den Tagen, der Woche, den Monaten und dem Jahr oder der Retention, die von der Backup-Anwendung festgelegt und von ExaGrid im Retentionsspeicher gespeichert wird.

Die Lösung bietet eine Retentionssperre, allerdings nur für einen einstellbaren Zeitraum, da so die Löschvorgänge verzögert werden. ExaGrid hat sich entschieden, Retention Time-Lock nicht für immer zu implementieren, da die Kosten für die Speicherung nicht zu bewältigen wären. ExaGrid verfügt bereits über die Langzeitspeicherung von Datensicherungen, so dass es überflüssig wäre, einen separaten Speicher mit Retentionssperre zu haben. Mit dem Ansatz des verzögerten Löschens von ExaGrid wird lediglich bis zu 6 % zusätzlicher Speicherplatz benötigt, um die Löschvorgänge zu verzögern. ExaGrid ermöglicht die Verzögerung von Löschungen von 1 bis 30 Tagen.

Wiederherstellungsprozess – 5 einfache Schritte

- Rufen Sie den Wiederherstellungsmodus auf.
    - Die Uhr des Retention-Time-Locks wird angehalten und alle Löschvorgänge auf unbestimmte Zeit unterbrochen, bis die Datenwiederherstellung abgeschlossen ist.
- Wenden Sie sich an den zuständigen ExaGrid-Kundensupporttechniker (Level 2).
    - Der Datensicherungsadministrator kann die Wiederherstellung über die ExaGrid-GUI durchführen. Da dies jedoch kein üblicher Vorgang ist, empfehlen wir, den ExaGrid-Kundensupport zu kontaktieren.
- Bestimmen Sie den Zeitpunkt des Vorgangs, damit Sie die Wiederherstellung planen können.
- Ermitteln Sie, welche Datensicherung auf dem ExaGrid die Deduplizierung vor dem Vorgang abgeschlossen hat.
- Führen Sie die Wiederherstellung mit der Datensicherungsanwendung durch.

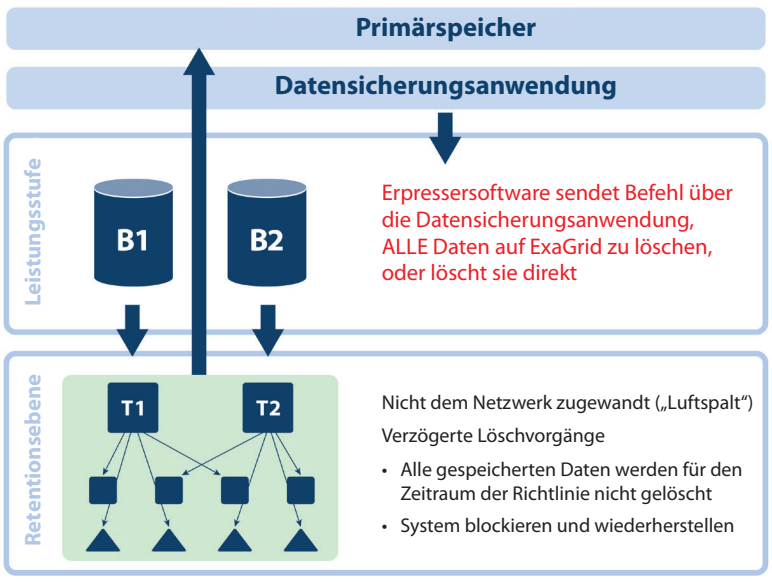
Die Vorteile von ExaGrid im Einzelnen:

- Verwaltung eines einzigen Systems anstelle mehrerer Systeme sowohl für die Datenspeicherung und -sicherung als auch für die Wiederherstellung nach einer Ransomware-Attacke
- Einzigartige zweite Retentionsebene, die nur für die ExaGrid-Software und nicht für das Netzwerk sichtbar ist
- Daten werden nicht gelöscht, da Löschanfragen verzögert werden und somit nach einer Ransomware-Attacke wiederhergestellt werden können
- Wöchentliche, monatliche, jährliche und andere Bereinigungen finden weiterhin statt, um die Speicherkosten im Einklang mit den Retentionszeiten zu halten
- Nur maximal 6 % an zusätzlichem Speicherplatz erforderlich
- Die Menge der gespeicherten Daten wächst nicht ungebremst, sondern bleibt im Rahmen der für die Datensicherung festgelegten Retentionszeit
- Alle gespeicherten Daten bleiben erhalten und werden nicht gelöscht

Beispielszenarien

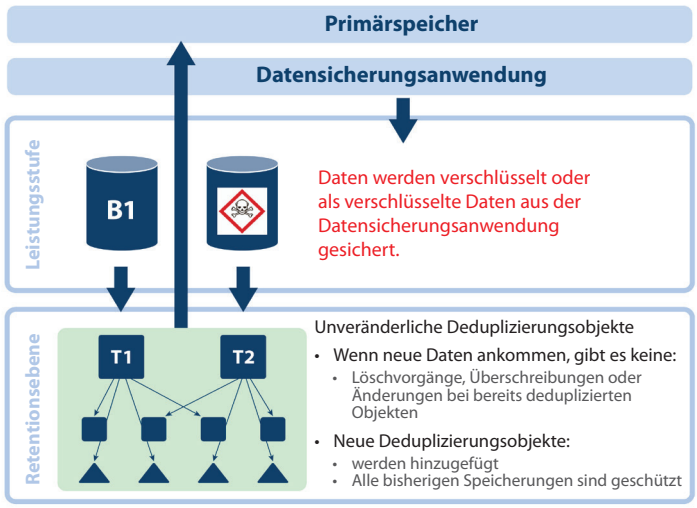
- Daten werden in der Landezone im Festplatten-Cache von ExaGrid über die Datensicherungsanwendung oder durch Hacken des Datenaustauschprotokolls gelöscht. Da für die in der Retentionsebene gelagerten Daten ein verzögerter Time Lock für die Datenlöschung eingestellt ist, bleiben die dort vorhandenen Objekte unangetastet und stehen für die Wiederherstellung bereit. Wenn ein Angriff mit Erpressersoftware eintritt, dann stellen Sie für ExaGrid einfach einen neuen Wiederherstellungsmodus ein und führen die Datenwiederherstellung durch. Die Zeit, die Ihnen zur Verfügung steht, um auf den Angriff mit Erpressersoftware aufmerksam zu werden, entspricht dem im ExaGrid-System eingestellten Time Lock. Nehmen wir einmal an, Sie haben für die Länge des Time Locks 10 Tage angegeben. Dann haben Sie 10 Tage Zeit, um auf die Attacke mit Erpressersoftware aufmerksam zu werden und zum Wiederherstellen der Daten Ihr ExaGrid-System in den neuen Wiederherstellungsmodus zu schalten.

Schutz vor Löschungen von gesicherten Daten auf ExaGrid



- Die Daten werden in der Landezone im Festplatten-Cache von ExaGrid verschlüsselt oder am primären Speicherort verschlüsselt und so in ExaGrid gesichert, dass ExaGrid über verschlüsselte Daten in der Landezone verfügt und diese in der Retentionsebene dedupliziert. Die in der Landezone abgelegten Daten sind verschlüsselt. Da jedoch alle zuvor deduplizierten Objekte unveränderlich sind, können sie zu keinem Zeitpunkt durch neu hinzugekommene verschlüsselte Daten verändert werden. ExaGrid verfügt über alle noch vor dem Angriff mit Erpressersoftware durchgeführten Datensicherungen, und diese können unverzüglich wiederhergestellt werden. Das System kann nicht nur von der letzten deduplizierten Sicherung wiederhergestellt werden, sondern bewahrt auch alle Sicherungsdaten gemäß den Retentionsanforderungen auf.

Schutz vor Löschungen von gesicherten Daten auf ExaGrid



Leistungsmerkmale:

- Alle Löschbefehle werden um die in der Schutzrichtlinie angegebene Anzahl von Tagen verzögert.
- Verschlüsselte Daten, die in ExaGrid geschrieben werden, löschen oder verändern keine vorherigen Sicherungen im Repository.
- Daten in der Landezone, die verschlüsselt sind, löschen oder ändern keine früheren Sicherungen im Repository.
- Stellen Sie die verzögerte Löschung in 1-Tages-Schritten von 0 bis 30 Tagen ein.
- Schützt vor dem Verlust aller aufbewahrten Datensicherungen, einschließlich monatlicher und jährlicher Datensicherungen.
- Die Zwei-Faktor-Authentifizierung (2FA) schützt vor Änderungen an der Time-Lock-Einstellung.
    - Nur Nutzer mit der Rolle „Sicherheitsbeauftragter“ sind berechtigt, Änderungen an der Time-Lock-Einstellung zu genehmigen.
    - 2FA mit Login/Passwort und systemgeneriertem QR-Code schützt alle Konten.
- Separates Passwort für primären Standort und zweiten ExaGrid-Standort.

Vereinigte Staaten 350 Campus Drive / Marlborough, MA 01752 / +1 (800) 868-6985
Vereinigtes Königreich 200 Brook Drive / Green Park, Reading, Berkshire RG2 6UB / +44 (0) 1189 497 051
Singapur 1 Raffles Place, #20-61 / One Raffles Place Tower 2 / 048616 / +65 6808 5574

exagrid.com