LÖSUNGSÜBERSICHT

# Ransomware stoppen mit InfiniGuard® InfiniSafe®

## DIE HERAUSFORDERUNG

Ransomware ist Schadsoftware, die Daten verschlüsselt und so quasi in Geiselhaft nimmt.

In der Vergangenheit konnten Unternehmen mit einem gut funktionierenden Backup-Prozess die eigenen Daten auf den betroffenen Produktionssystemen wiederherstellen. Ransomware-Code wird jedoch immer intelligenter und greift mittlerweile auch häufig Backups an. Angesichts der Tatsache, dass Unternehmen im Durchschnitt alle 11 Sekunden[1] Opfer eines Ransomware-Angriffs werden, genügt der alte Ansatz „Nach einem Angriff stellen wir einfach das Backup wieder her!“ nicht mehr.

Die betroffenen Firmen haben keine guten Auswahlmöglichkeiten. Manche bezahlen das Lösegeld und haben das Glück, den Kodierungsschlüssel zu erhalten. Viele bezahlen, bekommen aber nichts für das Lösegeld. Andere nehmen teure Dienste zur Wiederherstellung der verschlüsselten Daten in Anspruch, und wieder andere müssen massenweise Offline-Bandkassetten hervorkramen – und sich auf einen mühsamen Recovery-Prozess einstellen.

Die Kosten? IDC schätzt, dass Ransomware große Unternehmen allein 20 Milliarden US-Dollar pro Jahr kostet. Diese Zahl steigt aber noch, wenn man auch mittlere und kleine Unternehmen als Ziele von Ransomware berücksichtigt.

### Ransomware heute

In den ersten Monaten des Jahres 2021 meldete der Cybersicherheitsanbieter BlackFog[2] einige schwerwiegende Cyberangriffe: Bei einem Angriff auf den Victor Central School District in New York wurden Daten und Systeme verschlüsselt und Benutzer ausgesperrt. Alle Schulen im Bezirk mussten geschlossen werden. Im März musste der Computerhersteller Acer ein Lösegeld in Höhe von 50 Millionen US-Dollar zahlen, damit die Hacker die erbeuteten vertraulichen Daten nicht veröffentlichen.

Noch nicht so lange her ist der berüchtigte Ransomware-Angriff auf Colonial Pipeline, den Betreiber einer Pipeline, über die 45 Prozent aller an der amerikanischen Ostküste verbrauchten Kraftstoffe laufen. Nach dem Angriff, der einer russischen Hackergruppe zugeschrieben wird, schaltete der Pipelinebetreiber seine Systeme unverzüglich ab, um eine Ausbreitung des Angriffs zu verhindern. Dennoch hatten die Tankstellen in weiten Teilen des Landes Schwierigkeiten, Kraftstoffe zu beschaffen.

Auch kleinere Unternehmen sind betroffen. Das Sicherheitsunternehmen Infrascale schätzt, dass 46 Prozent der kleinen Unternehmen bereits von Ransomware-Angriffen betroffen waren, und 73 Prozent berichteten, dass sie Lösegeld bezahlt hätten.[3] Diese Lösegeldforderungen belaufen sich zwar nicht auf 50 Millionen US-Dollar, aber sie sind teuer und bieten keine Garantie dafür, dass die Hacker ihr wenig glaubhaftes Versprechen halten werden.

## Die wichtigsten Funktionen und Vorteile von InfiniGuard InfiniSafe im Überblick:

- Schnelle Wiederherstellungen auf Unternehmensebene im Petabyte-Bereich
- Schutz des Backups vor Cyberangriffen durch unveränderliche Snapshots, die nicht gelöscht, verschlüsselt oder geändert werden können
- Nachweis der Einhaltung gesetzlicher Vorschriften mit konsolidierten Backups und unveränderlichen Snapshots
- Unterstützung mehrerer gleichzeitiger Backup- und Recovery-Vorgänge ohne Leistungseinbußen
- Validierung der Recovery-Umgebung
- Redundante Deduplizierungsengines in einer active/active/passive Konfiguration zum Schutz von Daten und zur Ausführung von Backup- und Recovery-Vorgängen
- Senkung der Energiekosten und des Verwaltungsaufwands durch Konsolidierung der Datensicherung von bis zu 50 PB*
- Enorme Skalierbarkeit und Multi-Protokoll-Unterstützung für VTL, NFS, CIFS, OST, RMAN und DB/2
- Minimierung von Umsatz- und Reputationsverlusten durch nahezu sofortige und sichere Wiederherstellung von Daten
- Wiederherstellung von Daten ohne Beeinträchtigung der Integrität, und zwar unabhängig von der Ursache: Cyberangriffe, technische Fehlfunktionen, Naturkatastrophen oder menschliches Versagen

[1] Cybersecurity Ventures https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021
[2] BlackFog https://www.blackfog.com/the-state-of-ransomware-in-2021
[3] Infrascale-Umfrage 2020 https://www.infrascale.com/press-release/infrascale-survey-reveals-close-to-half-of-smbs-have-been-ransomware-attack-targets/

INFINIDAT

## Das Backup als letzte Rettung – schön wäre es!

Sie sind auf jeden Fall besser dran, wenn Ihr Backup den Angriff unbeschadet übersteht. Eindringlinge haben jedoch dazugelernt und greifen heute zuerst Backup-Systeme an. Sie schränken Ihre Wiederherstellungsfähigkeiten ein, um ihre eigene Position zu stärken. Traditionelle Backup- und DR-Methoden lassen sich nicht auf Cyber-Recovery anwenden. Deshalb müssen Ihre Pläne die spezifischen Anforderungen an die Cyber-Wiederherstellung berücksichtigen.

Normalerweise erhöhen IT-Teams die Backup-Geschwindigkeit durch synthetische Vollbackups und deduplizierten Backup-Speicher. Eine groß angelegte Recovery im Falle eines Cyberangriffs bedeutet, dass die Daten aus mehreren Generationen von Backups zusammengesetzt werden müssen. Dadurch kommt es zu hochgradigem Random I/O auf dem Backend-Speicher, was wiederum eine langwierige Recovery und möglicherweise gravierende geschäftliche Auswirkungen bedeutet.

## DIE LÖSUNG: InfiniGuard mit InfiniSafe

InfiniSafe ist Bestandteil von Infinidats Backup- und Recovery-Lösung InfiniGuard. InfiniSafe ergänzt die Datenschutzarchitektur von InfiniGuard, die eine nahezu sofortige Wiederherstellung zu einem Bruchteil der Kosten konkurrierender PBBAs ermöglicht. InfiniGuard nutzt unsere Multi-Petabyte-Datenspeicherlösung InfiniBox® als Backend und fügt eine innovative Softwareschicht hinzu, um das Datenlayout für eine schnelle Recovery zu optimieren, ohne die Backup-Geschwindigkeit zu beeinträchtigen.

Die innovative Technologie von InfiniGuard nutzt eine breite DRAM-Schicht (Dynamic Random Access Memory) als primären Cache und eine noch breitere SSD-Schicht (Solid-State-Drives) als sekundären Cache. Ein proprietärer TRIE-Algorithmus (ein Knotenbaum anstelle eines Binärbaums oder eines Hashing-Algorithmus) sagt E/A-Muster voraus und speichert Daten im Voraus , um die Backup- und Wiederherstellungszeit zu beschleunigen.

Anstatt zu versuchen, Daten von mehreren Backup-Appliances, Medientypen und Speicherorten wiederherzustellen, konsolidiert InfiniGuard mehrere Backups in einer einzigen, leicht zu verwaltenden Appliance, die sich auf 2 PB nutzbare Kapazität und bis zu 50 PB* effektive Kapazität skalieren lässt.

## Ein genauerer Blick auf InfiniSafe

Die nativen InfiniSafe-Funktionen von InfiniGuard bringen Sicherheit und Recovery auf die nächste Stufe. InfiniSafe schützt vor den Konsequenzen von Ransomware-Angriffen mit vier grundlegenden Technologien, die zentral für eine Cyber-Recovery-Lösung sind:

**1. Unveränderliche Snapshots**

Unveränderliche Snapshots können nicht gelöscht oder bearbeitet werden. Der fachkundige Support von Infinidat arbeitet mit Ihnen

**InfiniGuard mit InfiniSafe sorgt durch die unveränderlichen Snapshots von Infinidat für den Schutz Ihres gesamten Backup-Speichers. Jede Deduplizierungsengine (DDE) kann einzeln zu einem bestimmten Zeitpunkt wiederhergestellt werden. InfiniSafe oder Discovery-Tests können auch in einer Standby-Umgebung aktiviert werden.**


INFINIDAT

zusammen, um Ihre System-Snapshots so zu konfigurieren, dass sie optimal auf Ihre Cybersicherheitsbedürfnisse abgestimmt sind, einschließlich Aufbewahrungseinstellungen, Zeitpläne und entsprechende Richtlinien. Es kann nicht passieren, dass ein Hacker oder ein unerfahrener IT-Mitarbeiter diese Einstellungen ändert oder einen vorhandenen unveränderlichen Snapshot löscht.

**2. Logischer Schutz mit Air-Gap-Isolation**

Die zu schützenden Daten von anderen Bereichen des Systems zu isolieren, ist von entscheidender Bedeutung. Mit anderen Lösungen müssen Daten in ein separates System kopiert oder repliziert werden, was die Kosten und Komplexität erhöht. Die InfiniSafe-Technologie führt diesen Schritt lokal aus und spart so Kosten und Aufwand.

**3. Abgeschirmtes forensisches Netzwerk**

Ein vollständig privates Netzwerk dient zur Validierung und Wiederherstellung von Daten.

**4. Nahezu sofortiges Recovery**

Für die Wiederherstellung nach einem Angriff ist es unerlässlich, Daten so schnell wie möglich verfügbar zu machen. InfiniSafe gibt Ihnen all Ihre nachweislich vertrauenswürdigen und validierten Daten zurück und macht sie innerhalb von Minuten für die Wiederherstellung verfügbar, unabhängig von der Größe des Repositorys. Selbst im Petabyte-Bereich müssen Sie keine Abstriche bei der Zeit machen.

Die Recovery muss systematisch, schnell und überprüfbar sowie von jedem beliebigen Punkt in der Datenhistorie aus nahezu sofort möglich sein. Eine benutzerfreundliche, isolierte Testumgebung ermöglicht es Unternehmen, Daten vor der Wiederherstellung der Betriebsumgebung zu überprüfen. Zudem unterstützt diese Umgebung Routinevalidierungen von sicheren Backups, ohne den täglichen Backup-Betrieb zu unterbrechen – und zwar ohne Sekundärsysteme und ohne Datenverschiebung.

## ZUSAMMENFASSUNG

Cyberangriffe sind eine echte und zunehmende Gefahr, und Unternehmen sollten die potenziell schmerzhaften Folgen nicht unterschätzen. Es ist bestens bekannt, dass Ihre Backup-Umgebung besonders anfällig für Cyberangriffe ist. Ihre Fähigkeit, effektiv zu reagieren, wird reduziert, und Angreifer verschaffen sich eine gute Verhandlungsposition. Seien Sie klüger. Implementieren Sie InfiniGuard mit InfiniSafe, um sich vor einer Vielzahl von Bedrohungen zu schützen – von Cyberangriffen, technischen Ausfällen und Naturkatastrophen bis hin zu reinem menschlichen Versagen. InfiniGuard mit InfiniSafe gibt Ihnen die Sicherheit, die Sie benötigen, um Ihre Daten schnell wiederherzustellen und Ihren Geschäftsbetrieb rasch wieder aufzunehmen.


** Effektive Kapazität. Tatsächliche Ergebnisse können abweichen.*

dach@INFINIDAT.com