arcserve®

REPORT

Reaktionen auf Ausfallzeiten: **Fünf „Gewusst-wie“-Schlüsselstrategien**

Reaktionen auf Ausfallzeiten: Fünf „Gewusst-wie“-Schlüsselstrategien

Die Welt der Datensicherung entwickelt sich stetig weiter, da Organisationen immer wieder den „perfekten Sturm“ an Herausforderungen überstehen müssen, der ihre IT-Infrastrukturen bedroht. Dieser „Sturm“ beeinträchtigt die Möglichkeit von IT-Abteilungen, Arbeitsabläufe effizient durchzuführen, und bringt wirtschaftlich denkende Entscheidungsträger in Dilemmata beim Ausarbeiten von Budgets. Kein Wunder, dass viele IT-Führungskräfte durch eine lange Liste von Sorgen nachts um ihren Schlaf gebracht werden:

- Unendliches Wachstum von strukturierten und unstrukturierten Datenmengen
- Explosion der Anzahl an Angriffen durch Schadsoftware/Erpressungstrojaner
- Gestiegene Notwendigkeit, Vorbild zu sein hinsichtlich Regeleinhaltung und Datenverantwortung
- Uneinheitliche Infrastrukturen zur Datensicherung bei einer immer größer werdenden Anzahl von Endanwendern
- Zunehmende Komplexität aufgrund des Zusammenspiels lose integrierter Lösungen
- Kontrollverlust bei Schlüsselmerkmalen wie RPOs und RTOs
- Die Masse an Virtualisierungsmöglichkeiten und die Wichtigkeit von Cloud-basierten Speicherstrukturen

Um diesen Herausforderungen zu begegnen, legen viele Organisationen die Last der Verwaltung komplexer IT-Lösungen auf den Schultern von IT-Generalisten ab – von denen viele die Aufgabe haben, weniger komplexe und kostengünstigere Lösungen zu finden für den Schutz und die Verwaltung von und den Zugang zu kritischen Daten. Aus diesem Grund sollten Organisationen fünf Schlüsselstrategien durchdenken, welche das Alles-oder-Nichts bedeuten bezüglich der Fähigkeit, angemessen auf Ausfallzeiten zu reagieren.

1 | **Risikomanagement:** Versicherungsstrategie trifft auf Datensicherung

Die meisten Organisationen sind verpflichtet (oder zumindest sehr dazu angehalten), einen Notfallplan oder Datenrettungsmaßnahmen zur Hand zu haben. Viele dieser Pläne stammen jedoch aus einem anderen Zeitalter der Datenverarbeitung, und haben daher keinerlei Bezug zu Rentabilität und tatsächlichen Kostenersparnissen, welche IT-Entscheidungsträger der freien Wirtschaft heutzutage beim Ausarbeiten von Budgetplänen berücksichtigen müssen. Hier trifft Versicherungsstrategie auf Datensicherung.

Heute müssen Organisationen in der Lage sein, auf kritische Daten zugreifen zu können – wann und wo auch immer dies notwendig ist. Jedes Mal, wenn eine IT-Führungskraft die Anpassungsfähigkeit seiner

IT-Infrastruktur verbessert, verzeichnet dessen Firma Kostenersparnisse, eine signifikante Reduzierung bezüglich Risiko/Verlust, und verbessert ihre operative Effizienz. Der Grund dafür ist in den wirtschaftlichen Gegebenheiten von Datensicherung und Datenrettung zu finden, oder genauer, in den Kosten von Anwendungen und Datenverfügbarkeit, die durch direkte und indirekte Kosten beziffert werden können, wie etwa Einfluss auf die Reputation, Verlust an Kunden oder deren Fähigkeit, Einkäufe zu tätigen, was beim Auftreten regulativer Situationen und bei der Produktivität von Mitarbeitern negativ zu Buche schlägt. Durch eine eher versicherungstechnische Herangehensweise an Daten- und Systemverfügbarkeit kann man Folgendes bestimmen:

- Den zu erwartenden Verlust basierend auf statistischer Wahrscheinlichkeit
- Wie Naturkatastrophen aktuelle Ressourcen beeinflussen ebenso wie die Kosten, die Dinge wieder zum Laufen zu bringen
- Das Risiko der Systembeeinträchtigung durch Schadsoftware/Erpressungstrojaner, sowie Kosten und Dauer, Daten wiederherzustellen durch das Zahlen oder Nicht-Zahlen von Lösegeld
- Inwieweit das Geschäft in der Lage wäre, seine Produkte und/oder Dienstleistungen zur Verfügung zu stellen, und welche Prozesse nötig wären, um sicherzustellen, dass die Produktivität von Mitarbeitern nicht sinkt oder das Umsatzvolumen nicht beeinträchtigt wird
- Die monetäre Auswirkung, wenn ein POS oder eine E-Commerce-Webseite für fünf Minuten, fünfzehn Minuten oder länger nicht zugänglich wäre. Abhängig vom jeweiligen Geschäftsmodell, könnte der Verlust der Möglichkeit zur Durchführung von Transaktionen für mehr als wenige Sekunden einen massiven Geschäftsverlust bedeuten

Dieser versicherungstechnische, oder eher wirtschaftlicher ausgerichtete Ansatz hinsichtlich Sicherung und Wiederherstellung, erlaubt es einer Organisation, ein Modell zu erstellen, welches die Risiken und Kosten durch zu erwartenden, nicht beabsichtigten Datenverlust mit reellen Zahlen beziffert. Dadurch kann eine Firma ihre kritischsten und schwächsten Bereiche effizienter priorisieren und ihre Investitionen entsprechend planen.

2 Systemverfügbarkeit: Nicht alle Daten werden auf die gleiche Weise erstellt

Es ist allgemein bekannt, dass die meisten, wenn nicht alle, Arten von Geschäftsmodellen ohne E-Mail oder kritische Transaktionsanwendungen nicht funktionieren würden – vor allem diejenigen, die ein Business im wahrsten Sinne des Wortes am Laufen halten oder ihren Kunden die Möglichkeit bieten, Produkte und/oder Dienstleistungen zu erwerben. Man muss auch kein Einstein sein, um zu verstehen, dass der Schutz dieser Systeme und Daten der Schlüssel dazu ist, ungeplante Ausfallzeiten zu überstehen. Vor diesem Hintergrund steckt viel mehr drin, als man auf den ersten Blick sehen kann, wenn man bedenkt, dass diese Systeme und Anwendungen fast immer miteinander verknüpft sind – mehr oder weniger effizient – und unterschiedlich kritische Grade aufweisen. Bei der Überprüfung ihrer aktuellen und künftigen Strategien zur Verfügbarkeit ist es für Führungskräfte wichtig, einige Schlüsselbereiche zu berücksichtigen:

- Die Kritikalität von Anwendungen: Wenn es darauf ankommt, sollte die eigentliche Frage lauten: „Wie schnell muss man an bestimmte Daten rankommen?“ Marketingbroschüren und interne Datenaustausch-Anwendungen können normalerweise eine Ausfallzeit von einigen Stunden verkraften, wohingegen Transaktionssysteme oft auftragsentscheidend sind und innerhalb von Sekunden verfügbar sein müssen. Die finanzielle Auswirkung, die bestimmte Systeme haben, kann mittels des weiter oben beschriebenen Risikomanagement-Ansatzes beziffert werden
- Gegenseitige Abhängigkeit von Anwendungen und Systemen: Normalerweise sind die meisten Anwendungen eingebettet oder integriert in eine Wertschöpfungskette oder einen Arbeitsablauf, z.B. EDI-Aufträge, welche eine komplette Lieferkette anstoßen. Zu dieser Komplexität gesellt sich die Tatsache, dass diese Anwendungen üblicherweise in einem abgegrenzten Bereich verwaltet werden, mit negativer Auswirkung auf deren Leistung und die Fähigkeit, die gesamte Infrastruktur zu erfassen. Wie würde sich der Ausfall eines Systems auf die jeweils anderen auswirken? Den Grad dieser Interdependenzen innerhalb einer Organisation und deren Auswirkungen auf das gesamte IT-Ökosystem zu verstehen ist wichtig
- Wartungspläne und Verfügbarkeit: Jede Anwendung hat ihre jeweils eigenen Wartungspläne und Dienstgütenotwendigkeiten. Darauf basierend ist es wichtig, zu bestimmen, wie schnell bestimmte auftragskritische Daten verfügbar sein müssen. Viele Lösungen sind mehr oder weniger „von der Stange“, benötigen umfangreiche Erweiterungen auf anderen Gebieten oder das Hinzufügen zusätzlicher Einzellösungen, wenn das Geschäft wächst. Behalten Sie das im Kopf, wenn es um Vorhersagen künftiger Abhängigkeiten oder Änderungen bei der Infrastruktur geht

Durch das Berücksichtigen dieser Schlüsselbereiche kann man den Datenverfügbarkeitsindex bestimmen sowieso potentielle Lücken im Arbeitsablauf oder in der Wertschöpfungskette bei Anwendungen, die das Geschäft am Laufen halten, erkennen – und entsprechend handeln.

3 Komplexität: Mehr Prozesse, mehr Probleme

Die weiter oben genannten Punkte bezüglich der Datenverfügbarkeit haben die wahren Schuldigen für das Nicht-Ausschöpfen einer effizienten Geschäftskontinuität benannt: Die Komplexität der IT-Infrastruktur und, um genauer zu sein, die Lösungen zur Datensicherung. Die Herausforderung, und folglich das Hauptziel, ist das Erreichen eines bestimmten Grades an Vorhersagbarkeit und die Konstanz von Datenwiederherstellung, ganz gleich um welche Art der Unterbrechung es geht, die unweigerlich jede Infrastruktur treffen wird. IT-Führungskräfte und Unternehmensleiter sollten diese Herausforderung aus einer Netto-Ergebnis-Perspektive heraus angehen: Die Berücksichtigung tatsächlicher RPOs und RTOs sowieso das Festlegen von Maßnahmen, um das Geschäft wieder auf die Beine zu bekommen innerhalb eines Zeitrahmens, der den geschäftlichen Notwendigkeiten entspricht. Dies bedeutet insbesondere das Orchestrieren von Maßnahmen zur Wiederherstellung oder Ausfallsicherung kritischer Systeme auf eine Art und Weise, welche vorhersagbare Ergebnisse hervorbringt.

Leider ist dies fast unmöglich, wenn eine Firma mehrere Sicherungslösungen oder diskrete Prozesse nutzt, welche nicht gut miteinander im Einklang funktionieren. Das Vereinheitlichen der Datensicherung, Datenwiederherstellung und der Infrastruktur der Verfügbarkeit, sei es vor Ort oder durch Zuhilfenahme von Cloud-Lösungen, ist der einzige Weg, um Pläne zu testen und eine effiziente Ausführung im Falle einer ungeplanten Unterbrechung zu garantieren. Zu guter Letzt lässt sich festhalten, dass, je geringer der Grad an Komplexität von Sicherungs- und Wiederherstellungsprozessen ist, desto mehr Kontrolle hat man über RPOs und RTOs.

4 Erpressungstrojaner: Kein Sicherheitsproblem, sondern ein Problem der Datenwiederherstellung

Laut „Internet Crime Complaint Center" haben Erpressungstrojaner US-Organisationen allein im letzten Jahr 24 Million Dollar[1] gekostet , und Berichten des US-Justizministeriums zufolge haben Angriffe durch Erpressungstrojaner im Jahr 2016[2] um 300 % zugenommen . Diese statistischen Daten unterstreichen ein wachsendes Problem, welches Unternehmen jeder Größe betrifft; eines, das Unternehmensleiter nicht ignorieren können, und was unweigerlich die jeweiligen IT-Abteilungen zur Lösung vorgesetzt bekommen werden.

Anders als andere ungeplante Unterbrechungen des Flusses von logischen Daten, kann ein Angriff durch Erpressungstrojaner auch einen sehr hohen Einfluss auf den Ruf eines Unternehmens haben. Der jüngste Vorfall bei Delta Air Lines illustriert nicht nur die hohen Kosten durch Erpressungstrojaner, sondern auch die Auswirkungen auf das Kundenvertrauen – was oft den größten Schaden darstellt.

Die beste Strategie zur Verringerung des Schadens durch Erpressungstrojaner ist, proaktiv statt reaktiv zu handeln. Lässt man einer Organisation die Möglichkeit, eigene Entscheidungen zu treffen, vermeidet man die Notwendigkeit, mit Hackern verhandeln zu müssen, sollte ein Erpressungstrojaner sich einmal ausgebreitet und geschäftskritische Daten infiziert haben. Eine äußerst effiziente Möglichkeit, dies zu erreichen, ist das Implementieren und regelmäßige Testen einer robusten Wiederherstellungslösung mit herkömmlichen und Cloud-basierten Optionen, welche die Möglichkeit bieten, „die Zeit zurückzudrehen" und geschäftssensible Daten wiederherzustellen – ohne Lösegeld.

In vielerlei Hinsicht ist der Angriff durch Erpressungstrojaner die größte Bedrohung, der Organisationen heutzutage ausgesetzt sind; jedoch bietet sich Business-Unternehmen dadurch Eines: die Möglichkeit, Geschäftskontinuität und Notfallstrategien neu durchzudenken und so sicherzustellen, dass kein Bereich übersehen wird. Durch die Kombination von solider Bedrohungsaufspürung und Schadsoftware-Eliminierung mit Hilfe eines robusten Datenverfügbarkeitsplan, sind Organisationen für das Überstehen eines Angriffs durch Erpressungstrojaner gut gerüstet, und damit für den Rattenschwanz an negativen Folgen, den ein solcher Angriff haben kann.

[1] http://finance.yahoo.com/news/victims-paid-more-24-million-222700088.html

[2] https://www.justice.gov/criminal-ccips/file/872771/download

5 Das Nutzen der Cloud: Wie und wann es für Ihre Infrastruktur sinnvoll ist

Viel ist geschrieben worden über das Nutzen von Cloud-Dienstleistungen zur Ergänzung oder sogar zum Ersetzen von herkömmlichen Sicherungs- und Wiederherstellungs-Infrastrukturen, allerdings sind viele Dinge zu berücksichtigen, wenn es darum geht, wie und wann man die Einführung einer Cloud-Komponente in Betracht zieht. Unter anderem sollten IT-Entscheider und Unternehmensleiter Folgendes berücksichtigen:

- Die tatsächliche Art des Dienstes, sei es „Backup as a Service“ (BaaS), „Disaster Recovery as a Service“ (DRaaS) oder das Aufbewahren von Daten bzw. Auslagern von Arbeitsabläufen
- Die Art und Weise des Wechsels von einer vor Ort-Lösung für Geschäftskontinuität/Notfallplan hin zu einer hybrideren Infrastruktur, inklusive der Art der Cloud-Sicherung (Festplatte, Band oder eine Kombination aus Beidem), falls eine Archivierung nötig ist, die Mechaniken zur Datenaufnahme –und Wiederherstellung (wie man Daten in die Cloud und wieder zurück bringt), und Kostenflexibilität

Wichtiger ist jedoch, diese Überlegungen im Kontext der Notwendigkeiten der ursprünglich festgelegten RPOs und RTOs anzustellen. Zusätzlicher Diskussionsstoff betreffen die Einrichtungen und den Ort des Anbieters, welche gut durchdacht sein wollen bezüglich der Einhaltung von Regeln und des Auswirkungsbereichs eines möglichen Notfalls (zum Beispiel gilt es als „best practice“, auf Datensicherungs- und Ausfallsysteme „außerhalb der eigenen Region“ zugreifen zu können).

Schlussüberlegungen

Die meisten Organisationen sind sich der Dringlichkeit des Aufrechterhaltens von anpassbaren Systemen und der Garantie von Datenverfügbarkeit angesichts sich ständig weiter entwickelnder Bedrohungen bewusst. Grundsätzlich kommt es darauf an, eine Lösung für eine komplexe Überlegung zu finden: Welchen Gütegrad benötige ich vom Standpunkt von aktuell gültigen RPOs und RTOs aus, und welche Investitionen sollte ich zum Erreichen dieser Ergebnisse und zur Maximierung der Rentabilität tätigen.

Organisationen, welche Strategien rund um Risikominimierung, proaktiver Reaktion auf Erpressersoftware, Datenverfügbarkeit für System-Ökosphären, Prozessvereinfachung und der Rolle der Cloud einsetzen, sind für jegliche Geschäftserfordernisse gut aufgestellt. Während der „perfekte Sturm“, der viele IT-Infrastrukturen trifft, sicher besorgniserregend ist, so stellt er auch eine Möglichkeit dar, auf höherer Management-Ebene sinnvolle Überlegungen bezüglich Geschäftskontinuität und Notfallplan anzustellen; und die Diskussion über Datenverlust zu nutzen, um sich tatsächlich dessen gewahr zu sein, dass man nicht nur ein IT-Unternehmen ist, sondern auch ein Geschäftsunternehmen.