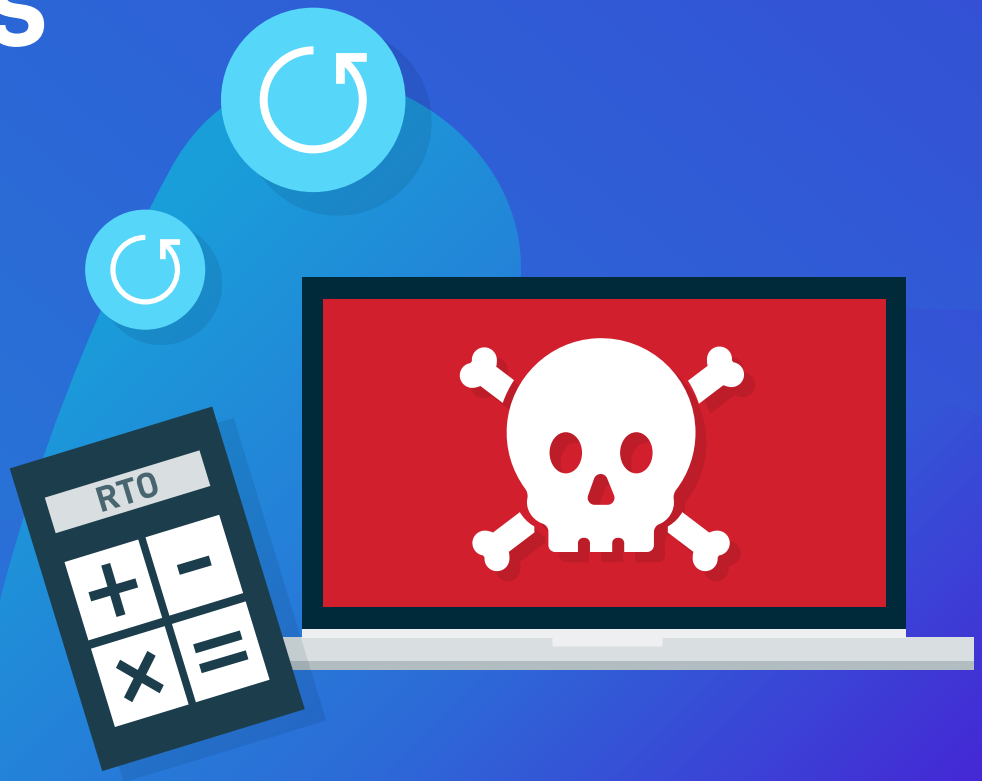
E-Book

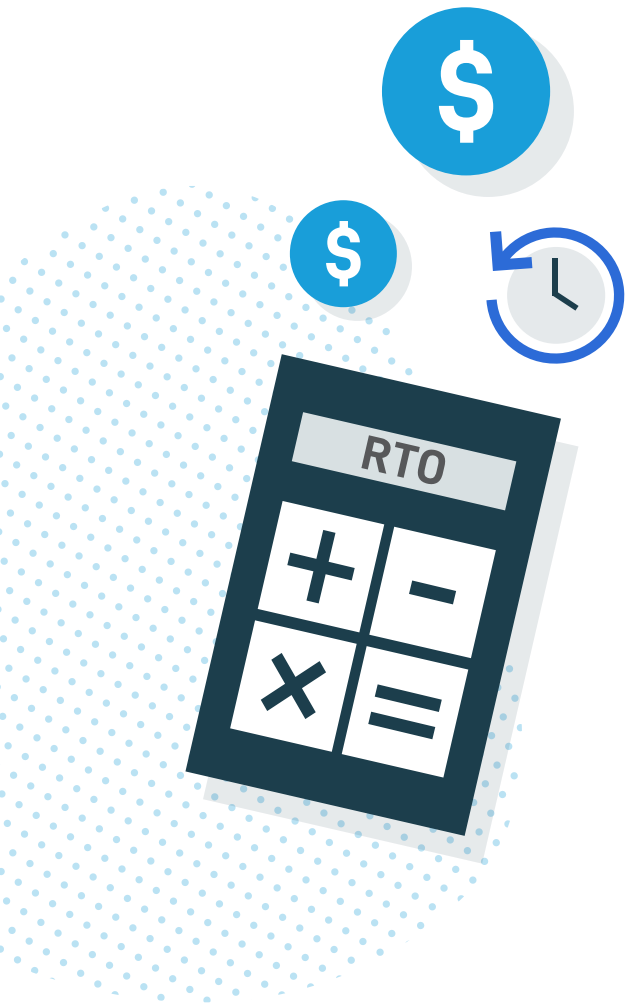
4 Gründe, warum CEOs sich mit dem Thema Business Continuity und Disaster Recovery beschäftigen sollten



Einführung

Man wird nicht CEO, wenn man nicht bereit ist, auch manchmal Risiken einzugehen. Es gibt jedoch einen Unterschied zwischen dem Eingehen von Risiken, um einen möglichst großen Erfolg zu erzielen und dem Eingehen unnötiger, vermeidbarer Risiken. In einer Zeit, in der ein großer Teil des Geschäfts von Daten und Computern abhängt, legt ein proaktiver CEO Wert auf einen soliden Business Continuity und Disaster Recovery (BCDR) Plan. Denn warum sollte ein Unternehmenschef die Schäden riskieren, die dadurch entstehen können, dass es nach einem Systemausfall, der Zerstörung einer Anlage, einem Ransomware-Angriff oder dem Verlust wichtiger Daten nicht gelingt, schnell wieder in den Normalbetrieb zurückzukehren?

Leider haben noch nicht alle die Notwendigkeit eines BCDR-Plans erkannt. Damit Sie eine solche Investition rechtfertigen können, finden Sie nachfolgend vier wichtige Gründe, warum Ihnen als CEO das Thema Business Continuity und Disaster Recovery am Herzen liegen sollte.



1. Weil Ausfallzeiten teuer sind

Wenn Ihre Mitarbeiter nicht mehr auf geschäftskritische Anwendungen und Daten zugreifen können, schlägt sich das unmittelbar auf die Produktivität und den Umsatz durch. Auch wenn das wie eine Selbstverständlichkeit klingt, berücksichtigen viele Unternehmen nicht die Gesamtkosten, die ihnen durch Ausfallzeiten entstehen. Um besser zu verstehen, wie sich die Schäden summieren, sollten Sie sich das folgende Beispiel ansehen, das mit Dattos Kostenrechner für Wiederherstellungszeiten und Ausfallzeitkosten erstellt wurde.

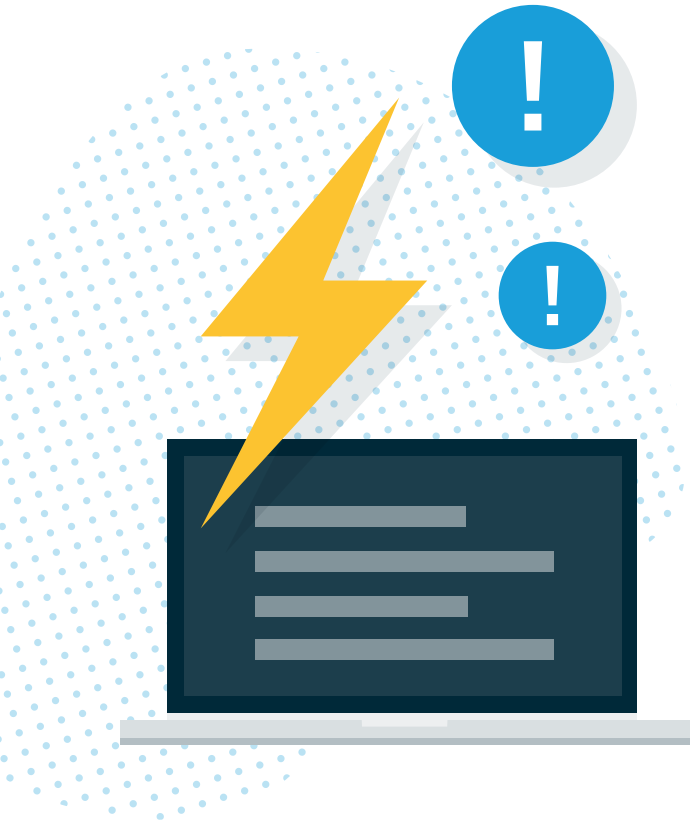
Nehmen wir an, Ihr Unternehmen hat 100 Mitarbeiter und Mitarbeiterinnen, der durchschnittliche Ertrag pro Stunde beträgt 1.500 EUR und der Backup-Datensatz hat 2 TB. Bei diesen Parametern würde ein vollständiges lokales Backup mehr als 8 Stunden dauern. Die damit verbundenen Kosten für Ausfallzeiten würden sich auf Ertragsausfälle in Höhe von 34.000 EUR belaufen.

Moderne BCDR-Produkte können schnell eine virtuelle Instanz einer Anwendung und all ihrer Daten auf einem virtuellen Server, der innerhalb der Backup-Umgebung gehostet ist, starten. Dadurch können Benutzer den Betrieb fortsetzen, während die primären Anwendungsserver wiederhergestellt werden. Daher ist die Wahl einer BCDR-Lösung, durch die die Ausfallzeiten minimiert werden, aus geschäftlicher Sicht sinnvoll.

2. Backups alleine reichen nicht aus

Backup und Business Continuity sind nicht das Gleiche.

Man tut sich schwer, heutzutage noch ein Unternehmen zu finden, das nicht irgendeine Form der Datensicherung durchführt. Was aber passiert, wenn eine Überschwemmung Ihre Primär- und Backup-Server außer Gefecht setzt? Sie müssen sicher sein können, dass die Systeme, von denen Ihr Unternehmen abhängig ist, weiter funktionieren, egal was passiert.



Das Aufbewahren einer Datenkopie zur Wiederherstellung im Katastrophenfall an einem externen Ort, ist eine Möglichkeit, sicherzustellen, dass der Betrieb aufrecht erhalten werden kann. Früher bedeutete dies, dass Bänder an einen anderen Standort oder in einen externen Tresor transportiert wurden. Heute können BCDR-Lösungen Anwendungen von den Backup-Instanzen virtueller Server ausführen. Die besten Lösungen arbeiten aus der Cloud, ein Ansatz, der als Disaster Recovery as a Service (DRaaS) bezeichnet wird.

Die Möglichkeit, Anwendungen in der Cloud auszuführen, während die Infrastruktur vor Ort wiederhergestellt wird, bedeutet eine grundlegende Veränderung für die Disaster Recovery. Als CEO sind Sie bestrebt, die modernsten Technologien im Einsatz zu haben.

3. Katastrophen sind sehr unterschiedlich.

Nicht jede Katastrophe schafft es in die Schlagzeilen. Die meisten IT-Ausfallzeiten sind die Folge von gewöhnlicher Datenlöschung – versehentlich oder böswillig –, Schäden an der Computerhardware oder nachlässigem Umgang mit der Sicherheit. So hat beispielsweise eine kürzlich veröffentlichte Umfrage von OWI Labs ergeben, dass 81 % der Befragten trotz Sicherheitsrisiken gelegentlich oder regelmäßig ein öffentliches WLAN nutzen. Ein Ransomware-Angriff oder ein Virus kann einen Betrieb genauso leicht zum Erliegen bringen wie ein starker Sturm oder ein Stromausfall. Diese Vorfälle sind normalerweise auf menschliches Versagen zurückzuführen und damit nicht zu verhindern.

Daher ist das Vorhandensein einer Technologie, die es Ihrem Unternehmen ermöglicht, den Betrieb nach solchen auf menschliches Versagen zurückzuführenden Katastrophen aufrecht zu erhalten, mindestens genauso wichtig, wie der Schutz vor einem Sturm, von dem nicht klar ist, ob er Ihr Unternehmen jemals treffen wird.

4. Resilienz ist wichtig

Den Zugriff auf Anwendungen und Daten nach einer Katastrophe sicherzustellen ist nur ein Teil von BCDR. Zu prüfen, inwieweit Ihr Unternehmen in der Lage wäre, den IT-Betrieb wiederherzustellen, kann ein guter Ausgangspunkt für unternehmensweite Business-Continuity-Anstrengungen sein. Eine gute BCDR-Planung sollte jedoch das Unternehmen als Ganzes betrachten, und das Ziel sollte sein, neben der Cyber- auch die Business-Resilienz zu entwickeln. Viele BCDR-Planungen beginnen daher mit der Durchführung einer Business-Impact-Analyse oder einer Risikobewertung. Diese Untersuchungen können Schwachstellen Ihres Unternehmens bei der Fähigkeit, den Betrieb aufrecht zu erhalten, aufdecken, die weit über die IT hinausgehen.

Ihnen ist bewusst, dass Ihr Unternehmen früher oder später von einer Natur- oder anderen Katastrophe betroffen sein kann. Wenn das passiert, möchten Sie so gut wie möglich vorbereitet sein.

Fazit

Business Continuity und Disaster Recovery ist eine unternehmensweite Verantwortung. Wenn Sie Ihr Unternehmen nicht vor menschlichem Versagen, Hardwareausfällen und/ oder Naturkatastrophen schützen, kann das nachteilig sein und sich auf alle Beteiligten auswirken. Wenn Sie erst einmal einen robusten BCDR-Plan eingeführt haben, wissen Sie, dass Sie auf jede Katastrophe, die Sie treffen könnte, gut vorbereitet sind.

Wir können Ihnen helfen, diese Sicherheit zu bekommen. Wenn Sie mit Datto zusammenarbeiten, garantieren wir vollständige Ransomware-freie Backups und eine schnelle Datenwiederherstellung. Die Datto-Cloud steht immer zur Verfügung, daher ist es immer möglich, eine saubere Kopie einer Datei, E-Mail oder eines ganzen Servers wiederherzustellen. Die Backups sind gegen Ransomware, Beschädigung von Daten und versehentliches oder böswilliges Löschen von Dateien oder E-Mails geschützt.

Möchten Sie mehr erfahren? Nehmen Sie noch heute Kontakt mit uns auf.

MarketNow

Datto MarketNow | Phone: +1.888.294.6312 | Email: marketnow@datto.com |
Datto Inc. | https://www.datto.com