HISCOX
WISSEN VERSICHERT.

Backups – elementar wichtig

Wenn ein Unternehmen eine regelmäßige Datensicherung macht, klingt das erst mal super, oder? So kann im Falle eines Ransomware-Angriffs schnell alles wiederhergestellt werden. Nicht so schnell! In der Praxis gibt es hier oft Probleme.

Sehr häufig enden Ransomware-Angriffe damit, dass Backups verschlüsselt werden. Nachfolgend erhalten Sie einen Überblick darüber, was beim Aufsetzen von Backups – je nach Unternehmensgröße – entscheidend ist.

KLEINERE UNTERNEHMEN

Das Ideal...

In kleineren Unternehmen sollte das Backup getrennt vom restlichen System gespeichert werden – zum Beispiel auf einem externen Festplattenlaufwerk. Solange das Backup zum Zeitpunkt des Angriffs physisch vom restlichen System getrennt ist, ist es vor Verschlüsselungen geschützt.

Die Auslagerung von Daten in die „Wolke" ist nicht so sicher, wie man denkt

Die heutigen Ransomware-Versionen sind sehr gut darin, sich Zugang zu cloudbasierten Backups zu verschaffen und diese auch zu verschlüsseln. Generell sollten Sie bedenken, dass ein Backup, wenn es mit dem Hauptsystem verbunden ist (wie es bei der Cloud der Fall ist), mit angreifbar ist und somit auch verschlüsselt werden kann.

Bei einigen cloudbasierten Backup-Produkten werden mehrere Dateiversionen gespeichert. Wenn also die verschlüsselten Dateiversionen nach einem Angriff automatisch mit der Cloud synchronisiert werden, kann der Kunde die vorherigen unverschlüsselten Dateiversionen theoretisch wiederherstellen.

Allerdings haben Hacker dies erkannt und damit begonnen, Ransomware-Varianten zu entwickeln, die die zuvor gespeicherten Dateiversionen löschen. Fazit: Das einzig effektive Backup ist ein vom System getrenntes Backup.

GRÖSSERE UNTERNEHMEN

Größere Unternehmen sollten über mehrere Backups verfügen. Generell gilt die **Backup-Regel 3–2–1**: Unternehmen sollten drei Backups auf zwei verschiedenen Speichermedien haben, wovon eins immer vom restlichen System getrennt ist.

Ein Beispiel:

Ein Unternehmen nutzt ein primäres Rechenzentrum in Berlin, in dem die meisten der kritischen Daten und Systeme gehostet sind. In Abständen von 15 Minuten wird ein automatisches Backup der Daten in einem weiteren Rechenzentrum in Hamburg erstellt. In beiden Rechenzentren wird ein klassisches Festplattenlaufwerk als Speichermedium verwendet.

Wenn das Rechenzentrum in Berlin ausfällt, erfolgt die Umschaltung auf das Rechenzentrum in Hamburg, sodass maximal 15 Minuten an Daten verloren gehen.

HISCOX
WISSEN VERSICHERT.

GRÖSSERE UNTERNEHMEN

Aktiv/Aktiv-Systeme vs. Aktiv/Passiv-Systeme

Das Setup unseres Beispiels wird als Aktiv/Aktiv-System bezeichnet, da beide Rechenzentren ständig verbunden und in Betrieb sind. Aktiv/Aktiv-Systeme vermindern äußerst wirksam das Risiko von Systemversagen, insbesondere bei Unternehmen, deren Umsatzgenerierung stark von der Systembetriebszeit abhängig ist.

Allerdings sind sie bei Ransomware-Angriffen wirkungslos. Wenn in unserem Beispiel das Rechenzentrum in Berlin durch einen Ransomware-Angriff lahmgelegt werden würde, würde innerhalb von 15 Minuten ganz einfach eine Umschaltung auf das Rechenzentrum in Hamburg erfolgen. Daher ist es wichtig, auch über Offline- (oder Aktiv/Passiv-)Systeme zu verfügen. Bezogen auf die Backup-Strategie bedeutet dies, dass das Backup nicht mit dem Hauptnetzwerk verbunden und somit vor Ransomware geschützt ist.

In unserem Beispiel erfolgt dies mit mehreren Backup-Bändern. Dies mag archaisch erscheinen, aber Bandlaufwerke sind noch oft beliebt, da sie relativ kostengünstig und wartungsfreundlich sind.

Täglich wird ein Backup-Band der neuen oder geänderten Dateien erstellt. Diese werden vor Ort und nur für die betreffende Woche aufbewahrt. Samstags z.B. wird dann jeweils eine wöchentliche Vollsicherung erstellt. Diese Bänder werden einen Monat vor Ort aufbewahrt. Am Monatsende wird ein weiteres Backup-Band erstellt, das extern für die Ewigkeit aufbewahrt wird. Dies bedeutet, dass Daten von jedem Tag des vergangenen Monats sowie Daten eines jeden Monats der mindestens letzten 10 Jahre wiederhergestellt werden können.

Die Wichtigkeit externer Backups - ein Beispiel

Ein Unternehmen der Digitalwirtschaft wurde Opfer eines Hacker-Angriffs: Ein Insider, vermutlich ein ehemaliger IT-Administrator, der entlassen wurde, hatte sich Zugang zum System verschafft und konnte so alle Daten, inkl. der Backups löschen und mehrfach überschreiben. Hätte das Unternehmen zusätzlich Backups extern (idealerweise an einem anderen Standort) gespeichert oder aufbewahrt, wäre der Schaden deutlich geringer ausgefallen.

Übung macht den Meister

Backups richtig erstellen ist schwer. In der Regel lässt sich nur durch Wiederherstellungstests herausfinden, ob Backups auch wirklich funktionieren. In der Praxis sehen wir, dass ungeprüfte Backup-Lösungen oft nicht so funktionieren, wie erwartet. Darüber hinaus lernt das interne IT-Team durch die Prüfung von Backups, wie der Betrieb im Falle eines Angriffs schneller aus einem Backup wiederhergestellt werden kann.

Aktiv/Aktiv

(Online)-Systeme schützen wirksam vor Hardware-Ausfällen, bieten aber nur wenig Schutz vor Datenkorruption (z. B. Ransomware).

Aktiv/Passiv

(Offline)-Systeme schützen wirksam vor Datenkorruption (z. B. Ransomware), sind aber aufgrund des Offline-Charakters langsam in der Wiederherstellung und daher kein idealer Schutz vor Hardware-Ausfällen.

Hiscox
Arnulfstraße 31, 80636 München
T +49 89 54 58 01 100 E hiscox.info@hiscox.de