Im Fokus von Ransomware. Ist DRaaS die Lösung für KMUs?

Ransomware, defekte Hardware oder Naturkatastrophen, es kann jeden treffen. Ein Backup sichert Daten, aber wie sicher ist das und was passiert, wenn auch noch die eigene IT-Infrastruktur ausfällt? Ist Disaster Recovery as a Service (DRaaS) die optimale Lösung, auch für KMUs, die noch nicht in der Cloud sind?

Die Autorin
Karin Würzberger, Marketing Manager bei Cyberlink

36 Prozent aller Schweizer KMUs waren schon Opfer eines folgenschweren Cyberangriffs,* jedoch zählen nur 56 Prozent der Unternehmen Cybervorfälle zu den drei grössten Geschäftsrisiken.** Ransomware verursacht eine durchschnittliche Ausfallzeit von 23 Tagen,*** hohe Kosten und gefährdet im schlimmsten Fall die Existenz des Unternehmens. Nehmen KMUs die Bedrohung immer noch nicht ernst genug, obwohl sich kaum ein Unternehmen lange Ausfallzeiten leisten kann? Wie könnte ein effektiver und bezahlbarer Grundschutz aussehen und was sollten KMUs zumindest in Betracht ziehen?

DRaaS ist mehr als klassisches Backup.
Während es beim klassischen Backup nur um Datensicherung geht, berücksichtigt DRaaS alles, um schnellstmöglich Geschäftsprozesse mit aktuellen Daten wiederherzustellen und die firmeneigene IT-Infrastruktur wieder voll funktionsfähig zu machen. Mit DRaaS wird die IT-Infrastruktur inklusive Applikationen samt Daten in eine Cloud-Umgebung gespiegelt. Im Desaster-Fall ist ein Umschalten auf das gespiegelte Ersatzsystem (Failover) jederzeit möglich – die Datenverarbeitung wird in die Cloud verlagert. DRaaS stellt Business Continuity sicher, ohne dass der produktive Betrieb in eine Cloud ausgelagert werden muss.

* FHNW 2021
** Allianz, Allianz Risiko Barometer 2021
*** Coveware

Wie funktioniert DRaaS im Katastrophenfall?
Wann genau Firmencomputer mit Ransomware infiziert worden sind, ist meist nicht sofort ersichtlich. Oft kann monatelang weitergearbeitet werden, bis Daten eines Tages verschlüsselt sind, Mitarbeitende nicht mehr arbeiten können und Lösegeldforderungen ins Haus flattern. Durch die Verzögerung sind aber nicht nur Produktivdaten, sondern auch einige, der inzwischen erstellten Replikationen betroffen. DRaaS schützt also nicht vor Datenverschlüsselung, aber die Suche nach dem letzten nicht verschlüsselten Stand wird durch DRaaS erheblich verkürzt, weil ein Replika nach dem anderen in der gespiegelten IT-Infrastruktur in der Cloud überprüft werden kann. Es gilt, Systeme und Daten in den Zustand wiederherzustellen, den sie unmittelbar vor dem Desaster-Fall hatten, damit Mitarbeitende schnellstmöglich und mit minimalem Datenverlust weiterarbeiten können. Im Katastrophenfall übernehmen also die replizierten Maschinen den Betrieb und reduzieren damit lange Ausfallzeiten. Mit DRaaS entstehen meist wenig bis keine Ausfallzeiten (Recovery Time Objectives – RTO) und dem Datenverlust wird entgegengewirkt. Sobald die hausinterne IT-Infrastruktur wiederhergestellt oder ersetzt wurde, werden Prozesse und Daten wieder zurückmigriert.

Mit ausgereifter DRaaS-Technologie auch schrittweise in die Cloud.
Es gibt keinen perfekten Schutz gegen Ransomware und Naturkatastrophen, jedoch entscheiden sich immer mehr KMUs für DRaaS als bestmögliche Lösung. Durch die Auslagerung an einen Managed Service Provider entfällt neben der zeitaufwendigen Orchestrierung einer Disaster-Recovery-Lösung auch die kostenintensive Bereitstellung und Wartung einer eigenen DR-Umgebung. Für ausgeschaltete VMs entstehen keinerlei Compute-Kosten und im Desaster-Fall kommen für tatsächlich verbrauchte Ressourcen die normalen IaaS-Tarife zur Anwendung. Cyberlink-Kunden bezahlen so nur das, was sie auch nutzen und das bei vollständiger Kostentransparenz.

DRAAS VON CYBERLINK AUF EINEN BLICK.

- Sicherung von Daten & IT-Infrastruktur
- Kostengünstiger in der Wiederherstellung als klassische Backup-Systeme
- Keine eigene Hardware und IT-Infrastruktur zur Absicherung notwendig
- Lokale VMs werden in vordefinierten Abständen (z. B. alle 10 Minuten) in die Cyberlink Private Cloud repliziert
- Eine der modernsten Cloud-Plattformen der Schweiz
- Datenhaltung in der Cyberlink Private Cloud & ausschliesslich in Schweizer Rechenzentren
- Flexibel & bedarfsgerecht anpassbar
- Servicequalität statt langer Vertragslaufzeiten

Eine, der modernsten Cloud-Plattformen der Schweiz bietet Sicherheit.
Die Virtual Private Cloud (VPC) von Cyberlink wird ausschliesslich in hochsicheren Tier-3-Rechenzentren im Raum Zürich betrieben, bietet modernste Infrastructure as a Service (IaaS) und wird regelmässig von einem unabhängigen Auditor nach ISAE-3402 überprüft. Die Datacenter-Infrastrukturen genügen strengsten Sicherheitsanforderungen wie jenen der Eidgenössischen Finanzmarktaufsicht (FINMA).

cyberlink

Kontakt
Daniel Hildinger, Key Account Manager
sales@cyberlink.ch