Christian Ruoff

Mehr Schutz vor Cyberkriminalität durch geschickte Backup-Strategie

Die Internetkriminalität nimmt immer neue Formen an, auf die sich IT-Verantwortliche einstellen müssen. Die aktuellen Cyberattacken auf Unternehmen und Organisationen, bei denen mittels der Verschlüsselungs-Trojaner „Locky" und „TeslaCrypt" Daten verschlüsselt und von den Kriminellen nur gegen Lösegeld wieder freigegeben werden, verdeutlichen die Risiken. Eine intelligente Backup-Strategie ist eine erfolgversprechende Abwehrmaßnahme gegen derartige Angriffe. Sie muss unbedingt einen Medienbruch beinhalten, um Daten wiederherstellen zu können, die noch nicht infiziert oder gar unlesbar geworden sind.

Ransomware auf dem Vormarsch

Diese sogenannte Ransomware (Erpresser-Software) wurde über eine Woche nach ihrem Bekanntwerden laut Googles Virenwarndienst „VirusTotal" von nur drei der 54 beobachteten Virenscanner erkannt. Dabei trieben die Trojaner schon seit Wochen ihr Unwesen. Dies hat zur Folge, dass der Befall mit Schadsoftware erst bemerkt wird, wenn es bereits zu spät ist. Mehrere Unternehmen und Verwaltungen in Deutschland sind betroffen und mussten teilweise den Betrieb einstellen. So war sogar das Fraunhofer-Institut in Bayreuth Opfer des Hacker-Angriffs. In den USA haben sich schon erste betroffene Krankenhäuser auf die Zahlung eingelassen, um auf wichtige Patientendaten wieder zugreifen zu können.

Aktuell zielen die Attacken mehrheitlich auf Windows-Systeme. Aber seit kurzem sind auch andere Systeme gefährdet. So gibt es erste nachweisbare Angriffe auf Mac-Systeme. Die Erfolgsquote bei den Erpressungen bestärkt die Cyberkriminellen, auch weitere Betriebssysteme anzugreifen. Da diese Form der Internetkriminalität scheinbar sehr erfolgversprechend für die Angreifer ist, kann in nächster Zeit mit Angriffen auch auf weitere Betriebs- und Serversysteme gerechnet werden. Dabei ist es gar nicht schwer, sich auf Bedrohungsszenarien vorzubereiten und zügig im Falle einer Datenzerstörung oder -verschlüsselung zu reagieren. Der Schlüssel dafür ist eine erprobte Backup- und Wiederherstellungs-Strategie, die zügig zum Normalbetrieb zurückführt.

Die SEP AG, ein deutscher Hersteller von Backup-Lösungen mit Sitz in Weyarn bei München, hat sich mit der Lösung „SEP sesam" auf die Sicherung und Wiederherstellung heterogener IT-Umgebungen spezialisiert. SEP sieht im Falle der Crypto-Trojaner die Datenbank als Hauptangriffsziel. Denn gerade unternehmenskritische Datenbanken sind bei den Erpressern besonders beliebt, da eine Organisation hier am gravierendsten im Geschäftsbetrieb betroffen ist. Der Angriff entspricht in der Regel einem Desasterfall.

Die Wiederherstellung muss dann so zügig wie möglich erfolgen. Das schlägt sich in den RTOs (Recovery Time Objectives) nieder, also in der definierten Wiederanlaufzeit, die bis zur vollständigen Verfügbarkeit von Applikationen vergehen darf. Aber was passiert, wenn auch die Backup-Daten infiziert sind und bei der Wiederherstellung ebenfalls nicht gelesen werden können? SEP gibt dafür folgende Empfehlungen, um die in den SLAs (Service Level Agreements) definierten RTOs einzuhalten und bestenfalls zu unterschreiten.

Ausgeklügelte Strategie verhindert eine Totalverschlüsselung der (Backup-)Daten

Neben den klassisch einzuhaltenden Backup-Szenarien, also wöchentliche Komplettsicherung aller Daten (Full-Backup) und der mindestens täglichen Sicherung der zwischenzeitlich geänderten Daten (inkrementelles Backup) sind weitere Maßnahmen nötig. So sollten die Backup-Daten mittels „Medienbruch" auf einem separaten Bandlaufwerk (Tape) und (wenn durchführbar) an einem anderen Ort aufbewahrt werden. Dabei muss die eingesetzte Backup-Software die Verwaltung von Ladern und Wechseldatenträgern beherrschen. So kann die Schadsoftware nicht mehr auf die Daten zugreifen. Der Aufbewahrungszeitraum sollte angesichts der unentdeckten Ausbreitungsdauer verlängert werden. Die aktuellen Fälle zeigen: Dieser Zeitraum muss mindestens vier bis sechs Wochen betragen, da die Schadsoftware für die Antiviren-Lösungen nicht erkennbar ist und ein Befall erst bemerkt wird, wenn alle Daten bereits verschlüsselt sind.

Wie in allen Backup-Szenarien summieren sich die Datenmengen bei jeder Sicherung, insbesondere beim Full-Backup. Deduplizierung kann hier helfen und intelligent das Volumen der im Backup-Speicher aufbewahrten Datenmenge minimieren. Die Si3-Deduplizierung, die in SEP sesam eingesetzt wird, kann die Datenmenge um bis zu 90 Prozent verringern. Deduplizierung dient nicht nur zur Einsparung von Speicher-Hardware bei der Sicherung, sondern ist die Basis für eine bandbreitensparende Replikation der gesicherten Daten auf die genannten Bandlaufwerke.

Nach dem Angriff: Wiederherstellungsplan muss greifen

Ist ein Angriff passiert, muss zunächst der Zeitpunkt des Angriffs eingegrenzt werden. Dann kann die Datenwiederherstellung ansetzen. Die Lösung von SEP ist in der Lage, einzelne Backups eines beliebigen Sicherungszeitpunktes auf einem abgeschotteten System wiederherzustellen. Im sogenannten Read-Only-Modus können auf bereinigten Backup-Festplatten die Daten von Wechselmedien, wie Bandlaufwerken, eingelesen und analysiert werden.

Wenn der Verschlüsselungsbefehl der Cyberkriminellen noch nicht zur Ausführung gekommen ist, lassen sich so zumindest die Daten lesen. SEP sesam unterstützt hier Forensik Linux-Distributionen wie beispielsweise KALI, die speziell für die Analyse nach einem Cyberangriff entwickelt wurden. Die Schadsoftware hat während der forensischen Analyse keine Möglichkeit, das integre System zu infizieren. Ist der letzte sichere Datensatz gefunden, werden die Systeme damit sauber wiederhergestellt und der Betrieb der IT-Systeme kann wieder normal anlaufen. Vorher müssen die Abwehrmechanismen nochmals überprüft werden, um einen neuerlichen Angriff auszuschließen.

Wiederherstellungsszenarien testen

Um jederzeit eine zügige Wiederherstellung zu gewährleisten, sollten generell regelmäßige Wiederherstellungstests von allen Systemen geprobt werden.

Die praktische Erfahrung zeigt aber, dass dies von den meisten IT-Verantwortlichen vernachlässigt wird. Gesetzliche Vorgaben und Unternehmensrichtlinien stellen meist hohe Anforderungen an die Verfügbarkeit der Unternehmensdaten, für deren Umsetzung die Backup-Strategie eine tragende Säule ist. So kann beispielsweise auch die Dokumentation von Wiederherstellungstests rechtlich relevant werden. Außerdem sind geübte IT-Administratoren im Ernstfall wesentlich routinierter und schneller bei der Wiederherstellung unternehmensrelevanter Systeme, weshalb durch die Praxistests der Wiederanlauf-Prozess oft entscheidend optimiert wird.

Fazit

Beim Schutz vor Bedrohungen ist längst nicht mehr nur die Firewall und die Antivirensoftware mit einzubeziehen. Die neuen Bedrohungen stärken das Bewusstsein für eine durchdachte Datensicherungs- und Wiederherstellungsstrategie. Backup und Recovery sind eine wichtige Säule beim Thema IT-Sicherheit in Unternehmen und Organisationen.

Internet:	Abbildung 1 mit Legende www.siehe.eu/da210
Stichwort:	Ransomware, Backup, Wiederherstellung, Cyberattacken
Autor:	Christian Ruoff, Head of Business Development, SEP AG, Weyarn. **Kontakt: redaction@gliss-kramer.de**

Abbildung 1: Ablauf der Wiederherstellung nach einem Cyberangriff