arcserve®
Protect what's priceless.

8855 Columbine Road, Suite #150
Eden Prairie, Minnesota 55347
Phone: +1 844 639 6792

Hacker nehmen kritische Infrastrukturen aufs Korn und für Betreiber ist der Schutz von Daten oberstes Gebot

Kritische Infrastrukturen sind für das reibungslose Funktionieren unserer Gesellschaft und Wirtschaft unerlässlich. Ohne ein stabiles Netz von Krankenhäusern, Flughäfen, Stromversorgern und Schulen ist unser modernes Leben nicht möglich. Die meisten Menschen sehen diese Dienste als selbstverständlich an. Aber auch Cyberkriminelle wissen, wie abhängig wir von ihnen sind. Florian Malecki, Senior Director, International Product Marketing bei Arcserve, erläutert, welche Maßnahmen Betreiber dieser hochsensiblen Infrastrukturen ergreifen müssen, um die Dienste auch nach einer Cyberattacke aufrechtzuerhalten.

Kritische Infrastrukturen sind im Allgemeinen gut geschützt. Da diese Strukturen hochsensibel sind, stellen sie für Cyberkriminelle ein ganz besonderes Ziel dar und sie unternehmen große Anstrengungen, um die Sicherheitsmechanismen auszuhebeln. Genau das macht kritische Infrastrukturen so verwundbar. Wenn diese Dienste nur für ein bis zwei Tage ausfallen, können sie das öffentliche Leben erheblich beeinträchtigen. Cyberkriminelle wissen, dass viel auf dem Spiel steht, wenn sie diese Systeme stören. Sie wissen auch, dass sie eine gute Chance haben, hohen Profit zu machen. Denn die Kosten und der Arbeitsaufwand für eine manuelle Wiederherstellung von Daten nach einem Ransomware-Angriff sind so hoch, dass die Opfer oft bereit sind, das Lösegeld zu zahlen, um die Kontinuität der Dienste aufrechtzuerhalten. Dabei ist das Zahlen eines Lösegelds keine Garantie für die Entschlüsselung der Daten. Laut einer Studie von Sophos erhalten nur 8 Prozent aller Unternehmen und Organisationen alle

arcserve®
Protect what's priceless.
8855 Columbine Road, Suite #150
Eden Prairie, Minnesota 55347
Phone: +1 844 639 6792

verschlüsselten Dateien zurück. Tatsächlich erhielten Unternehmen und Organisationen, die das Lösegeld bezahlt haben, im Durchschnitt nur 65 Prozent ihrer Daten wieder, 29 Prozent bekamen nicht mehr als die Hälfte ihrer Daten zurück.

Ein prominentes Beispiel aus den USA, das das Ausmaß eines Angriffs auf eine kritische Infrastruktur zeigt und die Verletzbarkeit der Technologie-Infrastruktur offenlegt, war der Ransomware-Angriff auf die Colonial Pipeline. Im Mai 2021 legten Cyberkriminelle die größte US-Treibstoffpipeline lahm und sorgten vorübergehend für Treibstoffengpässe an der gesamten Ostküste. In seiner Aussage vor dem Senatsausschuss für innere Sicherheit und Regierungsangelegenheiten räumte CEO Joseph Blount ein, dass sein Unternehmen nur einen Tag nach Entdeckung der Malware fast 5 Millionen Dollar Lösegeld zahlte.

Ein Problem, das sich weiter verschärft

Kritische Infrastrukturen, wie sie beispielsweise von Bundes-, Landes- und Kommunalbehörden betrieben werden, sind immer öfter Ziel von Ransomware-Angriffen. So wurden laut dem jüngsten State of Ransomware Report von Emsisoft fast 2.400 US-amerikanische Behörden, Gesundheitseinrichtungen und Schulen im vergangenen Jahr Opfer von Ransomware-Angriffen. In einigen Fällen hatten diese Angriffe sogar lebensbedrohliche Folgen: Sie unterbrachen den Notruf, zwangen Krankenwagen zur Umleitung und verzögerten die medizinische Behandlung der Patienten. Auch in Deutschland häufen sich die Ransomware-Angriffe auf Gesundheitseinrichtungen. So legte beispielsweise ein Hackerangriff im September 2020 die IT der Düsseldorfer Uniklinik lahm. Die Urologische Klinik in Planegg wurde zu Beginn dieses Jahres ebenfalls Ziel eines Cyberangriffs.

8855 Columbine Road, Suite #150
Eden Prairie, Minnesota 55347
Phone: +1 844 639 6792

Zwar gab es dort keine Lösegeldzahlungen, aber die Hacker bekamen durch ihre Attacke offenbar Einblicke in sensible Patientenunterlagen.

Ransomware-Angriffstechniken entwickeln sich ständig weiter. Zudem haben die Angriffe zugenommen, während die Ausgaben für die Modernisierung kritischer Infrastrukturen mit dieser Entwicklung nicht Schritt gehalten haben. Der öffentliche Sektor verlässt sich oft auf traditionelle Technologien, die in der Vergangenheit funktioniert haben, aber mittlerweile in die Jahre gekommen sind. Viele Behörden verwenden weiterhin veraltete Hardware, Software und Netzwerke, die anfällig für aktuelle Bedrohungen sind. Hinzu kommt aufgrund der COVID-19-Pandemie, dass in vielen Bereichen Firmen auf das Arbeiten von zu Hause umgestellt haben. Organisationen ermöglichen den Datenzugriff von entfernten Standorten aus über weniger sichere Netzwerke. Dies nutzen Hacker aus. So berichtet Bitdefender, dass die Zahl der Ransomware-Angriffe im Jahr 2020 um atemberaubende 485 Prozent gestiegen ist und viele Ziele sich im öffentlichen Sektor befinden. Erst kürzlich wurde Tulsa in Oklahoma, eine der 50 größten Städte der USA, durch einen Ransomware-Angriff in die Knie gezwungen. Dieser Angriff wirkte sich auf das Netzwerk der Stadt so stark aus, dass die offiziellen Websites lahmgelegt wurden.

Auch Ransomware as a Service (RaaS) sorgt dafür, dass die Zahl der Ransomware-Angriffe steigt. Dieses abonnementbasierte Modell ermöglicht es praktisch jedem, bereits entwickelte Ransomware-Tools für Angriffe zu nutzen. Die Entwickler der Malware kassieren dabei einen Prozentsatz von jeder Lösegeldzahlung. Insgesamt ist das Problem der Cyberkriminalität inzwischen immens: Der Schaden beläuft sich laut Cybercrime Magazine auf 6 Billionen Dollar pro Jahr. Würde man alle Cyberkriminellen an einem Ort

8855 Columbine Road, Suite #150
Eden Prairie, Minnesota 55347
Phone: +1 844 639 6792

versammeln, so hätte dieser nach den USA und China die drittgrößte Wirtschaft der Welt.

Die 3-2-1-1-Backup-Strategie bietet Schutz

Die Betreiber kritischer Infrastrukturen, müssen ihre Bemühungen zur Identifizierung, zur Abschreckung, zum Schutz, zur Aufdeckung und zur Reaktion auf cyberkriminelle Handlungen verbessern. Was können sie also tun, um sich selbst und die Infrastrukturen zu schützen? Einer der wichtigsten Schritte ist die Einführung einer Datenschutzstrategie nach dem 3-2-1-1-System. Diese sieht vor, dass mindestens drei Kopien der Daten aufbewahrt werden. Zwei Kopien sollen vor Ort auf unterschiedlichen Medien (oder auf zwei Festplatten auf unterschiedlichen Systemen) gespeichert sein. Eine dritte Kopie wird an einem entfernten Ort und eine weitere Kopie auf unveränderlichem Objektspeicher (Appliance oder in der Cloud) aufbewahrt. Unveränderliche Objektspeicher sichern die Daten kontinuierlich, indem alle 90 Sekunden ein Snapshot davon erstellt wird. Selbst im Katastrophenfall lassen sich die Daten schnell wiederherstellen. Unveränderliche Snapshots sind schreibgeschützte Versionen von Metadaten für Daten und Dateien. Diese Snapshots ermöglichen eine punktgenaue Datenwiederherstellung. Snapshots ermöglichen es, bei einem Ausfall, einer Naturkatastrophe oder einem Ransomware-Angriff zu einem früheren Dateistatus zurückzukehren. Unveränderliche Snapshots können nicht überschrieben oder gelöscht werden, sodass die Datenintegrität vor Verlust durch menschliches Versagen, Hardwarefehler oder Ransomware-Angriffe geschützt ist. Organisationen können selbst im Katastrophenfall oder bei einem Ransomware-Angriff alle Systeme und Daten rasch und vollständig wiederherstellen und damit eine möglichst geringe Beeinträchtigung der sensiblen Dienste sicherstellen.

arcserve®
Protect what's priceless.

8855 Columbine Road, Suite #150
Eden Prairie, Minnesota 55347
Phone: +1 844 639 6792

Die durch Cyberattacken verursachten Kosten werden wahrscheinlich noch weiter steigen und auch das Risiko für Datenverluste wird weiter zunehmen. Angesichts der sich kontinuierlich verändernden und zunehmenden Zahl von Cyberangriffen müssen Betreiber kritischer Infrastrukturen Möglichkeiten finden, wie sie sich vor Ransomware und die dadurch entstehenden Schäden schützen können. Die Einführung einer Datenschutzstrategie sorgt dafür, dass ihre IT-Struktur selbst vor raffiniertesten Ransomware-Angriffen geschützt ist.

Unternehmenskontakt
Jock Breitwieser
Arcserve
+1 408.800.5625
jock.breitwieser@arcserve.com

Agenturkontakt
TC Communications
Arno Lücht
+49 8081 9546-19
Thilo Christ
+49 8081 9546-17
arcserve@tc-communications.de
www.tc-communications.de