arcserve®
Protect what's priceless.

6600 City W. Parkway, Suite 215
Eden Prairie, Minnesota 55344
Phone: +1 844 639 6792

NIS2 trifft auf SaaS-Infrastruktur

Tipps wie die Richtlinie sichergestellt wird

Von Sven Richter, Arcserve

Die NIS2 (Network Information Security Directive)-Richtlinie zur Sicherheit von Netzwerken setzt neue Maßstäbe für die Cybersicherheit. Sie ist bekanntlich für öffentliche und private Einrichtungen in 18 Sektoren bindend, die entweder mindestens 50 Beschäftigte haben oder einen Jahresumsatz und eine Jahresbilanz von mindestens 10 Millionen Euro. Nach Schätzungen sind bis zu 40.000 deutsche Unternehmen von der NIS2-Richtlinie betroffen. Ziel der Direktive ist es, die Widerstandsfähigkeit von Organisationen im Bereich der Cybersicherheit stärken, indem umfassende Risikomanagementmaßnahmen implementiert werden, einschließlich dem Datensicherungsmanagement und der Notfallwiederherstellung.

Drei wichtige Schritte für die Vorbereitung zur NIS2-Konformität

Die Erfüllung der strengen Anforderungen von NIS2 beginnt mit der dem Map-Prioritize-Test-Framework. Dieses beinhaltet drei wichtige Schritte und ist für jede Art von Organisation geeignet, die NIS2 erfüllen muss.

An erster Stelle steht die **Kartierung kritischer Systeme**. Sie beschreibt eine detaillierte Bewertung der kritischen Infrastruktur, einschließlich lokaler sowie öffentlicher und privater Cloud-Umgebungen. Hierbei werden wichtige Systeme inklusive Software und SaaS-Anwendungen beziehungsweise Entra IDs erfasst und priorisiert, um Identitäten und Anmeldeinformationen zu schützen.

6600 City W. Parkway, Suite 215
Eden Prairie, Minnesota 55344
Phone: +1 844 639 6792

Der zweite Schritt ist die **Priorisierung der wichtigen Daten**. Hierbei werden insbesondere solche Daten identifiziert, die für die Aufrechterhaltung des Betriebs entscheidend sind. Darunter fallen beispielsweise Finanz- und Kundendaten. Zudem wird in diesem Schritt für den Fall einer Cyberattacke, einer Naturkatastrophe oder einer technischen Panne priorisiert, welche Daten zuerst wiederhergestellt werden müssen, um Ausfallzeiten zu minimieren und die Geschäftskontinuität zu gewährleisten.

Der dritte Schritt ist das **Testen der Sicherungssysteme**. Die beste Planung und die beste Sicherungslösung helfen nichts, wenn bei einem Notfall die Widerherstellungsroutinen nicht funktionieren und sich die Ausfallzeit unnötig in die Länge zieht. Regelmäßige Tests können Gewissheit und Vertrauen für den Notfallwiederherstellungsplan schaffen. Zudem zeigen sie verbesserungswürdige Bereiche auf, die vor einem Zwischenfall gelöst werden können, anstatt in einer ernsten Lage für Überraschung zu sorgen.

Auf die SaaS-Backup-Lösung kommt es an

Die Einhaltung von NIS2 erfordert den Einsatz einer zuverlässigen Sicherungs- und Wiederherstellungslösung. Unabhängig davon, ob die Lösung sich nahtlos in die existierende IT-Infrastruktur integriert, muss sie zwingend zur Erreichung der NIS2-Anforderungen beitragen. Folgende Kriterien müssen auf alle Fälle erfüllt sein:

Datensouveränität und Datenschutz

Eine Lösung muss die EU-Vorschriften NIS2 (und DSGVO) erfüllen. Daher ist es ratsam, einen Lösungsanbieter zu wählen, der ausdrücklich Garantien hinsichtlich der Datensouveränität bietet und sicherstellt, dass die Daten im Einklang mit den spezifischen Gesetzen gespeichert und

6600 City W. Parkway, Suite 215
Eden Prairie, Minnesota 55344
Phone: +1 844 639 6792

verarbeitet werden. Dabei sind insbesondere starke Zugangskontrollen unerlässlich, um sensible Daten vor unberechtigtem Zugriff zu schützen.

Keine Kompromisse bei der Wiederherstellungszeit (RTO)

Eine NIS2-gerechte Backuplösung muss granulare und nach Prioritäten geordnete Wiederherstellungsoptionen unterstützen, um ohne Kompromisse eine schnelle Wiederherstellung wichtiger Daten zu gewährleisten. Erst damit ist sichergestellt, dass Ausfallzeiten minimiert und die Geschäftskontinuität gewährleistet sind.

Maximaler Schutz mit Verschlüsselung und Unveränderlichkeit

Selbst wenn es Cyberkriminellen oder andere Gefährdern gelingt, auf ein Backup zuzugreifen, müssen diese nutzlos sein. Dies wird mit Lösungen erreichet, welche die Daten während der Übertragung und im Ruhezustand verschlüsseln und zudem unveränderbare Backups unterstützen, um unbefugte Änderungen, Löschungen oder Manipulation durch Ransomware zu verhindern.

Anbieterabhängigkeiten vermeiden

Die Vergangenheit zeigt, dass Organisationen, die auf einen zentralen Anbieter setzen, von dessen Sicherheitsbemühungen abhängig sind und Fehler zu dramatischen Situationen führen können. Daher ist eine sinnvolle Verteilung zweckmäßig – auch beim SaaS-Anbieter. Dieser sollte eine logische und physische Trennung von der öffentlichen Cloud gewährleisten. In Kombination mit Air-Gapping-Maßnahmen schützt dieser Ansatz die Backups vor Ransomware-Angriffen und gewährleistet einen kontinuierlichen Zugriff, selbst wenn die Dienste des öffentlichen Cloud-Anbieters unterbrochen sind.

arcserve®
Protect what's priceless.

6600 City W. Parkway, Suite 215
Eden Prairie, Minnesota 55344
Phone: +1 844 639 6792

Die Compliance gemäß NIS2 und anderen Direktiven kann sich schnell zu einer komplexen Aufgabe in der IT ausweiten. Organisationen, die auf eine Backup-Lösung setzen, die für den Schutz gehosteter Daten in SaaS-Anwendungs-Clouds wie Microsoft 365, Entra ID, Microsoft Dynamics 365, Salesforce, Google Workspace oder Zendesk entwickelt wurde, haben beste Chancen, konform zu NIS2 und weiteren Vorgaben zu sein.

Folgen Sie Arcserve auf LinkedIn oder X und lesen Sie unsere neuesten Artikel zum Thema Datenschutz und -management im Arcserve Blog.

###

Über Arcserve
Arcserve ist der Pionier für einheitliche Daten-Resilienz-Lösungen. Seit mehr als 40 Jahren vertrauen fast 150.000 Kunden und über 30.000 Vertriebspartner in 150 Ländern auf Arcserve, um ihre Datenresilienz zu stärken, verlorene Daten wiederherzustellen und die Kontinuität ihres Geschäftsbetriebs zu gewährleisten. Mit einem einheitlichen Ansatz für Datensicherung und -wiederherstellung, erstklassigem technischen Support und dem niedrigen Total Cost of Ownership (TCO) hilft Arcserve Unternehmen, ihre Daten zu verwalten, zu schützen und - was am wichtigsten ist - in jeder Situation wiederherzustellen.
Erfahren Sie mehr unter arcserve.com und folgen Sie Arcserve auf Twitter oder LinkedIn.

Unternehmenskontakt
Alex Plotnikov
Arcserve
alex.plotnikov@arcserve.com

Agenturkontakt
TC Communications
Arno Lücht
+49 157 524 437 49
Thilo Christ
+49 171 622 06 10
arcserve@tc-communications.de