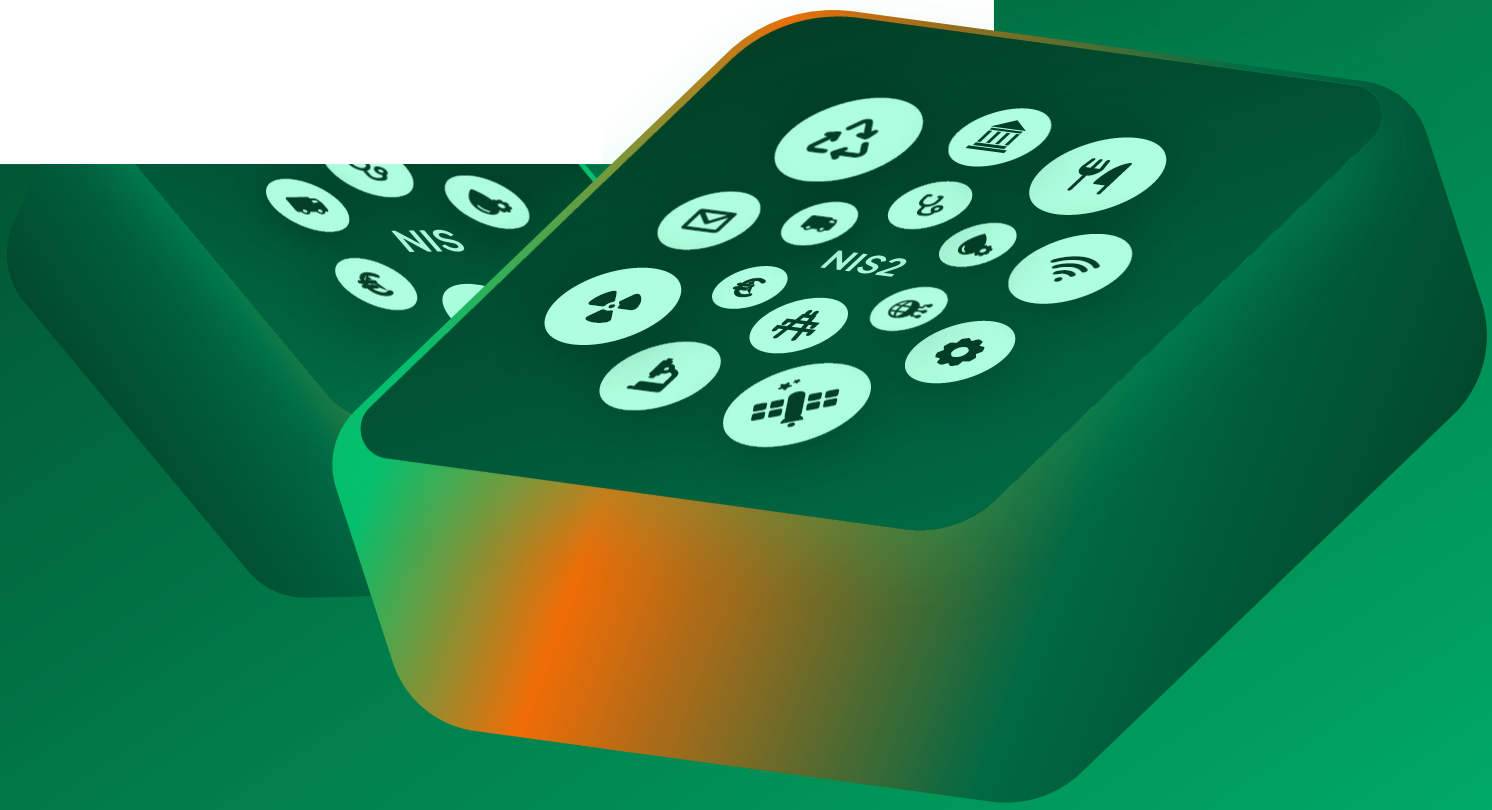
keepit

NIS2 Directive

Wie Sie sich auf die neue Cybersecurity Richtlinie vorbereiten

Ab dem 17. Oktober 2024 legt die EU-Richtlinie zur Netz- und Informationssicherheit (NIS2) erweiterte Standards für das Management von Cybersicherheitsrisiken und Meldepflichten fest. Um die Richtlinie einzuhalten, müssen Unternehmen Maßnahmen ergreifen, um Cyberrisiken zu minimieren und ihre Betriebskontinuität sicherzustellen.



keepit®

*** Betriebskontinuität:** Bezieht sich auf das hohe Niveau der Bereitschaft einer Organisation, kritische Funktionen und Prozesse während oder nach einem Notfall oder einer Störung weiter auszuführen

Was jetzt zu tun ist

Bereiten Sie Ihr Unternehmen mithilfe bewährter Verfahren vor

Sie sollten nun eine Risikoanalyse durchführen, um festzustellen, welche Ihrer Daten geschäftskritisch sind und gesichert werden müssen, einen soliden Disaster Recovery Plan erstellen und kontinuierlich testen, ob er funktioniert. Verwenden Sie für die Analyse den methodischen Rahmen „Identifizieren-Priorisieren-Testen“:

1. Kritische Systeme identifizieren

Bewerten und analysieren Sie kritische Prozesse Ihres Betriebs und kritische Systeme on-prem, in der native Cloud und in der Public Cloud.

Identifizieren und priorisieren Sie wichtige Daten, um Betriebskontinuität zu gewährleisten.* Vergessen Sie SaaS-Anwendungen wie Entra ID nicht. Der Schutz von Identitäten und Anmeldeinformationen ist von entscheidender Bedeutung. Die Vernachlässigung von Identitäts- und Zugangsdaten kann die Betriebskontinuität beeinträchtigen, selbst wenn andere Daten vollständig wiederhergestellt sind. Microsoft selbst stuft Identitätssysteme deshalb als wichtiger ein als Systeme zur Lebenserhaltung von Menschen. Erfahren Sie mehr darüber.

2. Priorisieren: Worauf muss Ihr Unternehmen unbedingt zugreifen können?

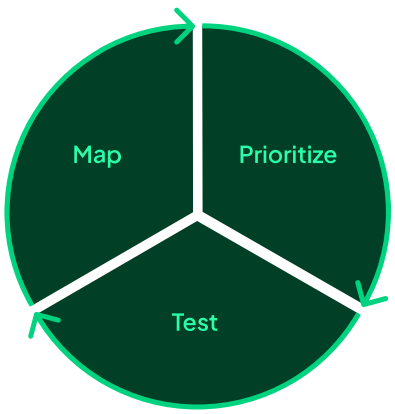
Welche Art von Daten haben Sie? Wie schützen Sie diese Daten? Auf welche wichtigen Daten müssen Sie im Falle eines Angriffs möglichst schnell wieder zugreifen können? Sind die E-Mails Ihres Geschäftsführers entscheidend für die Kontinuität Ihres Unternehmens? Oder sind es vielleicht

Ihre Logistikdaten, Kundendaten, Ihr Business-Intelligence-Dashboard oder Ihr Programmcode? Finden Sie heraus, welche Daten Sie bei der Wiederherstellung priorisieren müssen.

3. Testen Sie, ob Ihr Backup funktioniert

Tests sind ein Schlüsselelement für die Kontinuität. Stellen Sie sicher, dass die Datenwiederherstellung funktioniert wie geplant:

- Validieren Sie Ihre Wiederherstellungsfähigkeit umgehend.
- Bestimmen Sie akzeptable Ausfallzeiten.
- Testen Sie Backups regelmäßig, um sicher zu sein, dass Ihr dynamischer Disaster Recovery Plan und die unterstützende Software so funktionieren wie geplant.



keepit®

Einen Partner für Backup und Disaster Recovery auswählen

Nach der Implementierung des oben genannten methodischen Rahmens besteht Ihre nächste Aufgabe darin, auf Ihre Anforderungen zugeschnittene Lösungen zu finden. Halten Sie sich bei der Auswahl eines Anbieters an die branchenüblichen bewährten Verfahren für den Datenschutz. Bedenken Sie die folgenden Punkte:

Datenhoheit und Datenschutz:

Um EU-Vorschriften wie die DSGVO einzuhalten, müssen Sie sicherstellen, dass, wenn Sie Ihre Daten an einem geografischen Standort sichern, die dot geltenden Gesetze eingehalten werden. Implementieren Sie Zugriffskontrollen zum Schutz vor unbefugtem Zugriff und verarbeiten Sie alle Daten unter Einhaltung der geltenden Datenschutzgesetze. Entscheiden Sie sich für einen Anbieter, der mit den Vorschriften zur Datenaufbewahrung und zum Datenschutz vertraut ist, und der eine Garantie für die Nichtweitergabe von Daten bietet, um den Speicherort und den Zugriff auf Daten sicher zu kontrollieren.

Wiederherstellungszeit:

Sie müssen sich darüber im Klaren sein, dass es unmöglich ist, Petabytes an Daten innerhalb von Sekunden wiederherzustellen. Entscheiden Sie sich für eine Lösung, die eine rasche Wiederherstellung der als kritisch identifizierten Daten ermöglicht. Die Betriebskontinuität hängt sowohl von der ununterbrochenen Datenverfügbarkeit als auch von der Minimierung der Ausfallzeiten durch eine schnelle Wiederherstellung ab.

Entscheiden Sie sich für eine Lösung, die eine granulare, sofortige und nach Prioritäten geordnete Wiederherstellung von wichtigen Daten unterstützt.

Verschlüsselung und Unveränderlichkeit:

Da Backups ein natürliches Ziel für Cyberkriminelle sind, müssen sie sowohl im Ruhezustand als auch während der Übertragung durch robuste Maßnahmen geschützt werden. Essentiell ist die Verschlüsselung und Unveränderlichkeit der Daten, um Hacker daran zu hindern, Ihre Daten zu verändern oder zu löschen – selbst dann, wenn sie sich Zugang verschaffen würden.

Anbieterunabhängigkeit:

Wählen Sie einen Cloud-Backup-Anbieter, der eine Trennung von der öffentlichen Cloud Ihres SaaS-Anbieters gewährleistet. Nutzen Sie Air-Gapping-Maßnahmen und sichern Sie Ihre Daten auf einer separaten logischen und physischen Infrastruktur. Dies schützt vor Datenverlust bei Nichtverfügbarkeit der öffentlichen Cloud und verhindert, dass Ransomware-Angriffe Ihre Backups kompromittieren können.

keepit®

Wem vertrauen Sie die Sicherheit Ihrer Daten an? Gute Gründe, die für Keepit sprechen:

- Wir sind in Europa gegründet worden.
- Wir besitzen und betreiben unsere eigene Infrastruktur und Rechenzentren auf der ganzen Welt, dabeizwei EU-Standorte (Dänemark und Deutschland) und einen im Vereinigten Königreich.
- Wir gewährleisten volle Datenhoheit mit Nicht-Übertragungsgarantie, unabhängig vom Datenschutzschildstatus.
- Wir setzen führende Sicherheitsmaßnahmen wie Air-Gapping, Unveränderlichkeit und Verschlüsselung ein, sowohl bei Übertragung der Daten als auch im Ruhezustand.
- Wir gewährleisten die vollständige Einhaltung aktueller und künftiger EU-Vorschriften, wie NIS2 und DSGVO.

NIS2 auf einen Blick

Was ist der Zweck von NIS2?

Der Zweck der NIS2-Richtlinie ist die Stärkung der EU-weiten Cyberresilienz, die zur Aufrechterhaltung der Betriebskontinuität Maßnahmen in Bezug auf Backup-Management und Disaster Recovery verlangt. Daher müssen Unternehmen ein hohes Maß an Bereitschaft aufrechterhalten, um bei einer Störung (z. B. einem Cyberangriff) oder einem Notfall kritische Funktionen ausführen zu können. Der Schutz betriebskritischer SaaS-Daten hat dabei eindeutig Priorität.

NIS2 erfordert Backup und Disaster Recovery

In Artikel 21 der NIS2 Richtlinie werden mehrere Risikomanagementmaßnahmen im Bereich der Cybersicherheit aufgeführt, die Unternehmen zur Aufrechterhaltung des Betriebs einhalten müssen, insbesondere „Backup-Management und Wiederherstellung nach einem Notfall“. Erfahren Sie mehr über Artikel 21.

Für wen gilt die NIS2?

Die Richtlinie gilt für Sektoren und Einrichtungen, die als „wesentliche“ und „wichtige“ kritische Infrastrukturen eingestuft sind, wie Energie, Verkehr, Gesundheit und digitale Infrastruktur. Wie die Datenschutzgrundverordnung (DSGVO), die personenbezogene Daten schützt, gilt die NIS2 für Unternehmen an vorderster Front und auch für ihre Auftragnehmer.

Vereinbaren Sie noch heute einen Gesprächstermin

Wenn Sie eine Beratung in Bezug auf die Einhaltung regulatorischer Anforderungen wünschen und besprechen möchten, welche Schritte Ihr Unternehmen jetzt einleiten muss, um sich für die NIS2-Richtlinie vorzubereiten, helfen wir Ihnen gerne weiter.

Einen Gesprächstermin vereinbaren

www.keepit.com