NIS2 IM ÜBERBLICK

WER IST BETROFFEN?

Wesentliche Einrichtungen:

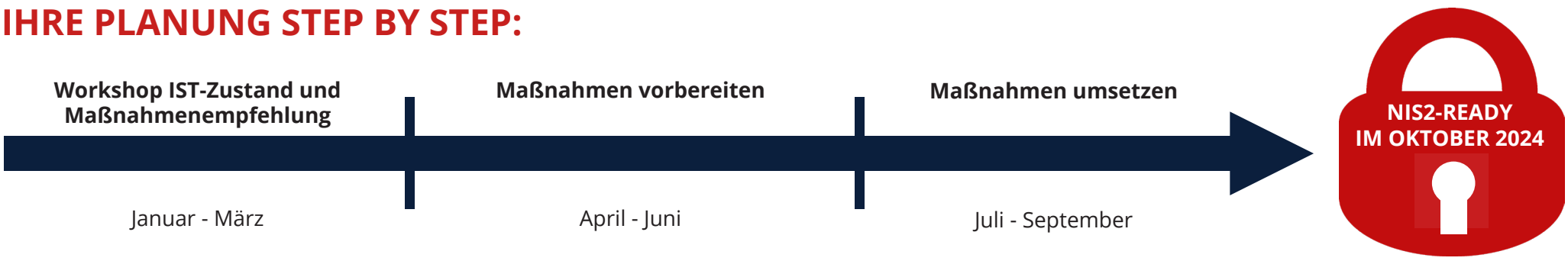
- mind. 250 Mitarbeitende oder mehr als 50 Mio. € Jahresumsatz
- Sektoren mit hoher Kritikalität: Energie, Verkehr, Bank- und Finanzwesen, Gesundheitswesen, Wasserversorgung, Digitale Infrastruktur, ITK-Dienste, Öffentliche Verwaltung, Weltraum

Wichtige Einrichtungen:

- 50 - 249 Mitarbeitende oder mehr als 10 Mio. € Jahresumsatz
- Sektoren mit hoher Kritikalität: Energie, Verkehr, Bank- und Finanzwesen, Gesundheitswesen, Wasserversorgung, Digitale Infrastruktur, ITK-Dienste, Öffentliche Verwaltung, Weltraum
- Sonstige kritische Sektoren: Post- und Kurierdienste, Abfallwirtschaft, Chemie, Ernährung, Herstellung von Waren, Digitale Dienste, Forschung

NIS2-ANFORDERUNGEN	SICHERHEITSZIELE DER NIS2-ANFORDERUNGEN			
Risikoanalyse und Sicherheit	Etablieren eines Verfahrens zur kontinuierlichen Risikobewertung	Pflege des Asset-Registers	Kontinuierliches Schwachstellenmanagement	
Bewältigung von Sicherheitsvorfällen	Anfertigung eines Incident Response Plans	Fortschrittliche Angriffserkennung auf den Endgeräten und Netzwerkmonitoring		
Business Continuity Management, Aufrechterhaltung und Wiederherstellung, Backup	Etablieren eines Business Continuity Managements	Erstellen eines Backup-Plans	Testen der Backups auf Wirksamkeit (Wiederherstellbarkeit)	Erstellen eines IT-Notfallhandbuchs
Sicherheit der Lieferketten	Prüfen der Lieferanten von informationstechnischen Systemen	Überprüfung der Mindestsicherheitsstandards der Lieferkette		
Management/Offenlegung von Schwachstellen, Sicherheit bei Beschaffung, Entwicklung und Wartung	Regelmäßige Überprüfungen der Systeme/Software	Security by Design/ by Default	Monitoring von Schwachstellen und entsprechendes Management	
Konzepte und Verfahren zur Bewertung der Wirsamkeit von Risikomanagementmaßnahmen/ Cybersicherheit	Regelmäßige Audits und Tests mit Berücksichtigung der jeweils aktuellen Sicherheitslage	Regelmäßige Schwach-stellenscans/PenTests		
Cyberhygiene inklusive Schulungen für Cybersicherheit	Durchführen von regelmäßigen Awareness-Maßnahmen und -Kampagnen	Überprüfungen der Awareness aller Mitarbeitenden (Phishing etc.)	Kontinuierliche Prüfung und Anpassung der Richtlinien (Passwort, Berechtigung, u. a.)	
Sicherheit des Personals, Zugriffskontrolle und Management von Anlagen	Sicherstellung der Eignung aller Mitarbeitenden	Zutritts-/Zugangskonzepte		
Konzepte und Verfahren für Kryptografie und Verschlüsselung	Kryptografiekonzept mit Festlegung der verwendeten Verschlüsselungsmethoden			
Multi-Faktor-Authentifizierung (MFA), kontinuierliche Authentifizierung	Einführung einer MFA für zentrale Systeme und externe Zugriffe	Ggf. gesicherte Notfallkommunikation		

IHRE PLANUNG STEP BY STEP:



Netzlink Informationstechnik GmbH, IT-Campus Westbahnhof, Westbahnhof 11, D-38118 Braunschweig
Tel. +49 531 707 34 30, info@netzlink.com

www.netzlink.com