



SINuS

IT-SECURITY SELF-ASSESSMENT

Mit SINuS den Überblick über Ihre IT und die Einhaltung der erforderlichen Vorgaben zu NIS2 und ISO behalten.





Herausgeber



DataSolution LUD GmbH

Isarstr. 13
D-14974 Ludwigsfelde

Ansprechpartner

Berit Schubert
T: +49 (0) 3378-202513
M: mail@ds-lud.de
W: www.sinus-nis.cloud

In Kooperation mit



mc-Technik Dienstleistungs- und Consulting
GmbH

Marienthaler Str. 24
D- 24340 Eckernförde

Ansprechpartner

Christiane Mestel
T: +49 (0) 4351-7321-520
M: c.mestel@mc-technik.de

Version | 1.0

Copyright

DataSolution LUD GmbH 2024



Informationsmanagementsystem SINuS auf Basis von Ninox

Ab Herbst 2024 muss die EU-Richtlinie NIS2 auch nach deutschem Gesetz umgesetzt werden. Mit dem Cybersicherheits-Stärkungsgesetz kommen dann auf viele Unternehmen und Einrichtungen umfangreiche Anforderungen zu, welche die Umsetzung zahlreicher Maßnahmen erforderlich machen. Mit **SINuS** können Sie schnell klären, wo sie stehen, Risiken bewerten und Maßnahmen herleiten.

IST-Stand herausfinden

Anhand von NIS-Bausteinen, welche in 19 Bausteine bzw. unterschiedlich priorisierten Kategorien gegliedert sind, lässt sich der IST-Stand der IT-Infrastruktur einfach und transparent ermitteln.

Eintrittswahrscheinlichkeit	Schaden	Risiko	Bearbeitungsstand
wahrscheinlich	hoch	hoch	50 %

NIS_Fragen	Frage_ID	Frage	Bearbeitungsstand	Datum letzte Bearbeitung	Risiko	aktiv
N06.01	N06.01	Erfordern Clients eine Authentisierung durch Benutzende, bevor sie verwendet werden können?	100 %	08.07.2024	hoch	ja
N06.02	N06.02	Wird eine Bildschirmsperre verwendet, wenn ein Client unbeaufsichtigt betrieben wird?	100 %	08.07.2024	niedrig	ja
N06.03	N06.03	Sind Benutzer dazu verpflichtet, sich vom IT-System und in Anwendungen abzumelden, wenn sie es nicht mehr be	100 %	08.07.2024	niedrig	ja
N06.04	N06.04	Werden Clients gegen Schadssoftware geschützt?	100 %	08.07.2024	mittel	ja
N06.05	N06.05	Ist der Bootvorgang von Clients abgesichert?	0 %		hoch	ja
N06.06	N06.06	Sind alle nicht benötigten Funktionen wie Netzwerkanschlüsse, WLAN-Funktion, Bluetooth-Funktion, Fernwartung	100 %	11.07.2024	hoch	ja

Grundlage für die Bewertung sind die NIS-Fragen, die zu jedem Baustein dazugehören und deren detaillierte, untergeordnete Prüffragen beantwortet werden müssen.

Eintrittswahrscheinlichkeit	Schaden	Risiko
unwahrscheinlich	hoch	niedrig

Prüffragen	Prüf_ID	Prüffrage	Antwort	Eintrittswahrscheinlichkeit	Stand	Datum bearbeitet
P02.02.01	P02.02.01	Werden Benutzerkonten, die längere Zeit inaktiv sind, di	In Ansätzen erfüllt	unwahrscheinlich	in Arbeit	07.07.2024
P02.02.02	P02.02.02	Werden bei längeren Abwesenheiten berechnete Person	teilweise erfüllt	sehr unwahrscheinlich	erledigt	07.07.2024

Je nach Erfüllungsgrad und Beantwortung der Prüffragen wird der Risikograd für die NIS-Frage und damit für den jeweiligen NIS-Baustein ermittelt.

Somit erhalten Sie einen umfangreichen, detaillierten IST-Stand in Bezug auf die jeweiligen NIS2-Anforderungen.



Risiken bewerten

Mit **SINuS** lässt sich effizient die Risikobewertung wahlweise nach den [BSI-Gefährdungen](#) und/oder die Anwendbarkeit der ISO Controls ([Statement of Applicability, SoA](#)) nach der ISO 27001:2022 Anhang A durchführen. Die Risiken werden anhand der Eintrittswahrscheinlichkeit und der Schadenshöhe bewertet und lassen sich so schneller identifizieren. Jeder Prüffrage werden mögliche Gefährdungslagen zugeordnet.

Prüffragen

Unternehmen: Sicher ist Besser GmbH

Prüf_ID: P01.01.01 | NIS_ID: N01 | Gefährdungen: G.27,G.18

ISO_Controls: CO 0502 Rollen und Verantwortlichkeiten im Bereich der Informationssicherheit

Verantwortlich: [Dropdown]

Prüffrage: Wurde für alle Geschäftsprozesse festgelegt, wer für diese und deren Informationssicherheit zuständig ist?

Antwort: fast erfüllt | Eintrittswahrscheinlichkeit: **unwahrscheinlich** | Datum bearbeitet: 09.08.2024 | Stand: in Arbeit

Maßnahme: Für Geschäftsprozesse ist festzulegen und zu dokumentieren, wer für diese und die Informationssicherheit zuständig ist. Dazu gehört die Benennung von Verantwortlichen für die Sicherheit, den Betrieb, die Wartung und die Überwachung von Geschäftsprozessen.

Maßnahmen zur Festlegung von Verantwortlichkeiten für Geschäftsprozesse und deren Informationssicherheit:

- Erstellung einer detaillierten Prozessdokumentation für alle Geschäftsprozesse
- Identifikation und Benennung eines Prozessverantwortlichen für jeden Geschäftsprozess
- Definition von Informationssicherheitsverantwortlichen für jeden Geschäftsprozess
- Erstellung eines Organigramms, das die Verantwortlichkeiten und Zuständigkeiten darstellt

Maßnahmen herleiten

Jede Prüffrage enthält mögliche Maßnahmen, Empfehlungen und Hinweise zur Reduzierung der jeweiligen Risiken. So können **neue TOM (Technische und organisatorische Maßnahmen)** zur Vermeidung von Bedrohungen hergeleitet und umgesetzt werden. Der umfangreiche Maßnahmenkatalog unterstützt bei der Entwicklung des eigenen Cybersicherheits-Managementsystems unter Berücksichtigung der Informationssicherheit, dem Datenschutz und der IT-Sicherheit.

Unternehmen: Sicher ist Besser GmbH | Anzahl Fragen: 241

Übersicht drucken

Filter zurücksetzen

Der Bearbeitungsstand gesamt liegt bei 10,18%

NIS_Baustein	Frage_ID_	Frage	Stand	Risiko	Priorität	Verantwortlich	Wiedervorlag
Organisation und Personal	N01.01	Wurde für alle Geschäftsprozesse festgelegt, wer für diese und deren I	erledigt	mittel	Prio 1		
Organisation und Personal	N01.02	Wurde für alle (Fach-), Anwendungen, IT-Systeme und Kommunikation:	erledigt	mittel	Prio 1		
Organisation und Personal	N01.03	Wurde für alle Räume und Gebäude festgelegt, wer für diese und dere	erledigt	mittel	Prio 1		
Organisation und Personal	N01.04	Wurden die Personen darüber informiert, welche Zuständigkeiten sie h	erledigt	mittel	Prio 1		
Organisation und Personal	N01.05	Sind alle Mitarbeitenden in der Lage, ihre Aufgaben ordnungsgemäß a	erledigt	mittel	Prio 1		
Organisation und Personal	N01.06	Gibt es für alle wesentlichen Geschäftsprozesse und Aufgaben Vertretu	offen	hoch	Prio 1		
Organisation und Personal	N01.07	Werden unvereinbare Aufgaben von verschiedenen Rollen und Person	offen	hoch	Prio 1		



Verbesserungsprozess verfolgen

In **SINuS** lässt sich die Umsetzung von Maßnahmen dokumentieren und so der Prozess zur stetigen Verbesserung der IT-Sicherheit im Blick behalten. Ziel ist, über einen definierten Zeitraum die Eintrittswahrscheinlichkeit und somit das Sicherheitsrisiko anhand von effektiven Maßnahmen zu reduzieren.

Als Cybersicherheits-Managementsystem konzipiert, kann der Änderungsprozess über einen Zeitstrahl (jährlich) dargestellt werden. Im **Management Review** lassen sich die Daten für die Führungsebene zusammenfassend aggregieren.

Management Review [Jahr]



Management Review für [Jahr]

1 Einleitung und Zweck

Im Rahmen dieses Management Reviews werden der aktuelle Status des Informationssicherheits-Managementsystems (ISMS) und die Fortschritte bei der Umsetzung der NIS-2 Richtlinie evaluiert. Die NIS-2 Richtlinie, die darauf abzielt, die Cybersicherheit und die Resilienz von Netz- und Informationssystemen innerhalb der EU zu stärken, erfordert eine systematische und kontinuierliche Überprüfung der Informationssicherheitsmaßnahmen.

1.1 Ziele des Management Reviews:

1.1.1 Bewertung der ISMS-Performance:

Die Leistungsfähigkeit des ISMS im Hinblick auf die Erreichung der definierten Sicherheitsziele wird analysiert. Dies umfasst die Überprüfung der Wirksamkeit der Sicherheitskontrollen und die Identifizierung von Verbesserungsbereichen.

1.1.2 Compliance mit der NIS-2 Richtlinie:

Es soll sichergestellt werden, dass alle Anforderungen der NIS-2 Richtlinie erfüllt werden. Dies beinhaltet die Anpassung der Sicherheitsrichtlinien und -prozesse an neue gesetzliche Vorgaben.



IT-Sicherheitsvorfälle dokumentieren

In **SINuS** lassen sich IT-Sicherheitsvorfälle entsprechend der gesetzlichen Vorgaben dokumentieren. Ein direkter Zugang zum Meldeportal aus dem System heraus, erleichtert den verpflichtenden Meldvorgang.

> **Dokumentation_Meldungen** ⓘ

Unternehmen
99 Testunternehmen

Art: IT-Sicherheitsvorfall | Datum Anfrage/Vorfall: 12.08.2024 | Datum Antwort: 14.08.2024 | Meldung Behörde: Ja

Datum Meldung Behörde: 14.08.2024 | Meldeportal: <https://mip2.bsi.bund.de/> | Übersicht Meldestellen: <https://mip2.bsi.bund.de/meldestellen-uebersicht/>

Beschreibung
Phishingangriff durch Spam-Mail

Link Dokumente

Betroffene Personenarten: Kunden | Betroffene Datenarten: E-Mailadresse

Merkmale von SINuS:

- Individuelle Zugangsdaten (Benutzer/Passwort)
- Mandanten- und Multi-Nutzer-Fähigkeit
- Zusammenarbeit mit Abteilungen und Teams
- Zugriff von jedem Gerät
- Zentrale Dokumentation an einem Ort
- Versionierung und Eingabekontrolle
- Revisionsicherheit und Backup

> **Unternehmen** | NIS_Bausteine | Maßnahmen | Gefährdungen | ISO Controls | Dokumentation_Meldungen ⓘ

Logo: | Unternehmensnr: 4711 | Unternehmen: Sicher Ist Besser GmbH | Adresszusatz: | Straße: Riskoweg 100 | PLZ: 12345 | Ort: Cyberspace | Branche: IKT Dienstleistungen

DSB: CM | Niederlassung_Standort:

Ansprechpartner

Anrede: Herr | Vorname AP: Harry | Nachname AP: Hacker | E-Mail: h.hacker@sicherbesser.de | Telefon: | Statusbericht jährlich zum: 01.10.2024 | Anzeige Gefährdungen: | Anzeige ISO Controls:

Weitere Ansprechpartner:

Weitere Ansprechpartner

Eingabe weitere Ansprechpartner

Anrede	Vorname	Nachname	Position	Email	Telefon
Frau	Susi	Sorglos	Datenschutzbeauftragte	s.sorglos@sicherbesser.de	



Preise für SINuS

SINuS Lizenz

170,00 € / Monat

- ✔ Nutzung des Templates
- ✔ inklusive 1 x Ninox-Lizenz
- ✔ jede weitere Ninox-Lizenz á 45,00 € / Monat
- ✔ Änderungsprogrammierungen
- ✔ Einführung in die Anwendung via Videocall
- ✔ Support als Zusatzleistung
- ✔ Mindestvertragslaufzeit 3 Jahre
- ✔ alle Preise zzgl. der gesetzlichen MwSt.

Support

20,00 € / Monat

- ✔ Aktualisierung der NIS-Fragen
- ✔ Aktualisierung der Prüffragen
- ✔ Aktualisierung der Maßnahmenempfehlungen
- ✔ Support via Telefon und E-Mail
- ✔ Feedback- und Vorschlagsmanagement
- ✔ alle Preise zzgl. der gesetzlichen MwSt.

SINuS kaufen

Preise auf Anfrage

- ✔ Kauf des Templates und Übernahme in die eigene Ninox-Cloud
- ✔ eigene Entwicklungswünsche auf Anfrage
- ✔ Einführung in die Anwendung via Videocall
- ✔ Support als Zusatzleistung

Ninox als Basis

Die Grundlage von SINuS ist Ninox, eine Plattform, auf der sich Anwendungen erstellen und individualisieren lassen. Somit können Arbeitsprozesse digitalisiert und vereinfacht werden. Die Zusammenarbeit im Team und durch mehrere Nutzer gleichzeitig bietet die Voraussetzung für effektive Tools, die auf der Basis von Ninox erstellt werden können.



Als langjähriger Solution Partner von Ninox können wir Sie auch in diesem Bereich unterstützen.

Weitere Informationen zu Ninox finden Sie [hier](#).

Sollten Sie Ninox für weitere bzw. eigene Lösungen in Betracht ziehen, können Sie die Lizenzen auch über uns als Anbieter von SINuS beziehen. Informationen dazu geben wir Ihnen gern auf Anfrage.



Wir haben Sie überzeugt und Sie möchten unsere Anwendung gern testen?

Dann gehen Sie wie folgt vor:

Wenn Sie die Anwendung für 30 Tage kostenfrei testen möchten, laden wir Sie zu einem Test-Team ein. Sie erhalten eine Einladungsmail von Ninox. Mit Bestätigung der Einladung haben Sie Zugriff auf die Test-Datenbank von SINuS. In der Testdatenbank sind ausgewählte Bausteine und Prüffragen vorhanden, allerdings noch nicht der volle Umfang.

Nach dem Testzeitraum bzw. wenn Sie sich zum Kauf der Lizenz entschließen, laden wir Sie in das Echt-Team ein.

Bei Kauf des Templates klären wir die Umsetzung entsprechend.

Bei Fragen können Sie sich gern telefonisch unter: 04351/7321-520 oder per E-Mail unter: datenschutz@mc-technik.de an uns wenden. Gern vereinbaren wir auch einen Demo-Termin.