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

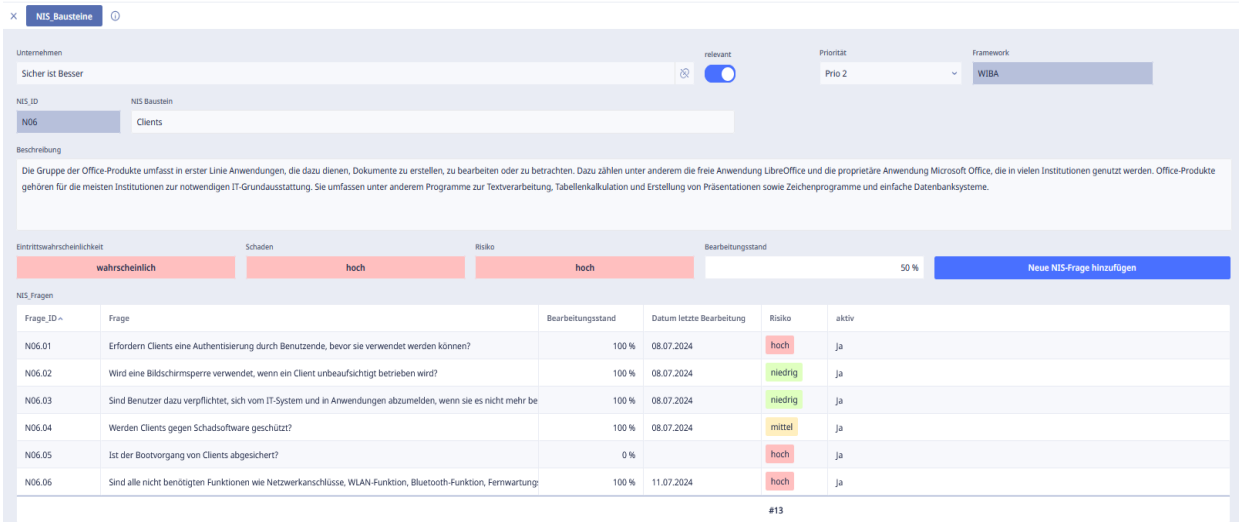
Copyright

Informationsmanagementsystem SINuS auf Basis von Ninox

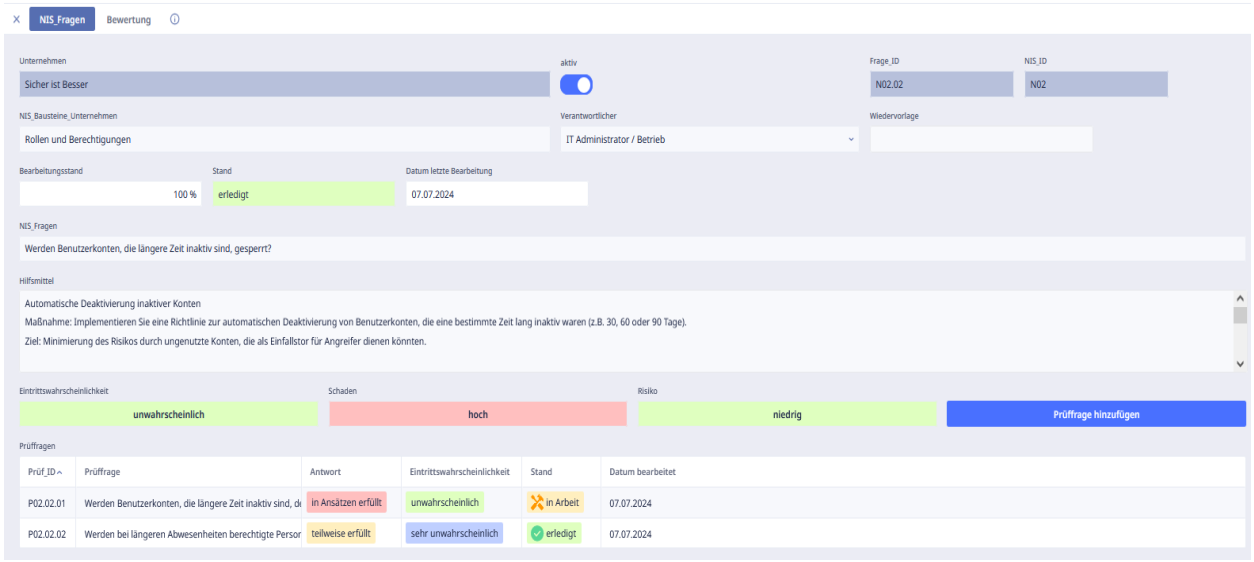
Ab Herbst 2024 muss die EU-Richtlinie NIS2 auch nach deutschem Gesetz umgesetzt werden. Mit dem Cybersicherheits-Stärkungsgesetz kommen dann auf viele Unternehmen und Einrichtungen umfangreiche Anforderungen zu, welche die Umsetzung zahlreicher Maßnahmen erforderlich machen. Mit **SINuS** können Sie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



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

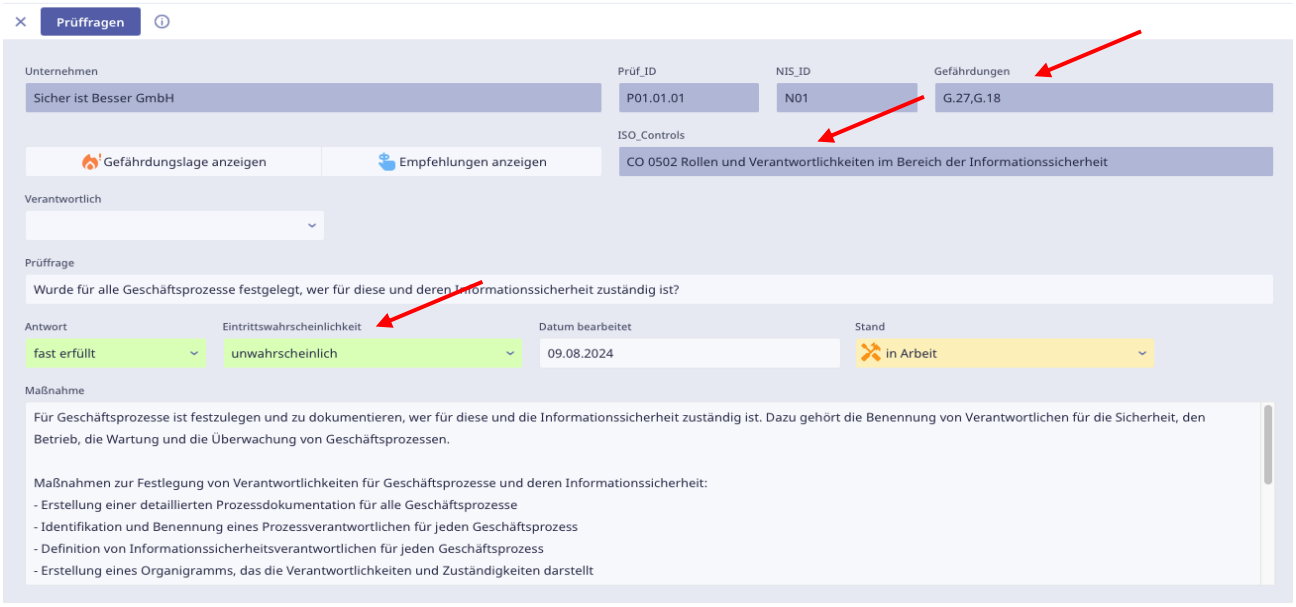


Je nach Erfüllungsgrad und Beantwortung der Prüffragen wird der Risikograd für die NIS-Frage und damit für den jeweiligen NIS-Baustein ermittelt.

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

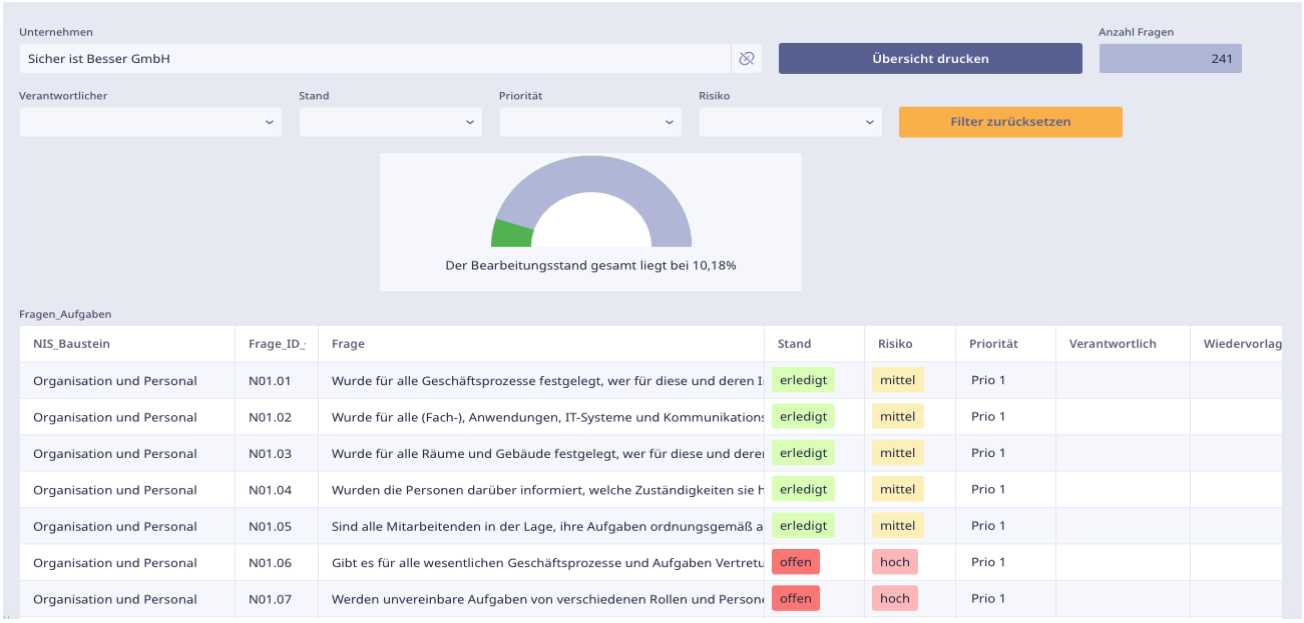
Risiken bewerten

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.



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.



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

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:

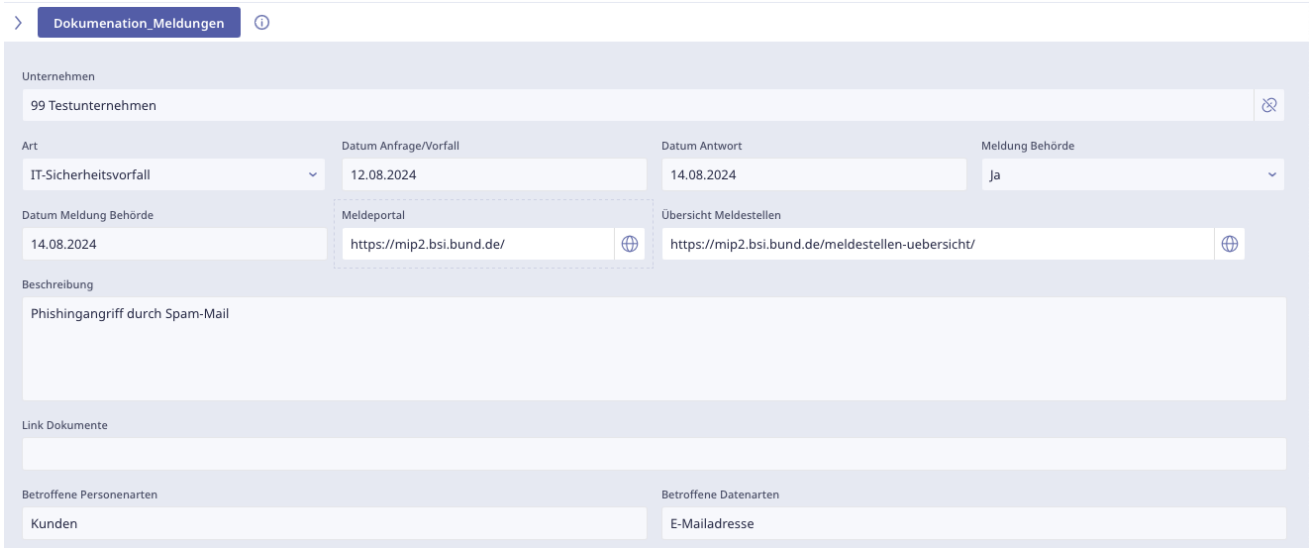
Die Leistungsfähigkeit des ISMS im Hinblick auf die Erreichung der definierten Sicherheitsziele wird analysiert. Dies umfasst die Überprüfung der Wirksamkeit der Sicherheitskontrollen und die Identifizierung von Verbesserungsbereichen.

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.

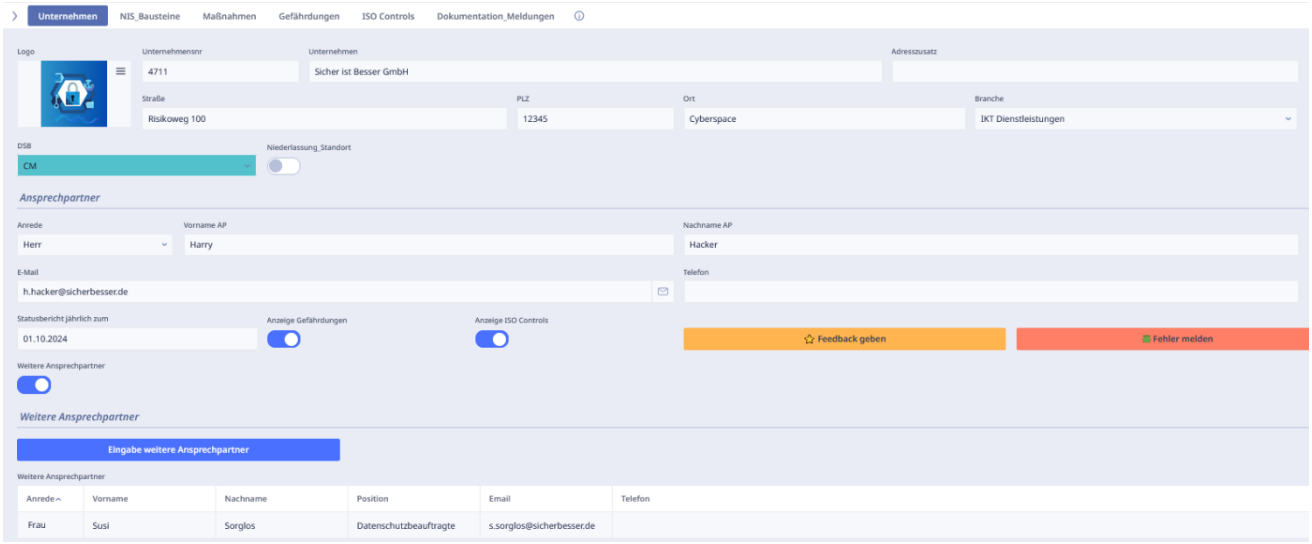
IT-Sicherheitsvorfälle dokumentieren

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



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
- Revisionssicherheit und Backup



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: daten-schutz@mc-technik.de an uns wenden. Gern vereinbaren wir auch einen Demo-Termin.