NETHINKS
INTELLIGENTE NETZWERKLÖSUNGEN

Zuschauerfragen

Webinar Kritis/NIS-2 und WAN-Vernetzung

VoIP

Network

Web & Mail

Webinar-Reihe mit NETHINKS und Telekom

NETHINKS GmbH | Rabanusstraße 14-16 | 36037 Fulda | T +49 661 25000-0 | F +49 661 25000-49 | info@NETHINKS.com | **www.NETHINKS.com**
Ansprechpartner: Uwe Bergmann | **Stand:** Fulda, 18.03.2025

Gliederung

1 Fragen der Zuschauer

1.1 Outsourcing

Frage: Welcher Grad an Outsourcing der erforderlichen Komponenten ist aus Ihrer Sicht zulässig/sinnvoll, was muss ich in jedem Fall selbst machen?

NETHINKS: Im Prinzip kann alles durch Partner im Outsourcing erledigt werden. Wichtig ist, dass die Verantwortung immer beim Unternehmen verbleibt. Man kann durch Lieferantenmanagement einiges auffangen (Lieferantenauditierung…). Beim Lieferanten vorhandene ISO27001-Zertifikate helfen oft einzuschätzen, dass die Regeln die auch für KRITIS und NIS-2 gelten eingehalten werden.

Telekom-Security: Es gibt nichts, das nicht ausgelagert werden kann. Wichtig hierbei ist immer, dass man seine Lieferanten und Dienstleister risikobasiert kategorisiert hat und basierend auf dieser Einteilung Anforderungen diese stellt. Das kann auch im Bereich einer ISO- Zertifizierung sein. Dabei muss beachtet werden, dass nicht alle Dienstleister eine Zertifizierung anstreben können.

1.2 Dokumentation und ISR

Frage: Gibt es Empfehlungen zur Art und Weise der Dokumentation von Sicherheitsvorfällen im Incident Response System?

NETHINKS: Wir haben uns mit einem Formular und Ticketsystem geholfen, das unseren Mitarbeiterinnen und Mitarbeitern die Eingabe von Störungen und Changes ermöglicht. Die mit dem Ticket-System verbundenen Prozesse stellen sicher, dass die Meldungen in definierter Zeit und Qualität bearbeitet werden. Das Ganze ist mit unserem ISB (Informationssicherheitsbeauftragtem) abgestimmt.

Telekom-Security: Wichtig im Incidentmanagement ist, dass Incidents kategorisiert, priorisiert und eskaliert werden können. Zudem müssen diese niederschwellig von den Mitarbeitenden gemeldet werden können. Die NIS-2 und KRITIS verlangen auch, dass Incidents von Beginn an dokumentiert werden und nach Beendigung Lessons Learnt gezogen werden. Die Erfahrung zeigt, dass sich diese Anforderungen in den meisten Organisationen mit einem Ticket-System ab besten bewerkstelligen lassen.

1.3 Zusammenarbeit mit Behörden

Frage: Wie ist Ihre Erfahrung in der Zusammenarbeit mit den zuständigen Behörden?

NETHINKS: Ähnlich wie bei Datenschutzvorfällen ist zu beobachten, dass auch die Behörden sich noch sortieren müssen. Von uns gemeldete Datenschutzvorfälle (es war nicht wirklich etwas Kritisches dabei) haben teilweise sehr lang gebraucht, um beantwortet zu werden.

Telekom-Security: Die Zusammenarbeit mit den Behörden in Bezug auf NIS-2 & KRITIS verläuft meistens sehr positiv und durchaus kollegial. Vor allem das BSI ist in vielen Fällen auch als Informationsquelle hervorragend geeignet und hilft auch bei der Registrierung von Organisationen, die neu in KRITIS fallen. Im Zweifel kann man dort auch immer nachfragen.

1.4 Notfallpläne

Frage: Gehören Notfall- und Wiederanlaufpläne für verschiedene KRITIS-Sektoren zur verpflichtenden Umsetzung, wenn mein Unternehmen KRITIS-relevant ist? Wer kann bei der Erstellung solcher Pläne unterstützen?

NETHINKS: Unbedingt: Das sind zentrale Forderungen, die sowohl von KRITIS/NIS-2 als auch von der ISO27001 gefordert werden. Nur mit geübten Notfall- und Wiederanlaufplänen kann sichergestellt werden, dass Schadensereignisse abgemildert werden können.

Telekom-Security: Die Vorgaben aus NIS-2 und dem KRITIS-Regelwerk richten sich gezielt an Betreiber kritischer Infrastrukturen mit dem zentralen Ziel, die Funktionsfähigkeit essenzieller Dienstleistungen dauerhaft sicherzustellen – insbesondere auch im Krisenfall. Damit verbunden ist die Anforderung, Störungen oder Ausfälle möglichst schnell zu beheben und die Versorgung der Gesellschaft rasch wiederherzustellen. Eine solche Resilienz lässt sich nur gewährleisten, wenn geeignete Krisen- und Notfallpläne nicht nur im Vorfeld entwickelt, sondern auch regelmäßig getestet und geübt werden.

1.5 Glasfaserausbau und Kritische Infrastruktur

Frage: Hat der Glasfaserausbau aus Ihrer Sicht eine wesentliche Bedeutung für die Sicherheit Kritischer Infrastrukturen? Oder geht sich das mit anderen Infrastrukturtechnologien auch aus?

NETHINKS: Jein: Wie schon im Webinar beantwortet, kann man seine Internet-Zugänge und auch WAN-Vernetzung auf Breitband-Produkten, wie es der FTTH-Ausbau ist, abstützen. Man muss im Einzelfall bewerten, ob damit die benötigte Verfügbarkeit sichergestellt werden kann. Die Einrichtung redundanter Anbindungen (Stichwort: Kanten- und Knotendisjunkt) ist mit Breitbandprodukten in der Regel nicht möglich.

1.6 Neue Bedrohungen

Frage: Wo sehen Sie welche neuen Bedrohungen für kritische Infrastruktur, auf die wir uns mittel- und langfristig vorbereiten müssen/können?

NETHINKS: Wir befinden uns politisch in einer sehr interessanten Phase. Kriegerische Auseinandersetzungen scheinen nicht mehr ausgeschlossen zu sein und speziell Cyber-Vorfälle, deren Ursache bei (fremd)-staatlichen Organisationen zu suchen ist, nehmen zu. Das ist zum einen stärker in den Fokus zu nehmen, zusätzlich sollte man aber auch das ganze Thema Automatisierung betrachten. Je höher die Automatisierung in einem Unternehmen, um so anfälliger gegen Störungen wird das Ganze. Meines Erachtens sollten man die Komplexität der Systeme als kritisches Element im Auge behalten.

Telekom-Security: Als Deutsche Telekom AG sind wir selbst Betreiber kritischer Infrastrukturen in Deutschland und beobachten seit einigen Jahren einen deutlichen Anstieg von Cyberangriffen auf unsere Systeme. Wie hier zu sehen: www.sicherheitstacho.eu Dieser Trend wird sich in den kommenden Jahren weiter verstärken – und zunehmend auch mittelständische Unternehmen betreffen. Die Annahme, als kleiner oder weniger prominenter Akteur kein Angriffsziel zu sein, ist längst überholt. Angriffe erfolgen heute zunehmend automatisiert, wobei Schwachstellen in IT-Systemen unabhängig von der Unternehmensgröße ausgenutzt werden können – mit potenziell gravierenden Folgen.

1.7 Registrierung als KRITIS-Unternehmen

Frage: Registrierung: muss ich meine Firma bei einer Behörde registrieren oder ist gemeint, dass ich selbst für mein Unternehmen herausfinden muss, ob meine Organisation KRITIS-betroffen ist?

Telekom-Security: Zur Registrierung gehört auch immer die Selbstidentifikation. Das heißt man muss als erstes im Unternehmen selbst prüfen, ob man über die Schwellenwerte fällt, die in der KRITIS-VO festgelegt sind. Kommt man in einem Kalenderjahr über diese Werte, muss man sich im folgenden Kalenderjahr bis 1. April als Betreiber einer kritischen Anlage registrieren. Hier der Link zur Verordnung: https://www.gesetze-im-internet.de/bsi-kritisv/ Die Registrierung kann hier durchgeführt werden: https://mip2.bsi.bund.de/de/

1.8 Ressourceneinsatz

Frage: Wie viele Ressourcen muss ich für die Einführung einplanen, welche Mischung intern/extern ist sinnvoll?

Telekom-Security: Die benötigten Ressourcen lassen sich nicht pauschal beziffern, da sie stark von der individuellen Ausgangslage Ihres Unternehmens abhängen – insbesondere davon, welche Strukturen, Prozesse und Kompetenzen bereits vorhanden sind. Grundsätzlich hat sich eine Kombination aus internen Ressourcen und externer Beratung bewährt. Gerade im mittelständischen Umfeld fehlen häufig Kapazitäten oder spezifisches Know-how, etwa zur Erstellung von Richtlinien oder zur Ausgestaltung eines ISMS.
Gerne erarbeiten wir gemeinsam mit Ihnen in einem persönlichen Gespräch ein unverbindliches, auf Ihre Anforderungen abgestimmtes Angebot inklusive einer Ressourcenschätzung.

1.9 Dauer, um KRITIS-Konform zu werden

Frage: Als kleinerer deutscher Versorger, wann empfehlen Sie mir spätestens mit dem Thema KRITIS/NIS zu starten? Wie lange wird es dauern, um Compliance zu erreichen?

Telekom-Security: Gerade für kleinere und mittelständische Versorger besteht die größte Herausforderung darin, von informellen Strukturen und gewachsenen Abläufen hin zu einer prozess- und risikoorientierten Organisation zu wechseln. NIS-2 legt dabei besonderen Wert auf systematische, dokumentierte Risikomanagementprozesse – ein Wandel, der nicht nur technische, sondern auch kulturelle Veränderungen im Unternehmen mit sich bringt.
Aus unserer Erfahrung empfiehlt es sich, möglichst frühzeitig mit der Vorbereitung zu beginnen. Die Einführung entsprechender Strukturen und das Etablieren eines gelebten Sicherheitsbewusstseins benötigen Zeit – insbesondere, wenn organisatorische Veränderungen nachhaltig verankert werden sollen.

1.10 Delegierung der Verantwortung?

Frage: Ist es zulässig, die Meldepflicht an das BSI an einen externen Dienstleister auszulagern? Wer übernimmt in diesem Fall die Verantwortung?

NETHINKS: Die Verantwortung liegt immer beim Unternehmen. Die kann man nicht delegieren. Dennoch ist die Zusammenarbeit mit Dienstleistern/Spezialisten durchaus hilfreich.

Telekom-Security: Ja, die operative Umsetzung der Meldepflicht – also etwa die technische Ausarbeitung und Übermittlung von Meldungen – kann an einen externen Dienstleister übertragen werden. Die Verantwortung dafür bleibt jedoch in jedem Fall beim Unternehmen selbst und ist nicht delegierbar.
Besonders hervorzuheben ist, dass die NIS-2-Richtlinie eine Erstmeldung innerhalb von 24 Stunden nach Kenntnisnahme eines sicherheitsrelevanten Vorfalls vorschreibt. Dieser enge Zeitrahmen stellt hohe Anforderungen an die internen Abstimmungs- und Entscheidungsprozesse. Wird ein externer Partner eingebunden, sind klare Zuständigkeiten und gut abgestimmte Prozesse essenziell, um Verzögerungen zu vermeiden.