IT-Notfallmanagement

Must-have für NIS2

Pragmatisches IT-Notfallmanagement für umfassende Security

adlon
Empowering Business with IT

Für den Ernstfall vorbereiten - NIS2 im Blick

Ein Notfall kann durch unterschiedliche Ereignisse in einem Unternehmen auftreten. Zu gemeinhin bekannten Notfällen wie Naturkatastrophen, Bränden oder Personalausfällen reihen sich in der heutigen Zeit verstärkt IT-bezogene Notfälle. Denn in einer immer mehr vernetzten und digitalisierten Arbeitswelt bildet die IT das Rückgrat eines gesamten Unternehmens. Wird diese angegriffen, etwa durch eine Ransomware-Attacke, führt dies zu betrieblichen Ausfällen bis hin zur existenziellen Bedrohung. Kein Wunder, dass die neue europäische Network-and-Security-Richtlinie 2.0 - kurz NIS-2 - auch ein IT-Notfallmanagement vorschreibt.

Befeuert durch NIS2 sind IT-Verantwortliche mehr denn je gefordert, ihr Unternehmen und ihre Systeme vor Angriffen zu schützen. Dazu gehören zum einen umfassende IT-Security-Maßnahmen und die Einrichtung eines Risikomanagements. Zum anderen gilt es, sich für den Ernstfall vorzubereiten - Stichwort Notfallmanagement. Denn trotz umfassender IT-Security-Vorkehrungen kann der Ausfall eines IT-Systems, eines Rechenzentrums oder zentraler Hardware-Komponenten nie ausgeschlossen werden. „Grundsätzlich braucht jedes Unternehmen ein IT-Notfallmanagement. Wer auch im Notfall überleben will - oder muss- , der kommt an einer Notfallplanung nicht vorbei. Durch die neue NIS2-Richtlinie der EU müssen viele Unternehmen in Sachen IT-Notfallmanagement und Risikomanagement jetzt den Turbo einschalten," weiß Sven Hillebrecht, General Manager und ISMB der ADLON.

Daher betrachten wir im Folgenden:

- Was umfasst das Notfallmanagement?
- Wie erstellt man einen Notfallplan und wie sieht ein solcher aus?
- Warum lohnt sich gerade eine pragmatische Vorgehensweise? Auf was ist bei der Umsetzung zu achten?
- Welche Maßnahmen sind präventiv notwendig?

> **Nur mit einem effektiven Notfallmanagement können Unternehmen während und nach eines Notfalls ihren Geschäftsbetrieb und ihre Existenz sicherstellen.**
> Sven Hillebrecht, General Manager & ISMB ADLON

Einstieg ins Notfallmanagement

Das Notfallmanagement (auch Business Continuity Management) ist Bestandteil von Informationssicherheit in einem Unternehmen. Mit ISO 22301 sind die Anforderungen an die Planung, den strukturierten Aufbau, die Implementierung, Überwachung und Verbesserung des Notfallmanagements spezifiziert. Das Notfallmanagement soll die Kontinuität des Geschäftsbetriebs bei Notfällen jeglicher Art sicherstellen. Durch planvolles und vorbereitetes Handeln auf Basis eines ausgearbeiteten Notfallplans soll angemessen auf Störungen reagiert werden. Das Ziel: kritische Geschäftsprozesse aufrechterhalten oder wiederherstellen. Schäden sollen trotz gravierender Unterbrechungen so gering wie möglich gehalten werden.

Beim Einstieg in das Notfallmanagement stehen IT-Verantwortliche schnell vor der Frage: Für welche Bereiche und Szenarien wird ein Notfallplan überhaupt benötigt? Häufige Bereiche sind:

- Endgeräte
- Hardware
- IT-Systeme und Applikationen
- Cloud-Services
- Internes Rechenzentrum
- …

Die Frage, für welche Bereiche ein Notfallplan erstellt werden muss, ist unternehmensindividuell zu beantworten. Grundlage bildet jedoch immer eine Business Impact Analyse. Diese gibt Aufschluss darüber, welche Prozesse und Ressourcen besonders abzusichern sind, damit ein Unternehmen auch im Notfall ihre fundamentale Geschäftstätigkeit aufrecht erhalten kann. Die Bewertung erfolgt anhand der Schwere der zu erwartenden Schäden eines Notfalls (z. B. finanziell, Auswirkung auf Kunden, Image, etc.) sowie der Kritikalität des Geschäftsprozesses.

Perfekt für den Notfall gerüstet mit einem Notfallplan

Nach der Identifikation und Bewertung der geschäftskritischsten Prozesse durch die Business Impact Analyse gilt es, einen Notfallplan zu erstellen. Eine der häufigsten Anwendungsfälle ist beispielsweise die Frage, wie prozessrelevante Datenbestände nach einer Ransomware-Attacke wieder zum Laufen gebracht werden.

Ein Notfallplan beschreibt zum einen die konkreten Abläufe und Sofort-Maßnahmen bei Eintritt eines Notfalls. Zum anderen werden hier die zur Wiederherstellung eines Ausfalls benötigten Ressourcen und Schritte sowie zeitlichen Rahmenbedingungen spezifiziert. **Ein Notfallplan ist klar strukturiert aufgebaut, verständlich und auch für Dritte leicht zu befolgen. Damit im Ernstfall jeder weiß, was zu tun ist.**

Die Erstellung eines Notfallplans erfordert eine enge Zusammenarbeit zwischen IT, Geschäftsleitung und den betroffenen Fachabteilungen. Daneben ist auch der Kommunikationsmanager hinzuzuziehen, der das Thema der Öffentlichkeitsarbeit betreut. Je nachdem, in welchem Bereich ein Notfallplan erstellt wird, sollten auch Partner und Dienstleister sowie Rechtsberater bei der Erstellung mitwirken. Zusätzlich muss für jeden Notfallplan ein Wiederherstellungsmanager (z. B. CIO, CEO) und ein Krisenstab benannt werden. Dieser bildet bei Eintreten des Notfalls das zentrale Gremium und den Kreis der Wiederhersteller.

Das Entwickeln eines Notfallplans - gerade auch für NIS2 - ist komplex und erfordert in der Praxis eine Reihe von Analysen, Workshops, Abstimmungen und: Erfahrung. Um strukturiert einen effektiven Notfallplan zu erstellen, setzen die meisten Unternehmen daher auf die Zusammenarbeit mit einem erfahrenen Partner. Denn ein solider und funktionstüchtiger Notfallplan ist die Voraussetzung, den wirtschaftlichen Schaden für ein Unternehmen im Notfall so gering wie möglich zu halten.

Auszug eines IT-Notfallplans

adlon
Empowering Business with IT

i. Einordnung des IT-Notfallplans
ii. Alarmierung und Eskalation
iii. IT-Sofortmaßnahmen
iv. IT-Notfall-Stab
v. Benötigte Ressourcen

Die folgenden Ressourcen werden für die Wiederherstellung eingesetzt:

Name der Ressource	Beschreibung	Menge/ Anzahl	Wann wird die Ressource benötigt	Verantwortlich für die Beschaf-fung der Ressource
Personen				
...				
Anwendungen/ Datenbanken				
...				
Daten in elektronischer Form				
z.B. Strategie für betriebliche Kontinuität und Pläne für alle Aktivitäten			z.B. innerhalb von 2 Stunden	
...				
Daten in Papierform				
...			z.B. sofort	
IT- und Kommunikations-ausstattung				
z.B. Arbeitsstationen			z.B. innerhalb von 2 Tagen	
...				

vi. Schritte zur Wiederherstellung
Die Informationen in diesem Abschnitt definieren die Tätigkeiten zur Umsetzung der Lösung/von Lösungen für die Wiederherstellung:

Wiederherrstellungs-Verfahren (wichtige Schritte/ individuelle Aufgaben)	Verantwortlicher für die Umsetzung	Kommunikation (Inhalte, an wen)	Umsetzungs-Protkoll (Datum/ Zeit)
[Bezeichnung Schritt Nr. 1]			
[Aufgabe Nr. 1.1]			
[Aufgabe Nr. 1.2]]			
...			
Bezeichnung Schritt Nr. 2			
[Aufgabe Nr. 2.1]			
[Aufgabe Nr. 2.2]			
...			

vii. Überführung in den Normalbetrieb
viii. Notfallübungen und -tests
x. Verzeichnisse

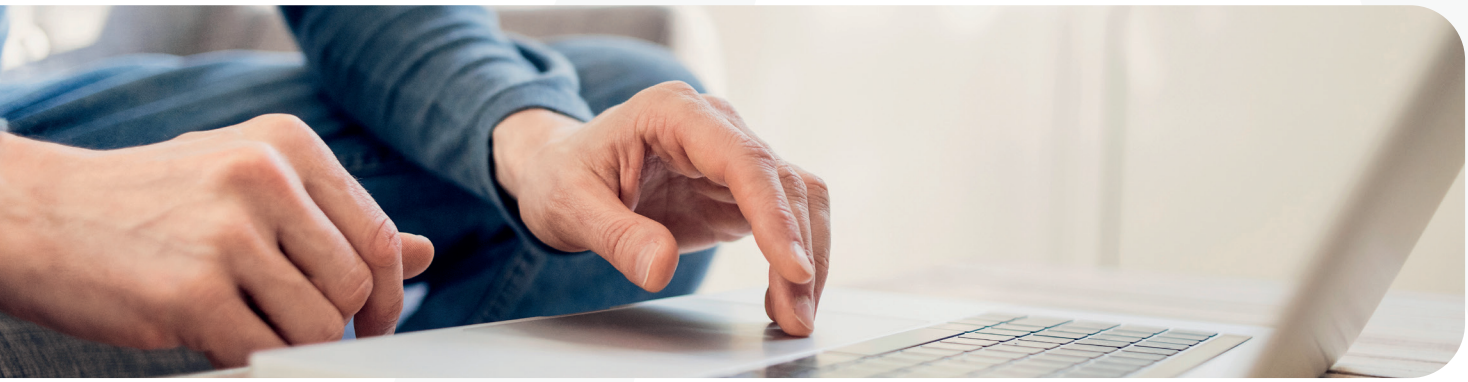
Pragmatische Vorgehensweise

Das Notfallmanagement ist komplex und sehr umfangreich. Sven Hillebrecht, General Manager und ISMB der ADLON, weiß: „Viele Unternehmen unterschätzen die Komplexität. Die Folge: Sie verzetteln sich. Entweder schon bei der Business Impact Analyse oder spätestens bei der Ausarbeitung des Notfallplans."

Vor diesem Hintergrund lohnt es sich, klare Prioritäten auf Basis der Business Impact Analyse abzuleiten und das Notfallmanagement Schritt für Schritt umzusetzen. „**Ich nenne das das „Puzzle-Notfallmanagement"**: Arbeiten Sie nicht einen riesigen Notfallplan aus, der alle Eventualitäten abdeckt. Machen Sie das komplexe Thema umsetzbar - das bedeutet: Arbeiten Sie zunächst einen kompakten Notfallplan aus für einen konkreten Notfall - beispielsweise den Ausfall des ERP-Systems. Unter der Voraussetzung, dass alles, außer das ERP System läuft. Ist dieser Plan erstellt, dann arbeiten Sie den nächsten Plan aus, z. B. einen Hardware-Notfallplan. Das führen Sie so lange weiter, bis für die wichtigsten Bereiche Notfallpläne vorliegen. Und diese können, je nach Notfalllage, dann flexibel miteinander zur Anwendung kommen."

> **Ein Notfallplan darf nicht nur ein Dokument sein, das in der Schublade verschwindet. Es muss regelmäßig durchgespielt, erprobt und angepasst werden.**
>
> Sven Hillebrecht, General Manager & ISMB ADLON

Beim Notfallmanagement ist auf ein pragmatisches und praxisnahes Vorgehen zu achten. Doch: Der Aufwand ist und bleibt hoch und die Zeit durch NIS2 knapp. Unterstützung und Sparring erhalten Unternehmen hierbei durch die Zusammenarbeit mit einem externen, erfahrenen Partner. Das lohnt sich, denn gerade in Sachen Notfallmanagement sollte nichts dem Zufall überlassen und allen NIS2-Anforderungen unbedingt Genüge getan werden. Fachwissen, Erfahrung und Informationssicherheits-Expertise spielen bei der Auswahl des geeigneten Partners eine große Rolle.



Weitere Anforderungen durch NIS2

Ein solides Notfallmanagement im IT-Bereich ist existenziell für jedes Unternehmen. Daneben erfordert NIS2 u.a. auch die Einrichtung eines Risikomanagements sowie regelmäßige Risikoanalysen. Apropos Risiken: Zu den häufigsten IT-Sicherheitsrisiken gehören heute - neben Ransomware-Attacken - Denial of Service-Angriffe, Supply-Chain-Attacken, Social-Engineering-Angriffe sowie Schwachstellen in Cloud-Diensten und IoT-Geräten.

Daher ist besonderer Fokus zu legen auf den:

- Schutz der Endgeräte
- Schutz der Identitäten und Konten
- Schutz der Kommunikation
- Schutz der Cloud Apps

Zum präventiven Schutz ist der Einsatz entsprechender Security-Technologien unabdingbar. Zu den im Markt führendsten Technologien gehören die Security-Tools von Microsoft. Darunter Defender for Endpoint, Defender for Identity, Defender for Office 365, Defender for Cloud Apps und Identity Protection.

Microsoft bietet mit seinen Technologien einen soliden Werkzeugkasten. Doch was viele Unternehmen bis heute unterschätzen: Für umfassenden Schutz reichen Technologien alleine nicht aus. Es bedarf eines aktiven Monitorings der Tools, einer schnellen Reaktion auf Alerts und Vorfälle sowie einer kontinuierlichen Betreuung und technologischen Weiterentwicklung. Das erfordert umfangreiches Know-how, ständige Weiterbildungen und umfassende personelle Kapazitäten - unabhängig von Urlaubszeiten und Personalengpässen.

Daher setzen immer mehr Unternehmen auf ein Managed SOC. Ein solches Security Operations Center (kurz SOC) beschreibt ein externes Team von Cyber-Sicherheitsexperten, welches die gesamte IT-Umgebung rund um die Uhr überwacht. Sven Hillebrecht: „Zur Minimierung relevanter Risiken gibt es Partner, die sich um die IT-Security ganzheitlich kümmern. ADLON setzt die gesamte Palette an Möglichkeiten ein, die Microsoft bietet."

> **Nach unserer Haltung „Security First" liegt es in unserer DNA, unsere Kunden zu stärken und als erfahrener Managed Security Partner für eine umfassende Notfallprävention zu sorgen.**
>
> Sven Hillebrecht, General Manager & ISMB ADLON

Um umfassenden präventiven Schutz gegen IT-Notfälle zu gewährleisten, ist ein Erfolgsfaktor die Zusammenarbeit mit einem Managed Security Service Provider (MSSP). Bei der Wahl ist darauf zu achten, dass der Partner Microsoft 365 Know-how mit Workplace Security-Expertise, ISMS-Fachwissen und Notfallmanagement-Kompetenz vereint. Und mit intelligenten Automatisierungen arbeitet, um auch die Kosten des Security Operations Centers so gering wie möglich zu halten.

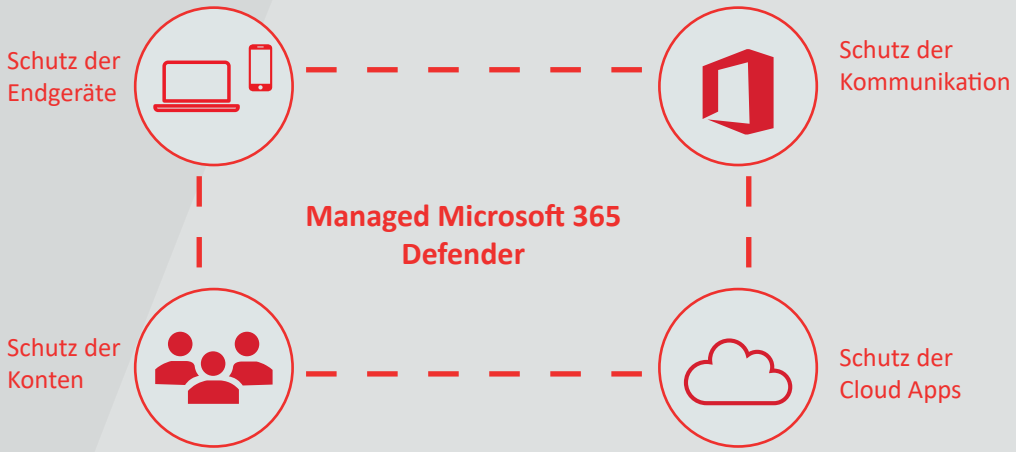
ADLON Managed Microsoft 365 Defender:

Rundum sicher, rundum sorglos!
Mit intelligenten Automatisierungen Kosten sparen und 24/7 für höchste Security sorgen

Einen ganzheitlichen Rundumschutz am digitalen Arbeitsplatz bietet ADLON mit dem Security Operations Service Managed Microsoft 365 Defender. Ein zertifiziertes Security-Expertenteam überwacht, managed und schützt dabei rund um die Uhr die:

- Endgeräte
- Identitäten und Konten
- Kommunikation
- Cloud Apps

Zudem kommen intelligente Automatisierungen ins Spiel. Mit diesem Komplettpaket können Unternehmen für umfassende Sicherheit an ihrem Microsoft 365-Arbeitsplatz sorgen - unabhängig von Ressourcen- und Personalengpässen. Und das Ganze für einen Bruchteil eines herkömmlichen Managed Security Operations Centers.



Mit dem ADLON Managed Microsoft 365 Defender-Service reduzieren Unternehmen so nicht nur Ihre IT-Sicherheitsrisiken, sondern auch kontinuierlich die Wahrscheinlichkeit für das Eintreten betrieblicher Ausfälle und IT-Notfälle. Zudem wissen Sie mit ADLON einen erfahrenen Security-Partner an Ihrer Seite, mit dem Sie nicht nur von hoher Expertise und schneller Reaktion profitieren, sondern auch von individueller Zusammenarbeit auf Augenhöhe.

Mehr Informationen finden Sie unter:
https://adlon.de/services/managed-workplace/managed-microsoft-365-defender/

Oder kontaktieren Sie uns direkt:
Tanja Loos - Sales Expert Digital Workplace | +49 751 7607-794 | Tanja.Loos@adlon.de

Prävention statt Krise

Die neue EU-Richtlinie NIS2 fördert und fordert Cybersicherheit auf breiter Ebene. Ein wichtiger Schritt, denn jedes Unternehmen, egal welcher Größe, kann schon morgen angegriffen werden und sich in einer akuten Notfallsituation befinden. Entscheidend ist, sich bestmöglich vorzubereiten. Und bei alldem Krise und neue Richtlinien als Chance und produktiven Zustand zu verstehen. Für umfassende IT-Security legen wir Ihnen drei Dinge ans Herz:

1. Bereiten Sie sich auf den Ernstfall vor und etablieren Sie ein solides Notfallmanagement. Bewährt hat sich hierbei ein pragmatisches, praxisnahes und schrittweises Vorgehen gemeinsam mit einem externen Partner.

2. Denken Sie nicht nur an den Notfall, sondern sorgen Sie für umfassende präventive Maßnahmen. Sichern Sie Ihre IT ganzheitlich mit einem erfahrenen Managed Security-Partner ab. Bauen Sie damit ein stabiles Security-Fundament auf.

3. Richten Sie ein soldies und gleichzeitig pragmatisches Risikomanagement ein. Führen Sie regelmäßige Risikoanalysen durch, achten Sie auf die Dokumentation und setzen Sie auf eine smarte digitale Tool-Unterstützung. In der Praxis bewährt sich hierbei vor allem ein Risikomanagement Cockpit basierend auf den M365-Bordmitteln. Mehr Informationen unter: adlon.de/loesungen/informationssicherheit/risikomanagement/

Gehen Sie jetzt die Themen Security, Risikomanagement und NIS2 an!

Kontaktieren Sie uns!

Tanja Loos
Head of Sales, Digital Workplace
+49 751 7607-794
Tanja.Loos@adlon.de

Sven Hillebrecht
General Manager und ISMB
+49 751 7607-731
Sven.Hillebrecht@adlon.de