RIEDEL Enterprise Defense

Choose R.E.D. to Protect

PRODUCT SHEET

RIEDEL

Was ist RIEDEL Enterprise Defense?

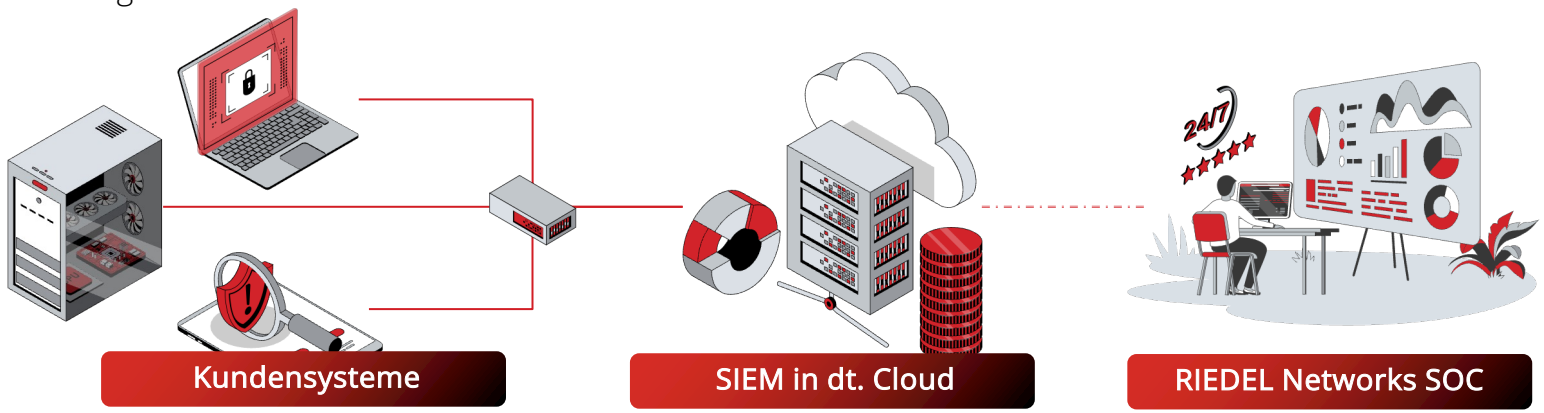
Machen Sie Ihr Unternehmen startklar für die NIS2-Richtlinie

Die Lösung im Überblick

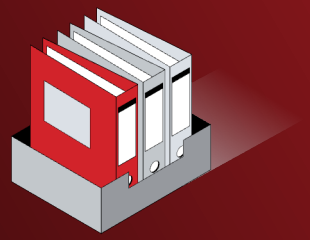
Mit **R**IEDEL **E**nterprise **D**efense (R.E.D.) stellen Sie sich und Ihr Unternehmen zukunftssicher im Bereich Cyber Security auf. R.E.D. führt eine Vielzahl von Technologien und Systemen zusammen, die für die erfolgreiche **Erkennung, Abwehr und Prävention von Cyber-Angriffen** erforderlich sind. Der **24/7 Managed Service** umfasst alle Aspekte der Schwachstellen- und Bedrohungsanalyse, des aktiven Schutzes gegen gezielte Angriffsversuche und folgende Präventionsmaßnahmen. All dies wird über das Security Operations Center (SOC) proaktiv überwacht und für den Kunden nachvollziehbar bereitgestellt.

Über die NIS2-Richtlinie

Die NIS2-Richtlinie ist eine EU-weite Gesetzgebung zur Netzwerk- und Informationssicherheit. Das Ziel: die Cyber-Sicherheit von Unternehmen stärken und ein einheitlich hohes Sicherheitsniveau in der EU sicherstellen. Dabei steht jedes Unternehmen selbst in der Pflicht zu beurteilen, ob es von der Network and Information Security-Richtlinie (kurz NIS2) betroffen ist. Entscheidend ist vor allem die Art der Geschäftstätigkeit in der EU. Insgesamt sind 18 Sektoren von der NIS2-Richtlinie betroffen.



Logs aller Devices werden aggregiert und vom RIEDEL Networks Security Operation Center (SOC) 24/7 überwacht. Schwachstellen werden geräteübergreifend analysiert und alle Vorgänge im Kundensystem proaktiv aufgezeichnet.



18. Oktober 2024

Stichtag zur Umsetzung der NIS2-Richtlinie.

RIEDEL

NIS2-RL als Security-Treiber

Es drohen Bußgelder in Millionenhöhe – zusätzlich zu möglichen Ausfallkosten

Betroffene Sektoren

Unternehmen der folgenden Sektoren fallen unter die neue NIS2-RL und sind gesetzlich zur Umsetzung spezifischer Cyber-Security Vorkehrungen verpflichtet:

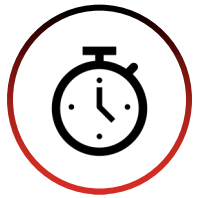
Energie, Verkehr / Transport, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Digitale Infrastruktur, Abfallbewirtschaftung, Produktion / Herstellung / Handel mit chemischen Stoffen sowie Produktion / Verarbeitung / Vertrieb von Lebensmitteln. Zudem Trinkwasser, Abwasser, Verwaltung von IKT-Diensten (B2B), Öffentliche Verwaltung, Weltraum, Post- und Kurierdienste, Verarbeitendes Gewerbe/ Herstellung von Waren, Anbieter digitaler Dienste und Forschung.

Weitere Unternehmen im Fokus

Zusätzlich sind nun auch die Unternehmen neu betroffen, die wesentliche Dienstleistungen oder Produkte im Zusammenhang mit den von NIS2 betroffenen Sektoren erbringen. Als Schwellenwert in puncto Unternehmensgröße gilt eine Beschäftigtenzahl von mehr als 50 Mitarbeitern oder wenn der Jahresumsatz 10 Millionen Euro erreicht bzw. überschreitet. Die Verantwortung zur Umsetzung der NIS2 liegt dabei beim Management und der Geschäftsführung, die bei Verstößen auch persönlich haftet.

EU-weite Gesetzgebung zur Netzwerk- und Informationssicherheit

Finanzielles Risiko durch Bußgelder in Millionenhöhe und Rechenschaftspflicht



Unwissenheit schützt nicht vor Strafe – Berichtspflichten im Schadensfall von 24 Stunden

Verantwortung für Umsetzung liegt bei Management & Geschäftsführung mit persönlicher Haftung

RIEDEL

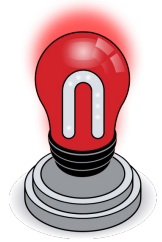
Berichtspflichten & Anforderungen

Systeme, IT-Abteilungen und Mitarbeiter – im Schadensfall muss es schnell gehen

Innerhalb von 24h ➡ Erste Meldung (Frühwarnung) an die zuständigen Behörden mit Angabe, ob der Sicherheitsvorfall evtl. auf rechtswidrige oder böswillige Handlungen zurückzuführen ist.

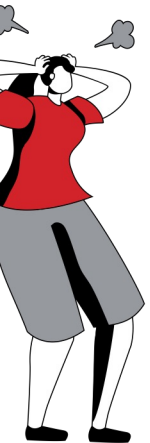
Innerhalb von 72h ➡ Ein Bericht mit den Indicators of Compromise muss an die Behörden ausgehändigt werden, der ohne dediziertes Security-Know-how zu einer fast unlösbaren Aufgabe wird.

Nach einem Monat ist ein Abschlussbericht fällig, der mindestens eine ausführliche Beschreibung des Sicherheitsvorfalls, seines Schweregrads und seiner Auswirkungen sowie Angaben zur Art der Bedrohung und den getroffenen Abhilfemaßnahmen beinhalten muss.

ALARM!  **ALARM!**

Ein Sicherheitsvorfall ist ein Ereignis, das die Informationssicherheit beeinträchtigt. Der Vorfall gefährdet die Vertraulichkeit, Verfügbarkeit oder Integrität der Daten, IT-Anwendungen, IT-Systeme oder IT-Dienste.

Es reicht aus, dass eines der Schutzziele Vertraulichkeit, Verfügbarkeit oder Integrität verletzt wird, damit das Ereignis als Sicherheitsvorfall eingestuft wird. Durch Sicherheitsvorfälle entstehen Risiken für Unternehmen, Organisationen und Personen. Große Schäden können die Folge sein.



mangelhaft geschützte IT-Systeme

externe Angreifer

Fehlerhafte Software

Ransomware

(D)DoS

Arbeitsfehler

Unvorsichtige Mitarbeiter

u.v.m.

Cross-Site-Scripting

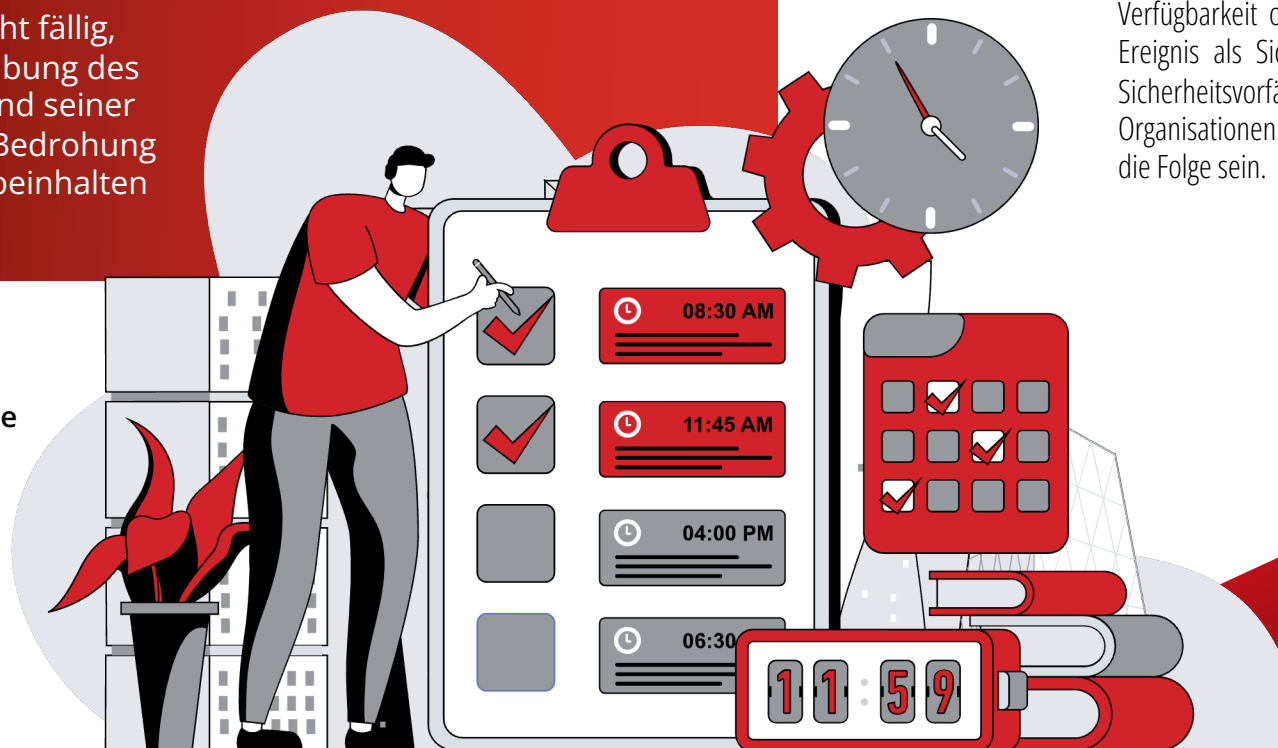
Phishing

Tail-Gating, USB-Sticks ...

Verschobene Updates

Sicherheitslücken

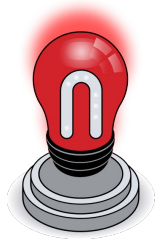
Verstöße gegen Richtlinien



RIEDEL

RIEDEL Enterprise Defense

Recht(lich) sicher unterwegs – alles aus einer Hand



Angriff erkannt!

Choose R.E.D. to Protect!

RIEDEL Enterprise Defense bezeichnet unseren bewährten **Managed** Service Ansatz im Security-Bereich. Kunden erhalten ein auf ihre Bedürfnisse angepasstes Sicherheitssetup, das im Wesentlichen die folgenden Bereiche beinhaltet:

- ✓ (D)DoS Protection
- ✓ Next Generation Firewalls
- ✓ SD-WAN
- ✓ SASE
- ✓ SIEM & SOC
- ✓ XDR (EDR+NDR)
- ✓ SOAR

Gerne erklären wir Ihnen im Detail, was hinter den einzelnen Bereichen steckt und wie das alles funktioniert.
Rufen Sie uns einfach an!

Sämtliche Bestandteile werden durch unser eigenes Security-Team aus einer Hand betreut (24/7) und können losgelöst, oder in Kombination mit bestehenden Netzwerk-Lösungen von RIEDEL Networks in Anspruch genommen werden.

Datenaggregation und Analyse aus internen und externen Quellen und Tools zur Gefahrenerkennung und -abwehr.

Allianz für Cyber-Sicherheit

Unsere Sicherheits-Suite enthält zahlreiche Informationen, Tools und Funktionen, die auch von Angreifern (Crackern, umgangssprachlich Hacker) genutzt werden. Im Bereich Cybersecurity spricht man bei der Gruppe der Angreifer vom sogenannten RED-Team. Unsere Lösung beinhaltet sowohl gängige Funktionen und Abläufe seitens klassischer Verteidigungsteams (BLUE), wird aber durch explizite Insights bestehender Angriffs-Module erweitert und bietet so einen umfangreicheren Schutz.

RIEDEL

RIEDEL Enterprise Defense

Governance, Risk & Compliance – Hier hört der Spaß auf

Klassifizierungsabschnitte

RIEDEL Enterprise Defense verfügt über die folgenden Standard-Klassifizierungsabschnitte und Unterabschnitte, auf die Sie zugreifen können, um die von den Ereignissen generierten Informationen zu überprüfen.

Cybersecurity – Packen Sie das Thema an. Jetzt!
Governance, Risk, Compliance

Security Information Management

• Security Events • Integrity monitoring • Office 365 • Amazon AWS • Google Cloud Platform • Github

Threat Detection and Response

• Vulnerabilities • Mitre ATT&CK • VirusTotal • Docker listener

Auditing and Policy monitoring

• Policy monitoring • System auditing • Security configuration assessment • OpenSCAP • CIS-CAT

Regulatory Compliance

• PCI DSS • NIST 800-53 • TSC • GDPR • HIPAA

RIEDEL

Warum RIEDEL Networks?

Choose R.E.D. to Protect

Erkennungsgrad
≥ 99,00%
nach MITRE ATT&CK

24x7 Operations

Wir sorgen für einen kontinuierlichen globalen Geschäftsbetrieb mit erfahrenen Technikern im NOC & SOC, die rund um die Uhr verfügbar sind.

alle Daten & Systeme sind in
Deutschland
gehostet

Unbegrenzt skalierbar

Modulare und widerstandsfähige Architektur mit Managed Kubernetes und Elastic, sowie automatischer Skalierung.

Verfügbarkeit
99,999% SLA
Für System & Backbone

Faires Pricing

Keine unkalkulierbare Berechnung, nicht nach Volumen (pro Mbps) und nicht nach Events per Second (EPS).

Wir sind
ACS - Mitglied
des BSI

Präventiver Support

Allen Gefahren zuvorkommen. Probleme vorhersehen, Störungen minimieren und Ihre betriebliche Leistung verbessern.

Alle 10 sec
In Echtzeit
berichtet der Endpoint an das SIEM

RIEDEL

Get in Touch

Der 18. Oktober kommt schneller, als man denkt!

RIEDEL Networks GmbH & Co. KG

RN-sales@riedel.net

+49 (0) 6033 9169 100

Nicht überzeugt? Gerne senden wir Ihnen unser Cyber Security Faule Ausreden-Quartett".

Dann unterhalten wir uns erneut.

Aufsichtsbehörde: Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Tulpenfeld 4, 53113 Bonn, Reg-Nr. 12/158

RIEDEL