ANTARES
NETLOGIX

NOTFALLMANAGEMENT

Notfälle passieren nicht. Solange man vorgesorgt hat.

Wissen Sie, wie lange Ihre IT benötigt, um nach einem Totalausfall vollständig wiederhergestellt zu werden? Und was dem Unternehmen diese Ausfallzeit kostet? Wer für den Umgang mit Ausnahmesituationen keinen Plan hat, dem drohen Chaos, lange Ausfallzeiten und finanzielle Verluste.

ANTARES NETLOGIX

Antares-NetlogiX Netzwerkberatung GmbH
Feldstraße 13, A-3300 Amstetten
T: +43 74 72 / 65 480-0 E: office@netlogix.at

www.netlogix.at

NOTFALLPLANUNG

auf Basis des BSI-Standards

Im Rechenzentrum eines Unternehmens ist es ein vorrangiges Ziel, Störfälle und Notsituationen professionell und koordiniert abzuarbeiten. **Ohne einen Plan wird es im Notfall sehr schnell stressig.** Menschen tendieren in solchen Situationen zu Aktionismus, einzelne Schnellschüsse können die Lage sogar verschlechtern.

Ein Teil- oder Komplett-Ausfall des IT-Systems kann unterschiedlichste Gründe haben: Von physischen Umständen bis zur digitalen Fremdeinwirkung. Zu den klassischen Szenarien in der Notfallprävention zählen beispielsweise:

1. TECHNISCHE URSACHEN

- Strom- bzw. Netzausfall
- Hard- und Software-Fehler

2. NATUREREIGNISSE (höhere Gewalt)

- Wasserschaden (z. B. Hochwasser)
- Brandschäden

3. DURCH MENSCHEN VERURSACHTE EREIGNISSE

- Fehler eines Anwenders bzw. Mitarbeiters
- Hackerangriffe (Ransomware, DDoS-Attacken etc.)

In der gewerblichen Luftfahrt ist es seit langer Zeit üblich, Notsituationen regelmäßig zu trainieren.

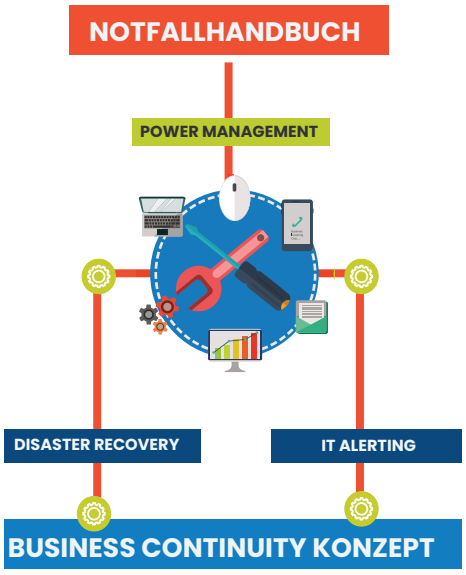
Das Ziel ist es, im Ernstfall die Situation sicher und strukturiert zu bewältigen.

Linienpiloten müssen zweimal pro Jahr im Simulator beweisen, dass sie kritische Ereignisse wie etwa den Ausfall eines Triebwerks oder Rauch im Cockpit professionell abarbeiten können.

BUSINESS CONTINUITY MANAGEMENT

Als betriebliches Kontinuitätsmanagement (engl.: BCM - Business Continuity Management) bezeichnet man die Entwicklung von Strategien, Plänen und Handlungen, um eine Organisation auf schädigende Ereignisse vorzubereiten. **Ein Notfallhandbuch ist ein wichtiges Element davon.**

Ähnlich einer Checkliste im Flugzeug bereitet man im Zuge eines BCM ein Notfallhandbuch vor. Verschiedene Notfälle werden hier in ruhigen Zeiten durchgespielt, um gut vorbereitet zu sein.



SO **FUNKTIONIERT'S**

Wir sorgen für einen 360°-Ansatz

- Wir beginnen beim **Notfallhandbuch**, übernehmen bestehende Prozesse und bilden diese ab. Zusätzlich kooperieren wir mit **IT-Fachanwälten** und setzen auf eigene **Organisations- und Projektspezialisten** sowie Security- und Netzwerkexperten. So ist ein konstanter Prozess garantiert!
- Die **Automatisierung des Notfallmanagements kann optional** erfolgen:
  - Mit **iQSol PowerApp** können die Shutdown-/Wiederanlauf-Prozeduren ermöglicht werden.
  - Die Notfallkommunikation kann über den **iQSol Alert Messaging Server** erfolgen.
  - Die vorhandene IT-Security kann mit **iQSol LogApp** konzentriert und korreliert werden.

WARUM?

Beweggründe für die Erstellung eines Notfallhandbuches

ISO 27001

Ein Notfallhandbuch ist ein wesentlicher Bestandteil eines Informationssicherheits-Managementsystems (ISMS). In der Norm ist genau definiert, wie ein solches ISMS aussehen soll:

- Ziele und Geltungsbereich formulieren
- Risiken analysieren, Risikobehandlung
- Rollen/Verantwortlichkeiten definieren
- Prozesse planen und umsetzen
- Zielerreichung überprüfen
- Verbesserung herbeiführen

Der **Anhang A** enthält einzelne Maßnahmen zur Zielerreichung.

A.5.24 Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen
A.5.25 Beurteilung und Entscheidung über Informationssicherheitsereignisse
A.5.26 Reaktion auf Informationssicherheitsvorfälle
A.5.27 Erkentnisse aus Informationssicherheitsvorfällen
A.5.28 Sammeln von Beweismaterial
A.5.29 Informationssicherheit bei Störungen
A.5.30 IKT-Bereitschaft für Business Continuity

BSI-Grundschutz (BSI-Standard 200-4):

Der BSI-Grundschutz liefert eine umfangreiche Sammlung zum Thema Notfallmanagement.

TISAX, ISA+, ISIS12 etc.:

Auch in anderen Normen (TISAX, ISA+, ISIS12 etc.) hat das Thema BCM einen festen Platz.

Gesetzliche Anforderungen (EU-DSGVO)

Artikel 32 – Sicherheit der Verarbeitung

(1) c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

(1) d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Artikel 33 - Meldung von Datenschutzverletzungen an die Behörde

Artikel 34 - Meldung von Datenschutzverletzungen an die Betroffenen

NIS2

Artikel 21 – Risikomanagementmaßnahmen im Bereich der Cybersicherheit

(2) a) Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;

(2) b) Bewältigung von Sicherheitsvorfällen;

(2) c) Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement.

Externe Anforderungen

von Kunden, Wirtschaftsprüfern, Cyber-Versicherern etc.

Abseits anerkannter Normen kann die Anforderung nach BCM auch von Kunden kommen. Immer mehr Wirtschaftsprüfer beharren beim Prüfbericht auf einem Notfallhandbuch, damit eine positive Bewertung erfolgen kann.

Qualitätssicherung & Risikomanagement im Unternehmen

Unabhängig von Normen und Standards kann ein Notfallhandbuch ein internes und freiwilliges Instrument sein, um als Unternehmen im Störfall weiter handlungsfähig zu bleiben.

MIT ANTARES IN 3 SCHRITTEN ZUM IT-NOTFALLMANAGEMENT

Wir unterstützen Sie bei der Erstellung Ihres Notfallhandbuchs

1 REIFEGRADANALYSE

Mit der Reifegradanalyse prüfen wir, ob die wichtigsten Maßnahmen für eine sichere IT umgesetzt sind – unabhängig von Firmengröße, Vorschriften und Regelwerken.

2 IT-NOTFALLHANDBUCH

Ein Notfallhandbuch ist ein wesentlicher Bestandteil eines Informationssicherheits-Managementsystems (ISMS) und dient als Leitfaden für Krisensituationen.

3 PLAYBOOKS

In unterschiedlichsten Playbooks werden die Handlungsabläufe für alle relevanten Ausnahmesituationen festgelegt.

Weitere Maßnahmen:

+ **Business-Impact-Analyse**
  Wissen Sie, welche IT-Services für Ihr Unternehmen besonders kritisch sind? Was kostet ein Ausfall von vier Stunden? Was passiert nach einem ganztägigen Ausfall? In der Business-Impact-Analyse werden die verschiedenen Szenarien monetär bewertet.
+ **Probebetrieb und Tests (z.B. Tabletop-Übungen)**
+ **Schulungen (Schulung des IT-Teams)**
+ **regelmäßige Überprüfungen**
  Wir vereinbaren regelmäßige Abstände, in denen wir das Notfallhandbuch aktualisieren. Somit steht im Notfall eine wertvolle Quelle zur Verfügung, die rasch und einfach hilft, Probleme zu lösen.
+ **Technische Folgeprojekte: z.B. Abhärtung Backup, Netzwerksegmentierung, Protokollierung**
+ **Weitere Maßnahmen**
  Besprechung strategischer Entscheidungen mit Management, Aufbau Gesamt-Notfallmanagement, Konkrete BCM-Maßnahmenplanung mit Fachbereichen, Einbindung Marketing/Öffentlichkeitsarbeit, Einbindung Datenschutz, Schulung des IT-Teams, Übungen (Tabletop)

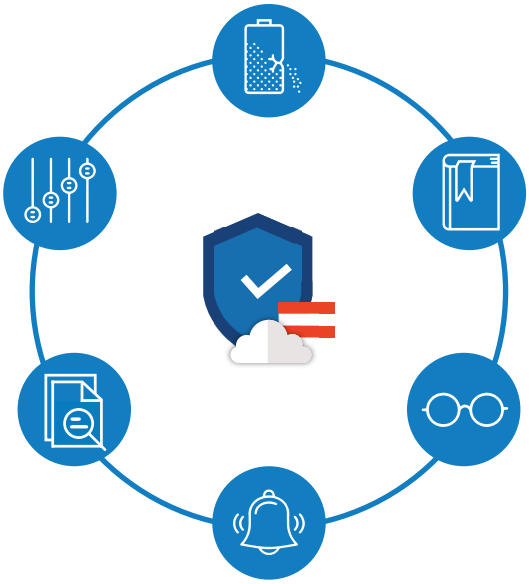
Wir bieten Ihnen eine zukunftssichere Notfallplanung

Neben den kompakten Leistungen rund um das Notfallhandbuch liefern wir weitere Dienstleistungen, die im Rahmen des Notfallhandbuchs erbracht werden können.

Reduktion der Wieder-anlaufzeit im Notfall

Zyklischer Ausbau des Notfallmanagements

Genaue Dokumentation der IT-Umgebung



Regelmäßige Risiko- und Schwachstellenanalysen
sowie laufende Kontrolle der getroffenen Vorkehrungen

Erkennung von Schwachstellen
in der Personal- oder Ablauforganisation

Simulation von Ausfällen
und der finanziellen Folgen für das Unternehmen

MUSTERHANDBUCH

auf Basis des BSI-Standards

Sie erhalten von uns entsprechende Textvorlagen, die an die jeweilige Unternehmensgröße angepasst sind.

1. Änderungshistorie
2. Einleitung
3. Konzeption
4. Notfallvorsorge
5. Notfalldefinition
6. Notfallbewältigung
7. Tests und Übungen
8. Aufrechterhaltung und kontinuierliche Verbesserung
9. Wichtige Informationen (zB Notrufnummern)

PLAYBOOK

für Incident Response Vorfälle

Folgende 6 Phasen werden im Incident Response Fall durchlaufen.

VORBEREITUNG UNTERNEHMENSNOTFALLMANAGEMENT

ABSTIMMUNG GESCHÄFTSFÜHRUNG

Strategische Schritte zum Aufbau des Unternehmensnotfallmanagements

GESAMT-NOTFALLMANAGEMENT

Organisatorischer Aufbau des Notfallmanagements mit den Fachbereichen (BSP: Produktion, Vertrieb, Finanzen, ...)

BETRIEBLICHE KONTINUITÄTSMASSNAHMEN

operative Schritte zum Aufbau eines Notbetriebes

ÖFFENTLICHKEITSARBEIT

Unterstützung beim Vorbereiten der Notfallkommunikation

RECHT/ DATENSCHUTZ

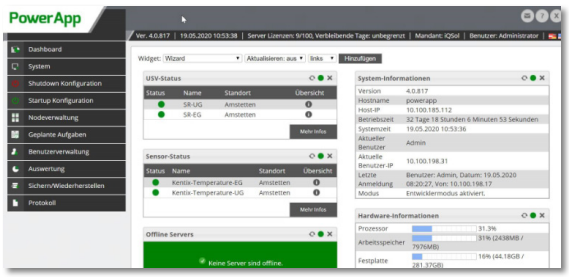
Unterstützung bei der Vorbereitung auf die org. Tätigkeiten in einem Notfall

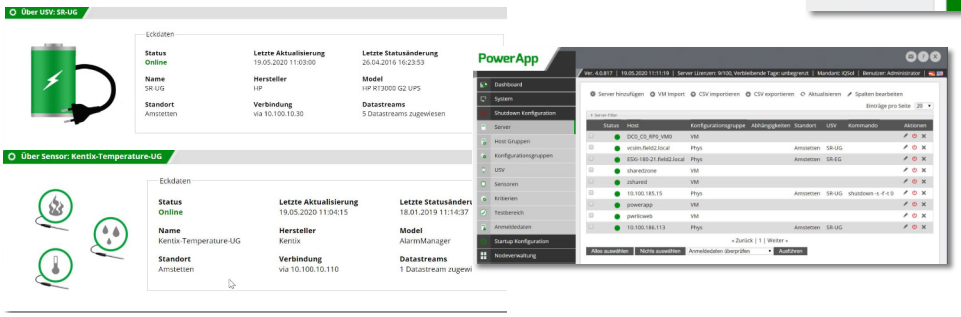
BUSINESS CONTINUITY: AUTOMATISIERUNG IN DER PRAXIS

Shutdown und Alarmierung mit iQSol

Shutdown: iQSol PowerApp

Wenn Server und Systeme vom Strom abgeschnitten werden, steht Ihre Business Continuity auf wackligen Beinen. PowerApp schützt Ihre Daten, bietet einen geordneten Server-Shutdown sowie -Restart und wahlweise die Live-Migration virtueller Systeme auf Knopfdruck.

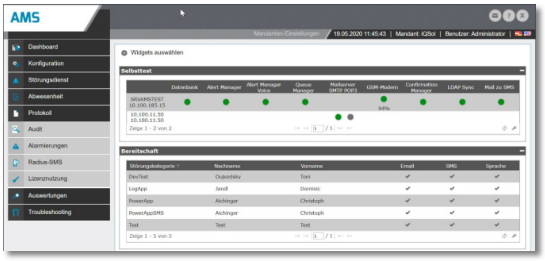




STATUS: Mittels PowerApp haben Sie immer einen aktuellen Status zu Ihren Servern und Systemen und können Ihre USV und Sensoren (Temperatur, Feuchtigkeit etc.) einbinden.

Alarmierung: iQSol Alert Messaging Server (AMS)

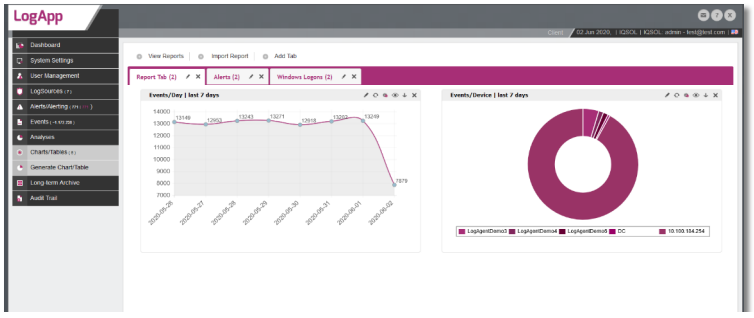
Das vollständig anpassbare Alarmierungssystem meldet, wann immer ein Fehler bzw. eine Störung auftritt oder sich gar ein Angreifer an Ihren Systemen zu schaffen macht. Die Lösung sendet Ihnen einfach eine E-Mail, eine SMS oder einen Voice-Anruf, um Sie über ungewöhnliche Aktivitäten zu informieren. Dank integrierter Dienstpläne und definierter Eskalationsprozeduren wird so jederzeit die richtige Person zum Handeln aufgefordert. Manche Kunden nutzen den AMS auch zur Zwei-Faktor-Authentifizierung.



Protokollierung: iQSol LogApp

Die LogApp bietet eine Vielzahl an Möglichkeiten, Logs von den verschiedensten Log-Quellen zu empfangen und zu verarbeiten. LogApp sammelt diese Ereignisse über LogAgents und über Syslog, normalisiert sie und wertet sie aus. Integrationsmöglichkeiten aus ERP-/CRM-Systemen und vielen weiteren Applikationen und Datenbanken erleichtern die Übersicht, wer wann und wo (un-)erlaubterweise zugegriffen hat.

Echtzeit-Reports am Dashboard



Durch die Möglichkeit, LogApps zu kaskadieren, können zahlreiche Szenarien hinsichtlich Event-Sammlung, Alarmierung und Archivierung abgebildet werden.
Sowohl die Zusammenführung aller Events der untergeordneten LogApps als auch eine selektive Weiterleitung sicherheitskritischer Events ist konfigurierbar. Alarmierungen können auf den untergeordneten oder auch nur auf der hierarchisch obersten LogApp-Ebene ausgelöst werden.

Hier erfahren Sie mehr!

iQSol
Security made in Austria.

Mehr über die iQSol-Lösungen

Alarmierung - Log Management - Power Management - Zertifikatsmanagement
www.iqsol.biz/produkte

INTEGRATION
KENTIX
Innovative Security

UMFASSENDE IT SECURITY – RUND UM DIE UHR

Managed Security Services von Antares-NetlogiX

Jetzt mehr erfahren!

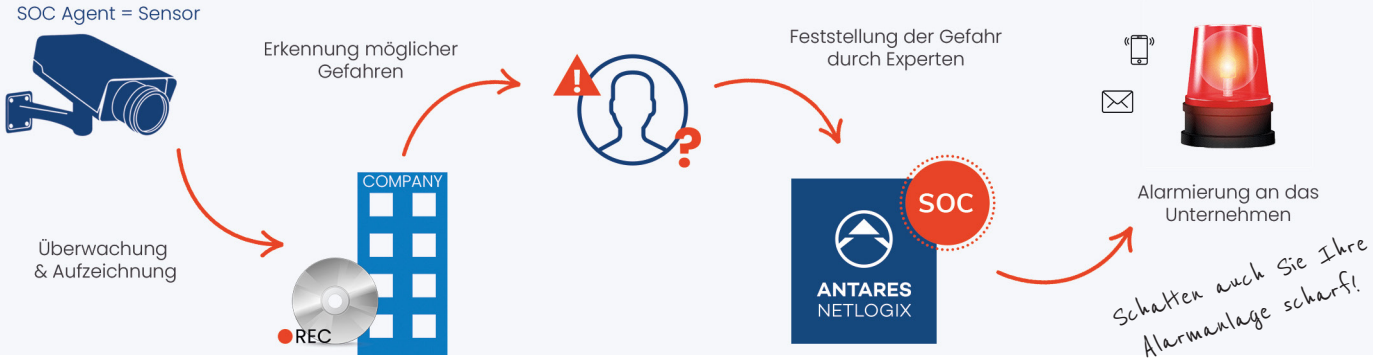
ANLX.CLOUD **24x7 SOC AS A SERVICE**

DIE ALARMANLAGE FÜR IHRE IT

Mit dem ANLX.Cloud SOC as a Service erhalten Sie eine ganzheitliche Verteidigungsstrategie und proaktive 360°-Security-Plattform – rund um die Uhr. Mit unserem Service können Sie sicher sein, dass Ihre gesamte Netzwerkumgebung von unseren Cybersecurity-Analysten kontinuierlich auf neue Bedrohungen hin überwacht wird. Reduzieren Sie Ihre Schwachstellen und erhöhen Sie Ihr Sicherheitsniveau mit hochqualifizierten Experten und im Notfall effizient funktionierenden Prozessen. Erkennen Sie Bedrohungen frühzeitig und minimieren Sie somit die Auswirkungen.

UNSER **SOC** IST DIE **ALARMANLAGE** FÜR IHRE IT – 24x7

Genauso wie ein Firmengebäude mit einer Alarmanlage geschützt ist, wird Ihre IT mit unserem Service gesichert.



Unser SOC Agent überwacht den Normalbetrieb Ihres Unternehmens und sammelt Log-Daten. Bei ungewöhnlichen Aktionen wird nicht sofort ein Alarm ausgelöst, sondern eine Analyse des Problems von unseren Experten durchgeführt. Wird tatsächlich eine Bedrohung festgestellt, erreicht Sie ein Alarm in Form eines Tickets per Mail oder als Anruf. Somit werden Fehlalarme vermieden und die Problemlösung kann sofort eingeleitet werden. Je nach Vereinbarung ergreift unser SOC-Team vorauthorisierte Sofort-Maßnahmen - damit ist Ihre IT rund um die Uhr effizient geschützt.

DAS SAGEN DIE ANLX.**EXPERTEN**

„In unserem SOC kombinieren wir auftretende Ereignisse, Software und Hardware mit Expertenwissen. So schaffen wir die Grundlage für die bestmögliche Sicherheit unserer Kunden. Wir überwachen die gesamte IT-Infrastruktur beginnend beim Client über den Server bis hin zu den Firewall-Systemen und Infrastrukturkomponenten im Netzwerk. Wir verhindern Vorfälle, indem wir auf nahezu alle Eventualitäten vorbereitet sind und im Notfall die richtigen Entscheidungen treffen."

Martin Stadler (stellv. Teamleiter Antares SOC)

IHRE **VORTEILE**

Vertrauen Sie auf unsere Expertise

- **HÖCHSTE SICHERHEIT:** Schnellere Schadensminderung mittels proaktiver Überwachung und zeitnaher Alarmierung durch unsere Cybersecurity-Analysten.
- **RASCH IMPLEMENTIERT:** Unser Know-how ermöglicht eine schnelle Integration und Einbindung Ihrer Systeme in unser Security Operations Center.
- **COMPLIANCE:** Alle sicherheitsrelevanten Ereignisse werden von uns dokumentiert und manipulationssicher archiviert. So erfüllen Sie auch Ihre Compliance-Anforderungen.

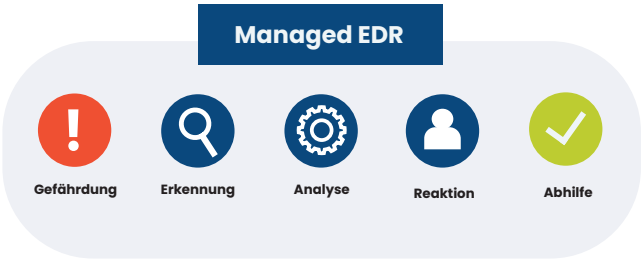
MANAGED ENDPOINT DETECTION & RESPONSE

ANLX.Cloud Managed Security Service

Genauere Infos!

Managed Endpoint Detection and Response (EDR) unterstützt Unternehmen bei der Suche nach Bedrohungen und der Reaktion auf diese, sobald sie entdeckt werden. Unser Service bietet Ihnen sowohl die Tools als auch den Zugang zu unseren Security-Analysten, welche für die **verhaltensbasierte Überwachung von Netzwerken, die Analyse von Vorfällen und die Reaktion auf Sicherheitsvorfälle zuständig sind.**

Ein oft übersehenes Problem, wenn es um Cyber-Sicherheit geht, ist die große Anzahl an Warnungen und Sicherheitsmeldungen, die IT-Teams regelmäßig erhalten. **Viele Vorgänge können nicht ohne Weiteres als bösartig identifiziert und müssen einzeln geprüft werden.** Das kann kleine Security Teams schnell überfordern.



Unsere Security-Analysten übernehmen diese Aufgabe und korrelieren die Bedrohungen, um Angriffe zeitnah zu erkennen.

IHR **VORTEIL**

kostengünstig, einfach & sicher

- Profitieren Sie von der langjährigen Erfahrung unseres Security-Teams im Bereich der Bedrohungsanalysen. Wir haben das Know-how, im Ernstfall einen Rollout innerhalb von Stunden umzusetzen.
- Unser SOC-Team ist immer up-to-date.
  Profitieren Sie von zeitnahen Informationen über aktuelle Bedrohungslagen.
- Im Krisenfall steht das Team bereit um Sie mit einem erweiterten Incident Response Service (Incident Response Koordinator, SOC EDR Service etc.) zu unterstützen.

IRGA

WWW.IRGA.AT

INCIDENT RESPONSE GROUP AUSTRIA - Die Allianz

Die IRGA ist eine Allianz von vier etablierten, hoch-spezialisierten österreichischen Unternehmen, die das gesamte Leistungsspektrum des Incident Response Managements abdeckt. Alle Mitglieder der IRGA Allianz verfügen über mehr als 20 Jahre Erfahrung im Bereich IT-Sicherheit und Verfügbarkeit. Wir begleiten Sie von der proaktiven Planung über die Eindämmung von Ransomware-Angriffen bis hin zum Wiederanlauf Ihrer IT-Infrastruktur.

INCIDENT RESPONSE KOORDINATOR. Unsere Koordinatoren sind die rechte Hand des Notfallmanagers und stehen Ihnen im Ernstfall innerhalb von 2 oder 4 Stunden zur Verfügung - rund um die Uhr. Sie sind bestens mit den Abläufen in der IT vertraut und werden laufend in der Reaktion auf Vorfälle geschult.

INCIDENT RESPONSE RETAINER. Optimierte Sicherheit: Greifen Sie rund um die Uhr auf unsere Experten für die Reaktion auf Vorfälle zurück. Vordefinierte Reaktionspläne und Kommunikationskanäle beschleunigen die Wiederherstellung nach Vorfällen. Die Retainer-Stunden können flexibel genutzt werden, das sorgt für Kostentransparenz.

ANTARES NETLOGIX | CoreTec | SCHOELLER | IT/DESIGN software projects & consulting