Dedalus

Services für mehr Sicherheit
Dedalus und r-tec

IT Security Services DACH

Cyber Security Portfolio
in Kooperation mit r-tec IT-Security GmbH

Die Cyberbedrohungslage öffentlicher Einrichtungen und insbesondere in Klinken hat in den vergangenen Jahren kontinuierlich und zuletzt drastisch zugenommen. Das Gesundheitswesen ist mittlerweile unter den Top 3 der am häufigsten angegriffenen Branchen.

Unser erweitertes Service-Portfolio mit einem starken Partner

Dedalus bietet seit langem professionelle und hochverfügbare Lösungen für den Betrieb von Dedalus-Anwendungen. Mit unseren Advanced Managed Services erhalten sie eine umfassende Betreuung ihrer Dedalus-Landschaft durch Experten, sodass Sie sich auf ihr Kerngeschäft konzentrieren können, während wir uns um die optimale Leistung und Sicherheit ihrer Systeme kümmern. Unsere Services orientieren sich an den Kriterien des Branchenspezifischen Sicherheitsstandards B3S und sind nach ISO 27001 und ISO 20000 sowie ISAE3402 zertifiziert.

Zusätzlich dazu haben sie die Möglichkeit, hochmoderne und resiliente Rechenzentrumsinfrastrukturen für ihre kritischen Anwendungen direkt von Dedalus zu erwerben. Dadurch erhalten sie nicht nur Zugang zu erstklassiger Technologie, sondern auch zu unserem Fachwissen und unserem erstklassigen Support.

Um den Schutz ihrer Patientendaten auf ein neues Level zu heben, haben wir unser Portfolio um Serviceleistungen des langjährigen und ausgewiesenen Sicherheitsspezialisten r-tec IT Security GmbH erweitert, um die Cybersicherheit für unsere Kunden weiter zu verbessern.

Umfassendes Portfolio zur Verbesserung der Cybersecurity

Wir freuen uns, Ihnen nachfolgend das gemeinsam mit r-tec entwickelte Leistungspaket vorstellen zu können, das speziell auf die Bedürfnisse von Krankenhäusern zugeschnitten ist. Unsere Lösungen sind darauf ausgerichtet, Ihnen bei der Bewältigung zentraler Sicherheitsaufgaben effektiv zur Seite zu stehen.

Unser Leistungspaket umfasst eine Vielzahl von Dienstleistungen, die sicherstellen, dass Ihre IT-Infrastruktur optimal geschützt ist. Von der eingehenden Analyse und Konzeptentwicklung bis zur Implementierung von IT-Sicherheitsmaßnahmen und der kontinuierlichen Überwachung Ihrer Systeme bieten wir Ihnen ein umfassendes Spektrum an Unterstützung.

Besonders berücksichtigen wir dabei die speziellen Anforderungen und Herausforderungen im Gesundheitswesen, einschließlich der kritischen medizinischen Geräte und deren Vernetzung. Unser Ziel ist es, Ihnen nicht nur bei der Prävention von Sicherheitsvorfällen zu helfen, sondern auch im Ernstfall schnell und effektiv zur Seite zu stehen.

Wir sind überzeugt davon, dass unsere Erfahrung und Expertise Ihnen dabei helfen können, die Sicherheit Ihrer Einrichtung zu erhöhen und gleichzeitig den reibungslosen Ablauf Ihrer täglichen Prozesse zu gewährleisten.

Was die r-tec IT-Security GmbH auszeichnet:

- Erfahrung von über 25 Jahren
- Ein Team von über 90 Experten
- Erfahrungen und Erkentnisse aus über 100 behobenen Vorfällen pro Jahr
- Zertifiziert nach ISO 27001, ISO 9001
- Erreichbarkeit rund um die Uhr 365 Tage
- Expertise im Bereich KRITIS
- Einsatz neuester Technologie – „Next Gen SIEM“
- BSI zertifizierter APT Responder

Die Services im Detail

Um einen möglichst umfassenden Schutz zu erreichen, umfassen unsere Sicherheitskonzepte Leistungen aus den Phasen Identify, Protect, Detect, Respond und Mitigate. Darüber hinausgehende Leistungen können aus dem umfangreichen Consultingportfolio von Dedalus und r-tec angeboten werden.

IDENTIFY	PROTECT	DETECT	RESPONSE	MITIGATE
• Penetration Tests • Client Check Up • Schwachstellen Scan • Webanwendungen • Awareness Veranstaltungen • Threat Information Service	• Cyber Security Check	• Managed Detection and Response	• Incident Response Readiness • Incident Response Readiness Assessment • Incident Response Playbooks • Incident Response	• System Management • Managed Firewalls • Endpoint Protection • DR Solutions

IDENTIFY

Es werden verschiedene Techniken angeboten, um Sicherheitslücken oder Schwachstellen zu identifizieren. Dabei kann die komplette Systemumgebung betrachtet werden.

Penetration Tests:
Ziel ist es, mit Pentest-Varianten verschiedene Angriffsvektoren zu prüfen sowie deren Kombinationen zu simulieren. Nur so kann die gesamte Angriffsfläche Ihres Unternehmens sichtbar gemacht und potenzielle Einfallstore identifiziert werden. Die Pentests reichen von externen Pentests auf die über das Internet erreichbare Systeme bzw. IP-Adressbereiche, über Phishing Kampanien bis hin zu Tests der Gebäudesicherheit.
Neben einzelnen Pentests, erstellen wir gemeinsam mit Ihnen den für Sie geeigneten Penetration Testplan.

Client Check-Up:
Anhand eines repräsentativen Clients werden dessen Härtungsmaßnahmen überprüft. Auf diese Weise wird das Gefährdungspotential der Clients hinsichtlich Angriffen und deren potentiellen Auswirkungen geprüft.

Schwachstellen Scan:
In diesem Arbeitspaket werden ausgewählte Systeme des Auftraggebers auf Schwachstellen und sicherheitsrelevante Fehlkonfigurationen untersucht. Es werden zunächst aktive Systeme und Dienste im Zielbereich identifiziert. Diese werden qualifiziert (Fingerprinting), um Versionsinformationen zu eingesetzten Betriebssystemen, Drittanbieter-Software sowie den bereitgestellten Netzwerkdiensten zu ermitteln.

Die Findings werden in einem Bericht zusammengefasst. Zusätzlich werden auch die Rohergebnisse und bei Dedalus Produkten Maßnahmen zur Verfügung gestellt

Webanwendungen:
Die ausgewählte Webanwendung wird nach automatisierter Analyse einer intensiven, manuellen Prüfung auf Schwachstellen und Fehlkonfigurationen unterzogen. Die Analyse findet dabei aus der Sicht eines externen Angreifers statt. Neben der Untersuchung auf Anwendungsebene wird der zugrundeliegende Webserver auf Sicherheitslücken und Konfigurationsschwächen analysiert.

Die Untersuchung von Webanwendungen basiert auf dem OWASP Testing Guide.

Awareness Veranstaltungen:
Das Bewusstsein für Cyber-Security fördern wir durch umfassende Social-Engineering Kampagne, zugeschnitten auf ihre Bedürfnisse. Im Repertoire haben wir Fortbildungen zur Steigerung des Mitarbeiterbewusstseins, Live-Hacking Veranstaltungen, sowie Schulungsprogramme.

Threat Information Service:
Mit dem Threat Information Service liefern wir Ihnen Informationen zu drohenden Cyberangriffen, zu aktuell erkannten Schwachstellen in gängigen Hardwaresystemen und Software sowie zu Zero-Day Threats. Darüber hinaus geben wir Ihnen Handlungsvorschläge und ergänzende Informationen durch Hintergrundrecherchen unserer Experten an die Hand, um Ihnen ein möglichst umfassendes Bild über die aktuelle Bedrohungslage zu bieten.

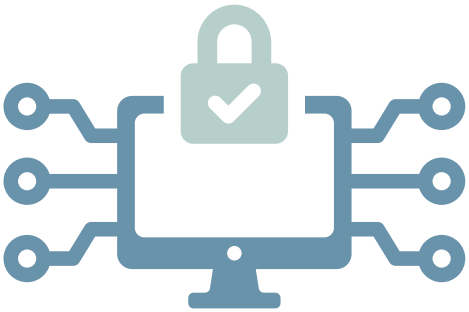
Passende Schutzmaßnahmen auswählen und implementieren

- Maßnahmen zur Erkennung von Schwachstellen und Sicherheitslücken
  - Validierung von Sicherheitsmaßnahmen
  - Compliance Überprüfung zur Erfüllung der gesetzlichen Anforderungen

PROTECT

Umfassender Schutz muss über viele Ebenen berücksichtigt werden, zur Bewältigung dieser Komplexität bieten wir einen umfassenden Cyber-Security-Check.

Cyber Security Check:
Auf Grundlage eines Cyber Security Checks ermitteln wir den Ist-Zustand Ihrer Cyber-Security-Landschaft, gleichen diesen mit dem aktuellen Stand der Technik ab und zeigen Ihnen so Potenziale und Handlungsfelder zur Verbesserung Ihrer Cyberabwehr auf. Dabei werden insbesondere branchenspezifische Vorgaben berücksichtigt. Das Ergebnis ist ein individueller, auf Ihre Anforderungen abgestimmter Cyber-Security-Plan.



DETECT

Experten überwachen Ihre IT-Umgebung rund um die Uhr, 365 Tage im Jahr, analysieren verdächtige Ereignisse, schlagen bei Angriffen Alarm und führen unmittelbar notwendige Maßnahmen zur Angriffsabwehr und Wiederherstellung des Regelbetriebs durch. Der Service aus dem DETECT beinhaltet folgende Services:

Managed Detection and Response:
Unsere Experten überwachen Ihre IT-Umgebung rund um die Uhr, 365 Tage im Jahr, analysieren verdächtige Ereignisse, schlagen bei Angriffen Alarm und führen unmittelbar notwendige Maßnahmen zur Angriffsabwehr und Wiederherstellung des Regelbetriebs durch.

LOG-Management:
Log-Dateien werden gesammelt Protokolle Ereignisdaten werden aus verschiedenen Quellen im gesamten Netzwerk analysiert und ausgewertet. Diese umfassende Protokollverwaltung ermöglicht die Erkennung von Anomalien, potenziellen Sicherheitsvorfällen und Compliance-Verstößen.

Echtzeit Überwachung:
Wir überwachen die Netzwerkaktivitäten ihres gesamten Systems in Echtzeit und ermöglichen so eine schnelle Identifizierung von verdächtigem Verhalten oder Sicherheitsvorfällen. Dieser proaktive Ansatz ermöglicht es den Sicherheitsteams, umgehend zu reagieren und die potenziellen Auswirkungen von Cyber-Bedrohungen zu minimieren.

Erkennung und Reaktion auf Vorfälle:
Das eingesetzte Next Generation SIEM verwendet fortschrittliche Korrelations- und Analysetechniken, um Muster zu erkennen, die auf Sicherheitsvorfälle hindeuten. Sobald ein Vorfall erkannt wird, generiert das System Warnmeldungen und liefert verwertbare Erkenntnisse, um eine schnelle und effektive Reaktion zu ermöglichen.

Einhaltung von Vorschriften:
Der Einsatz der Managed Detection und Response Lösung unterstützt sie bei der Einhaltung von Vorschriften, indem es Daten sammelt und analysiert, um die Einhaltung von Sicherheitsrichtlinien und Branchenvorschriften zu überprüfen. Gerade in stark regulierten Sektoren ist dies von Vorteil.

Analyse von Bedrohungsdaten:
Das Security Operations Center ist für die Analyse der Daten zuständig. Diese Informationen werden genutzt, um die Sicherheitslage zu erhöhen und potenzielle Angriffe proaktiv abzuwehren.

Untersuchung von Anomalien:
Das SOC-Team untersucht und reagiert auf Sicherheitsvorfälle, die vom eingesetzten System erkannt werden. Mit deren Fachwissen erfolgt eine gründliche Untersuchung des Vorfalls, die Identifizierung der Grundursache und die Implementierung effektiver Abhilfemaßnahmen.

Kontinuierliche Überwachung:
Mit dem SOC-Team bieten wir eine 24/7-Überwachung ihrer gesamten Systemlandschaft. Diese permanente Kontrolle ist unerlässlich, um Bedrohungen unabhängig vom Zeitpunkt ihres Auftretens sofort zu erkennen und darauf zu reagieren.

24/7 Einsatzbereitschaft:
Bei einem Vorfall steht ihnen unser einsatzerprobtes Incident Response Team zur Seite. Neben dem Expertenwissen aus der Bewältigung zahlreicher großer Angriffe profitieren Sie von modernsten Technologien der Marktführer in diesem Bereich.

Permanente Überwachung bei erhöhtem Kundenservice

- Unterstützung bei der Umsetzung durch erfahrenen Projektmanager
- Schnelle Reaktionszeiten im Falle eines Incidents
- Koordination von Maßnahmen und Kommunikation der Ergebnisse
- Einen dedizierten Ansprechpartner – zur effizienten Kommunikation

RESPONSE

Angriffen vorbereitet begegnen um den Betrieb schnell wiederherzustellen.
Bei Cyber-Security-Vorfällen, muss schnell gehandelt werden.
Mit den Incident Response Services bieten wir individuelle Pakete, um im Ernstfall sofort die richtigen Maßnahmen zu ergreifen.

Incident Response Readiness:
Die Vorbereitung auf den Ernstfall ist eine der wichtigsten Aufgaben des Security Incident Managements. Wir legen dafür die Grundlage und bauen gemeinsam mit Ihnen die Incident Response Readiness auf. So werden Sie in die Lage versetzt, effizient und effektiv auf IT-Sicherheitsvorfälle zu reagieren. Um dieses Vorhaben zu realisieren, entwickeln wir technische und organisatorische Maßnahmen, mit deren Hilfe sich identifizierte Security Incidents eindämmen und bereinigen lassen. Ziel ist es, den Normalbetrieb schnellstmöglich wiederherzustellen.

Incident Response Readiness Assessment:
Überprüfen Sie Ihre technischen und organisatorischen Response-Fähigkeiten: Durch das Incident Response Readiness Assessment erhalten Sie eine unabhängige Bewertung Ihrer bestehenden Prozesse, Abläufe und technischen Lösungen zur Erkennung und Behandlung von Sicherheitsvorfällen. Dafür nutzen unsere Experten neben internationalen Best Practices auch ihre umfangreiche Erfahrung aus abgeschlossenen Kundenvorfällen sowie fundierte Erkenntnisse zur aktuellen Bedrohungslage und zu neuen Angriffstechniken.

Incident Response Playbooks:
Wir bieten Ihnen die Möglichkeit Playbooks auf Basis unserer erprobten Vorlagen mit uns gemeinsam zu gestalten. Die ausgewählte Vorlage wird im Rahmen eines Workshops individuell an Ihre Bedürfnisse angepasst. Verfügbare Vorlagen sind u.A.: Phishing, Ransomware, Unberechtigte Zugriffe, Kompromittiertes Active Directory, Denial of Service, Datenabfluss, ...

Dedalus spezifische Incident Response Playbooks:
Auf Basis der etablierten Incident Response Playbooks, bieten wir eine spezifische Anpassung an Ihre Umgebung an. Dabei werden individuelle Systeme und Produkte der Dedalus Systemlandschaft berücksichtigt, um im Ernstfall noch zielgerichtetere Maßnahmen einleiten zu können.

Incident Response:
Mit unserem Incident Response Service stellen wir sicher, dass Ihrem Unternehmen im Ernstfall die richtigen Ressourcen und Kompetenzen zur Verfügung stehen. Sie zahlen eine feste monatliche Pauschale und wir bieten Ihnen dafür einen Bereitschaftsdienst mit garantierten Annahme- und Reaktionszeiten. Um wertvolle Zeit zu sparen führen wir im Vorfeld einen Workshop durch, um im Ernstfall optimal zusammen zu arbeiten.

MITIGATE

System Management:
Im Rahmen eines Advanced Managed Services Vertrages übernehmen wir für Sie das Patch Management der Dedalus Systemlandschaft.

Managed Firewalls:
Mittels verwalteter Firewalls wird die Dedalus Systemlandschaft von der restlichen Systemumgebung segmentiert. Dies erhöht die Resilienz gegenüber von Angriffen. Da Angriffe in der Regel über die Endpoints (PCs, Tablets, ..) stattfinden, kann durch die Segmentierung ein höherer Schutz erzielt werden.

Endpoint Protection:
Durch Dedalus verwaltete Systeme werden mittels einer Endpoint Protection geschützt. Die dort anfallenden LOG Informationen können an ein SIEM System, z.B. im Rahmen von Managed Detection and Response ausgeleitet werden.

DR Solutions:
Zu einem umfassenden Sicherheitskonzept gehört ebenfalls eine geschützte Desaster Recovery Lösung. Dedalus bietet hier verschiedene Pakete an, die je nach Anforderung Technologien wie Immutable Backup und Ransomware Schutz bieten. Zur Erfüllung der KRITIS Empfehlungen können die Vorhaltezeiten auf ein Jahr (GFS) erweitert werden und eine Kopie auf einen externen Cloud Speicher übertragen werden.

Resiliente Infrastrukturen

Die Dedalus Clinical Infrastructure Platform bietet mit ihren Security Features (CIP/SF) maximale Performance und vermeidet Abhängigkeiten, die die Stabilität oder Performance beeinträchtigen können. Mit dieser Plattform, deren Zugriffe ausschließlich über dedizierte, interne Firewalls erfolgen, werden Datenströme von und zur Dedalus CIP/SF auf das Wesentliche beschränkt und durch gängige Sicherheitsfunktionen der Firewalls auf Malware und Ransomware überprüft.

Angriffen vorbereitet begegnen, um den Betrieb schnell wiederherzustellen

- Individuell zugeschnittene Pakete für Sofortmaßnahmen im Ernstfall
- Vorbeugende Maßnahmen zur Minimierung des Risikos durch Technologien und Prozesse
- Verfahrens- und Notfallpläne zur präzisen Kommunikation
- Vollumfängliche Unterstützung in Krisensituationen

Dedalus

Dedalus HealthCare GmbH
Konrad-Zuse-Platz 1-3
53227 Bonn

dedalusgroup.de

Zugunsten einer flüssigen Lesbarkeit beziehen sich Personalbezeichnungen selbstverständlich immer auf alle Personen (m/w/d).