CYBER-SICHERHEIT

FACHKOM-PETENZ IM ÜBERBLICK

Insight

Einleitung

Cybersicherheit ist für Unternehmen jeder Größe von entscheidender Bedeutung, da die Häufigkeit und Komplexität von Cyberbedrohungen stetig zunimmt. Sicherheitsverletzungen können verheerende Folgen haben, darunter finanzielle Verluste, rechtliche Haftung,

Der Schutz Ihres Unternehmens vor Cyberbedrohungen ist nicht nur eine Frage der Compliance oder bewährter Verfahren; er ist unerlässlich, um Ihren Betrieb zu sichern und die Geschäftskontinuität zu gewährleisten.

Die Investition in robuste Cybersicherheitsmaßnahmen ist eine Investition in die zukünftige Resilienz und den Erfolg Ihres Unternehmens. Durch die Implementierung effektiver Cybersicherheitsstrategien können Sie Risiken mindern, Bedrohungen frühzeitig erkennen und darauf reagieren sowie eine starke Abwehr gegen Cyberangriffe aufbauen.

Cybersicherheit ist nicht nur eine Notwendigkeit, sondern ein strategisches Muss für Unternehmen, die in einer sicheren und widerstandsfähigen Softwareumgebung gedeihen möchten. Bei Insight verstehen wir die Bedeutung eines umfassenden Sicherheitsansatzes.

Insights Ansatz für Cybersicherheit

Cybersicherheit ist komplex und erfordert einen umfassenden Ansatz, der Endbenutzer, Sicherheitsteams und Tools einbezieht. Deshalb verfolgen wir einen ganzheitlichen Ansatz für Cybersicherheit in den Bereichen Technologie und Integration. Dieser Ansatz basiert auf wiederholbaren Methoden und bewährten Prozessen, die erfolgreiche Ergebnisse liefern. Unsere Experten begleiten Sie von Anfang bis Ende, was zu einer verbesserten Effizienz, Effektivität und strategischen Ausrichtung führt.

Das ganzheitliche Sicherheitsmodell von Insight

Insights Ansatz für Cybersicherheit

Wir verfügen über umfassende technische Kompetenzen in den fünf Technologiebereichen:

- Endpoints
- Applikationen
- Cloud
- Netzwerk, Rechenzentrum und IoT
- Datenzentrierung

Als führender Lösungsintegrator wissen wir, dass technische Exzellenz in diesen Bereichen nicht ausreicht. Sicherheit muss ganzheitlich angegangen werden, um sicherzustellen, dass alle Sicherheitsbereiche integriert und aufeinander abgestimmt sind. Dies erreichen wir durch die Anwendung von:

- Governance, Risiko & Compliance
- Identität und Zugriff
- Erkennung und Abwehr von Bedrohungen
- Menschliche Faktoren

Die Schnittstellen zwischen den Technologiedomänen bieten oft Potenzial für zusätzlichen Mehrwert, der dazu beiträgt, Ihre allgemeine Sicherheit auf kosteneffiziente Weise zu verbessern.

Wir helfen Ihnen dabei:

- Ihre Cybersecurity-Strategie zu verbessern,
- Risiken zu identifizieren und zu mindern,
- Komplexität durch Minimierung von Überschneidungen zu reduzieren,
- den Sicherheitsbetrieb zu optimieren,
- sicherzustellen, dass Sicherheitskontrollen Mehrwerte schaffen und die Rentabilität verbessern.

Die Technologie-Säulen

Endpoints

Die Zeiten, in denen ein einziges Gerät pro Benutzer in einem Unternehmen verwendet wurde, sind vorbei. Es ist sehr wahrscheinlich, dass Ihre Mitarbeiter mehrere Geräte verwenden. Endgeräte spielen eine entscheidende Rolle bei der Cybersicherheit von Unternehmen und dienen als Einstiegspunkte für Cyberbedrohungen und Schwachstellen. Die Herausforderungen bei der Sicherung von Endgeräten sind aufgrund der Verbreitung von Geräten, Remote-Arbeitsumgebungen und der zunehmenden Komplexität von Cyberangriffen auf Endgeräte gewachsen. Zu den häufigsten Herausforderungen gehören Endgeräte-Transparenz, Schwachstellenmanagement, Datenschutz und Applikationskontrolle.

Diese Geräte müssen verwaltet, ihre Sicherheit überwacht und aktualisiert sowie aktive Abwehrmaßnahmen zum Blockieren von Malware und Exploits bereitgestellt und aufrechterhalten werden. Unsere Endpoint Security Lösungen konzentrieren sich auf die Sicherung von Endgeräten wie Notebooks, Desktops, Servern und mobilen Geräten, die für den Zugriff auf Unternehmensnetzwerke und -daten verwendet werden.

Wir helfen Ihnen dabei:

- Einblick in Ihre Endgeräte auf Geräte- und Applikations-Level zu erhalten,
- Cyberbedrohungen in Echtzeit zu erkennen und darauf zu reagieren,
- sensible Daten auf Geräten vor unbefugtem Zugriff zu schützen,
- Malware-Infektionen und Cyberangriffe auf Endgeräte zu verhindern,
- Einblick in die Aktivitäten der Endgeräte für eine effektive Überwachung zu erhalten,
- Geräte für Remote-Arbeitsumgebungen zu sichern.

Applikationen

Da sich Cyberbedrohungen ständig weiterentwickeln, stehen Unternehmen vor großen Herausforderungen. Die zunehmende Komplexität moderner Anwendungen, die zahlreiche miteinander verbundene Komponenten und Integrationen von Drittanbietern umfassen, führt zu einer erweiterten Angriffsfläche. Hacker und böswillige Akteure entwickeln ständig neue Methoden, um Schwachstellen in Anwendungen auszunutzen.

Alle Unternehmen verwenden Applikationen, die regelmäßig gepatcht werden müssen, um Schwachstellen sowohl auf Endgeräten als auch in der Serverinfrastruktur zu beheben. Viele Unternehmen entwickeln auch ihre eigenen Anwendungen, sei es über Low/No Code-Plattformen oder durch traditionelle Entwicklung und DevOps. Für diese Unternehmen ist es entscheidend, Sicherheit und Datenschutz von Anfang an in den Lebenszyklus der Softwareentwicklung zu integrieren.

Unser erfahrenes Insight-Sicherheitsberatungsteam hilft Ihnen, die Risiken in Ihrer Anwendungsinfrastruktur zu reduzieren. Wir unterstützen Sie mit Schwachstellen- und Patch-Management, damit Ihre Standardanwendungen stets auf dem neuesten Stand bleiben. Zudem führen wir Penetrationstests für alle internen Webanwendungen durch.

Vertrauen Sie auf Insight, um Ihre Anwendungssicherheitsanforderungen direkt anzugehen und Ihnen zuverlässigen Schutz und Sicherheit zu bieten.

Wir helfen Ihnen dabei:

- Ihre Applikationen zu verwalten, um den Schwachstellen-und Patch-Zyklus im Blick zu behalten,
- Sicherheitskontrollen in Ihre DevOps-Prozesse zu integrieren, ohne Kompromisse bei der Entwicklungsgeschwindigkeit einzugehen,
- Bedrohungen frühzeitig zu erkennen und zu beheben, wodurch die Kosten für die Behebung gesenkt werden.

Cloud

Cloud-Computing bietet eine unübertroffene Skalierbarkeit und Wirtschaftlichkeit, stellt aber auch große Sicherheitsherausforderung dar. Unternehmen müssen ihre sensiblen Daten vor unbefugtem Zugriff, Verstößen und Sicherheitslücken schützen, gleichzeitig Vorschriften einhalten und den Ruf des Unternehmens wahren.

Ein proaktiver und risikobasierter Ansatz sowie die Zusammenarbeit mit Cloud-Providern sind notwendig, um ein solides Sicherheits-Framework zu schaffen.

Die Insight Cloud- und Sicherheitsexperten verfügen über jahrelange Erfahrung in der Erstellung, Sicherung und dem Betrieb von Multi-Cloud-Softwareumgebungen für Unternehmen jeder Größe und Komplexität. Wir entwickeln ein umfassendes Sicherheits-Framework mit proaktiver Überwachung, damit Sie sich auf Wachstum, Skalierbarkeit und Innovationen konzentrieren können.

Wir helfen Ihnen dabei:

- Transparenz in Ihrer Multi-Cloud-Softwareumgebung zu schaffen,
- Workloads zu sichern, wo immer sie generiert werden,
- die Compliance mit Sicherheits-Frameworks zu überwachen und aufrechtzuerhalten.

Sicherheit von Rechenzentren, Netzwerken und IoT

In der vernetzten Welt von heute wächst die digitale Landschaft rasant und schafft ein komplexes Technologienetzwerk, das Cyber-Bedrohungen, Daten-pannen und unbefugten Zugriffen Tür und Tor öffnet.

Ein mehrschichtiger Ansatz ist erforderlich, um die Sicherheit und Widerstandsfähigkeit moderner Unternehmen zu gewährleisten. Eine Kombination aus Firewalls, Verschlüsselung, Zugangskontrollen und regelmäßigen Sicherheitsaudits ist nur der Anfang. Mit hochentwickelten Bedrohungserkennungssystemen und Expertenanalysen müssen Sie den Bedrohungen immer einen Schritt voraus sein, um potenzielle Risiken proaktiv zu erkennen und zu mindern.

Wir beraten Sie bei der Lösung Ihrer Probleme in den Bereichen Rechenzentrums-, Netzwerk- und IoT-Sicherheit. Mit einem tiefen Verständnis von Geschäft, Technologie und Sicherheit schaffen wir die richtige Lösung für Ihr Unternehmen – von der Strategie und Planung über das Design bis hin zur Implementierung und Managed Services. Unsere Sicherheitsexperten helfen Ihnen, sich in der komplexen Technologie zurechtzufinden, die für den Aufbau und die Verwaltung effektiver Cybersicherheitsmaßnahmen erforderlich ist, um Doppelarbeit zu minimieren und eine kosteneffiziente Cybersicherheitsabwehr zu gewährleisten.

Dazu gehören z.B.:

- Transparenz in komplexen hybriden Architekturen
- Verbesserung der Betriebskontinuität
- Sicherheitskontrollen, die sowohl in Ihren On-premises- als auch Cloud-Netzwerken funktionieren
- Schützen Sie Ihre Daten von der Quelle bis zum Ziel

Datenzentrierung

Während Sicherheitsexperten viel Zeit damit verbringen, Anwendungen und Infrastrukturen abzusichern, ist die Sicherheit von Daten letztlich der Schlüssel zu fast allem, was wir tun.

Ob Mitarbeiterdaten, Kundenbestellungen, Produktionszahlen oder geistiges Eigentum - es sind die Daten, die durch Ihr Unternehmen fließen und die wahrscheinlich den größten Mehrwert für Ihre Endkunden und Ihr Unternehmen schaffen.

Daten sind ein guter Ausgangspunkt für eine ganzheitliche Sicherheitsstrategie. Ein datenzentrierter Ansatz sollte mit der Einbindung Ihrer Stakeholder im Unternehmen beginnen, nicht mit der Technologie.

Der Insight Ansatz konzentriert sich auf den Schutz der Daten und nicht nur auf die Sicherung der Systeme oder Netzwerke, die sie speichern und übertragen. Wir helfen Ihnen, immer einen Schritt voraus zu sein und das wertvollste Gut Ihres Unternehmens - Ihre Daten - effektiv zu schützen.

Dazu gehören z.B.:

- Identifizierung sensibler und veralteter Daten in Ihrem Bestand
- Unterstützung bei der Klassifizierung von Daten, um sicherzustellen, dass das richtige Kontrollniveau angewendet wird
- Einhaltung von Datenschutzbestimmungen
- Nachvollziehbarkeit der Datennutzung

Integrationsbereiche

Governance, Risiko & Compliance

Governance, Risiko und Compliance sind wesentliche Komponenten der Cybersicherheit für Unternehmen und umfassen die Richtlinien, Verfahren und Mechanismen zum Management von Cybersicherheitsrisiken und zur Sicherstellung der Einhaltung regulatorischer Anforderungen wie der DSGVO und NIS2. Unternehmen stehen vor der Herausforderung, effektive Governance-Strukturen zu schaffen, Cybersicherheitsrisiken zu identifizieren und zu bewerten sowie robuste Kontrollen zur Eindämmung von Bedrohungen zu implementieren.

Effektive GRC-Praktiken schaffen klare Rollen, optimieren Prozesse und mindern Cyberrisiken. Ein solider Ansatz erhöht den Reifegrad Ihrer Cybersicherheit, reduziert rechtliche und finanzielle Verbindlichkeiten, verbessert das Vertrauen Ihrer Kunden und die Einhaltung gesetzlicher Vorschriften. Stellen Sie sicher, dass die Sicherheit die Anforderungen Ihres Unternehmens unterstützt, ohne sie einzuschränken. Nutzen Sie Sicherheitsrisikobewertungen, um die Kosten dieses Risikos zu berechnen und zu bestimmen, wo Kontrollen am besten eingesetzt werden sollten. Stellen Sie gleichzeitig sicher, dass die von Ihnen ausgewählten Kontrollen auch wirksam sind.

Wir unterstützen Sie:

- Risikobewertung
- Definition der wirksamsten Kontrollen
- Entwicklung von Richtlinien und Prozessen
- Integrierte Experten auf allen Organisationsebenen bis hin zur CISO-Ebene

- NIS / NIS2
- DORA
- Acte EU AI
- ISO27001
- Cyber Essentials/+
- CIS18
- NIST CSF
- PCI-DSS

Identität und Zugriff

Identitäts- und Zugriffsmanagement ist ein wesentlicher Aspekt der Cybersicherheit für Unternehmen und umfasst die Prozesse und Technologien, die zur Verwaltung und Sicherung digitaler Identitäten und zur Kontrolle des Zugriffs auf Ressourcen eingesetzt werden. Unternehmen stehen vor der Herausforderung, sichere und effiziente Identitäts- und Zugriffsmanagementpraktiken zu gewährleisten, wie z. B. die Verwaltung von Benutzeridentitäten über mehrere Systeme hinweg, die Durchsetzung von Zugriffskontrollen mit geringsten Rechten und die Verhinderung unbefugten Zugriffs.

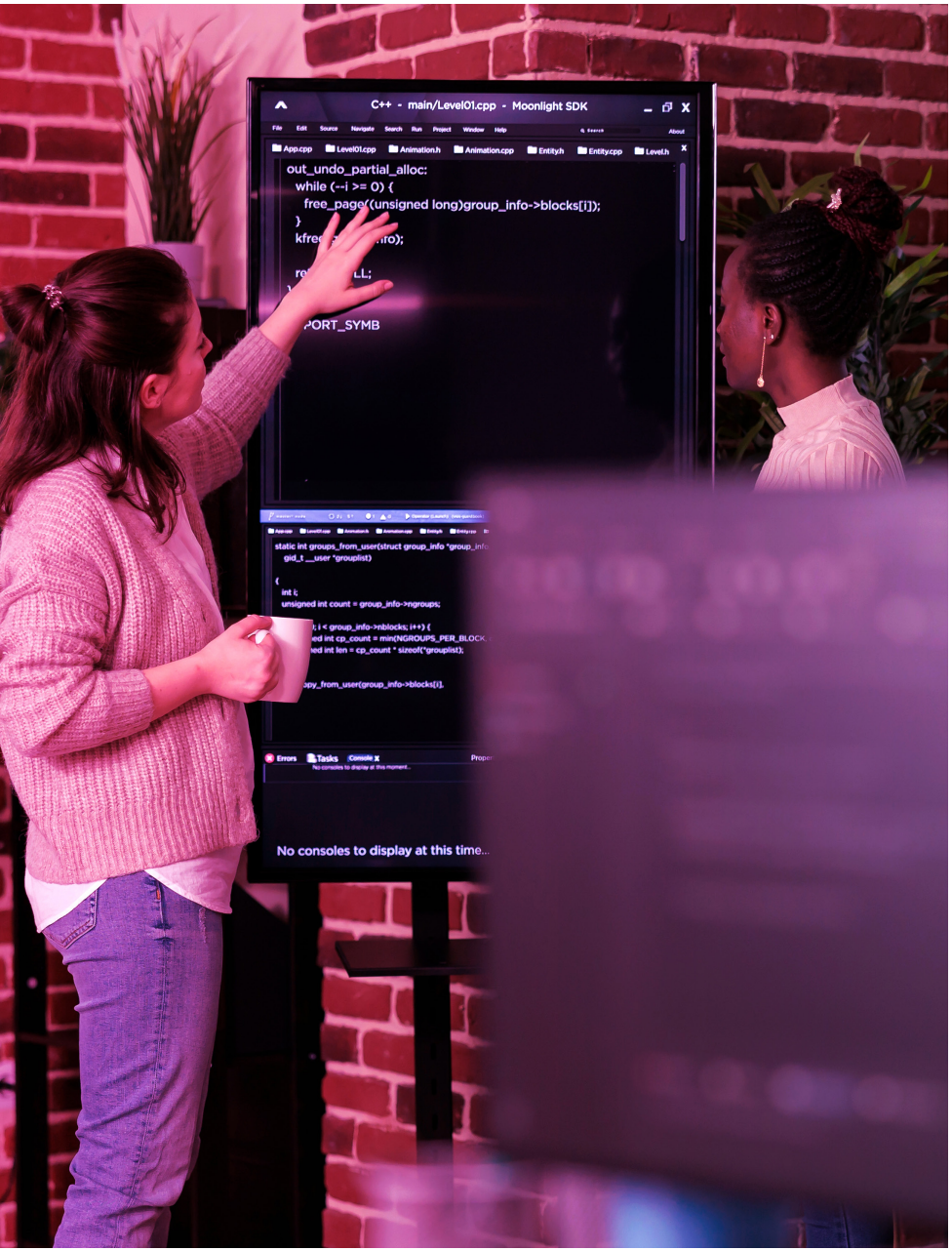
Hier bietet eine nahtlose Identitäts- und Zugriffsmanagementlösung, die in allen Bereichen Ihrer Technologie implementiert wird, eine stabile und umfassende Cyber-Lösung.

Wir helfen Ihnen dabei, Risikobereiche zu identifizieren und zu reduziere, und unterstützen Sie bei der Entwicklung kosteneffizienter Lösungen, die den Anforderungen Ihrer Unternehmensrichtlinien und -prozesse entsprechen.

Erleben Sie mehr Sicherheit, geringere Risiken und höhere Effizienz mit den auf Ihr Unternehmen zugeschnittenen Konzepten von Insight.

Dies erreichen wir indem:

- Wir Sie auf dem Weg zu Zero Trust begleiten.
- Sie einen geschäftsorientierten Ansatz für den Zugriff auf Daten und Anwendungen verfolgen.
- Wir sicherstellen, dass die richtigen Personen Zugriff auf Ihre Anwendungen und Daten haben.



Erkennung und Abwehr von Bedrohungen

Bedrohungserkennung und -abwehr sind entscheidende Komponenten einer robusten Cybersicherheitsstrategie für Unternehmen. Unternehmen stehen bei der Erkennung und Abwehr von Cyber-Bedrohungen vor zahlreichen Herausforderungen, darunter die sich ständig weiterentwickelnde Art der Angriffe, die Komplexität von IT-Softwareumgebungen und der Mangel an qualifizierten Fachkräften für Cybersicherheit.

Effektive Bedrohungserkennung erfordert Echtzeitüberwachung, Analyse von Sicherheitsereignissen und schnelle Reaktion auf Vorfälle, um die Auswirkungen von Sicherheitsverletzungen zu minimieren.

Die Sicherheitsexperten von Insight können Sie bei der Entwicklung von Lösungen zur Bedrohungserkennung und -abwehr auf verschiedenen Ebenen in allen Technologiebereichen Ihres Unternehmens zu unterstützen.

Wir entwickeln Lösungen mit fortschrittlichen Tools, Technologien und unserer Expertise als Sicherheitsberater, um Risiken zu identifizieren und zu mindern, bevor sie Ihrem Unternehmen erheblichen Schaden zufügen können. Insight nutzt Technologien wie SIEM und XDR, die von Sicherheitsanalysten ergänzt werden, um die enormen Datenmengen, die von Ihren Sicherheitstools generiert werden, zusammenzuführen, damit Sie intelligente Entscheidungen über Bedrohungen und Reaktionen in Ihrer gesamten Umgebung treffen können.

Wir helfen Ihnen dabei:

- Bedrohungen früher zu erkennen
- Risiken im gesamten Netzwerk zu reduzieren
- verwertbare Informationen über Bedrohungen zu erhalten
- Bedrohungen automatisiert abzuwehren

Menschliche Faktoren

Trotz ständiger Verbesserungen und Investitionen in die Sicherheitsinfrastruktur, -werkzeuge und -kontrollen kommt es immer wieder zu Verstößen, die nicht leicht zu erkennen und zu beheben sind. Es gibt viele spezialisierte Sicherheitskontrollen für verschiedene Arten von Bedrohhungen, von Angriffen auf Endgeräte bis hin zu Angriffen auf die Lieferkette, aber wenn man untersucht, wie diese Angriffe tatsächlich stattgefunden haben, gibt es drei Hauptgründe:

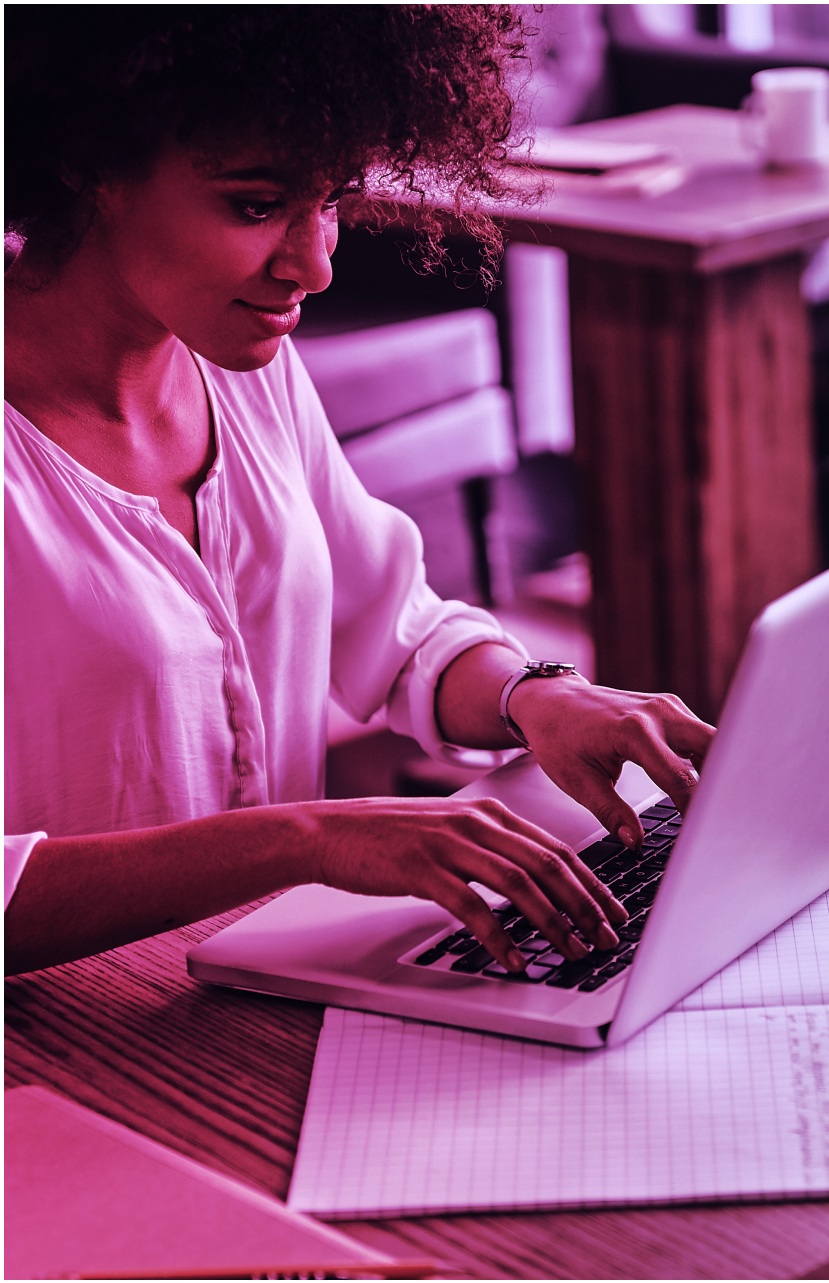
- Passwörter
- Phishing
- Patchen

IT-Teams können Technologie einsetzen, um das Risiko von Sicherheitsverletzungen zu verringern, aber Endbenutzer spielen immer eine Rolle bei der Unterstützung der Sicherheit eines Unternehmens. IT-Teams konzentrieren sich oft auf die Technologie und manchmal auf den Prozess und vergessen dabei die menschliche Seite, obwohl Menschen den Erfolg oder Misserfolg eines Projekts bestimmen können.

Mit Insight können Sie Ihre Mitarbeiterinnen und Mitarbeiter in die Lage versetzen, eine undurchdringliche erste Verteidigungslinie gegen Cyber-Bedrohungen zu bilden. Indem wir uns auf den Menschen konzentrieren, können wir Ihnen helfen, Schwachstellen direkt zu beheben, Ihre Sicherheitsposition zu stärken und Risiken zu minimieren.

Wir helfen Ihnen dabei:

- das Bewusstsein der Endbenutzer für Cybersicherheit zu erhöhen.
- Entwickler in der sicherheitsbewussten Programmierung zu schulen.
- Sicherzustellen, dass Ihre Administratoren über die erforderlichen Fähigkeiten verfügen, um einen Cyberangriff zu erkennen und darauf zu reagieren.
- das Risiko erfolgreicher Angriffe zu reduzieren.
- Kosten durch Vermeidung von Datenschutzverletzungen einzusparen.



Managed security

Die Angriffe auf Sicherheitssysteme nehmen ständig zu. Organisationen sehen sich zunehmend mit Cyber-Bedrohungen konfrontiert, die von raffinierten Hacker-Angriffen bis hin zu heimtückischen Ransomware-Angriffen reichen. Organisationen müssen komplexe regulatorische Compliance-Anforderungen erfüllen, sensible Daten schützen und den sich ständig weiterentwickelnden Cyber-Sicherheitsrisiken immer einen Schritt voraus sein. Sicherheitslösungen bieten eine Vielzahl von Warnungen und Alarmen. Zu wissen, auf welche dringend reagiert werden muss, ist der Schlüssel, um größeren Schaden von Ihrem Unternehmen abzuwenden.

All diese Herausforderungen erfordern umfassende und proaktive Cybersicherheitslösungen, um Unternehmen vor den vielfältigen und komplexen Bedrohungen zu schützen, denen sie täglich ausgesetzt sind. Cybersicherheitsbereitschaft und -Resilienz sind entscheidend für die Kontinuität und den Erfolg jedes modernen Unternehmens.

Hier kann Insight helfen – unser Team erfahrener Sicherheitsexperten steht Ihnen rund um die Uhr zur Verfügung, um Ihre Cybersicherheit durch proaktive Überwachung, Erkennung und Reaktion auf Bedrohungen mit Zugang zu den neuesten Technologien zu verbessern.

Unser Security Operations Centre (SOC) bietet zwei Managed Services an, die mit modernsten Mitteln Bedrohungen erkennen, untersuchen und darauf reagieren:

- **Managed Endpoint Detection and Response (MEDR)**
  Für Notebooks, Desktops und mobile Geräte.
- **Managed Extended Detection and Response (MXDR)**
  Kombiniert Logs und Feeds aus einer Vielzahl von Quellen, um die zuverlässigsten Informationen zu erhalten.

Unser Team aus erfahrenen Sicherheitsanalysten kombiniert KI, Threat Intelligence und Analytik, um Bedrohungen in Ihrer Softwareumgebung in Echtzeit zu erkennen und darauf zu reagieren.

Dies erreichen wir durch:

- Proaktives Bedrohungsmanagement
- Experten für Sicherheitsanalyse und Reaktion auf Vorfälle
- Zugang zu fortschrittlichen Sicherheitstechnologien
- Entwicklung von Sicherheitsstrategien und Roadmaps
- Skalierbares und kosteneffizientes Modell

So helfen wir Ihnen

Wir unterstützen Sie bei der Strategie, Implementierung und Verwaltung zukunftsfähiger IT-Sicherheitslösungen.

Assessment

- Unterstützung bei der Akkreditierung nach Branchenstandards wie ISO27001 oder NIS2
- Überprüfung Ihrer bestehenden Sicherheitskontrollen und Identifizierung von Rest-Risiken
- Erstellung einer priorisierten Roadmap, um Ihr gewünschtes Level an Sicherheit zu erreichen

Planung & Design

- Unterstützung bei der Umsetzung Ihrer Unternehmensherausforderungen in Sicherheitsprojekte
- Unterstützung und Beratung bei der Auswahl der passenden Anbieter, Produkte und Dienstleistungen
- Vorstellung von Workshops und technischem Design

Aufbau und Implementierung

- Verwirklichen Sie Ihre Pläne – vom Entwurf bis hin zu vollständig implementierten und dokumentierten Sicherheitskontrollen
- Insight betrachtet jedes Projekt im Kontext Ihrer gesamten Roadmap
- Übergabe an Ihre internen Teams zum Management oder Übergang zu unseren Managed Services

IT Operations Management

- Support-Services sorgen für optimale Sicherheit
- Managed Services, bei denen Insight die Verantwortung für Ihre Sicherheitskontrollen übernimmt

Unsere Sicherheitstechnologie-Partner

IT-Modernisierung ist Teamarbeit. Wir vereinen die Fähigkeiten von über 6.000 Software-, Hardware- und Cloud-Partnern sowie Publishern mit der umfassenden Branchenexpertise unseres Teams unter einem Dach, um marktführende Lösungen zu entwickeln, die Ihre digitale Transformation beschleunigen.

Durch die direkte Zusammenarbeit mit führenden Technologieunternehmen profitieren Sie von folgenden Vorteilen:

- Ein Ansprechpartner für den Zugang zu den neuesten Technologieprodukten und -lösungen.
- Ein Ökosystem aus kollaborativen, hochqualifizierten Teams zur Einrichtung und Verwaltung Ihrer IT-Softwareumgebung.
- Wettbewerbsfähige Preise und optimierte Vertragsverhandlungen.
- Partnerunabhängige Lösungen, die auf Ihre spezifischen Anforderungen zugeschnitten sind.

Warum sollten Sie eine Partnerschaft mit Insight eingehen?

Cybersicherheit ist komplex und erfordert einen umfassenden Ansatz, der Endbenutzer, Sicherheitsteams und Tools einbezieht. Deshalb haben wir wiederholbare Methoden und bewährte Prozesse entwickelt, die erfolgreiche Ergebnisse liefern. Unsere Experten begleiten Sie von Anfang bis Ende, was zu verbesserter Effizienz, Effektivität und strategischer Ausrichtung führt.

Wir haben:

- **über 20 Jahre Wissen und Erfahrung** im Bereich der Sicherheitstransformation
- **Intensive Partnerschaften** mit erstklassigen Anbietern
- **einen lösungsunabhängigen Ansatz,** um die besten Lösungen für Ihre Anforderungen zu finden

Member of Microsoft Intelligent Security Association

Microsoft Security | Microsoft Verified Managed XDR Solution

Cisco Partner
Advanced Security Architecture Specialized
SASE Specialized
XDR Specialized

Microsoft Solutions Partner
Security
Specialist
Cloud Security
Identity and Access Management
Information Protection & Governance
Threat Protection

Gold Microsoft Partner | Azure Expert MSP

Microsoft Solutions Partner
Microsoft Cloud

Ihre nächsten Schritte

Wenden Sie sich an Insight, um Ihre Cybersicherheits-strategie und Ihren täglichen Betrieb zu verbessern.

Angesichts der wachsenden Cybersicherheitsbedrohungen ist der Schutz Ihres Unternehmens für Kontinuität und Erfolg von entscheidender Bedeutung.

Unser umfassender Ansatz verbessert die Cybersicherheit, identifiziert und mindert Risiken, optimiert den Betrieb sowie Sicherheitskontrollen und maximiert gleichzeitig Ihre Investitionen.

Vertrauen Sie auf die bewährten Methoden und die Exper-tenberatung von Insight, um Ihre Cybersicherheitsabwehr zu stärken und die Resilienz sowie das Wachstum Ihres Unternehmens zu steigern.